Number Theory

- Properties of numbers. It's considered the most beautiful area in maths.
- Much of modern maths was developed to answer number theory questions.

Basics

- [Integer division] Lemma: Given numbers $a, b \in \mathbb{Z}$, we can uniquely find $a = qb + r$, s.t. $q, r \in \mathbb{Z}$ & $0 \leq r < b$ (Assume $b > 0$.).

Pf: - Existence: Follows from long division.

- Unique: $a = qb + r = q'b + r'$.

$\Rightarrow$ $b \mid (r - r')$ [i.e. b divides $r - r'$].

& $|r - r'| < b$.

$\Rightarrow$ $r - r' = 0$ $\Rightarrow$ unique r. □

- Defn: • b divides a, if $r = 0$.
  or $b \mid a$.

- Ex. $7 \nmid 101$, $7 \mid 105$.

• GCD of a, b, denoted $\gcd(a,b)$, is the largest $c \in \mathbb{N}$ s.t. $c \mid a$ & $c \mid b$.

• If $(a,b) = 1$ then we say a & b are coprime.

-Ex. $(5,11) = (5, 5\times2+1) = (5,1) = (5\times1+0,1) = (0,1)$

$(5,12) = (5, 5\times2+2) = (5,2) = (2\times2+1,2)$

$= (1,2) = (1, 2\times1+0) = (1,0)$.

$(6,9) = (6, 6\times1+3) = (6,3) = (3\times2+0,3) = (0,3)$

$= 3$.

▷ $(a \geq b) = (qb+r, b) = (r < b)$. [Exercise]

Euclid's gcd algorithm (~300 B.C.): gcd$(a \geq b)$:

- if $b =? 0$ then OUTPUT a.
- if $b =? 1$ " " 1.
- Compute $a =: bq+r$. OUTPUT gcd(b,r).

Exercise: Prove its correctness, by induction.

The underlying equations are:

$$\gcd(a,b) \to a =: q_1 \times b + r_1 .$$
$$\gcd(b,r_1) \to b =: q_2 \times r_1 + r_2 .$$
$$\vdots$$
$$\gcd(r_{k-1}, r_k) \to r_{k-1} =: q_{k+1} \times r_k + \underline{0}$$
$$\gcd(r_k, 0) \to r_k .$$

Theorem (Bézout's identity): $\exists\, \alpha, \beta \in \mathbb{Z}$ s.t.

$$\gcd(a,b) = \alpha \cdot a + \beta \cdot b .$$

Pf: • $r_1 = a - q_1 \cdot b$

• $r_2 = b - q_2 \cdot r_1 = b - q_2 \cdot (a - q_1 \cdot b)$

$= (-q_2)\, a + (1 + q_2 q_1) \cdot b$

(by induction on k):

• $r_k = \alpha \cdot a + \beta \cdot b \; ; \; \alpha, \beta \in \mathbb{Z}$.

□

▷ [Extended Euclid gcd algorithm] α, β are (efficiently) computable.

Ex.: If a, b are n-bits, how large can k be? [$2n$?] [Construct an eg.]

▷ $(a,b) = \alpha\cdot a + \beta\cdot b$

[Reduction] $= (\alpha + s\cdot b)\cdot a + (\beta - sa)\cdot b$.

Theorem (Unique Bézout's id.): Let $a > b > 0$,

$\exists$ **unique** α, β : $(a,b) = \alpha\cdot a + \beta\cdot b$,

where $0 \le \alpha < b'$ & $\underline{a'} := \frac{a}{(a,b)}$, $\underline{b'} := \frac{b}{(a,b)}$.

$-a' < \beta \le 0$

Pf: • a', b' are the coprime parts.

• By Euclid, $\exists\, \alpha, \beta$: $\alpha a' + \beta b' = 1$

– W.l.o.g. assume $0 \le \alpha < b'$ [By Reduction]

$\Rightarrow |\beta b'| = |1 - \alpha a'| < |b' a'| \Rightarrow |\beta| < a'$.

• [Uniqueness] Suppose $(a,b) = \alpha_1 a + \beta_1 b = \alpha_2 a + \beta_2 b$

$\Rightarrow (\alpha_1 - \alpha_2) a' = (\beta_2 - \beta_1) b' \Rightarrow b' \mid (\alpha_1 - \alpha_2) a'$.

• We've $|\alpha_1 - \alpha_2| < b' \overset{?}{\Longrightarrow} \alpha_1 - \alpha_2 = 0 = \beta_1 - \beta_2$

(cancel)

Claim: $(m,n) = 1$ & $m \mid n\alpha \Rightarrow m \mid \alpha$.

Pf: • Bézout's $\Rightarrow$ $u \cdot m + v \cdot n = 1$

$\Rightarrow$ $u \cdot m \cdot \alpha + v \cdot n \cdot \alpha = \alpha$

$\Rightarrow$ $m \mid \alpha$. □

$\Rightarrow (\alpha_1, \beta_1) = (\alpha_2, \beta_2) \Rightarrow (\alpha, \beta)$ is unique. □

- Fundamental theorem of arithmetic:

Thm (Unique factorization): $\forall n \in \mathbb{N}$, $\exists\, 2 \le p_1 < \cdots < p_k$ primes: $n = \prod_{i=1}^{k} p_i^{e_i > 0}$, in a unique way.

Pf: · [Existence]: Either n is prime or n has largest prime $\le n/2$. $\Rightarrow$ Gives $n = \prod_i p_i^{e_i}$.

· [Uniqueness] $n = \prod_{i=1}^{k} p_i^{e_i} = \prod_{j=1}^{\ell} q_j^{f_j}$.

$\Rightarrow$ (Cancellation) $p_1 = q_1$ & $e_1 = f_1$,

——, $p_\ell = q_\ell$ & $e_\ell = f_\ell$.

$\Rightarrow$ Uniqueness of factors. □

- We can study numbers via primes (& prime-powers).

Modular Arithmetic

- Eg. Sunday is the first day. What is the 184th day? Mod 7?
- Last digit of $2^{2^{100}}$? Mod 10?
  - ↳ Impossible to store/compute
  - ↳ But we can work with $\{0,1,\to 9\}$.
- **Defn:** • $r_d(n)$:= remainder of n/d.
  - Eg. $r_{10}(n)$, $n := 2^{2^{100}}$.

▷ $r_d(ab) = r_d(r_d(a) \cdot r_d(b))$.

Pf: • $a = d \cdot q_1 + r_d(a)$
• $b = d \cdot q_2 + r_d(b)$
• $ab = d \cdot q_3 + r_d(ab)$

$\Rightarrow ab = d \cdot (-) + r(a) \cdot r(b)$

& $r_d(\cdot) \in [0 \dots d-1]$. $\Rightarrow$ done! □

Given n: $\forall a, b \in \mathbb{Z}$:

- Defn: $a \equiv b \bmod n$ if $n \mid (a-b)$.

▷ "mod n" is an equivalence relation of $\mathbb{Z}$.

- Ex. $a \equiv b \bmod n \overset{?}{\iff} a = b$. (If $|a-b| < n$.)

- Ex. $r_{10}(2^{64})$: $2^8 \equiv 6 \mod 10$

$\Rightarrow 2^{8\times 2} \equiv 36 \equiv 6 \mod 10$

... $\Rightarrow 2^{64} \equiv 6 \mod 10$.

... $\Rightarrow 2^{2^n} \equiv 6 \mod 10$, $\forall n \geq 2$.

[The notation invented by Gauss, 1800s]

▷ $a \equiv b \mod n \iff \exists k : a = b + kn$. ← AP!

- Defn: $\{b+kn \mid k \in \mathbb{Z}\}$ is the residue class of $b \mod n$.

▷ $\forall n$, $\mathbb{Z}$ partitions into n residue classes mod n.

- **Defn:** • The residue classes are $0, 1, \to n-1$.
  • We call it $\mathbb{Z}/n := \{0, 1, \to n-1\}$.

▷ $\forall a, b \in \mathbb{Z}/n$: (i) $a \bmod n + b \bmod n \equiv (a+b) \bmod n$

- eg. $1 + (n-1) \equiv n \equiv 0 \bmod n$.

(ii) $(a \bmod n) \cdot (b \bmod n) \equiv (ab \bmod n)$.

- eg. $2 \cdot (n-1) \equiv -2 \equiv n-2 \bmod n$.

- eg. $2^{39} \bmod 10 \equiv 2^{32+4+2+1} \equiv 6 \cdot 2^2 \cdot 2^1 \equiv 6 \cdot 8 \equiv 8$.

Qn: What's division mod n?

- Undefined. eg. $1/2 \bmod 10 =: x \in \mathbb{Z}/10$.

$\Rightarrow 1 \equiv 2x \bmod 10$

$\Rightarrow 5 \equiv 0 \bmod 10 \Rightarrow$ ↯

$\Rightarrow \nexists\, 2^{-1} \in \mathbb{Z}/10$.

▷ $m^{-1} \bmod n$ doesn't exist, if m/n.

→ if $(m,n) \neq 1$.

- eg. $3^{-1} \bmod 10 \equiv 7$. [∵ $3 \times 7 \equiv 21 \equiv 1$]

▷ $\mathbb{Z}/n$ may not have "cancellation rule", i.e.

$a \cdot b \equiv 0 \not\Rightarrow a \equiv 0 \vee b \equiv 0$.

$a \cdot b \equiv a \cdot c \not\Rightarrow a \equiv 0 \vee b \equiv c$.

- Eg. $5^n \bmod 10 \equiv 5$ [$\because 5^2 \equiv 5$]
- $n = x_r x_{r-1} \cdots x_0$ in base-10.

$n \bmod 9 \equiv x_r + x_{r-1} + \cdots + x_0$

[$\because n = x_r 10^r + x_{r-1} 10^{r-1} + \cdots + x_0 \equiv \sum_i x_i$.]

$n \bmod 2 \equiv x_0$.

$n \bmod 11 \equiv \sum_i x_i \cdot (-1)^i$.

- Ex: • Find $(x,y) \in \mathbb{Z}^2$: $25x + 31y = 6$.
  • Find $(x,y) \in \mathbb{Z}^2$: $x^2 - 2y^2 = 1$.

Solving linear equations in $\mathbb{Z}/n$

- How do you solve $ax \equiv b \bmod n$?
  → If $a^{-1} \bmod n$ exists, then $x \equiv ba^{-1} \bmod n$.

Lemma: $a^{-1} \bmod n$ is easy to compute (or say that it doesn't exist) & is unique.

Pf: . Use Euclid gcd algo. to write:

$$(a,n) =: \ell \cdot a + k \cdot n \Rightarrow \ell \cdot a \equiv (a,n) \bmod n$$

- If $(a,n) = 1 \Rightarrow \ell \equiv a^{-1} \bmod n$.
- Say, $(a,n) =: g > 1 : \Rightarrow$ $a^{-1} \bmod n$ doesn't exist!

- Suppose $ax \equiv 1 \mod n$

$\Rightarrow \left(\frac{n}{g}\right) \cdot ax \equiv \left(\frac{n}{g}\right) \cdot 1 \mod n$

$\Rightarrow 0 \equiv (n/g) \mod n \Rightarrow$ ↯

$\Rightarrow a^{-1} \mod n$ doesn't exist. □

$ax_1 \equiv 1 \equiv ax_2$
$\Rightarrow a(x_1 - x_2) \equiv 0$
$\Rightarrow x_1 - x_2 \equiv 0 \mod n.$
$\Rightarrow$ uniqueness.

- Defn: · Given coprime (a, n), we use $(a^{-1} \mod n)$ to denote the unique inverse.

▷ n is prime & $n \nmid a$ $\Rightarrow (a, n) = 1 \Rightarrow a^{-1} \mod n$ exists.
$(a \not\equiv 0 \mod n)$

- Egs. $2^{-1} \bmod 11 \equiv 6$

$16^{-1} \bmod 13 \equiv 3^{-1} \equiv 9$

$92^{-1} \bmod 23 \equiv 0^{-1} \Rightarrow$ ↯.

- Ex: $25^{-1} \bmod 23$ using Euclid gcd algo.

Theorem (Fermat's little theorem, 1640): For prime p & $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$.

Pf: • $S := \{a, 2a, 3a, \ldots, (p-1)a\} \bmod p$.

• Consider $\prod_{i \in [p-1]} (ia) = ?$

▷ $ia \equiv ja \bmod p \Rightarrow i \equiv j \bmod p$ [$\Rightarrow |S| = p-1$]

[Pf: Say, $ia \equiv ja \Rightarrow (i-j)a \equiv 0 \mod p$

$\Rightarrow i-j \equiv 0.$]

▷ $S = [p-1] = (\mathbb{Z}/p) \setminus \{0\}.$

$\Rightarrow$

▷ $a \cdot 2a \cdot 3a \cdots (p-1)a \equiv (p-1)! \mod p.$

$\Rightarrow a^{p-1} \cdot (p-1)! \equiv$ "

$\Rightarrow a^{p-1} \equiv 1 \mod p.$ □

- Q: $a^n \equiv a \mod n$? for composite n?

- e.g. $n=4, a=3$: $3 \not\equiv 3^4 \equiv 1 \mod 4$

$2 \not\equiv 2^4 \equiv 0 \mod 4$

- Qn: Computing $a^n \bmod n$?

▷ Easy to compute by repeated → squaring & mod n arithmetic.

- Back to $ax \equiv b \bmod n$:

1) Compute $(a,n) =: g$ [Euclid gcd]
2) If $g=1$ OUTPUT $x \equiv (ba' \bmod n)$
3) [$g \geq 2$] $(a/g) \cdot x \equiv (b/g) \bmod (n/g)$
   3.1) If $g \nmid b$ then OUTPUT Fail.
   3.2) $a' \cdot x' \equiv b' \bmod n'$ [$(a', n') = 1$]
   3.3) Compute $x' \equiv b'/a' \bmod n'$ [$\Rightarrow ax' \equiv b \bmod n$]
3.4) OUTPUT $\{x' + k \cdot n', \ 0 \leq k < g\}$.

Euler's Totient Function $\varphi(n)$

- Numbers coprime to n, in $(\mathbb{Z}/n)$.
- **Defn:** • $(\mathbb{Z}/n)^* := \{ a \in \mathbb{Z}/n \mid (a,n)=1 \}$.
  • $\varphi(n) := |(\mathbb{Z}/n)^*|$.

- Eg. $\varphi(1) := 1 = \varphi(2)$, $\varphi(3) = 2 = \varphi(4) = \varphi(6)$
  $\varphi(5) = 4$.

▷ $\varphi(n) = n-1$, if n is prime (>1).

▷ For $n>2$, $\varphi(n) \geq 2$.

- $\varphi(n) = \varphi(n') \not\Rightarrow n = n'$.

▷ $\varphi(p^2) = p^2 - \#\{a \in \mathbb{Z}/p^2 \mid (a, p^2) > 1\}$

$= p^2 - p.$

▷ $\varphi(p^k) = p^k - p^{k-1} = p^k \cdot \left(1 - \frac{1}{p}\right)$; $k \geq 1$ & p prime.

Qn: For primes $p \neq q$, $\varphi(pq) \overset{=:n}{=} \varphi(p)\varphi(q)$?

Theorem (Multiplicative): If $(m, n) = 1$, then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Pf: • $(\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^* \xrightarrow{\Psi} (\mathbb{Z}/mn)^*$ [bijection ?]

$(a, b) \longmapsto \psi(a,b) =: c$

Idea: $\psi(a, b) := na + mb \mod mn$.

(i) ψ is a valid map: $na+mb \bmod mn$ doesn't change as long as we pick classes a & b.

- $na+mb \in (\mathbb{Z}/mn)^*$:

[Suppose not. $(na+mb, m) = g$.

$\Rightarrow (na, m) = g \Rightarrow (a, m) = g$

$\Rightarrow g = 1$.]

(ii) ψ is injective : Suppose $na+mb \equiv na'+mb' \bmod mn$.

$\Rightarrow n(a-a') \equiv m(b'-b) \bmod mn$

$\Rightarrow m \mid n(a-a') \Rightarrow m \mid (a-a') \Rightarrow \cdots$

$(a, b) \equiv (a', b') \in (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$.

(iii) ψ is surjective: Pick $c \in (\mathbb{Z}/mn)^*$.

Qn: Find (a,b) : $\psi(a,b) = c$?

$$na + mb \equiv c \mod mn.$$

$[\mod m]$: $na \equiv c \mod m \Leftrightarrow a \equiv c/n \mod m$

$\Rightarrow$ $mb \equiv c - na \mod mn$. $\Rightarrow$ a found.

$\Rightarrow$ $b \equiv \left(\frac{c-na}{m}\right) \mod n \Rightarrow b$ found.

[Check: $a \in (\mathbb{Z}/m)^*$ & $b \in (\mathbb{Z}/n)^*$.]

$\Rightarrow$ ψ is a bijection.

$\Rightarrow$ $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

□

Corollary: If $n = \prod_i p_i^{e_i}$ is the prime factorization then

$$\varphi(n) = \prod_i \varphi(p_i^{e_i})$$

$$= \prod_i p_i^{e_i}\left(1-\frac{1}{p_i}\right) = n \cdot \prod_i \left(1-\frac{1}{p_i}\right).$$

$$\Rightarrow \varphi(n)/n = \prod_{\text{prime } p \mid n}\left(1-\frac{1}{p}\right). \quad [n =: p_1^{e_1} \cdots p_\ell^{e_\ell}]$$

- Alternate proof is by inclusion-exclusion:

$$\varphi(n) = \sum_{I \subseteq [\ell]} (-1)^{|I|} \cdot \left(\frac{n}{\prod_{i \in I} p_i}\right)$$

$$=: \sum_{d \mid n} \mu(d) \cdot \frac{n}{d}$$

where Möbius Function μ is defined as:

$$\mu(k) := \begin{cases} (-1)^r, & \text{if } k = \text{product of } r \text{ primes} \\ 0, & \text{else} \\ 1, & k=1 \end{cases}$$

Theorem (Euler, 1736): $\forall a \in (\mathbb{Z}/n)^*$,
$a^{\phi(n)} \equiv 1 \mod n$.

Pf: · Redefine $S := \{a \cdot b \mid b \in (\mathbb{Z}/n)^*\}$.
· What's $\Pi\{s \in S\} \equiv ? \mod n$?

$$\equiv \quad a^{\varphi(n)} \cdot \prod \{ b \in (\mathbb{Z}/n)^* \}$$

$$[\triangleright \ \forall s \in S, \ s \in (\mathbb{Z}/n)^* .$$
$$\triangleright \ \forall b \neq b', \quad ab \not\equiv ab' \bmod n. \ ]$$

$$\equiv \quad \prod \{ b \in (\mathbb{Z}/n)^* \}$$

$$\Rightarrow \quad a^{\varphi(n)} \equiv 1 \bmod n. \qquad \square$$

More linear equations (over $\mathbb{Z}/n$)

- How to solve: $(a_1 x \equiv b_1 \bmod m) \wedge (a_2 x \equiv b_2 \bmod n)$?

- e.g. $x \equiv 1 \bmod 4 \wedge x \equiv 2 \bmod 6 \Rightarrow$ ↯

- So, $(m,n)>1$ creates a problem. What if $(m,n)=1$?

- Further, assume $a_i = 1$, $\forall i$; i.e.

$$x \equiv b_1 \bmod m \ \wedge \ x \equiv b_2 \bmod n.$$

- Assume $(m,n)=1$:

Theorem 1 (Chinese Remainder thm, ~300 AD): An $x \in \mathbb{Z}$ exists. Moreover, $x \bmod mn$ is unique!

Pf: • Consider $\psi' : \mathbb{Z}/m \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/mn$

$$(b_1, b_2) \longmapsto \psi'(b_1, b_2) \bmod mn$$

- Previously, $\psi(b_1, b_2) = b_1 n + b_2 m$.

- To correct ψ we redefine ψ' as:

$$\psi'(b_1, b_2) := b_1 \cdot n \cdot (n^{-1} \bmod m) + b_2 \cdot m \cdot (m^{-1} \bmod n)$$

▷ $\equiv b_1 \bmod m$

$\equiv b_2 \bmod n$

$\Rightarrow$ x has solution $\psi'(b_1, b_2)$.

▷ Moreover, ψ' is a bijection!

$\Rightarrow$ $x \bmod mn$ is unique ($\because \psi'$ injective). □

Exercise: Set of modular linear equations can be solved efficiently.

Theorem 2 (CRT): Let $n_1, n_2, \ldots, n_k$ be mutually coprime integers. Then, the system

$$x \equiv c_i \bmod n_i \,, \quad \forall i \in [k]$$

has a unique solution $x \bmod \prod_i n_i$ (& can be easily computed).

Pf:

Idea: $\psi'(c_1, \ldots, c_k) := \left(\sum_{j=1}^{k} c_j \cdot N_j\right) \Big/ \left(\sum_{j=1}^{k} N_j\right) \bmod N.$

where $N := \prod_{i=1}^{k} n_i$; $N_j := N / n_j$.

- Complete the pf.

□