Euclidean Algorithm.

1) $a, b \in \mathbb{Z}$, $b > 0$. Then $\exists\, q \in \mathbb{Z}$, $r \in \mathbb{Z}$, $0 \leq r < b$ such that $a = qb + r$.

2) $r = 0 \iff b \mid a$.

3) Prime : n that has only two divisors, namely $1, n$.

4) Fundamental theorem of Arithmetic (FTA)

Every $n \in \mathbb{N}$ can be written as a product of primes which is unique upto re-ordering.

$$n = p_1 p_2 \cdots p_k \quad , \quad p_j \text{ are prime.}$$

Ex 1 : Induction to reduce to the case

$p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Assume that $p \nmid a \underset{p \text{ prime}}{\iff} GCD(p, a) = 1$

Bezout's lemma $\Rightarrow \exists\, x, y$ s.t. $ax + py = 1$

$\Rightarrow abx + pby = b \Rightarrow p \mid b$

Bezout's lemma : Let $a, b \in \mathbb{Z}$. Then TFAE

1) $GCD(a, b) \mid d$.

2) $\exists\, x, y \in \mathbb{Z}$, s.t. $ax + by = d$.

Congruence

Def: $a \equiv b \mod n \iff n \mid a-b$

Notation: 1) $\mathbb{Z}/N\mathbb{Z} = \{0, 1, \dots, N-1\}$

$N+1 \equiv 1 \mod N$ $\quad$ ~~$[\ ]$~~$_N$

2) $\mathbb{Z}/N\mathbb{Z}^{\times} = \{a \in \mathbb{Z}/N\mathbb{Z} \mid a^{-1} \mod N \text{ exists}\}$

$= \{a \in \mathbb{Z}/N\mathbb{Z} \mid GCD(a, N) = 1\}$

Ex 3: As $p \nmid a \iff GCD(p, a) = 1$

$\iff \exists\, b$ s.t. $ab \equiv 1 \mod p$.

We need show that $ra \not\equiv sa \mod p$.

for $r \not\equiv s$, $1 \le r, s \le p-1$.

$ra \not\equiv sa \iff r\underbrace{ab}_{1} \not\equiv s\underbrace{ab}_{1} \iff r \not\equiv s \mod p$

Chinese Remainder theorem

Ex 5:
$x \equiv 1 \mod 2$
$x \equiv 4 \mod 5$
$x \equiv -2 \mod 7$

$GCD(2, 5) = 1 \qquad 1 = 2 \times 3 + 5 \times (-1)$

$x \equiv 4 \times 2 \times 3 + 1 \times 5 \times (-1) = 19 \mod 10$

Repeat the process with $x \equiv -2 \mod$

Ex 4 : $GCD(m,n) = 1$ $\exists x, y$.

$\Rightarrow mx + ny = 1$

$\Rightarrow mxa + nya = a$

$\cancel{\Rightarrow a(mx+ny) = a}$

$\Rightarrow$ As $m | a$ $\cancel{\Rightarrow m | nya}$ $a = mk$

$n | a$ $\Rightarrow a = nl$.

$\Rightarrow mx \times nl + ny \times mk = a$.

$\Rightarrow mn(xl + yk) = a \Rightarrow mn | a$

Different sol: $a = mk$.

$= p_1 \cdots p_r k$.

$a = nl = q_1 \cdots q_s l$.

As $GCD(m,n) = 1 \Rightarrow q_i \nmid p_j \Rightarrow q_i | k$

$\Rightarrow k = q_1 \cdots q_s y$.

$\Rightarrow a = \underbrace{p_1 \cdots p_r}_{m} \underbrace{q_1 \cdots q_s}_{n} y$

Euler's totient function

Def: $\varphi(N) := \# \{ a \mid 1 \le a \le N, \ GCD(a, N) = 1 \}$

$= \# (\mathbb{Z}/N\mathbb{Z})^\times$

Properties

1) $\varphi(p) = p-1$ $\quad$ p prime

2) $\varphi(p^k) = p^{k-1}(p-1)$ $\quad$ $k \in \mathbb{N}$, p prime

3) $\varphi(mn) = \varphi(m)\varphi(n)$ $\quad$ $GCD(m,n) = 1$

4) $\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$ $\quad$ $n \in \mathbb{N}$.

Ex 2: $\cancel{n}$ FTA $\Rightarrow n = p_1^{k_1} \cdots p_r^{k_r}$

for some distinct primes $p_1, \dots, p_r$ and $k_1, \dots, k_r \in \mathbb{N}$.

$$n^k = p_1^{k_1 k} p_2^{k_2 k} \cdots p_r^{k_r k}$$

$$\varphi(n^k) \overset{(4)}{=} n^k \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

$$\varphi(n) \overset{(4)}{=} n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

$$\frac{\varphi(n^k)}{\varphi(n)} = \frac{n^k}{n} = n^{k-1} \Rightarrow \varphi(n^k) = n^{k-1}\varphi(n)$$

Fermat's little theorem (FLT)

Let $p \nmid a \Leftrightarrow GCD(p, a) = 1$. Then

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

Generalized FLT

Let $n \in \mathbb{N}$, $GCD(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Order: We call e to be the order of z mod n if

1) $z^e \equiv 1 \mod n$.

2) e is the minimal positive number s.t. $z^N \equiv 1 \mod n$.

Primitive root: We call z to be a primitive root mod p if the order of z is $p-1$.

Q: Let $GCD(z, n) = 1$. What is the inverse of z mod n?

Ans: GFLT $\Rightarrow$ $z^{\varphi(n)} \equiv 1 \mod n$.

$\Rightarrow$ $z \times z^{\varphi(n)-1} \equiv 1 \mod n$

$\Rightarrow$ $z^{\varphi(n)-1}$ is the inverse of z mod n.

Ex 8: $z^e \equiv 1 \Rightarrow z \times z^{e-1} \equiv 1 \mod n$.

$\Rightarrow$ z^{e-1} is the inverse of z.

$\Rightarrow$ z is invertible $\Leftrightarrow$ $GCD(z, n) = 1$

Main theorem: The numbers of $z \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order d is $\varphi(d)$.

RMK: If $z^e \equiv 1 \mod p$ then $e(z) \mid e$

Quadratic residue

$p > 2$ prim[e]

Def: We call "a" to be a quadratic residue mod p $(p \nmid a)$ if $\exists\ x$ to $x^2 \equiv a \mod p$.

Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ +1 & \text{if } p \nmid a \text{ and } a \text{ is quad. res.} \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is quad non-re[s.]} \end{cases}$$

Properties: 1) If $a \equiv b \mod p$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

5) Gauss's reciprocity: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

Ex 18: $\left(\frac{a^2 b}{p}\right) \underset{2)}{=} \left(\frac{a^2}{p}\right)\left(\frac{b}{p}\right)$ $\quad p \nmid ab$

But $\left(\frac{a^2}{p}\right) = 1$ because a^2 is obviously a quadratic residue.

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^2 = 1$$

Ex 17: $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) = 0$.

Theorem: Every $x \in \mathbb{Z}/p\mathbb{Z}^{\times}$ can be written as z^j for some $z \in \mathbb{Z}/p\mathbb{Z}^{\times}$ and $0 \le j \le p-2$.

$\left(\frac{x}{p}\right) = 1 \iff \left(\frac{z^j}{p}\right) = 1 \iff j = \text{even}$

$\left(\frac{x}{p}\right) = -1 \iff \left(\frac{z^j}{p}\right) = -1 \iff j = \text{odd}$.

We know that $\left(\frac{z}{p}\right) = -1$.

$\left(\frac{z^j}{p}\right) = \left(\frac{z}{p}\right)^j = (-1)^j$.

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}^{\times}} \left(\frac{x}{p}\right) = \sum_{j=0}^{p-2} \left(\frac{z^j}{p}\right) = \sum_{j=0}^{p-2} (-1)^j = 0$$

There are $\frac{p-1}{2}$ many even j in $[0, p-2]$

— — $\frac{p-1}{2}$ — odd j — —

Euler's criterion: If $\gcd(a,p) = 1$ then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Corollary to Euler's criterion

1) If $p \equiv 3 \mod 4$ and $\left(\frac{a}{p}\right) = 1$ then $a^{\frac{p+1}{4}}$ is a solution to

$$x^2 \equiv a \mod p.$$

2) If $p \equiv 1 \mod 4$ and $\left(\frac{a}{p}\right) = -1$ then $a^{\frac{p-1}{4}}$ is a solution to

$$x^2 \equiv -1 \mod p.$$

Ex 15: As $29 \equiv 1 \mod 4$

$$\left(\frac{2}{29}\right) = (-1)^{\frac{29^2-1}{8}} = (-1)^{\frac{(29-1)(29+1)}{8}}$$

$$= (-1)^{\frac{28 \times 30}{8}} = -1.$$

$x = 2^{\frac{29-1}{4}} = 2^7 \mod 29$ is a solution

$= 128 \mod 29 \equiv 12 \mod 29.$

$x \equiv -12 \mod 29$ is a solution.

$29 \mid x^2 - 12^2 \Rightarrow 29 \mid (x+12)(x-12)$

$\Rightarrow 29 \mid x+12$ or $29 \mid x-12.$

Finite Continued fraction

$$[a; a_1, a_2, \dots, a_N]$$

$$= a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots \cfrac{1}{a_N}}}.$$

Lemma: Every rational number can be written as a finite continued fraction.

Proof uses Euclid's algorithm.

Lemma: Every irrational number can be written as an infinite continued fraction expansion.

Algorithm: $r \rightsquigarrow a = \lfloor r \rfloor$

$$\rho_1 = \frac{1}{r - a} \rightsquigarrow a_1 = \lfloor \rho_1 \rfloor$$

$$\rho_2 = \frac{1}{\rho_1 - a_1} \rightsquigarrow a_2 = \lfloor \rho_2 \rfloor$$

— - — -

$$r = [a; a_1, a_2, \dots]$$

Convergents: $r_n = [a; a_1, \dots a_n]$

$$= \frac{s_n}{t_n}, \quad GCD(s_n, t_n) = 1$$

Ex 20: Prove that if

$r = [a; a_1, a_2, \ldots]$ then

$r = [a; a_1, a_2, \ldots, a_{n-1}, \rho_n]$

Ans: Use induction.

Base case: $n = 1$. We need to show

$$r \overset{??}{=} [a; \rho_1] = a + \frac{1}{\rho_1}$$

$$= a + r - a = r$$

Inductive hyp: $r = [a; a_1, a_2, \ldots, a_{n-1}, \rho_n]$

We need to show that $r = [a; a_1, \ldots, a_n, \rho_{n+1}]$

$$[a; a_1, \ldots, a_n, \rho_{n+1}] = a + \cfrac{1}{a_1 + \cfrac{\vdots}{a_n + \cfrac{1}{\rho_{n+1}}}}$$

$$\rho_{n+1} = \frac{1}{\rho_n - a_n} \qquad = a + \cfrac{1}{a_1 + \cfrac{\cdots 1}{\cancel{a_n} + \rho_n - \cancel{a_n}}}$$

$$= [a; a_1, \ldots, a_{n-1}, \rho_n] = r$$

Def: $r_n = \dfrac{s_n}{t_n}$

Properties: 1) s_n & t_n are increasing sequences.

2) $GCD(s_n, t_n) = 1$

3) $r_n - r_{n-1} = \dfrac{(-1)^n}{t_n t_{n-1}}$

4) $r_0 < r_2 < r_4 \cdots < r < \qquad r_5 < r_3 < r_1$.

5) $r_n = \dfrac{s_n}{t_n}$ approximates r.

Ex 23: Find the continued fraction expansion of $\sqrt{n^2+1}$.

Ans: $n^2 < n^2+1 < \underbrace{n^2+2n+1}_{=(n+1)^2}$

$\Rightarrow \underset{n+1}{n} < \underset{n+1}{\sqrt{n^2+1}} < \underset{n+1}{n+1}$

$\Rightarrow \lfloor \sqrt{n^2+1} \rfloor = n = a$

$$P_1 = \frac{1}{\sqrt{n^2+1} - n} \times \frac{\sqrt{n^2+1}+n}{\sqrt{n^2+1}+n} = \sqrt{n^2+1}+n.$$

$\lfloor P_1 \rfloor = \underset{a_1}{\underset{"}{2n}}$ as $2n < n+\sqrt{n^2+1} < 2n+1$

$$P_2 = \frac{1}{\sqrt{n^2+1} - n} = P_1 \Rightarrow a_1 = a_2 = a_3 \cdots$$

$\Rightarrow \sqrt{n^2+1} = [n; \overline{2n}]$

Ex: $\sqrt{17} = [4; \overline{8}]$

Ex: Let $r = [a; a_1, a_2, a_3]$. What is the continued fraction expansion of $\dfrac{r}{5r+3}$?

Ex : If $r = [a; b]$

what is the expansion of $r+1$?

Ans $r = a + \frac{1}{b} \Rightarrow r+1 = a+1 + \frac{1}{b}$

$= [a+1; b]$

Ans : $\cancel{\frac{r}{5}}$ $\frac{r}{5r+3} = \frac{1}{5 + 3/r}$

$\cancel{= [0; 5}$ $= \frac{1}{3} \frac{1}{5/3 + 1/r}.$

$= \frac{1}{3} [0; \frac{5}{3}, r]$

$= \frac{1}{3} [0; \frac{5}{3}, a, a_1, a_2, a_3].$

$\frac{1}{r} = [0; a, b] = 0 + \frac{1}{a + \frac{1}{b}} = \frac{1}{r}.$

Diophantine approximation

Def: Let $r \in \mathbb{R} \setminus \mathbb{Q}$. A rational number $\frac{s}{t}$ is a good approximation to r if $\left|r - \frac{s}{t}\right| < \left|r - \frac{s'}{t'}\right|$ for any $\frac{s'}{t'}$ with $t' < t$.

Thm: For all irrational r the n'th convergents $r_n = \frac{s_n}{t_n}$ are good approximants

Thm: Let $r \in \mathbb{R} \setminus \mathbb{Q}$ and $s, t \in \mathbb{Z}$, $t > 0$ with $GCD(s, t) = 1$.

If $\left| r - \frac{s}{t} \right| < \frac{1}{2t^2}$ then $\frac{s}{t}$ is a convergent to r.

Pell's equation

$$x^2 - dy^2 = \pm 1, \quad d \text{ is square-free.}$$

Algorithm to solve:

1) $\sqrt{d} = [a; \overline{a_1, \ldots, a_\ell}]$ then the solutions are $(s_{\ell-1}, t_{\ell-1})$ ← Fund. Soln., $(s_{2\ell-1}, t_{2\ell-1})$, $(s_{3\ell-1}, t_{3\ell-1})$ ...

2) $(s_{\ell-1}, t_{\ell-1})$ is the fundamental solution. We write

$$v_n + w_n\sqrt{d} = \left(s_{\ell-1} + t_{\ell-1}\sqrt{d}\right)^n$$

$v_n, w_n \in \mathbb{Z}$. Then $v_n^2 - d w_n^2 = \pm 1$. In fact

$$v_n^2 - d w_n^2 = \left(s_{\ell-1}^2 - d\, t_{\ell-1}^2\right)^n$$

Ex 27: Let $\sqrt{d}$ has periodic continued fraction expansion with ~~Then~~ even period. Show that $x^2 - dy^2 = -1$ has no solution.

Ans: Theorem 48 $\Rightarrow (v_n, w_n) = (s_{n\ell-1}, t_{n\ell-1})$

we have $s_{n\ell-1}^2 - d\,t_{n\ell-1}^2 = (-1)^{n\ell}$.

As ℓ is even $(-1)^{n\ell} = 1 \quad \forall n \Rightarrow$

$v_n^2 - d w_n^2 = +1 \Rightarrow$ there is no solution to $x^2 - dy^2 = -1$.

Sums of squares

Prop: If $p \equiv 3 \mod 4$ then $x^2 + y^2 = p$ has no solution in (x, y).

Thm: If $\left(\frac{-1}{p}\right) = 1$ then p can be represented as a sum of two squares.

Hermite's algorithm

Step 1: Find z s.t. $z^2 \equiv -1 \mod p$.

Step 2: Compute convergents of $\frac{z}{p}$. Find n s.t. $t_n < \sqrt{p} < t_{n+1}$. Then $(t_n, p s_n - z t_n)$ is a solution to $x^2 + y^2 = p$

Algebraic numbers

A complex number a is called algebraic if $\exists$ $f(x) \in \mathbb{Q}[x]$ non-zero s.t. $f(a) = 0$.

Algebraic integers

A complex number a is called an algebraic integer if $\exists$ a monic $f(x) \in \mathbb{Z}[x]$ s.t. $f(a) = 0$.

Minimal polynomial

Given an algebraic number a, the minimal polynomial is the $f \in \mathbb{Q}[x]$, monic s.t. $f(a) = 0$ & f has the least degree.

Gauss's lemma

An algebraic number is an algebraic integer if and only if its minimal polynomial $\in \mathbb{Z}[x]$.

Quadratic numbers

$$\mathbb{Q}(\sqrt{d}) = \{ s + t\sqrt{d}, \quad s, t \in \mathbb{Q} \}$$

Integers ring of $\mathbb{Q}(\sqrt{d})$

$$= \mathbb{Z}[\sqrt{d}] \quad \text{if } d \equiv 2, 3 \bmod 4$$

$$= \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \quad \text{if } d \equiv 1 \bmod 4$$

Unit group of ring of integers

$$\mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Z}, \; a^2 - b^2 d = \pm 1 \right\}$$

We can find the unit group by solving the Pell's equation $a^2 - b^2 d = \pm 1$.