MTHSC 412 Section 2.4 – Prime Factors and Greatest Common Divisor

Kevin James

Definition

Suppose that $a, b \in \mathbb{Z}$. Then we say that $d \in \mathbb{Z}$ is a greatest common divisor (gcd) of a and b if the following conditions are satisfied.

1. $d \geq 0$.
2. $d|a$ and $d|b$.
3. If $c|a$ and $c|b$ then $c|d$.

Notation

If d is the gcd of a and b we may write $(a, b) = d$.

My Convention

It is sometimes useful to define $(0, 0) = 0$.

Theorem

Let $a, b \in \mathbb{Z}$ *with at least one of them nonzero. Then there exists a unique gcd* d *of* a *and* b*. Moreover* d *can be realized as an integral linear combination of* a *and* b*. That is, there are* $m, n \in \mathbb{Z}$ *such that*

$$d = am + bn.$$

Further, d *is the smallest positive integer of this form.*

Proof

Suppose that $a, b \in \mathbb{Z}$ with at least one being nonzero.

Existence: First we note that if $a = 0$ then $(a, b) = (0, b) = |b|$ and
$|b| = a \cdot 0 + (\pm 1) \cdot b$.

The case that $b = 0$ is similar. So, we now assume that a and b are nonzero.

Let $S = \{ax + by \quad | \quad x, y \in \mathbb{Z}; ax + by > 0\}$.

Note that either a or $-a$ is in S. So, $S \neq \emptyset$.

Using the well ordering principle, let d be the least element of S.

Since, $d \in S$, there are $x, y \in \mathbb{Z}$ such that $d = ax + by$.

It is also clear that d is the smallest such number which is positive.

By the division algorithm, we can write $a = dq + r$ with $0 \leq r < d$.

Then $r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq)$.

However, $r < d \Rightarrow r \notin S$, (b/c d is the least element of S).

Thus $r = 0$ and $d|a$.

We can prove that $d|b$ in a similar way.

Proof continued ...

Finally suppose that $c|a$ and $c|b$.
Then we have $a = ck$ and $b = cm$ for some $k, m \in \mathbb{Z}$.
Thus $d = ax + by = ckx + cmy = c(kx + my)$ and $c|d$.
So, d is the gcd of a and b.
Uniqueness: Suppose now that we have two gcd's d and e.
Since $d|a$ and $d|b$ and since e is a gcd, $d|e$.
Since $e|a$ and $e|b$ and since d is a gcd, $e|d$.
So, $d = ek$ and $e = dm$ for some $k, m \in \mathbb{Z}$.
$\Rightarrow d = dmk \Rightarrow mk = 1 \Rightarrow m, k = \pm 1$.
So, $d = \pm e$. However, $e, d \geq 0 \Rightarrow e = d$. $\square$

FACT

If $a = bq + r$ *then* $(a, b) = (b, r)$.

EXERCISE

Prove this!

HINT:

Show that any common divisor of a and b is also a divisor of r and that any common divisor of b and r is a divisor of a.

Euclidean Algorithm

Given a and b not both zero, first note that $(a, b) = (|a|, |b|)$. So we may replace a and b by $|a|$ and $|b|$ respectively.
Thus after rearrangement if necessary we can assume that $a \geq 0$ and that $b > 0$.
Use the division algorithm to write

$$a = bq + r; \quad 0 \leq r < b$$

Then recall that $(a, b) = (b, r)$.
Now repeat the process with a replaced by b and b replaced by r.
Continue in this manner until you encounter a remainder of 0 and note that $(b, 0) = b$.

Compute the $(246, 180)$.
$246 = 180(1) + 66 \Rightarrow (246, 180) = (180, 66)$.
$180 = 66(2) + 48 \Rightarrow (180, 66) = (66, 48)$.
$66 = 48(1) + 18 \Rightarrow (66, 48) = (48, 18)$.
$48 = 18(2) + 12 \Rightarrow (48, 18) = (18, 12)$.
$18 = 12(1) + 6 \Rightarrow (18, 12) = (12, 6)$.
$12 = 6(2) + 0 \Rightarrow (12, 6) = (6, 0) = 6$!

The Euclidean algorithm produces:

$$
\begin{aligned}
a &= bq_1 + r_1 & \Rightarrow \quad & r_1 = a - bq \\
b &= r_1q_2 + r_2 & \Rightarrow \quad & r_2 = b - r_1q_2 \\
r_1 &= r_2q_3 + r_3 & \Rightarrow \quad & r_3 = r_1 - r_2q_3 \\
r_2 &= r_3q_4 + r_4 & \Rightarrow \quad & r_4 = r_2 - r_3q_4 \\
&\vdots & & \vdots \\
r_{i-2} &= r_{i-1}q_i + r_i & \Rightarrow \quad & r_i = r_{i-2} - r_{i-1}q_i \\
&\vdots & & \vdots \\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} & \Rightarrow \quad & r_{n-1} = r_{n-3} - r_{n-2}q_{n-1} \\
r_{n-2} &= r_{n-1}q_n + r_n & \Rightarrow \quad & r_n = r_{n-2} - r_{n-1}q_n \\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned}
$$

Note that $(a, b) = r_n$ and we can use successive back substitution to write r_n in terms of r_k and r_{k-1} eventually expressing r_n in terms of a and b.

Example

Let's reconsider our previous example: $(246, 180) = 6$.

$$\begin{aligned}
246 &= 180(1) + 66 & \Rightarrow \quad & 66 = 246 + (-1)180 \\
180 &= 66(2) + 48 & \Rightarrow \quad & 48 = 180 + (-2)66 \\
66 &= 48(1) + 18 & \Rightarrow \quad & 18 = 66 + (-1)48 \\
48 &= 18(2) + 12 & \Rightarrow \quad & 12 = 48 + (-2)18 \\
18 &= 12(1) + 6 & \Rightarrow \quad & 6 = 18 + (-1)12 \\
12 &= 6(2) + 0 & &
\end{aligned}$$

Now write

$$\begin{aligned}
6 &= 18 + (-1)12 = 18 + (-1)[48 + (-2)18] = (3)18 + (-1)48 \\
&= (3)[66 + (-1)48] + (-1)48 = (3)66 + (-4)48 \\
&= (3)66 + (-4)[180 + (-2)66] = (11)66 + (-4)180 \\
&= (11)[246 + (-1)180] + (-4)180 = (11)246 + (-15)180.
\end{aligned}$$

So, take $x = 11$ and $y = -15$.

Definition

Two integers a and b are *relatively prime* or *coprime* if $(a, b) = 1$.

Theorem

If a and b are coprime and $a|bc$ then $a|c$.

Proof.

Since a and b are coprime, there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Since $a|bc$ there is $k \in \mathbb{Z}$ such that $bc = ak$. So,

$$\begin{aligned} 1 = ax + by \quad &\Rightarrow \quad c = acx + bcy \\ &\Rightarrow \quad c = acx + aky \quad \text{(because } bc = ak\text{)} \\ &\Rightarrow \quad c = a(cx + ky) \\ &\Rightarrow \quad a|c. \end{aligned}$$

$\square$

DEFINITION

An integer p is a *prime* if $p > 1$ and if the only positive divisors of p are 1 and p.

THEOREM (EUCLID'S LEMMA)

If p is a prime and $p|ab$ then $p|a$ or $p|b$.

PROOF.

Suppose that $p|ab$. If $p|a$ then the conclusion of the theorem holds.
Now, suppose that $p \not| a$.
Then $(a, p) = 1$ because the only positive divisors of p are 1 and p.
Thus by our previous theorem, $p|b$. $\square$

Corollary

1. *If* $p|(a_1 a_2 \ldots a_n)$ *then* $p|a_i$ *for some* $1 \le i \le n$*.*
2. *If* $p|a^m$ *then* $p|a$*.*

Proof.

We will prove part 1 by induction on n.
The result is trivial when $n = 1$.
Now suppose that the result holds for $n = k$ for some $k \ge 1$.
Now, suppose that $p|(a_1 a_2 \ldots a_{k+1}) = (a_1 a_2 \ldots a_k) \cdot a_{k+1}$.
If $p|a_{k+1}$ then the conclusion of the theorem holds.
If $p \not| a_{k+1}$ then by Euclid's lemma, $p|(a_1 a_3 \ldots a_k)$.
In thisr case, our induction hypothesis implies that $p|a_i$ for $a \le i \le k$ and the conclusion of the theorem holds.
Part 2 follows from part 1. $\square$

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n \geq 2$ can be expressed as a product of primes and this factorization is unique up to rearrangement of the factors.

Proof

Existence: Since 2 is prime, the theorem holds for n=2.
Suppose that the theorem holds for $2 \leq n \leq k$ for some $k \geq 2$.
Let's consider $k+1$.
If $k+1$ is prime then it is already factored.
If $k+1$ is not prime then it has a divisor other than itself and 1.
Thus we can write $k+1 = mr$ with $1 < m \leq r < k+1$.
Since $2 \leq m \leq r \leq k$ our induction hypothesis implies that both m and r can be factored into primes, say
$m = p_1 \cdot \cdots \cdot p_j$, $r = q_1 \cdot \cdots \cdot q_i$.
Then $k+1 = mr = p_1 \cdot \cdots \cdot p_j q_1 \cdot \cdots \cdot q_i$ is a prime factorization of $k+1$.
It follows by strong induction than any $n \geq 2$ has a factorization into primes.

Proof continued ...

Uniqueness: Suppose that we have two factorizations of n:
$n = p_1 \dots p_t$ and $n = q_1 \dots q_s$ with $t \leq s$.
$\Rightarrow p_1 \dots p_t = q_1 \dots q_s$
Thus $p_1 | (q_1 \dots q_s)$.
By our corollary, $p_1 | q_i$ for some $1 \leq i \leq s$.
After relabeling the q_i's we may assume that $p_1 | q_1$.
Since, q_1 is prime, it follows that $p_1 = q_1$ and we have
$p_1 \dots p_t = p_1 q_2 \dots q_s \Rightarrow p_2 \dots p_t = q_2 \dots q_s$.
Repeating this argument, we see that after relabeling the q_i's, we will have $p_1 = q_1$, $p_2 = q_2$, ..., $p_{t-1} = q_{t-1}$ and $p_t = q_t \dots q_s$.
Since p_t is prime, it follows that there must be only one prime on the right (i.e. $s = t$) and $p_t = q_t$. $\square$

Corollary

If $n \geq 2$ *then there are primes* $p_1 < p_2 < \cdots < p_k$ *and positive integers* $e_1, \ldots, e_k$ *such that*

$$n = p_1^{e_1} \ldots p_k^{e_k},$$

and this factorization is unique.

Theorem (Euclid's Theorem)

There are infinitely many primes.

Proof.

We will show that any finite list of primes is incomplete.
Suppose that $p_1, p_2, \ldots, p_k$ is a list of primes.
Consider $n = (p_1 p_2 \ldots p_k) + 1$.
Now FTA guarantees us that n has at least one prime factor, say q.
If $q | (p_1 \ldots p_k)$ then we would be able to write
$(p_1 \ldots p_k) = qm$ and $n = qr$ for some $m, r \in \mathbb{Z}$, and
then we would have
$1 = n - (p_1 \ldots p_k) = qm - qr = q(m - r) \Rightarrow q | 1$
which cannot be true.
Thus $q \not| (p_1 \ldots p_k)$, and we have found a prime q which was not on our list.
Thus any finite list of primes is incomplete. $\square$