Number Theory

Theory

All variables below stand for integers.

Def. If $b = aq$, then we say that a **divides** b, and write $a|b$, or that b is **divisible** by a, and we write $b \vdots a$.

Fundamental properties.

- $a|b$, $b|c \Rightarrow a|c$.
- $a|b$, $a|c \Rightarrow a|b \pm c$. More generally, $a|bx + cy$ for all x and y.

Def. For every pair a, b there exist unique q and r such that

$$a = bq + r, \qquad 0 \leq r < b.$$

q and r are called **quotient** and **remainder** upon division of a by b.

- If two numbers have the same remainder upon division by b, then they can be written as $bq_1 + r$ and $bq_2 + r$. Their difference is $b(q_1 - q_2)$, and thus it is divisible by b.
- Note that when we divide by b, there are b possible remainders. Thus given $b + 1$ numbers, there are at least 2 numbers with the same remainder. Their difference is divisible by b.

Def. The largest number that divides both a and b is called **the greatest common divisor** of a and b, and is denoted by (a, b).

- $(a, a) = a$, $(a, 1) = 1$, $(a, 0) = a$, $(a, b) = (b, a)$.

Def. A number is called **prime** if it has exactly two divisors, 1 and itself. An integer that is not prime is called composite.

- There are infinitely many primes.

Euclid's lemma. If p is prime, $p|ab$, then either $p|a$ or $p|b$.

Fundamental theorem of arithmetic. Every positive integer can be uniquely represented as a product of primes (uniquely up to order of the multiples).

Def. a and b are called **relatively prime** or coprime if $(a, b) = 1$.

Theorem. For any pair a, b, there exist integers x and y such that $ax + by = (a, b)$.

Special case: If a and b are relatively prime, then there exist x and y such that $ax + by = 1$.

Def. We say that a and b are **congruent** mod m, and write $a \equiv b (\text{mod } m)$ if $m|(a - b)$. Equivalently, $a - b = mq$ for some q, or $a = b + mq$, or a and b have the same remainder upon division by m.

Example: $12 \equiv 7 (\text{mod } 5)$ because they have the same remainder upon division by 5.

- Congruences can be added, subtracted, and multiplied: if $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$, then $a \pm c \equiv b \pm d (\text{mod } m)$ and $ac \equiv bd (\text{mod } m)$
- Cancellation rule: if $(c, m) = 1$, $ca = cb (\text{mod } m)$, then $a \equiv b (\text{mod } m)$.

Fermat's theorem. If p is prime, then $a^p \equiv a (\text{mod } p)$.
Corollary: if p is prime and $p \not| a$, then $a^{p-1} \equiv 1 (\text{mod } p)$.

Examples: $p = 5$. $1^4 = 1 \equiv 1 (\text{mod } 5)$, $2^4 = 16 = 1 \equiv 1 (\text{mod } 5)$, $3^4 = 81 = 1 \equiv 1 (\text{mod } 5)$, $4^4 = 256 = 1 \equiv 1 (\text{mod } 5)$.

Useful formulas.

- $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$
- if n is odd, $a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \ldots + (-1)^{n-2}ab^{n-2} + (-1)^{n-1}b^{n-1})$