Prime Numbers

A natural number $a > 1$ is prime if the only numbers which divides a are 1 and a. So a is prime if $a \mid a$, $1 \mid a$, and if $c \mid a$ then $c = a$ or $c = 1$. The integer a is said to be composite if a is not prime. Hence there exists a positive integer $c \neq a$ and $c \neq 1$ such that $c \mid a$

Lemma 4.20. *Given any natural number $n > 1$, there exists a prime p such that $p \mid n$.*

Proof. Proof by contradiction

Suppose there is no prime which divides n. Let C be the set of integers greater than 1 which are not divisible by a prime number. Since $n \in C$ we know that C is not the empty set. Hence by the Well Order Principle, C has a least element, say k. Now, k can not be prime because $k \mid k$ and $k \in C$. Since k is not prime there exist a such that $1 < a < k$ and $a \mid k$. If there exists a prime, p that divides a then $p \mid k$ as $a \mid k$. Otherwise $a \in C$ which contradicts that m is the least element in C.

□

Theorem 4.21. *There are an infinite number of primes.*

Proof. Proof by contradiction

Assume that there are an finite number of primes, say $p_1, p_2, \ldots, p_k$. Consider the integer $n = (p_1 p_2 \cdots p_k) + 1$. By Lemma 4.20 there exists a prime $p_i \in \{p_1, p_2, \ldots, p_k\}$ which divides n. Moreover $p_i \mid p_1, p_2, \ldots, p_k$ which implies that $p_i \mid n - p_1 p_2 \cdots p_k = 1$. This means $p_i = 1$ which contradicts that p_i is prime.

□

Theorem 4.22. *Every integer n greater than 1 can be written as*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$$

where p_i are distinct primes and k_i are integers.

In Theorem 4.22 $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$ is the *prime factorization/decomposition* of n.

Example 4.23. Write the factorization of 2088. To write prime factorization of 2088 find small prime which divide it and write the number. Since $2 \mid 2088$ we have $2088 = 2 \cdot 1044$. Similarly, $2 \mid 1044$ which implies $2088 = 2 \cdot 2 \cdot 522 = 2^2 \cdot 522$. Continuing this process we get

$$\begin{aligned} 2088 &= 2^2 \cdot 522 \\ &= 2^3 \cdot 261 \\ &= 2^3 \cdot 3 \cdot 87 \\ &= 2^3 \cdot 3^2 \cdot 29. \end{aligned}$$

Since $2, 3, 29$ are all prime we know that $2^3 \cdot 3^2 \cdot 29^1$ is the prime factorization 2088.

Problem 4.24. *Write the prime factorization of* 127*.*

Problem 4.25. *Let x, a and b be integers such that $x \mid ab$. If x and a are relatively prime prove that $x \mid b$.*