THEORY OF NUMBERS
THE FUNDAMENTAL THEOREM OF ARITHMETIC

Theorem Euclids Algorithm Suppose $a > 0,\ b$ are integers. $\exists$ unique $q,\ r$ such that $b = aq + r$ and $0 \leq r < a$.

Proof (i) Existence

Choose the greatest value of q such that $b - aq \leq 0$ and write $r = b - aq$ so $r > 0$. If $r \geq a$ then $b - a(q+1) \geq 0$ which contradicts the definition of q.

(ii) Uniqueness

Suppose $\exists q',\ r'\ q'',\ r''$ with $q' > q''$. Then $a \leq a(q' - q'') = r'' - r' < a$ which gives us a contradiction.

Definition A modulus of integers is a set S of integers such that

(i) S contains a non-zero element

(ii) $m \in S, n \in S \Rightarrow m - n \in S$

Theorem Every modulus of integers is equivalent to the set of all integer multiples of some natural number.

Proof Let k be the least positive element in S. Let T be the set of all integral multiples of k.

(i) $T \subset S$

$$\begin{aligned} k \in S &\Rightarrow k - k = 0 \in S \\ &\Rightarrow 0 - k = -k \in S \\ &\Rightarrow k - (-k) = 2k \in S \end{aligned}$$

etc. (proof by induction).

(ii) $S \subset T$

Let $x \in S$ By Euclids algorithm $\exists q,\ r$ such that $x = qk + r$ $0 \leq r \leq k,\ x \in S,\ qk \in S$ therefore $r \in S$ therefore $r = 0$ therefore $x \in T$.

Theorem Suppose $a,\ b$ are not both zero. $\exists$ a unique natural number d such that

(i) $d|a\ d|b$

(ii) if $t|a$ and $t|b \Rightarrow t|d$

(iii) $\exists x,\ y$ such that $d = ax + by$

d is called the highest common factor (H.C.F) of $a,\ b$ denoted by (a, b).

Proof **(1)** Existence

Consider the set of all numbers of the form $ax + by$. This set is a modulus S which has a generator d.

(iii) follows from the definition of $d,\ a \in S\ b \in S$ therefore (i) follows. (ii) follows from (iii)

(2) Uniqueness

Suppose $d',\ d''$ satisfy (i) to (iii).

$$\begin{aligned} d'|a \text{ and } d'|b &\Rightarrow d'|d'' \\ d''|a \text{ and } d''|b &\Rightarrow d''|d' \\ &\Rightarrow d' = d'' \end{aligned}$$

Corollary Suppose $a_1 \ldots a_n$ are not all zero. $\exists$ a unique $d = (a_1 \ldots a_n)$ such that

(i) $d|a_1 \ldots d|a_n$

(ii) $t|a_1 \ldots t|a_n \Rightarrow t|d$

(iii) $\exists x_1 \ldots x_n$ such that $d = a_1x_1 + \ldots + a_nx_n$

The equation $a_1x_1 + \ldots + \_nx_n = k$ is soluble $\Leftrightarrow k|a$

Theorem Suppose p is prime and $p|ab$. Then either $p|a$ or $p|b$ or both.

Proof Suppose p does not divide a. Then (p, a)=1. Hence $\exists x,\ y$ such that $1 = px + ay$ therefore $b = bpx + aby$ therefore $p|b$.

Fundamental Theorem of arithmetic Every positive integer ≥ 2 is representable as a finite product of positive primes, the representations being unique, apart from order.

Proof Suppose $n = p_1p_2 \ldots p_r = q_1 \ldots q_s$ is the smallest n with two such representations. Then $p_1|q_j$ say. $p_q \ldots p_r = q_1 \ldots q_{j-1}q_{j+1} \ldots q_s$ this is smaller then n. So the result follows.