MthT 491 Divisibility and Prime Numbers

Definition. *An integer $p > 1$ is called* a prime number*, or a* prime*, if there is no divisor d of p satisfying $1 < d < p$. If an integer $p > 1$ is not a prime, it is called a* composite number*.*

N.B. We don't call 1, 0, or negative integers either *prime* or *composite*.

Equivalent definition?

Definition. *A positive integer $p \neq 1$ is called* a prime number*, or a* prime*, if there is no positive divisor d of p satisfying $d \neq 1, p$. If a positive integer $p \neq 1$ is not a prime, it is called a* composite number.

Our first result is the easy version of the *Fundamental Theorem of Arithmetic*.

Theorem. [**N–Z**] *(1.14). Every integer $n > 1$ can be expressed as a product of primes (with perhaps only one factor).*

Proof. Let's try a proof by contradiction. Suppose there is an integer $n > 1$ which cannot expressed as a product of primes. By the WOP, there is a smallest n, call it n_0 which cannot expressed as a product of primes. We know that $n_0 > 1$ and that n_0 is not a prime. But then $n_0 = n_1 n_2$, $1 < n_1, n_2 < n_0$. But then both n_1 and n_2 can be expressed as a product of primes. This is a contradiction since we now have both

$$A \equiv n_0 \text{ cannot be expressed as a product of primes}$$

$$\neg A \equiv n_0 \text{ can be expressed as a product of primes}$$

are true.

For integers $n > 1$, the factorization into primes is unique. This is the *Fundamental Theorem of Arithmetic*.

Theorem. [**N-Z**]*, Theorem 1.15. If $p \mid ab$, p being a prime, then $p \mid a$ or $p \mid b$.*

Proof. (not intuitive without buildup!) Let k be an integer such that $ab = pk$. If p does not divide a, then $\gcd(p, a) = 1$. (The gcd must be either p or 1). For some integers x, y, $1 = px + ay$ and $b = pbx + bay = pbx + pky = p\,(bx + ky)$. Thus $p \mid b$.

Theorem. *The factoring of any integer $n > 1$ into primes is unique apart from the order of the prime factors.*

Proof. Another proof by contradiction!. If the Theorem is not true, there is a *smallest* integer n for which the factorization is not unique. Dividing out any common factors, we have

$$\begin{aligned} n &= p_1 p_2 \cdots p_r \\ &= q_1 q_2 \cdots q_s. \end{aligned}$$

Without loss of generality, $p_1 < q_1$. Let

$$\begin{aligned} N &= (q_1 - p_1) q_2 \cdots q_r \\ &= N - p_1 q_2 \cdots q_s \\ &= p_1 \left(p_2 \cdots p_r - q_2 \cdots q_s \right). \end{aligned}$$

But p_1 does not divide $(q_1 - p_1)$ (Why?). We have $0 < N < n$, and N has two distinct factorings, on involving p_1, and the other without p_1.

Weird Examples of Non–Unique Prime Factorization

1. Let **E** consist of even integers of the form $2k$, $k = 0, \pm 1, \pm 2, \ldots$.

$$\mathbf{E} = \{0, \pm 2, \pm 4, \ldots\}.$$

Usual multiplication and addition is well defined. Working very carefully, the *primes* are those numbers $p = 2 \cdot \text{odd} > 1$ and the *composite numbers* are $n = 2 \cdot \text{even} > 1$. So

$$\begin{aligned} \text{primes} &= \{2, 6, 10, 14, \ldots\}, \\ \text{composites} &= \{4, 8, 12, \ldots\}. \end{aligned}$$

Prime factoring is not unique since $60 = 2 \cdot 30 = 6 \cdot 10$ has (at least) two factorings into primes.

2. Let **W** consist of all integers of the form $4k + 1$, $k = 0, \pm 1, \pm 2, \ldots$.

$$\mathbf{W} = \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\}.$$

Usual multiplication works, in the sense that the product of two numbers in **W** remains in **W**. Addition does not work within the class. Working very carefully, the *primes* are those numbers $p = 4k + 1 > 1$ which have no factors (divisors!) of the form $4j + 1$ except for p and 1. Thus $1, 5, 9, 13, 17, 21, 29, 33, 37, 41, 49$ are *primes*, but $25 = 5 \cdot 5, 45 = 5 \cdot 9$ are not a *prime* in this context. We have two prime factorizations for $(21)^2 = 441$;

$$\begin{aligned} (21)^2 &= 21 \cdot 21 \\ &= (3 \cdot 7) \cdot (3 \cdot 7) \\ &= (3 \cdot 3) \cdot (7 \cdot 7) \\ &= 9 \cdot 49. \end{aligned}$$

Show that 33^2 has two *prime* factorizations in this context.