The Divison Algorithm

Theorem 2.9 (Division Algorithm). *Let a and b be integers, with $b > 0$. Then there exist unique integers q and r such that*

$$a = bq + r$$

where $0 \le r < b$.

Proof:

Must show both existance and uniqness

Existance

Let $S = \{a - bk \mid k \in \mathbb{Z} \text{ and } a - bk \geq 0\}$

- $0 \in S \Rightarrow b$ divides a $\therefore$ $q = \frac{a}{b}$ and $r = 0$
- $0 \notin S$ To use well-ordering we need S non-empty
  - If $a < 0$ then $a - b(2a) = a \cdot (1 - 2b) \in S$ since $b > 0$ and $a < 0$
  - If $a \geq 0 \Rightarrow a - b \cdot 0 \in S$

$\therefore$ S is non-empty

$\therefore$ By the well-ordering Principle S must have a smallest element

Say $r = a - bq$

Show that $r < b$

Suppose that $r \geq b$, then

$$a - b(q+1) = a - bq - b = r - b \geq 0$$

But this $\Rightarrow$ $a - b(q+1) \in S$ but $a - b(q+1) \leq a - bq = r$

but r is least element $\therefore$ Contradiction.

Show uniqueness:

Suppose r, r', q, q' s.t. $a = bq + r$ $\quad 0 \le r < b$

and $a = bq' + r'$ $\quad 0 \le r' < b$

$\Rightarrow \quad bq + r = bq' + r'$

$\downarrow$

we may assume $r' \ge r$

$b(q - q') = r' - r$

$\therefore$ b divides $r' - r$ and $0 \le r' - r \le r' < b$

$\Rightarrow r' - r < b$

and b divides $r' - r$

$\Rightarrow r' - r = 0$

$r' = r$

$\therefore q = q'$

$\therefore$ unique.

$\blacksquare$

Let $a, b \in \mathbb{Z}$

- d is a common divisor of a, b if $d | a$ and $d | b$

d divides a

greatest common divisor

$\gcd(a,b) = d$ s.t all other common divisors of a, b also divide d

- if $\gcd(a,b) = 1 \Leftrightarrow a, b$ are relitively prime

Theorem 2.10. *Let a and b be nonzero integers. Then there exist integers r and s such that*

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Corr) If a, b relitivly prime then $\exists$ r, s s.t

$$1 = ar + bs$$

This gives Euclidean Alg.

Primes

- p is a prime number if only $1 | p$ and $p | p$.

Lemma1

Let $a, b \in \mathbb{Z}$ p prime If $p | ab$ then either

$p | a$ or $p | b$.

Thorem:

$\exists$ infinite number of primes

Therem 2.15 (Fundemental Theorem of Arithmetic)

$a = p_1 \cdots p_n$ for $p_1, \ldots, p_n$ prime
can be repitition of p_j's.

and this is unique.

Groups

Informal Definition :

A Group is a set which is closed under an associative operation s.t. $\exists$ an identity element and inverse

i.e. if $a, b, c \in G$ ← Group $\quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$

The Integers mod n

Recall that $a \equiv b \pmod{n}$ iff $a - b = k \cdot n$ for some $k \in \mathbb{Z}$

- Integers mod n partition $\mathbb{Z}$ into n different eq. classes

- $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$ (Additive group)

- i.e. $\mathbb{Z}_{12}$ = integers mod 12

$$[0] = \{ \ldots, -12, 0, 12, 24, \ldots \}$$

$$\vdots$$

$$[11] = \{ \ldots, -1, 11, 23, 35, \ldots \}$$

by convention $\mathbb{Z}_{12} = \{0, \ldots, 11\}$

- Note addition and multiplication are defined mod n

$(a + b) \bmod n$

$(a \cdot b) \bmod n$

Ex 1

$7+4 = 1 \pmod 5$ $\qquad$ $7 \cdot 3 = 1 \pmod 5$

$3+5 = 0 \pmod 8$ $\qquad$ $3 \cdot 4 = 0 \pmod{12}$

Note Product of non-zero things can be zero

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

1 is multiplicative identity

Table 3.3: Multiplication table for $\mathbb{Z}_8$

$\mathbb{Z}_8$ is a Group under addition but not multiplication

Proposition 3.4. *Let $\mathbb{Z}_n$ be the set of equivalence classes of the integers mod n and $a, b, c \in \mathbb{Z}_n$.*

1. *Addition and multiplication are commutative:*

$$a + b \equiv b + a \pmod n$$
$$ab \equiv ba \pmod n.$$

2. *Addition and multiplication are associative:*

$$(a + b) + c \equiv a + (b + c) \pmod n$$
$$(ab)c \equiv a(bc) \pmod n.$$

3. *There are both additive and multiplicative identities:*

$$a + 0 \equiv a \pmod n$$
$$a \cdot 1 \equiv a \pmod n.$$

4. *Multiplication distributes over addition:*

$$a(b + c) \equiv ab + ac \pmod n.$$

5. *For every integer a there is an additive inverse $-a$:*

$$a + (-a) \equiv 0 \pmod n.$$

6. *Let a be a nonzero integer. Then $\gcd(a, n) = 1$ if and only if there exists a multiplicative inverse b for $a \pmod n$; that is, a nonzero integer b such that*

$$ab \equiv 1 \pmod n.$$