Number theory is one of the oldest and most active fields of mathematics. The beauty of the subject stems from the simplicity of many of the problems to state. Number theory is, in short, the study of numbers. In particular, we are usually interested in the integers,

$$\mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, 3, \ldots \}$$

and the rational numbers,

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

One may wonder what else do we want to know about numbers; it seems, especially to nonmathematicians, that we know all there is to know about numbers. We will begin by listing a few deep problems in number theory that can be easily stated.

(1637)

**Fermat's Last Theorem**: Originally stated by Fermat, he claimed that the equation

$$x^n + y^n = z^n$$

has no solution in integers for $n > 2$. This was proven by Andrew Wiles in 1994.
have no solutions \((x, y, z) \in \mathbb{Z}^3\) with \(xyz \neq 0\) and \(n \geq 3\).

Of course, \(n = 2\) is the Pythagorean theorem. That all high school math student learn. So even in this case, we could ask for all the rational triple \((x, y, z) \in \mathbb{Q}^3\) that satisfy \(x^2 + y^2 = z^2\).

For \(n \geq 3\), this was finally proven in 1995 by Andrew Wiles, and it was beyond the course. For \(n = 3\), we will characterize all rational solutions later in the term.

**Twin Prime Conjecture:**

Prime numbers \(p_1\) and \(p_2\) are called twin primes if \(p_2 - p_1 = 2\); i.e., if \(p_1\) and \(p_1 + 2\) are both prime numbers. For example, 3 and 5, 5 and 7, 11 and 13 are all twin primes. While it is easy to show there are only many primes, it is still not known if there are only many twin primes!

**Pell's Equation:**

We would like to determine solutions \((x, y) \in \mathbb{Q}^2\).
of the equation

\[ x^2 - dy^2 = 1 \]

for \( d \in \mathbb{Z} \). It again seems like this may be an easy problem, but it turns out we must develop the notion of continued fractions to study this equation!

**Congruent Numbers:**

We say an integer \( n \) is a congruent number if there is a right triangle with \( n \) natural side lengths that have area \( n \). This is again a very simple problem to state but requires very difficult modern mathematics to solve. We will look at this problem later in the term and see how elliptic curves arise in the solution of this problem.
Quick Review of Induction:

This is really prerequisite material, but we will review an example so we are all on the same page.

Example: Prove that \( n! > n^3 \) for every integer \( n \geq 6 \).

Proof: We proceed with induction on \( n \). The base case is \( n = 6 \). Observe that

\[
6! = 720
\]

and \( 6^3 = 216 \), so indeed \( 6! > 6^3 \) for \( n = 6 \).

Assume inductively that \( k! > k^3 \) for every integer \( 6 \leq k \leq N \) for some integer \( N \). Now observe

\[
(N+1)! = (N+1)N!
\]

\[
> (N+1)N^3.
\]

We would now like to say that \( N^3 > (N+1)^3 \). To start off this were true, then we would have

\[
(N+1)! > (N+1)^3
\]

\[
> (N+1)^3
\]

and by induction we would be done. So we have reduced the problem to showing

\[
N^3 \geq (N+1)^2 \quad \text{for } N \geq 6.
\]
To see this, observe that this is equivalent to showing
\[ N^3 > N^2 + 2N + 1. \]
Now since \( N \geq 6 \), \( 6N^2 \geq 2N \) and \( N^3 > 1 \), we have \( N^3 > N^2 + 2N + 1 \) < \( N^2 + 2N^2 + N^2 = 4N^3 \).

When \( N \geq 6 \), \( N^3 = N \cdot N^2 > 6N^2 > 4N^3 \), so we have
\[ N^3 > 4N^3 > N^3 + 2N + 1 = (N+1)^2. \]

Thus, by induction we have the result. \( \square \)

Not all inductions will be as easy or as difficult as this, depending on your recipient.

Divisibility theory of the integers:

**Def:** Let \( a, b \in \mathbb{Z} \). We say \( a \) divides \( b \), and write \( a | b \)
if \( \exists c \in \mathbb{Z} \) s.t. \( b = ac \).

This is essentially the same notion you are used to from elementary school.
Thm 2.2: For $a, b, c \in \mathbb{Z}$ we have

1. $a|0$, $a|1a$, $a|a$
2. $a|1$ iff $a=\pm 1$
3. If $a|b$ and $c|d$, then $ac|bd$
4. If $a|b$ and $b|c$, then $a|c$
5. $a|b$ and $b|a$ iff $a=\pm b$
6. If $a|b$ and $b \neq 0$, then $|a| \leq |b|$
7. If $a|b$ and $c|d$, then $a|(bx+cy)$ for any $x, y \in \mathbb{Z}$.
Example: if \(\alpha I \beta\) and \(\beta I \gamma\), prove \(\alpha I \gamma\).

Proof: Since \(\alpha I \beta\), then exists \(n \in \mathbb{Z}\) s.t. \(\beta = a \cdot n\).

Similarly, since \(\beta I \gamma\), there exists \(m \in \mathbb{Z}\) s.t. \(\gamma = b \cdot m\).

Combining these, we have \(\gamma = b \cdot m = a \cdot n \cdot m\). Since \(m \in \mathbb{Z}\), we have \(\alpha I \gamma\) as claimed.

Of course, we can also divide integers that do not divide evenly into each other by considering 
	

\[\text{Thm } 2.1 \text{ (Division Algorithm): Let } a, b \in \mathbb{Z}, b > 0, \text{ then exists unique integers } q, r \text{ with } a = bq + r,\]

\[0 \leq r < b.\]

\[q = \text{quotient}, \quad r = \text{remainder}.
\]

Proof: Consider the set

\[S = \{a - nb : n \in \mathbb{Z}, a - nb \geq 0 \}.
\]

each we can show the set is nonempty, we will have a remainder at least. Then we will need to show we can choose \(n\) so that \(a - nb\) is between 0 and \(b\).
By assumption $b > 1$. We always have $1a \geq c$, so

$$a - (1a) b = a + 1a b > 0.$$ Then we have at least one positive element in $S$. We can now apply the well-ordering principle (this is a nonempty set of nonnegative integers) to conclude there is a smallest element $r \in S$. It remains to show that $r < b$.

Let $q$ be such that

$$a - bq = r.$$ 

Suppose $r \geq b$. Then we have $a - bq \geq b$

$$\Rightarrow a - b(q+1) \geq 0 \quad \text{and} \quad a - b(q+1) < r$$ which contradicts the minimality of $r$. Thus, $0 \leq r < b$.

To finish the proof, we only need to show $r$ and $q$ are unique. Suppose $a = bq + r$, $0 \leq r < b$ and $a = bq' + r'$, $0 \leq r' < b$. Substituting the two we obtain

$$b(q-q') = r - r'.$$

If $q \neq q'$, then taking absolute values we obtain

$$b|q - q'| = |r - r'|.$$ 

However, if $q = q'$, then $|q - q'| = 0$ and since $0 \leq r < b$ and
0 ≤ r < b, we must have \(|r - r'1| < b|q - q'|\). 

Thus \(q = q' = |r - r'1| = 0 \Rightarrow r = r'\). Thus \(q\) and \(r\) are unique.

Let's look at an example to how the division algorithm can be used to help us prove general statements.

**Example:** Prove that the cube of any integer is of the form \(9k, 9k+1\) or \(9k+2\) for some integer \(k\).

**Proof:** Let \(n\) be an integer. Applying the division algorithm with \(b = 9\), we have

\[n = 9q + r, \quad 0 ≤ r < 9.\]

Now we only need to cube each of the possibilities:

- \(r = 0\): \(n = 9q\) : \(n^3 = 9(9q^3) = 9k.\)
- \(r = 1\): \(n = 9q + 1\) : \(n^3 = 729q^3 + 243q + 27q^3 + 27q + 1 = 9(81q^3 + 27q^3 + 3q) + 1\)
- \(r = 2\): \(n = 9q + 2\) : \(n^3 = 9(81q^3 + 54q^3 + 12q) + 8\)
- \(r = 3\): \(n = 9q + 3\) : \(n^3 = 9(81q^3 + 81q^3 + 27q^3 + 3)\)
- etc..
2.2 The Greatest Common Divisor:

The greatest common divisor of two integers is another concept familiar from elementary school and is exactly what the name suggests; it is the largest integer that divides with no remains into both integers. Formally,

**Def:** Let \( a, b \in \mathbb{Z} \) with \( a \neq 0 \) and \( b \neq 0 \). The greatest common divisor of \( a \) and \( b \), written \( \gcd(a,b) \), is the positive integer \( d \) satisfying:

- \( d \) divides both \( a \) and \( b \)
- If \( e \) divides both \( a \) and \( b \), then \( e \leq d \).

**Example:** The gcd of 14 and 21 is 7.

The SAGE command for calculating the GCD is \( \gcd(a,b) \).

We will see in the next section how to calculate the GCD by an efficient algorithm, but it is good to be able to use the computer as well!

The following facts are elementary and are useful:
One of the nice properties of the gcd is that if \( d = \gcd(a, b) \),

\[ \exists m, n \in \mathbb{Z} \text{ s.t.} \]

\[ d = am + bn. \]

We say \( d \) is a \underline{linear combination} of \( a \) and \( b \).

**Thm 2.3:** Let \( a, b \in \mathbb{Z} \) \( \neq 0 \). Then \( \exists m, n \in \mathbb{Z} \) s.t.

\[ \gcd(a, b) = am + bn. \]

**Proof:** This proof has a similar flavor to the previous one a

the division algorithm. Let

\[ S = \{ am + bn | am + bn \geq 0, m, n \in \mathbb{Z} \}. \]

It is clear that \( S \neq \emptyset \), for example \( a^0 \in S \) if \( a \neq 0 \)

and \( b^0 \in S \) if \( b \neq 0 \), since \( a^0 = a \cdot 0 + b \cdot 0 \) and similarly

for \( b^0 \). Now \( S \) is a nonempty set of nonnegative integers, so

has a minimal element \( d \) by the well-ordering principle.

By the definition of \( S \) we have \( \exists m, n \in \mathbb{Z} \) s.t.

\[ d = am + bn. \]

This does not prove \( d \) is the gcd though! We prove \( d \) is

the gcd. The first step is to show \( \gcd(a, b) \) and \( \gcd(b, a) \). Use the

division algorithm to write

\[ a = dq + r, \quad \text{with } 0 \leq r < d. \]
\[ r = a - dq \\
= a - (am + bn)q \\
= a[(1 - mq) + b(-nq)]. \]

Thus, either if \( d|x \), then \( r > 0 \) and \( r < d \) and so \( r \in S \). But this contradicts the minimality of \( d \), so we must have \( r = 0 \) and \( d | a \). Similarly for \( d | b \).

This gives \( \theta \) of the definition.

\[ r > 0 \]

Suppose \( d | a \) and \( d | b \). Then we have \( d | (am + bn) \), so \( d | n \).

In particular, \( d | 1 \). Thus, \( e \leq d \) and \( e \) is an even.

One should observe here that we have shown \( m \) and \( n \) exist, but not how to find them! This happens often in mathematics when we can show something must exist but the proof does not show us how to find it! Fortunately in this case there is an algorithm that allows us to find \( m \) and \( n \).

The command in SAGE to find \( m \) and \( n \) is given by:

\[ d, \ m, n = xgcd(a, b). \]

This will initially return nothing, but stores the value
of $m$ and $n$. Then just type $m \div n$ to get the result. Alternatively, type

d, m, n = \text{gcd}(a, b) \div m; n.

**Def:** Let $a, b \in \mathbb{Z}$ and $ab \neq 0$, we say $a$ and $b$ are relatively prime if $\text{gcd}(a, b) = 1$.

**Example:** 15 and 28 are relatively prime.

We saw before that if $d = \text{gcd}(a, b)$, then for $m, n \in \mathbb{Z}$ there exists $m, n \in \mathbb{Z}$ s.t. $d = am + bn$. This does NOT mean that $d = \text{gcd}(a, b)$. For example, $\text{gcd}(3, 2) = 1$, but we can write

$$15 = 3(2) + 3(-15).$$

So having a linear combination is NOT enough to determine the gcd unless $\text{gcd}(a, b) = 1$. 
**Theorem 2.4:** Let $a, b \in \mathbb{Z}$, not both 0. Then $a$ and $b$ are relatively prime iff there exist $m, n \in \mathbb{Z}$ such that
\[1 = am + bn.\]

**Proof:** One direction is already done, namely if $\gcd(a, b) = 1$ then we know such $m$ and $n$ exist. Suppose now that we have $m, n \in \mathbb{Z}$ such that
\[1 = am + bn.\]

We wish to show $1 = \gcd(a, b)$. Suppose $d = \gcd(a, b)$. Then $d$ divides both $a$ and $b$, so $d \mid (am + bn)$, i.e., $d \mid 1$. Thus, $d = 1$ and we are done. \[\square\]

**Corollary:** If $\gcd(a, b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

**Proof:** Exercise.

**Corollary:** if $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.

Observe that this corollary is not true if $\gcd(a, b) \neq 1$. For example, $6 \mid 12$ and $4 \mid 12$, but $6 \cdot 4 \neq 12 \cdot 12$. 


Proof: Since \( a \mid b \) and \( b \mid c \), there exist integers \( m, n \) such that
\[
c = am \quad \text{and} \quad c = bn.
\] We use that \( \gcd(a, b) = 1 \) to conclude that there exist integers \( r, s \) such that
\[
r = ar + bs. \tag{1}
\] Multiplying both sides of (1) by \( c \) we have
\[
c = acr + bcs.
\] Now use our initial equations \( c = am \) and \( c = bn \) to conclude:
\[
c = a(br)r + b(ans) = ab(nr + ms).
\] Thus, \( ab \mid c \). \( \Box \)

The following result, which is easy to prove, will be used heavily.

**Theorem 2.5 (Euclidean Lemma):** If \( ab \mid c \) and \( \gcd(a, b) = 1 \), then \( ab \mid c \).

**Proof:** As before, \( \exists m, n \in \mathbb{Z} \) so that
\[
1 = am + bn.
\] Multiplying by \( c \):
\[
c = acm + bcn.
\] Use now that \( ab \mid c \) to get \( \exists r \in \mathbb{Z} \) so that \( bc = ar \).
Then we have
\[ c = ac + bn \]
\[ = ac + an \]
\[ = a(c + bn) , \]

Thus, a|c. \[ \square \]

**Example:** The sum of the squares of two odd integers cannot be a perfect square.

**Proof:** Let \( m = 2k + 1 \) and \( n = 2l + 1 \) be two odd integers. Then

\[ m^2 + n^2 = (4k^2 + 4k + 1) + (4l^2 + 4l + 1) \]
\[ = 4(k^2 + k + l^2 + l) + 2 \]
\[ = 2(2k^2 + k + l^2 + l + 1) , \]

an odd integer.

Thus, we got 2 times an odd integer. If this were a perfect square, we would need another 2! \[ \square \]
Q.4 The Euclidean Algorithm:

We now formalize this idea by proving that for every pair of integers \(a, b\), \(a \neq b\), there exist integers \(m, n\) so that

\[
gcd(a, b) = am + bn.
\]

Unfortunately, our proof of this fact did not yield a method for determining \(m\) and \(n\). The Euclidean algorithm is a method for determining \(m\) and \(n\).

Assume wlog that \(a \geq b > 0\). The division algorithm allows us to write

\[
a = bq + r, \quad 0 \leq r < b.
\]

If \(r = 0\), then \(b|a\) and \(gcd(a, b) = b\) and \(b = a \cdot 0 + b \cdot 1\).

So we are done. Suppose \(r \neq 0\). Then divide \(r\) into \(b\):

\[
b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1.
\]

If \(r_2 = 0\) we stop, if not we divide \(r_2\) into \(r_1\):

\[
r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2.
\]

Continuing in this pattern we obtain a decreasing sequence of positive integers \(b > r_1 > r_2 > r_3 \ldots\)
Thus, for some \( n \) we must have \( r_n = 0 \).

**Lemma:** If \( a = bq + r \), then \( \text{gcd} (a, b) = \text{gcd} (b, r) \).

**Proof:** Let \( d = \text{gcd} (a, b) \), \( e = \text{gcd} (b, r) \). Since \( b \) and \( c \mid r \), \( c \mid a = bq + r \). Thus \( c \mid d \) because \( c \) is a common divisor of \( a \) and \( b \). Similarly, \( d \mid a \) and \( d \mid b \), so \( d \mid (a - bq) = r \). Thus \( d \mid e \) and so \( d = e \).

We can apply this lemma to our process above to obtain

\[
\text{gcd} (a, b) = \text{gcd} (b, r) \\
= \text{gcd} (r, c) \\
= \cdots = \text{gcd} (r_{n-1}, 0) = r_n.
\]

Thus, the last nonzero remainder is the gcd! This gives an alternative to computing prime factorizations to compute gcd's! (Much more efficient!)

To obtain the linear combination, we can back-substitute.
Suppose our equations are
\[ a = bq_1 + r_1, \]
\[ b = r_1 q_2 + r_2, \]
\[ r_1 = r_2 q_3 + r_3, \]
\[ \vdots \]
\[ r_{n-2} = r_{n-3} q_n + 0. \]

We can back substitute to obtain the desired expression.

\[ r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \]

\[ \Rightarrow r_{n-1} = r_{n-3} - q_{n-1} r_{n-2} \] (5)

Now use the previous equation

\[ r_{n-4} = r_{n-3} q_{n-2} + r_{n-2} \]

to replace \( r_{n-2} \) in (5)

\[ (5) \quad r_{n-1} = r_{n-3} - q_{n-1} (r_{n-4} - r_{n-3} q_{n-2}). \]

Next we replace \( r_{n-3} \) and so on until we have \( a \) and \( b \) left. This is best seen with an example.
Example: Compute $\gcd(348, 1532)$ and determine $m$ and $n$ so that

$$\gcd(348, 1532) = 348m + 1532n.$$ 

Solution:

1532 = 348(4) + 140

348 = 140(2) + 68
140 = 68(2) + 4
68 = 4(17) + 0

Thus, $\gcd(348, 1532) = 4$.

Write

4 = 140 + 68(-2).
68 = 348 + 140(-2)
140 = 1532 + 348(-4).

Back substitution:

① 4 = 140 + (348 + 140(-2))(-3)

= 140 + 140(4) + 348(-3)

= 140(\phi) + 348(-\phi)

② 4 = 140(\phi) + 348(-\phi)

4 = (1532 + 348(-4))(\phi) + 348(-\phi)

4 = 1532(\phi) + 348(-\phi).
Thus, \( m = -32 \) and \( n = 5 \).

As was noted last time, the SAGE command for this is

\[ x \in \mathbb{Z}, m, n = x \gcd(a, b) . \]

The text also gives a short treatment of least common multiple. You should read this, but it is not really different and we won't discuss it in class, unless it becomes necessary.

Essentially, one proves \( \text{lcm}(a, b) = \frac{ab}{\gcd(a, b)} \), and so one can reduce any thing about the lcm back to questions about the gcd.
Now that we have seen that the gcd of \(a\) and \(b\) can be written as a linear combination of \(a\) and \(b\), we are in a position to study the solutions to the equation

\[
ax + by = c.
\]

This is the first real "number theory" of the course, though it will be brief and not real difficult. In general, a diophantine equation is an equation in a finite # of variables that we wish to solve with integer values.

In some cases there will be finitely many or no solutions, in other cases there may be infinitely many solutions.

The case with which we will deal with \(ax + by = c\) should not lead you to believe diophantine equations are easy to study in general. Recall \(x^n + y^n = z^n \in \mathbb{Z}\) in a diophantine equation and showing it has no nontrivial solutions for \(n \geq 3\) was very difficult.
Let $d = \gcd(a, b)$. If the equation $ax + by = c$ has a solution with $x, y \in \mathbb{Z}$, then we must have $d | c$ since $d | a$ and $d | b$ so $d | (ax + by)$. So immediately we see that if $d | c$, there are no integer solutions to $ax + by = c$.

Now suppose $d \nmid c$. We know $\exists m, n \in \mathbb{Z}$ s.t.

$$d = am + bn.$$ \hspace{1cm} (1)

$$d \nmid c \Rightarrow s \in \mathbb{Z} \text{ s.t. } c = ds. \text{ Thus,}$$

$$c = ds = am + bn s.$$ \hspace{1cm} (2)

So we have $x = ms$, $y = ns$ is a solution to the Diophantine equation.

We have easily determined when the equation $ax + by = c$ has integer solutions. The next question is if we can determine all the integer solutions when they exist. One way to accomplish such a goal is to give all solutions in terms of a set of known solutions. Suppose $x_0, y_0$ is a solution to the equation.

$$ax + by = c.$$ \hspace{1cm} (3)

Let $x_1, a x_0, y_1$ be another solution. We have

$$a x_1 + by_1 = c = ax_0 + by_0.$$
We can write

$$a(x_0 - x_1) = b(y_1 - y_0).$$

Let $d = \gcd(a, b)$. Then exists $r, s \in \mathbb{Z}$ s.t. $dr = a$, $ds = b$.

We claim that $\gcd(r, s) = 1$. Suppose $\gcd(r, s) > 1$. Then

either $r$ and $s$ share a common divisor $d$, and $d | a$ and $d | b$.

Thus, $\gcd(r, s) = 1$.

Write

$$rd(x_0 - x_1) = ds(y_1 - y_0).$$

$$\Rightarrow$$

$$r(x_0 - x_1) = s(y_1 - y_0).$$

Since $\gcd(r, s) = 1$ and $r \mid s(y_1 - y_0)$, we can apply Euclid's lemma to conclude $r \mid (y_1 - y_0)$. So $t \in \mathbb{Z}$ s.t.

$$y_1 - y_0 = rt.$$

i.e.,

$$y_1 = y_0 + rt = y_0 + \left(\frac{a}{d}\right)t.$$

Substituting back in,

$$r(x_0 - x_1) = srt.$$

i.e.,

$$x_0 - x_1 = st.$$

Thus,

$$x_1 = x_0 - \left(\frac{b}{d}\right)t.$$

So we have shown that given a solution $x_0, y_0$, we can
Write any other solution in the form

\[ x_1 = x_0 - \left( \frac{b}{a} \right) t \quad t \in \mathbb{Z} \]
\[ y_1 = y_0 + \left( \frac{a}{d} \right) t \]

It is easy to check by simple substitution that for any \( t \in \mathbb{Z} \), \((x_0, y_0)\) a solution of \( ax + by = c \) then

\[ x_1 = x_0 - \left( \frac{b}{a} \right) t \]
\[ y_1 = y_0 + \left( \frac{a}{d} \right) t \]

is also a solution. Thus we have found all solutions in terms of \((x_0, y_0)\). We summarize with the following theorem.

**Thm 2.9:** The linear Diophantine equation \( ax + by = c \)

iff \( d = \gcd(a, b) \) \( | c \). If \((x_0, y_0)\) is a solution of the equation, then all other solutions are of the form

\[ x = x_0 - \left( \frac{b}{d} \right) t \]
\[ y = y_0 + \left( \frac{a}{d} \right) t \]

for \( t \in \mathbb{Z} \).

Beside being of interest because we like to find integer solutions to the Diophantine equations in general, linear Diophantine equations
We can apply the Euclidean alg. (or just inspection in this case) to obtain

\[ 5(61) + 3(21) = 2. \]

Thus, \[ 100 = 5(-100) + 3(300). \]

At \( x = -100, \ y = 300 \)

in a solution. However, we can't have a negative \( x \) or \( y \) in \( \mathbb{Z} \), so we need to find a positive solution. We need

\[ x = -100 - 3t > 0 \]
\[ y = 300 + 5t > 0 \]

i.e.,
\[ t \leq \frac{-100}{3} \]
\[ t < \frac{-100}{5} \]

And
\[ 200 > -5t \]

i.e.,
\[ -\frac{200}{5} < t \]

i.e.,
\[ -40 < t < -33.3 \]

Thus, \( t \) can be \(-39, -38, -37, \ldots, -34\).

This gives \( x = 17, 14, \ldots, 2 \)
\[ y = 5, 10, \ldots, 30 \]

and \( z = 78, 76, \ldots, 68 \).
also often show up in word problems.

**Example:** One hundred bushels of grain are distributed among 100 persons in such a way that each man receives 3 bushels, each woman 2 bushels, and each child \( \frac{1}{2} \) bushel. How many men, women, and children are there in the village?

**Solution:** Let \( x = \# \) men, \( y = \# \) women, \( z = \# \) children.

Then we have 3 unknowns and 2 equations:

\[ x + y + z = 100 \]  \( (1) \)

and

\[ 3x + 2y + \frac{1}{2}z = 100 \]  \( (2) \)

We can remove \( z \) from equation (2):

\[ z = 100 - x - y \]

so

\[ 3x + 2y + \frac{1}{2} (100 - x - y) = 100 \]

i.e.

\[ 2.5x + 1.5y = 50 \]  \( (5) \)

Clear the denominators:

\[ 5x + 3y = 100 \]

Since \( \gcd(5,3) = 1 \) and \( 1 \mid 100 \), we have a solution to this equation.
3.1 The Fundamental Theorem of Arithmetic:

**Def:** An integer $p > 1$ is called a **prime number** if the only divisors of $p$ are 1 and $p$. An integer $n > 1$ that is not prime is said to be **composite**.

The important thing about prime numbers as we will see in a minute, is that they are the building blocks of all the numbers! So by understanding primes, we can often understand general properties.

**Example:** $2, 3, 5, 7, 11, 13, \ldots, 17419, \ldots, 132291, \ldots$

**Aside:** To compute the $n$th prime number using SAGE, one uses the command `nth_prime(n)`.

So for example, `nth_prime(3) = 5`.

One can also compute the next prime after any given number, with the command `next_prime(n)`.

For example, `next_prime(12345) = 12347`.

The following theorem is an important property of prime numbers.
In fact, this theorem could be used as the definition of prime and often is in a more abstract setting.

**Thm 3.1:** If $p$ is prime and $pl_a$, then $pl_a = pl_b$.

**Proof:** Suppose $pl_b$. Then $pl_a = pl_b$. If $pl_a$ we are done so assume $pl_b$. We need to show that $pl_b$. However, since $p$ is prime and $pl_a$, we must have $gcd(a, p) = 1$. Euclid's lemma then gives that $pl_b$.

To see this can actually be used as the definition, we must show that if $p > 1$ and whenever $pl_a$ then $pl_a = pl_b$, then there are no positive divisors of $p$ other than $1$ and $p$.

Let $1 < m < p$ be a divisor of $p$. Then $3m + 2 < mn = p$. Necessarily we have $1 < m < p$ as well. Then $p | mn$ since $pl_p$, and by assumption $pl_m$ or $pl_n$. However, since $1 < m, n < p$, we must have $p = m$ or $p = n$. Thus the only divisors of $p$ are $1$ and $p$. This shows Thm 3.1 could be taken as the definition of prime and then we would have a theorem that stated the only divisors of a prime are $1$ and $p$.

This is how one defines prime ideal in abstract algebra.
The following 3 result are easily corollaries.

**Corollary 3.1.1:** If \( p \) is a prime and \( p \mid a \cdot s \cdot \cdots \cdot a_n \),
then \( p \mid a_i \) for some \( 1 \leq i \leq n \).

**Corollary 3.1.2:** If \( p, q, \ldots, q_n \) are all primes and \( p \mid q_1 \cdots q_n \),
then \( p = q_i \) for some \( 1 \leq i \leq n \).

We now show that primes are in fact the building blocks of all integers.

**Theorem 3.2 (The Fundamental Theorem of Arithmetic):** Every positive integer \( n > 1 \) can be written as a product of primes. This factorization is unique up to reordering the primes.

**Proof:** Suppose the smallest integer \( n \) with no prime factors is \( n > 1 \).

Observe that 2 is prime so it clearly the product of primes. We proceed by induction. Suppose that all integers \( 2 \leq n \leq N \) are the product of primes. Consider \( n+1 \). If \( n+1 \) is prime we are done. Suppose \( n+1 \)
is not prime. Then \( \exists a, b \in \mathbb{Z} \) with \( 2 \leq a, b \leq N \)
so that \( N = ab \), we can apply our induction hypothesis to obtain a prime factorization of \( a \) and \( b \). But this in turn gives a prime factorization of \( N \). Thus, by induction we see all integers \( \geq 1 \) have a prime factorization. It remains to show uniqueness.

Let \( n = p_1 \cdots p_r = q_1 \cdots q_s \) be two prime factorizations of \( n \). We wish to show \( p_1 \cdots p_r = q_1 \cdots q_s \).

Why we can assume \( p_1 \leq p_2 \leq \cdots \leq p_r \) and \( q_1 \leq q_2 \leq \cdots \leq q_s \).

Observe that \( p_i \mid q_i \) and \( p_i = q_j \) for some \( 1 \leq j \leq s \). This implies \( p_i \mid q_i \). However, we can play the same game to get \( q_i \mid p_i \) for some \( 1 \leq i \leq r \), i.e.,

\( q_j \mid p_i \). Thus, \( p_i = q_j \). Now we can cancel to arrive at \( p_{i_0} \cdots p_{i_r} = q_{j_0} \cdots q_{j_s} \). We can continue this way.

If \( r < s \), then we eventually obtain \( 1 = q_{j_n} \cdots q_{j_s} \), #.

Then \( r = s \). Here we get \( s = r \) and so \( r = s \). Then we are done.

\((\mathbb{Z}^\times_n)\)) example when this fails!

We can write our prime factorization in a canonical form as \( N = p_1^{e_1} \cdots p_r^{e_r} \) with \( p_1 < p_2 < \cdots < p_r \) and
Then: Let \( p \) be a prime \#. Then \( \sqrt{p} \) is irrational, i.e.,
\[
\sqrt{p} \not\in \mathbb{Q}.
\]

Proof: Suppose \( a, b \in \mathbb{Q} \) with \( \sqrt{p} = \frac{a}{b} \). Then we can assume \( \gcd(a, b) = 1 \). Then \( a^2 = pb^2 \). Thus \( pla^2 \) and hence \( pla \). Thus \( \exists a, \text{s.t.} \ a = pa \). Rearranging our equation we obtain \( p^3 a^2 = pb^2 \), i.e., \( pa^3 = b^3 \). But then \( pb^3 = a \). Thus, \( pla \) and \( plb \Rightarrow pl \gcd(a, b) = 1 \). Thus \( \sqrt{p} \not\in \mathbb{Q} \). \( \Box \)

The next natural question is now that we know what primes are, how many are there?

Let \( x \) be a real number. The function \( \pi(x) \) counts how many primes there are less than \( x \), i.e.,
\[
\pi(x) = \# \{ p: p \leq x, \ p \text{ prime} \}.
\]

You will see what this function behaves like for large values of \( x \) in the homework. A couple sample values are
\[ \pi(10) = 4 \]
\[ \pi(50) = 15 \]
\[ \pi(1000) = 46 \]

One can check whether an integer is prime in SAGE using the command `is_prime(n)`. If \( n \) is prime, this will return `true`; it will return `false` otherwise.

As is probably already known by all of you, there are infinitely many primes. We give a few proofs of this fact.

**Thm:** There are infinitely many primes.

**Proof:** Suppose there are only finitely many primes, \( p_1, \ldots, p_n \). Consider the integer \( N = p_1 \cdots p_n + 1 \). The fundamental theorem of arithmetic implies there must be a prime that divides \( N \). Thus, \( p_j \mid N \) for some \( 1 \leq j \leq n \). But we also have that \( p_j \mid p_1 \cdots p_n \), and as \( p_j \mid 1 \), \( p_j \neq 1 \). Thus there must be infinitely many primes.
Proof: Suppose there are only finitely many primes

\[ p_1, \ldots, p_n. \]

Consider an integer

\[ N = p_1 \cdots p_n + p_1 p_2 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}. \]

The fundamental theorem of arithmetic implies there is a prime \( p \mid N \). Then, for \( j \geq 2 \), \( j \mid N \) s.t. \( p_j \mid N \).

But \( p_j \not\mid N \).

Wlog assume \( j = 2 \). Then \( p_1 \mid (p_2 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}) \)
and \( p_1 \mid N \Rightarrow p_1 \mid p_2 \cdots p_n, \) \( \therefore \) there are infinitely many primes.

The last proof we will give has a different flavor, though it relies on the fundamental theorem of arithmetic as well. The Riemann zeta function is defined by

\[ \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \]

At times this function has analytic continuation so that \( s \in \mathbb{C} \) with a pole at \( s = 1 \). If you are unfamiliar with complex analysis, just recall from calculus that

\[ \zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n}, \]

always but \( \zeta(s) \) converges for \( s > 1 \), \( s \in \mathbb{R} \).
We have

\[ S(5) = \lim_{n \to \infty} \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots \]

We can use the fundamental theorem to write

\[ S(5) = \prod_{p} (1 - \frac{1}{p^5})^{-1} \]

To get an idea why this is true, we start writing out the first few terms:

\[ (1 - \frac{1}{3^5})^{-1} (1 - \frac{1}{3^5})^{-1} (1 - \frac{1}{3^5})^{-1} \cdots \]

We observe the geometric series: \( \frac{1}{1-x} = \sum_{n=0}^{\infty} x^n \), so

\[ (1 - \frac{1}{3^5})^{-1} = \frac{1}{1 - \frac{1}{3^5}} = \sum_{n=0}^{\infty} \frac{1}{3^{5n}} = \left( \frac{3^5}{3^5 - 1} + \frac{1}{3^5} + \frac{1}{3^{10}} + \cdots \right) \]

So we have

\[ (1 - \frac{1}{3^5})^{-1} (1 - \frac{1}{3^5})^{-1} \cdots \]

\[ = \left( 1 + \frac{1}{3^5} + \frac{1}{3^{10}} + \cdots \right) \left( 1 + \frac{1}{3^5} + \frac{1}{3^{10}} + \cdots \right) \cdots \]

\[ = \frac{1}{3^5} + \frac{1}{3^{10}} + \cdots \]

\[ + \frac{1}{3^{10}} + \frac{1}{3^{15}} + \cdots \]

\[ + \frac{1}{3^{15}} + \frac{1}{3^{20}} + \cdots \]

So these two terms give all the \( \frac{1}{h^5} \) with \( n = 2^m \cdot 3^r \).
for \( u, v \in \mathbb{Z} \). Continuing in this way we get the result that

\[
\zeta(s) = \prod_{\rho} (1 - \frac{1}{\rho^s})^{-1}.
\]

**Proof:** Suppose there are only finitely many primes \( p_1, \ldots, p_n \). Then we have that

\[
\zeta(s) = (1 - \frac{1}{p_1^s})^{-1} \cdots (1 - \frac{1}{p_n^s})^{-1}.
\]

In particular, \( \zeta(s) \) is a finite product. But then \( \zeta(s) \) must be a #. This contradicts that \( \zeta(s) \) is a divergent series. This means there must be only finitely many primes.

Do we now have several ways to show that an infinitely many primes? What about the sum

\[
\sum_{p \text{ prime}} \frac{1}{p} ?
\]

We know this is smaller than the divergent harmonic series, but does it converge or diverge? It turns out it diverges!
In your homework you will prove this using §5.1. Here we will actually get a bound on the series

\[ \sum_{p \leq y} \frac{1}{p} \]

for \( y \in \mathbb{N}. \)

**Thm.** For every \( y \in \mathbb{N}, y \geq 2, \)

\[ \sum_{p \leq y} \frac{1}{p} > \log \log y - 2. \]

Observe that once we have shown this, letting \( y \to \infty \) gives that the series \( \sum_{p \leq y} \frac{1}{p} \) diverges. This is a much stronger result though because it tells how fast the series is growing. (Very slowly!)

Note that this series diverging gives yet another proof that there are only many primes.

**Proof:** Let \( y \in \mathbb{N}, y \geq 2. \) Let \( N \) be the set of integers whose prime factorization contain only primes, \( \leq y. \)

There are only finitely many primes \( p \) so as we may rearrange the summation

\[ \sum_{n \in N} \frac{1}{n}. \]
\[ \sum_{n \in \mathbb{N}} \frac{1}{n} \leq \prod_{p \in \mathbb{P}} \left( 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) \]

(just like above!) If \( n \) is not, then clearly \( n \in \mathbb{N} \) and so 

\[ \sum_{n \in \mathbb{N}} \frac{1}{n} \] 

includes the sum \( \sum_{n \leq y} \frac{1}{n} \). We may apply

the integral test from calculus.

\[ \int_{1}^{\frac{1}{y}} \frac{1}{x} \, dx \]

\[ \log(N+1) \]

to conclude

\[ \sum_{\mathbf{N} \in \mathbb{N}} \frac{1}{n} > \int_{1}^{\frac{1}{y}} \frac{1}{x} \, dx = \log(N+1) \geq \log_{\mathbb{N}} \]

when \( N \) is the largest integer \( y \), i.e., \( N \leq y < N+1 \).

Thus, \( \sum_{n \in \mathbb{N}} \frac{1}{n} > \log_{\mathbb{N}} \)

Thus, we have

\[ \prod_{p \in \mathbb{P}} \left( 1 - \frac{1}{p} \right) = \prod_{p \in \mathbb{P}} \left( 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) \]

\[ = \prod_{p \in \mathbb{P}} \sum_{n \in \mathbb{N}} \frac{1}{n} > \log_{\mathbb{N}} \]

Claim: \( e^{\log x} \geq (1 - x)^{-1} \) for all \( 0 \leq x \leq 1/2 \).
**Proof:** We show that if \( f(v) = e^{v + v^2} (1 + v) \), then \( f(v) > 1 \) for all \( 0 \leq v \leq \frac{1}{2} \). \( f(0) = 1 \), so we are done if we show \( f \) is an increasing function. Then

\[
f'(v) = -e^{v + v^2} + (1 + v)(1 + 2v)e^{v + v^2}
\]

\[
= v(1 - 2v)e^{v + v^2} > 0
\]

for \( 0 \leq v \leq \frac{1}{2} \). \( \Box \)

Let \( v = \frac{1}{p} \). Then \( e^{\frac{1}{p} + \frac{1}{p^2}} \geq (1 - \frac{1}{p})^{-1} \).

\[
\prod_{p \in \mathbb{P}} e^{\frac{1}{p} + \frac{1}{p^2}} > \prod_{p \in \mathbb{P}} (1 - \frac{1}{p})^{-1} > \log y. \quad (\ast\ast)
\]

But \( \prod_{p \in \mathbb{P}} e^{\frac{1}{p} + \frac{1}{p^2}} = e^{\sum_{p \in \mathbb{P}} (\frac{1}{p} + \frac{1}{p^2})} \),

so taking logs of both sides \( (\ast\ast) \) we have

\[
\sum_{p \in \mathbb{P}} (\frac{1}{p} + \frac{1}{p^2}) > \log y \log \log y
\]

i.e.,

\[
\sum_{p \in \mathbb{P}} \frac{1}{p} + \sum_{p \in \mathbb{P}} \frac{1}{p^2} > \log \log y.
\]

However, we have

\[
\sum_{p \in \mathbb{P}} \frac{1}{p^2} < \sum_{n=2}^{\infty} \frac{1}{n^2} < \int_{1}^{\infty} \frac{dy}{y^2} = 1.
\]

Thus,

\[
\sum_{p \in \mathbb{P}} \frac{1}{p} > \log \log y - 1. \quad \Box
\]
**Theorem:** The $n$th prime $p_n$ satisfies $p_n < 2^{2^n-1}$ for $n > 2$.

**Proof:** We proceed by induction on $n$. The case $n = 2$ is clear, as $n = 2$ gives $p_2 = 3$ and $2^{2^2-1} = 2^3 = 8$. Assume the statement is true for $2 \leq n < N$ for some integer $N$. Recall when we showed there are infinitely many primes that there is a prime $p$ with $p > p_j$ for $1 \leq j < N$ and $p | p_1 \cdots p_{N+1}$. Since $p_{N+1}$ is the next prime after $p_N$, we must have $p_{N+1} \leq p$.

Thus, $p_{N+1} \leq p_1 \cdots p_{N+1}$. Now apply the inductive hypothesis:

$$p_{N+1} \leq 2 \cdot 2^3 \cdots 2^{2^{N-1}} + 1$$

$$= 2^{1+3+ \cdots + 2^{N-1}} + 1$$

$$= 2^{2^{N-1}} + 1$$

$$\leq 2^{2^{N-1}} + 2^{2^{N-1}} - 1$$

$$= 2^{2^{N-1}}.$$ 

Thus, by induction we have $p_n \leq 2^{2^{2^{n-1}}}$ for all $n > 2$. However, we know for $n > 2$ that $p_n$ is odd, so it cannot be a power of 2. Thus $p_n < 2^{2^{2^{n-1}}}$.
Proof: Let $x \in \mathbb{N}$ with $x > 2$. Choose $k \in \mathbb{N}$ so that

\[2^k \leq x < 2^{k+1}.
\]
This is clearly possible.

Our previous result shows that there are at least $k+1$ prime numbers less than $2^k$, thus $\pi(x) \geq k+1$. The logarithm is an increasing function, so

\[
\log x < \log 2^{2^k}
\]

\[
= 2^k \log 2
\]

\[
= 2^k \cdot 1.0792
\]

\[
< 2^k.
\]

i.e., $\log x < 2^k$. Thus,

\[
\log \log x < k \log 2
\]

\[
< k.
\]

Thus, $\log \log x + 1 < k + 1 < \pi(x)$,

which gives the result. \(\Box\)

Thm: There are arbitrarily large gaps between consecutive prime numbers.

Proof: Let $n$ be any integer. Consider the sequence of consecutive integers given by:

\[n^2, n^2 + 1, n^2 + 2, \ldots, n^2 + 10^3\]
Each of these is composite, so we have a sequence of \( n - 1 \) consecutive composite numbers. As \( n \to \infty \), the gaps between primes in such a sequence get arbitrarily large.

As we have the opposite ends of the spectrum. The twin prime conjecture said there are infinitely many primes \( p \) so that \( p + 2 \) is prime as well. These primes have as small a gap as possible. On the other hand, we have just shown there are gaps so large as we would like between consecutive primes! This should convince you that prime numbers and how they appear among the integers is a pretty difficult thing to understand!

We conclude our study of primes with a few more conjectures and results.

\[ \text{Goldbach's Conjecture: Every even integer greater than 4 is the sum of two odd primes.} \]

This is still unknown! Your text has a good summary of when the conjecture stands right now!
Dirichlet's Theorem: Let $a, b \in \mathbb{Z}_{>0}$ with $\gcd(a, b) = 1$. The sequence

$$a, a+b, a+2b, a+3b, \ldots$$

contains infinitely many primes.

This is a known result, but requires much more background than we have for this class. As a special case we have:

Thus: There are only many primes of the form $4k+3$.

This is a specific example of Dirichlet's theorem with $a = 3$, $b = 4$.

However, we can prove this theorem without resorting to Dirichlet's theorem.

Proof: Suppose there are only finitely many such primes, say $p_1, \ldots, p_n$. Let $N = 4p_1 \cdots p_n - 1$

$$= 4(p_1 \cdots p_n - 1) + 3.$$

As in the case of the proof of only many primes, there must be a prime other than $p_1, \ldots, p_n$ that divides $N$; otherwise we get $p_5 | 1 - 1$. We also have $N \equiv 3 \pmod{2N}$. So there is an odd prime other
That is not of the form $4k+3$ that divide $N$. Odd primes are of the form $4k+1$ or $4k+3$. Since $N$ cannot be divisible by any prime of the form $4k+3$, it must be divisible by primes of the form $4k+1$. However, this contradicts that $N$ is of the form $4n+3$ since $(4k+1)(4k+1) = 4x+1$.

Thus far, everything we have discussed has had to do with

divisibility in one form or another. We have basically worked from the definition to gain insights. We will now introduce a new tool, the theory of congruences. This was first established by Gauss. You should read the section in the text for some relevant historical background.

**Def:** Let $n \in \mathbb{Z}_{\geq 0}$. We say integers $a$ and $b$ are

congruent modulo $n$, written

\[ a \equiv b \pmod{n} \]

if $n \mid (a-b)$.

**Examples:**

1. $2 \equiv 9 \pmod{7}$

2. $6 \equiv -1 \pmod{7}$
\(\text{Thm 4.1:} \) \(a\), \(b\) \(\in \mathbb{Z}\). Then \(a \equiv b \pmod{n}\), iff \(a\) and 
\(b\) have the same remainder when divided by \(n\).

**Proof:** \(\Rightarrow\) Let \(a \equiv b \pmod{n}\) and write
\[
a = nq_1 + r_1, \quad 0 \leq r_1 < n
\]
\[
b = nq_2 + r_2, \quad 0 \leq r_2 < n.
\]
We have \(a - b = n(q_1 - q_2) + (r_1 - r_2)\).

Since \(n \mid (a-b)\) and \(n \mid (n(q_1 - q_2))\), we must have \(n \mid (r_1 - r_2)\). But \(0 \leq r_1, r_2 < n\)
\[\Rightarrow\] \(r_1 = r_2\).

\(\Leftarrow\) Suppose \(a\) and \(b\) have the same remainder when divided
by \(n\). Then we can write
\[
a = nq_1 + r
\]
\[
b = nq_2 + r
\]
for some \(q_1, q_2, r \in \mathbb{Z}\). Then
\[
a - b = n(q_1 - q_2)
\]
\[\Rightarrow n \mid (a-b) \Rightarrow a \equiv b \pmod{n}. \blacksquare\]

This way of thinking can be useful in solving problems!

\textbf{Example:} the following

We will see an application in a moment.
We can use Theorem 4.1 combined with the claim of

to conclude that given any integer \( n \), \( n \) must be

congruent modulo \( n \) to \( 0, 1, \ldots, n-1 \), as these are

the possible remainders. The set \( \{0, 1, \ldots, n-1\} \) is called

the set of **least nonnegative residues modulo** \( n \).

Of course, we can form other sets as well that have

the property that every integer must be congruent modulo

\( n \) to something in the set. For example, \( \{n, n+1, \ldots, 2n-1\} \)

is another such set since \( n \equiv 0 \pmod{m} \), \( n+1 \equiv 1 \pmod{m} \),

\( \ldots \), \( 2n-1 \equiv n-1 \pmod{m} \). Any set \( a_1, \ldots, a_n \) of

integers with the property that every integer is congruent

to one of the \( a_i \)'s is called a **complete residue

system** modulo \( n \).

We have one more theorem before we see some applications:

**Thm 4.2:** Let \( n \geq 1 \) be fixed and let \( a, b, c, d \) be

arbitrary integers. Then

1. \( a \equiv a \pmod{n} \)
2. If \( a \equiv b \pmod{n} \), then \( b \equiv a \pmod{n} \)
3. If \( a \equiv b \pmod{n} \) and \( b \equiv c \pmod{n} \), then \( a \equiv c \pmod{n} \)
4. If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( a + c \equiv b + d \pmod{n} \) and \( ac \equiv bd \pmod{n} \).

5. If \( a \equiv b \pmod{n} \), then \( a + c \equiv b + c \pmod{n} \) and \( ac \equiv bc \pmod{n} \).

6. If \( a^2 \equiv b \pmod{n} \), then \( a^k \equiv b^k \pmod{n} \) \( \forall \ k \geq 0 \).

**Proof:** Let the class pair \( x \) denote \( x^2 \).

**Cautio:** If \( ac \equiv bc \pmod{n} \), it is **not** necessarily true that \( a \equiv b \pmod{n} \)!

For example, \( 0 \cdot 4 \equiv 0 \cdot 1 \pmod{6} \) but \( 4 \not\equiv 1 \pmod{6} \)!

We will come back to this in a moment.

**Example:** Show that the equation \( x^2 + y^2 = 3z^2 \) has no nontrivial solutions in the integers.

**Proof:** Suppose \( (x, y, z) \) is such a solution. We can assume \( \gcd(x, y, z) = 1 \) for otherwise we can divide it out. Consider the equation \( \pmod{3} \). We have

\[
x^2 + y^2 \equiv 0 \pmod{3}.
\]

Observe that
\[
0^2 \equiv 0 \pmod{3},
1^2 \equiv 1 \pmod{3},
2^2 \equiv 1 \pmod{3}.
\]
We have that \(0,1,2\) form a complete residue system modulo 3, so \(x\) and \(y\) must each be congruent to one of them. But then \(x^2 + y^2 \equiv 0 \text{ (mod 3)}\), \(x\) must have \(x \equiv 0 \text{ (mod 3)}\) and \(y \equiv 0 \text{ (mod 3)}\). Thus \(3| x\) and \(3| y\). As we can write \(x = 3k\), \(y = 3l\) and the equation becomes

\[3^2 (k^2 + l^2) = 3z^2\]

\[\Rightarrow 3|z^2\] 

**Example:** Find the remainder of \(3^{57} - 1\) when divided by 8.

**Solution:** Observe \(3^2 \equiv 1 \text{ (mod 8)}\). So

\[3^{57} = (3^2)^{28} \equiv 1^{28} \equiv 1 \text{ (mod 8)}\]. Thus

\[3^{57} - 1 \equiv 3 \cdot 1 - 1 = 2 \text{ (mod 8)}.\] And

remainder is 2.

We now revisit the problem of cancelling across a congruence.

**Thm 4.3:** if \(ca \equiv cb \text{ (mod n)}\), then \(a \equiv b \text{ (mod } \frac{n}{d})\) when \(d = \gcd(c, n)\).
Proof: Let $a = bc \pmod{n}$. Then

$n \mid (ac - bc)$,

so $c \equiv k \pmod{n}$, $n \mid (ac - bc)$,

$= c(a - b)$

We know $\exists r, s, \gcd(r, s) = 1$, so that $n = dr$, $c = ds$.

$\Rightarrow dr \cdot k = ds(a - b)$

$\Rightarrow nk = 5(a - b)$

$\Rightarrow n \mid (a - b)$.

Thus, $a \equiv b \pmod{n}$.

Note that this says if $\gcd(r, n) = 1$, then we are free to cancel the $c$ away without worry!

Example: Prove that $27 \mid 2^{5n+1} + 5^{n+2}$ for all $n \geq 1$.

Proof: This is the type of statement we have been proving by induction without using congruences. Let's see how easy it is with congruences. Observe that $2^5 = 32$ and $32 \equiv 5 \pmod{27}$. Thus, $2^{5n+1} \equiv 2 \cdot 5^n \pmod{27}$.

$5^{n+2} = 5^2 \cdot 5^n = 25 \cdot 5^n \equiv -2 \cdot 5^n \pmod{27}$.

Thus,

$2^{5n+1} + 5^{n+2} = 2 \cdot 5^n + (-2) \cdot 5^n \pmod{27}$

$\equiv 0 \pmod{27}$. 

For another example of how powerful the theory of congruences can be, consider problem 1 from homework 1.

**Example:** Show $3 | 4^n - 1$ for all $n \geq 1$.

**Proof:** $4^n \equiv 1^n \equiv 1 \pmod{3} \quad \forall n \geq 1,$ so $4^n - 1 \equiv 0 \pmod{3} \quad \forall n \geq 1.$

The theory of congruences can also be used to give simple proofs of standard divisibility theorems from grade school.

Recall when we write an integer base 10 such as $5,234$ we really mean

$$5 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4.$$

**Thm 4.5:** Let $N$ be a positive integer with

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0.$$ 

We have $9 | N$ iff $9 | (a_n + a_{n-1} + \cdots + a_1 + a_0)$.

**Proof:** We use the fact that $10 \equiv 1 \pmod{9}$ to see

$$N \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{9}.$$

Now $9 | N$ iff $9 | (a_n + a_{n-1} + \cdots + a_1 + a_0)$

in clear.
Theorem 4.6: Let \( N \) be a positive integer with
\[
N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0.
\]
Then, \( 11 \mid N \) if and only if
\[
11 \mid (a_n - a_{n-1} + a_2 - \cdots + (-1)^{n} a_0).
\]

Proof: We use that \( 10 \equiv -1 \pmod{11} \). Thus,
\[
N \equiv a_n (-1)^n + \cdots + a_2 (-1) + a_0 \pmod{11}.
\]
We get the result as in the last theorem.

Such calculations can be used in real-world applications.


These numbers consist of 9 digits \( a_1, a_2, \ldots, a_9 \) and then a 10th digit that is a "check digit" to make sure the other 9 are actually correct and work. Then the 10th is defined by
\[
a_{10} \equiv \sum_{k=1}^{9} k a_k \pmod{11}.
\]

The ISBN of an book is 0073051888. We need
\[
1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 3 + 5 \cdot 0 + 6 \cdot 5 + 7 \cdot 1 + 8 \cdot 8 + 9 \cdot 8
\]
\[
\equiv 8 \pmod{11}.
\]
This is true, as can easily be checked.

Suppose we had the problem that two of the numbers in an ISBN were transposed.
Suppose \( i < j \) and an ISBN \( a_1 \ldots a_i \ldots a_j \ldots a_q \) was accidentally written as \( a_1 \ldots a_j \ldots a_i \ldots a_q \). Can we tell this is wrong?

We know that
\[
a_1 + \Theta a_2 + \ldots + \Theta a_i + \ldots + ja_j + \ldots + qa_q \equiv a_o \pmod{11}.
\]

Can
\[
a_1 + \Theta a_2 + \ldots + i a_j + \ldots + ja_i + \ldots + qa_q \equiv a_0 \pmod{11}?
\]

Observe that
\[
\begin{align*}
a_1 + \Theta a_2 + \ldots + i a_j + \ldots + ja_i + \ldots + qa_q \\
&= a_1 + \Theta a_2 + \ldots + i a_i + \ldots + j a_j + \ldots + qa_q \\
&\quad + (j-i)a_i + (i-j)a_j,
\end{align*}
\]
\[
\equiv a_1 + (j-i)a_i + (i-j)a_j \pmod{11}.
\]

So the question is whether
\[
(j-i)a_i + (i-j)a_j \equiv 0 \pmod{11}.
\]

Suppose this is the case. Observe that \( i-j \) is relatively prime to 11, this is because 1 \leq i, j \leq 9 and if 11 \mid (i-j), then \( i \equiv j \pmod{11} \). \( \Rightarrow \) \( i = j \), \#.

So if
\[
(j-i)a_i + (i-j)a_j \equiv 0 \pmod{11},
\]
then
\[
(j-i)a_i \equiv (j-i)a_j \pmod{11}
\]
\[
\Rightarrow a_i \equiv a_j \pmod{11} \#.
\]

Thus we can see to tell the difference!
As was the case when studying divisibility earlier, now that we have some machinery built up we would like to use it to study solutions to equations. In particular, we would like to look at solutions of equations

\[Ax \equiv b \pmod{n}\]

(linear congruences) as well as multiple linear congruences,

\[a \equiv a_1 \pmod{n}, \quad x \equiv a_2 \pmod{n}, \quad \ldots \quad x \equiv a_r \pmod{n}.

We begin with linear congruences. We are really only interested in solutions \(\pmod{n}\), so if \(x_0\) is a solution to

\[x + mn \equiv x_0 + mn \pmod{n}\]

and so \(x_0 + mn\) is a solution for any integer \(m\)

\[
\begin{pmatrix}
  a \cdot (x_0 + mn) \\
= a \cdot x_0 + am \cdot n \\
\equiv b \pmod{n}
\end{pmatrix}
\]

and so is not really any new information. So when we look for solutions, we only look \(\pmod{n}\). This shows that
Worst case scenario we could just plug in $x = 0, 1, \ldots, n-1$ to see if there are any solutions. Of course if $n$ is very large this is not real practical.

Note that $x$ is a solution iff $n \mid ax - b$

$$\iff \exists x + ny \in \mathbb{Z} \text{ s.t. } ny = ax - b$$

$$\iff ax + n(-y) = b.$$ 

So finding a solution to $ax \equiv b \pmod{n}$ is the same as solving the Diophantine equation $ax + ny = b$.

**Thm 4.7:** The linear congruence $ax \equiv b \pmod{n}$ has a solution iff $\gcd(a,n) \mid b$. If $\gcd(a,n) \mid b$, then there are $\gcd(a,n)$ incongruent solutions mod $kn$. 

**Proof:** Let $d = \gcd(a,n)$. Then the prior statement is equivalent to our previous result on linear Diophantine equations, this is just phrased in a new language. Now suppose we have a solution $x_0$. Remember, other solutions then have $x = x_0 + \frac{n}{d} t$ for $t \in \mathbb{Z}$. Therefore we now need to see for which $t$ these are
distinct modulo \( b \). We claim that

\[ x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{2n}{d}, \ldots, \quad x_0 + \frac{(d-1)n}{d} \]

are all distinct modulo \( n \). Furthermore, any other \( x_0 + \frac{n}{d} t \) must be congruent to one of these.

If we can show this, we will be done.

Suppose \( x_0 + \frac{n}{d} t_1 = x_0 + \frac{n}{d} t_2 \pmod{n} \)

where \( 0 \leq t_1 < t_2 \leq d-1 \). Then we have

\[ \frac{n}{d} t_1 \equiv \frac{n}{d} t_2 \pmod{n} \]

Since \( \gcd\left( \frac{n}{d}, n \right) = \frac{n}{d} \), we can cancel the \( \frac{n}{d} \) to obtain

\[ t_1 \equiv t_2 \pmod{d} \cdot \frac{d}{n} \]

Thus, there are all distinct modulo \( n \).

We now must show \( x = x_0 + \frac{n}{d} t \) is congruent to one of the above. Use the Division Algorithm to write

\[ t = q d + r, \quad 0 \leq r < d-1. \]

Then,

\[ x_0 + \frac{n}{d} t = x_0 + \frac{n}{d} (q d + r) \]

\[ = x_0 + nd + \frac{n}{d} r \]

\[ \equiv x_0 + \frac{n}{d} r \pmod{n}. \]
Example: Solve the linear congruence

\[ 34x \equiv 60 \mod 98. \]

Solution: Begin by observing that \( \gcd(34, 98) = 2 \), and

\[ 34x \equiv 60 \equiv 98y \mod 98 \]

so there are solutions. In fact, we have exactly 2 incongruent solutions modulo 98. Solutions are equivalent to solution of the Diophantine problem

\[ 34x - 98y = 60 \]

in,

\[ 34x + 98y = 60 \]

when we replaced \(-y\) with \(y\) (since we are only interested in \(x\), this won't affect us!). Since \( \gcd(34, 98) = 2 \), we can find \(m, n\) so that

\[ 34m + 98n = 2. \]

\[ m = -23, \quad n = 8 \]

Thus,

\[ 34(-23) + 98(8) = 2. \]

Multiplying by 30 we have

\[ 34(-690) + 98(240) = 60 \]

Thus, \( x = -690 \) is one solution.

Note that \( \boxed{-690} \).
Thus, \( x = 94 \) is one solution to the equation. The other solution is

\[
94 + \frac{98}{2} = 143
\]

\[\equiv 45 \pmod{98}.\]

Thus, our two congruent solutions are 45 and 94.

The next natural step is to try and solve two congruences,

\[a_1 x \equiv b_1 \pmod{m_1}\]
\[a_2 x \equiv b_2 \pmod{m_2}\]

simultaneously. Each equation only has a solution if \( \gcd(m_i, a_i) \mid b_i \). If this is the case, divide by \( d_i = \gcd(m_i, a_i) \) to obtain new equations

\[
\frac{a_1}{d_1} x \equiv \frac{b_1}{d_1} \pmod{\frac{m_1}{d_1}}.
\]
\[
\frac{a_2}{d_2} x \equiv \frac{b_2}{d_2} \pmod{\frac{m_2}{d_2}}.
\]

Each of these equations has a solution, say

\[x \equiv c_1 \pmod{\frac{m_1}{d_1}}\]
and

\[x \equiv c_2 \pmod{\frac{m_2}{d_2}}.\]
\[ X \equiv c_2 \pmod{m_2}. \]

Now we want to determine which of these solutions solve both of the congruences simultaneously, then we have reduced solving

\[ a_j x \equiv b_j \pmod{n_j}, \]
\[ a_2 x \equiv b_2 \pmod{m_2}. \]

Simultaneously down to the problem of solving

\[ X \equiv c_1 \pmod{m_1}, \]
\[ X \equiv c_2 \pmod{m_2}. \]

Simultaneously.

**Theorem 4.8 (The Chinese Remainder Theorem):** Let \( n_1, n_2 \) be

positive integers with \( \gcd(n_1, n_2) = 1 \). Then

\[ X \equiv a_1 \pmod{n_1}, \]
\[ X \equiv a_2 \pmod{n_2}. \]

has a simultaneous solution which is unique

modulo \( n_1n_2 \).

**Proof:** Let \( x \) be a solution of the equation

\[ X \equiv a_1 \pmod{n_1}. \]
Then \( \exists \, y \in \mathbb{Z} \) s.t.
\[
x - a_1 = n_1 y
\]
i.e.,
\[
x = a_1 + n_1 y.
\]

Putting this into the second equation we have
\[
a_1 + n_1 y \equiv a_2 \pmod{n_2},
\]
i.e., we want to solve the congruence
\[
n_1 y \equiv (a_2 - a_1) \pmod{n_2}.
\]
Since \( \gcd(n_1, n_2) = 1 \), this equation has a solution. Write
\[
n_1 s + n_2 t = 1.
\]

Then
\[
n_1 s (a_2 - a_1) + n_2 t (a_2 - a_1) = a_2 - a_1,
\]
i.e.,
\[
n_1 (s(a_2 - a_1)) \equiv a_2 - a_1 \pmod{n_2}.
\]

So letting
\[
x = a_1 + n_1 s (a_2 - a_1)
\]
we see that
\[
x \equiv a_1 \pmod{n_1}
\]
and
\[ X \equiv a_1 + n_1 s(a_2 - a_1) \]
\[ \equiv a_1 + (a_2 - a_1) \pmod{n_1} \]
\[ \equiv a_2 \pmod{n_1}. \]

Thus, \( X \) is a solution simultaneously to each congruence.

Now observe that if \( X' \) is another simultaneous solution, then
\[ X \equiv X' \pmod{n_1} \]
\[ X \equiv X' \pmod{n_2}. \]

Since \( n_1 \mid (x-x') \) and \( n_2 \mid (x-x') \), \( \text{lcm}(n_1, n_2) \mid (x-x') \).

However, \( \gcd(n_1, n_2) = 1 \Rightarrow \text{lcm}(n_1, n_2) = n_1 n_2 \), thus,
\[ n_1 n_2 \mid (x-x'), \text{ i.e., } X \equiv X' \pmod{n_1 n_2}. \]
Thus \( X \) is the unique solution modulo \( n_1 n_2 \).

It may occur that we want a simultaneous solution to several equations. We can just apply the above theorem to find solutions in pairs. You'll prove this in your homework, but now we give an example.
Example: Solve the simultaneous congruence

\[ x \equiv 5 \pmod{11}, \quad x \equiv 14 \pmod{69}, \quad x \equiv 15 \pmod{31}. \]

Solution: We first find a simultaneous solution to the congruence

\[ x \equiv 5 \pmod{11}, \]
\[ x \equiv 14 \pmod{69}. \]

Write \( x - 5 = 11y \), i.e., \( x = 5 + 11y \).

Substituting this into the second equation gives

\[ 5 + 11y \equiv 14 \pmod{69}, \]

i.e.,

\[ 11y \equiv 9 \pmod{69}. \]

Next we need \( s, t \in \mathbb{Z} \)

s.t.

\[ 11s + 69t = 1. \]

We find \( s = 8, \ t = -3 \). Multiplying by 9 we have

\[ 11(72) + 69(-27) = 9. \]

Thus,

\[ 11(72) \equiv 9 \pmod{69} \]

Substituting back in we obtain

\[ x = 5 + 11(72) = 797 \]
\[ \equiv 159 \pmod{319}. \]
is a solution to the first pair of congruences. To find a solution to all three congruences it now equivalent to solving the congruences

\[ x \equiv 159 \pmod{319} \]
\[ x \equiv 15 \pmod{31} . \]

Write

\[ x = 159 + 319z \]

and substitute into the second equation:

\[ 159 + 319z \equiv 15 \pmod{31} \]

i.e.,

\[ 9z \equiv 11 \pmod{31} . \]

We now find \( m, n \in \mathbb{Z} \) s.t. \( 9m + 31n = 1 \).

We have

\[ 1 = 9(7) + 31(-2) \]

Multiplying by \( 11 \):

\[ 11 = 9(77) + 31(-22) , \]

i.e.,

\[ 9(77) \equiv 11 \pmod{31} , \]

Thus,

\[ x = 159 + 319(77) \]
\[ x = 24722 \]
\[ \equiv 4944 \pmod{9889} . \]

Thus, \( x = 4944 \pmod{9889} \) is a simultaneous solution, as you can check.

If you want to solve a system with SAGE, say

\[ x \equiv a \pmod{m} , \]
\[ x \equiv b \pmod{n} , \]

the command is

\[ x = \text{crt}(a, b, m, n) ; x . \]

For example,

\[ x = \text{crt}(5, 14, 11, 29) ; x \]

returns

797.

The text also treats solving

\[ ax + by \equiv c \pmod{n} \]

as well as the simultaneous congruences.
\[ a \times x + b \times y \equiv r \pmod{n} \]
\[ c \times x + d \times y \equiv s \pmod{n} , \]

but we will leave this for the reader to work out. It is not difficult and uses the same ideas we have been using.

Next we may ask about solving congruence of higher degrees, any
\[ f(x) \equiv 0 \pmod{n} \]
for \( f(x) \) a polynomial of degree \( n \times r \). We will deal with polynomial of degree \( n \) when we get to quadratic reciprocity. As in the case over \( \mathbb{Z} \), there is not a nice easy way in general. The advantage to congruence is we can always solve them, just plug in \( x = 0, \ldots, n-1 \) and see which work. Of course, as \( n \) gets large this is not real efficient.

We can get a partial result. Suppose we want to solve
\[ f(x) \equiv 0 \pmod{p^n} \]
for \( p \) a prime. We will see how we can use the solution modulo \( p^n \) to get the solution modulo \( p^{n+1} \). This allows
to start modulo $p$ and work our way up. If we are
going to do it computationally, this reduces our computations
significantly. Also, if $m = p^{e_1} \cdots p^{e_r}$, then if $x$ is
a solution of $f(x) \equiv 0 \pmod{m}$, i.e., $f(x) \equiv 0 \pmod{p^{e_i}}$
for each $i = 1, \ldots, r$. Thus we can at least reduce the
problem down to studying equations modulo $p$.

We begin by observing that if $x$ is s.t. $f(x) \equiv 0 \pmod{p^n}$,
then $f(x) \equiv 0 \pmod{p^k}$ for $1 \leq k \leq n$. Clearly if $p^n | f(x)$,
so does $p^k$ for $1 \leq k \leq n$. Thus, if $x$
is a solution of $f(x) \equiv 0 \pmod{p^n}$, $x$ is also a solution of
$f(x) \equiv 0 \pmod{p^k}$, which we are assuming we know all $k$. Let
$x_1, \ldots, x_m$ be all $m$ the solutions of $f(x) \equiv 0 \pmod{p^n}$. So
we must have $x \equiv x_i \pmod{p^n}$ for some $i \in \{1, \ldots, m\}$. We
then have $x = x_i + pt$, or $x = x_i + p^nt$. We
want to determine for which $i$ such $t$ exists to make
$x + p^nt$ a solution modulo $p^n$.

We have the following theorem giving the result:
\textbf{Theorem:} Let \( f \) be a polynomial with integer coefficients of degree \( r \geq 1 \). Let \( p \) be prime, \( n \geq 1 \). Let \( y \) be a solution of
\[ f(x) \equiv 0 \pmod{p^n}. \]

Then \( y \equiv x_i + tp^n \pmod{p^n} \) where \( 0 \leq x_i \leq p^n \) and \( x_i \) satisfies
\[ f(x_i) \equiv 0 \pmod{p^n}. \]

\( \exists t \in \mathbb{Z} \) such that \( t \) satisfies the congruence
\[ tf'(x_i) \equiv -\frac{f(x_i)}{p^n} \pmod{p} \] \hspace{1cm} (8)

Furthermore, if \( h \) is the number of solutions of (8), then
\[ h = \begin{cases} 
1 & \text{if } p \nmid f'(x_i) \\
0 & \text{if } p \mid f'(x_i) \text{ and } p^{n+1} \mid f(x_i) \\
p & \text{if } p \mid f'(x_i) \text{ and } p^n \nmid f(x_i). 
\end{cases} \]

\textbf{Proof:} Let \( x_1, \ldots, x_m \) be the solutions to \( f(x) \equiv 0 \pmod{p^n} \).

Let \( y_i \equiv f(y_i) \equiv 0 \pmod{p^n} \), \( \forall 1 \leq i \leq m \) and \( t \in \{0, 1, \ldots, p-1\} \), \( y = x_i + tp^n \).

We consider the polynomial
\[ f(y) = f(x_i + tp^n) \]
and expand it in a Taylor series. For each \( y_i \), write
\[ f(y) = f(x_i + x) \]
and the Taylor series around \( x = x_i \) is:
\[ f(y) = f(x_i) + (y-x_i)f'(x_i) + \frac{(y-x_i)^2}{2} f''(x_i) + \ldots \]

\[ = f(x_i) + x f'(x_i) + \frac{x^2}{2} f''(x_i) + \ldots \]

\[ = f(x_i) + t p^n f'(x_i) + t^2 p^{2n} f''(x_i) + \ldots \]

Looking at the module \( p^{n+1} \), we have

\[ f(y) \equiv f(x_i) + t p^n f'(x_i) \pmod{p^{n+1}}. \]

We have \( f(y) \equiv 0 \pmod{p^{n+1}} \) by assumption, so

\[ t p^n f'(x_i) \equiv - f(x_i) \pmod{p^{n+1}}. \]

We know \( f(x_i) \equiv 0 \pmod{p^n} \), so \( p^n f(x_i) \). As we have

\[ t p^n f'(x_i) + f(x_i) = s p^{n+1} \quad \text{and} \]

\[ \frac{d}{dt} f(x_i) = \frac{p^n}{p}. \]

Thus,

\[ t^p p^n f'(x_i) + p^n = s p^{n+1}, \quad \text{i.e.,} \]

\[ t f'(x_i) + \ell = s p. \]

Hence

\[ t f'(x_i) \equiv - f(x_i) \pmod{p^n}. \]

This gives the first part of the theorem.

Let \( \ell \) be the number of solutions of \((*)\).

If \( p | f(x_i) \), then this is a linear congruence and

\[ \gcd(p, f(x_i)) = 1, \quad \text{so it has exactly 1 solution.} \]
Example: Find all solution of the congruence

\[ x^3 + 2x + 2 \equiv 0 \pmod{19}, \]

Solution: As \( 19 = 7^2 \), we begin by solving the congruence

\[ x^3 + 2x + 2 \equiv 0 \pmod{7}. \]

This is easy to calculate, with substitution, obtaining

\[ x_1 \equiv 3, \quad x_2 \equiv 3 \pmod{7}. \]

\[ f'(x_1) = 3x^2 + 2. \]

As we want solution \( x \)

\[ t \equiv f'(x_1) \equiv -\frac{f(x_1)}{7} \pmod{7}. \]

The two values of \( x_i \) give:

\[ t (0) \equiv -\frac{14}{7} \pmod{7}. \]

Thus \( p | f'(3) \) and \( p^n | f(x_1) \), as we have new solution corresponding to \( x_1 = 3 \).

\[ f'(3) = 1 \pmod{7} \]

\[ f(3) = 0 \pmod{7}, \quad f(3) = 35. \]
So \( t f(3) \equiv \frac{-f(3)}{7} \pmod{7} \) becomes

\[
\begin{align*}
t &\equiv -5 \pmod{7} \\
t &\equiv 2 \pmod{7}
\end{align*}
\]

Thus, we obtain one solution (as we shall see in \( \frac{1}{7} f(3) \))

given by

\[
y = 3 + 2 \cdot (47) = 17 \pmod{49}.
\]

We will come back to solving polynomial congruences when we study quadratic reciprocity. Our next step is developing the necessary background is studying Fermat's Little Theorem.

**Thm 5.1:** (Fermat's Little Theorem) Let \( p \) be a prime number.

Then \( a^p \equiv a \pmod{p} \) for any \( a \in \mathbb{Z} \).

We will give a couple of proofs of this fact. The first we will give is using abstract algebra.

**Proof 1:** Recall that \( \mathbb{Z}/p\mathbb{Z}^* \) is a group with \( p-1 \) elements.

Thus, \( a^{p-1} \equiv 1 \pmod{p} \) for any \( a \in \mathbb{Z}/p\mathbb{Z}^* \). This gives the result for any \( a \in \mathbb{Z} \) with \( \gcd(a,p) = 1 \) upon multiplying by \( a \). If \( \gcd(a,p) > 1 \), then
\(a \equiv 0 \pmod{p}\) and clearly \(a^p \equiv a^0 \equiv 0 \pmod{p}\). Thus, the result is true for all \(a \in \mathbb{Z}\).

Our second proof uses induction and relies on the following lemma.

**Lemma:** Let \(p\) be prime and \(1 \leq k \leq p-1\). Then \(p \mid \binom{p}{k} \).

**Proof:** Recall that

\[
\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1) \cdots (p-k+1)}{k!}.
\]

Thus,

\[k! \binom{p}{k} = p(p-1) \cdots (p-k+1).
\]

It is clear that \(p \mid (p(p-1) \cdots (p-k+1))\), so

\[k! \binom{p}{k} \equiv 0 \pmod{p}.
\]

Since \(p\) is prime, \(p \mid k! \binom{p}{k}\), so \(p \mid \binom{p}{k}\) as desired.

**Proof of a F.L.T. like this:** We proceed by induction on \(a\). The case

\(a = 0 \mod{p}\) and \(a = 1\) are both trivial. Now suppose the result holds for all \(1 \leq k \leq a\) and \(a \in \mathbb{Z}_{>0}\).

We have

\[(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \ldots + \binom{p}{p}a + 1
\]

\[\equiv a^p + 1 \pmod{p} \quad \text{(by lemma)}
\]

\[\equiv a + 1 \pmod{p} \quad \text{(by ind. hyp)}.
\]
Thus, \( a^p \equiv a \pmod{p} \) \( \forall a \geq 0 \) by strong induction. To get the result for \( a < 0 \), we use that \( a \equiv r \pmod{p} \) for some \( 0 \leq r < p \), so \( a^p = r^p \equiv r \equiv a \pmod{p} \).

Thus, the result holds for all \( a \in \mathbb{Z} \).

**Proof 3:** Consider the integers \( a, 2a, \ldots, (p-1)a \). Our first claim is more or these are congruent to one another \( \pmod{p} \) if \( \gcd(p, a) = 1 \). If not, say \( i \cdot a \equiv j \cdot a \pmod{p} \), then since \( \gcd(a, p) = 2 \) we can cancel the \( a \) to obtain \( i \equiv j \pmod{p} \). Thus, \( i = j \) since \( i \) and \( j \) are both less than \( p \) and positive. Then \( 0 \).

The pigeonhole principle gives that
\[
\{ a, 2a, \ldots, (p-1)a \} = \{ 1, 2, \ldots, p-1 \}
\]
for \( \gcd(a, p) = 1 \). Thus,
\[
a \cdot 2a \cdot 3a \cdots (p-1)a = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},
\]
i.e., \( a^{p-1} \equiv (p-1)! \pmod{p} \). Since \( \gcd(p, (p-1)! ) = 1 \), we can cancel the \( (p-1)! \) to obtain
\[
a^{p-1} \equiv 1 \pmod{p}
\]
if \( \gcd(a, p) = 1 \). Multiply through by \( a \) to get the desired form.
If \( \gcd(a, p) > 1 \), then \( a \equiv 0 \pmod{ap} \) and clearly the proof is true.

Before we study some applications of Fermat's little theorem, we give a natural generalization. We begin by defining Euler's \( \phi \) function, which will be studied further in the future.

**Def.** Let \( n \) be a positive integer. Euler's \( \phi \)-function is defined by \( \phi(n) = \# \) of positive integers less than \( n \) that are relatively prime to \( n \).

**Example:** \( \phi(5) = 4 \)  
\( \phi(8) = 4 \)  
\( \phi(77) = 60 \)  
The command is

\[ \texttt{Euler\_phi(n)} \]  
in \SAGE.

**Thm.** Let \( m \) and \( n \) be relatively prime positive integers.

Then \( \phi(mn) = \phi(m) \phi(n) \).

Let \( m = p_1^{e_1} \cdots p_r^{e_r} \)

then

\[ \phi(m) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = m \prod_{i=1}^{r} (1 - \frac{1}{p_i}) \]

This theorem is showing that \( \phi \) is what is known as an a multiplicative function.
Let \( n = n_1 n_2 \). Suppose \( x \) is such that \( \gcd(x, n) = 1 \).

Reducing \( x \) modulo \( n_i \), give an \( a_i \) with

\[ 0 < a_i < n_i, \quad \gcd(a_i, n_i) = 1, \quad \text{and} \quad x \equiv a_i \pmod{n_i}. \]

Similarly, we get \( a_2 \) with

\[ 0 < a_2 < n_2, \quad \gcd(a_2, n_2) = 1, \quad \text{and} \quad x \equiv a_2 \pmod{n_2}. \]

Note that \( \gcd(a_i, n_i) = 1 \) and \( \gcd(a_2, n_2) = 1 \). Thus we see that for any \( x \) we obtain a pair \((a_i, a_2)\) s.t.

\[ \gcd(a_i, n_i) = 1 \quad \text{and} \quad 1 \leq a_i < n_i. \]

Thus, we must have \( \phi(n) \leq \phi(n_1) \phi(n_2) \).

Now let \((a_1, a_2)\) be a pair of integers so that

\[ 1 \leq a_i < n_i, \quad \gcd(a_i, n_i) = 1. \]

The Chinese remainder theorem gives us \( x \) s.t.

\[ x \equiv a_i \pmod{n_i}, \]

\[ x \equiv a_2 \pmod{n_2}, \]

with \( 1 \leq x < n_1 n_2 \). Hence \( \gcd(n_1, a_2) = 1 \), we have \( \gcd(x, n_1) = 1 \). Thus, we see that for each pair \((a_i, a_2)\) with \( 1 \leq a_i < n_i, \quad \gcd(a_i, n_i) = 1 \), we obtain a unique \( x \) s.t.

\[ \gcd(x, n_1) = 1 \quad \text{and} \quad 1 \leq x < n_1 n_2. \]

Note \( \gcd(x, n) = 1 \) necessarily! Thus, \( \phi(n) \phi(n_1) \phi(n_2) \)

And so we have that \( \phi(n) = \phi(n_1) \phi(n_2) \).
Now let $n = p_1^{e_1} \cdots p_r^{e_r}$. Repeatedly applying what we have just shown gives
\[
\varphi(n) = \prod_{i=0}^{r} \varphi(p_i^{e_i}).
\]
Thus, we only need to compute $\varphi(p^e)$ for $p$ a prime and $e \geq 1$. Let $a$ be an integer with $1 \leq a \leq p^e$.

Then $\gcd(a, p^e) = 1$ unless $a$ happens to be
\[
p, 2p, 3p, \ldots, p^{e-1}p.
\]
There are precisely $p^{e-1}$ such numbers. Thus, there are $p^e - p^{e-1}$ other integers $a$ with a relatively prime to $p^e$ and $1 \leq a \leq p^e$. Thus,
\[
\varphi(p^e) = p^e - p^{e-1}
\]
\[
= p^e \left(1 - \frac{1}{p}\right).
\]
This gives the desired result. \(\square\)

**Thm. (Euler's Thm.):** Let $n$ be a positive integer and $a \in \mathbb{Z}$

s.t. $\gcd(a, n) = 1$. Then

\[ a^{\varphi(n)} \equiv 1 \pmod{n}. \]

**Proof:** As with Fermat's little theorem, this follows easily if we use abstract algebra, noting that the group $(\mathbb{Z}/n\mathbb{Z})^*$ has order $\varphi(n)$. \(\square\)
To prove Euler's Theorem without abstract algebra we need a little set-up.

**Definition:** Let \( m > 1 \) be an integer. A **reduced residue system modulo** \( m \) is a set of integers \( X \) s.t. \( \gcd(x, m) = 1 \), \( x \not\equiv x_i \pmod{m} \text{ if } i \neq j \), and every integer \( x \) that is relatively prime to \( m \) is congruent to \( x_i \) for some \( i \).

**Lemma:** Let \( a \in \mathbb{Z} \) s.t. \( \gcd(a, m) = 1 \). Let \( x_1, \ldots, x_{\varphi(m)} \) be a reduced residue system modulo \( m \). Then \( a \cdot x_1, \ldots, a \cdot x_{\varphi(m)} \) is a reduced residue system modulo \( m \).

**Proof:** This is an easy exercise!

**Proof (Euler's Theorem):** Let \( x_1, \ldots, x_{\varphi(m)} \) be a reduced residue system modulo \( m \). Then \( a \cdot x_1, \ldots, a \cdot x_{\varphi(m)} \) is also a reduced residue system modulo \( m \). Thus, for each \( i \), there is exactly one \( j \) s.t.

\[ x_i \equiv a \cdot x_j \pmod{m} , \]

Thus,

\[ \{ x_1, \ldots, x_{\varphi(m)} \} = \{ a \cdot x_1, \ldots, a \cdot x_{\varphi(m)} \} . \]
So we have

\[ aX_1 \cdots aX_{\varphi(m)} \equiv X_1 \cdots X_{\varphi(m)} \pmod{m}. \]

i.e.,

\[ a^{\varphi(m)} X_1 \cdots X_{\varphi(m)} \equiv X_1 \cdots X_{\varphi(m)} \pmod{m}. \]

Since \( \gcd(x_i, m) = 1 \) for each \( i \), we can cancel

\[ X_1 \cdots X_{\varphi(m)} \] to obtain the result.

Our first application of Fermat's Little Theorem is to studying quadratic congruences. We are able to obtain some preliminary results before studying quadratic reciprocity. We will then use Fermat's Little Theorem to study public-key cryptography.

**Lemma:** Let \( p \) be a prime number. Then \( x^2 \equiv 1 \pmod{p} \)

if and only if \( x \equiv \pm 1 \pmod{p} \).

**Proof:**

1. If \( x \equiv \pm 1 \pmod{p} \), then clearly \( x^2 \equiv 1 \pmod{p} \).

2. If \( x^2 \equiv 1 \pmod{p} \), then \( x^2 - 1 = 0 \pmod{p} \). Thus, \( p \mid (x^2 - 1) \equiv (x - 1)(x + 1) \). Thus, \( p \mid (x - 1) \) or \( p \mid (x + 1) \), i.e., \( x \equiv \pm 1 \pmod{p} \).

We now need Wilson's Theorem for our next result.
Thm 5.4: Let \( p \) be a prime. Then \((p-1)! \equiv -1 \pmod{p}\).

Proof: The result is clear for \( p = 2, 3 \), so we may assume \( p > 5 \). Let \( a \in \mathbb{Z} \) s.t. \( 1 \leq a \leq p-1 \). Since gcd\((a, p) = 1\), there is a unique \( \bar{a} \in \mathbb{Z} \) s.t. \( 1 \leq \bar{a} \leq p-1 \) and
\[
\bar{a} \bar{a} \equiv 1 \pmod{p}.
\]
(Linear congruence results.) Thus, \( a \) and \( \bar{a} \) from a pair s.t. \( a \bar{a} \equiv 1 \pmod{p} \). Thus, their contribution to \((p-1)! \equiv 1 \pmod{p}\). The only thing we need to worry about is if \( a = \bar{a} \). But this happens only if \( a^2 \equiv 1 \pmod{p} \), i.e., from our previous result if \( a^2 \equiv 1, p-1 \pmod{p} \). Thus, if we pull off the term \( 1 \) and \( p-1 \) from \((p-1)!\), we can pair off the rest of the terms in this way:
\[
(p-1)! \equiv (p-1) \cdot \prod_{a \neq 1} (a \equiv -1 \pmod{p}) \\
\equiv p-1 \pmod{p} \\
\equiv -1 \pmod{p}.
\]

We can apply Wilson's theorem (Thm 5.4) to deduce the following theorem, a special case of quadratic reciprocity.
**Theorem 5.5:** Let $p$ be a prime. The congruence

$$x^2 \equiv -1 \pmod{p}$$

has solutions iff $p=2$ or $p \equiv 1 \pmod{4}$.

**Proof:**

If $p=2$, then $-1 \equiv 1 \pmod{2}$ and no $x \equiv 1 \pmod{2}$ provides a solution. We may now assume $p$ is an odd prime.

We rewrite Wilson's theorem as

$$(1 \cdot 2 \cdots \frac{p-1}{2})(\frac{p+1}{2} \cdots (p-1)) \equiv -1 \pmod{p}. \quad (\star)$$

By using $\frac{p-1}{2}$, we have

$$\prod_{j=1}^{\frac{p-1}{2}} j (p-j) \equiv -1 \pmod{p}.$$ 

Here we have just paired off the terms in $(\star)$.

Observing that $j (p-j) \equiv -j^2 \pmod{p}$, we have

$$\prod_{j=1}^{\frac{p-1}{2}} j (p-j) \equiv \prod_{j=1}^{\frac{p-1}{2}} -j^2 \pmod{p}$$

$$\equiv (-1)^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j^2 \pmod{p}.$$ 

Now if $p \equiv 1 \pmod{4}$, then there exists an $m \in \mathbb{Z}$ such that $p-1 = 4m$.

Thus,

$$(-1)^{\frac{p-1}{2}} = (-1)^{2m} = 1.$$ 

So if we set

$$x = \left(\frac{p-1}{2}\right)!,$$

then this provides a solution of the congruence since we will have

$$x^2 \equiv -1 \pmod{p},$$
\[
\left[\left(\frac{p-1}{2}\right)\right]^2 \equiv \prod_{j=1}^{\frac{p-1}{2}} (j^2) \equiv \prod_{j=1}^{\frac{p-1}{2}} j (p-j) \pmod{p} \equiv -1 \pmod{p}.
\]

Suppose conversely now that \( x \) is a solution of \( x^2 \equiv -1 \pmod{p} \).

Clearly \( p \nmid x \). If \( p = 2 \) we are done, so suppose \( p > 2 \).

Then raising both sides of the congruency to \( \left(\frac{p-1}{2}\right) \) we have

\[
x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.
\]

However, Fermat's little theorem gives \( x^{p-1} \equiv 1 \pmod{p} \).

As we must have

\[
(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.
\]

Now \( (-1)^{\frac{p-1}{2}} = \pm 1 \) and \( -1 \not\equiv 1 \pmod{p} \) \( (p > 2) \)

and so we must have that \( (-1)^{\frac{p-1}{2}} = 1 \), not just congruent. But this is equivalent to \( \frac{p-1}{2} \) is even, i.e. \( p-1 = 4m \) for some \( m \).

Note that this theorem and the following ones are normally encountered in an abstract algebra class when studying \( \mathbb{Z}[i] \), the Gaussian integers.
Corl: Let $p$ be a prime number with $p \equiv 1 \pmod{4}$. Then there exist $a, b \in \mathbb{Z}_{>0}$ such that $p = a^2 + b^2$.

**Proof:** We apply the previous theorem to conclude there exists $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod{p}$. Define a function

$$f(u,v) = u + xv.$$

Let $N = L\sqrt{p}$. (Recall that $L$ is the greatest integer less than or equal to $y$, in $L \leq y < L+1$.) Assume $p$ is prime, $\sqrt{p} \in \mathbb{Z}$ and $0 < N < \sqrt{p} < N+1$. We consider the set of integer pairs $(u,v)$ with $0 \leq u \leq N$, $0 \leq v \leq N$.

The values of $u$ and $v$ each take $N+1$ values, so we have $(N+1)^2$ different pairs $(u,v)$. Since $N+1 > \sqrt{p}$, we have more than $p$ pairs. The pigeonhole principle then gives that we must have $f(u,v)$ is congruent modulo $p$ to $f(m,n)$ for some $u,v,m,n$ in our range, $(u,v) \neq (m,n)$.

Thus, we have

$$f(u,v) \equiv f(m,n) \pmod{p}.$$
i.e.,

\[ U + x \equiv m + xn \pmod{p}. \]

Hence,

\[ U - m \equiv x(n - v) \pmod{p}. \]

Set \( a = u - m, \quad b = v - u \). Then

\[ a \equiv -bx \pmod{p}. \]

Multiply both sides,

\[ a^2 = (-bx)^2 \equiv b^2x^2 \pmod{p} \]

\[ \equiv -b^2 \pmod{p}. \]

Thus, \( a^2 + b^2 = 0 \pmod{p} \). Hence we have \( p \mid (a^2 + b^2) \).

Again \( (a, v) \equiv (b, n) \), we have \( a^2 + b^2 > 0 \). Now we must show \( a^2 + b^2 \) cannot be larger than \( p \). Observe that

\( U \equiv N \) and \( m \geq 0 \), so

\[ a = u - m \leq N. \]

Similarly \( a \geq -N \) and \( -N \leq b \leq N \).

Thus, \( |a| \leq \sqrt{p} \) and \( |b| \leq \sqrt{p} \) \( \Rightarrow \)

\[ a^2 + b^2 < 2p. \]

However, \( p \) is the only multiple \( n \) in the range \((a, n)\), so it must be that \( a^2 + b^2 = p \).
We would now like to establish the result in the opposite direction; namely, if \( \exists a, b \in \mathbb{Z}_0 \) s.t. \( a^2 + b^2 = p \), then \( p \equiv 1 \pmod{4} \) (odd primes have 4 congruent). We accomplish this with the following lemma.

**Lemma:** Let \( q \) be an odd prime s.t. \( q \mid (a^2 + b^2) \) for \( a, b \in \mathbb{Z}_0 \).

If \( q \equiv 3 \pmod{4} \), then \( q \mid a \) and \( q \mid b \).

Before we prove the lemma, let's see how it gives the converse we are interested in.

Suppose \( p \) is an odd prime and \( \exists a, b \in \mathbb{Z}_0 \) s.t. \( p = a^2 + b^2 \). Let \( p \equiv 1 \pmod{4} \) be done. Since the only other case is \( p \equiv 3 \pmod{4} \) (\( p \) an odd prime) the lemma shows that we would have \( q \mid a \) and \( q \mid b \Rightarrow p^2 \mid p. \# \). Then, \( p \equiv 1 \pmod{4} \).

As it only remains to prove the lemma.

**Proof:** Suppose \( q \) is an odd prime s.t. \( q \mid (a^2 + b^2) \)

for some \( a, b \in \mathbb{Z}_0 \) with \( q \nmid a \) or \( q \nmid b \). Why we may assume \( q \nmid a \Rightarrow gcd(a, q) = 1 \). Thus \( \exists m, n \in \mathbb{Z} \) s.t. \( am + qn = 1 \). Thus, \( am \equiv 1 \pmod{q} \). Since \( q \mid (a^2 + b^2) \), we have \( a^2 + b^2 \equiv 0 \pmod{q} \), i.e.,
\[ a^2 \equiv -b^2 \pmod{q}. \] Multiply both sides by \( m^2 \) to obtain

\[(am)^2 \equiv -(bm)^2 \pmod{q}, \text{ i.e.} \]

\[-(bm)^2 \equiv 1 \pmod{q} \]  

\[ (bm)^2 \equiv -1 \pmod{q} \]. But this says we have a solution

to the congruence

\[ x^2 \equiv -1 \pmod{q}. \]

\[ \Rightarrow q \equiv 1 \pmod{4} \] \( \blacksquare \)
Public Key Cryptography

The notion that sensitive information should be encoded dates back to Roman times and possibly earlier. Julius Caesar was known to encrypt messages by a simple shifting algorithm; say, shift everything one letter to the right. Thus, "cl camc cl skw cl conqunr" would be sent as

"j dbnf, j txr, j dporysife"

The person receiving this message would then shift all the letters one to the left to decode the message. The problem with this is that it is very easy to break. One could just try all 26 possibilities and break the code!

A more difficult problem than the simplicity of the encryption method is the problem of relating the method of encryption and decryption. Suppose we want to write encrypted messages. Making a code that is difficult to break is not so hard to do. For example, the North had an encryption process in the Civil War that the South was never able to crack. The difficulty in that it was based on using a book with certain
rules in order to decrypt the messages. Think of modern security trying to work in this way. You want to place an order at Amazon. Do you need to give them your credit card? However, in order to set up an encryption scheme you need to physically get the scheme to Amazon. (If you send it over open channels it could be intercepted!) On top of that, then Amazon needs a different scheme for each customer!

This clearly is not the way to transmit information on the internet.

The solution is to have a public-key system. This is a system where you can publish a "key" to encrypt messages to be sent to you, but only you have the "key" that unlocks the message. Basically, think you make available "passwords" to everyone, but only you have the key that unlocks it, and the same key unlocks all the passwords that come to you!

There are various ways to set up a public-key cryptosystem. We will discuss the RSA system as the main ingredient in Fermat's little theorem. The RSA system was invented in 1977 by three
We read the following lemma.

The information n and e are displayed on your website.

e-mail,聊天 from our website, however you can get them.

And decrypting and sending to "p" and "g",

encrypt message sent to you. You keep it secret.

The information n and e are displayed on your website.

The information n and e are displayed on your website.

We read the following lemma.

The information n and e are displayed on your website.

The information n and e are displayed on your website.

The information n and e are displayed on your website.

The information n and e are displayed on your website.

The information n and e are displayed on your website.

The information n and e are displayed on your website.
Lemma: For $b \in \mathbb{Z}$, $b^{ed} \equiv b \pmod{n}$.

Proof: Recall that $de = \phi(\mu n)$

$$= 1 - (p-1)(q-1)f.$$  
$$= 1 + (p-1)(q-1)f.$$  
$$= f'(=-f).$$

Using this we have

$$b^{ed} = b^{1 + (p-1)(q-1)f'}$$

$$= b(b^{(p-1)(q-1)f'})$$

$$= b \pmod{p} \quad \text{by FLT if } \gcd(b, p) = 1.$$

Thus, $b^{ed} \equiv b \pmod{p}$ if $\gcd(b, p) = 1$. Of course, if $\gcd(b, p) > 1$, then $p|b$ and so $b^{ed} \equiv 0 \pmod{p}$ as well. Similarly, we have

$$b^{ed} \equiv b \pmod{q}$$

$\forall b \in \mathbb{Z}$.

Thus, $p | (b^{ed} - b)$ and $q | (b^{ed} - b)$

$$\Rightarrow \gcd(p, q) | (b^{ed} - b). \quad \text{Hence, } p \neq q \Rightarrow \gcd(p, q) = pg = n.$$

Hence,

$$b^{ed} \equiv b \pmod{n}$$

$\forall b \in \mathbb{Z}$. 

$\Box$
Next we set up a labelling system for our letters. One could include punctuation as well if desired.

\[ 00 = \text{space} \quad 01 = A \quad 02 = B \quad \ldots \quad 25 = Y \quad 26 = Z. \]

Suppose we wanted to encode the message

"I love number theory."

First we write this out as a number

\[ 09 \ 00 \ 12 \ 15 \ 22 \ 05 \ 00 \ 14 \ 21 \ 13 \ 02 \ 05 \ 18 \ 00 \ 20 \ 08 \ 05 \ 15 \ 18 \ 25. \]

Call this large number \( X \). As long as \( n > x \), we can break \( X \) into pieces. We will see such a case when we perform \( \phi \) in a moment.

Recall that \( n \) and \( e \) are public knowledge, so anyone
Wishing to send us an encoded message has access to them.

They calculate

\[ X^e \pmod{n} \]

Call the result of this calculation \( Y \). Note that this is performed quickly by a computer. However, extracting \( X \) back from this information is not easy to do! Even the person who encoded the message would be unable to recover the original message if it were forgotten!

However, we know the value \( n \) (private information). Then, we calculate

\[ Y^d \pmod{n} \]

By an lemma this gives

\[ (X^e)^d \equiv X \pmod{n} \]

Thus, we are able to retrieve the original message.

We now see how this works with a numerical example.

We use fairly small primes for clarity, though much larger
would be needed for security.
Let \( p = 59 \), \( q = 73 \). Then \( n = 4307 \) and \( k = 4176 \).

We pick \( d = 121 \). (Note that \( \gcd(121, 4176) = 1 \) as required.)

To calculate \( e \), we need to find \( e, f \in \mathbb{Z} \) so that

\[
121e + 4176f = 1.
\]

This is easily accomplished, \( e = 2761 \).

We wish to encrypt the message

"I love number theory".

The \( n \) here is rather small, so we will need to break \( x \) into several pieces. Since the largest 4 digit "word" can be \( 9999 \), we see all 4 digit words are smaller than \( n \) so we break \( x \) into 4 digit pieces.

0900 1215 2205 0014 2113
0205 1800 2008 0515 1835

Note that \( x \) divided evenly into pieces of 4. If this were not the case, we could add "spare" 00's at the end without affecting the message.

We use SAGE to compute
\[ 0900 \times 2761 \equiv 1265 \pmod{4307} \]
\[ 1215 \times 2761 \equiv 2526 \pmod{4307} \]
\[ 2205 \times 2761 \equiv 2967 \pmod{4307} \]
\[ 0014 \times 2761 \equiv 1991 \pmod{4307} \]
\[ 2113 \times 2761 \equiv 4275 \pmod{4307} \]
\[ 0205 \times 2761 \equiv 0783 \pmod{4307} \]
\[ 1503 \times 2761 \equiv 1758 \pmod{4307} \]
\[ 0205 \times 2761 \equiv 0880 \pmod{4307} \]
\[ 0515 \times 2761 \equiv 3682 \pmod{4307} \]
\[ 1835 \times 2761 \equiv 3869 \pmod{4307} \]

So the message would be sent as

1265 2526 2967 1991 4275 0783
1758 0880 3682 3869

Of course, you don't want people reading an encoded message claiming to be you. There is a way to prevent this by using an electronic signature. Suppose your information is

\[ p = 71 \quad k = 3640 \]
\[ q = 53 \quad d = 1111 \]
\[ n = 3763 \quad e = 3391 \]
The only thing I am able to see though is

\[ n = 3763 \]
\[ e = 3391. \]

To sign your message, you need to encode your name as follows:

John Doe
1015 0814 0004 1505

Encrypted:

\[ 1015_{1111} \equiv 2152 \pmod{3763} \]
\[ 0814_{1111} \equiv 0422 \pmod{3763} \]
\[ 0004_{1111} \equiv 3059 \pmod{3763} \]
\[ 1505_{1111} \equiv 1434 \pmod{3763}. \]

As you can sign the letter as

Sincerely,

John Doe
2152 0422 3059 1434
\[ n = 3763 \]
\[ e = 3391. \]

Now everyone can look at
And see that the letter is really from John Doe, but more can encode it to look like John Doe because more else has the "d" to encode with.

As I know the message is really from you. Now I decode the message using my "d":

\[
1265^{231} \equiv 0900 \pmod{4307}
\]

\[
2526^{151} \equiv 1215 \pmod{4307}
\]

\[
3869^{101} \equiv 1825 \pmod{4707}.
\]

Now I write:

```
1215 1215 0305 0014 0412
0105 1960 0908 0515 1825
```

and substitute letters to find that John Doe loves numbers theory.
On the homework you will be asked to choose your own number to send an encoded message back and forth with me. You'll send me your number, I will send you an encoded question. You will find the answer to the question and send it encoded back to me.

So how would we do this using 

Do not do this in the notebook. Our necessary functions are built into Mathematica, so how is how I did it.

```
SAGE: mathematica.example()

open up mathematica

N = 09001215...1825

Mod[(IntegerDigits[n, 10^4])^2961, 4307]

return

{1265, 2526, 2967, ... 3869}.

One can determine the number of digits of

n by

N = Sum[DigitCount[n, 10^j], {j, 1, 10}].

With `SAGE`

n = mathematica(Stefan)

n. Digit Count()
We now continue with our study of solving polynomial congruences.

Thus far we have seen how to solve linear congruences of the form

\[ a x \equiv b \pmod{n} \]

as well as how to use solutions of \( f(x) \equiv 0 \pmod{m} \) to produce solutions of \( f(x) \equiv 0 \pmod{mn} \). Our next step is to study quadratic congruences of the form

\((*)\) \quad \[ a x^2 + bx + c \equiv 0 \pmod{p} \]

where \( p \) is an odd prime and \( p \not| a \).

Since \( \gcd(p, a) = 1 \), we have that equation \((*)\) is equivalent to equation

\[ 4a (ax^2 + bx + c) \equiv 0 \pmod{p} \]

However,

\[ 4a (ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac) \]

we have that \((*)\) is equivalent to

\[ (2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}. \]

Setting \( y = 2ax + b \) and \( d = b^2 - 4ac \), we are left with

\[(\#) \quad y^2 \equiv d \pmod{p}.\]

(Check that we have equivalent as an exercise!)
Note that we have reduced solving quadratic congruence down to
solving congruence of the form

\[ x^2 \equiv a \pmod{p}. \]

e.g. if \( p \mid a \), then \( x = 0 \) is a solution. From now on we assume
\( p \nmid a \).

Let \( x_0 \) be a solution so that

\[ x_0^2 \equiv a \pmod{p}. \]

Then we have

\[ (x_0-p)^2 = (p-x_0)^2 = p^2 - 2px_0 + x_0^2 \]

\[ \equiv a \pmod{p}. \]

Thus, \( p-x_0 \) is another solution. \( \forall \ x_0 \equiv p-x_0 \pmod{p} \), we
have \( 2x_0 \equiv 0 \pmod{p} \) \( \Rightarrow p \mid x_0 \). This contradicts \( p \nmid a \), so
then are two solutions. Thus, any congruence has exactly
2 solution or no solution. (Your homework shows \( f(x) \equiv 0 \pmod{p} 
has at most 2nd of solution).

What we are really trying to do is determine all the perfect
square modulo \( p \).

**Def.** Let \( p \) be an odd prime and \( \gcd(a,p)=1 \). \( \forall \)

\[ x^2 \equiv a \pmod{p} \] has a solution, then \( a \) is said to
be a **quadratic residue modulo** \( p \). Otherwise it is
Example: Consider $p=17$. To find the quadratic residue we can compute all the squares $a^2 \pmod{17}$. This is enough because if $a^2 \equiv b^2 \pmod{17}$, then $a^2 \equiv b^2 \pmod{17}$. So we are able to compute all quadratic residue by just looking at a complete residue system.

We have

\[\begin{align*}
1^2 & \equiv 1 \pmod{17} \\
2^2 & \equiv 4 \pmod{17} \\
3^2 & \equiv 9 \pmod{17} \\
4^2 & \equiv 16 \equiv 13 \pmod{17} \\
5^2 & \equiv 8 \pmod{17} \\
6^2 & \equiv 2 \pmod{17} \\
7^2 & \equiv 15 \equiv 10 \pmod{17} \\
8^2 & \equiv 13 \equiv 9 \pmod{17}
\end{align*}\]

Thus, the quadratic residues are \{1, 2, 3, 4, 6, 7, 8, 9, 10, 13, 15, 16\} and the nonresidues are \{3, 5, 6, 7, 10, 11, 12, 14\}. Note that there are the same number of quadratic residues as nonresidues.

Eventually we will prove this is true in general.
Before we can go into quadratic residues any further we need to develop the notion of primitive roots.

We know from Euler's theorem that any integer \( a \) with \( \gcd(a, n) = 1 \) satisfies

\[ a^{\phi(n)} \equiv 1 \pmod{n}. \]

However, it is often the case that there are smaller integers that we can raise \( a \) to and get 1 modulo \( n \). For example, we know that

\[ \phi(16) = 8 \]

but

\[ 15^{2} \equiv 1 \pmod{16}. \]

This leads to the following definition:

**Def:** Let \( n \in \mathbb{Z}_{+} \) and \( a \in \mathbb{Z} \) with \( \gcd(a, n) = 1 \). The order of \( a \) modulo \( n \), written \( \text{ord}_{n}(a) \), is the smallest positive integer \( s \) such that

\[ a^{s} \equiv 1 \pmod{n}. \]

Thus, in our example we had \( \text{ord}_{16}(15) = 2 \).

We only include \( a \in \mathbb{Z} \) with \( \gcd(a, n) = 1 \) since if \( \gcd(c, n) = d > 1 \), we do not have a power we can raise \( a \) to and get 2. If we did, then

\[ a^{(a^{\text{ord}_{n}(a)-1})} \equiv 1 \pmod{n} \Rightarrow \gcd(a, n) = 1. \]
Theorem: Let \( a \) be a non-zero integer
modulo \( n \). Then \( a^{\text{ord}_n(a)} \equiv 1 \) (mod \( n \)) if and only if \( \text{ord}_n(a) \) is a divisor of \( n \).

Proof: \( \Rightarrow \) Let \( \text{ord}_n(a) = k \). Write \( h = qk + r \) with \( 0 \leq r < k \).

Then we have
\[
1 = a^h \quad (\text{mod } n) \\
= a^{qk+r} \quad (\text{mod } n) \\
= (a^k)^q \cdot a^r \quad (\text{mod } n) \\
= a^r \quad (\text{mod } n)
\]

But this contradicts the minimality of \( k \) unless \( r = 0 \). Hence \( a^h \equiv 1 \) (mod \( n \)).

\( \Leftarrow \) Suppose \( a^r \equiv 1 \) (mod \( n \)) with \( 0 \leq r < k \). Then,
\[
1 = a^h = a^{qk+r} = (a^k)^q \cdot a^r \\
= 1^q \cdot a^r \equiv 1 \quad (\text{mod } n)
\]

This theorem significantly reduces our computations in looking for orders; we only need to look at those integers \( k \) that divide \( \varphi(n) \).

Another basic fact is given by the following theorem.

Theorem: Let \( a \in \mathbb{Z} \) with \( \text{ord}_n(a) = k \). Then \( a^i \equiv a^j \) (mod \( n \)) if and only if \( i \equiv j \) (mod \( k \)).

Proof: \( \Rightarrow \) Suppose \( a^i \equiv a^j \) (mod \( n \)). Since \( \gcd(a, n) = 1 \), we can cancel out powers of \( a \). Why assume that \( i \equiv j \) (mod \( k \))?
Cancelling powers of \( a \) we obtain
\[
\alpha^{i-j} \equiv 1 \pmod{n}.
\]

The previous theorem implies \( k | i-j \), i.e., \( i \equiv j \pmod{n} \).

"\( \Rightarrow \)" Suppose \( i \equiv j \pmod{k} \). Write \( i = j + kt \) for some \( t \in \mathbb{Z} \).

Then we have
\[
\alpha^i = \alpha^{j + kt} = \alpha^j \alpha^{kt} = \alpha^j \alpha^{kt} \pmod{n} = \alpha^j \pmod{n}.
\]

This theorem immediately shows that if \( \operatorname{ord}_n(a) = k \), then
\( a, a^2, \ldots, a^k \) are all distinct modulo \( n \). Note that
if \( \operatorname{ord}_n(a) = \phi(n) \), then we have \( a, a^2, \ldots, a^{\phi(n)} \) are \( \phi(n) \) distinct elements modulo \( n \), so form a reduced residue system modulo \( n \).

**Thm:** If \( \operatorname{ord}_n(a) = k \) and \( h = 2k \), then \( a^h \) has order
\[
\frac{k}{\gcd(h, k)} \mod n.
\]

**Proof:** We need to show that \( \alpha^{\frac{k}{\gcd(h, k)}} \equiv 1 \pmod{n} \) and
that \( \frac{k}{\gcd(h, k)} \) is the smallest such integer.

Let \( \operatorname{ord}_n(a^h) = r \). First observe that
\[
(a^h)^{\frac{k}{\gcd(h, k)}} = a^{\frac{hk}{\gcd(h, k)}}
\]
\[
= (a^k)^{\frac{h}{\gcd(h, k)}} \equiv 1 \pmod{n}.
\]
We have necessarily that \( r \mid \frac{k}{\gcd(h, k)} \). We also have that

\[
a^h \equiv (a^h)^{\frac{k}{\gcd(h, k)}} \equiv 1 \pmod{n}
\]

\[
\Rightarrow k \mid hr. \text{ Thus, } \frac{k}{\gcd(h, k)} \mid \frac{hr}{\gcd(h, k)}. \text{ Hence}
\]

\[
\gcd\left(\frac{h}{\gcd(h, k)}, \frac{k}{\gcd(h, k)}\right) = 1, \text{ we have that } \frac{k}{\gcd(h, k)} \mid r.
\]

Thus, \( r = \frac{k}{\gcd(h, k)} \) as claimed.

**Cor:** Let \( \text{ord}_n(a) = k \), then \( \text{ord}_n(a^h) = k \) if \( \gcd(h, n) = 1 \).

**Def:** if \( \gcd(h, n) = 1 \) and \( \text{ord}_n(a) = \phi(n) \), we say \( a \) is a **primitive root modulo** \( n \).

Note that in abstract algebra terms this says that \( a \) is a generator of \( \left( \mathbb{Z}/n\mathbb{Z} \right)^* \), i.e., \( \langle a \rangle = \left( \mathbb{Z}/n\mathbb{Z} \right)^* \).

The reason these primitive roots are important is exactly this fact. In our language, what this is saying is the following theorem.

**Thm:** Let \( \gcd(h, n) = 1 \) and let \( a \) be a primitive root.

If \( a, a^2, \ldots, a^{\phi(n)} \) is a reduced residue system modulo \( n \), then

\[
\{ a, a^2, \ldots, a^{\phi(n)} \} \equiv \{ a, a_2, \ldots, a_{\phi(n)} \} \pmod{n}
\]
Proof: This fact is clear from the fact that the $a_i$ are
independent and the fact that the sets have the same
number of elements.

Claim: If there is a primitive root modulo $n$, then there are
$\phi(n)$ of them.

Proof: Let $a$ be a primitive root modulo $n$. Then
$a, a^2, \ldots, a^{\phi(n)}$ give all the relatively prime elements
modulo $n$. Thus, any other primitive root must be among these elements. An element $a^b$ has order
$\phi(n)$ iff $\text{gcd}(b, \phi(n)) = 1$ since the order of
$a^b$ is given by
$$\frac{\phi(n)}{\text{gcd}(b, \phi(n))}.$$ 

This is precisely $\phi(n)$ integers $1 \leq b \leq \phi(n)$ that
are relatively prime to $\phi(n)$.

Here is an easy way to find primitive roots modulo $n$.
(There are probably much better ways, but I was having
issues with the commands in SAGE that are preprogrammed.

\[ \mathbb{Z} = \text{Integers}(n). \quad \text{(this constructs} \ \mathbb{Z}/n\mathbb{Z}). \]

for \( i \) in range \((0, \text{n})\):

    if \( \gcd(i, \text{n}) = 1 \):

        print

        if \( R(i) \cdot \text{multiplicative_order}(i) = \text{euler_phi}(\text{n}) \):

            print \( i \)

For example, if we run this with \( n=10 \) it

returns \( 3, 7 \). Then, 3 and \( 7 \) are primitive roots modulo 10.

If we run this with \( n=736 \), it returns nothing

letting us know there are no primitive roots modulo 736.

This naturally leads to the question of for which

\( n \) do primitive roots exist?

We begin by showing that if \( n=p \) a prime then there
is a primitive root modulo \( p \). In terms of abstract
algebra, this is just the statement that \( (\mathbb{Z}/p\mathbb{Z})^* \)
is cyclic. This takes some effort to prove even with abstract
algebra.
In the homework you will prove the following theorem:

Theorem 1 (Legendre): If $p$ is prime and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

with $a_n \not\equiv 0 \pmod{p}$, then $f(x) \equiv 0 \pmod{p}$ has at most $n$ distinct solutions modulo $p$.

Recall that if the modulus isn't prime, this statement is not necessarily true! For example, $f(x) = x^2 - 1$ has 4 distinct solutions modulo 15!

Corollary: If $p$ is a prime and all $p-1$, then

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

has exactly $p-1$ solutions.

Note that this does not give us the existence of primitive roots. It could be that all the solutions have order less than $p-1$ as far as the theorem tells us!

Proof: We use the fact that $\phi(p-1)$ to conclude $\exists \alpha \in \mathbb{Z}$

$s.t \ p-1 = \alpha k$. Thus, $f(x) \in \mathbb{Z}[x]$ on $\mathbb{Z}$

$$x^{p-1} - 1 = (x^{d-1} - 1) f(x).$$

In particular, one can calculate that

$$f(x) = x^{d(t-1)} + x^{d(t-2)} + \cdots + x^{d+1}.$$
Lagrange's theorem gives that

\[ f(x) \equiv 0 \pmod{p} \]

has at most \( d \cdot (p - d) = p - 1 - d \) solutions. Fermat's little theorem gives that \( x^{p-1} - 1 \equiv 0 \pmod{p} \) has \( p-1 \) incongruent solutions modulo \( p \).

We claim that any solution of

\[ x^{p-1} \equiv 1 \pmod{p} \]

that is not a solution of

\[ f(x) \equiv 0 \pmod{p} \]

must satisfy the congruence

\[ x^{d \cdot (p-1)} - 1 \equiv 0 \pmod{p}. \]

This follows immediately from the factorization of \( x^{p-1} - 1 \) and the fact that \( p \) is prime. Thus, \( x^{d \cdot (p-1)} - 1 \equiv 0 \pmod{p} \) must have at least

\[ (p-1) - (p-1-d) = d \]

incongruent solutions modulo \( p \). Since Lagrange's theorem says it can have at most \( d \), we have the result.
We need the following theorem of Gauss:

**Theorem:** For each \( n \in \mathbb{Z}_n \),

\[
\sum_{d|n} \phi(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right).
\]

**Proof:** We separate the integers \( 1 \leq i \leq n \) by setting

\[
S_d = \{ m : \gcd(m,n) = d, 1 \leq m \leq n \}.
\]

We have shown that \( \gcd(m,n) = d \iff \gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1 \).

This gives that \( S_d \) contains integers relatively prime to \( \frac{n}{d} \) that do not exceed \( \frac{n}{d} \). This is precisely \( \phi\left(\frac{n}{d}\right) \).

Since each integer lies in some \( S_d \), we have

\[
\sum_{d|n} \#S_d = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{e|n} \phi(e).
\]

We will use this theorem to prove the following result:

**Theorem:** Let \( p \) be a prime and \( d \in \mathbb{Z}_p \). There are \( \phi(d) \) distinct numbers modulo \( p \) with \( \text{ord}_p d = d \).
Proof: Let $\Psi(d)$ be the number of integers $k \equiv 1 \pmod{p-1}$ and 
ord_p(k) \equiv d. Each $k$ with $1 \leq k \leq p-1$ must have order
$e \mid p-1$ for some $e$, since $\phi(p) = p-1$. Thus,

$$p-1 = \sum_{d \mid p-1} \Psi(d).$$

We also know that

$$p-1 = \sum_{d \mid p-1} \phi(d).$$

and so

$$\sum_{d \mid p-1} \phi(d) = \sum_{d \mid p-1} \Psi(d).$$

If we can show that $\Psi(d) \leq \phi(d)$ for all $d \mid p-1$, we
will have $\Psi(d) = \phi(d)$ as desired since then

$$\sum_{d \mid p-1} \Psi(d) \leq \sum_{d \mid p-1} \phi(d) = \sum_{d \mid p-1} \Psi(d).$$

$e \mid p-1$.

Let $e \mid p-1$. Either $\Psi(e) = 0$ or $\Psi(e) > 0$. If $\Psi(e) = 0$,
then trivially we have $\Psi(e) \leq \phi(e)$. Thus, assume
$\Psi(e) > 0$; i.e., there is an $e \mid p-1$ and $\ord_p(e) = e$.

Thus we have $e$ distinct integers $a, a^2, \ldots, a^e$
all $\leq e$.

Thus $X^e - 1 \equiv 0 \pmod{p}$.

But we have shown there are all the solutions to the
congruence. Thus, any integer of order $e$ must be congruent to one of these. However, among the $\psi$'s there are only $\psi(e)$ by order $e$, namely the one in $\psi(d)(k,e)=1$. Thus, $\psi(e)=\psi(d)$.

Thus we have the result.

This theorem shows that there are always primitive root modules $p$ since $p-1 \mid p-1$.

Before we return to quadratic congruences, we prove a couple of interesting results concerning primitive roots. We will determine exactly when an integer $n$ has a primitive root.

**Theorem:** If $\gcd(m,n) = 1$ and $m, n > 1$, then there are no primitive roots modulo $mn$.

**Proof:** We claim that the order of any integer $a \equiv \frac{\psi(mm)}{2}$ is less than or equal to $\frac{\psi(mm)}{2}$. If we show this, then clearly there are no primitive roots modulo $mn$.

Since $m$ and $n$ are both greater than 1, each has an odd prime that divides it. Thus, if $p \mid m$ is odd, then $p-1 \mid \psi(m)$ and $\frac{\psi(m)}{2}$ is even. Similarly, we get $\psi(n)$ is even. Thus, $\gcd(\psi(m),\psi(n)) = 2$. 


We have if \( d = \text{gcd}(\phi(m), \phi(n)) \),
\[
h \cdot \text{lcm}(\phi(m), \phi(n)) = \frac{\phi(n) \cdot \phi(m)}{d} \leq \frac{\phi(m) \cdot \phi(n)}{2}.
\]

By Euler we know
\[
a^{\phi(m)} \equiv 1 \pmod{m}.
\]

\[\Rightarrow \quad \phi\left( a^{\phi(m)} \right) \equiv 1 \pmod{m}
\]

\[\Rightarrow \quad a^{h} \equiv 1 \pmod{m}.
\]

Similarly, we get \( a^{h} \equiv 1 \pmod{m} \). Since \( \text{gcd}(m, n) = 1 \), we have
\[
a^{h} \equiv 1 \pmod{mn}, \quad \text{hence} \quad \text{ord}(a) \mid h = \frac{\phi(m) \cdot \phi(n)}{d}.
\]

The next step is to investigate powers of \( \phi \).

Then: For \( k \geq 3 \), there are no primitive roots modulo \( 2^k \).

Proof: We claim that for any odd integer \( a \), if \( k \geq 3 \),

\[
a \cdot 2^{k-2} = 1 \pmod{2^k}.
\]

Hence this claim.

For a moment, let's see how to finish the proof:

The integers relatively prime to \( \phi(2^k) \) are the odd integers less than \( 2^k \), which there are \( 2^{k-1} \) of, i.e., \( \phi(2^k) = 2^{k-1} \).

However, given the claim we know \( \text{ord}_{2^k}(a) \cdot 2^{k-2} = 6(3^2)^{1/2} \)
for all odd \( a \). Thus, there are no primitive roots. As it only remains to prove \((*)\) to finish the proof. We prove this by induction on \( k \).

\[ k = 3: \]
\[ a^2 \equiv 1 \pmod{2^3} \]

Just check the cases: \( 1^2, 3^2, 5^2, 7^2 \equiv 1 \pmod{2^3} \).

Now assume the statement is true for all \( 3 \leq n \leq N \) for some \( N \in \mathbb{Z}^+ \). In particular,

\[ a^{2^{N-3}} \equiv 1 \pmod{a^N}. \]

As \( \exists \ t \in \mathbb{Z}^+ \) \( a^t \equiv 1 \pmod{a^N} \),

we square both sides to obtain

\[ a^{2^{N-3}} = 1 + t \cdot 2^N. \]

As desired, thus \((*)\) holds for all \( k \geq 3 \) by induction.

We combine these results to conclude:

\textbf{Claim:} if \( n \) is divisible by 2 odd primes \( n = 2^m p^r \) where \( p \) is odd prime, \( m \geq 3 \) then there are no primitive roots \( \pmod{n} \).
Proof: This example is just a special case of the theorem above with
\[ q \equiv (m, n) \equiv 1. \]

Thus, we only have to consider
\[ n = 2, 4, p^k, \] and \[ 2p^k \]
where \( p \) is an odd prime as possibilities for having primitive roots.

The positive is that we will have a complete classification when \( n \) has a primitive root. The negative is that we must find or construct
have primitive roots and p-primitive roots and primitive roots can make life much easier!

We must prove some rather painful technical lemmas to
prepare us to prove our main result.

Lemma: Let \( p \) be an odd prime. There exists a primitive root
\( r \) of \( p \) such that
\[ r^{p-1} \not\equiv 1 \mod (p^2). \]

Proof: We already know that non-primitive roots modulo \( p \),
so choose one and call it \( r \). If we have that
\[ r^{p-1} \equiv 1 \mod (p^2), \]
we are done. Assume \( r^{p-1} \equiv 1 \mod (p^2) \). Then we have
\[(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2} + \ldots \]
\[\equiv r^{p-1} \pmod{p} \]
\[\equiv 1 \pmod{p}.\]

Then an odd prime divides \( r+1 \), so \( r+1 \) is also a primitive root modulo \( p \). (They are equal modulo \( p \), due to a theorem modulo \( p^2 \) we have:

\[(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2} + (p^2-1)r^{p-3} + \ldots \]
\[\equiv r^{p-1} - (p-1)r^{p-2} \pmod{p^2} \]

We assumed \( r^{p-1} \equiv 1 \pmod{p^2} \), so

\[(r+p)^{p-1} \equiv 1 + (p-1)r^{p-2}. \]

Hence \( r \) is a primitive root modulo \( p \), \( p \) divides \( r^{p-1} - 1 \).

\[(r+p)^{p-1} \equiv 1 \pmod{p^2}. \]

So we have the result. \( \ast \)

**Corollary:** Let \( p \) be an odd prime. Then \( r \) is a primitive root modulo \( p^2 \). More precisely, if \( r \) is a primitive root modulo \( p \),

then \( r \) or \( r+p \) is a primitive root modulo \( p^2 \).

**Proof:** Observe that \( \varphi(p^2) = p(p-1) \), so if \( r \) is primitive mod \( p \),

then \( r \) has order \( p-1 \) or \( p(p-1) \) modulo \( p^2 \). (It must divide
\[ \phi(p^2), \text{ and if we had } r \equiv 1 \pmod{p}, \text{ then } r \equiv 1 \pmod{mp}. \]
\[ \Rightarrow r \equiv 1 \pmod{mp} \Rightarrow r \equiv 1 \pmod{mp}! \quad \text{if } r \text{ has order } \phi(p) \text{ modulo } p^2 \text{ we are done. If } r \text{ has order } p-1 \text{ modulo } p^2, \text{ then we just seen that } r^{mp} \text{ must have order } \phi(p). \quad \text{(We can't have order } p-1 \text{ from last proof).} \]

**Lemma:** Let \( p \) be an odd prime and \( r \) a primitive root modulo \( p \) so that \( r^{p-1} \not\equiv 1 \pmod{p^2} \). Then for each \( k \in \mathbb{Z} \),
\[ r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^2}. \]

**Proof:** We prove this by induction on \( k \). The case \( k = 2 \) uses our previous lemma. Suppose the result holds for \( 2 \leq n \in \mathbb{N} \) from \( n = 2, 3, \ldots \). Since \( r \) is primitive modulo \( p \),
\[ \gcd(r, p) = 1 \text{ so Euler's } \]
\[ r^{\varphi(p^{n-1})} \equiv 1 \pmod{p^{n-1}} \]
\[ \text{let } \]
\[ r^{p^{n-2}(p-1)} \equiv 1 \pmod{p^{n-1}}. \]
\[ \text{As } j \in \mathbb{Z} \text{ set } \]
\[ r^{p^{n-2}(p-1)} = 1 + k r^{p^{n-1}}. \]
\[ \text{for } p \not| t \text{ (by induction hyp).} \]
Raising both sides to the $p$ we get:

$$r^{p^{N+1}(p-1)} = (1 + t r^{N+1})^p$$

$$= 1 + t p^{N+1} \pmod{p^{N+1}}$$

Hence, since $p \nmid t$, this gives that

$$r^{p^{N+1}(p-1)} \neq 1 \pmod{p^{N+1}}$$

as desired.

We are now able to prove the following theorem.

**Thm:** Let $p$ be an odd prime and let $k \in \mathbb{Z}_+$. There exists a primitive root modulo $p^k$.

**Proof:** Choose $r$ a primitive root so that

$$r^{p^{k-2}(p-1)} \neq 1 \pmod{p^k}.$$

Let $n = \text{ord}_{p^k}(r)$. We know $n | \phi(p^k) = p^{k-1}(p-1)$.

Using the fact that $r^n \equiv 1 \pmod{p^k}$, we also have

$$r^n \equiv 1 \pmod{p}$$

as well. Thus, we can write

$$n = p^m(p-1)$$

for some $0 \leq m < k-1$. If $n \neq p^{k-1}(p-1)$, then we would have $n | p^{k-2}(p-1)$ and $n$
Thus \( n = p^{\alpha n} (p-1) \) and \( r \) is a primitive root modulo \( p^k \).

Finally, we deal with the case \( n = 3p^k \).

\textbf{Case:} There are primitive roots modulo \( 3p^k \) for \( p \) an odd prime and \( k \geq 1 \).

\textbf{Proof:} Let \( r \) be a primitive root modulo \( p^k \). We may assume \( r \) is odd. (If not, \( r+p^k \) is odd and still a primitive root modulo \( p^k \!\).) As \( \gcd (r, 3p^k) = 1 \),

the order of \( r \) modulo \( 3p^k \) must divide

\[ \varphi(3p^k) = \varphi(3) \varphi(p^k) = 2 \varphi(p^k). \]

However,

\[ r^{\varphi(p^k)} \equiv 1 \pmod{p^k} \Rightarrow r^{\varphi(p^k)} \equiv 1 \pmod{3p^k} \]

\[ = \varphi(3)p^k. \]  Thus, \( \varphi(p^k) = k \).

We will now use this theory to study quadratic congruences further. We sum up with the following theorem.
Theorem: Let $n \in \mathbb{Z}_{>1}$. There is a primitive root modulo $n$ iff 
$n = 2, 4, p^k, 2p^k$ 
for $p$ an odd prime.
Now that we have studied primitive roots we return to studying quadratic congruences. Recall we were interested in determining for which values of $a$ the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution. Also recall the following definition:

**Def:** Let $p$ be prime and $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. We say that $a$ is a solution to $x^2 \equiv a \pmod{p}$ if there is an integer $x$ such that

$$x^2 \equiv a \pmod{p}.$$

We say $a$ is a **quadratic residue** modulo $p$.

The first result we prove is Euler's criterion. Let us briefly formulate the problem theoretically. It is very useful for proving theorems and computing with small values of $p$. However, it is most something to use for large $p$. The quadratic reciprocity law will give us an effective way to work with large primes.

**Theorem (Euler's Criterion):** Let $p$ be an odd prime, $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. Then $a$ is a quadratic residue modulo $p$ if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

**Proof:** $\Rightarrow$ Let $x$ be a quadratic residue modulo $p$. Then $x \equiv a^{(p-1)/2} \pmod{p}$. Replacing both sides with $(p-1)/2$ we have
\[ y^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}. \] Hence, \( y^{p-1} \equiv 1 \pmod{p} \) by Euler's theorem, thus \( a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \).

\[ \iff \]

Assume \( a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \). Let \( r \) be a primitive root modulo \( p \). Then exist \( k \in \mathbb{Z} \) s.t. \( r^k = a \). We have

\[ (r^k)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \]

Thus, \( r^{k \cdot \frac{p-1}{2}} \equiv 1 \pmod{p} \) or \( k \cdot \frac{p-1}{2} \mid (p-1) \)

\[ \iff k \mid 2j. \] As \( j \in \mathbb{Z} \), there exist \( k = 2j \). Thus,

\[ (r^j)^2 \equiv 1 \pmod{p} \]

and so \( a \) is a quadratic residue.

One should note that since \( (a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p} \), we must have \( a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p} \). (We now define the only \( x \) for \( x^2 \equiv 1 \pmod{p} \) as \( x = \pm 1 \).) As we could write Euler's criterion as \( "a\) is quadratic nonresidue iff \((a^{\frac{p-1}{2}}) \not\equiv -1 \pmod{p} \)."

**Example:** Consider the prime 137. (Use SAGE here).

Observe that \( 3^{\frac{137-1}{2}} \equiv -1 \pmod{137} \), so 3 is a quadratic nonresidue. 56 the same.

Observe that \( 7^{\frac{137-1}{2}} \equiv 1 \pmod{137} \), so 7 is a quadratic residue modulo 137.
We now introduce the Legendre symbol, a useful shorthand for talking about quadratic residues.

**Def:** Let $p$ be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol $\left( \frac{a}{p} \right)$ is defined by

$$\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue of } p \\
-1 & \text{if } a \text{ is a quadratic nonresidue of } p \\
0 & \text{if } p | a.
\end{cases}$$

**Example:** $p = 137$

$$\left( \frac{3}{137} \right) = -1$$
$$\left( \frac{5}{137} \right) = -1$$
$$\left( \frac{7}{137} \right) = 1.$$

**Theorem:** Let $p$ be an odd prime and $a, b \in \mathbb{Z}$.

1. If $a \equiv b \pmod{p}$, then $\left( \frac{a}{p} \right) = \left( \frac{b}{p} \right)$.
2. If $\gcd(a, p) = 1$, then $\left( \frac{a^2}{p} \right) = 1$.
3. $\left( \frac{a}{p} \right) = a^{\frac{p-1}{2}} \pmod{p}$.
4. $\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right)$.
5. $\left( \frac{-1}{p} \right) = 1$, $\left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}$.

**Proof:** Most of these are very easy. We prove property 5 as it
is the only one that really requires any work. Using (3) we have
\[
\left( \frac{a \cdot b}{p} \right) = \left( \frac{a}{p} \right) \cdot \left( \frac{b}{p} \right) \pmod{p}.
\]
Thus, \( \left( \frac{a \cdot b}{p} \right) \equiv \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \pmod{p} \). If \( p \mid a \) or \( p \mid b \), then
the statement is clear, that \( \left( \frac{a \cdot b}{p} \right) \equiv \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \pmod{p} \). Assume \( p \nmid a \),
\( p \nmid b \). Then \( \left( \frac{a \cdot b}{p} \right) = \pm 1 \), \( \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \pm 1 \). Since \( p = 2 \) or odd,
we have that \( \left( \frac{a \cdot b}{p} \right) \equiv \pm 1 \pmod{p} \) iff \( \left( \frac{a}{p} \right) = \pm 1 \). Thus,
\[
\left( \frac{a \cdot b}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right).
\]

And: \( \frac{a}{p} \) is an odd prime, then
\[
\left( \frac{-1}{p} \right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}
\]

Example: Determine if \( x^2 \equiv 12 \pmod{37} \) has any solutions.

If it does, find them.

We are asking if 12 is a quadratic residue of 37. That
is, the same as asking to determine \( \left( \frac{12}{37} \right) \).

\[
\left( \frac{12}{37} \right) = \left( \frac{2^2 \cdot 3}{37} \right) = \left( \frac{2^2}{37} \right) \left( \frac{3}{37} \right)
\]

\[
= \left( \frac{2}{37} \right) \left( \frac{3}{37} \right)
\]

\[
\equiv \left( \frac{3}{37} \right) \equiv 3^{\frac{36}{2}} \equiv 3^6 \equiv 1 \pmod{37}.
\]

Thus, there is a solution! Now we just check the element to
See which is a solution.

\[ 7^2 \equiv 12 \pmod{37} \]

Thus, \( 7 \) and \( 37-7=30 \) are the two solutions!

**Theorem:** Let \( p \) be an odd prime, then

\[ \sum_{a=\frac{p+1}{2}}^{p-1} \left( \frac{a}{p} \right) = 0. \]

**Proof:** Let \( r \) be a primitive root modulo \( p \). Then for each \( 1 \leq a \leq p-1 \), there exists a unique \( 1 \leq k \leq p-1 \) such that \( a \equiv r^k \pmod{p} \). Thus,

\[ \left( \frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \equiv \left( r^k \right)^{\frac{p-1}{2}} = \left( r^{\frac{p-1}{2}} \right)^k \]

\[ \equiv (-1)^k \pmod{p}. \]

Here we have used that for a primitive root \( r \), \( r^{\frac{p-1}{2}} \equiv -1 \pmod{p} \).

This is in fact a homework problem!

Thus, for each \( a \) we have

\[ \left( \frac{a}{p} \right) \equiv (-1)^k \pmod{p}. \]

Since \( (-1)^k = \pm 1 \), we have \( \left( \frac{a}{p} \right) = (-1)^k \). The principle applied to associating the \( a \)'s with the \( k \)'s gives

\[ \sum_{a=1}^{p-1} \left( \frac{a}{p} \right) = \sum_{k=1}^{p-1} (-1)^k = 0. \]
**Corl.** There are the same number of quadratic residues as nonresidues.

**Proof:** if there were more quadratic residues, then

$$\sum_{\alpha=1}^{\frac{p-1}{2}} \left( \frac{\alpha}{p} \right) > 0.$$  

Similarly for more quadratic nonresidues. \[\square\]

**Corl:** Let \( r \) be a primitive root modulo \( p \). All of the quadratic residue modulo \( p \) occur as \( r^2, r^4, \ldots, r^{p-1} \), and all the nonresidues occur as \( r, r^3, r^5, \ldots, r^{p-2} \).

**Proof:** we know \( r, r^2, \ldots, r^{p-1} \) are all of the distinct elements modulo \( p \) since \( r \) is primitive. Hence they must be quadratic residues by the previous corollary.

It is easy to see the even powers are quadratic residues:

$$\left( r^k \right)^2 \equiv r^{2k} \pmod{p}.$$  

Since this accounts for half of the elements, it must be the other half are nonresidues. \[\square\]

The following lemma will be fundamental in our proof of the quadratic reciprocity law:
Hensel's Lemma: Let \( p \) be an odd prime and let \( a \in \mathbb{Z} \) s.t. \( \text{gcd}(a, p) = 1 \). Let \( n \) be the one number of elements \( \mathbb{Z}/p\mathbb{Z} \) that \( a \) is\( a, 2a, 3a, \ldots, (\frac{p-1}{2})a \),

where \( \text{remainder upon division by } p \) exceed \( \frac{p}{2} \). Then

\[
\left( \frac{a}{p} \right) = (-1)^n.
\]

Before we prove this lemma, we state the quadratic reciprocity law as it is an ultimate goal here.

**Quadratic Reciprocity Law:** Let \( p \) and \( q \) be distinct odd primes. Then

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.
\]

Let us compute an example using the law to see its power.

**Example:** Determine if the equation

\[
x^2 \equiv 5 \pmod{123479}
\]

has any solutions.

So we want to determine

\[
\left( \frac{5}{123479} \right).
\]

**Quadratic reciprocity shows:**

\[
\left( \frac{5}{123479} \right) \left( \frac{123479}{5} \right) = (-1)^{\frac{123479-1}{2} \cdot \frac{5-1}{2} = 1}.
\]
Thus, \( \left( \frac{5}{123479} \right) = \left( \frac{123479}{5} \right) \) since each is \( \pm 1 \).

We now apply the fact that if \( a \equiv b \pmod{p} \), then \( \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) \).

Since \( 123479 \equiv 4 \pmod{5} \), we have

\[
\left( \frac{5}{123479} \right) = \left( \frac{4}{5} \right) = \left( \frac{3}{5} \right)^2 = 1.
\]

So these are solutions! This is much easier than computing

\[
\frac{123479 - 1}{5} = \frac{123478}{5} \pmod{123479}.
\]

We will see many more applications of quadratic reciprocity after we have proven it. Before we prove Gauss's lemma we illustrate it with an example.

**Example:** Let \( p = 17, a = 3 \). Then \( P_{\frac{a}{2}} = 8 \), as

\[
S = \{ 3, 6, 9, 12, 15, 18, 21, 24 \}
\]

**Modulo p,**

\[
S = \{ 3, 11, 3, 4, 6, 7, 9, 12, 15 \}.
\]

Thus, only 9, 12, 15 are large. Then \( P_{\frac{a}{2}} = 8, 5 \), as

\[
\left( \frac{3}{17} \right) = (-1)^3 = -1.
\]

One can check this by computing

\[
3^8 \equiv -1 \pmod{17}
\]
Proof (Gauss lemma): We begin by observing that since \( \gcd(a, p) = 1 \),
more qm the element in \( S \) are congruent to 0 mod p and
more n are congruent to each other, (check this!). Let \( r_1, r_m \)
be the element that are between 0 and \( p/2 \) when reduced
modulo p and \( s_1, s_m \) the ones that reduce to between \( p/2 \)
and p. Note that \( \min = \frac{p-1}{2} \).

Claim: \( p - s_i \equiv r_j \) for all \( i \in \{1, \ldots, m\} \).

Proof: Suppose \( i, j \) s.t. \( p - s_i = r_j \). Then we know \( r_i \)
\( U, V \) s.t. \( 1 \leq U, V \leq \frac{p-1}{2} \), \( S_i \equiv Ua \mod p \),
\( r_j \equiv V a \mod p \).

Then,
\[
(u + v)a = S_i + r_j \equiv 0 \mod p.
\]
\[
\Rightarrow u + v \equiv 0 \mod p \text{ because } u + v \leq \frac{p-1}{2} + \frac{p-1}{2} + 1.
\]

So we have \( \frac{p-1}{2} \) distinct numbers \( r_1, r_m, p - r_1, \ldots, p - r_m \)
between 1 and \( \frac{p}{2} \),
all lying in \( S \). The pigeonhole principle gives that there
must be exactly the integers 1, 2, \ldots, \( \frac{p}{2} \) in some order.

Thus,
\[
g_1 g_2 \ldots g_m (p - s_1) \ldots (p - s_m) \equiv (\frac{p-1}{2})! \mod p.
\]

Similarly,
\[
g_1 g_2 \ldots g_m (-s_1) \ldots (-s_m)
\]

\[(-1)^m g_1 \ldots g_m s_1 \ldots s_m\]
However, we also know that \( r_1, \ldots, r_m, s_1, \ldots, s_n \) are precisely the elements of \( S \) in some order. Thus,

\[
\prod_{i} r_1 \cdots r_m s_1 s_2 \cdots s_n \equiv a \cdot d \cdots (\frac{p^2}{5}) \text{ (mod } p) 
\equiv a \frac{p^m}{S} (\frac{p^m}{5})!.
\]

Combining these equations, we have:

\[
(-1)^n \frac{p^m}{S} \left( \frac{p^m}{5} \right)! \equiv \left( \frac{p^m}{5} \right)! \text{ (mod } p).
\]

Since \( \frac{p^m}{5} \equiv p \pmod{p} \), we have \( \gcd(p, \frac{p^m}{5}) = 1 \) and then we can cancel the \( \frac{p^m}{S} \) to obtain

\[
(-1)^n \frac{p^m}{5} \equiv 1 \text{ (mod } p).
\]

i.e.,

\[
\frac{p^m}{5} \equiv (-1)^n \text{ (mod } p).
\]

Now just use that \( \frac{p^m}{5} \equiv \left( \frac{a}{p} \right) \text{ (mod } p) \).

We need one more lemma before quadratic reciprocity. This lemma will allow us to rephrase what Gauss' lemma says in a way that can be applied to quadratic reciprocity.

**Lemma:** Let \( p \) be an odd prime and \( a \) an odd integer. If \( \gcd(a, p) = 1 \),

\[
\left( \frac{a}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{a}{p}}.
\]
Proof: As in the previous proof, set

\[ S = \{ a, a_2, \ldots, (\frac{p-1}{3})a \}. \]

Write

\[ Ka = q_k p + t_k \]

for \( q_k \in \mathbb{Z}_p \), \( 1 \leq t_k \leq p-1 \) by the division algorithm.

Then we have \( \frac{Ka}{p} = q_k + \frac{t_k}{p} \) \( \Rightarrow \frac{Ka}{p} = q_k \).

Thus, given \( ka \in S \), we have

\[ (1) \quad Ka = L \frac{Ka}{p} p + t_k. \]

Recall that if \( t_k < p \), it is among what we denote as \( r_1, \ldots, r_m \) and if \( t_k > p \), it is among \( s_1, \ldots, s_n \).

Sum over all the equations \((1)\) for \( ka \in S \):

\[ \sum_{k=1}^{p-1} Ka = \sum_{k=1}^{p-1} L \frac{Ka}{p} p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k. \]  \( \ast \ast \)

We use again that \( r_1, \ldots, r_m, s_1, \ldots, s_n \) are

the integers \( 1, \ldots, \frac{p-1}{3} \) \( \mod p \).

Thus we have:

\[ \sum_{k=1}^{p-1} x = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p-s_k) = p m + \sum_{k=1}^{m} r_k - s_k. \]

Subtracting the first \((1)\) we have

\[ (a-1) \sum_{k=1}^{p-1} Ka = \left( \sum_{k=1}^{p-1} L \frac{Ka}{p} - n \right) + 2 \sum_{k=1}^{n} s_k. \]

Looking at this modulo \( 3 \) we have: (since we are interested in proving \((n)\) this is enough.)
\[
\sum_{k \equiv 1 \pmod{2}}^{\frac{p-1}{2}} \frac{k \alpha}{\rho} \equiv (-1)^n \left( \sum_{k \equiv 1 \pmod{2}}^{\frac{p-1}{2}} \left\lfloor \frac{k \alpha}{\rho} \right\rfloor \right) \pmod{2}.
\]

i.e.,

\[
n = \sum_{k \equiv 1 \pmod{2}}^{\frac{p-1}{2}} \left\lfloor \frac{k \alpha}{\rho} \right\rfloor \pmod{2}.
\]

Now we apply Gauss' Lemma:

\[
\left( \frac{a}{\rho} \right) = (-1)^n = (-1)^{\sum_{k \equiv 1 \pmod{2}}^{\frac{p-1}{2}} \left\lfloor \frac{k \alpha}{\rho} \right\rfloor}.
\]

The proof of quadratic reciprocity will use some geometry, as was encountered in a previous proof.

**Proof (quadratic reciprocity):** Consider the following rectangle

\[
\frac{p-1}{2}
\]

\[
y = \left( \frac{a}{\rho} \right) x.
\]

The key step is to count the number of lattice points in this rectangle in two different ways to arrive at a result, not counting the edge!
Given \( p \) and \( q \) as odd, then we can write

\[
\left( \frac{p-1}{2} \right) \left( \frac{q-1}{2} \right)
\]

lattice points in the rectangle. This is the first way. Now consider

the diagonal across the rectangle. Let \( y = \frac{q}{p} x \).

Since \( \gcd(p,q) = 1 \), none of the lattice points can lie on the diagonal.

We now count the lattice points in \( T_1 \) and in \( T_2 \).

We begin with \( T_1 \). Consider a point \((k,0)\) on the \( x\)-axis. The

number of integers in the interval \( 0 < y < \frac{k}{p} \) is precisely

\[
L_{\frac{k}{p}}^\leq k.
\]

Thus, for any \( k \) with \( 0 < k < \frac{p}{2} \), we have precisely \( L_{\frac{k}{p}}^\leq k \)

lattice points on the line where \((k,0)\) below the diagonal. Thus,

there are

\[
\sum_{k=1}^{p-1} L_{\frac{k}{p}}^\leq k
\]

lattice points in \( T_1 \). Similarly, there are

\[
\sum_{k=0}^{q-1} L_{\frac{k}{p}}^\leq k
\]

lattice points in \( T_2 \). Thus,

\[
\left( \frac{p-1}{2} \right) \left( \frac{q-1}{2} \right) = \sum_{k=1}^{p-1} \sum_{k=0}^{q-1} L_{\frac{k}{p}}^\leq k.
\]

Applying the previous lemma we have

\[
\left( \frac{p-1}{2} \right) \left( \frac{q-1}{2} \right) = \left( \sum_{k=0}^{p-1} \sum_{k=0}^{q-1} L_{\frac{k}{p}}^\leq k \right).
\]

\[
\left( \frac{p-1}{2} \right) \left( \frac{q-1}{2} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{q} \right)
\]

as desired.  \( \Box \)
Theorem: Let $p$ be an odd prime. Then
\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv \pm 1 \pmod{8} \\
-1 & \text{if } p \equiv \pm 3 \pmod{8}
\end{cases}
\]

Proof: Since $2$ is clearly not an odd prime, we cannot use quadratic reciprocity here. Instead we apply Gauss' lemma with $a = 2$. The set $S$ is then:
\[ \{ 2, 4, 6, \ldots, p-3 \} \]

Since these are all less than $p$, reducing modulo $p$ does not change anything.

Let $p = 8k + 1$. Then $\frac{p}{2} = 4k + \frac{1}{2}$ and so the $S_2$, $S_3$ are $\{ 4k + 2, 4k + 4, \ldots, 8k \}$. There are $2k$ elements in this set so \( \left( \frac{2}{p} \right) = (-1)^{2k} = 1 \) in this case.

Let $p = 8k - 1$. Then $\frac{p}{2} = 4k - \frac{1}{2}$ and so the $S_2$, $S_3$ are $\{ 4k - 2, 4k, \ldots, 8k - 3 \}$. Again there are $2k$ elements in this set so \( \left( \frac{2}{p} \right) = (-1)^{2k} = 1 \).

Let $p = 8k + 3$. Then $\frac{p}{2} = 4k + \frac{3}{2}$. Then $S_2$, $S_3$ are $\{ 4k+3, 4k+7, \ldots, 8k+3 \}$. There are $2k+1$ elements in this set so \( \left( \frac{2}{p} \right) = (-1)^{2k+1} = -1 \) in this case.

Finally, let $p = 8k + 5$. Then $\frac{p}{2} = 4k + \frac{5}{2}$ and $S_2$, $S_3$ are $\{ 4k+5, 4k+1, \ldots, 8k+5 \}$. Again there are $2k+1$ elements and so \( \left( \frac{2}{p} \right) = -1 \) in the case.
Example: Determine if \( x^2 \equiv 60 \pmod{83} \) has any solutions.

First note that 83 is prime, so we really just want to determine if

\[
\left( \frac{60}{83} \right) = 1 \pmod{83}.
\]

Since 60 = 2^2 \cdot 3 \cdot 5, we have

\[
\left( \frac{60}{83} \right) = \left( \frac{2^2}{83} \right) \left( \frac{3}{83} \right) \left( \frac{5}{83} \right)
\]

\[
= \left( \frac{3}{83} \right) \left( \frac{5}{83} \right).
\]

\[
\left( \frac{3}{83} \right)(\frac{83}{3}) = (-1)^{\frac{83-1}{2}} \left( \frac{3}{83} \right) = (-1)
\]

83 \equiv 2 \pmod{3}, so \( \left( \frac{83}{3} \right) = \left( \frac{2}{3} \right) = \left( \frac{2^2}{3} \right) = \left( \frac{2}{3} \right)^2 = 1 \pmod{3} \)

Thus, \( \left( \frac{3}{83} \right) = -1 \Rightarrow \left( \frac{3}{83} \right)^2 = 1 \pmod{83} \)

\[83 \equiv 3 \pmod{5}, \text{ so } \left( \frac{83}{5} \right) = \left( \frac{3}{5} \right) \text{ thus,}
\]

\[
\left( \frac{3}{5} \right) \left( \frac{5}{3} \right) = (-1)^{\frac{83-1}{2}} \left( \frac{3}{5} \right) = 1.
\]

\[
\left( \frac{3}{5} \right) = \left( \frac{3}{5} \right)^2 = 1
\]

Thus, \( \left( \frac{3}{5} \right)^2 = 1 \Rightarrow \left( \frac{3}{5} \right) = -1 \).

Combining all the we have

\[
\left( \frac{60}{83} \right) = \left( \frac{2^2}{83} \right) \left( \frac{3}{83} \right) \left( \frac{5}{83} \right) = -1
\]

As there are no solutions to the congruence.
Theorem: Let $p > 3$ be an odd prime. Then

$$
\left( \frac{3}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv \pm 1 \pmod{12} \\
-1 & \text{if } p \equiv \pm 5 \pmod{12}
\end{cases}
$$

Proof: The q.r. law gives that

$$
\left( \frac{3}{p} \right) (\frac{p}{3}) = \left( \frac{3}{p} \right) (\frac{3^{3/2}}{p}) = (-1) = (-1)^{\frac{p-1}{2}}.
$$

Now $\left( \frac{p}{3} \right) = \left( \frac{2}{3} \right)$ when $p \equiv r \pmod{3}$. There are only two possible choices here, $r = 1, 2$. If $r = 1$, then

$$
\left( \frac{3}{p} \right) = \left( \frac{1}{3} \right) = 1.
$$

Thus, if $p \equiv 1 \pmod{3}$, then $\left( \frac{3}{p} \right) = (-1)^{\frac{p-1}{2}}$.

If $r = 2 \pmod{3}$, then $\left( \frac{3}{p} \right) = \left( \frac{2}{3} \right) = -1$. Thus,

if $p \equiv 2 \pmod{3}$, then $\left( \frac{3}{p} \right) = (-1)^{\frac{p-1}{2}}(-1)$.

We know that $(-1)^{\frac{p-1}{2}} = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4} \\
-1 & \text{if } p \equiv 3 \pmod{4}
\end{cases}$

Thus, if $p \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{3}$, then $\left( \frac{3}{p} \right) = 2$.

i.e. if $p \equiv 1 \pmod{3}$ then $\left( \frac{3}{p} \right) = 1$.

Similarly, if $p \equiv 3 \pmod{4}$ and $p \equiv 1 \pmod{3}$, then $\left( \frac{3}{p} \right) = -1$.

If $p \equiv 7 \pmod{12}$ and $p \equiv -5 \pmod{12}$ (CRT!)

if $p \equiv 1 \pmod{4}$ and $p \equiv 3 \pmod{3}$, then $\left( \frac{3}{p} \right) = -1$.

if $p \equiv 5 \pmod{12}$.

if $p \equiv 3 \pmod{4}$ and $p \equiv 3 \pmod{3}$, then $\left( \frac{3}{p} \right) = 1$.

$\Rightarrow p \equiv -1 \pmod{12}$. \( \qed \)
Example: Prove that there are infinitely many primes of the form $8k+3$.

Proof: Suppose there are only finitely many, $p_1, p_2, \ldots, p_n$. Consider

$N = (p_1 \cdots p_n)^2 + 1$. There is at least one prime $p$ that divides $N$. Then,

$(p_1 \cdots p_n)^2 \equiv -1 \pmod{p}$

$\Rightarrow \left( \frac{-1}{p} \right) = 1$. So we need to calculate when this happens.

$\left( \frac{-3}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{3}{p} \right)$

We know $\left( \frac{-1}{p} \right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$, and

$\left( \frac{3}{p} \right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$

We need either $\left( \frac{-3}{p} \right) = 1$ or $\left( \frac{-3}{p} \right) = -1$.

Observe that if $p \equiv 1 \pmod{4}$, then $p \equiv -1 \pmod{8}$ and

if $p \equiv 3 \pmod{4}$, then $p \equiv -3 \pmod{8}$. Then there are two possibilities:

- $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$.
- All primes $p | N$ are $1 \pmod{8}$, then $N \equiv 1 \pmod{8}$. But $N \equiv 2 \pmod{8}$. Then there is at least one $p | N \equiv 3 \pmod{8}$. But then $p | N$ and $p | (p_1 \cdots p_n)^2 + 1 \Rightarrow$ there is no only one prime of the form $8k+3$.}$
We have now completely solved the problem of determining when

\[ x^2 \equiv a \pmod{p} \]

has a solution for \( p \) a prime number. We would now like to deal with the equation

\[ x^2 \equiv a \pmod{n} \quad (\#) \]

for \( n \) composite. First observe that if \( a \equiv 0 \pmod{n} \) then \( x \equiv 0 \) is clearly a solution so we restrict ourselves to the case that \( a \neq 0 \). Write \( n = p_1^{e_1} \cdots p_r^{e_r} \) with \( p_i \neq p_j \) if \( i \neq j \). First suppose there is a solution to \((\#)\). Then clearly we have solutions to

\[ x^2 \equiv a \pmod{p_i^{e_i}} \]

\[ x^2 \equiv a \pmod{p_i^{e_i}} \]

namely just reduce our original solution modulo \( p_i^{e_i} \) for each \( i \). Conversely, suppose we have a solution to the equations \((\#)\). Then we have \( x \equiv c_i \pmod{p_i^{e_i}} \) for some \( c_i \). Using the CRT we obtain an \( x \) with \( x \equiv c_i \pmod{p_i^{e_i}} \) for all \( i \) such that \( x \) gives a solution to \((\#)\). Thus, solving \((\#)\) is equivalent to solving

\[ x^2 \equiv a \pmod{p} \]

for prime powers. We now study this problem.
We begin with the case that we have an odd prime $p$ and $gcd(a, p^3) = 1$.

Recall the theorem we proved before dealing with solutions to congruences of the form

$$f(x) \equiv 0 \pmod{p^n}.$$ 

**Theorem (from earlier text):** Let $f(x) \in \mathbb{Z}[x]$ be any $f(x)$. Let $p$ be a prime and $n \geq 1$. Let $x_1$ be a solution to the congruence

$$f(x) \equiv 0 \pmod{p^n}.$$

Then $x_1$ lifts to a solution to the congruence

$$f(y) \equiv 0 \pmod{p^n}$$

iff there is a solution to the congruence

$$t \equiv \frac{-f(x_1)}{p^n} \pmod{p}.$$  \hspace{1cm} (1)

In particular, if we let $h$ be the number of solutions to (1), then

$$h = \begin{cases} 
1 & \text{if } p \nmid f'(x_1) \\
0 & \text{if } p \mid f'(x_1) \text{ and } p^{n+m} \nmid f(x_1) \\
1 & \text{if } p \mid f'(x_1) \text{ and } p^{n+m} \mid f(x_1). 
\end{cases}$$

Note that if more than one solution to

$$f(x) \equiv 0 \pmod{p^n}$$

lift to a solution modulo $p^{n+m}$, then there are no solutions?

We use this to give an easy proof of the following theorem:
Thin: Let $p$ be an odd prime and $a \in \mathbb{Z}$ with $\gcd(a,p)=1$. Then

$$x^2 \equiv a \pmod{p^k}$$

has a solution iff \( \left( \frac{a}{p} \right) = 1 \).

Proof: First observe that if \( x^2 \equiv a \pmod{p^k} \) be a solution, so does \( x^2 \equiv a \pmod{p} \)

and so \( \left( \frac{a}{p} \right) = 1 \).

Suppose now that \( \left( \frac{a}{p} \right) = 1 \). Observe that solving

$$x^2 \equiv a \pmod{p^k}$$

is the same as solving

$$f(x) \equiv 0 \pmod{p^k}$$

where \( f(x) = x^2 - a \). Now \( px \) is prime \( \gcd(a,p)=1 \)

and so \( px \) \( f'(x) \) for \( x \) a solution to \( x^2 \equiv a \pmod{p} \).

Thus, the solution lifts to a unique solution modulo \( p^k \),
call it \( x_2 \). The same arg. that shows \( px \ f'(x_2) \), so \( x_2 \) lifts to \( x_2 \) modulo \( p^k \). Thus, we have inductively

solutions for all \( k \geq 1 \).

We now deal with the case \( p=2 \). Note that for \( k=1 \), we know

$$x^2 \equiv 1 \pmod{2}$$

definitely has a solution, \( k=2 \) can be handled by operating everyting odd

modulo 4:

$$f^2 \equiv 1 \pmod{4}$$

$$3^2 \equiv 1 \pmod{4}$$

Thus,

$$x^2 \equiv a \pmod{4}$$
has a solution iff $a \equiv 1 \pmod{4}$, we need to deal with the general case.

**Thm:** Let $a$ be an odd integer. The congruence (K71)

$$x^2 \equiv a \pmod{2^k} \quad (\text{**K71**})$$

has a solution iff $a \equiv 1 \pmod{8}$.

**Proof:** First note that the sequence of odd integers modulo 8 is an all congruent to 1, thus for (**K71**) to have a solution, there be a solution to

$$x^2 \equiv a \pmod{8}$$

$\Rightarrow a \equiv 1 \pmod{8}$. (We have $k \geq 3$ since we have already dealt with $k=1,2$.) Now we need to show that if $a \equiv 1 \pmod{8}$, then

$$x^2 \equiv a \pmod{2^k}$$

always has a solution for $k \geq 3$. We proceed by induction on $k$. The base case of

$$x^2 \equiv 1 \pmod{8}$$

is clear. Assume that

$$x^2 \equiv a \pmod{2^n}$$

does a solution $x_0$. We pursue a solution to

$$x^2 \equiv a \pmod{2^{n+1}}$$

and so have the result by induction.

We know $\exists x \in \mathbb{Z}$ s.t.

$$x_0^2 = a + 2^n t.$$ 

Since $a$ is odd, $x_0$ must also be odd, and so $x_0$ is odd.
Thus, there is a \( y \in \mathbb{Z} \) such

\[ x_0 y = -t \pmod{a}. \]

Namely, write

\[ x_0 \alpha + 2\beta = 1 \]

\[ \Rightarrow \quad x_0 \alpha (-t) + 2\beta (t) = -t \]

so \( y = \alpha (t) \).

Consider \( x_1 = x_0 + y 2^{n-1} \). Then

\[ x_1^2 = (x_0 + y 2^{n-1})^2 \]

\[ = x_0^2 + yx_0 2^n + y^2 2^{n-2} \]

\[ \equiv \alpha (t) \pmod{a} \]

\[ \equiv \alpha + (t+2s) \beta \pmod{a} \]

\[ \equiv \alpha + 2^n t + yx_0 2^n + 0 \pmod{a} \]

\[ \equiv \alpha + 2^n t + (t+2s) \beta \pmod{a} \]

\[ \equiv \alpha + 2^{n+1} \beta \pmod{a} \]

\[ \equiv \alpha \pmod{a}. \]

Thus, \( x_0 y 2^{n-1} \) is a solution \( \pmod{a} \) and we have the result by induction. \( \square \)
We now drop the assumption that \( \gcd(a, p) = 1 \) when we now include \( p = 2 \) as well. Write \( a = p^r b \) with \( \gcd(p, b) = 1, \, r \geq 1 \). We split into two cases: \( r \) even and \( r \) odd.

Suppose \( r \) is even, so \( r = 2s \) with \( s \geq 1 \). Then we want to solve

\[
X^2 \equiv p^{2s} b \pmod{p^r}.
\]

If \( \bar{b} \) is a solution \( y \) to the congruence

\[
X^2 \equiv b \pmod{p^s},
\]

then we have

\[
(y p^s)^2 \equiv p^{2s} b \pmod{p^r}
\]

so we have a solution. Since \( \gcd(b, p) = 1 \), a solution to \( x^2 \equiv b \pmod{p^r} \) exists if and only if \( (b/p) = 1 \) (\( p \) odd), \( b \equiv 1 \pmod{p} \) if \( p = 2 \). Then, we are able to reduce this case to the case already dealt with.

Suppose now that \( a = p^r b \) with \( r \) odd. Note that if \( \bar{b} \) is a solution to \( \bar{b} = x \pmod{p^s} \), then \( p^r | x^2 = (y p^s)^2 \).

Then \( p^r | x^2 = p^{2s} | x \). Thus we obtain the equation

\[
p^{rm} y^2 = p^r b + p^r t.
\]
for some \( t \) to \( 2 \). Thus, what we want is a solution to the congruence

\[ py^3 \equiv b \pmod{p^{k-r}}. \]

However,

\[ p^{k-r} \mid (py^3 - b) \]

\[ \Rightarrow \]

\[ p \mid (py^3 - b) \]

\[ \Rightarrow \]

\[ p \mid b. \quad \# \]

Thus there are no solutions if \( r \) is odd.

Back to the general case, recall that if we have a solution

\[ x^2 \equiv a \pmod{p^m}, \quad (\#) \]

we obtain a solution

\[ x^2 \equiv a \pmod{p^k} \]

for every prime \( p \) of \( p^{k-1} \). Thus, if \( p^e \mid a \) with \( e \) odd for some prime \( p^{k-1} \), proceed, or if \( a = 2^e b \) \( \equiv b \pmod{p^{k-1}} \), then there are no solutions to \( (\#) \). We summing with the following theorem.
Thm: Let $n = 2^e \cdot p_1^{e_1} \cdots p_r^{e_r}$ w/ $p_i$ odd. The congruence

$$x^2 \equiv a \pmod{n}$$

has a solution iff for each prime $p_i$, $p_i^{e_i} \mid n$ w/ $e_i$ even and $\left( \frac{a^{e_i}}{p_i} \right) = 1$ and

$$p_1^{e_1} \cdots p_r^{e_r} \equiv 1 \pmod{e_1}$$
if $e > 0$. 
CONGRUENT NUMBERS AND ELLIPTIC CURVES

JIM BROWN

ABSTRACT. These are essentially the lecture notes from a section on congruent numbers and elliptic curves taught in my introductory number theory class at the Ohio State University spring term of 2007. The students in this class were assumed to only have a basic background in proof theory (such as sets and induction) and the material we had covered up to this point in the term (primes, congruences, and quadratic reciprocity). These notes are self-contained modulo basic facts from those subjects and do not assume a background of abstract algebra. Any abstract algebra that is needed is introduced. Calculations used in these notes were performed with SAGE ([6]) as the students in this class used this program throughout the term. Homework exercises are contained in the notes as well. These notes owe a great deal to the wonderful treatment of the subject by Koblitz ([3]).

1. INTRODUCTION

One of the traits that sets number theory apart from many other branches of mathematics is the fact that many of the most difficult problems are very easy to state. In fact, the statement of many of these problems can be understood by a student in a high school mathematics class. The beauty of these problems is the modern mathematics that flows from their study. The problem these notes focus on is finding an efficient way to determine if an integer is a congruent number.

Definition 1.1. An integer $N$ is a congruent number if there exists a right triangle with rational sides so that the area of the triangle is $N$.

Example 1.2. The number $N = 6$ is a congruent number as one sees by considering the $3 - 4 - 5$ triangle.

Given a positive integer $N$, we would like a criterion that is easy to check telling us whether or not $N$ is a congruent number. We begin our study of congruent numbers in the natural place, namely, right triangles. This is the focus of the following section.

Key words and phrases. Congruent numbers, elliptic curves.
2. Pythagorean Triples

In this section we study what information we can obtain on congruent numbers from a basic study of right triangles.

Definition 2.1. Let \(X, Y,\) and \(Z\) be rational numbers. We say \((X, Y, Z)\) is a Pythagorean triple if \(X^2 + Y^2 = Z^2\). If \(X, Y, Z \in \mathbb{Z}\) and \(\gcd(X, Y, Z) = 1\) we say \((X, Y, Z)\) is a primitive Pythagorean triple.

We begin our study of Pythagorean triples by looking at those triples with \(X, Y, Z \in \mathbb{Z}\).

Theorem 2.2. Let \((X, Y, Z)\) be a primitive Pythagorean triple. Then there exists \(m, n \in \mathbb{N}\) so that \(X = 2mn, Y = m^2 - n^2\) and \(Z = m^2 + n^2\). Conversely, any \(m, n \in \mathbb{N}\) with \(m > n\) define a right triangle.

Proof. It is clear that given \(m\) and \(n\) in \(\mathbb{N}\) we obtain a right triangle with integer sides using the given formulas. We need to show that given a right triangle with integer sides \(X, Y,\) and \(Z\) that we can find such an \(m\) and \(n\). Observe that we have \(X^2 + Y^2 = Z^2\) by the Pythagorean theorem. Suppose \(X\) and \(Y\) are both odd. In this case we have \(X^2 \equiv Y^2 \equiv 1 \pmod{4}\) and so \(Z^2 \equiv 2 \pmod{4}\). However, the squares modulo 4 are 0 and 1. Thus it must be that \(X\) or \(Y\) is even. If both were even we would also obtain that \(2 \mid Z\) which would contradict \(\gcd(X, Y, Z) = 1\). Assume without loss of generality that \(X\) is even so that \(\frac{X}{2}\) is an integer. Write

\[
\left(\frac{X}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 - \left(\frac{Y}{2}\right)^2 = \left(\frac{Z - Y}{2}\right) \left(\frac{Z + Y}{2}\right).
\]

If \(p\) is a prime that divides \(\frac{X}{2}\), then \(p^2 \mid \left(\frac{X}{2}\right)^2\). Since \(p\) is prime, we have that \(p \mid \left(\frac{Z - Y}{2}\right)\) or \(p \mid \left(\frac{Z + Y}{2}\right)\). Note that \(p\) cannot divide both for if it did we would have \(p \mid \left(\frac{Z - Y}{2}\right) + \left(\frac{Z + Y}{2}\right)\) which would contradict \(\gcd(X, Y, Z) = 1\). Thus we obtain that \(p^2 \mid \left(\frac{Z - Y}{2}\right)^2\) or \(p^2 \mid \left(\frac{Z + Y}{2}\right)^2\). Running through all the primes that divide \(\frac{X}{2}\), we see that we can write \(\left(\frac{X}{2}\right)^2 = m^2n^2\) where \(m\) is composed of those primes that divide \(\left(\frac{Z + Y}{2}\right)\) and \(n\) is composed of those primes that divide \(\left(\frac{Z - Y}{2}\right)\). This gives that \(X = 2mn, Y = m^2 - n^2\), and \(Z = m^2 + n^2\), as desired. \(\Box\)

This theorem allows us to construct as many congruent numbers as we want. Namely, for any \(m, n \in \mathbb{N}\) we have that \(N = \frac{1}{2}(2mn)(m^2 - n^2)\) is a congruent number. The following table gives examples of congruent numbers obtained from this process.
CONGRUENT NUMBERS AND ELLIPTIC CURVES

Table 1. Congruent numbers from Pythagorean triples

<table>
<thead>
<tr>
<th>m</th>
<th>n</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>5</td>
<td>13</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>8</td>
<td>15</td>
<td>17</td>
<td>60</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>24</td>
<td>7</td>
<td>25</td>
<td>84</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>16</td>
<td>12</td>
<td>20</td>
<td>96</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>10</td>
<td>24</td>
<td>26</td>
<td>120</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>40</td>
<td>9</td>
<td>41</td>
<td>180</td>
</tr>
</tbody>
</table>

Exercise 1. Prove there are infinitely many distinct congruent numbers.

Of course, we want to deal with triangles with rational sides as well. Suppose we have a right triangle with sides $X, Y, Z \in \mathbb{Q}$ and area $N$. It is easy to see that we can clear denominators and obtain a right triangle with integers sides and congruent number $a^2N$ where $a$ is the least common multiple of the denominators of $X$ and $Y$. Thus, we can go from a right triangle with rational sides to a right triangle with integer sides and a new congruent number that is divisible by a square. Conversely, given a right triangle with integer sides $X, Y,$ and $Z$ and congruent number $N = a^2N_0$, we can form a right triangle with rational sides and congruent number $N_0$ by merely dividing $X$ and $Y$ by $a$. Thus, in order to classify congruent numbers it is enough to study positive integers $N$ that are square-free.

Example 2.3. Consider the $40 - 9 - 41$ triangle given by $m = 5$ and $n = 4$. This triangle has area $180 = 5 \cdot 6^2$. Thus, 5 is a congruent number given by a triangle with sides $\frac{3}{2}, \frac{20}{3},$ and $\frac{41}{6}$.

Some further examples are given in the following table.

Table 2. Congruent numbers from rational right triangles

<table>
<thead>
<tr>
<th>X</th>
<th>Y</th>
<th>Z</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/2</td>
<td>20/3</td>
<td>41/6</td>
<td>5</td>
</tr>
<tr>
<td>4/9</td>
<td>7/4</td>
<td>65/36</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>15/2</td>
<td>17/2</td>
<td>15</td>
</tr>
<tr>
<td>7/2</td>
<td>12</td>
<td>25/2</td>
<td>21</td>
</tr>
<tr>
<td>4</td>
<td>17/36</td>
<td>145/36</td>
<td>34</td>
</tr>
</tbody>
</table>
This method allows us to use the Pythagorean triples given in Theorem 2.2 to produce congruent numbers arising from triangles with rational sides. The difficulty is not in producing lots and lots of congruent numbers, the difficulty is determining if a given integer \( N \) is a congruent number. Using the method described thus far, if we cannot find a triangle with area \( N \), it does not mean \( N \) is not congruent. It may just be that we have not looked hard enough to find the triangle. For example, the integer 157 is a congruent number. However, the simplest triangle giving area 157 has sides given by

\[
X = \frac{6803298487826435051217540}{411340519227716149383203}, \quad Y = \frac{411340519227716149383203}{2166655693714761309610}.
\]

Clearly we are going to need a new method to solve this problem.

Before we embark on a new method of attack, we note that we have yet to see why such an \( N \) is called a congruent number. The following theorem answers this question. It says that if \( N \) is a congruent number we obtain three squares of rational numbers that are congruent modulo \( N \).

**Theorem 2.4.** Let \( N \) be a square-free positive integer. Let \( X, Y, Z \) be positive rational numbers with \( X < Y < Z \). There is a 1-1 correspondence between right triangles with sides \( X, Y, Z \) and area \( N \) and numbers \( x \in \mathbb{Q} \) so that \( x, x + N, x - N \) are all squares of rational numbers.

**Exercise 2.** Prove theorem 2.4.

### 3. FROM CONGRUENT NUMBERS TO ELLIPTIC CURVES

The goal of this section is to see that a triangle with area \( N \) and rational sides \( X, Y, Z \) gives rise to a rational point on an elliptic curve. The terms "rational point" and "elliptic curve" will be defined. Note that \( N \) being a congruent number is equivalent to the existence of rational numbers \( X, Y, Z \) so that

\[
(1) \quad Z^2 = X^2 + Y^2
\]

\[
(2) \quad N = \frac{1}{2} XY.
\]

As is often the case when we are stuck on a problem involving finding solutions to equations, we play around with the equations and see where it leads us. If we multiply equation (2) by 4 and add and subtract it from equation (1) we obtain the equations

\[
(X + Y)^2 = Z^2 + 4N
\]
and

\[(X - Y)^2 = Z^2 - 4N,\]

i.e., we have equations

\[(3) \quad \left( \frac{X + Y}{2} \right)^2 = \left( \frac{Z}{2} \right)^2 + N\]

and

\[(4) \quad \left( \frac{X - Y}{2} \right)^2 = \left( \frac{Z}{2} \right)^2 - N.\]

Multiplying equations (3) and (4) together we obtain

\[\left( \frac{X^2 - Y^2}{4} \right)^2 = \left( \frac{Z}{2} \right)^4 - N^2.\]

Thus, a rational right triangle with area \(N\) produces a rational solution to the equation

\[(5) \quad v^2 = u^4 - N^2,\]

namely \(v = \left( \frac{X^2 - Y^2}{4} \right)\) and \(u = \left( \frac{Z}{2} \right)\). Multiplying equation (5) by \(u^2\) we obtain

\[(uv)^2 = u^6 - N^2u^2.\]

If we set \(x = u^2 = \left( \frac{Z}{2} \right)^2\) and \(y = uv = \frac{Z(X^2 - Y^2)}{8}\), then we find that a rational right triangle with area \(N\) produces a rational solution to the equation

\[(6) \quad E_N : y^2 = x^3 - N^2x.\]

This curve is an example of type of curve known as an elliptic curve. We will come back to these curves in subsequent sections. For now we have the following result stating that this process can be reversed and we can use certain points on elliptic curves of the form \(E_N\) to show that \(N\) is a congruent number.

**Proposition 3.1.** Let \(x_0, y_0 \in \mathbb{Q}\) so that

\[y_0^2 = x_0^3 - N^2x_0.\]

Suppose \(x_0\) satisfies:

1. \(x_0\) is the square of a rational number
2. \(x_0\) has even denominator
3. the numerator of \(x_0\) is relatively prime to \(N.\)

There exists a right triangle with rational sides and area \(N\) which corresponds to \(x_0.\)
Proof. Let \( x_0 = u^2 \) with \( u \in \mathbb{Q} \). We now reverse the steps used to arrive at the equation \( y^2 = x^3 - N^2x \). Set \( v = y_0/u \) so that \( v^2 = (x_0^3 - N^2x_0)/x_0 = x_0^2 - N^2 \). Thus,

\[
(7) \quad x_0^2 = N^2 + v^2.
\]

Let \( t \) be the denominator of \( u \). Since \( u^2 = x_0 \) and \( x_0 \) has even denominator, we must have \( 2 \mid t \). It is not difficult to see that \( v^2 \) and \( x_0^2 \) have the same denominator. Multiplying equation (7) by \( t^2 \) we obtain that \( t^2N, t^2v, t^2x_0 \) is a Pythagorean triple of integers. In fact, since the numerator of \( x_0 \) and \( N \) have no common factor we can conclude that \( \gcd(t^2N, t^2v, t^2x_0) = 1 \). We can now apply Theorem 2.2 to conclude that there exists \( m, n \in \mathbb{N} \) so that \( t^2N = 2mn, t^2v = m^2 - n^2 \), and \( t^2x_0 = m^2 + n^2 \).

Consider now the triple \( X = \frac{2m}{t}, Y = \frac{2n}{t}, Z = 2u \). This determines a right triangle:

\[
X^2 + Y^2 = \frac{4}{t^2}(m^2 + n^2)
= \frac{4}{t^2}(t^2x_0)
= 4x_0
= (2u)^2
= Z^2.
\]

The area of this triangle is given by

\[
\frac{1}{2}XY = \frac{1}{2}\frac{4mn}{t^2}
= \frac{2mn}{t^2}
= N.
\]

Thus, we have a triangle with rational sides and area \( N \) as claimed. \( \square \)

Though we will need the above proposition for a future proof, the following exercise is much easier to prove and is more useful for actually turning points \( x_0, y_0 \in \mathbb{Q} \) satisfying \( y_0^2 = x_0^3 - N^2x_0 \) into a triangle with rational sides and area \( N \).

Exercise 3. Define sets \( A \) and \( B \) by

\[
A = \left\{ (X, Y, Z) \in \mathbb{Q}^3 : \frac{1}{2}XY = N, X^2 + Y^2 = Z^2 \right\}
B = \left\{ (x, y) \in \mathbb{Q}^2 : y^2 = x^3 - N^2x, y \neq 0 \right\}.
\]
Prove that there is a bijection between $A$ and $B$ given by maps
\[ f(X, Y, Z) = \left( -\frac{NY}{X + Z}, \frac{2N^2}{X + Z} \right) \]
and
\[ g(x, y) = \left( \frac{N^2 - x^2}{y}, \frac{2xN}{y}, \frac{N^2 + x^2}{y} \right). \]

4. A QUICK TOUR OF THE PROJECTIVE PLANE

To properly work with the elliptic curves $E_N$ we will need what is known as the "point at infinity". In order to introduce this point at infinity, we require a brief introduction to the projective plane.

Consider the tuples of complex numbers $(x, y, z)$ with $(x, y, z) \neq (0, 0, 0)$. Define an equivalence relation on these tuples by $(x, y, z) \sim (a, b, c)$ if $x = \lambda a$, $y = \lambda b$, $z = \lambda c$ for some nonzero $\lambda \in \mathbb{C}$. We denote the equivalence class containing $(x, y, z)$ by $(x : y : z)$. The set of equivalence classes of tuples is the projective plane $\mathbb{P}_C^2$, i.e.,
\[ \mathbb{P}_C^2 = \{(x : y : z) : x, y, z \in \mathbb{C}, (x, y, z) \neq (0, 0, 0)\}. \]

We add and multiply in the projective plane coordinate-wise, i.e., for $(x_1 : y_1 : z_1), (x_2 : y_2 : z_2) \in \mathbb{P}_C^2$, one has
\[ (x_1 : y_1 : z_1) + (x_2 : y_2 : z_2) = (x_1 + x_2 : y_1 + y_2 : z_1 + z_2) \]
and
\[ (x_1 : y_1 : z_1)(x_2 : y_2 : z_2) = (x_1x_2 : y_1y_2 : z_1z_2). \]

Exercise 4. Check that componentwise addition and multiplication are well-defined on $\mathbb{P}_C^2$.

Remark 4.1. Projective planes can be constructed over sets other than the complex numbers. For example, $\mathbb{P}_R^2$ and $\mathbb{P}_Q^2$ are both defined analogously to $\mathbb{P}_C^2$.

The projective plane is a generalization of the ordinary $xy$-plane. If we set $z = 1$, then we regain the familiar points $(x, y)$. This follows from the fact that in each equivalence class where $z \neq 0$, there is a unique point $(x, y, 1)$ that is obtained by normalizing by multiplication by $z^{-1}$. The new points we gain are the ones where $z = 0$, i.e., the line at infinity. It is the point $(0 : 1 : 0)$ on this line that we are interested in as it will be the only point on the line at infinity that lies on the elliptic curve $E_N$.

Given a curve $f(x, y) = 0$, we can associate to this a curve in the projective plane. A monomial $x^i y^j$ is said to be of degree $i + j$. The degree of $f(x, y)$ is the maximum of the degrees of all the monomials
occurring in \( f(x, y) \). Let \( n \) be the degree of \( f(x, y) \). The homogeneous polynomial \( F(x, y, z) \) associated to \( f(x, y) \) is the polynomial obtained by multiplying each monomial \( x^i y^j \) of \( f(x, y) \) by \( z^{n-i-j} \). Note each monomial of \( F(x, y, z) \) has degree \( n \). Given a homogeneous polynomial \( F(x, y, z) \) of degree \( n \), we obtain a polynomial \( f(x, y) \) by setting \( z = 1 \).

**Example 4.2.** Let \( f(x, y) = y^2 - x^3 + N^2 x \). The associated homogeneous polynomial is given by \( F(x, y, z) = y^2 z - x^3 + N^2 x z^2 \).

One would like to consider our homogeneous polynomials as functions on the projective plane. Unfortunately this is not well-defined as for \( \lambda \neq 0 \), one has \( (x : y : z) = (\lambda x : \lambda y : \lambda z) \) but \( F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z) \neq F(x, y, z) \). However, we do have \( F(x, y, z) = 0 \) if and only if \( F(\lambda x, \lambda y, \lambda z) = 0 \). Thus, we can consider the curves \( F(x, y, z) = 0 \) as curves in the projective plane.

**Definition 4.3.** A point \( P = (x_0 : y_0 : z_0) \) is said to be on the curve \( F(x, y, z) = 0 \) if \( F(x_0, y_0, z_0) = 0 \). We say \( P \) is a rational point on the curve \( F(x, y, z) = 0 \) if \( P \) is on the curve and \( x_0, y_0, z_0 \in \mathbb{Q} \). If we write \( C : F(x, y, z) = 0 \) for the curve, the set of rational points is denoted \( C(\mathbb{Q}) \).

**Example 4.4.** The points \((0 : 0 : 1)\) and \((0 : 1 : 0)\) are on the curve \( E_N : y^2 z - x^3 + N^2 x z^2 = 0 \).

## 5. Generalities on elliptic curves

In this section we study elliptic curves. We will restrict ourselves to elliptic curves of the form we are interested in for the most part. We begin with a few general definitions before restricting to the case of interest.

**Definition 5.1.** A curve \( F(x, y, z) = 0 \) is said to be singular at a point \( P = (x_0 : y_0 : z_0) \) if \( P \) is on the curve and \( \frac{\partial F}{\partial x}(x_0, y_0, z_0) = 0 \), \( \frac{\partial F}{\partial y}(x_0, y_0, z_0) = 0 \), and \( \frac{\partial F}{\partial z}(x_0, y_0, z_0) = 0 \). If \( P \) is on the curve but the curve is not singular at \( P \) it is said to be nonsingular at \( P \). A curve that is nonsingular at all the points on the curve is said to be nonsingular.

For the curves we are interested in, most of the action will take place in the familiar \( xy \)-plane with only a single point at infinity. In this case one should think of the concept of nonsingular at a point as the familiar concept from calculus of there being a well-defined tangent line at the point.
Example 5.2. Consider the curve \( F(x, y, z) = y^2z - x^3 = 0 \). In the \( xy \)-plane we have the following graph:

![Graph of the curve](image)

From the graph of the curve one would expect that it is singular at the point \((0 : 0 : 1)\) as there is no well-defined tangent line there and nonsingular everywhere else. We now verify this. Observe that \( \frac{\partial F}{\partial x} = -3x^2 \) and \( \frac{\partial F}{\partial y} = 2yz \). The only point on the curve in the \( xy \)-plane where both of these partials vanish is \((0 : 0 : 1)\). Thus, the curve is singular at the point \((0 : 0 : 1)\) and nonsingular at all other points in the \( xy \)-plane. The points on the curve that are not in the \( xy \)-plane occur when \( z = 0 \). Thus, we have only the projective point \((0 : 1 : 0)\). We see that \( \frac{\partial F}{\partial z} = y^2 \) and since we are looking at the point \((0 : 1 : 0)\), we see the curve is nonsingular at the point \((0 : 1 : 0)\). Thus, \( F \) is nonsingular at every point except the point \((0 : 0 : 1)\).

Exercise 5. Let \( N \) be a positive integer and consider the curve \( F(x, y, z) = y^2z - x^3 + N^2xz^2 \). Prove that \( F(x, y, z) = 0 \) is a nonsingular curve.

Definition 5.3. An elliptic curve over \( \mathbb{Q} \) is a nonsingular curve of the form

\[
E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_5z^3
\]

with \( a_i \in \mathbb{Q} \) for \( 1 \leq i \leq 5 \).

We will only be interested in the elliptic curves

\[
E_N : y^2z = x^3 - N^2xz^2
\]
for $N$ a positive square-free integer. Note that the exercise above shows that these curves are actually elliptic curves. In fact, you should have seen in that exercise that the only point not in the familiar $xy$-plane is the point $(0 : 1 : 0)$, which we refer to as the point at infinity. This allows us to work primarily in the $xy$-plane with $z = 1$. As we will be doing numerous calculations with SAGE for elliptic curves, it is important to note here that the SAGE command to construct the elliptic curve $E_N$ is as follows:

```python
code
sage: E=EllipticCurve([-N^2, 0]); E
Elliptic Curve defined by $y^2 = x^3 - N^2x$ over Rational Field
```

One of the reasons that elliptic curves are so special in the world of curves is the fact that we can define an addition on the points of the curve. In particular, we can define an operation $\oplus$ so that if $P, Q \in E_N(\mathbb{Q})$ then $P \oplus Q \in E_N(\mathbb{Q})$. (This is true for any elliptic curve, but we restrict ourselves to the curves of interest.) In particular, this will make the set $E_N(\mathbb{Q})$ into an abelian group! We will come back to the notion of an abelian group and give a definition, but first we define the addition on $E_N(\mathbb{Q})$ and show some basic properties.

The fact that the equation defining $E_N$ is a cubic implies that any line that intersects the curve must intersect it at exactly three points if we include the point at infinity as well and count a tangent as a double intersection point. This would lead one to guess that defining the point $P \oplus Q$ is as simple as setting it equal to the third intersection point of the line through $P$ and $Q$. Unfortunately, defining addition in this way would miss the important property of associativity!

![Figure 1](image)

**Figure 1.** Graphical representation that on $E_6$ one has $P \oplus Q = (12, -36)$ for $P = (-3, 9)$ and $Q = (0, 0)$. 
Exercise 6. Define an operation on the points on the curve $E_N$ by $P \boxplus Q = R$ where $R$ is the third intersection point of the line through $P$ and $Q$ with $E_N$ as pictured above. Show with pictures that this addition is not associative. In other words, show that given points $P_1, P_2, P_3$ on the curve $E_N$, that $P_1 \boxplus (P_2 \boxplus P_3)$ is not necessarily equal to $(P_1 \boxplus P_2) \boxplus P_3$.

What turns out to be the correct addition $P \oplus Q$ is to take the third point of intersection $R$ of the line through $P$ and $Q$ and the elliptic curve and reflect it over the $x$-axis as pictured below.

![Graphical representation of elliptic curve addition](image)

**Figure 2.** Graphical representation that on $E_6$ one has $P \oplus Q = (12, 36)$ for $P = (-3, 9)$ and $Q = (0, 0)$.

Note that what we are really doing is finding the point $R$ and then taking another line through $R$ and the point at infinity and taking the third intersection point with $E_N$ as $P \oplus Q$. This makes it easy to see that the point at infinity acts as the 0 element. In the future we will often write $0_{E_N}$ for the point at infinity to reflect this fact.

Exercise 7. Convince yourself with pictures that $P \oplus Q = Q \oplus P$, $P \oplus 0_{E_N} = P$, and if $P = (x, y)$, then $-P = (x, -y)$, i.e., $P \oplus (-P) = 0_{E_N}$. If you are really brave try to see that the addition is associative as well!

This method shows that given two points $P$ and $Q$ on $E_N$ we get a third point $P \oplus Q$ on $E_N$. What we have not shown yet is given $P, Q \in E_N(\mathbb{Q})$ that $P \oplus Q \in E_N(\mathbb{Q})$. In order to show this we compute
the coordinates of \( P \oplus Q \) in terms of those of \( P \) and \( Q \). Write \( P = (x(P), y(P)) \) and similarly for \( Q \) and \( P \oplus Q \). Note that if we define \( R \) as above being the third intersection point of the line through \( P \) and \( Q \) with \( E_N \), then \( x(R) = x(P \oplus Q) \) and \( y(R) = -y(P \oplus Q) \), so it is enough to determine \( x(R) \) and \( y(R) \) in terms of \( x(P), x(Q), y(P) \) and \( y(Q) \). We deal with the case \( P \neq Q \) and leave the case of \( P = Q \) as an exercise. Let \( \ell \) be the line through \( P \) and \( Q \), i.e., \( \ell \) is the equation \( y - y(P) = m(x - x(P)) \) where \( m = \frac{y(Q) - y(P)}{x(Q) - x(P)} \). Define

\[
f(x) = x^3 - N^2x - (m(x - x(P)) + y(P))^2.
\]

From the definition of \( \ell \) we see that \( f(x(P)) = f(x(Q)) = f(x(R)) = 0 \). Since \( f(x) \) is a degree three polynomial in \( x \) and we have three roots of \( f(x) \) these are necessarily all the roots. Recall the following basic result from algebra.

**Theorem 5.4.** Let \( g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \). Let \( \alpha_1, \ldots, \alpha_n \) be the roots of \( g(x) \). Then

\[
-a_{n-1} = \sum_{i=1}^{n} \alpha_i.
\]

**Exercise 8.** Prove Theorem 5.4. (Hint: \( g(x) = \prod_{i=1}^{n}(x - \alpha_i) \).)

Theorem 5.4 allows us to conclude that

\[
x(P) + x(Q) + x(R) = m^2.
\]

Thus, \( x(R) = m^2 - x(P) - x(Q) \). The fact that \( P, Q \in E_N(\mathbb{Q}) \) shows that \( m, x(P), x(Q) \in \mathbb{Q} \) and so \( x(P \oplus Q) = x(R) \in \mathbb{Q} \) as well. It remains to calculate \( y(R) \). For this, we merely plug \( y(R) \) in for \( y \) in the equation of \( \ell \) giving

\[
y(R) = m(x(R) - x(P)) + y(P).
\]

Since everything on the right hand side of this equation is in \( \mathbb{Q} \), so is \( y(R) \) and hence \( y(P \oplus Q) = -y(R) \in \mathbb{Q} \).

**Exercise 9.** Calculate \( 2P = P \oplus P \) in terms of \( x(P) \) and \( y(P) \). Note that the only difference from the above calculation is that in this case \( \ell \) will need to be the tangent line.

**Example 5.5.** Consider the elliptic curve \( E_6 \). It is easy to see that the points \( (0 : 0 : 1) \) and \( (\pm 6 : 0 : 1) \) are on this curve. We can use SAGE to find other nontrivial points. Define the elliptic curve in SAGE as above labelling it as \( E \). To find points one uses the command:
sage: E.point_search(10)

The 10 in this command is telling it how many points to search; essentially it is checking all points up to a certain "height". The only thing we need to remember is that the bigger the number we put in, the longer the process takes. Staying under 20 is generally a good idea. Upon executing this command you will receive a large amount of information. At this point all we are interested in are the points it gives us. Some points it gives us are \((-2:8:1), (12:36:1), (18:72:1), (50:35:8), \) etc. Note that the last point is equivalent to the point \(\left(\frac{50}{8}:\frac{35}{8}:1\right)\) upon normalizing so that \(z = 1\). We can now use SAGE to add any of these points for us.

sage: \(P = E([-2,8]); Q = E([12,36]), R = E([50,35,8])\)

sage: \(P + Q\)
\((-6:0:1)\)
sage: \(Q + R\)
\((-12:36:1)\)
sage: \(5\times P\)
\((-1074922978 : 394955797978664 : 1)\)

You should compute a couple of these by hand to make sure you are comfortable working with the formulas derived above!

6. A SHORT INTERLUDE ON ABSTRACT ALGEBRA

Those familiar with abstract algebra can safely skip this section. For those not familiar we give a brief introduction so that we have a rudimentary vocabulary. In the future if you do study abstract algebra you will be able to come back and see how this theory fits in with what you learn.

**Definition 6.1.** A group is a nonempty set \(G\) together with a binary operation \(\oplus\) so that

1. \(g \oplus h \in G\) for every \(g, h \in G\),
2. There exists an element \(0_G \in G\) so that \(g \oplus 0_G = g = 0_G \oplus g\) for every \(g \in G\),
3. For every \(g \in G\), there exists \(-g \in G\) so that \(g \oplus (-g) = 0_G = (-g) \oplus g\),
4. \((g \oplus h) \oplus k = g \oplus (h \oplus k)\) for every \(g, h, k \in G\).

If in addition one has that \(g \oplus h = h \oplus g\) for every \(g, h \in G\) we say that \(G\) is an abelian group.

**Example 6.2.**
1. The sets \(\mathbb{Z}, \mathbb{Q}, \mathbb{R},\) and \(\mathbb{C}\) are each abelian groups under the operation \(\oplus = +\) and the identity \(0_G = 0\).
(2) The sets $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, and $\mathbb{C} - \{0\}$ are all abelian groups with the operation $\oplus$ being multiplication and the identity $0_G = 1$. Note that $\mathbb{Z} - \{0\}$ is not a group under multiplication as it does not satisfy property (3). For example, 2 would have inverse $\frac{1}{2} \not\in \mathbb{Z}$.

(3) Define $G$ by

$$G = \text{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}.$$

This set is a group under matrix multiplication with identity given by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(4) The set $G = E_N(\mathbb{Q})$ with $\oplus$ defined as above is an abelian group with identity element the point at infinity.

As it will be necessary for us to compare groups, we define the appropriate type of map used to study groups.

**Definition 6.3.** A map $f : G \to H$ between groups $(G, \oplus_G)$ and $(H, \oplus_H)$ is said to be a **group homomorphism** if $f(g_1 \oplus_G g_2) = f(g_1) \oplus_H f(g_2)$ for every $g_1, g_2 \in G$. If $f$ is also bijective we say that $f$ is a **group isomorphism**. If there is an isomorphism between two groups $G$ and $H$ we say the groups are **isomorphic** and write $G \cong H$.

Essentially a group homomorphism is a map that respects the operations of the groups. Two groups that are isomorphic can be thought of as the same group in disguise.

**Definition 6.4.** A subset $H \subset G$ of a group $(G, \oplus_G)$ is a **subgroup** if it is also a group under the operation $\oplus_G$.

**Exercise 10.** Let $(G, \oplus)$ be a group and $H \subset G$. Show it is enough to prove that $H$ is nonempty and $h_1 \oplus (-h_2) \in H$ for every $h_1, h_2 \in H$ to conclude that $H$ is a subgroup of $G$.

In our study of elliptic curves we will need the following result.

**Theorem 6.5.** Let $G$ be a finite group, i.e., $\#G < \infty$ and $H$ a subgroup of $G$. Then necessarily $\#H \mid \#G$.

We do not give a proof as it would take us too far astray. However, you can think of it as the generalization of the result that $\text{ord}_n(a) \mid \phi(n)$.

**Exercise 11.** If one thinks of Theorem 6.5 as a generalization of the fact that $\text{ord}_n(a) \mid \phi(n)$, what is the group $G$ and what is the subgroup $H$?
Exercise 12. Show that the set
\[ \text{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, \ ad - bc = 1 \right\} \]
is a subgroup of $\text{GL}_2(\mathbb{R})$.

Exercise 13. Let $(G, \oplus)$ be an abelian group. Let $n$ be an integer and for $g \in G$ write $ng$ to denote the element $g \oplus g \oplus \cdots \oplus g$ where the addition occurs $n$ times. Of course if $n < 0$ we mean the additive inverse of $g$ is added to itself $n$ times and if $n = 0$ we mean the element $0_G$. Prove that the set
\[ G[n] = \{ g \in G : ng = 0_G \} \]
is a subgroup of $G$. Define
\[ G_{\text{tors}} = \{ g \in G : ng = 0_G \text{ for some } n \in \mathbb{Z} \}. \]
Prove that $G_{\text{tors}}$ is a subgroup of $G$.

We will also need the notion of a field. This is a generalization of the familiar sets $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

Definition 6.6. Let $F$ be a nonempty set with two operations $\oplus$ and $\odot$ so that the following properties hold:
(1) The set $F$ is an abelian group under $\oplus$,
(2) For every $a, b \in F$ one has $a \odot b \in F$,
(3) There exists an element $1_F \in F$ not equal to $0_F$ so that for every $a \in F$ one has $a \odot 1_F = a = 1_F \odot a$,
(4) For every $a, b, c \in F$ one has $(a \odot b) \odot c = a \odot (b \odot c)$,
(5) For every $a, b \in F$ one has $a \odot b = b \odot a$,
(6) For every $a, b, c \in F$ one has $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

We then say that $F$ is a commutative ring with identity. If in addition $F$ satisfies the property that for every element $a \in F$ not equal to $0_F$ there exists an element $a^{-1} \in F$ so that $a \odot a^{-1} = 1_F$ we say $F$ is a field.

Example 6.7. The sets $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all fields under the operations of ordinary addition and multiplication. The set $\mathbb{Z}$ is a commutative ring with identity but not a field.

Definition 6.8. Let $(R, \oplus_R, \odot_R)$ and $(S, \oplus_S, \odot_S)$ be commutative rings with identities. A map $f : R \to S$ is a ring homomorphism if it satisfies the following properties:
(1) $f(1_R) = 1_S$,
(2) For every $r_1, r_2 \in R$ one has $f(r_1 \oplus_R r_2) = f(r_1) \oplus_S f(r_2)$,
(3) For every $r_1, r_2 \in R$ one has $f(r_1 \odot_R r_2) = f(r_1) \odot_S f(r_2)$.
If in addition $f$ is bijective we say $f$ is a ring isomorphism. If there is a ring isomorphism between two rings $R$ and $S$ we say they are isomorphic and write $R \cong S$.

The most important example for us will be the field $\mathbb{Z}/p\mathbb{Z}$ where $p$ is a prime. We now introduce this set. It is expected that you are familiar with congruence class arithmetic. Let

$$\mathbb{Z}/p\mathbb{Z} = \{ \bar{i} : 0 \leq i \leq p - 1 \}$$

where $\bar{i} = \{ m \in \mathbb{Z} : m \equiv i \pmod{p} \}$. One can add and multiply these congruence classes by $\bar{i} \oplus \bar{j} = \bar{i + j}$ and $\bar{i} \odot \bar{j} = \bar{ij}$. From now on we use normal multiplication and addition notation for these operations.

**Exercise 14.** Write out addition and multiplication tables for $\mathbb{Z}/5\mathbb{Z}$. In other words, write out the results for all possible additions and multiplications of the five elements $\bar{0}, \bar{1}, \bar{2}, \bar{3},$ and $\bar{4}$ of $\mathbb{Z}/5\mathbb{Z}$.

The properties showing that $\mathbb{Z}/p\mathbb{Z}$ is a field follow directly from the properties of congruence class arithmetic. We highlight the only one that requires that we use a prime in our definition.

**Proposition 6.9.** Let $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ with $\bar{a} \neq \bar{0}$. There exists $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$ with $\bar{b} \neq \bar{0}$ and $\bar{a}\bar{b} = \bar{1}$.

**Proof.** The fact that $\bar{a} \neq \bar{0}$ implies that $p \nmid a$. Thus, it must be the case that $\gcd(a, p) = 1$. Hence there exists $m, n \in \mathbb{Z}$ so that $am + pn = 1$. Observe that $am \equiv 1 \pmod{p}$. Thus, if we set $\bar{b} = \bar{m}$ we have the result.

The fields $\mathbb{Z}/p\mathbb{Z}$ are also groups under addition (as all fields are!) It is customary to write $\mathbb{F}_p$ instead of $\mathbb{Z}/p\mathbb{Z}$ when we are thinking of $\mathbb{Z}/p\mathbb{Z}$ as a field instead of just a group. We follow this notation throughout these notes.

7. BACK TO ELLIPTIC CURVES

We are now finally able to gather our work thus far and start getting results on congruent numbers.

**Definition 7.1.** Let $P \in E_N(\mathbb{Q})$. We say $P$ is a torsion point if there exists $n \in \mathbb{Z}$ so that $nP = 0_{E_N}$. The set of all torsion points is denoted $E_N(\mathbb{Q})_{\text{tors}}$. For a particular integer $n$, we write $E_N(\mathbb{Q})[n]$ to denote the set $\{ P \in E_N(\mathbb{Q}) : nP = 0_{E_N} \}$. If $P$ is a torsion point and $n$ is the smallest positive integer so that $nP = 0_{E_N}$ we say that $P$ has order $n$.

Note that exercise 13 shows that $E_N(\mathbb{Q})[n]$ and $E_N(\mathbb{Q})_{\text{tors}}$ are both subgroups of $E_N(\mathbb{Q})$. 
Exercise 15. The points in \(E_N(\mathbb{Q})[2]\) are the points so that \(2P = 0_{E_N}\). Give a geometric description of these points. Use this description to find all such points.

Our goal is to completely determine the group \(E_N(\mathbb{Q})_{\text{tors}}\). To this end we will prove the following theorem.

**Theorem 7.2.** For \(N\) a positive square-free integer, one has

\[
E_N(\mathbb{Q})_{\text{tors}} = \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\}.
\]

The proof of this theorem, and the subsequent results on congruent numbers require us to consider elliptic curves not just defined over \(\mathbb{Q}\) but also elliptic curves defined over the field \(\mathbb{F}_p\). To accomplish this, we consider the curve

\[
E_N : y^2 = x^3 - N^2 x.
\]

We call this the reduction of the curve \(E_N\) modulo \(p\). Note that the \(p\) does not show up in the notation for the reduction. This is standard notation and it is assumed the reader can keep track of what \(p\) is being used.

**Example 7.3.** Consider the curve \(E_7\). We reduce this curve modulo 3 to obtain \(\overline{E}_7\). By checking all of the points \((\bar{i} : \bar{j} : \bar{1})\) and \((\bar{i} : \bar{j} : \bar{0})\) for \(0 \leq i, j \leq 2\) we find that

\[
\overline{E}_7(\mathbb{F}_3) = \{(\bar{0} : \bar{1} : \bar{0}), (\bar{0} : \bar{0} : \bar{1}), (\bar{1} : \bar{0} : \bar{1}), (\bar{2} : \bar{0} : \bar{1})\}.
\]

We do need to be careful here as for some primes \(p\) the curve \(\overline{E}_N\) may have singular points!

**Exercise 16.** Show that \(\overline{E}_N\) is nonsingular if and only if \(p \nmid 2N\).

We also need to make sure that we still have an addition on \(\overline{E}_N\) in order to consider it as an elliptic curve over \(\mathbb{F}_p\). Let \(P = (x(P), y(P))\) and \(Q = (x(Q), y(Q))\) be points in \(\overline{E}_N(\mathbb{F}_p)\) for \(p\) a prime with \(p \nmid 2N\). We can define the point \(P \oplus Q = (x(P \oplus Q), y(P \oplus Q))\) by the same formulas used before. Namely, for \(x(P) \neq x(Q)\) we define

\[
x(P \oplus Q) = m^2 - x(P) - x(Q)
\]

\[
y(P \oplus Q) = m(x(R) - x(P)) + y(P)
\]

where we note that \(m = (y(P) - y(Q))(x(P) - x(Q))^{-1}\) makes sense since \(\mathbb{F}_p\) is a field and \(x(P) - x(Q) \neq 0\). If \(x(P) = x(Q)\) we define \(P \oplus Q = (\bar{0} : \bar{1} : \bar{0})\) as was the case before (this condition forces \(y(P) = -y(Q)\)).

**Exercise 17.** Check that the equations defining \(2P\) make sense when considered on \(\overline{E}_N(\mathbb{F}_p)\).
If one wants to work with the reduction $E_N$ in SAGE, one uses the command

sage: $E = \text{EllipticCurve(FiniteField($p$), [$-N^2$, 0])}$; $E$

Elliptic Curve defined by $y^2 = x^3 - N^2x$ over the finite field of size $p$.

Once the curve is defined in this way one can work as before with the curve.

Since we are interested in information about $E_N(Q)$ it may seem pointless to study $E_N(F_p)$. However, while we cannot count the number of points in $E_N(Q)$ easily, we can count the number of points in $E_N(F_p)$ by merely checking all of the points since there are now only finitely many possibilities! Thus, it is much easier to study $E_N(F_p)$ and we can use this information at primes $p \nmid 2N$ to piece information together about $E_N(Q)$.

We can define a map from $P^2_Q$ to $P^2_F_p$ as follows. Let $(x : y : z) \in P^2_Q$. By multiplying by an appropriate integer we can clear the denominators and arrange so that $\gcd(x, y, z) = 1$. Thus, we have $x_1, y_1, z_1 \in \mathbb{Z}$ so that $(x_1 : y_1 : z_1) = (x : y : z)$ and $\gcd(x_1, y_1, z_1) = 1$. This means we can always choose $(x : y : z)$ so that $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$. Define the map by $(x : y : z) \mapsto \left(\bar{x} : \bar{y} : \bar{z}\right)$. Note that this is well defined since we cannot have $\bar{x}, \bar{y}, \text{ or } \bar{z}$ all equal to $\bar{0}$ since $\gcd(x, y, z) = 1$. It is important here that we are able to work in projective coordinates so that we can clear denominators and define this map. Note that by our above definition of addition on $E_N(F_p)$ we have that the map $P^2_Q \to P^2_F_p$ restricts to a group homomorphism $E_N(Q) \to E_N(F_p)$.

In general one does not have that the map $P^2_Q \to P^2_F_p$ is an injection.

We have the following proposition determining when two points map to the same point under this map.

**Proposition 7.4.** Let $P = (x_1 : y_1 : z_1)$ and $Q = (x_2 : y_2 : z_2)$. Then $P$ and $Q$ map to the same point in $P^2_F_p$ if and only if $p \mid x_1y_2 - x_2y_1$, $p \mid x_2z_1 - x_1z_2$, and $p \mid y_1z_2 - y_2z_1$.

**Proof.** First suppose that $P$ and $Q$ map to the same point, i.e., $\bar{P} = (\bar{x}_1 : \bar{y}_1 : \bar{z}_1) = (\bar{x}_2 : \bar{y}_2 : \bar{z}_2) = \bar{Q}$. Necessarily we have that $p$ cannot divide $x_1, y_1, \text{ and } z_1$. Without loss of generality we assume $p \nmid x_1$. 

Since $\overline{P} = \overline{Q}$ we also get that $p \mid x_2$. We then have

\[
\begin{align*}
(x_1 x_2 : x_1 \overline{y}_2 : x_1 \overline{z}_2) &= (x_2 : \overline{y}_2 : \overline{z}_2) \\
&= \overline{Q} \\
&= \overline{P} \\
&= (x_1 : \overline{y}_1 : \overline{z}_1) \\
&= (x_2 \overline{x}_1 : x_2 \overline{y}_1 : x_2 \overline{z}_1).
\end{align*}
\]

Since the first $x$-coordinates are equal, we must have the $y$ and $z$-coordinates equal as well. Thus, $p \mid (x_1 y_2 - x_2 y_1)$ and $p \mid (x_1 z_2 - x_2 z_1)$.

If $p \mid y_1$, then $p \mid y_2$ and so clearly $p \mid (y_1 z_2 - y_2 z_1)$. If $p \nmid y_1$, we can replace $x_1$ with $y_1$ in the above argument to obtain that $p \mid (y_1 z_2 - y_2 z_1)$.

Suppose now that $p \mid x_1 y_2 - x_2 y_1$, $p \mid x_2 z_1 - x_1 z_2$, and $p \mid y_1 z_2 - y_2 z_1$.

If $p \nmid x_1$, then

\[
\begin{align*}
\overline{Q} &= (x_2 : \overline{y}_2 : \overline{z}_2) \\
&= (x_1 x_2 : x_1 \overline{y}_2 : x_1 \overline{z}_2) \\
&= (x_2 \overline{x}_1 : x_2 \overline{y}_1 : x_2 \overline{z}_1) \\
&= \overline{P}
\end{align*}
\]

where we have used for example that $x_1 \overline{y}_2 = x_2 \overline{y}_1$ by our assumption.

Now assume that $p \mid x_1$. Then we must have either $p \nmid y_1$ or $p \nmid z_1$. However, our assumption gives that $x_2 z_1 \equiv 0 \pmod{p}$ and $x_2 y_1 \equiv 0 \pmod{p}$. Since either $y_1$ or $z_1$ is nonzero modulo $p$, we must have $x_2 \equiv 0 \pmod{p}$. Now assume without loss of generality that $y_1 \not\equiv 0 \pmod{p}$.

Then we have

\[
\begin{align*}
\overline{Q} &= (\overline{u} : \overline{y}_1 \overline{y}_2 : \overline{y}_1 \overline{z}_2) \\
&= (\overline{u} : \overline{y}_1 \overline{y}_2 : \overline{y}_2 \overline{z}_1) \\
&= \overline{P}
\end{align*}
\]

where we have used that $\overline{y}_1 \overline{z}_2 = \overline{y}_2 \overline{z}_1$.

\[\blacksquare\]

**Example 7.5.** It is not true in general that the map $E_N(\mathbb{Q}) \to \overline{E}_N(\mathbb{F}_p)$ is a surjection. Consider the reduction of the elliptic curve $E_{21}$ modulo 5. One can verify that the point $(\overline{2}, \overline{4})$ is in $\overline{E}_{21}(\mathbb{F}_5)$ but $(2, 4)$ is not in $E_{21}(\mathbb{Q})$.

**Exercise 18.** Let $p$ be a prime with $p \nmid 2N$. The only 2-torsion points in $\overline{E}_N(\mathbb{F}_p)$ are the points $(\overline{0} : \overline{1} : \overline{0}), (\overline{0} : \overline{0} : \overline{1}),$ and $(\pm \overline{N} : \overline{0} : \overline{1})$.

For $p \nmid 2N$, we write $a_{E_N}(p) = p + 1 - \#\overline{E}_N(\mathbb{F}_p)$. We can extend the definition by the following rules. Set $a_{E_N}(p') = a_{E_N}(p^{-1})a_{E_N}(p)$.
\( p \alpha_{E_N}(p^{r-2}) \) for \( r \geq 2 \) and \( p \) a prime with \( p \not|\ 2N \) and \( \alpha_{E_N}(mn) = \alpha_{E_N}(m) \alpha_{E_N}(n) \) for relatively prime \( m \) and \( n \) with \( \gcd(mn,2N) = 1 \).

**Lemma 7.6.** Let \( p \) be a prime with \( p \not|\ 2N \) and \( p \equiv 3 \pmod{4} \). Then \( \alpha_{E_N}(p) = 0 \).

**Proof.** We begin by noting that \((\overline{0} : \overline{1} : \overline{0}), (\overline{0} : \overline{0} : \overline{1}), (\pm \overline{N} : \overline{0} : \overline{1})\) are all in \( E_N(F_p) \) by exercise 18. These points are all distinct because of the fact that \( p \not|\ 2N \). We now count the points \((x,y) \in E_N(F_p)\) with \( x \neq \overline{0}, \pm \overline{N} \). Note that this is enough as the only point \((x : y : z)\) in \( E_N(F_p) \) with \( z = \overline{0} \) is \((\overline{0} : \overline{1} : \overline{0})\). Thus there are \( p-3 \) possible values for \( x \). We pair the remaining values of \( x \) off as \( \{x,-x\} \). We claim that \( x \neq -x \). It is at this point that we use that \( x \neq \overline{0}, \pm \overline{N} \) for if \( x = -x \), then \( \overline{2}x = \overline{0} \) which implies that \( x \) must be a 2-torsion point. By exercise 18 we must have \( x = \overline{0}, \pm \overline{N} \), a contradiction. Thus we have that each set \( \{x,-x\} \) has cardinality 2. Let \( f(x) = x^3 - \overline{N}^2x \).

It is clear that \( f(x) \) is an odd function, i.e., \( f(x) = -f(-x) \) for all \( x \). The fact that \( p \equiv 3 \pmod{4} \) gives that \( \left( \frac{-1}{p} \right) = -1 \), i.e., \( -1 \) is not a quadratic residue modulo \( p \). Suppose \( f(x) \) is not a square modulo \( p \), i.e., \( \left( \frac{f(x)}{p} \right) = -1 \). Thus, \( \left( \frac{-f(x)}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{f(x)}{p} \right) = 1 \), so \( -f(x) \) is a square modulo \( p \). Similarly, if \( f(x) \) is a square then \( -f(x) \) is not a square. This shows that for each pair \( \{x,-x\} \) we obtain a pair of points in \( E_n(F_p) \), either \( (x, \pm \sqrt{f(x)}) \) or \( (-x, \pm \sqrt{-f(x)}) \) depending upon whether \( f(x) \) or \(-f(x) \) is a quadratic residue modulo \( p \). Thus, for the \( p-3 \) different values of \( x \) we obtain \((p-3)/2\) pairs of points \( \{x,-x\} \) which give rise to \( p-3 \) distinct points in \( E_N(F_p) \). Combining these with the four 2-torsion points we already had gives \( \alpha_{E_N}(p) = (p+1) - (p+1) = 0 \), as claimed.

This lemma as well as Proposition 7.4 are both key ingredients in the proof of Theorem 7.2. We will also need the following theorem known as Dirichlet's theorem on primes in arithmetic progressions.

**Theorem 7.7.** Let \( a,b \in \mathbb{Z} \) with \( \gcd(a,b) = 1 \). The arithmetic progression

\[ a,a+b,a+2b,\ldots \]

contains infinitely many primes.

**Proof.** (of Theorem 7.2) Let \( P \) be a point of \( E_N(Q)_{\text{tors}} \) that is not \( \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\} \). Using Exercise 18 we see that \( P \) cannot have order 2. Let \( m \) be the order of \( P \).

We claim that \( E_N(Q)_{\text{tors}} \) either has a subgroup of odd order or a subgroup of order 8. First, if \( m \) is odd then clearly \( \langle P \rangle \) is a subgroup
of $E_N(\mathbb{Q})_{\text{tors}}$ of odd order. So we can assume that $m$ is even. If $m$ is not a power of 2, say $m = 2^ab$ with $a, b \in \mathbb{Z}$, $b > 1$ and odd, then $\langle aP \rangle$ is a subgroup of $E_N(\mathbb{Q})_{\text{tors}}$ of order $b$, i.e., of odd order. Thus we can assume that $m$ is a power of 2. Since $P$ does not have order 2 we know that $m = 2^j$ with $j \geq 2$. Suppose $P$ has order 4 and let $Q = (N : 0 : 1)$. One can check that the set $\{(0 : 1 : 0), Q, P, 2P, 3P, P \oplus Q, 2P \oplus Q, 3P \oplus Q\}$ is a subgroup of $E_N(\mathbb{Q})_{\text{tors}}$ and has order 8. (Note you must show this is a subgroup and none of the elements are equal to each other!) If $j \geq 3$, then we can write $m = 8b$ with $b \geq 1$. In this case we have that $\langle bP \rangle$ is a subgroup of $E_N(\mathbb{Q})_{\text{tors}}$ of order 8. Thus, in all cases we see that $E_N(\mathbb{Q})_{\text{tors}}$ contains either a subgroup of odd order or a subgroup of order 8. Denote this subgroup by $S$ and enumerate the points as $S = \{P_1, \ldots, P_{\#S}\}$.

Our goal is to show that $S$ injects into $\overline{E}_N(\mathbb{F}_p)$ for all but finitely many primes $p$. Write the points of $\langle P \rangle$ as $P_i = (x_i : y_i : z_i)$ for $1 \leq i \leq \#S$. Consider two points $P_i$ and $P_j$ in $\langle P \rangle$ with $i \neq j$. In order to determine when $S$ injects into $\overline{E}_N(\mathbb{F}_p)$, we need to determine when $\overline{P}_i = \overline{P}_j$. Proposition 7.4 shows that $\overline{P}_i = \overline{P}_j$ if and only if $p \mid x_i y_j - x_j y_i$, $p \mid x_j z_i - x_i z_j$, and $p \mid y_i z_j - y_j z_i$. The fact that $P_i$ and $P_j$ are distinct points shows that if we consider them as vectors in $\mathbb{R}^3$ they are not proportional. Thus, the cross product is not the zero vector which implies that $(x_i y_j - x_j y_i, x_j z_i - x_i z_j, y_i z_j - y_j z_i)$ is not the zero vector. Let

$$d_{i,j} = \gcd(x_i y_j - x_j y_i, x_j z_i - x_i z_j, y_i z_j - y_j z_i).$$

Thus we have that $\overline{P}_i = \overline{P}_j$ if and only if $p \mid d_{i,j}$. If we let $D = \lcm(d_{i,j})$, then for $p > D$ we have that $\overline{P}_i \neq \overline{P}_j$ for all $i \neq j$. This shows that for all but finitely many primes, namely for all the primes larger than $D$ we have that $S$ injects into $E_N(\mathbb{Q})_{\text{tors}}$. Thus, for all but finitely many $p$ we must have that $\#S \mid \#\overline{E}_N(\mathbb{F}_p)$. We now use this to reach a contradiction.

Lemma 7.6 combined with the fact that $\#S \mid \#\overline{E}_N(\mathbb{F}_p)$ for all but finitely many $p$ implies that $p \equiv -1(\text{mod } \#S)$ for all but finitely many primes $p$ with $p \equiv 3(\text{mod } 4)$. If $\#S = 8$, then we have that there are only finitely many primes of the form $3 + 8k$, contradicting Theorem 7.7. If $\#S$ is odd and $3 \nmid \#S$, then this gives only finitely many primes of the form $4(\#S)k + 3$, contradicting Theorem 7.7 again. Finally, if $3 \mid \#S$, then we get that there are only finitely many primes of the form $12k + 7$, again contradicting Theorem 7.7. Since we have obtained a contradiction in all possible cases, it must be that there can be no such $P$. □
Exercise 19. With the set-up as in the proof of Theorem 7.2, prove that \( \{(0 : 1 : 0), Q, P, 2P, 3P, P \oplus Q, 2P \oplus Q, 3P \oplus Q\} \) is a subgroup of \( E_N(\mathbb{Q})_{\text{tors}} \) and has order 8.

Given a point \( P \in E_N(\mathbb{Q}) \) so that \( P \notin \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\} \) Theorem 7.2 implies that \( P \) has infinite order.

Corollary 7.8. Let \( P \in E_N(\mathbb{Q}) \) with \( P \notin \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\} \). Then
\[
\langle P \rangle = \{nP : n \in \mathbb{Z}\} \cong \mathbb{Z}.
\]

Proof. Define a map \( \varphi : \mathbb{Z} \to \langle P \rangle \) by \( \varphi(n) = nP \). This map is surjective by definition of \( \langle P \rangle \). Suppose \( \varphi(m) = \varphi(n) \). Then we have \( mP = nP \), i.e., \( (m-n)P = 0_{E_N} \). The fact that \( P \) is not a torsion point implies \( m = n \) and so \( \varphi \) is injective. It only remains to show that \( \varphi \) is a homomorphism. To see this observe that we have
\[
\varphi(m+n) = (m+n)P
= mP \oplus nP
= \varphi(m) \oplus \varphi(n),
\]
as required. \( \square \)

If there is such a point \( P \) with \( P \notin E_N(\mathbb{Q})_{\text{tors}} \) then we say that the rank of \( E_N(\mathbb{Q}) \) is positive. The rank essentially measures how many "independent" such points there are, namely, if \( Q \) is another point with \( Q \notin E_N(\mathbb{Q})_{\text{tors}} \) and \( Q \notin \langle P \rangle \) then \( Q \) is independent of \( P \). The rank of the elliptic curve is how many independent points there are not in \( E_N(\mathbb{Q})_{\text{tors}} \). More algebraically we have the Mordell-Weil theorem.

Theorem 7.9. One has the following isomorphism of groups
\[
E_N(\mathbb{Q}) \cong E_N(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r
\]
where in this case \( \oplus \) refers to a direct sum and \( r \) is the rank of the elliptic curve \( E_N \).

We are finally able to relate this material back to congruent numbers via the following theorem.

Theorem 7.10. Let \( N \) be a positive square-free integer. Then \( N \) is a congruent number if and only if the rank of \( E_N \) is positive.

Proof. Let \( N \) be a congruent number. We saw in Proposition 3.1 that \( N \) leads to a point \( x \in E_N(\mathbb{Q}) \) so that \( x(P) \in (\mathbb{Q}_{>0})^2 \). Since \( N \) is square-free, we have that \( x(P) \neq 0, \pm N \). Thus, the point \( P \) cannot be in \( E_N(\mathbb{Q})_{\text{tors}} \). This proves one direction of the theorem.
Suppose now that the rank of \( E_N \) is positive. This implies that there exists \( P \in E_N(\mathbb{Q}) \) with \( y(P) \neq 0 \). This shows that \( P \) is in the set \( B \) of exercise 3 and so corresponds to a triangle with area \( N \).

**Exercise 20.** Prove that if the rank of \( E_N \) is positive then \( N \) is a congruent number.

We have now reduced the problem of determining when a number \( N \) is a congruent number to determining the rank of the elliptic curve \( E_N \). This will be the subject of the following section.

### 8. A MILLION DOLLAR PROBLEM

As we have reduced determining if \( N \) is a congruent number down to determining if the rank of \( E_N \) is positive, we would like to have an easy way to determine the rank of \( E_N \). Unfortunately, determining the rank of an elliptic curve is not an easy problem at all! We will see how the rank of \( E_N \) is related to the value at 1 of the \( L \)-function of the elliptic curve.

Recall that we defined \( a_{E_N}(p) \) by

\[
a_{E_N}(p) = p + 1 - \#E_N(\mathbb{F}_p)
\]

for all primes \( p \nmid 2N \). The \( L \)-function of the elliptic curve \( E_N \) is defined by

\[
L(s, E_N) = \prod_{p \nmid 2N} (1 - a_{E_N}(p)p^{-s} + p^{1-2s})^{-1}
\]

where \( s \) is a complex number with real part suitably large. This function can be analytically continued to the entire complex plane, so we do not spend time worrying about where it converges. Our interest in this function is the conjecture of Birch and Swinnerton-Dyer. This conjecture is one of the Clay Mathematics Institute's Millenium problems. What this means is that it was deemed an interesting enough problem that the institute has offered 1 million dollars to anyone who can prove or disprove the conjecture. (The conjecture is certainly believed to be true based on lots of evidence in its favor!) We will refer to the conjecture as the BSD conjecture from now on.

**Conjecture 8.1.** (Birch and Swinnerton-Dyer) There are infinitely many rational points on the elliptic curve \( E_N \) if and only if \( L(1, E_N) = 0 \).

The conjecture is much more general than stated here and actually gives more information about the \( L \)-function at \( s = 1 \), but this form of the conjecture is enough for our purposes.
Proposition 8.2. (Assuming BSD) The integer $N$ is a congruent number if and only if $L(1, E_N) = 0$.

Proof. This follows immediately from the work in the previous section as well the conjecture. □

The work of [1], [2], [9], and [7], show that for $E_N$ one has if $r > 0$ then $L(1, E_N) = 0$. (In fact, this is true of any elliptic curve with complex multiplication.) The other direction is still an open problem. Though determining if $L(1, E_N) = 0$ is not necessarily an easy problem, it is not difficult to at least do some numerical approximations to get a very good idea if $L(1, E_N) = 0$ or not.

As was done in the previous section, we can extend the definition of $a_{E_N}(n)$ to include values of $n$ that are not prime. Recall we set

$$a_{E_N}(p^r) = a_{E_N}(p^{r-1})a_{E_N}(p) - pa_{E_N}(p^{r-2})$$

for $p \nmid 2N$ and $r \geq 2$ and

$$a_{E_N}(mn) = a_{E_N}(m)a_{E_N}(n)$$

for relatively prime $m$ and $n$ with $\gcd(mn, 2N) = 1$.

Exercise 21. Prove that $a_{E_N}(1) = 1$ for all $N$.

This allows us to write $L(s, E_N)$ as a summation instead of a product:

$$L(s, E_N) = \sum_{\substack{n \geq 0 \\gcd(n, 2N) = 1}} a_{E_N}(n)n^{-s}.$$

One can now calculate as many values for $a_{E_N}(n)$ as one would like and use the resulting finite sum upon substituting $s = 1$ as an approximation for $L(1, E_N)$. We can do computations to this end via SAGE. Suppose we have defined $E$ as our elliptic curve in SAGE. The command

```
sage: E.ap(q)
```

returns the value $a_{E_N}(q)$ for the prime $q$. If one would like a list of the values for the primes between 2 and 100 instead the command is:

```
sage: for q in primes(2,100):
    print q, E.ap(q)
```

If one would like the first 100 values of $a_{E_N}(n)$ the command is

```
sage: E.anlist(100)
```

These commands can be used to construct finite sum approximations to $L(1, E_N)$. Of course, SAGE has a built in command to do this as well:

```
sage: E.Lseries(1)
```
Exercise 22. Is 56 a congruent number? If so, give a triangle with rational side lengths and area 56. If not, prove it is not. (You may assume BSD is true).

It is still desirable to have a criterion that does not involve resorting to elliptic curves to compute if $N$ is a congruent number. Assuming the validity of BSD, Tunnell was able to prove the following theorem which reduces the problem of determining if $N$ is a congruent number to comparing the orders of finite sets. This theorem uses modular forms and as such is too far afield to cover in these notes. It should be observed though that since these are relatively small finite sets one can compute the orders of these sets in cases where computing with elliptic curves is too time consuming.

Theorem 8.3. ([8]) If $N$ is square-free and odd (respectively even) and $N$ is the area of a rational right triangle, then

$$\#\{x, y, z \in \mathbb{Z} \mid N = 2x^2 + 2y^2 + 32z^2\} = \frac{1}{2} \#\{x, y, z \in \mathbb{Z} \mid N = 2x^2 + y^2 + 8z^2\}$$

(respectively

$$\#\{x, y, z \in \mathbb{Z} \mid N/2 = 4x^2 + y^2 + 32z^2\} = \frac{1}{2} \#\{x, y, z \in \mathbb{Z} \mid N/2 = 4x^2 + y^2 + 8z^2\}.$$]

If BSD is true for $E_N$, then the equality implies $N$ is a congruent number.

Exercise 23. Determine if 2006 is a congruent number. What about 2007? You may assume BSD holds true.

Thus, we have come full circle in our discussion of congruent numbers. We began with an innocent looking problem about areas of triangles with rational side lengths. We then saw how elliptic curves arise naturally in the study of congruent numbers. From here we saw that a million dollar open conjecture actually arises in the study of congruent numbers. Finally, we see that if this million dollar conjecture is true, determining if a number is a congruent number comes down to determining the cardinality of a finite set, a simple counting problem.

REFERENCES


DEPARTMENT OF MATHEMATICS, THE OHIO STATE UNIVERSITY, COLUMBUS, OH 43210
E-mail address: jimlb@math.ohio-state.edu
Continued Fractions:

Def: A finite continued fraction is a fraction of the form

\[ a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n + \frac{1}{d_n}}}}} \]

where the \( a_i \)'s are real #',s, \( a_i \geq 0 \) if \( i > 0 \). We say that the odd numbers \( a_1, \ldots, a_n \) are the partial denominators of this fraction. We say the fraction is simple if all the \( a_i \)'s are in \( \mathbb{Z} \).

It is easy to see that any finite continued fraction is a rational number. For example, we have

\[
\frac{123}{36} = 3 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1}}}}}}}
\]

To see this, observe that

\[
3 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1}}}}}}} = 3 + \frac{1}{2 + \frac{1}{2 + \frac{1}{3}}}
\]
\[ = 3 + \frac{5}{12} \]
\[ = \frac{41}{12} = \frac{123}{36}. \]

It turns out that the converse holds as well:

**Theorem:** Any number \( \frac{a}{b} \in \mathbb{Q} \) can be written as a simple continued fraction.

**Proof:** Let \( \frac{a}{b} \in \mathbb{Q} \) with \( b > 0 \). We apply the division algorithm to obtain

\[
\frac{a}{b} = b \left( a_0 + r_1 \right) \quad 0 < r_1 < b \\
\frac{b}{r_1} = r_1 \quad a_1 \geq 0 \\
\vdots \\
\frac{r_{n-2}}{r_{n-1}} = r_{n-1} \left( a_n + r_n \right) \quad 0 < r_n < r_{n-1} \quad a_n \geq 0 \\
\frac{r_{n-1}}{r_n} = r_n \quad a_{n+1} \geq 0.
\]

We can write these equations as

\[
\frac{a}{b} = a_0 + \frac{r_1}{b} \\
= a_0 + \frac{1}{\frac{b}{r_1}} \\
\frac{b}{r_1} = a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\frac{r_2}{r_1}} \\
\vdots
\]

\[
\frac{r_{n-2}}{r_{n-1}} = a_n + \frac{r_{n-1}}{r_n} = a_n + \frac{1}{\frac{r_{n-1}}{r_n}} \\
\frac{r_{n-1}}{r_n} = a_{n+1} \geq 0.
\]
\[
\frac{r_{n-1}}{r_n} = a_n.
\]

We may continue the equations to obtain the result.

**Example:** Compute the continued fraction of \( \frac{13}{93} \).

Apply Euclid's algorithm to 13 and 93:

\[
93 = 13 \cdot 7 + 2 \quad \Rightarrow \quad \frac{93}{13} = 7 + \frac{2}{13}
\]

\[
13 = 2 \cdot 6 + 1 \quad \Rightarrow \quad \frac{13}{2} = 6 + \frac{1}{2}
\]

\[
2 = 3 \cdot 1 + 0
\]

So we have

\[
\frac{13}{93} = \frac{1}{\frac{93}{13}} = \frac{1}{7 + \frac{2}{13}} = \frac{1}{7 + \frac{1}{\frac{13}{2}}} = \frac{1}{7 + \frac{1}{6 + \frac{1}{2}}}
\]

Thus, as you can see, can be huge pain to write out. We use the...
\begin{equation}
\left[ a_0; a_1, a_2, \ldots, a_n \right]
\end{equation}

to represent

\begin{equation}
a_n + \cfrac{1}{a_{n-1} + \frac{1}{\ddots + \frac{1}{a_2 + \frac{1}{a_1}}}}.
\end{equation}

Thus, \( \frac{13}{97} = \left[ 0; 7, 6, 2 \right] \).

The relevant SAGE command is

\begin{verbatim}
continued_fraction(x).
\end{verbatim}

For example,

\begin{verbatim}
continued_fraction(173/97)
\end{verbatim}

returns

\begin{equation}
\left[ 0, 1, 7, 4, 1, 4 \right].
\end{equation}

Note that we have said nothing as of yet in regard to uniqueness. Observe that if \( a_n > 1 \), then

\begin{align*}
a_{n+1} &= \frac{a_n + a_{n-1}}{t} = \frac{(a_{n-1})^2 + t}{t}.
\end{align*}

and so

\begin{equation}
\left[ a_0; a_1, \ldots, a_n \right] = \left[ a_0; a_1, \ldots, a_{n-1}, \frac{t}{a_n} \right].
\end{equation}
If \( a_n = 1 \), then
\[
\frac{1}{a_n} = a_{n-1} + a_n = g_{n-1} + 1
\]

and so
\[
[a_0; a_1, \ldots, a_{n-1}, a_n] = [a_0; a_1, \ldots, a_{n-1} + 1].
\]

So each rational number has at least 2 representations. Let them
out these are the only ones!

**Def:** Let \( [a_0; a_1, \ldots, a_{n-1}, a_n] \) be a continued fraction. The continued

fraction \( [a_0; a_1, \ldots, a_{n-1}, a_n] \) is called the \( k^\text{th} \)

convergent and denoted by \( c_k \). We set \( c_0 = a_0 \).

**Example:**
\[
\frac{13}{93} = [0; 7, 6, 2].
\]

Thus,
\[
c_0 = c_1 = c_2 = c_3 = 0.
\]
\[
c_1 = 0 + \frac{1}{7} = \frac{1}{7}
\]
\[
c_2 = 0 + \frac{1}{7 + \frac{1}{6}} = \frac{6}{43}
\]
\[
c_3 = 0 + \frac{1}{7 + \frac{1}{6 + \frac{1}{2}}} = \frac{13}{93}
\]

The **SAGE command**

\[
v = continued\_fraction(\frac{13}{93})
\]
Convergent \((v, \mu)\)

gives \(C_k\).

**Note:** Let \(C_k = [a_0; a_1, \ldots, a_k]\) be the \(k\)-th convergent of \(a\)

continued fraction. If we replace \(a_k\) with \(a_k + \frac{1}{a_{k+1}}\), then

we obtain

\[ [q_0; a_1, \ldots, a_k + \frac{1}{a_{k+1}}] = [q_0; a_1, \ldots, a_k, a_{k+1}] \]

\[ = C_{k+1}. \]

This fact will be used when we prove properties of convergents

as they allow us to easily apply induction.

**Define:** \(P_0 = a_0, P_1 = 1, q_0 = 1, q_1 = a_0.\)

and \( P_k = q_k P_{k-1} + P_{k-2}, q_k = q_k q_{k-1} + q_{k-2}. \) \(0 \leq k \leq n\)

where \([a_0; a_1, \ldots, a_n]\) is a finite continued fraction.

**Theorem:** The \(k\)-th convergent of the simple continued fraction \([a_0; a_1, \ldots, a_n]\) is convergent

\[ C_k = \frac{P_k}{q_k} \] \(0 \leq k \leq n.\)

**Proof:** We use induction, but as the relation goes down a couple

of steps to calculate the next one, we must establish its form for

\(P_0 = a_0, P_1 = 1, q_0 = 1, q_1 = a_0.\)

and \( P_k = q_k P_{k-1} + P_{k-2}, q_k = q_k q_{k-1} + q_{k-2}. \) \(0 \leq k \leq n\)

where \([a_0; a_1, \ldots, a_n]\) is a finite continued fraction.

**Theorem:** The \(k\)-th convergent of the simple continued fraction \([a_0; a_1, \ldots, a_n]\) is convergent

\[ C_k = \frac{P_k}{q_k} \] \(0 \leq k \leq n.\)

**Proof:** We use induction, but as the relation goes down a couple

of steps to calculate the next one, we must establish its form for
Case 0: \( P_0 = a_0, P_{-1} = a_0, q_0 = a_0 q_{-1} + q_{-2} = 1. \)

Thus, \( \frac{P_0}{q_0} = a_0. \)

Case 1: \( P_1 = a_1, P_0 = a_1, a_0 + 1, q_1 = a_1 q_0 + q_{-1} = a_1 + 1 = a_1. \)

\[
\frac{P_1}{q_1} = \frac{a_1 a_0 + 1}{a_1} = a_0 + \frac{1}{a_1} = q_1.
\]

Hence, we assume inductively that for \( 2 \leq k \leq n, \) we have

\[
\frac{P_k}{q_k} = C_k,
\]

i.e.,

\[
C_k = \frac{a_k P_{k-1} + P_{k-2}}{a_k q_{k-1} + q_{k-2}}.
\]

Note here that the \( P_{k-1}, P_{k-2}, q_{k-1}, q_{k-2} \) depend only on

the initial conditions and \( a_0, a_1, \ldots, a_k. \) Thus, if we have

a different value for \( C_k, \) this will not affect the equality.

We replace \( a_k \) by \( a_k + \frac{1}{a_k}. \) Thus we have:

\[
C_{k+1} = [a_0, a_1, \ldots, a_k, a_k + \frac{1}{a_k}]
\]

\[
= \frac{(a_k + \frac{1}{a_k}) P_{k-1} + P_{k-2}}{(a_k + \frac{1}{a_k}) q_{k-1} + q_{k-2}}
\]

\[
= \frac{a_k a_{k-1} P_{k-1} + P_{k-1} + q_{k-1} q_{k-1} P_{k-2}}{a_k a_{k-1} q_{k-1} + q_{k-1} + q_{k-1} q_{k-2}}
\]

...
\[ \frac{a_{kn} (a_{k} p_{k-1} + p_{k-2}) + p_{k-1}}{a_{kn} (a_{k} q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{kn} p_k + p_{k-1}}{a_{kn} q_k + q_{k-1}} \]

as desired. Thus the result holds by induction. □

This result allows one to calculate the convergent recursively, which can be much easier!

**Example:** Recall that \( \frac{13}{73} = [0; 7, 6, 37] \).

So we have:

\[
\begin{align*}
    P_0 &= 0 \cdot P_1 + P_0 = 0 & \quad & 9_0 = 0 \cdot 9_{-1} + 9_{-2} = 1, \\
    P_1 &= 7P_0 + P_{-1} = 1 & \quad & 9_1 = 7q_0 + q_{-1} = 7, \\
    P_2 &= 6P_1 + P_0 = 6 & \quad & 9_2 = 6q_1 + q_0 = 43, \\
    P_3 &= 2P_2 + P_1 = 13 & \quad & 9_3 = 2q_2 + q_1 = 93 \\
\end{align*}
\]

Thus, the convergent is:

\[
\begin{align*}
    C_0 &= 0, \\
    C_1 &= \frac{1}{7}, \\
    C_2 &= \frac{63}{43}, \\
    C_3 &= \frac{13}{97}.
\end{align*}
\]

Which is exactly what we calculated last time!
**Thm:** Let \( Q_k = \frac{P_k}{q_k} \) be the \( k^{th} \) convergent of the finite simple continued fraction \( \pi = q_0, q_1, \ldots, q_n \). Then

\[
P_k q_{k-1} - q_k P_{k-1} = (-1)^{k-1} \quad \text{for} \quad k \leq n.
\]

Before we prove this theorem we state and prove an easy corollary.

**Cor:** For \( k \leq n \), \( P_k \) and \( q_k \) are relatively prime.

**Proof:** Suppose \( d = \gcd(P_k, q_k) \). Then \( d \mid (P_k q_{k-1} - q_k P_{k-1}) = (-1)^{k-1} \)

\[\Rightarrow d = 1.\]

**Proof (Thm):** We prove this by induction on \( k \). The base case of \( k = 1 \) is handled easily,

\[
P_{\pi_0} q_{\pi_0} - q_{\pi_0} P_{\pi_0} = (q_{\pi_0}, q_{\pi_0} - 1) - q_{\pi_0} = 1 = 1^{11}.
\]

Assume the statement is true for all \( 1 \leq j < k \).

for some \( k \). Then,

\[
P_{\pi_k} q_{\pi_k} - q_{\pi_k} P_{\pi_k} = (q_{\pi_k}, q_{\pi_k} - 1) q_{\pi_k}
\]

\[\quad - (q_{\pi_k} q_{\pi_k} q_{\pi_k - 1} P_{\pi_k}) q_{\pi_k}
\]

\[= q_{\pi_k} P_{\pi_k} q_{\pi_k} + P_{\pi_k} q_{\pi_k} - q_{\pi_k} P_{\pi_k} q_{\pi_k} - 9_{\pi_k} P_{\pi_k}.
\]

\[= q_{\pi_k} P_{\pi_k} q_{\pi_k} + P_{\pi_k} q_{\pi_k} - q_{\pi_k} P_{\pi_k} q_{\pi_k} - 9_{\pi_k} P_{\pi_k}.
\]
\[
\begin{align*}
&= - (p_k q_{k+1} - p_1 q_k) \\
&= - (-1)^k \quad \text{(by induction hyp.)} \\
&= (-1)^k.
\end{align*}
\]

Thus the result holds by induction. \(\square\)

We now investigate our first application of continued fractions. We show they can be used to investigate the Diophantine equation

\[ax + by = c.\]

We already studied this before. We can safely assume \(\text{gcd}(a, b) \mid c\)

for otherwise there is no solution. In fact, if \(\text{gcd}(a, b) \mid c\)

we can divide it out of the equation as we may as well also

assume that \(\text{gcd}(a, b) = 1.\) Write \(\frac{a}{b} = [a_0; a_1, \ldots, a_n].\) We

have

\[c_{n+1} = \frac{p_n}{q_{n+1}}, \quad c_n = \frac{p_n}{q_n} = \frac{a}{b}.\]

In particular, we have \(p_n b = q_n a\) and since \(\text{gcd}(a, b) = 1,\)

we must have \(p_n = a\) and \(q_n = b.\) (Note if \(\text{gcd}(a, b) \neq 1\) this would not necessarily be true!)
Our previous theorem gives

\[ p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1} \]

i.e.

\[ a q_{n-1} - b p_{n-1} = (-1)^{n-1} \]

Thus, if we set \( x = q_{n-1} \) and \( y = -p_{n-1} \) we have

\[ ax + by = (-1)^{n-1} \]

If \( n \) is odd, then \( n-1 \) is even and so we have

\[ ax + by = 1 \]

In particular, this gives \( x = q_{n-1} \) and \( y = -p_{n-1} \) as a solution to our original equation.

If \( n \) is even, then \( n-1 \) is odd and so

\[ ax + by = -1 \]

Thus,

\[ a(-y) + b(-x) = 1 \]

and our solution is \( x = -q_{n-1} \), \( y = p_{n-1} \). Thus, we obtain a solution to the Diophantine equation arising from the \( n-1 \) converse of \( \frac{a}{b} \).
Example: Find solutions to the Diophantine equation

\[65x + 465y = 5\]

We begin by dividing \(\gcd(65, 465) = 5\) \(\rightarrow\) an equation:

\[13x + 93y = 1.\]

The convergents \(\dfrac{13}{93}\) have already been computed,

\[C_3 = \dfrac{6}{93}.\]

Thus, \(p_3 = 6, q_3 = 93. \) Since \(n = 3 < \varphi(5) = 4\),

\[x = 6, \quad y = \dfrac{-6}{93},\]

is a solution, i.e.

\[13(43) + 93(-6) = 1.\]

Hence,

\[13(5.43) + 93(5.6) = 5\]

\(\times\) \(\text{if you want to show this relationship, consider adding it.}\)
Thus we have

$$605(43) + 465(-6) = 5$$

So $x = 43, y = -6$ is a solution to the original equation. To obtain all solutions, we have

$$x = 43 + 93t, \quad y = -6 - 13t.$$ 

**Lemma:** Let $G_k = \frac{P_k}{Q_k}$ for the simple continued fraction

$$[\alpha_0; \alpha_1, \ldots, \alpha_n].$$

Then $Q_{k-1} \leq Q_k$ for $1 \leq k < \infty$ with strict inequality when $k \geq 1$.

**Proof:** Once again we use induction on $k$. $Q_0 = 1 \leq Q_1 = 9$. Thus the base case holds. Assume it is true for $1 \leq k < n$. Then

$$Q_{k+1} = Q_k Q_{k+1} + Q_k > Q_k Q_k = Q_k^2$$

Thus the result is true by induction. □

We conclude the basics of finite simple continued fraction

with the following theorem, telling us how the convergents

converge to $[\alpha_0; \alpha_1, \ldots, \alpha_n]$. 
Thm: Let $C_n$ be the convergent of a finite simple continued fraction. We have

$$C_0 < C_2 < C_4 < \ldots$$

and

$$C_1 > C_3 > C_5 > \ldots$$

Moreover, every convergent with an odd subscript is larger than every convergent with an even subscript.

Proof: We begin by observing that

$$C_{k+2} - C_k = (C_{k+2} - C_{k+1}) + (C_{k+1} - C_k)$$

$$= \left( \frac{P_{k+2}}{q_{k+2}} - \frac{P_{k+1}}{q_{k+1}} \right) + \left( \frac{P_{k+1}}{q_{k+1}} - \frac{P_k}{q_k} \right)$$

$$= \left( \frac{P_{k+2}q_{k+1} - P_{k+1}q_k}{q_{k+1}q_{k+2}} \right) + \left( \frac{P_{k+1}q_k - P_kq_{k+1}}{q_kq_{k+1}} \right)$$

$$= \frac{(-1)^{k+1}}{q_{k+1}q_{k+2}} + \frac{(-1)^k}{q_kq_{k+1}}$$

$$= \frac{(-1)^k (q_{k+2}q_k - q_kq_{k+2})}{q_kq_{k+1}q_{k+2}}$$

We know that $q_k > 0$ for all $k > 0$ (look at the def!), and $q_{k+2}q_k - q_kq_{k+2} > 0$ by the previous lemma. Then,
we have that \( C_{k+2} - C_k \) has the same sign as \((-1)^k\).

Thus, if \( k \) is even, \( C_{k+2} - C_k \) is positive and so we have

\[
C_{2j+2} > C_{2j}
\]

for all \( j \). Hence

\[
C_0 < C_2 < C_4 < \ldots
\]

e.g., \( k = 2k \), \( C_{2k+2} - C_{2k} \) is negative, and so

\[
C_{2j+1} < C_{2j+1}
\]

\[
\Rightarrow \quad C_1 < C_3 < \ldots
\]

Now we just need to show that \( C_{2r-1} \) is greater than \( C_{2r} \)

for all \( r \). Recall that

\[
P_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}.
\]

Thus,

\[
C_k - C_{k-1} = \frac{P_k}{q_{k-1}} - \frac{P_{k-1}}{q_k}
\]

\[
= \frac{P_k q_{k-1} - q_k p_{k-1}}{q_k q_{k-1}}
\]

\[
= (-1)^{k-1} \frac{q_{k-1}}{q_k q_{k-1}}.
\]

Thus, we have

\[
C_{2j} - C_{2j-1} = (-1)^{2j-1} \frac{q_{2j-1}}{q_{2j} q_{2j-1}} < 0.
\]

\[
\Rightarrow \quad C_{2j} < C_{2j-1}.
\]
Thus,
\[ C_5 < C_{5+1} < C_{5+2} < \cdots < C_n. \]

This gives the result.

What this theorem is telling us is that the odd convergents are converging from above and the even convergents are converging from below.

It will be important to note that we did not use the length of the continued fraction at all in this proof. This will allow us to conclude the same property for simple infinite continued fractions.

**Def.:** An infinite continued fraction is a continued fraction of the form

\[
A_0 + \frac{b_0}{A_1 + \frac{b_2}{A_2 + \frac{b_3}{A_3 + \cdots}}} = A_0 + \frac{b_0}{A_1 + \frac{b_1}{A_2 + \frac{b_2}{A_3 + \cdots}}}
\]

Where \( A_0, A_1, A_2, \ldots, b_0, b_1, b_2, \ldots \) are real numbers.
We will be interested in simple continued fractions. These are of the form

\[ a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}} \]

with the \( a_i \) integers and \( a_1, a_2, \ldots \) all positive. Again we use the compact notation \([a_0; a_1, a_2, \ldots]\) to denote the continued fraction. The first thing we need to establish is that this actually makes sense, i.e., that

\[ \lim_{n \to \infty} [a_0; a_1, \ldots, a_n] \]

converges to a real number.

Using the theorem proved last time we have

(2) \( c_0 < c_2 < c_3 < \ldots < c_{2n} < \ldots < c_{2n+1} < \ldots < c < c_1 < c \)

Thus, \([c_{2n}]\) is a monotonically increasing sequence bounded above by \( c \). Similarly, \([c_{2n+1}]\) is a monotonically decreasing sequence bounded below by \( c_0 \). Thus, we see that
must converge, say to \( x \) and \( \beta \). We would like to conclude that
\( x = \beta \) and so both sequences can be defined to have limit \( x \).

Recall
\[
P_{n+1} a_n - P_n a_{n+1} = (-1)^{2n+1}.
\]

Thus,
\[
P_{n+1} a_n - P_n a_{n+1} = \frac{P_{n+1} a_n - P_n a_{n+1}}{9 x n}
\]
\[
< \frac{1}{9 x n}.
\]

However, we know \( 9 x \) is an increasing unbounded sequence and so as \( n \to \infty \), we get \( x = \beta \). Thus we have that our infinite simple continued fraction actually makes sense!

Prove: Suppose \( a_0, a_1, a_2, \ldots \) \( 1 = \frac{a}{b} = c_0 \). Then
\[
\frac{a}{b} = \lim_{n \to \infty} c_n.
\]
We know that \( \frac{a}{b} \) must lie
strictly between $C_n$ and $C_{nn}$ for any $n$ (converge, not a smaller
depending on the parity of $n$).

\[ 0 < \left| \frac{a}{b} - C_n \right| < \left| C_{nn} - C_n \right| \]

\[ = \left| \frac{P_n}{q_{nn}} - \frac{p_n}{q_n} \right| = \frac{1}{q_n q_{nn}} \]

i.e.,

\[ \left| \frac{a}{b} - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{nn}} \]

\[ \Rightarrow \left| q_n a - b p_n \right| < \frac{b}{q_{nn}} \] (assume $a > 0, b > 0$)

Since $q_n$ increases without bound, we choose large enough $n$
\[ \text{so that } b < q_{nn} \Rightarrow 0 < \frac{b}{q_{nn}} < 1. \]

\[ \Rightarrow 0 < \left| q_n a - b p_n \right| < 1 \]

This is a contradiction because $q_n a - b p_n \in \mathbb{Z}$.  

**Thm:**  \( \{a_0, a_1, a_2, \ldots\} \cong \{b_0, b_1, b_2, \ldots\} \) then \( a_n = b_0 \) for all $n \geq 0$.

**Proof:** We begin by noting the following 2 facts:
(1) Since \( [a_0; a_1, a_2, \ldots, a_n] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_n]} \),
we have

\[
\lim_{n \to \infty} [a_0, a_1, \ldots, a_n] = a_0 + \lim_{n \to \infty} \frac{1}{[a_1; a_2, \ldots, a_n]}
\]

\[
= a_0 + \frac{1}{[a_1; a_2, \ldots, \ldots]}
\]

Thus,

\[
[a_0, a_1, a_2, \ldots, \ldots] = a_0 + \frac{1}{[a_1; a_2, \ldots, \ldots]}
\]

(2) Let \( x = [a_0; a_1, a_2, \ldots, \ldots] \). Then \( c_0 < x < c_1 \), i.e.,
\[
a_0 < x < a_0 + \frac{1}{a_1}
\]

Since \( a > 1 \), we have
\[
a_0 < x < a_0 + 1
\]

Thus, we have \( Lx_1 = a_0 \).

Now assume

\[
[a_0; a_1, a_2, \ldots, \ldots] = [b_0; b_1, b_2, \ldots] \Rightarrow x
\]

Thus, from (1) above we have

\[
a_0 + \frac{1}{[a_1; a_2, \ldots, \ldots]} = b_0 + \frac{1}{[b_1; b_2, \ldots, \ldots]} \Rightarrow x
\]

\[
(b_0, b_1) \Rightarrow a_0 = Lx_1 = b_0 \Rightarrow \text{There is a root } x
\]

\[
[a_0; a_1, a_2, \ldots, \ldots] = [b_0; b_1, b_2, \ldots]
\]

Proceed now by induction to finish the proof for \( n \).
Since all our continued fractions are now infinite, it becomes more difficult to write them down explicitly. This is much like the case when we do decimal expansion. As in that situation, it can happen that we are lucky and get a block of integers that repeat. Namely, we may have

\[ [a_0; a_1, \ldots, a_m, b_1, \ldots, b_n, \ldots] \]

In this case, we write

\[ [a_0; a_1, \ldots, a_m, \overline{b_1, \ldots, b_n}] \]

If \( b_1, \ldots, b_n \) is the smallest block that repeats, we say that \( b_1, \ldots, b_n \) is the period of the expansion, and the length of the period is \( n \).

We finally compute some examples.

**Example:** What number does the continued fraction \([1; \overline{5,6}]\) represent?

Note that since 5, 6 repeat, we can set \( x = [1; \overline{5,6}] \) and write

\[ [1; \overline{5,6}] = 1 + \frac{1}{5 + \frac{1}{6 + \frac{1}{x}}} \]
So we really need to figure out $x$. We have

$$x = 5 + \frac{1}{6 + \frac{1}{x}} = 5 + \frac{x}{6x + 1}$$

$$= \frac{30x + 5 + x}{6x + 1}$$

i.e., we have that $x$ satisfies:

$$6x^2 + 5 = 31x + 5 \iff 6x^2 - 30x - 5 = 0$$

$$\iff x = \frac{-30 \pm \sqrt{900 - (-5)(4)}}{12}$$

$$= \frac{5}{2} \pm \frac{\sqrt{930}}{12}$$

Thus, we have

$$\left[ 1; \frac{5.6}{2} \right] \approx 1 + \frac{1}{\frac{5}{2} \pm \frac{\sqrt{930}}{12}}$$

(since $x > 0$, and

$$\frac{5}{2} - \frac{\sqrt{930}}{12} < 0$$

$$= 1 + \frac{12}{30 + \sqrt{930}} \left( \frac{30 - \sqrt{930}}{30 - \sqrt{930}} \right)$$

$$= 1 + \frac{360 - 12\sqrt{930}}{900 - 930} = 1 + \frac{360 - 12\sqrt{930}}{-30}$$

$$= 1 + \frac{60 - 2\sqrt{930}}{5} = \frac{65 - 2\sqrt{930}}{5}$$
Recall when we were working with finite continued fractions, first we
saw each finite simple continued fraction in a rational number. We
then proved that each rational number could be expressed in a
finite simple continued fraction. We have shown that a simple
infinite continued fraction must be an irrational number. We
now show each irrational number in a simple infinite
continued fraction.

Thm: Every irrational number has a unique representation
as a simple infinite continued fraction.

Proof: We have already seen that if

\[ \left[ a_0; a_1, \ldots \right] = [b_0; b_1, \ldots] \]

then \( a_i = b_i \), for all \( i \), if a number has a representation
as an infinite continued (simple) fraction, it is necessarily
unique. We actually give an algorithm to associate
the continued fraction to the real number.

Let \( x_0 \) be our real number. Set

\[ X_1 = \frac{1}{x_0 - L x_0} \]
\[ x_k = \frac{1}{x_{k-1} - L x_{k-1}} \quad k \geq 1 \]

Let \( a_0 = L x_0 \), \( a_1 = L x_1 \), etc.

The \( a_k \) are defined inductively by

\[ a_k = L x_k \] where \( x_{k+1} = \frac{1}{x_k - a_k} \quad k \geq 0. \]

It is clear that if \( x_i \) is irrational, so is \( x_{i+1} \). Since \( x_0 \) is irrational, so are all the \( x_i \)'s. Thus we have

\[ 0 < x_k - a_k = x_k - L x_k > 1. \]

\[ \Rightarrow \quad \frac{1}{x_k - a_k} > 1 \quad \text{for all } k \]

\[ \Rightarrow \quad x_{k+1} > 1 \quad \text{for all } k \quad (\text{since } x_{k+1} = \frac{1}{x_k - a_k}) \]

Thus, \( a_{k+1} = L x_{k+1} > 1 \) for all \( k \geq 0 \). This gives an infinite sequence of integers so that \( a_k > 1 \) except possibly for \( k = 0 \). By making substitutions we obtain

\[ x_0 = a_0 + \frac{1}{x_1} \]

\[ = a_0 + \frac{1}{a_1 + \frac{1}{x_2}} \]
\[
= \cdots = \{a_0, a_1, \ldots, a_n, x_{n+1}\} \quad \forall n \geq 0
\]

We now show that \(x_0 = \{a_0, a_1, a_2, \ldots\}\). We have

\[
x_0 = C_n = \{a_0, a_1, \ldots, a_n, x_{n+1}\} = \frac{p_n}{q_n} = \frac{x_{n+1}p_n + q_{n+1}p_{n-1}}{x_{n+1}q_n + q_{n+1}}.
\]

However, we see that \(C_n = C_n\) for \(0 \leq n\) were \(C_n\) are the convergents of \(\{a_0, a_1, a_2, \ldots\\} a\) that

\[
x_0 = \frac{x_{n+1}p_n + q_{n+1}p_{n-1}}{x_{n+1}q_n + q_{n+1}}.
\]

Thus,

\[
x_0 - x_n = \frac{x_{n+1}p_n + q_{n+1}p_{n-1}}{x_{n+1}q_n + q_{n+1}} - \frac{p_n}{q_n} = \frac{q_n p_n x_{n+1} + q_n^2 - x_{n+1}q p_n - q_n p_{n-1}}{q_n \{x_{n+1}q_n + q_{n+1}\}} = \frac{-1 (p_n q_{n+1} - p_{n-1}q_n)}{q_n \{x_{n+1}q_n + q_{n+1}\}} = \frac{-1 (-1)^{n-1}}{q_n \{x_{n+1}q_n + q_{n+1}\}}.
\]
\[ x_0 = [a_0; a_1, \ldots, a_n, x_{mm}] = (a_n + \frac{1}{x_{mm}}) \]

We now show that in fact \( x_0 = [a_0; a_1, a_2, \ldots] \).

Let \( n_0 \) be a fixed positive integer. Then the first \( n \) convergents \( C_k = \frac{p_k}{q_k} \) are the same for \([a_0; a_1, \ldots, a_n, x_{mm}]\) as for \([a_0; a_1, a_2, \ldots] \). Denote the convergents of \([a_0; a_1, a_2, \ldots, a_n, x_{mm}]\) by \( C_k' \) and the convergents of \([a_0; a_1, a_2, \ldots] \) by \( C_k \). Recall that

\[ C_{nn} = [a_0; a_1, \ldots, a_n, a_{nn}] \]
\[ = [a_0; a_1, \ldots, a_n + \frac{1}{a_{nn}}] \]

Thus,

\[ x_0 = C_{nn}' = [a_0; a_1, \ldots, a_n, x_{nn}] \]
\[ = [a_0; a_1, \ldots, a_n + \frac{1}{x_{nn}}] \]
\[ = \frac{P_{nn}'}{Q_{nn}'} = \frac{a_{nn} P_n + P_{nn}}{a_{nn} Q_n + Q_{nn-1}} \]
\[ = (a_n + \frac{1}{x_{nn}}) \]
By definition \( x_{n+1} > a_n x_n \), so

\[
|x_0 - c_n| = \frac{1}{q_n(x_0q_n + q_{n+1})} < \frac{1}{q_n(q_nq_{n+1} - q_{n+1})} = \frac{1}{q_n q_{n+1}}.
\]

Since the \( q_n \) are integers increasing with bound \( n \to \infty \), we see that

\[
\lim_{n \to \infty} c_n = x_0
\]

as desired.

**Corollary:** If \( c_n = p_n/q_n \) is \( n \to \infty \) convergent to \( x \), then

\[
|x - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.
\]

**Example:** Compute the continued fraction of \( \sqrt{5} \).

Note that \( 1^2 < 2 < 3^2 = 9 \), so \( \sqrt{5} \in (1, 2) \).

Thus, \( x_0 = 1 + (\sqrt{5} - 1) = \frac{2}{1} \), \( a_0 = 1 \).

\[
x_1 = \frac{1}{x_0 - \ell x_0} = \frac{1}{\sqrt{5} - 1} = \sqrt{5} + 1
\]

Thus, \( a_1 = \sqrt{5} + 1 = \sqrt{5} + 1 = 2 \).

\[
x_2 = \frac{1}{x_1 - \ell x_1} = \frac{1}{\sqrt{5} + 1 - 2} = \frac{1}{\sqrt{5} - 1}
\]
\[ \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = x_1 \]

Thus, \( a_1 = a_2 \). We see that now we will get
\[ x_2 = x_3, \text{ etc., as we have} \]
\[ \sqrt{2} = [1; 2] \]

**Example:** Find the first few convergents for \( \pi \).

\[ x_0 = 3 + (\pi - 3), \quad a_0 = 3 \]
\[ x_1 = \frac{1}{x_0 - Lx_0} = \frac{1}{0.1415} = 7.047, \quad a_1 = 7 \]
\[ x_2 = \frac{1}{x_1 - Lx_1} = \frac{1}{7.067 - 7} = 7.067, \quad a_2 = 15 \]
\[ = 15.9965 \ldots \]
\[ x_3 = \frac{1}{x_2 - Lx_2} = \frac{1}{15.9966 - 15} = 1.0034 \ldots \]

Thus,

\[ \pi = [3; 7, 15, 1, \ldots] \]

We could continue to compute more convergents, but we would never end up with a repeating pattern. In fact, we already
must know the decimal expansion of \( \pi \) in order to compute its
convergent.

Continued fraction \( \pi \) gives

\[ [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1]. \]

One must be careful with the last few digits computed by \( \sqrt{5} \).

For instance, we know \( \sqrt{5} = [2; 4, 2, \ldots, 2, 4, 2] \).

\[ \sqrt{5} = [2; 4, 2, \ldots, 2, 4, 2]. \]

One of the main applications of continued fractions is to obtain
approximation to irrational numbers. Irrational numbers are easy to
deal with. However, irrational numbers can be very difficult
to deal with, in which case having a good rational approximation is
important. For instance, whereas you do a numerical computation with
if you are really using a rational approximation. When one tries

\[ \text{to obtain a good rational approximation to an irrational } \pi \text{ one}
\]

usually means finding the closest rational \( \frac{a}{b} \) when \( b \) is bounded
by some fixed number.

Given any irrational number \( x \), \( x \) is \( \frac{a}{b} \) with

\[ \frac{a}{b} \text{ and } b < \text{ fixed number}. \]
\[
\frac{c}{b} < x < \frac{c+1}{b}.
\]

Thus, we have

\[
| x - \frac{c}{b} | < \frac{1}{b}.
\]

If we let \( a = c \) or \( c+1 \) depending on which is closer to \( x \), \( \frac{c}{b} \) or \( \frac{c+1}{b} \), we have

\[
| x - \frac{a}{b} | < \frac{1}{2b}.
\]

We saw before in our corollary that if \( [a_0; a_1, \ldots] \) is the continued fraction of \( x \), then

\[
| x - \frac{C_k}{q_k} | = | x - \frac{P_k}{q_k} | < \frac{1}{2q_k^2}.
\]

As continued fractions give us significantly better approximations.

Then, mainly we would expect to get.

**Thm:** If \( 1 \leq b \leq q_n \), then the rational number \( \frac{a}{b} \) satisfies

\[
| x - \frac{P_n}{q_n} | \leq \frac{1}{2q_n}.
\]

This theorem is saying that the continued fraction converges among the best possible rational number approximations to \( x \) and \( \frac{1}{b} \).
If \( z < 0 \), then \( q \cdot y = b \cdot q_{nn} z + q_{nn} \cdot z = y < 0 \).

(This is because \( q_{nn} z < 0 \)).

If \( z > 0 \), then \( q \cdot y > 0 \) (since \( b < q_{nn} \)) \( \Rightarrow y > 0 \). Then \( y < 0 \) and \( z > 0 \) have opposite signs.

Since \( x \) lies between \( \frac{p_n}{q_n} \) and \( \frac{p_{nn}}{q_{nn}} \), we must have that

\[
q_{nn} x - p_{nn} \quad \text{and} \quad q_{nn} x - p_{nn}.
\]

have opposite signs as well (depending upon whether \( n \) is odd or even).

Thus,

\[
y(q_{nn} x - p_{nn}) \quad \text{and} \quad z(q_{nn} x - p_{nn})
\]

must have the same sign. Then,

\[
|x_{n+1} - x| = |(q_{nn} y + q_{nn} z) x - (p_{nn} y + p_{nn} z)|
\]

\[
= |y(q_{nn} x - p_{nn}) + z(q_{nn} x - p_{nn})|
\]

\[
= |y| |q_{nn} x - p_{nn}| + |z| |q_{nn} x - p_{nn}| \quad \text{(since both have the same sign)}
\]

\[
> |y| |q_{nn} x - p_{nn}|
\]

\[
> |q_{nn} x - p_{nn}|
\]

i.e., \( |x_{n+1} - x| > |q_{nn} x - p_{nn}| \) as desired.

We can now use this lemma to prove the theorem.
Proof (continued): Suppose

\[ |x - \frac{p_n}{q_n}| > |x - \frac{a}{b}|. \]

Then,

\[ |q_n x - p_n| = q_n |x - \frac{p_n}{q_n}| \]

\[ > q_n |x - \frac{a}{b}| \]

\[ > b |x - \frac{a}{b}| \]

\[ = 16x - a_1. \]

This contradicts the lemma. \( \Box \)

Example: This theorem allows us to conclude that convergents are very good approximations. Recall

\[ \pi = [3; 7, 15, 1, 292, 1, \ldots] \]

Then

\[ c_1 = \text{convergent}(\pi, 1) = \frac{22}{7} \]

\[ c_2 = \frac{333}{106} \]

\[ c_3 = \frac{355}{113} \]

\[ c_4 = \frac{103993}{33102} \]

We know that \[ |\pi - c_k| < \frac{1}{k^2}. \]
Before we prove this theorem, we need the following technical lemma.

**Lemma:** Let \( C_n = \frac{p_x}{q_n} \) be the \( n \)-th convergent of \( x = \{a_0, a_1, \ldots\} \).

\[ a \text{ and } b \text{ are integers, let } 1 \leq b < q_n, \text{ then} \]

\[ 1q_n x - p_n,1 \leq \left| b x - a \right|. \]

**Proof:** Consider the system of equations

\[ \begin{align*}
px + q_n z &= a \\
q_n y + q_n z &= b.
\end{align*} \]

The determinant of this system is \( p q_n - p_n q_n = (-1)^n a \).

It has a unique integer solution. In particular,

\[ \begin{align*}
y &= (-1)^n (a q_n - b p_n) \\
z &= (-1)^n (b p_n - a q_n).
\end{align*} \]

**Claim:** \( y \geq 0 \).

**Proof:**

\( y = 0 \), then \( a q_n = b p_n \). However, \( \gcd(p_n, q_n) = 1 \)

\[ \Rightarrow b | q_n. \text{ But we assume } b \nmid q_n. \# \]

\( y = 0 \), then \( \text{we have } b \nmid q_n \). \( \text{Thus, } p_n = b q_n \).

And

\[ \left| b x - a \right| = \left| q_n y - px \right| = \left| q_n y - px \right| \]

\[ \leq 1y \leq 1q_n x - p_n > 1q_n x - p_n \]

Thus, \( y \geq 0 \). Then, \( y > 0 \) the result is true.

We may assume \( z \leq 0 \).
Where for example we have

\[ |\pi - c_1| < \frac{1}{49} \]

\[ |\pi - c_2| < \frac{1}{11230} \]

\[ |\pi - c_3| < \frac{1}{10769} \]

\[ |\pi - c_4| < \frac{1}{10956246} \]

Our previous theorem tells us for instance that we cannot

find a rational number with denominator less than 106 close

\[ \pi \approx \frac{333}{106} \]

It would be nice if whenever one had \( |x - \frac{a}{b}| < \frac{1}{b^3} \) then

\( \frac{a}{b} \) must be a convergent of \( x \). This isn't quite true. What we do have

in the following theorem.

**Theorem:** Let \( x \in \mathbb{R} \). Let \( x = \frac{a}{b} \), \( a, b \in \mathbb{Z}, b > 0 \). If

\[ |x - \frac{a}{b}| < \frac{1}{2b^3} \]

then \( \frac{a}{b} \) is one of the convergents \( \frac{p_n}{q_n} \). 
Proof: Suppose \( \frac{a}{b} \) is not a convergent. Since the \( q_n \) are increasing integers, \( q_n \leq b < q_{n+1} \). We have

\[
1 q_n x - p_n | x - p_n \leq b | x - \frac{p_n}{q_n} | < b \left( \frac{1}{q_n} \right) = \frac{1}{2 b q_n}.
\]

Thus,

\[
| x - \frac{p_n}{q_n} | < \frac{1}{2 b q_n}.
\]

Since \( \frac{a}{b} = \frac{p_n}{q_n} \), we have \( a q_n - b p_n = 0 \) and \( \delta = 2 \).

\[
| x - \frac{p_n}{q_n} | < \frac{1}{b q_n}.
\]

Using the inequality,

\[
\frac{1}{b q_n} < \left| \frac{b q_n - a q_n}{b q_n} \right| = \left| \frac{p_n}{q_n} - \frac{a}{b} \right| \leq \left| \frac{p_n}{q_n} - x \right| + \left| x - \frac{a}{b} \right| < \frac{1}{2 b q_n} + \frac{1}{2 b^2}.
\]

Thus,

\[
2 b < q_n, \quad b < q_{n+1}.
\]
Our remaining goal will be to find continued fractions for the linear solutions to Pell's equation.

\[ x^2 - dy^2 = 1. \]

Before we can do this, we need to spend a bit of time on periodic continued fractions. Recall a *periodic* continued fraction is periodic if \( F_m \) satisfies

\[ [a_0, a_1, \ldots] = [a_m, a_{m-1}, \ldots] \]

where the overline represents the fact that the \( b_m, \ldots \) repeat forever.

We have seen for example that \( \sqrt{2} = [1; 2] \). It turns out that *finite* numbers of the form \( a + b\sqrt{d} \) are \( a, b, d \in \mathbb{Z} \) and all have periodic continued fractions. If a continued fraction is periodic then it must represent a number of this form.

**Def:** Let \( x \in \mathbb{R} \). We say \( x \) is a *quadratic irrational* number if \( x = a + b\sqrt{d} \).

**Thm:** Any periodic simple continued fraction is a quadratic irrational number, and vice versa.
Proof: Let \( x = [a_0, a_1, \ldots, a_n, \ldots, b_n] \) and 
\[ y = [b_0, \ldots, b_n]. \]

Note that 
\[ y = [b_0, \ldots, b_n, y] = \frac{y P_n + P_{n-1}}{y q_n + q_{n-1}}. \]

As 
\[ y = \frac{y P_n + P_{n-1}}{y q_n + q_{n-1}}, \]
we have 
\[ \frac{y P_n + P_{n-1}}{y q_n + q_{n-1}}. \]

By clearing the denominators, we obtain a quadratic equation in \( y \). Thus, we must have that either \( y \) is a quadratic irrational number or a rational number. However, we know an infinite continued fraction cannot be rational so we must have that \( y \) is a quadratic irrational number.

We have 
\[ x = [a_0, a_1, \ldots, a_n, y] = \frac{P_{n+1}}{q_{n+1}} = \frac{y P_n + P_{n-1}}{y q_n + q_{n-1}}, \]
where we use \( \frac{P_i}{q_i} \) to denote the convergent of \( x \). We know \( x \notin \mathbb{Q} \) because it is an infinite continued fraction. We showed above that \( y \) is a quadratic irrational, i.e., \( \in \mathbb{Q}, b_0, c, d \in \mathbb{Z}, dc > 0 \).  

Let 
\[ y = \frac{c}{b} + \sqrt{d}. \]

Plugging this in and clearing the denominators by multiplying by the conjugate shows \( x \) is a quadratic irrational as well. This proves one direction of the theorem. The "easy" direction.
We now wish to show that if we have a quadratic irrational then its continued fraction is periodic. To do this, we need to have a reasonable way to compute the continued fraction of $\sqrt{D}$.

First, observe that we can write any quadratic irrational in the form $x = \frac{a + \sqrt{D}}{b}$. (For example, if $x = \frac{a}{b} + \frac{c}{d} \sqrt{D}$, then $x = \frac{ad + c(b^2)}{bd}$.) Note that $D$ cannot be a perfect square since $x \neq \infty$. Multiplying the top and bottom by $b$ we have

$$x = \frac{ab + \sqrt{b^2D}}{b^2}.$$

This shows we can write

$$x = \frac{m_0 + \sqrt{D}}{\mathcal{B}_0 b},$$

where $\mathcal{B}_0 = D - m_0^2$, $D$, $b$, $m_0$ are integers, $\mathcal{B}_0 \neq 0$ and $D$ is not a perfect square. We put it in this form so we can easily compute the continued fraction expansion.

Recall that when we showed $x = a + \sqrt{D}$ had a continued fraction expansion, we used that we could define

$$a_i = \lfloor x \rfloor,$$

$$x_{i+1} = \frac{1}{x_i - a_i} \quad x_0 = x.$$
and defined the way we had \( x = [a_0 : a_1 : \ldots : 1] \). We now show that if we set \( x_0 = x \), \( x_i = \frac{m_i + \sqrt{D}}{q_i b_i} \),

\[ a_i = L x_i \], \( m_i = a_i q_i - m_i \), \( q_i = \frac{D - m_i^2}{q_i b_i} \),

they also satisfy the above equations, and so give the continued fraction expansion of \( x \).

Let \( a_0 = L x_0 \). We define the sequence \( x_i, a_i, m_i, q_i \) as above.

**Claim 1:** \( m_i, q_i \in \mathbb{Z}, q_i \neq 0 \) and \( |q_i| \leq |D - m_i^2| \).

**Proof:** We use induction on \( i \). The case \( i = 0 \) was handled above.

Assume the statement for \( i = n \). Then

\[ m_{n+1} = a_n q_n - m_n \in \mathbb{Z} \]

by induction hypothesis.

\[ q_{n+1} = \frac{D - m_{n+1}^2}{q_n b_n} = \frac{D - m_n^2 + 2a_n m_n - a_n^2 q_n b_n}{q_n b_n} \]

by own induction hypothesis and so \( q_{n+1} \in (D - m_n^2) \). Then

We have that \( q_{n+1} \neq 0 \) for otherwise we would have

\( D = m_n^2 \), but \( D \) is not a perfect square. Finally,

\[ b_{n+1} = \frac{D - m_{n+1}^2}{q_{n+1}} \] and \( b_{n+1} \in \mathbb{Z} \), as \( q_{n+1} \mid (D - m_n^2) \)
Claim 3: \[ x_{in} = \frac{1}{x_c - a_c} \]

**Proof.** Noting the equivalence to solving \( x_c - a_c = \frac{1}{x_{in}} \),

\[
x_c - a_c = \frac{m_i + \sqrt{D}}{b_i \Phi_i} - a_c
\]

\[
= \frac{m_i + \sqrt{D} - a_i b_i}{\Phi_i b_i}
\]

\[
= \frac{\sqrt{D} - m_{in}}{\Phi_i b_i}
\]

\[
= \frac{\Phi_i \sqrt{D} - m_{in}^2}{b_i \Phi_i \left( \sqrt{D} + m_{in} \right)}
\]

\[
= \frac{\Phi_i \text{tan} b_{in}}{\sqrt{D} + m_{in}}
\]

\[
= \frac{1}{x_{in}}
\]

as desired. \( \square \)

As we have shown that \( x = [a_0, a_1, \ldots] \). Of course, the goal is to show this continued fraction is periodic as...
we shall have a lot to work to do!

Write \( \bar{x}_0 = \frac{m_2 - \sqrt{D}}{g_{12} b_1} \).

Now recall that when expanding \( x \) in a continued fraction, we have

\[
x = [a_0, a_1, \ldots, a_n, x_0]
\]

\[
= \frac{x_0 P_{n-1} + P_{n-2}}{x_0 q_{n-1} + q_{n-2}}.
\]

Taking the conjugate of each side yields:

\[
\bar{x} = \frac{\bar{x}_0 P_{n-1} + \bar{P}_{n-2}}{\bar{x}_0 q_{n-1} + \bar{q}_{n-2}}
\]

(Exercise: \( x_0 P_{n-1} + q_{n-2} \) and \( \bar{x}_0 q_{n-1} + \bar{q}_{n-2} \) are equal and \( \bar{a}_0 = \frac{\bar{a}_0}{b_0} \).)

Solving the above equation for \( \bar{x}_0 \) we have

\[
\bar{x}_0 = \frac{-q_{n-2}}{q_{n-1}} \left( \frac{\bar{x} - P_{n-2} \bar{q}_{n-2}}{\bar{x} - P_{n-1} \bar{q}_{n-1}} \right).
\]

As \( n \to \infty \), \( P_{n-2} \bar{q}_{n-2} \) and \( P_{n-1} \bar{q}_{n-1} \) both converge to \( x \),

which is not equal to \( \bar{x} \) since \( \sqrt{b} \) \( \neq \bar{x} \).

As \( n \to \infty \),

\[
\left( \frac{\bar{x} - P_{n-2} \bar{q}_{n-2}}{\bar{x} - P_{n-1} \bar{q}_{n-1}} \right) \to 1.
\]
Thus, for large enough $n$ we have 

$$ \left( \frac{\frac{x}{\sqrt{n}} - \mu_{n-1}}{x - \mu_{n-1}} \right)^n > 0 $$

and so $\bar{x}_n < 0$. Thus for $n > N$ we have $\bar{x}_n < 0$. We know that $x_n > 0$ for $n > 1$. (Note: a positive integer)

And so for $n > N$ we have $x_n - \bar{x}_n > 0$. Thus,

Using that $x_n = \frac{m_n + \sqrt{b}}{b_n}$ we have

$$ \frac{m_n + \sqrt{b}}{b_n} b_n = \frac{m_n - \sqrt{b}}{b_n} b_n > 0 $$

i.e.

$$ \frac{2 \sqrt{b}}{b_n} > 0 \quad \text{for } n > N. $$

Thus, $b_n > 0$ for $n > N$. 

We also have since $b_{mm} = \frac{D - m_m^2}{b_n}$

that

$$ b_n b_{mm} = D - m_{mm}^2 \leq D $$

$$ b_n \leq b_n b_{mm} \leq D $$

and

$$ m_{nn}^2 < m_{nn}^2 + b_n b_{mm} < \frac{D}{b_n} $$ (since $b_n > 0$ for $n > N$)
\[ \Rightarrow \text{for } n > N, \quad |m_{n+1}| < \sqrt{D}. \]

We know \( D \) is a fixed positive integer, and so for \( n > N \) we know that \( q_b \) and \( m_{n+1} \) can only take on finitely many values. Thus, for \( n > N \), the pairs \((m_n, b_n)\) can only take on finitely many values. Hence, for distinct integers \( j, k \) we have \((m_j, b_j) = (m_k, b_k)\), where \( j < k \).

Thus,
\[
X_j = \frac{m_j + \sqrt{D}}{q_j} = \frac{m_k + \sqrt{D}}{q_k} = X_k.
\]

Thus,
\[
x = [a_0; \overline{a_j, a_{j+1}, \ldots, a_{j+n-1}, a_k}].
\]

Because \( a_j = [X_j] = [X_k] = a_k \), and
\[
m_{k+n} = a_k b_k - m_k
\]
\[
= a_j b_j - m_j
\]
\[
= m_{j+n}
\]

\[
b_{k+n} = \frac{D - m_k^2}{b_k} = \frac{D - m_j^2}{b_j}
\]
\[
= b_{j+n}.
\]
In fact, one can actually show that if $\sqrt{D} \notin \mathbb{Q}$, then

$$\sqrt{D} = \left[ a_0; \overline{a_1, a_2, \ldots, a_n, a_0} \right].$$

We will not need this, however, and so will not spend time proving it.

We now return to Pell's equation

$$x^2 - Dy^2 = 1.$$ 

We can immediately remove several cases:

**D = -1:** Then $x^2 - Dy^2 \geq 0$ unless $x = y = 0$. The only solution in this case is $(\pm 1, 0)$.

**D = -1:** We are looking at $x^2 - y^2 = 1$, so we have the solutions $(\pm 1, 0), (0, \pm 1)$.

**D = 0:** We are looking at $x^2 = 1$, so $(\pm 1, y)$ is a solution for any $y$. Not very interesting, always as big as even appear in the equation now.

Suppose $D$ is a perfect square, $D = N^2$. Then we can write the equation
$x^2 - Dy^2 = 1$

$(x + N_y)(x - Ny) = 1$

Since we are only interested in integral $x, y$, this gives

$x - N_y = \pm 1, \quad x - Ny = \pm 1$; and must be equal

Thus,

$x = \frac{(x + N_y) + (x - N_y)}{2} = \pm 1$

So in this case, the only solutions are $(\pm 1, 0)$.

We now get to the interesting part of the problem, namely when $D$ is a positive integer that is not a square.

**Theorem:** Let $(p, q)$ be a positive solution of $x^2 - Dy^2 = 1$. Then $pq$ is a convergent of the continued fraction expansion of $\sqrt{D}$.

Before we prove the theorem we note that if $(x_0, y_0)$ is a solution,

$x \sim (x_0, \pm y_0), \quad (x_0, \mp y_0)$. Thus we can always obtain all of the solutions by studying only those for $x_0, y_0 > 0$.

**Proof:** Since $(p, q)$ is a solution, we have
\[(*) \quad (p - \sqrt{b})(p + \sqrt{b}) = 1.\]

Thus, we must have \(p > q\sqrt{b}\). Otherwise, actually, the full answer from \(p^2 - 4q^3 = 1\), and \(D = 2q\).

The equation (*) gives

\[
\frac{p}{q} - \sqrt{b} = \frac{1}{2(p + \sqrt{b}q)}.
\]

Thus,

\[
0 < \frac{p}{q} - \sqrt{b} < \frac{\sqrt{b}}{2(p + \sqrt{b}q)} \quad \frac{\sqrt{b}}{2(q^2 + \sqrt{b})} = \frac{\sqrt{b}}{2q^2} = \frac{1}{2b}.
\]

Thus, we have before that \(q\left| \frac{p}{b} - 1 \right| < \frac{1}{2b} \Rightarrow p \sim q\),

a convergent \(q \sim \sqrt{b}\) implies \(q \sim q\sqrt{b} \sim \sqrt{b}\). \(\Box\)

Be careful with this theorem! It says if we have a solution then it is a convergent. It does NOT say if we have a convergent then it provides a solution! We do have a partial result in this classical manner.
Theorem: Let \( p/q \) be a convergent of the continued fraction expansion of \( \sqrt{5} \).

Then: \( (p,q) \) is a solution of one of the equations

\[
x^2 - Dy^2 = k
\]

for \( |k| < 1 + 2\sqrt{5} \).

Proof: Let \( p/q \) be a convergent of \( \sqrt{5} \). Then we know

\[
\left| \frac{p}{q} - \sqrt{5} \right| < \frac{1}{q^2}.
\]

i.e.,

\[
|p - q\sqrt{5}| < \frac{1}{q}.
\]

Thus,

\[
\left| p + q\sqrt{5} \right| = \left| p - q\sqrt{5} + 2q\sqrt{5} \right|
\]

\[
< \left| p - q\sqrt{5} \right| + 2q\sqrt{5}
\]

\[
< \frac{1}{q} + 2q\sqrt{5}
\]

\[
< \sqrt{5} \left( 1 + 2\sqrt{5} \right) \quad \left( \frac{1}{2} \leq q \right).
\]

Combining the two cases

\[
|p - q\sqrt{5}| < \frac{1}{q}
\]

and

\[
|p + q\sqrt{5}| < \sqrt{5} \left( 1 + 2\sqrt{5} \right)
\]

gives

\[
|p^2 - 5q^2| < 1 + 2\sqrt{5}
\]

as desired.
Example: We have that \( \mathbf{d} = [ 5, 2, 1, 0, 0, 0 ] \). The first few convergents are:

\[
\begin{align*}
C_1 &= \frac{11}{2} \\
C_2 &= \frac{16}{3} \\
C_3 &= \frac{37}{5} \\
C_4 &= \frac{70}{13} \\
C_9 &= \frac{9801}{1820} \\
C_{19} &= \frac{192119201}{352735270}
\end{align*}
\]

Then we have \( q_n^2 - 29 q_n^2 = : \)

1: 24 5
2: -5
3: 4

9: 1
Then, the first two solutions of \( x^2 - 2y^2 = 1 \) we encounter are \((9, 4), (13, 6)\) and \((192119201, 35675670)\).

We have shown if \( x^2 - 2y^2 = 1 \) has a solution, then this solution must be a convergent of \( \sqrt{2} \). Of course, we still need to show that these actually are solutions! The result we proved before that the continued fraction of \( \sqrt{2} \) is periodic will be essential.

Recall that when proving \( \sqrt{2} \) has a periodic continued fraction, we defined \( a_i \) and \( b_i \) so that:

\[
M_0 = 0, \quad b_0 = 1
\]

\[
m_i+1 = a_i b_i - m_i, \quad b_{i+1} = \frac{D - m_i^2}{b_i}
\]

with \( a_i, b_i \in \mathbb{Z} \), \( b_i > 0 \), \( b_{i+1} | (D - m_i^2) \), and \( x_i = \frac{m_i + \sqrt{2}}{b_i} \)

for \( i \geq 0 \).

**Theorem:** Let \( \frac{p_i}{q_i} \) be convergents of the continued fraction expansion of \( \sqrt{2} \). Then

\[
p_i^2 - 2q_i^2 = (-1)^{k+1} b_{k+n}
\]

when \( b_{k+n} > 0 \) for \( t = 0, 1, \ldots \).
\[ \sqrt{D} = [a_n, a_{n-1}, \ldots, a_2, a_1, x_{n+1}] \]

Then we have

\[ \sqrt{D} = \frac{x_{n+1} P_n + P_{n-1}}{x_{n+1} Q_n + Q_{n-1}} \]

We know we can write \( x_{n+1} = \frac{M_n + \sqrt{D}}{b_{n+1}} \), so we substitute this in:

\[ \sqrt{D} = \frac{\frac{M_n + \sqrt{D}}{b_{n+1}} P_n + P_{n-1}}{\frac{M_n + \sqrt{D}}{b_{n+1}} Q_n + Q_{n-1}} \]

\[ = \frac{(M_n + \sqrt{D}) P_n + b_{n+1} P_{n-1}}{(M_n + \sqrt{D}) Q_n + b_{n+1} Q_{n-1}} \]

Thus,

\[ \sqrt{D} \left( M_n Q_n + b_{n+1} Q_{n-1} - P_n \right) = M_n P_n + b_{n+1} P_{n-1} - D Q_n \]

However, the LHS \( e \leq a \) and \( \sqrt{D} \leq a \) so we must have

\[ M_n Q_n + b_{n+1} Q_{n-1} = P_n \quad \text{(1)} \]

and

\[ M_n P_n + b_{n+1} P_{n-1} = D Q_n \quad \text{(2)} \]

Multiply (1) by \( \frac{P_n}{\sqrt{D}} \) and the \( -2 \) by \(-9_n \) and add them together to get:
\[ P_n^2 - D_n^2 = b_{kn} \left( P_{n-1} Q_{n-1} - P_n Q_n \right) \]
\[ = (-1)^{n-1} b_{kn} \]

as desired. It only remains to show \( b_{kn} > 0 \). We showed this before for large enough \( n \). We know that

\[ C_{kn} < \sqrt{D} < C_{2kn} \quad k \geq 0. \]

Thus,
\[ \frac{P_n}{b_{kn}} < \sqrt{D} \quad \Rightarrow \quad P_n < \sqrt{D} b_{kn} \]

\[ \Rightarrow \quad P_{kn}^2 - D_{kn}^2 < 0. \]

Similarly, we have

\[ P_{kn}^2 - D_{kn}^2 > 0. \]

Thus,
\[ \frac{P_{kn}^2 - D_{kn}^2}{P_{kn}^2 - D_{kn}^2} = - \frac{b_{kn}}{b_{kn}} \quad k \geq 1. \]

And this is always negative since the interpretations of the LHS are opposite again. Thus, \( \frac{b_{kn}}{b_{kn}} > 0 \).

\[ b_1 = D - 9 > 0 \quad \Rightarrow \quad b_2 > 0 \quad \text{and induction} \]

Thus \( b_k > 0 \) for \( k \geq 1 \).
At this point we know any solution to \( X^2 - D_1 y^2 = 1 \) must be a convergent of \( \sqrt{D_1} \) and that the convergent satisfies

\[
P_k^2 - D_1 q_k^2 = (-1)^k b_{k+1}.
\]

Thus, for \((p_k, q_k)\) to have any chance of being a solution of Pell's equation we must have \( b_{k+1} = 1 \) (remember \( b_k > 0 \)).

Proof: Write \( \sqrt{D} = [a_0; a_1, a_2, \ldots, a_n] \). We know that for any \( k \) we have

\[
X_{k+1} = X_k.
\]

Then,

\[
\frac{m_{k+1} + \sqrt{D}}{b_{k+1}} = \frac{m_1 + \sqrt{D}}{b_1}.
\]

i.e.,

\[
\sqrt{D} (b_{k+1} - b_1) = m_{k+1} b_1 - m_1 b_1.
\]

Hence, \( \sqrt{D} \neq 0 \) we have \( b_{k+n} = b_1 \)

and \( m_{k+n} = m_1 \).

Then we have
\[ b_i = D - m_i^2 = D - 4m_{kn1}^2 = b_{kn1}b_{kn1} = b_{kn1}b_i \]
\[ b_i = b_{kn1} \]

Therefore, \( b_{kn1} = 1 \). Hence, we have \( b_K = 1 \) if \( n \not\equiv 0 \mod 4 \).

Now we need the other direction. Let \( k \) be a positive integer with \( b_k = 1 \). Then

\[ X_k = m_k + \sqrt{D} \]

\[ \Rightarrow \]
\[ L_{X_k} = L_{m_k + \sqrt{D}} \]
\[ = m_k + L_{\sqrt{D}} \]
\[ = m_k + a_o \]

Now

\[ X_{k+1} = \frac{1}{X_k - L_{X_k}} \]

\[ \Rightarrow \]
\[ X_k = L_{X_k} + \frac{1}{X_{k+1}} \]
\[ = m_k + a_o + \frac{1}{X_{k+1}} \]

We know that

\[ X_1 = \frac{1}{X_o - a_o} \Rightarrow a_o + \frac{1}{X_1} = X_o = \sqrt{D} \]
\[ = X_k - m_k \]
\[ = a_o + \frac{1}{X_{k+1}} \]
\[ X_i = x_{kn} \quad \text{But then the set} \quad \{a_1, \ldots, a_k\} \]

repeats in the expansion of \( \sqrt{D} \). \( \Rightarrow \) \( n | kn \).

\[ \text{Then: } \quad \text{Let} \quad P_k/Q_k \text{ be the convergent of the continued fraction expansion} \]
\[ \text{of} \quad \sqrt{D}. \text{ Let} \quad n \text{ be the length of the period.} \]

(i) \( \text{If} \ 2 | kn \), \( \text{then the positive solutions of} \ x^2 - Dy^2 = 1 \]
\[ \text{are given by} \quad X = P_{kn}, \quad Y = Q_{kn} \quad k = 1, 2, 3, \ldots \]

(ii) \( \text{If} \ 2 \nmid kn \), \( \text{then all positive solutions of} \ x^2 - Dy^2 = 1 \]
\[ \text{are given by} \quad X = P_{2kn}, \quad Y = Q_{2kn} \quad k = 1, 2, 3, \ldots \]

\[ \text{Proof: } \quad \text{We have basically already shown this. We know all solutions} \]
\[ \text{are convergents, and} \]
\[ P_k^2 - DQ_k^2 = (-1)^{kn} b_{kn} \]

\[ \text{we have} \ b_{kn} = 1 \text{ if} \ n | kn. \quad \text{As if} \ P_k, Q_k \text{ is a} \]
\[ \text{solution then} \ b_{kn} = 1 \text{ and} \ (-1)^{kn} = 1. \quad \text{As} \ kn \]
\[ \text{must be even and} \ n | kn. \quad \text{As} \ k = 1 \text{ we get} \]
\[ k = tn, \quad \text{and} \ 2 | kn. \quad \text{If} \ n \text{ is even, then} \]
\[ k = tn - 1 \]
And if \( n \) is odd, then \( t \) must be even so

\[ K = 25n - 1. \]

Example: Find a solution to \( x^2 - 31y^2 = 1. \)

\[ \sqrt{31} = [5; 1, 1, 3, 5, 3, 1, 1, 10] \]

So \( n = 8 \) in this ease. Since \( n \) is even, the

theorem says \( P_{n-1}/Q_{n-1} \) an solution for \( x+1, 0 \).

Thus, we need \( P_7, Q_7 \) for our first solution.

\[ C_7 = \frac{1520}{873}, \quad (1520, 873) \text{ is a solution} \]

\[ C_{15} = \frac{4620799}{829936}, \quad (4620799, 829936) \text{ is} \]

another solution.

The problem with this method is that one has to keep

computing convergents to get solutions. To get \( C_{15} \), we have to

compute \( C_8, \ldots, C_{14} \) first. This is not an ideal way to obtain

solutions. We would like to be able to use our first solution to

give us all other solutions.
**Def**: A solution \((x_0, y_0)\) of Pell's equation is a fundamental solution if given another positive solution \((x_1, y_1)\), then \(x_0 < x_1, y_0 < y_1\).

**Then**: Let \((x_0, y_0)\) be the fundamental solution of \(x^2 - dy^2 = 1\). Then every pair \((x_n, y_n)\) defined by

\[x_n + y_n \sqrt{d} = (x_0 + y_0 \sqrt{d})^n, \quad n = 1, 2, \ldots\]

is also a solution.

**Proof**: Observe that we have

\[x_n + y_n \sqrt{d} = (x_1 + y_1 \sqrt{d})^n = (x_0 + y_0 \sqrt{d})(x_{n-1} + y_{n-1} \sqrt{d})^n\]

\[= (x_0 + y_0 \sqrt{d})(x_{n-1} + y_{n-1} \sqrt{d}) = (x_1 x_{n-1} + y_1 y_{n-1}) + (x_1 y_{n-1} + x_{n-1} y_1) \sqrt{d}.\]

Thus,

\[x_n = x_1 x_{n-1} + y_1 y_{n-1}, \quad y_n = x_{n-1} y_1 + x_1 y_{n-1}.\]

**Claim**: \((x_1 - y_1 \sqrt{d})^n = x_n - y_n \sqrt{d}\).

**Pf**: Use induction on \(n, \ n = 1\) trivial. Assume the result for \(n - 1\). Then

\[(x_1 - y_1 \sqrt{d})^n = (x_1 - y_1 \sqrt{d})(x_1 - y_1 \sqrt{d})^{n-1}\]

\[= (x_1 - y_1 \sqrt{d})(x_{n-1} - y_{n-1} \sqrt{d}) = (x_1 x_{n-1} + y_1 y_{n-1}) + (x_1 y_{n-1} + x_{n-1} y_1) \sqrt{d}\]

\[= x_n - y_n \sqrt{d}, \quad \text{as desired.}\]
Define $x_n, y_n$ as both positive, it is clear $x_n$ and $y_n$ must be positive. We have:

\[ x_n^2 - D y_n^2 = (x_n + y_n \sqrt{5})(x_n - y_n \sqrt{5}) \]

\[ = (x_1 + y_1 \sqrt{5})^n (x_1 - y_1 \sqrt{5})^n \]

\[ = (x_1^2 - D y_1^2)^n \]

\[ = 1^n = 1 \]

**Example:** Recall that we found $(1520, 273)$ as a fundamental solution to $x^2 - 31y^2 = 1$. Then,

\[ (1520 + 273 \sqrt{31})^n \]

Applying this to give solutions $x_n, y_n$ as well:

- $n = 2 \quad x_2 = 4620799 \quad y_2 = 829920$
- $n = 3 \quad x_3 = 14047227440 \quad y_3 = 2522950527$

Finally, we checked this method yields all solutions.
Then: Let \((x, y)\) be a fundamental solution of \(x^2 - Dy^2 = 1\). Then every positive solution of the equation \(y^2 = \sqrt{D}\) is given by \(x_n, y_n\) where \(x_n, y_n\) are obtained by

\[x_n + y_n \sqrt{D} = (x_1 + y_1 \sqrt{D})^n, \quad n = 1, 2, \ldots\]

Proof: Suppose \(u, v\) that \(u, v\) is solution but not one of \(x, y\).

We know that \(x + y \sqrt{D} > 1\), so \(\lim_{n \to \infty} (x + y \sqrt{D})^n = \infty\) as we can find \(n \in \mathbb{Z}\) such that

\[(x + y \sqrt{D})^n < u + v \sqrt{D} < (x + y \sqrt{D})^{n+1}.

i.e.,

\[x_n + y_n \sqrt{D} < u + v \sqrt{D} < (x_n + y_n \sqrt{D})^n.

Multiply this by \(x_n - y_n \sqrt{D}\) (this is positive?!) and set

\[1 = x_n^2 - y_n^2 \sqrt{D} < (x_n - y_n \sqrt{D})(u + v \sqrt{D}) < x_n + y_n \sqrt{D}.

Let \(r = x_n u - Dy_n v\), \(s = x_n v - y_n u\), and then

\[(x_n - y_n \sqrt{D})(u + v \sqrt{D}) = r + s \sqrt{D}, \quad (x)

Then we have

\[r^2 - Ds^2 = (x_n u - Dy_n v)^2 - D(x_n v - y_n u)^2 = (x_n u)^2 - 2x_n u D v + D(y_n u)^2.

- \]
\[ (x^2 - Dy^2)(u^2 - Dv^2) = 1, \quad 1 = 1. \]

Then, \((r, s)\) is a solution to \(x^2 - Dy^2 = 1\) with

\[ 1 < r + s\sqrt{b} < x_1 + y_1\sqrt{b}. \]

If we can show \(r\) and \(s\) are both positive, we will have a contradiction.

Since \(1 < r + s\sqrt{b}\) and \((r + s\sqrt{b})(r - s\sqrt{b}) = r^2 - Ds^2 = 1\),
we must have \(r - s\sqrt{b} > 0\) and \(r + s\sqrt{b} < 1\).

Thus,

\[ 2r = (r + s\sqrt{b}) + (r - s\sqrt{b}) > 1 + 0 > 0. \]
\[ 2s\sqrt{b} = (r + s\sqrt{b}) - (r - s\sqrt{b}) > 1 - 1 = 0. \]

\[ = 2. \]  \# Thus it must be that all solutions arise from \((x_1, y_1, \sqrt{b})\).

Finally, consider the equation \(x^2 - Dy^2 = -1\). We saw before that

\[ P_k^2 - Dq_k^2 = (-1)^{k+1} b_{kn} \]

and \(b_{kn} = 1\) if \(n\) is odd and \(b_{kn} = 0\) if \(n\) is even. This allows us to conclude that if we want solutions to \(x^2 - Dy^2 = -1\), we should look at those \(k\) when \(k + 1\) is odd and \(n\) even.
So we can write \( K + 1 = n t \) for some \( t \).

As

Suppose \( n \) is even. Then \( K + 1 = \text{even} \). This can't yield any solutions.

Suppose \( n \) is odd. Then \( K + 1 = \text{odd} \) if \( t \) is also odd. No one solution.

Let \( t = \frac{1}{2} \).

n odd

\[
P_n(2en) - 1 \quad 9n(2en) - 1 \quad \text{for } t = 0, 1, 2, \ldots
\]
We have completely classified the integer solutions to the equation

\[ x^2 + y^2 = z^2 \]

when studying congruent numbers. The natural question is what about

\[ x^3 + y^3 = z^3 \]

or more generally

\[ x^n + y^n = z^n \]

for \( n > 2 \). Fermat asserted that he could prove that there were no solutions

\[ x,y,z \in \mathbb{Z} \text{ with } xy \neq 0. \]

This became known as Fermat's Last Theorem. It remained unproven until the 1990s when a proof was finally given by Andrew Wiles. This is a very difficult proof and actually uses elliptic curves! What we are going to do is prove the result for the rather easy cases of \( n = 3 \) and \( n = 4 \).

It turns out that \( n = 4 \) is much easier than \( n = 3 \) as we begin here. Fermat actually gave a proof in this case via his method of descent. What he actually proved is that an \( n \)-terminal integer solution to \( x^4 + y^4 = z^2 \), which immediately implies
The result since we can write

\[ x^n + y^n = z^n \]

\[ = (z^2)^2. \]

**Theorem:** The equation \( x^n + y^n = z^2 \) has no solution in positive integers.

**Proof:** Consider \( x, y, z \in \mathbb{Z}_{>0} \) s.t.

\[ x^n + y^n = z^2 \quad \text{(1)} \]

Let \( d = \gcd(x, y) \). Then \( d^n | x^n, y^n \Rightarrow d^n | z^2 \Rightarrow d^2 | z. \) Write \( x = x_1d, y = y_1d, z = zd. \) Then

\[ x_1^n + y_1^n = z_1^2. \]

And \( \gcd(x_1, y_1) = 1. \) This gives that \( x_1^n, y_1^n, z_1 \) is a primitive Pythagorean triple. Thus \( x_1, y_1, z_1 \in \mathbb{Z}_{>0} \).

\[ x_1^n = 2mn \]
\[ y_1^n = m^2 - n^2 \]
\[ z_1^n = m^2 + n^2. \]

Recall that we showed before that \( y_1 \) is necessarily odd. This implies that \( m \) and \( n \) are of opposite parity,
i.e., one is odd and one is even. We need to determine which is which. We have

\[ y_i^2 + n^2 = m^2 \]

is a primitive Pythagorean triple and \( y_i \) is odd, so we must have \( n \)
even and \( m \) odd.

Let \( u = m \) and \( v = 2n \). Since \( n \) is even, we can write \( n = 2n' \). We have that

\[ uv = x_i^2, \]

and \( \gcd(u, v) = 1 \). Thus we have that \( u \) and \( v \) must each

be a perfect square. (See p1x1. Then \( p^2 | uv \) and since \( \gcd(u, v) = 1 \),
p^2 \mid p^2 | u \). This splits the primes, denoting \( x_i^2 \) up ... continue this.\)

So \( u = a^2 \) and \( v = b^2 \). Thus, \( m = a^2 \)

and \( 2n = b^2 \) so \( 2ab^2 = kd_{1}b \). Thus, \( 2n = 4b^2 \)

\( = \alpha c^2 \), for \( 2c = b \). Now observe we have

\[ a^4 = m^2 = y_i^2 + n^2 \]

\[ = y_i^2 + 4c^4. \]

Thus, a solution of \( x^4 + y^4 = z^2 \) leads to a solution

(mentioned at the equation)

\[ a^4 = y^4 + 4c^4. \]
Moreover,

\[ a^4 = m^2 - m^2 + n^2 = Z_1 \leq Z. \]

Thus we obtain a solution of \((***)\) with \(a < Z\).

We will now show a solution of \((***)\) leads to a solution of \((**')\) with \(Z_2 < a\). This will give a contradiction as we will then have a strictly decreasing sequence of positive integers.

Let \((a, b, c)\) be such that \((\text{pos. int.})\)

\[ a^4 = b^2 + 4c^2. \quad (**') \]

Let \(e = \gcd(a, c)\). Then \(e^4 | b^2 \Rightarrow e^2 | b\). Conversely,

\[ a_1 = \frac{a}{e}, \quad b_1 = \frac{b}{e^2}, \quad c_1 = \frac{c}{e}. \]

We have that \(a_1, b_1, c_1\) satisfy \((**')\) with \(\gcd(a_1, c_1) = 1\). Thus, we have

\[
(a_1^2)^2 = b_1^2 + (2c_1)^2
\]

and so \(a_1^2, b_1, 2c_1^2\) are a primitive Pythagorean triple. So \(\exists m', n'\) s.t.

\[
2c_1^2 = \Delta m'n' \Rightarrow c_1^2 = m'n'.
\]

\[
b_1 = (m')^2 - (n')^2
\]

\[
a_1^2 = (m')^4 + (n')^2.
\]

Using this

\[
c_1^2 = m'n'.
\]
And thus $gcd(m', n') = 1$, we see that $m'$ and $n'$
must be perfect squares, i.e., $P_{m'}$ and $P_{n'}$.

\[ M = c \cdot x_2^2 \]
\[ n' = c \cdot y_2^2. \]

Let $Z_2 = a_1$, we have

\[ x_1^4 + y_1^4 = (m')^2 - (n')^2 = a_1^2 = Z_2^2. \]

And so $(x_2^4, y_2^4, Z_2)$ is a positive solution to $(4)$.

Moreover, $Z_2 = a_1 \leq a$.

Hence $Z_2 < Z_1$. We can now apply the same process

1. $Z_2$ to get $Z_3$ by

\[ Z_3 < Z_2 < Z_1. \]

This process can be repeated forever. However, there are

positive integers $m', n'$. Then there can be no solution to

(3) to begin with.

Though the proof of this theorem were tedious, it did

not really require anything more than prime numbers, Pythagorean.
Def: A complex number \( \xi \) is an algebraic integer (w.r.t. \( \mathbb{Z} \)) if \( \exists \) a polynomial \( f(x) \) with integer coefficients such that
\[
f(\xi) = a_0 \cdot \xi^n + a_1 \cdot \xi^{n-1} + \ldots + a_n = 0
\]
with \( a_i \in \mathbb{Z} \).

Example: 1) \( \sqrt{2} \) is an algebraic integer,
\[f(x) = x^2 - 2\]
satisfies \( f(\sqrt{2}) = 0 \).

2) \( i \) is an algebraic integer,
\[f(x) = x^2 + 1\]
satisfies \( f(i) = 0 \).

3) \( \sqrt[n]{a} \) is an algebraic integer,
\[f(x) = x^n - a\]
satisfies \( f(\sqrt[n]{a}) = 0 \).

The reason they are called algebraic integers is they generalize the notion of integers to larger sets. (fields)
Thm: All integers are algebraic integers. The only algebraic integers in $\mathbb{Q}$ are those elements in $\mathbb{Z}$.

Proof: Let $m \in \mathbb{Z}$. Then, clearly $m$ is an algebraic integer as $f(x) = x - m$ has integer coefficients and satisfies $f(m) = 0$.

Now suppose $\frac{b}{c} \in \mathbb{Q}$ is an algebraic integer. Then $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathbb{Z}$, $n \in \mathbb{N}$, $b/c \neq \mathbb{Z}$, and $n$ can be different for different algebraic integers (of course!) until $f(b/c) = 0$. We may assume $\frac{b}{c} = \frac{a}{b}$ is in lowest terms so that $gcd(b,c) = 1$. Then

$$\left(\frac{b}{c}\right)^n + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + \cdots + a_1\left(\frac{b}{c}\right) + a_0 = 0.$$ 

Multiply both sides by $b^n$:

$$b^n + a_{n-1}c b^{n-1} + \cdots + a_1 c^n b + c^n a_0 = 0.$$ 

Thus $b^n = c \left(-a_{n-1}b^{n-1} - \cdots - a_1 c^n b + c^n a_0 \right)$, and

$$c | b^n \Rightarrow c = \pm 1.$$ 

So, $\frac{b}{c} \in \mathbb{Z}$.

In general, given a set $K \subseteq \mathbb{C}$ we write $\mathbb{Q}_K$ for the set of all algebraic integers in $K$. (Normed we take $K$ to be a finite field of $\mathbb{Q}$ and then $\mathbb{Q}_K$ is a ring!)

Thus $\mathbb{Q}_\mathbb{Z} = \mathbb{Z}$. 

We will mainly be interested in the set
\[ K = \mathbb{Q} (\sqrt{m}) = \left\{ a + b \sqrt{m} : a, b \in \mathbb{Q} \right\} \]
for \( m \in \mathbb{Z} \).

**Def.:** The **minimal polynomial** of an algebraic integer \( \alpha \) is the polynomial \( g(x) \in \mathbb{Q}[x] \) of smaller degree so that \( g(\alpha) = 0 \).

**Thm.:** The minimal polynomial of an algebraic integer is monic with integer coefficients.

This theorem is not difficult to prove, but would require us to talk about polynomials, more which we don't really have time to do.

**Def.:** Let \( \alpha \in \mathbb{Q}(\sqrt{m}) \) \( \alpha = a + b \sqrt{m}, \ a, b \in \mathbb{Q} \). We define the **norm** \( N \) of \( \alpha \) by
\[ N(\alpha) = \overline{\alpha} \overline{\alpha} \]
where \( \overline{\alpha} = a - b \sqrt{m} \) is the **conjugate** of \( \alpha \). (\( \sqrt{m} \notin \mathbb{Q} \) here!)

**Note:** \( N(\alpha) = a^2 - b^2 m \).
Let $\alpha$ and $\beta$ be algebraic integers. We say $\alpha \parallel \beta$ if the \textit{unit} $\gamma$, $\gamma = x + y\sqrt{5}$, $x, y \in \mathbb{Z}$, satisfies $\gamma \alpha = \beta$.

Theorem: \begin{enumerate}
    \item $N(\alpha \beta) = N(\alpha) N(\beta)$
    \item $N(\alpha) = 0 \iff \alpha = 0$
    \item If $\alpha$ is an algebraic integer, then $N(\alpha) \in \mathbb{Z}$.
    \item If $\alpha$ is an algebraic integer, then $N(\alpha) = 1 \iff \alpha \in \mathbb{Z}$ or $\alpha$ is a unit.
\end{enumerate}

Proof: \begin{enumerate}
    \item Exercise. This is just a calculation, compare each side.
    \item If $\alpha = 0$, it is clear $N(\alpha) = 0$. Now suppose $N(\alpha) = 0$,
    \begin{align*}
        \text{i.e.,} \quad \alpha = a + b\sqrt{5}, \quad \text{then} \quad a^2 - 5b^2 = 0.
    \end{align*}
    \begin{align*}
        \text{If } b \neq 0, \text{ then } \quad m = (\frac{a}{b})^2 = \frac{a^2}{5b^2} = \frac{a^2}{5} \in \mathbb{Z} \iff b = 0 \iff a = 0.
    \end{align*}
    \item Let $f(x)$ be the minimal polynomial of $\alpha$. If $\deg f(x) = 1$, then $f(x) = x - \alpha \Rightarrow x - \alpha \in \mathbb{Z} \iff N(\alpha) = 1 \in \mathbb{Z}$.
    Suppose $\deg f(x) > 1$ in the $\mathbb{Q}$ is $\mathbb{Z}$. Then we have
    \begin{align*}
        \alpha = a + b\sqrt{5} \Rightarrow \quad x^2 - \alpha^2 x + (a^2 - 5b^2) = 0 \quad \text{when } x = \alpha
    \end{align*}
    \begin{align*}
    \begin{align*}
        \text{Assume the } \deg f(x) = 1 \text{ and } \deg \text{ of } f(x) = 1, \text{ we must have this for } 1 \text{ for } f(x). \text{ Our earlier theorem said this has integer coefficients}, \text{ in } \mathbb{Z}. \text{ It is } N(\alpha) \in \mathbb{Z}.
    \end{align*}
    \end{align*}
    \item Suppose $N(\alpha) = \pm 1$. Then $\alpha \bar{\alpha} = 1 \Rightarrow \alpha \bar{\alpha} = 1$ is a unit.
    \begin{align*}
    \begin{align*}
        \text{hence } \alpha \bar{\alpha} = \pm 1 \Rightarrow \alpha \bar{\alpha} = 1 \in \mathbb{Z}.
    \end{align*}
    \end{align*}
    \item Suppose $\alpha \bar{\alpha} = \pm 1$. Then $\bar{\alpha} \in \mathbb{Z}$, hence $\alpha \bar{\alpha} = 1$.
\[ N(x)N(y) = N(xy) = \pm 1. \] Thus, \( N(x) \equiv 1 \mod{2} \) and since \( N(z) \in \mathbb{Z} \), we must have \( N(x) = \pm 1 \).

**Theorem:** Let \( K = \mathbb{Q}(\sqrt{-3}) \). Then

\[ \mathcal{O}_K = \mathbb{Z}\left\{ \frac{1 + \sqrt{-3}}{2} \right\} = \{a + b\left(\frac{1 + \sqrt{-3}}{2}\right) : a + b \in \mathbb{Z}\}. \]

**Proof:** A statement similar to this is true in general, but we are only interested in \( \mathbb{Q}(\sqrt{-3}) \) so we stick to that case.

First we show elements of the form \( a + b\left(\frac{1 + \sqrt{-3}}{2}\right) \) are actually algebraic. Let \( \alpha = a + b\left(\frac{1 + \sqrt{-3}}{2}\right) \). Observe that \( \overline{\alpha} = a + b\left(\frac{1 - \sqrt{-3}}{2}\right) \) and then we have

\[ f(\alpha) = 0 \]

for \( f(x) = x^2 - \overline{\alpha} \overline{a + b} x + a \overline{\alpha} \). Our goal is to show \( \alpha + \overline{\alpha} \) and \( a \overline{\alpha} \) are integers.

\[ \alpha + \overline{\alpha} = 2a + b + \mathbb{Z} \]

\[ a \overline{\alpha} = (a + b) \frac{1}{2} - 3b^2 \frac{1}{4} \]

\[ = a^2 + b + b^2 \cdot \mathbb{Z}. \]

Thus, \( \alpha + \overline{\alpha} \) is the sum of a monic poly of integer coefficients on \( \mathbb{Z} \), so \( \alpha \) is algebraic, integer. Now we must show these are all algebraic integers.
algebraic integers.

Let \( a = \frac{a_1 + b\sqrt{-3}}{2c} \in \mathbb{Q}(\sqrt{-3}) \) with \( \gcd(a, b, c) = 1 \). We can write any element in this form. (exercise.) Suppose \( \alpha \) is an algebraic integer. Then we must have

\[
f(\alpha) = x^2 - (a+\bar{a})x + \alpha \bar{\alpha}\]

her coefficients in \( \mathbb{Z} \) are \( f(\alpha) = 0 \) and the poly of lower degree has \( \alpha = \bar{\alpha} \) zero. So our algebraic integers have \( \alpha \) has coefficients in \( \mathbb{Z} \). Thus, \( \alpha + \bar{\alpha} = \frac{2a}{c} \in \mathbb{Z} \) and \( c \mid a^2 + 3b^2 \) since

\[
\frac{a^2 + 3b^2}{c^2} = \alpha \bar{\alpha}. \]

If \( c = 1 \), then we have \( \alpha = a + b\sqrt{-3} \)

which we can write as \( (a-b) + 2b\left(\frac{1 + \sqrt{3}}{2}\right) \in \mathbb{Z}\left[\frac{1 + \sqrt{3}}{2}\right] \).

Suppose now that \( c > 1 \).

If \( c > 1 \), then \( \alpha + \bar{\alpha} = \frac{2a}{c} \in \mathbb{Z} \)

so \( c \mid 2a \). Let \( p \) be a prime in \( \mathbb{P} \) and \( p \mid a \). Then we have \( c^2 \mid a^2 + 3b^2 \) to get \( n \in \mathbb{Z} \) so \( nc^2 = a^2 + 3b^2 \).

But then \( p^2 \mid 3b^2 \Rightarrow p 
\# \) since \( \gcd(1, b, c) = 1 \).

So we must have \( c = 2 \). Thus, \( a^2 + 3b^2 \equiv 0 \pmod{4} \)

\( \Rightarrow a \) and \( b \) are both odd or even. They can't both be even because then \( \gcd(a, b, c) \neq 1 \).

Thus, \( a + b\sqrt{-3} = \frac{a-b}{2} + b\left(\frac{1 + \sqrt{3}}{2}\right) \in \mathbb{Z}\left[\frac{1 + \sqrt{3}}{2}\right] \).
Theorem: The units in $\mathbb{Q}(\sqrt{-3})$ are exactly the elements
\[ \pm 1, \quad \frac{1 \pm \sqrt{3}}{2}, \quad -1 \pm \sqrt{3}. \]

Proof: We need to determine the algebraic integers that can have norm $\pm 1$. First, observe that for $a + b \sqrt{-3}$ with $a, b \in \mathbb{Z}$,
\[ N(a + b\sqrt{-3}) = a^2 + 3b^2 \geq 0. \]
As we can never have norm $-1$ in this case, we only have norms $1$ when $a = \pm 1, b = 0$. So $\pm 1$ are units.

Consider now $\frac{a + b\sqrt{3}}{2} \in \mathbb{Z}(1 + \sqrt{3})$ with $a, b, c$ odd. Then
\[ N\left(\frac{a + b\sqrt{3}}{2}\right) = \frac{a^2 + 3b^2}{4} = \pm 1. \]
Again, the only possible cases are equal to $0$, so we really want to study
\[ \frac{a^2 + 3b^2}{4} = 1. \]

i.e.,
\[ a^2 + 3b^2 = 4. \]
However, we need $a$ and $b$ odd. If $b > 1$, then $3b^2 > 9$. So $b = \pm 1$. This forces $a = \pm 1$ as well.

This gives the result.
Def: Let \( \mathbb{Q}(\sqrt{m}) \) be an algebraic integer that is not a unit.

We say \( \alpha \) is prime if it is divisible only by units and unit times \( \alpha \).

**Warning:** The notion of prime you are used to, with one caveat. Here we allow negative \( \alpha \). If \( \alpha \) is prime, then \(-\alpha \) is as well! This is forced on us because there is not a well-defined ordering for \( \mathbb{Q}(\sqrt{-m}) \), such as \( \mathbb{Q}(\sqrt{-3}) \).

**Thm:** Let \( \alpha \in \mathbb{Q}(\sqrt{m}) \) and suppose \( N(\alpha) = \pm 1 \) when \( \alpha \) is a prime.

Then \( \alpha \) is necessarily prime.

**Proof:** Suppose \( \alpha = \beta \gamma \). Then \( N(\beta)N(\gamma) = \pm 1 \) \( \Rightarrow \) \( \pm \beta \gamma \in \mathbb{Z} \). But this implies \( \beta \gamma \in \mathbb{Z} \). Either way, one of them is \( \pm 1 \) and so \( \beta \gamma \) is a unit. \( \square \)

**Thm:** Every algebraic integer in \( \mathbb{Q}(\sqrt{m}) \) that is not zero or a unit can be factored into a product of primes.

**Proof:** Let \( \alpha \in \mathbb{Q}(\sqrt{m}) \) with \( \alpha \neq 0 \) and \( \alpha \) not a unit. If \( \alpha \) is prime we are done. If not, write

\[ \alpha = \alpha_1 \alpha_2 \]

If \( \alpha_1 \) and \( \alpha_2 \) are primes we are done. If not, repeat with

\[ \alpha_1 \]
Continuing this process we obtain

\[ \alpha = \alpha_1, \ldots, \alpha_n. \]

If this process does not terminate with primes, then we have \( n \) can be arbitrarily large and

\[ N(\alpha) = \prod_{i=1}^{n} N(\alpha_i) \quad \Rightarrow \quad |N(\alpha)| = \prod_{i=1}^{n} |N(\alpha_i)| \geq 2^n. \]

But this is for any \( n \), as contradicted. \( \Box \)

What we are really interested in is not just factorization into primes, rather we want to know when an algebraic integer factors into primes, if it factors uniquely as we had for \( \mathbb{Z} \). This is not true in general as you saw in an earlier comment. Fortunately we do have that \( \mathbb{Q}(\sqrt{-7}) \) has unique factorization. This takes a couple of steps to prove.

The first step is to show that we can generalize the Euclidean algorithm to this setting. Again, this is not possible for all \( \mathbb{Q}(\sqrt{m}) \).

**Theorem:** Let \( \alpha \) and \( \beta \in \mathbb{Q}(\sqrt{m}) \) be algebraic integers or \( \beta \neq 0 \). Then there exist integers \( r \) and \( s \) in \( \mathbb{Q}(\sqrt{m}) \) such that

\[ \alpha = \beta r + s \quad \text{and} \quad |N(s)| < |N(\beta)|. \]
Proof: Let \( \alpha \) and \( \beta \) be as in the statement of the theorem.

We have that

\[
\frac{\alpha}{\beta} = r + s \sqrt{3} \quad \text{for } r, s \in \mathbb{Q}.
\]

Choose \( x \in \mathbb{Z} \) so that \( x \) is as close as possible to \( 2s \), and choose \( y \in \mathbb{Z} \) so that \( y = x \mod(2) \) and \( y \) is as close as possible to \( 2r \). Then we have

\[
|2s - x| \leq \frac{1}{2},
\]

and

\[
|2r - y| \leq 1.
\]

Since \( x \equiv y \mod(2) \), we have that \( y = \frac{y + x - 1}{2} \) is an algebraic integer.

Let \( s = \alpha - \beta y \). One can check using an characterization of the algebraic integers of \( \mathbb{Q}(\sqrt{3}) \) or the ring \( \mathbb{Z}[\left(1 + \sqrt{3}\right)/2] \) that the product and sum of algebraic integers is again an algebraic integer and so \( s \) is an algebraic integer.

Observe that \( \alpha = \beta y + s \) by definition and

\[
N(s) = N(\beta \alpha - \beta y)
\]

\[
= N(\beta) N\left(\frac{s}{\beta} - y\right)
\]

\[
= N(\beta) N\left((r - \frac{y}{\beta}) + (s - \frac{y}{\beta}) \sqrt{3}\right)
\]

\[
= N(\beta) \left((r - \frac{y}{\beta})^2 + 3(s - \frac{y}{\beta})^2\right).
\]

Thus,
\[ |N(\sqrt{5})| \leq |N(\sqrt{11})| \left( \frac{1}{7} + \frac{3}{\sqrt{10}} \right) < |N(\sqrt{11})| \]

\[ |25 - x| \leq \frac{1}{2} \Rightarrow 15 - \frac{3}{2} \leq \frac{1}{2} \]

and \[ |25 - y| \leq \frac{1}{2} \Rightarrow 15 - \frac{3}{2} \leq \frac{1}{2}. \]

We are now able to use this result to show that \( \mathbb{Q}(\sqrt{5}) \) has unique factorization.

**Theorem:** Every integer \( x \in \mathbb{Q}(\sqrt{5}) \) that is not 0 or a unit can be factored uniquely into primes, with the exception of units, in multiplicity by units.

**Proof:**

The proof of this theorem essentially follows the same way as in the case of \( \mathbb{Z} \) since there is a Euclidean algorithm.

**Lemma:** Let \( \alpha, \beta \in \mathbb{Q}(\sqrt{5}) \) have a common factor other than units. Then \( E \), \( F \in \mathbb{Q}(\sqrt{5}) \) exist.

\[ \alpha E + \beta F = 1. \]
\[ P = \sum x + \beta s : x, s, \beta \in \mathbb{R} \]

We know that \( N(x_0 + \beta s) \leq \mathbb{Z}_{\geq 0} \), so we can choose \( x, s \), so that \( N(x_0 + \beta s) \) is the smallest positive value.

Let \( \epsilon = x_0 + \beta s \). We apply the Euclidean alg to \( \epsilon \) and \( \epsilon \):

\[ \alpha = \epsilon \lambda + \mu \quad \Rightarrow \quad N(\mu) < N(\epsilon) \]

So we have

\[ \mu = \alpha - \epsilon \lambda = \alpha - (x_0 + \beta s) \lambda \]

\[ = \alpha \left( 1 - \lambda x_0 - \beta s \lambda \right) \]

Thus, \( \mu \) is an integer. Moreover, by the alg \( \epsilon \) and \( \epsilon \) we see \( N(\mu) = \alpha \Rightarrow \mu = 0 \). Thus, \( \alpha = \epsilon \lambda \)

\[ = \epsilon \lambda \epsilon \lambda ^{-1} \].

Now run the same alg with pair \( \epsilon, \epsilon \) to get \( \epsilon \lambda \). Thus, we must have \( \epsilon = \epsilon = 1 \), so

\[ \epsilon \lambda \epsilon ^{-1} = 1. \]

So

\[ \alpha \epsilon \epsilon ^{-1} \cdot \beta (S, \epsilon ^{-1}) = 1. \]

Lemma: If \( \pi \in p \) is a pair of \( \mathbb{G}(\sqrt{5}, \mathbb{Z}) \) and it \( \pi \alpha \beta \), then

\[ \pi \alpha = \pi \beta. \]
Proof: Suppose \( \mathfrak{p} \parallel \alpha \). Then the only common factor shared between \( \mathfrak{p} \) and \( \alpha \) can be units (by primality) = 
\[ \exists x, y \in \mathbb{Z} \text{ s.t.} \]
\[ \mathfrak{p} x + \alpha y = 2. \]

Thus, \[ \beta = \mathfrak{p} (\mathfrak{p} \beta) + \alpha (\mathfrak{p} \beta). \]

Since \( \mathfrak{p} \mid \alpha \beta \), \( \mathfrak{p} \) divides the RHS = \( \mathfrak{p} \lbrack \beta \rbrack. \]

By induction we extend this to \( \mathfrak{p} \mid (\alpha_1, \alpha_2) \), then \( \mathfrak{p} \mid \alpha \rbrack \]
for some \( 1 \leq i \leq n. \)

We can now prove that we have unique factorization for \( \mathbb{Z}[\sqrt{-3}] \).

Proof: Let \( \alpha \in \mathbb{Z}[\sqrt{-3}] \) with \( \alpha \neq 0 \), unit and let
\[ \alpha = \mathfrak{w}_1 \quad \mathfrak{w}_2 = \mathfrak{p}_1 \cdots \mathfrak{p}_s \]
be two prime factorizations. We have \( \mathfrak{w}_1 \mid \mathfrak{p}_1 \cdots \mathfrak{p}_s \)
\[ \Rightarrow \mathfrak{w}_1 = \mathfrak{p}_j \] for some \( j \) where assume \( j = 1 \). Then
\[ \mathfrak{w}_2 = \mathfrak{p}_2 \cdots \mathfrak{p}_s \]
Continue this process.

We must have the necessary background to prove FLT for square 3.
We will actually prove that
\[ \alpha^2 + \beta^3 + \gamma^3 = 0 \quad \text{for } \alpha \beta \gamma \neq 0 \]
has no solutions in \( \mathbb{Q} \) for \( \kappa = \mathbb{Q}(\sqrt{-3}) \). This is a more general result as \( \mathbb{Z} \subseteq \mathbb{Q} \), and we can always write
\[ x^3 + y^3 + (-z)^3 = 0 \]
if \( x, y, z \) were a solution to the equation
\[ x^3 + y^3 = z^3. \]

To simplify notation, set \( U = \frac{-1 + \sqrt{-3}}{2} \), which we can before is in \( \mathbb{Z} \) and is in fact a unit. It satisfies the equation
\[ U^2 + U + 1 = 0. \]

And so
\[ U^3 = 1. \]

Thus, the units of \( \mathbb{O}_K \) can given by
\[ \pm 1, \pm U, \pm U^2 \]
(check as an exercise!)

Observe that \( N(\sqrt{-3}) = 3 \) and so \( \sqrt{-3} \) is a prime of \( K \).

We set \( \omega = \sqrt{-3} \) as well as case notation. The associate...
Lemma 1: Let $x \in \mathbb{Q}$. Then $x$ is congruent to $0$ or $\pm 1$.

Proof: We can write $x = \frac{a + b \sqrt{3}}{2}$ with $a \equiv b \pmod{2}$.

We know that $\frac{b + a \sqrt{3}}{2}$ is also in $\mathbb{Q}$ by our characterization of $\mathbb{Q}$. Thus,

$$\frac{1}{2} \left( a + b \sqrt{3} \right) = \frac{a + b \sqrt{3}}{2} = \frac{1}{2} \left( b + a \sqrt{3} \right) = 2a \pmod{\sqrt{3}}.$$ 

We know that $2a \in \mathbb{Z}$ and everything in $\mathbb{Z}$ is congruent to $0$, $1$, or $2 \pmod{3}$. Since $\mathbb{Q} \mid 3$ contains $\mathbb{Z}$, we have $rac{1}{2} \left( a + b \sqrt{3} \right) \equiv 0$, $1$ (mod $2$).}

Lemma 2: Let $\alpha, \beta \in \mathbb{Q}$ and $\overline{\alpha}, \overline{\beta}$.

- If $\overline{\alpha} \equiv 1 \pmod{2}$, then $\alpha^3 \equiv 1 \pmod{2}$.
- If $\overline{\alpha} \equiv -1 \pmod{2}$, then $\alpha^3 \equiv -1 \pmod{2}$.
- If $\overline{\alpha} + \overline{\beta} \equiv 0 \pmod{2}$, then $\alpha^3 + \beta^3 \equiv 0 \pmod{2}$.
- If $\overline{\alpha} \alpha^3 + \beta^3 \equiv 0 \pmod{2}$, then $\alpha^3 - \beta^3 \equiv 0 \pmod{2}$.
Proof: Observe that \( \omega^4 = 9 \) as we will use this fact.

(i) \( \alpha = \pm 1 \pmod{15} \) by Lemma 1.

As \( \exists \beta \in \mathbb{Z}_7 \), \( \alpha = \pm 1 + \beta \omega \). Suppose \( \alpha \equiv 1 \pmod{15} \).

Then \( \alpha = 1 + \beta \omega \), and

\[
\alpha^3 = (1 + \beta \omega)^3 = 1 + 3\beta \omega - 9\beta^2 + \beta^3 \omega^3
\]

\[
\equiv 1 + 3\beta \omega + \beta^3 \omega^3 \pmod{15}.
\]

We also have \( (\omega - 3 + \omega^3) \)

\[
3\beta \omega + \beta^3 \omega^3 = \omega^3 (\beta^3 - \beta)
\]

\[
= \omega^3 \beta (\beta - 1)(\beta + 1).
\]

Lemma 1 gives that \( \beta (\beta - 1)(\beta + 1) \equiv 0 \pmod{15} \), and

\[
\omega^3 \beta (\beta - 1)(\beta + 1) \equiv 0 \pmod{15}.
\]

Then,

\[
\alpha^3 \equiv 1 \pmod{15}.
\]

The same arg goes \( \theta \) as well.

(ii) \( \alpha^3 - \alpha = \alpha (\alpha - 1)(\alpha + 1) \equiv 0 \pmod{15} \) by Lemma 2.

\[
\Rightarrow \quad \alpha^3 + \alpha \equiv \alpha + \alpha \pmod{15}
\]

\[\forall \alpha \equiv 1 \pmod{15}, \text{ then } \beta \equiv -1 \pmod{15} \text{ and vice versa.}
\]

\[\Rightarrow \text{ by } (i) \text{ that we have } \alpha^3 \equiv 1 \pmod{15} \text{ and } \beta^3 \equiv -1 \pmod{15}.
\]

\[
\alpha^3 + \beta^3 \equiv 0 \pmod{15}.
\]

This same type of arg goes \( \theta \) as well.

\[\text{Lemma 3: Let } \alpha, \beta, \gamma \in \mathbb{Z} \text{ and suppose } \alpha^3 + \beta^3 + \gamma^3 = 0. \text{ If }
\]

\[\gcd(\alpha, \beta, \gamma) = 1 \text{ then } \text{ divides one and only one of } \alpha, \beta, \gamma.
\]

\[\text{gcd}(\alpha, \beta, \gamma) = 1 \text{ then } \text{ divides one and only one of } \alpha, \beta, \gamma.
\]
Proof: Suppose $u$ divides more of them. Then the previous lemma 1 gives

\[ 0 = a^3 + b^3 + c^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{u^3}, \]

Thus, $u^3$ divides $3$ of them. However, $u^3 = 9$.

So this is a contradiction. Thus $u$ divides $a, b, or c$. It is clear it cannot divide $3$ of them, so $u$ divides

\[ a^3 + b^3 + c^3. \]

Would imply it divided all three $a, b, c$. This contradiction proves $u = 1.

\[ \ast \]

**Lemma 4:** Suppose $u$ divides $a, b, and c$ with $a + b + c$. And units $\epsilon_1, \epsilon_2$, and an integer $r$ such that

\[ \alpha^3 + \epsilon_1 \beta^3 + \epsilon_2 \gamma^3 = 0. \]

Then $\epsilon_1 = \pm 1$ and $r = 0$.

Proof: Make $r$ a positive integer, we have

\[ \alpha^3 + \epsilon_1 \beta^3 \equiv 0 \pmod{u^3}. \]

Lemma 3 gives

\[ \alpha^3 + \epsilon_1 \beta^3 \equiv \pm 1 + \epsilon_2 (\pm 1) \equiv 0 \pmod{u^3}. \]

We know the unit $\epsilon_1$ must be $\pm 1, \pm 2, \pm 3$, and

As plugging in all possibilities, we get...
\[ x^3 + y^3 + z^3 = 0, \quad \pm x, \quad \pm (1+u), \quad \pm (1+u^2) \] with all possible combinations of signs. We claim this cannot happen unless the case \( \pm 1 \pm \varepsilon_1(\pm 1) \equiv 0 \pmod{\mathfrak{a}^3} \).

\[ \pm 1 \pm \varepsilon_1(\pm 1) \equiv \pm 2 \; \text{in this case,} \; N(\pm 1 \pm \varepsilon_1(\pm 1)) = 4 \; \text{and} \]

\[ N\left( \mathfrak{a}^3 \right) = 27, \quad \text{so} \quad \mathfrak{a}^3 \not\equiv 2. \]

\[ \pm 1 + \varepsilon_1(\pm 1) \equiv 1 - u, 1 - u^2: \] Assume 1 - u and 1 - u^2 are associates of \( \mathfrak{a} \), this would give \( \mathfrak{a}^3 \mid \mathfrak{a}^3 \), #.

\[ \pm 1 + \varepsilon_1(\pm 1) \equiv 1 + u, 1 + u^2: \] 1 + u = -u^2, 1 + u^2 = -u, then as both units but \( \mathfrak{a}^3 \) is not a unit, as cannot clearly be a unit.

Thus we must have \( x^3 + y^3 + z^3 \equiv 0 \pmod{\mathfrak{a}^3} \) \( \Rightarrow \) by Lemma 2 \( \Rightarrow \) that \( x^3 + y^3 + z^3 \equiv 0 \pmod{\mathfrak{a}^4} \). Thus, \( \mathfrak{a}^4 \mid \mathfrak{a}^3 (\mathfrak{a}^3 y^3) \)

\( \Rightarrow r > 2. \)

\[
\text{Lemma 5: There do not exist } x, y, \text{ a unit } \varepsilon, \text{ and an integer } r \geq 2 \text{ such that}
\]

\[ x^3 + y^3 + z^3 + 2(\overline{\mathfrak{a}}^{3r})^3 = 0. \quad (\AA) \]

This 6th lemma is essentially what we want remaining. Before we prove it, we see how it gives us the theorem we desire:
**Theorem:** There are no nonzero \( \alpha, \beta, \gamma \in \mathbb{R} \) at
\[
\alpha^3 + \beta^3 + \gamma^3 = 0.
\]

**Proof:** Suppose \( \alpha, \beta, \gamma \in \mathbb{R} \) are nonzero with
\[
\alpha^3 + \beta^3 + \gamma^3 = 0.
\]

Divide out by \( \gcd(\alpha, \beta, \gamma) \) so that we can assume \( \gcd(\alpha, \beta, \gamma) = 1 \). Lemma \ref{lemma3} gives that \( \alpha, \beta, \gamma \) divide exactly one of \( \alpha, \beta, \gamma \), say \( \alpha \mid \gamma \), let \( m \parallel Y \) (this means \( m \) is the largest integer so that \( m \parallel Y \)). Then \( Y = m\gamma \), with \( \gcd(m, \gamma) = 1 \), \( Y \in \mathbb{Z}^+ \). Lemma \ref{lemma4} gives \( \gcd(\alpha, m\gamma) = 1 \) and we have
\[
\alpha^3 + \beta^3 + (m\gamma)^3 = 0.
\]
This contradiction Lemma \ref{lemma5}.

There it only remains to prove Lemma \ref{lemma5}.

**Proof (Lemma \ref{lemma5}):** We prove this by descent. Since our solutions cannot be ordered themselves, our descent proceeds with the norm of the elements.

Suppose \( \alpha, \beta, \gamma \) is a solution. We may assume \( \gcd(\alpha, \beta, \gamma) = 1 \) and \( \gcd(\alpha, \gamma) = 1 \).
We have

$$\alpha^3 + \beta^3 \equiv 0 \pmod{5^3}$$

with $3r > 0$.

We can factor $\alpha^3 + \beta^3$ in $D_0$ as

$$\alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + u\beta)(\alpha + u^2\beta).$$

**Claim:** If $p_0$ is a prime so that $p_0$ divides two of $\alpha + \beta$, $\alpha + u\beta$, $\alpha + u^2\beta$, then $p_0$ is an associate of $\overline{5}$.

**Pf:** There are several cases to check, all pretty much the same.

For example, if $p_0 | \alpha + \beta$ and $p_0 | \alpha + u\beta$, then

$$p_0 | (\alpha + \beta) - (\alpha + u\beta) = \beta(1 - u).$$

Similarly, $p_0 | \alpha(1 - u)$.

However, $gcd(\alpha, \beta) = 1$ which is an associate of $\overline{5}$. Thus, $p_0$ is an associate of $\overline{5}$. The other cases are analogous. \(\square\)

Using this same type of arg., one can use $\alpha + u\beta$ to show that the difference between $\alpha + \beta$, $\alpha + u\beta$, $\alpha + u^2\beta$ is divisible by $5^2$ but not by $5^3$. The choice that $5$ of the three can still be divisible by $5$. For $3$ of the three were divisible by $5^3$, their difference would be.

Thus we have if we let $a, b, c \in \mathbb{Z}$ s.t.
\( a, b, c \) \( \equiv 1, 1, 3r-2 \) since \( a+b+c = 3r \). Thus,

\[
\frac{\alpha+\beta}{\omega^a}, \quad \frac{\alpha+\omega^b}{\omega^b}, \quad \frac{\alpha+\omega^c}{\omega^c}
\]

are elements of \( \mathbb{Z}_3 \) with no common prime factors.

Thus, we have that equation (1) can be written as

\[
\left( \frac{\alpha+\beta}{\omega^a} \right) \left( \frac{\alpha+\omega^b}{\omega^b} \right) \left( \frac{\alpha+\omega^c}{\omega^c} \right) = -2Y^3 \tag{2}
\]

This gives that each element on the LHS of equation (2) must be an associate of a cube in \( \mathbb{Z}_3 \):

\[
\alpha+\beta = \varepsilon_1 \omega^a \lambda_1^3
\]

\[
\alpha+\omega^b = \varepsilon_2 \omega^b \lambda_2^3 \tag{3}
\]

\[
\alpha+\omega^c = \varepsilon_3 \omega^c \lambda_3^3
\]

with \( \varepsilon_i \) units.

Using that \( U^3 = 1 \) we have:

\[
(\alpha+\beta) + U(\alpha+\omega^b) + U^2(\alpha+\omega^c)
\]

\[
= (\alpha+\beta) (1+U+U^2) = 0.
\]

Thus, we have
\[ \varepsilon_1 \omega^a \lambda_1^3 + \varepsilon_2 \omega^b \lambda_2^3 + \varepsilon_3 \omega^c \lambda_3^3 = 0 \quad (3) \]

where \( \varepsilon_1 = a \varepsilon_3, \varepsilon_2 = a^2 \varepsilon_3 \) are units.

Equation (3) is symmetric in \( a, b, c \) so an can set \( a = 1, b = 1, c = 3r - 2 \), which gives:

\[ \varepsilon_1 \omega \lambda_1^3 + \varepsilon_2 \omega \lambda_2^3 + \varepsilon_3 \omega^{3r-2} \lambda_3^3 = 0. \]

Dividing by \( \varepsilon_2 \omega \):

\[ \lambda_1^3 + \varepsilon_2 \lambda_2^3 + \varepsilon_3 \left( \omega^{3r-2} \lambda_3 \right)^3 = 0 \quad (4) \]

where \( \varepsilon_2 = \frac{\varepsilon_2}{\varepsilon_1}, \varepsilon_3 = \frac{\varepsilon_3}{\varepsilon_1} \) are units.

Since \( \varepsilon_2 \neq 0 \), equations (2) and (2) give \( \lambda_1, \lambda_2, \lambda_3 \neq 0 \).

Lemma 1 may give \( \varepsilon_2 = \pm 1 \) and \( r - 1 \geq 0 \). However, equation (4) is of the form (4) because \( \varepsilon_2 \lambda_2^3 \) is either \( \lambda_2^3 \) or \( (-\lambda_2)^3 \) \( (\varepsilon_2 = \pm 1) \). We have

\[ N(\lambda_1^3 \lambda_2^3 \omega^{3r-1} \lambda_3) = N(\omega^{-3} (\alpha + \rho)(\alpha + \rho + 1)(\alpha + \rho + 1)) \]

\[ = N(\omega^{3r-3} \chi^3) < N(\alpha^3 \beta^3 \omega^{3r} \chi^3) \]

hence

\[ N(\omega^{3r-3}) = N(\omega)^{3r-3} = 3^{3r-3} \]

And

\[ N(\alpha^3 \beta^3 \omega^{3r}) = N(\alpha) N(\beta) 3^{3r} \quad \text{and} \quad N(\alpha), N(\beta) > 1 \]

and \( 3^{-3} < 1 \).
Thus, from our original solution \( x, p, \delta \) we produce another solution \( x', p', \delta' \) of strictly smaller norm. Moreover, the norm of a norm for a nonzero element \( v \) is a positive integer. Repeating this process produces a strictly decreasing sequence of positive integers. Thus, there could be no solution to begin with. \( \square \)