MTHSC 412 Section 1.3 – Primes and Unique Factorization

Kevin James

Definition

An integer p is said to be prime if $p \neq 0, \pm 1$ and the only divisors of p are ± 1 and $\pm p$.

Example

2, 3, 5, 7, 11, 13, 17, 19, 23 and 29 are primes.
4, 6, 8, 9, 10, 12 are not.

Fact

- *p is prime if and only if $-p$ is prime.*
- *If p and q are prime and $p|q$, then $p = \pm q$.*

Theorem

Let $0, \pm 1 \neq p \in \mathbb{Z}$. Then p is a prime if and only if whenever $p|bc$, $p|b$ or $p|c$.

Proof.

($\Rightarrow$): Suppose that p is prime and that $p|bc$.
Let $d = (p, b)$.
Then $d \geq 1$ and $d|p$. So, $d = 1$ or $|p|$.
Case 1: $d = |p|$. In this case, we have $d = \pm 1 \cdot p$.
Also, $d|b$. So, $b = dk$ for some $k \in \mathbb{Z}$.
So, $b = dk = p \cdot (\pm k)$, and $p|b$.
Case 2: $d = 1$. In this case, we have $p|bc$ and $(p, b) = 1$.
So, by theorem 1.5 in our book, $p|c$.
($\Leftarrow$): Exercise. $\square$

Corollary

If p is a prime and $p|a_1 a_2 \cdot \cdots \cdot a_n$ then p divides at least one of the a_i's.

Proof.

We are given that $p|(a_1) \cdot (a_2 \cdot \cdots \cdot a_n)$.
By the previous theorem, we can conclude that $p|a_1$ or $p|(a_2 \cdot \cdots \cdot a_n)$.
In the latter case, we can again apply the theorem, to conclude that either $p|a_2$ or $p|(a_3 \cdot \cdots \cdot a_n)$.
Thus after at most $n-1$ applications or our theorem, we can conclude that $p|a_i$ for some $1 \leq i \leq n$. $\square$

Theorem

Suppose that $0, \pm 1 \neq n \in \mathbb{Z}$*. Then* n *can be expressed as a product of primes.*

Note

We allow expressions involving only one prime. Thus any prime is easily expressible as a product of primes.

Proof

Since $n = p_1 \cdot \cdots \cdot p_k$ if and only if $-n = (-p_1)p_2 \cdot \cdots \cdot p_k$, we may assume without loss of generality that $n \geq 2$.

Let S denote the set of all integers greater than 1 which cannot be expressed as a product of primes.

We will show that $S = \emptyset$.

Assume for the sake of contradiction that $S \neq \emptyset$.

Then by the well ordering principle, S has a smallest element m.

Since $m \in S$, m cannot be a prime.

Thus m has some divisor other than $\pm 1, \pm m$, say a.

We may assume that $a > 1$ and thus that $m = ab$ where $1 < a, b < m$ and $a, b \in \mathbb{Z}$.

Now, since, a and b are integers greater than 1 but smaller than m, $a, b \notin S$.

Thus, a and b can be expressed as a product of primes, say $a = p_1 \cdot \cdots \cdot p_t$ and $b = q_1 \cdot \cdots \cdot q_r$.

Thus, $m = ab = p_1 \cdot \cdots \cdot p_t \cdot q_1 \cdot \cdots \cdot q_r$ which is a product of primes.

Proof continued ...

Thus $m \notin S$ which contradicts our choice of $m \in S$.
So, we conclude that $S = \emptyset$ and thus all integers greater than 1 can be expressed as a product of primes, and as mentioned above this implies that all integers other than 0 and ± 1 can be expressed as a product of primes. $\square$

Theorem (Fundamental Theorem of Arithmetic)

Every $0, \pm 1 \neq n \in \mathbb{Z}$ can be written as a product of primes. This factorization is unique up to rearrangement and sign change.

Corollary

Every integer $n > 1$ can be expressed uniquely as $n = p_1 \cdot \cdots \cdot p_t$ where the $p_1 \leq p_2 \leq \cdots \leq p_t$ and where the p_i's are positive primes.

Theorem

Let $n > 1$. If n has no positive prime factor less than or equal to $\sqrt{n}$, then n is prime.