Number Theory

1. Divisibility and Congruence.

1.1. Divisibility.

1.1.1. Basic Concepts.

Notation: Integers - $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$. Naturals - $\mathbb{N} = \{0, 1, 2, \dots\}$

Well-ordering principle: (WOP): Every non-empty subset $S \subset \mathbb{N}$ contains a minimal element. Note: WOP $\Leftrightarrow$ Principle of mathematical Induction.

Definition: Have $x, y \in \mathbb{Z}$. Say x divides y if $\exists\, z \in \mathbb{Z}$ such that $y = xz$. Write $x | y$.

Remark: $x | 0$, $1 | x$ $\forall\, x \in \mathbb{Z}$.

Division Algorithm: Given $x \in \mathbb{Z}$, $y \in \mathbb{Z} \setminus \{0\}$, then there is a unique pair q, r such that $x = qy + r$, where $q \in \mathbb{Z}$ is the quotient, $r \in \{0, 1, \dots, y-1\}$ is the remainder.

1.1.2. Greatest Common Divisor.

Definition: Given $x, y \in \mathbb{Z}$, an integer $z \in \mathbb{Z}$ is a common $\left\{\begin{matrix}\text{divisor}\\ \text{multiple}\end{matrix}\right\}$ of x, y if $\left\{\begin{matrix} z|x \text{ and } z|y \\ x|z \text{ and } y|z \end{matrix}\right\}$.

Proposition: For $x, y \in \mathbb{Z} \setminus \{0\}$, there is a unique common divisor $d > 0$ of x, y divisible by all common divisors of x, y. Write $d = \gcd(x, y) = (x, y)$.

Note: $z | x \Leftrightarrow z | -x$. Thus, $\gcd(x, y) = \gcd(|x|, |y|)$.

Sketch Proof: Uniqueness: $\exists\, d, d' \Rightarrow d | d'$ and $d' | d \Rightarrow d = d'$, as $d, d' > 0$.

Existence: $S = \{ax + by : a, b \in \mathbb{Z},\ ax + by > 0\} \subset \mathbb{N}$. $|x| \in S \Rightarrow S$ non-empty.
By WOP, let d be the minimal element of S. If $z | x$, $z | y$, then z divides every element of $S \Rightarrow z | d$. Must show $d | x$, $d | y$.
Division algorithm $\Rightarrow x = qd + r$, $0 \le r < d$. So, $r = x - q(ax + by) \in S$, so $r = 0$ by minimality of d. So $d | x$. Similarly for $d | y$.

If $\gcd(x, y) = 1$, say that x is relatively prime to y, or that x, y are coprime.

1.1.3. Euclid's Algorithm.

This takes input : $x, y \in \mathbb{Z} \setminus \{0\} \longmapsto d = \gcd(x, y) = ax + by$ (a, b not unique).
In general we can assume that $x \geq y > 0$. We use the division algorithm.

Example: gcd(72, 20).

$$72 = 3.20 + 12$$
$$20 = 1.12 + 8$$
$$12 = 1.8 + 4 \quad \leftarrow \text{ so } \gcd(72,20) = 4.$$
$$8 = 2.4 + 0$$

And, $4 = 12-8 = 12-(20-12) = 2.12 - 20 = 2.(72-3.20) - 20 = 2.72 - 7.20.$

In general: $x_0 = x$, $x_1 = y$.

$$x_0 = q_0 x_1 + x_2, \quad x_1 > x_2$$
$$x_1 = q_1 x_2 + x_3, \quad x_2 > x_3$$
$$\vdots$$
$$x_{n-1} = q_{n-1} x_n + x_{n+1}, \quad x_n > x_{n+1}$$
$$x_n = q_n x_{n+1} + 0.$$

$x_1 > x_2 > \cdots > 0 \Rightarrow$ must stop after a finite number of steps.

Claim: $x_{n+1} = \gcd(x,y)$.

Proof: (i) $x_{n+1} | x_n \Rightarrow x_{n+1} | x_{n-1} \Rightarrow$ inductively, $x_{n+1} | x_i \ \forall i \Rightarrow x_{n+1} | x, x_{n+1} | y$.

(ii) $x_{n+1} = x_{n-1} - q_{n-1} x_n = x_{n-1} - q_{n-1}(x_{n-2} - q_{n-2} x_{n-1}) = \cdots = ax + by.$

$\therefore x_{n+1} = \gcd(x,y)$ by §1.1.2.

1.1.4. Prime Numbers

Definition: An integer $n > 1$ is a prime number if it has precisely 2 positive divisors.

Lemma: Every integer $n > 1$ is divisible by some prime number p.

Proof: $n \in \{a > 1 : a | n\} =: S \subset \mathbb{N}$ - non-empty. WOP $\Rightarrow \exists$ minimal element $p \in S$.

Note: if $d > 1$, $d | p \Rightarrow d \in S \Rightarrow d = p$.

Theorem: There are infinitely many prime numbers.

Proof: Given primes $p_1, \ldots, p_k$ $(k \geq 1)$, put $n = p_1 p_2 \cdots p_k + 1$, so $n > 1$. By lemma $\exists$ prime $p | n$.

If $p | p_i$ then $p | 1$ - #. So $p \notin \{p_1, \ldots, p_k\}$.

1.1.5. Fundamental Theorem of Arithmetic.

Theorem (F.T.A.): Every integer $n \geq 1$ can be written in a unique way as $n = p_1^{a_1} \cdots p_k^{a_k}$ - ⊛

Where - $a_i > 0$, $\{p_i\}$ distinct primes. (Uniqueness up to permutation of factors.)

Proof: Existence: Let $S = \{n \geq 1 :$ decomposition ⊛ does not exist$\} \subset \mathbb{N}$. Want to show $S = \emptyset$.

If $S \neq \emptyset$, WOP $\Rightarrow \exists$ minimal $n \in S$. $1 \notin S \Rightarrow n > 1$, so §1.1.4 $\Rightarrow \exists$ prime $p | n$.

Minimality $\Rightarrow \frac{n}{p} \notin S \Rightarrow \frac{n}{p} = p_1^{a_1} \cdots p_k^{a_k} \Rightarrow n = p \cdot p_1^{a_1} \cdots p_k^{a_k}$ - # $\Rightarrow S = \emptyset$.

Uniqueness: Let $S = \{n \geq 1 : \exists$ two different decompositions ⊛ of $n\}$. Again, want $S = \emptyset$.

If $S \neq \emptyset$, $\exists$ minimal $n \in S$, $n > 1$. $\Rightarrow \exists$ prime $p | n$.

So, $p | n = \begin{cases} p_1^{a_1} \cdots p_k^{a_k} \\ q_1^{b_1} \cdots q_l^{b_l} \end{cases} \Rightarrow p = \begin{cases} \text{one of the } p_i \\ \text{one of the } q_j. \end{cases}$

Euclid's Lemma: Let p be a prime, and $x, y \in \mathbb{N} \setminus \{0\}$. If $p | xy$ then $p | x$ or $p | y$.
Proof: Assume $p \nmid x$. Want to show $p | y$. Look at $d = \gcd(p, x)$.
Now, $d | p$, but $d \neq p \Rightarrow d = 1$. $\therefore 1 = ap + bx$ (some $a, b \in \mathbb{Z}$).
$\Rightarrow y = apy + bxy$, but $p|p$, $p | xy \Rightarrow p | y$.

Corollary: Let $x = p_1^{a_1} \cdots p_k^{a_k}$, $y = p_1^{b_1} \cdots p_k^{b_k}$ (p_i - distinct primes). Then,
(i) $x | y \iff a_i \leq b_i \ \forall i$.
(ii) $\gcd(x, y) = p_1^{\min(a_1, b_1)} \cdots p_k^{\min(a_k, b_k)}$

Example: $72 = 2^3 . 3^2 . 5^0$, $20 = 2^2 . 3^0 . 5^1 \Rightarrow \gcd(72, 20) = 2^2 . 3^0 . 5^0 = 4$.

1.1.6. Least Common Multiple.

Proposition: For any $x, y \in \mathbb{Z} \setminus \{0\}$, there is a unique common multiple $e > 0$ which divides all common multiples. Write $e = \operatorname{lcm}(x, y)$.
Sketch Proof: Uniqueness: $\exists e, e' \Rightarrow e | e'$, $e' | e \Rightarrow e = e'$.
Existence: $x = \pm p_1^{a_1} \cdots p_k^{a_k}$, $y = \pm p_1^{b_1} \cdots p_k^{b_k}$. Then, $e = p_1^{\max(a_1, b_1)} \cdots p_k^{\max(a_k, b_k)}$ satisfies all we want by previous corollary.

Corollary: $\gcd(x, y) . \operatorname{lcm}(x, y) = |xy|$
Proof: $\min(a_i, b_i) + \max(a_i, b_i) = a_i + b_i$.

Remark: Can define $\gcd(x, y, z) = \prod_{i=1}^{k} p_i^{\min(a_i, b_i, c_i)}$, $\operatorname{lcm}(x, y, z) = \prod_{i=1}^{k} p_i^{\max(a_i, b_i, c_i)}$, but there is no relation in general between $\gcd(x, y, z)$, $\operatorname{lcm}(x, y, z)$ and xyz.

1.2. Congruences.

1.2.1. Basic Facts.

Definition: Fix $n \geq 1$ - "modulus". Then, $a, b \in \mathbb{Z}$ are congruent modulo n if $n | a - b$. Write $a \equiv b \pmod n$

Note: "$\equiv$" is an equivalence ~~class~~ relation on $\mathbb{Z}$ (ie, reflexive, symmetric, transitive).
An equivalence class for $\equiv$ is called a residue class (mod n).

The residue class represented by $a \in \mathbb{Z}$ is denoted by $a \pmod n$.
Also, $\{$residue classes (mod n)$\} = \mathbb{Z}/n\mathbb{Z}$ and has n elements $(0 \pmod n), \ldots, n-1 \pmod n)$.
If $a \pmod n = x \in \mathbb{Z}/n\mathbb{Z}$, $b \pmod n = y \in \mathbb{Z}/n\mathbb{Z}$, then $x = y$ in $\mathbb{Z}/n\mathbb{Z}$ iff $a \equiv b \pmod n$.

Results: $x \equiv y \pmod n$, $x' \equiv y' \pmod n \Rightarrow$ (i) $x \pm x' \equiv y \pm y' \pmod n$, (ii) $xx' \equiv yy' \pmod n$.
So the operations $+, -, \cdot$ make sense in $\mathbb{Z}/n\mathbb{Z}$ - it is a ring.
But, $x^{x'} \not\equiv y^{y'} \pmod n$ in general. Eg: $5 \equiv 2 \pmod 3$, $2 \equiv 5 \pmod 3$, but $5^2 \not\equiv 2^5 \pmod 3$

1.2.2. Division in $\mathbb{Z}/n\mathbb{Z}$.

Question: When does $1/x$ exist in $\mathbb{Z}/n\mathbb{Z}$? Ie, if $x = a \pmod n$, $y = b \pmod n$, we want $x.y = 1 \in \mathbb{Z}/n\mathbb{Z}$, or $ab \equiv 1 \pmod n$. Given $a \in \mathbb{Z}$, is there such a $b \in \mathbb{Z}$?

Lemma: Given $a \in \mathbb{Z}$, $\exists\ b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod n$ iff $\gcd(a,n) = 1$.

Proof: ($\Rightarrow$) If $ab = 1 + nc$ and $d = \gcd(a,n)$ then $d \mid ab$, $d \mid nc \Rightarrow d \mid 1 \Rightarrow d = 1$.

($\Leftarrow$) if $d = \gcd(a,n) = 1$, then $1 = ax + ny$, some $x, y \in \mathbb{Z} \Rightarrow ax \equiv 1 \pmod n$. Take $b = x$.

Definition: A residue class $x \in \mathbb{Z}/n\mathbb{Z}$ is called <u>invertible</u> if $\exists\ y \in \mathbb{Z}/n\mathbb{Z}$ with $xy = 1 \in \mathbb{Z}/n\mathbb{Z}$.

The lemma now implies that this is the case iff $x = a \pmod n$ such that $\gcd(a,n) = 1$.

Notation: $(\mathbb{Z}/n\mathbb{Z})^* = \{\text{invertible residue classes}\} = \{a \pmod n : 1 \le a \le n,\ \gcd(a,n) = 1\}$.

If $n = p$, prime, write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$.

Note: Every non-zero $x \in \mathbb{Z}/n\mathbb{Z}$ invertible $\Leftrightarrow$ n a prime.

1.2.3. Euler Function.

Definition: For $n \ge 1$, let $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^* = \left|\{a : 1 \le a \le n,\ \gcd(a,n) = 1\}\right|$.

Proposition: (i) If p prime, then $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$

(ii) $\varphi(n) = n \prod_{p \mid n} (1 - 1/p)$.

Proof: (i) $\varphi(p^k) = \left|\{a : 1 \le a \le p^k\}\right| - \left|\{pb : 1 \le b \le p^{k-1}\}\right| = p^k - p^{k-1}$.

(ii) Follows from ...

Inclusion-Exclusion Principle: $|A_1 \cup \dots \cup A_N| = \sum_{1 \le i \le N} |A_i| - \sum_{1 \le i < j \le N} |A_i \cap A_j| + \dots - (-1)^N |A_1 \cap \dots \cap A_N|$

Now, $n = p_1^{a_1} \cdots p_N^{a_N}$, p_i distinct primes, $a_i > 0$. Let $A_i = \{a : 1 \le a \le n,\ p_i \mid n\}$

Then, $\varphi(n) = n - |A_1 \cup \dots \cup A_N| = n - \sum |A_i| + \sum |A_i \cap A_j| - \dots = n\left(1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \dots\right) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

1.2.4. Theorems of Euler and Fermat.

Euler's Theorem: If $x \in (\mathbb{Z}/n\mathbb{Z})^*$, then $x^{\varphi(n)} = 1$ in $\mathbb{Z}/n\mathbb{Z}$. (Ie, if $a \in \mathbb{Z}$, $\gcd(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$).

Proof: x invertible $\Rightarrow$ multiplication by x is a bijection on $(\mathbb{Z}/n\mathbb{Z})^*$

$\therefore \prod_{y \in (\mathbb{Z}/n\mathbb{Z})^*} y = \prod_{y \in (\mathbb{Z}/n\mathbb{Z})^*} (xy) \in \mathbb{Z}/n\mathbb{Z}$. $\therefore$ $A = A x^{\varphi(n)}$, but $\frac{1}{A}$ exists in $\mathbb{Z}/n\mathbb{Z} \Rightarrow 1 = x^{\varphi(n)}$.

Fermat's Little Theorem: If $n = p$, prime: (i) $a^{p-1} \equiv 1 \pmod p$ $\forall a \in \mathbb{Z}$, $p \nmid a$, (ii) $a^p \equiv a \pmod p$ $\forall a \in \mathbb{Z}$.

Proof: (i) Follows from Euler's Theorem.

(ii) If $p \nmid a$, follows from (i), else if $p \mid a$, then both sides are congruent to $0 \pmod p$.

Corollary: If $n = pq$ ($p \neq q$, primes), and if $m \equiv 1 \pmod{p-1}$, $m \equiv 1 \pmod{q-1}$ then $a^m \equiv a \pmod{pq}$ $\forall a \in \mathbb{Z}$.

Proof: If $p \mid a$, then $a^m \equiv 0 \pmod p$, $a \equiv 0 \pmod p$ $\Rightarrow$ $a^m \equiv a \pmod p$.

If $p \nmid a$, then $a^m = a(a^{p-1})^s$ (where $m = 1 + (p-1)s$), but $a^{p-1} \equiv 1 \pmod p$, so $a^m \equiv a \pmod p$.

The same argument shows $a^m \equiv a \pmod q$.

Hence, $p \mid a^m - a$, $q \mid a^m - a$ $\Rightarrow$ $pq \mid a^m - a$, as $p \neq q$.

1.2.5. The RSA Algorithm.

Encryption - "public key cryptography". Text $\xmapsto{F}$ Cipher text $\xmapsto{F^{-1}}$ Text.

The idea is that there are functions $F: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that, given F, it is practically impossible to compute F^{-1}.

We take $n = pq$ ($p \neq q$, primes), $r, s \geq 1$ such that $rs \equiv 1 \pmod{p-1}$, $rs \equiv 1 \pmod{q-1}$.

$F(x) = x^r$, $F: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Corollary $\Rightarrow$ $F^{-1}(x) = x^s$.

Public data: pq, r. Secret data: p, q, s.

This works because it is almost impossible to ~~compute~~ factorise n (for large p, q), and it is relatively easy to generate big primes p, q.

1.3. Solutions of Congruences.

Given $P(x) = a_0 + a_1 x + \cdots + a_d x^d$, $a_i \in \mathbb{Z}$, consider a congruence $P(x) \equiv 0 \pmod n$.

Look for solutions $x \in \mathbb{Z}/n\mathbb{Z}$

1.3.1. Chinese Remainder Theorem. (CRT)

Theorem: If $n_1, n_2 \geq 1$, $\gcd(n_1, n_2) = 1$, $a_1, a_2 \in \mathbb{Z}$, then the system of congruences $\{x \equiv a_1 \bmod n_1,\ x \equiv a_2 \bmod n_2\}$ has a unique solution $\pmod{n_1 n_2}$

Remark: If $\gcd(n_1, n_2) > 1$, x may not exist. Eg: $\{x \equiv 1 \pmod 6,\ x \equiv 0 \pmod 4\}$.

Proof of Theorem: Uniqueness: solutions $x, y \in \mathbb{Z}$. If $\left\{\begin{array}{l} x \equiv y \pmod{n_1} \\ x \equiv y \pmod{n_2} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} n_1 \mid x-y \\ n_2 \mid x-y \end{array}\right\} \Rightarrow x \equiv y \pmod{n_1 n_2}$

- since $\operatorname{lcm}(n_1, n_2) = n_1 n_2 / \gcd(n_1, n_2) = n_1 n_2 \mid (x-y)$.

Existence: $\gcd(n_1, n_2) = 1 \Rightarrow \exists\, u, v \in \mathbb{Z}$ such that $n_1 u + n_2 v = 1$.

Take $x = a_1 n_2 v + a_2 n_1 u$. $\Rightarrow$ $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$

Remarks: (i) "Algebraic version": $(a_1 \in)\ \mathbb{Z}/n_1\mathbb{Z} \times (a_2 \in)\ \mathbb{Z}/n_2\mathbb{Z} \xleftrightarrow{\text{bijection}} (x \in)\ \mathbb{Z}/n_1 n_2\mathbb{Z}$.

(ii) $x \in (\mathbb{Z}/n_1 n_2 \mathbb{Z})^* \Leftrightarrow a_i \in (\mathbb{Z}/n_i\mathbb{Z})^*$, $i = 1, 2$.

(iii) If $n_1, .., n_k$ satisfy $\gcd(n_i, n_j) = 1$ $\forall i \neq j$ then $\{x \equiv a_i \pmod{n_i}\}$, $i = 1, .., k$, has a unique solution modulo $n_1 \cdots n_k$.

(iv) (iii) holds for a solution of (iii) $\Rightarrow (\mathbb{Z}/n_1\cdots n_k\mathbb{Z})^* \overset{\text{bijection}}{\longleftrightarrow} (\mathbb{Z}/n_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^*$.

Counting elements: $\varphi(n_1\cdots n_k) = \varphi(n_1)\cdots\varphi(n_k) \Rightarrow$ another proof of $\varphi(p_1^{a_1}\cdots p_k^{a_k}) = \varphi(p_1^{a_1})\cdots\varphi(p_k^{a_k})$ $(p_i \neq p_j)$

Notation: If $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ $(a_i \in \mathbb{Z})$, and $n \geq 1$, let $N(P, n)$ be the number of solutions of $P(x) \equiv 0 \pmod n$, of the form $x \in \mathbb{Z}/n\mathbb{Z}$.

Remark: If $P'(x) = a_0' + a_1' x + \cdots + a_d' x^d$ such that $a_i \equiv a_i' \pmod n$ $\forall i \geq 0$, then $N(P, n) = N(P', n)$. $(P(x) \equiv P'(x) \pmod n \ \forall x \in \mathbb{Z})$.

Proposition: If $\gcd(n_1, n_2) = 1$ then $N(P, n_1 n_2) = N(P, n_1)\, N(P, n_2)$

Proof: Chinese Remainder Theorem. LHS $= |\{x \in \mathbb{Z}/n_1 n_2\mathbb{Z} : P(x) \equiv 0 \pmod{n_1 n_2}\}|$

RHS $= |\{x_1 \in \mathbb{Z}/n_1\mathbb{Z} : P(x_1) \equiv 0 \pmod{n_1}\}| \times |\{x_2 \in \mathbb{Z}/n_2\mathbb{Z} : P(x_2) \equiv 0 \pmod{n_2}\}|$.

And, $\{P(x) \equiv 0 \pmod{n_1 n_2}\} \Leftrightarrow \{P(x_1) \equiv 0 \pmod{n_1},\ P(x_2) \equiv 0 \pmod{n_2}\}$

Example: $P(x) = x^2 - x$, $n_1 = 4$, $n_2 = 25$. So, $n_1 n_2 = 100$.

$P(x) \equiv 0 \pmod 4 \Rightarrow x^2 \equiv x \pmod 4 \Rightarrow x \equiv 0, 1 \pmod 4$

$P(x) \equiv 0 \pmod{25} \Rightarrow x^2 \equiv x \pmod{25} \Rightarrow x \equiv 0, 1 \pmod{25}$

$P(x) \equiv 0 \pmod{100} \Rightarrow x^2 \equiv x \pmod{100} \Rightarrow x \equiv 0, 1, 25, 76 \pmod{100}$

1.3.2. Linear Congruences.

Lemma: Let $a, n \geq 1$, $b \in \mathbb{Z}$. Then, the congruence $ax \equiv b \pmod n$ has a solution $x \in \mathbb{Z}$ iff $\gcd(a,n) \mid b$.

Proof: Write $d = \gcd(a,n)$. If $ax \equiv b \pmod n \Leftrightarrow ax = b + ny$, $y \in \mathbb{Z} \Rightarrow d \mid b$.

If $d \mid b$, then $d = au + nv$, $(u, v \in \mathbb{Z})$. Multiply by b/d: $b = a\left(\frac{bu}{d}\right) + n\left(\frac{bv}{d}\right) \Rightarrow a\left(\frac{bu}{d}\right) \equiv b \pmod n$

Remark: If $d \mid b$, then the number of solutions $\pmod n$ is equal to d.

Proof: x, y solutions $\Rightarrow n \mid a(x-y) \Rightarrow \frac{n}{d} \mid \frac{a}{d}(x-y) \Rightarrow \frac{n}{d} \mid x - y$, as $\gcd(n/d, a/d) = 1$.

Conversely, if y is a solution and if $\frac{n}{d} \mid x-y$, then x is a solution.

All solutions $\pmod n$ are: $y,\ y + n/d, \ldots, y + \frac{n}{d}(d-1)$

1.3.3. Lagrange's Theorem.

Let p be a prime number. Let $P(x) \in \mathbb{Z}[X] = \{\sum_{i=0}^{d} a_i X^i : a_i \in \mathbb{Z}, d \geq 0\}$.

Congruence: $P(X) \equiv 0 \pmod p$ ⊛ It makes sense to consider $P(X) \pmod p$.

Ie, $P(X) = \sum_{i=0}^{d} a_i X^i \rightsquigarrow \bar{P}(X) = \sum_{i=0}^{d} a_i \pmod p\ X^i \in \mathbb{F}_p[X]$. Then, ⊛ $\Leftrightarrow \bar{P}(X) = 0$ in $\mathbb{F}_p$.

Lagrange's Theorem: Let p be prime, $Q(X) \in \mathbb{F}_p[X]$ a non-zero polynomial of degree d. Then, $Q(X) = 0 \in \mathbb{F}_p$ has at most d solutions in $\mathbb{F}_p$.

Remark: For $Q = \bar{P}$, Q non-zero $\Leftrightarrow$ at least one coefficient of P is not divisible by p.

Proof of Theorem: Observe, if $Q(X) \in \mathbb{F}_p[X] \Rightarrow Q(X) = (X-u)Q_1(X) + Q(u)$, $u \in \mathbb{F}_p$.

Assume $Q(X) = b_0 + b_1X + \cdots + b_dX^d$ ($b_d \neq 0$ in $\mathbb{F}_p$) vanishes for $X = u_1, \ldots, u_{d+1} \in \mathbb{F}_p$, ($u_i$ distinct). Now, $Q(X) = (X-u_1)Q_1(X) + \cancel{Q(u_1)}^{=0}$.

Let $X = u_2 \Rightarrow 0 = Q(u_2) = (u_2-u_1)Q_1(u_2) \Rightarrow Q_1(u_2) = 0$, as $u_2 - u_1 \neq 0 \Rightarrow$ invertible (mod p).

Continue... Get $Q(X) = b_d(X-u_1)\cdots(X-u_d) \in \mathbb{F}_p$. Let $X = u_{d+1}$.

$\Rightarrow 0 = b_d(u_{d+1}-u_1)\cdots(u_{d+1}-u_d) \Rightarrow b_d = 0$ as each $(u_{d+1}-u_i) \neq 0$ and so is invertible. ※

Corollary (Wilson's Theorem): If p is prime, then $(p-1)! \equiv -1 \pmod p$

Proof: Consider $P(x) = x^{p-1} - 1 - (x-1)(x-2)\cdots(x-(p-1))$, $\in \mathbb{Z}[x]$, degree $\leq p-2$.

Fermat's Theorem $\Rightarrow P(u) \equiv 0 \pmod p$ for $u = 1, \ldots, p-1$.

So, Lagrange $\Rightarrow$ all coefficients of $P(x)$ are divisible by $p \Rightarrow p \mid P(0) = -1 - (-1)^{p-1}(p-1)!$

$\Rightarrow$ Wilson's Theorem.

1.4. Primitive Roots and Congruences.

1.4.1. Orders and Exponents.

Definition: The order of $a \pmod n \in (\mathbb{Z}/n\mathbb{Z})^*$ is the smallest $d > 0$ such that $a^d \equiv 1 \pmod n$. (d exists, and $d \leq \varphi(n)$ by Euler's Theorem).

The exponent of $(\mathbb{Z}/n\mathbb{Z})^*$ is the smallest $d > 0$ such that $a^d \equiv 1 \pmod n$ $\forall\, a \pmod n \in (\mathbb{Z}/n\mathbb{Z})^*$

a is a primitive root (mod n) if it has order $\varphi(n)$ $\left[\Leftrightarrow \{a^i \pmod n : 1 \leq i \leq \varphi(n)\} \in (\mathbb{Z}/n\mathbb{Z})^*\right]$

Proposition: Let d be the order of $a \pmod n \in (\mathbb{Z}/n\mathbb{Z})^*$, and $b, c \in \mathbb{Z}$.

Then, $a^b \equiv 1 \pmod n \Leftrightarrow d \mid b$, and $a^b \equiv a^c \pmod n \Leftrightarrow b \equiv c \pmod d$.

Proof: If $d \mid b$, then $a^b = (a^d)^{b/d} \equiv 1 \pmod n$

If $a^b \equiv 1 \pmod n$, write $b = qd + r$, $0 \leq r < d \Rightarrow a^r = a^b(a^d)^{-q} \equiv 1 \pmod n$

Minimality of $d \Rightarrow r = 0 \Rightarrow d \mid b$.

$a^b \equiv a^c \pmod n \Leftrightarrow a^{b-c} \equiv 1 \pmod n$, and apply first result.

Criterion: The order of $a \pmod n \in (\mathbb{Z}/n\mathbb{Z})^*$ is equal to a given $d > 0$ iff $a^d \equiv 1 \pmod n$ and $\forall$ primes $p \mid d$, $a^{d/p} \not\equiv 1 \pmod n$ — $\oplus$

Proof: ($\Rightarrow$) By definition.

($\Leftarrow$) Assume $\oplus$ holds, and put e = order of $a \pmod n$. We want $d = e$.

Now, proposition $\Rightarrow e \mid d$. If $e \neq d$, then $e \mid d/p$, some prime $p \mid d$.

$\Rightarrow a^{d/p} = (a^e)^{d/pe} \equiv 1 \pmod n$ — ※.

Corollary: Exponent of $(\mathbb{Z}/n\mathbb{Z})^* = \operatorname{lcm}\{\text{orders of } a \pmod n\}$.

Example: $n = 12$.

$(\mathbb{Z}/n\mathbb{Z})^* =$	$\{1 \pmod{12}$,	$5 \pmod{12}$,	$7 \pmod{12}$,	$11 \pmod{12}\}$
Orders:	1	2	2	2

Exponent $= 2$ (as $11^2 \equiv 7^2 \equiv 5^2 \equiv 1^2 \equiv 1 \pmod{12}$)

Lemma: If d = order of $a \pmod{n} \in (\mathbb{Z}/n\mathbb{Z})^*$ and $m>0$, then order of $a^m \pmod{n} = d/\gcd(d,m)$.

Proof: $a^{bm} = (a^m)^b \equiv 1 \pmod{n} \iff d \mid bm \iff \frac{d}{\gcd(d,m)} \mid b \cdot \frac{m}{\gcd(d,m)} \iff \frac{d}{\gcd(d,m)} \mid b$.

1.4.2. Existence of Primitive Roots.

Theorem: A primitive root $\pmod{n}$ exists $\iff n = 1, 2, 4$, or $p^k, 2p^k$ ($p>2$, prime).

Remark: For $n = 2^k$, $k>2$, every element can be expressed in $(\mathbb{Z}/2^k\mathbb{Z})^*$ uniquely as $a \equiv \pm 5^{\partial} \pmod{2^k}$, $1 \le \partial \le \frac{1}{2}\varphi(2^k) = 2^{k-2}$.
Exponent of $(\mathbb{Z}/2^k\mathbb{Z})^*$ is 2^{k-2}.

1.4.3. Congruences.

Notation: Let $N_d(n)$ = the number of solutions of $x^d \equiv 1 \pmod{n}$ in $\mathbb{Z}/n\mathbb{Z}$.

Observations: (i) If $\gcd(m,n)=1$ then $N_d(mn) = N_d(m)N_d(n)$ - follows from C.R.T.

(ii) If e = exponent of $(\mathbb{Z}/n\mathbb{Z})^*$, $f = \gcd(d,e)$, then $N_d(n) = N_f(n)$.

Proof: Claim that: $x^f \equiv 1 \pmod{n} \iff x^d \equiv 1 \pmod{n}$

($\Rightarrow$) Obvious, as $f \mid d$.

($\Leftarrow$) $f = du + ev$ $(u,v \in \mathbb{Z}) \Rightarrow x^f = (x^d)^u (x^e)^v \equiv 1 \pmod{n}$.

(iii) If there is a primitive root $\pmod{n}$, then $d \mid \varphi(n) \Rightarrow N_d(n) = d$.

Proof: Let $a \pmod{n}$ be a primitive root, $x \equiv a^m \pmod{n}$ for some m.
$x^d \equiv a^{md} \pmod{n}$. This is $\equiv 1 \pmod{n} \iff \varphi(n) \mid md \iff \frac{\varphi(n)}{d} \mid m$.
Solutions $\longleftrightarrow m = \varphi(n)/d \cdot (0, 1, \dots, d-1) \leftarrow d$ values.

(iv) If $n = 2^k$ $(k>2)$, if $d = 2^j$ $(j \le k-2)$ (as exponent of $(\mathbb{Z}/2^k\mathbb{Z})^* = 2^{k-2}$)
$\Rightarrow N_d(2^k) = \begin{cases} 2d, & j>0 \\ 1, & j=0. \end{cases}$

Proof: Write $x \equiv \pm 5^m \pmod{2^k}$. Now use same argument as in (iii)
$(x^{2^j} \equiv (\pm 1)^{2^j} 5^{2^j m})$.

Remark: (i) - (iv) give formulae for $N_d(n)$ in general.

Example: $x^{30} \equiv 1 \pmod{216}$. $216 = 2^3 \cdot 3^3$. What is $N_{30}(216)$?
$N_{30}(8 \cdot 27) = N_{30}(8) \cdot N_{30}(27)$, by (i).
$(\mathbb{Z}/8\mathbb{Z})^*$ has exponent 2. $(\mathbb{Z}/27\mathbb{Z})^*$ has exponent $\varphi(27) = 18$.
Now, $N_{30}(8) \overset{(ii)}{=} N_2(8) \overset{(iv)}{=} 4$, $N_{30}(27) \overset{(ii)}{=} N_6(27) \overset{(iii)}{=} 6 \Rightarrow N_{30}(216) = 4 \cdot 6 = 24$.

1.4.4. Index. (Discrete Logarithm).

Definition: If $a \pmod{n}$ is a primitive root $\pmod{n}$, the index of $x \in (\mathbb{Z}/n\mathbb{Z})^*$ wrt the base a is the unique element $m \in \mathbb{Z}/\varphi(n)\mathbb{Z}$ such that $x \equiv a^m \pmod{n}$. Write $m = \mathrm{ind}_a(x)$.

Rule: $\mathrm{ind}_a(xy) = \mathrm{ind}_a(x) + \mathrm{ind}_a(y)$, $\in \mathbb{Z}/\varphi(m)\mathbb{Z}$.

Example: $x^4 \equiv 3 \pmod{23}$. $\varphi(23) = 22 = 2.11$. Check that 5 is a primitive root (mod 23) via criterion 1.4.1 (see: $5^2 \not\equiv 1$, $5^{11} \not\equiv 1 \pmod{23}$)
So, $4\,\mathrm{ind}_5(x) \equiv \mathrm{ind}_5(3) \pmod{22}$, and $\mathrm{ind}_5(3) \pmod{22}$ is 16.
So, $2\,\mathrm{ind}_5(x) \equiv 8 \pmod{11} \Rightarrow \mathrm{ind}_5(x) \equiv 4 \pmod{11}$, ie, $\mathrm{ind}_5(x) \equiv 4, 15 \pmod{22}$
So, $x \equiv 5^4, 5^{15} \pmod{23} \Rightarrow x \equiv \pm 4 \pmod{23}$

Theorem 1.4.2: A primitive root exists (mod n) $\Leftrightarrow n = 1, 2, 4, p^k, 2p^k$ ($p>2$, prime).

Proof: Step 1: Claim: if $n = n_1 n_2$, $(n_1, n_2) = 1$, $n_1, n_2 > 2 \Rightarrow$ exponent of $(\mathbb{Z}/n\mathbb{Z})^*$ divides $\frac{1}{2}\varphi(n)$
$\Rightarrow$ no primitive root.

Proof: $n_1, n_2 > 2 \Rightarrow \varphi(n_1), \varphi(n_2)$ even. And, $(n_1, n_2) = 1 \Rightarrow \varphi(n) = \varphi(n_1)\varphi(n_2)$

For $(a,n) = 1$, $\left.\begin{aligned} a^{\frac{1}{2}\varphi(n)} &= (a^{\varphi(n_1)})^{\frac{1}{2}\varphi(n_2)} \equiv 1 \pmod{n_1} \\ &= (a^{\varphi(n_2)})^{\frac{1}{2}\varphi(n_1)} \equiv 1 \pmod{n_2} \end{aligned}\right\} \Rightarrow a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}$, by CRT.

Step 2: $n = 1, 2$: $(\mathbb{Z}/n\mathbb{Z})^* = \{1 \pmod{n}\}$, $n = 4$: $3 \pmod 4$ is a primitive root.

Step 3: Assume that a is a primitive root (mod p^k), $p>2$, prime. Let b be the odd element among a, $a+p^k$.

Observe: $b^m \equiv 1 \pmod{2p^k} \overset{(CRT)}{\Longleftrightarrow} \begin{cases} b^m \equiv 1 \pmod{p^k} \Leftrightarrow a^m \equiv 1 \pmod{p^k} \\ b^m \equiv 1 \pmod 2 \quad \text{(always true)}. \end{cases}$

$\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k) \Rightarrow$ order of $b \pmod{2p^k}$ = order of $a \pmod{p^k} = \varphi(p^k) = \varphi(2p^k)$
$\Rightarrow b$ is a primitive root (mod $2p^k$).

Step 4: Assume that a is a primitive root (mod p). Then $\exists\, x \in \mathbb{Z}$ such that $b = a + px$ is a primitive root (mod p^k) $\forall\, k \geq 1$.

Proof: $a^{p-1} = 1 + py$ ($y \in \mathbb{Z}$). Want to arrange $b^{p-1} \not\equiv 1 \pmod{p^2}$ - ⊛

$b^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}px \pmod{p^2} \equiv 1 + p(y - a^{p-2}x) \pmod{p^2}$

As $p \nmid a^{p-2}$, we can find x such that $y - a^{p-2}x \not\equiv 0 \pmod p \Rightarrow$ ⊛ holds.

Claim: d = order of $b \pmod{p^k} = \varphi(p^k) = (p-1)p^{k-1}$ $\forall\, k \geq 1$.

Proof: $k=1$ - automatic.

$k>1$: we know $d \mid (p-1)p^{k-1}$, and $(p-1) \mid d$, as a is a primitive root (mod p).
$\Rightarrow d = (p-1)p^j$, $0 \leq j \leq k-1$. We want $j = k-1$.
Now, $b^{p-1} = 1 + pz$, $p \nmid z$ (by ⊛)
So, $b^d = (b^{p-1})^{p^j} = (1+pz)^{p^j} = 1 + p^j pz + \binom{p^j}{2}p^2z^2 + \cdots \equiv 1 + p^{j+1}z \pmod{p^{j+2}}$ (as $p>2$)
But $d \equiv 1 \pmod{p^k} \Rightarrow j = k-1$ [if $j < k-1$ then $p^{j+1}z \not\equiv 0 \pmod{p^k}$ - ※].
$\Rightarrow$ claim $\Rightarrow$ step 4.

Remark: We showed: b a primitive root (mod p^2) $\Rightarrow$ b a primitive root (mod p^k) $\forall\, k \geq 2$.

To finish the proof of Theorem 1.4.2, we have only to prove:

Subtheorem: If p is prime then $\exists\, x \in \mathbb{F}_p^*$ such that $\mathbb{F}_p^* = \langle x \rangle$.

Proof: Idea: x will have largest possible order.

Substep 1: If $x \in \mathbb{F}_p^*$ has order d, then $\{1, x, \ldots, x^{d-1}\} = \{y \in \mathbb{F}_p^* : y^d = 1\}$.

Proof: LHS $\subseteq$ RHS. But $|LHS| = d$, $|RHS| \leq d$ (by Lagrange's Theorem). $\therefore$ LHS = RHS.

Substep 2: If $x, y \in \mathbb{F}_p^*$ of orders d, e with $e \mid d$, then $y = x^m$, some m.

Proof: $\left.\begin{aligned} \{z \in \mathbb{F}_p^* : z^e = 1\} &= \{1, y, y^2, \dots\} \\ \{z \in \mathbb{F}_p^* : z^d = 1\} &= \{1, x, x^2, \dots\} \end{aligned}\right\} \Rightarrow y = x^m.$

Substep 3: If $x \in \mathbb{F}_p^*$ has maximal order N, then order of any $y \in \mathbb{F}_p^*$ divides N.

Proof: Assume $\exists\, y$ of order $d \nmid N \Rightarrow \exists$ prime $l \mid d$, $l \nmid N$. $\Rightarrow z = y^{d/l} \in \mathbb{F}_p^*$, order l.

Claim: order of $u = xz$ is Nl.

Proof: Use criterion 1.4.1. $u^{Nl} = (x^N)^l (z^l)^N = 1$.

$u^N = z^N \neq 1$, as $l \nmid N$. If $q \mid N$ is a prime, $u^{Nl/q} = (x^{N/q})^l \neq 1$, as $l \neq q$ (to order q).

$\Rightarrow$ order of u is Nl - # to maximality of N.

So we have proved Theorem 1.4.2.

2. Quadratic Reciprocity Law.

2.1. Quadratic Congruences.

2.1.1. Quadratic Residues (QR) and Non-residues (QN).

$ax^2 + bx + c \equiv 0 \pmod n$. If $(a,n) = 1$, can write as: $(2ax + b)^2 \equiv b^2 - 4ac \pmod{4n}$

Special quadratic quadratic congruence: $x^2 \equiv a \pmod n$ - ⊛

Definition: For $a \in \mathbb{Z}$, $(a,n) = 1$, say that: (i) a is a quadratic residue (mod n) if ⊛ has solutions

(ii) a is a quadratic non-residue (mod n) if not.

Observe: If $n = n_1 n_2$ with $(n_1, n_2) = (a, n) = 1$, then a is a QR (mod n) iff a is QR both (mod n_1) and (mod n_2) (by CRT)

Theorem: If $p > 2$ prime, $p \nmid a$, then a is a QR (mod p) iff a is a QR (mod p^n) $\forall n \geq 1$

Proof: ($\Leftarrow$) trivial.

($\Rightarrow$) Use induction on n: $\exists\, x_1 \in \mathbb{Z}$ such that $x_1^2 \equiv a \pmod p$.

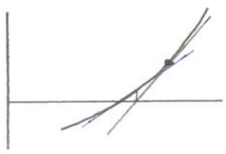
We want solutions of $x_n^2 \equiv a \pmod{p^n}$. Assume $\exists\, x_n$. We want x_{n+1}.

Try $x_{n+1} = x_n + p^n y$ - look for y.

$x_{n+1}^2 - a = x_n^2 - a + 2x_n p^n y + p^{2n} y \Rightarrow \frac{x_{n+1}^2 - a}{p^n} \equiv \frac{x_n^2 - a}{p^n} + 2x_n y \pmod p$.

- Linear congruence for y. §1.3.2 $\Rightarrow$ soluble as $(2x_n, p) = 1 \Rightarrow$ we can find y such that $\frac{x_n^2 - a}{p^n} + 2x_n y \equiv 0 \pmod p \Rightarrow x_{n+1}^2 \equiv a \pmod{p^{n+1}}$.

Remark: Method $\Leftrightarrow$ Newton's method for solving equations $f(x) = 0$ in $\mathbb{R}$.
$f(x) = x^2 - a$, $f'(x) = 2x$.



Remark: For $p = 2$, $k \geq 3$, a is a QR (mod 2^k) $\Leftrightarrow$ a is a QR (mod 8)

$\Leftrightarrow a \equiv 1 \pmod 8$ - for $2 \nmid a$.

2.1.2. Legendre's Symbol.

From now on, $p>2$, prime.

Definition: For $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a QR } (\text{mod } p) \\ -1 & \text{if } a \text{ is a QN } (\text{mod } p) \end{cases}$

Observe: Minimum number of solutions of $x^2 \equiv a \pmod p$ in $\mathbb{F}_p$ is equal to $1 + \left(\frac{a}{p}\right)$

Proof: If $\left(\frac{a}{p}\right) = -1$, there is no solution, by definition.

If $\left(\frac{a}{p}\right) = 0$, so $p \mid a$, then $x^2 \equiv 0 \pmod p \iff x \equiv 0 \pmod p$ – 1 solution.

If $\left(\frac{a}{p}\right) = 1$, then $\exists \leq 2$ solutions (Lagrange – §1.3.3). There is at least one solution x, but $-x$ is another. (As, $p \neq 2$, $p \nmid a \Rightarrow p \nmid 2x \Rightarrow x \not\equiv -x \pmod p$)

Lemma: Let g be a primitive root $(\text{mod } p)$ and $a \equiv g^m \pmod p$. Then, $\left(\frac{a}{p}\right) = (-1)^m$.

Proof: "($\Leftarrow$)" if m is even, then $a \equiv (g^{m/2})^2 \pmod p \Rightarrow a$ is a QR $(\text{mod } p)$.

"($\Rightarrow$)" if a is a QR $(\text{mod } p)$, then $a \equiv x^2 \pmod p$, some x. We have $x \equiv g^n \pmod p$, as g a primitive root, some n. So, $g^m \equiv g^{2n} \pmod p \Rightarrow m \equiv 2n \pmod{p-1}$ $\Rightarrow m$ even (as $p-1$ even).

Corollary: (i) Number of QR $(\text{mod } p)$ = number of QN $(\text{mod } p)$

(ii) Euler's Criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod p$

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, $a, b \in \mathbb{Z}$.

(iv) $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$

Proof: (i) By lemma, QR $\iff m = 2i$, $1 \leq i \leq \frac{1}{2}(p-1)$, QN $\iff m = 2i-1$, $1 \leq i \leq \frac{1}{2}(p-1)$

(ii) If $p \mid a$, then both sides equal $0 \pmod p$.

If $p \nmid a$, then if $\left(\frac{a}{p}\right) = 1$, $a \equiv g^{2m} \pmod p$, $a^{\frac{1}{2}(p-1)} \equiv (g^{p-1})^m \equiv 1 \pmod p$.

if $\left(\frac{a}{p}\right) = -1$, $a \equiv g^{2m+1} \pmod p$, so $a^{\frac{1}{2}(p-1)} \equiv g^{(p-1)m} \cdot g^{\frac{1}{2}(p-1)} \equiv g^{\frac{1}{2}(p-1)} \not\equiv 1 \pmod p$

– as the order of g $(\text{mod } p)$ is $p-1$.

(iii) By (ii): $\{0, 1, -1\} \ni \text{LHS} = \left(\frac{ab}{p}\right) \equiv (ab)^{\frac{1}{2}(p-1)} = a^{\frac{1}{2}(p-1)} \cdot b^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \text{RHS} \in \{0, 1, -1\}$, $(\text{mod } p)$

$\Rightarrow$ LHS = RHS, as $p > 2$.

(iv) By (ii): LHS $= \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)} = \text{RHS} \pmod p$ ("=" as in (iii)).

2.1.3. Quadratic Reciprocity Law (QRL)

Remark: $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$ – solubility of $x^2 \equiv -1 \pmod p$ depends only on $p \pmod 4$.

Roughly speaking, QRL states: solubility of $x^2 \equiv a$ depends only on $p (\text{mod } 4|a|)$, $p \nmid a$.

Theorem (QRL): If $p \neq q$ are primes (>2), then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{1}{4}(p-1)(q-1)}$

Additional Facts: $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}$

Reformulation of QRL: Let $q^* = \left(\frac{-1}{q}\right) q = (-1)^{\frac{1}{2}(q-1)} \cdot q$.

QRL becomes: $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$ $\left(\ldots = \left(\frac{(-1)^{\frac{1}{2}(q-1)} q}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{1}{2}(q-1)} \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)} \cdot \left(\frac{q}{p}\right). \right)$

Example: $q=3$, $q^*=-3$. $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1, & p \equiv 1 \pmod 3 \\ -1, & p \equiv 2 \pmod 3 \end{cases}$

So, $x^2 \equiv -3 \pmod p$ soluble $\Leftrightarrow$ $p \equiv 1 \pmod 3$

Example: $\left(\frac{42}{97}\right) = ?$ $\quad x^2 \equiv 42 \pmod{97}$. $42 = 2.3.7. = 2.(-3).(-7). = 2.3^*.7^*$

So, $\left(\frac{42}{97}\right) = \left(\frac{2}{97}\right).\left(\frac{-3}{97}\right).\left(\frac{-7}{97}\right) = -1.\left(\frac{97}{3}\right).\left(\frac{97}{7}\right). = -1.(1).(-1) = 1$

$\Rightarrow x^2 \equiv 42 \pmod{97}$ has 2 solutions.

2.2. Quadratic Reciprocity Law - Proof.

2.2.1. Idea.

Example: As above, for $q=3$: $x^2 \equiv -3 \pmod p$ is soluble $\Leftrightarrow p \equiv 1 \pmod 3$

"$\sqrt{-3}$ exists in $\mathbb{F}_p$" $\qquad \Updownarrow \exists\, y \in \mathbb{F}_p^*$ of order 3

-ie y = "cubic root" of 1.

In $\mathbb{C}$, $\zeta_3 = e^{2\pi i/3} = \frac{1}{2}(1+\sqrt{-3}) \Rightarrow \sqrt{-3} = 2\zeta_3 - 1$

In general, $\zeta_q = e^{2\pi i/q}$ - qth root of unity.

Want a relation between ζ_q and $\sqrt{q^*}$

Example: $\left.\begin{array}{l} q=3,\ \sqrt{-3} = \zeta_3 - \zeta_q^2 \\ q=5,\ \sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 \end{array}\right\}$ "G_1"

2.2.2. Gauss Sums.

Notation: $q>2$, prime. $\zeta_q = e^{2\pi i/q}$ is a root of $\frac{T^q-1}{T-1} = T^{q-1} + T^{q-2} + \dots + 1 = 0$.

Gauss Sums: For $a \in \mathbb{F}_q^*$, let $G_a = \sum_{x=1}^{q-1} \left(\frac{x}{q}\right)\zeta_q^{ax} = \sum_{x\in\mathbb{F}_q^*} \left(\frac{x}{q}\right)\zeta_q^{ax}$.

Theorem: (i), $G_a = \left(\frac{a}{q}\right) G_1$, (ii) $G_1^2 = q^*$.

Proof: (i) $G_1 = \sum_{x\in\mathbb{F}_q^*} \left(\frac{x}{q}\right)\zeta_q^{x} = \sum_{y\in\mathbb{F}_q^*}\left(\frac{ay}{q}\right)\zeta_q^{ay}$, letting $x = ay$, $y \in \mathbb{F}_q^*$

$= \left(\frac{a}{q}\right) G_a \Rightarrow G_a = \left(\frac{a}{q}\right)^{-1} G_1 = \left(\frac{a}{q}\right) G_1$.

(ii) $G_1^2 = \sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*} \left(\frac{x}{q}\right)\left(\frac{y}{q}\right)\zeta_q^{x+y} = \sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\left(\frac{x^2 z}{q}\right)\zeta_q^{x(1+z)}$, letting $y = xz$ for fixed x.

$= \sum_{z\in\mathbb{F}_q^*}\left(\frac{z}{q}\right)\sum_{x\in\mathbb{F}_q^*}\left(\zeta_q^{1+z}\right)^x$, and $\zeta_q^{1+z} = \begin{cases} 1 & \text{if } z=-1 \\ \text{a } q^{th} \text{ root of unity (not 1)} & \text{if } z \neq -1 \end{cases}$

$\therefore G_1^2 = \left(\frac{-1}{q}\right)(q-1) + \sum_{\substack{z\in\mathbb{F}_q^* \\ z\neq -1}}\left(\frac{z}{q}\right)(-1)$, as $T^{q-1} + T^{q-2} + \dots + T + 1 = 0$

$= \left(\frac{-1}{q}\right)q - \sum_{z\in\mathbb{F}_q^*}\left(\frac{z}{q}\right) = q^*$, since the sum is zero.

Remark: If $q \equiv 1 \pmod 4$, then $G_1 = \sqrt{q}$

If $q \equiv 3 \pmod 4$, then $G_1 = i\sqrt{q}$ (proofs difficult)

2.2.3. Proof of QRL.

Theorem: For $p \neq q$ primes (>2), $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$.

Proof: We shall work with numbers of the form $Q(\zeta_q) = a_0 + a_1 \zeta_q + \dots + a_N \zeta_q^N$.

We know $P(\zeta_q) = 0$, where $P(T) = T^{q-1} + T^{q-2} + \dots + 1$.

Division $\Rightarrow$ $Q(T) = P(T)\,Q_1(T) + R(T)$. R has integral coefficients, degree $\leq q-2$

Let $\mathbb{Z}[\zeta_q] = \{a_0 + a_1\zeta_q + \dots + a_{q-1}\zeta_q^{q-1} : a_i \in \mathbb{Z}\}$

Facts: (i) $x, y \in \mathbb{Z}[\zeta_q] \Rightarrow x \pm y,\ xy \in \mathbb{Z}[\zeta_q]$

(ii) Given $x \in \mathbb{Z}[\zeta_q]$, the a_i's are unique.

(iii) $\mathbb{Z}[\zeta_q] \cap \mathbb{Q} = \mathbb{Z}$.

Definition: For $x, y \in \mathbb{Z}[\zeta_q]$, write $x \equiv y \pmod{p\mathbb{Z}[\zeta_q]}$ iff $x - y = pz$, some $z \in \mathbb{Z}[\zeta_q]$.

Facts: (iv) $x \equiv y$ and $x' \equiv y'$ $\Rightarrow$ $xx' \equiv yy'$

(v) $(x+y)^p \equiv x^p + y^p \pmod{p\mathbb{Z}[\zeta_q]}$, by binomial theorem.

We may now proceed:

$G_1^p = \left(\sum_{x \in \mathbb{F}_q^*} \left(\frac{x}{q}\right) \zeta_q^x\right)^p \equiv \sum_{x \in \mathbb{F}_q^*} \left(\frac{x}{q}\right)^p \zeta_q^{px} \pmod{p\mathbb{Z}[\zeta_q]}$, but $\left(\frac{x}{q}\right)^p = \left(\frac{x}{q}\right)$, so $G_1^p \equiv G_p$, so $\equiv \left(\frac{p}{q}\right) G_1$

Multiply by G_1: $G_1^{p+1} \equiv \left(\frac{p}{q}\right) G_1^2 = \left(\frac{p}{q}\right) q^* \pmod{p\mathbb{Z}[\zeta_q]}$, and LHS $= G_1^2 (G_1^2)^{\frac{1}{2}(p-1)} = q^* (q^*)^{\frac{1}{2}(p-1)}$

$\Rightarrow$ $q^*\left((q^*)^{\frac{1}{2}(p-1)} - \left(\frac{p}{q}\right)\right) = pz$ where $z \in \mathbb{Z}[\zeta_q]$. But LHS $\in \mathbb{Z}$, so $z \in \mathbb{Q} \cap \mathbb{Z}[\zeta_q] = \mathbb{Z}$

$\Rightarrow$ $q^*(q^*)^{\frac{1}{2}(p-1)} \equiv \left(\frac{p}{q}\right) q^* \pmod{p}$

As $p \nmid q^*$, get that $(q^*)^{\frac{1}{2}(p-1)} \equiv \left(\frac{p}{q}\right) \pmod{p}$, but LHS $\equiv \left(\frac{q^*}{p}\right) \pmod{p}$ by Euler's criterion.

So, $\left(\frac{q^*}{p}\right) \equiv \left(\frac{p}{q}\right) \pmod{p}$, hence $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$, as $p > 2$.

Remark: The same method proves that $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$. Use $G_1 = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7$.

2.2.4. Gauss' Lemma

Observe: Every $x \in \mathbb{Z}$, $p \nmid x$, satisfies $x \equiv \pm r \pmod{p}$, $1 \leq r \leq \frac{1}{2}(p-1)$ – for one r, one sign.

Gauss' Lemma: Let $a \in \mathbb{Z}$, $p \nmid a$. For each $1 \leq i \leq \frac{1}{2}(p-1)$, write $ai \equiv \varepsilon_i r_i \pmod{p}$, with $\varepsilon_i = \pm 1$, $1 \leq r_i \leq \frac{1}{2}(p-1)$. Then $\prod_{i=1}^{\frac{1}{2}(p-1)} \varepsilon_i = \left(\frac{a}{p}\right)$

Proof: Denote $\prod_{i=1}^{\frac{1}{2}(p-1)} i = \left(\frac{1}{2}(p-1)\right)!$ by A. (so $p \nmid A$). Have $ai \equiv \varepsilon_i r_i \pmod{p}$.

Take product: $a^{\frac{1}{2}(p-1)} . A \equiv (\prod \varepsilon_i) . \prod r_i$. But $\prod r_i = A$

(For, $\{r_i : 1 \leq i \leq \frac{1}{2}(p-1)\} = \{1, 2, \dots, \frac{1}{2}(p-1)\}$ since $ai \not\equiv \pm aj \pmod{p}$ $\forall i \neq j$, $1 \leq i, j \leq \frac{1}{2}(p-1)$)

Divide by A $\Rightarrow$ $a^{\frac{1}{2}(p-1)} \equiv \prod \varepsilon_i \pmod{p}$, and LHS $\equiv \left(\frac{a}{p}\right)$, by Euler's criterion

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

Proof: $2.1, 2.2, \dots, 2.\lfloor \frac{1}{4}(p-1) \rfloor$ have $\varepsilon_i = 1$, and $2.\lfloor \frac{1}{4}(p+3) \rfloor, \dots, 2.\left(\frac{1}{2}(p-1)\right)$ have $\varepsilon_i = -1$.

Gauss' Lemma $\Rightarrow$ $\left(\frac{2}{p}\right) = \prod \varepsilon_i = (-1)^{\frac{1}{2}(p-1) - \lfloor \frac{1}{4}(p-1) \rfloor} = (-1)^{\lfloor \frac{1}{4}(p+1) \rfloor} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8} \\ -1 & \text{if } p \equiv 3, 5 \pmod{8} \end{cases}$

2.2.5. Jacobi Symbol.

Definition: For $n, m \geq 1$ such that $(n, 2m) = 1$, define $\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{a_1} \cdots \left(\frac{m}{p_k}\right)^{a_k}$, where $n = p_1^{a_1} \cdots p_k^{a_k}$.

Observe: Whenever defined, $\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$, $\left(\frac{m}{n_1 n_2}\right) = \left(\frac{m}{n_1}\right)\left(\frac{m}{n_2}\right)$

Theorem (Reciprocity Law for Jacobi Symbols): (i) $\left(\frac{-1}{m}\right) = (-1)^{\frac{1}{2}(m-1)}$ $(2 \nmid m)$

(ii) $\left(\frac{2}{m}\right) = (-1)^{\frac{1}{8}(m^2-1)}$ $(2 \nmid m)$

(iii) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \cdot (-1)^{\frac{1}{4}(m-1)(n-1)}$, $(m, 2n) = 1$, $(2 \nmid n)$

Proof: Write $m = \prod p_i^{a_i}$, $n = \prod q_j^{b_j}$, p_i, q_j primes. Apply QRL.

Observe: $\frac{1}{2}(m_1 m_2 - 1) \equiv \frac{1}{2}(m_1 - 1) + \frac{1}{2}(m_2 - 1)$, $(\text{mod } 2)$, $2 \nmid m_1, m_2$.

$\frac{1}{8}(m_1^2 m_2^2 - 1) \equiv \frac{1}{8}(m_1^2 - 1) + \frac{1}{8}(m_2^2 - 1)$ $(\text{mod } 2)$.

Continue. (Exercise).

Example: $\left(\frac{327}{797}\right) \overset{(iii)}{=} \left(\frac{797}{327}\right) = \left(\frac{143}{327}\right) \overset{(iii)}{=} -\left(\frac{327}{143}\right) = -\left(\frac{41}{143}\right) \overset{(iii)}{=} -\left(\frac{143}{41}\right)$

$= -\left(\frac{20}{41}\right) = -\left(\frac{5}{41}\right)\left(\frac{2}{41}\right)^2 = -\left(\frac{5}{41}\right) \overset{(iii)}{=} -\left(\frac{41}{5}\right) = -\left(\frac{1}{5}\right) = -1$

Remark: $(-1)^{\frac{1}{4}(m-1)(n-1)} = \begin{cases} -1 & \text{if } m, n \equiv 3 \ (\text{mod } 4) \\ 1 & \text{otherwise} \end{cases}$

Warning: If $n = pq$, p, q primes (>2), $p \neq q$, and $(a, n) = 1$, then:

(i) a is a QR $(\text{mod } n)$ $\Leftrightarrow$ a is a QR $(\text{mod } p)$ and $(\text{mod } q)$ $\Leftrightarrow$ $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$.

(ii) $\left(\frac{a}{n}\right) = 1 \Leftrightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$

In particular, a is a QR $(\text{mod } n)$ $\overset{\Rightarrow}{\not\Leftarrow}$ $\left(\frac{a}{n}\right) = 1$

3. Arithmetic Functions, Prime Numbers.

3.1 Arithmetic Functions.

3.1.1. Basic Definitions.

Consider maps $f: \mathbb{N}_+ \to \mathbb{C}$.

Examples: (0) $\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$

(i) n^k

(ii) $\varphi(n) = \#\{1 \leq i \leq n : (i, n) = 1\}$

(iii) $\sigma_k(n) = \sum_{d \mid n} d^k$

(iv) Fix $m \geq 1$. $f(n) = \begin{cases} \left(\frac{m}{n}\right) & \text{if } (n, 2m) = 1 \\ 0 & \text{otherwise} \end{cases}$

(v) Möbius function: $\mu(1) = 1$, $\mu(p_1 \cdots p_k) = (-1)^k$, p_i distinct primes, $\mu(p^2 n) = 0$.

Definition: $f: \mathbb{N}_+ \to \mathbb{C}$ is strongly multiplicative if $f(mn) = f(m) f(n)$ $\forall m, n \geq 1$. Eg: (0), (i), (iv)

$f: \mathbb{N}_+ \to \mathbb{C}$ is multiplicative if $f(mn) = f(m) f(n)$ if $(m, n) = 1$. Eg: (ii), (iii), (v)

Observe: if f is multiplicative, then $f(n.1) = f(n)f(1) \Rightarrow f(1) = 0 \Rightarrow f(n) = 0$, or, $f(1) = 1$.
So from now on, $f(1) = 1$.

Definition: A convolution of $f, g: \mathbb{N}_+ \to \mathbb{C}$ is $(f * g)(n) = \sum_{d|n} f(d)\, g(n/d)$

Note: $g * f = f * g$.
Special case: $\mathbb{1}(n) = 1 \ \forall n$. $(f * \mathbb{1})(n) = \sum_{d|n} f(d)$ - strongly multiplicative.
In particular, $\sigma_k = n^k * \mathbb{1}$.

Lemma: If f, g are multiplicative, then $f * g$ is multiplicative.
Proof: Let $(m,n) = 1$. $h(mn) = \sum_{d|nm} f(d)\, g(mn/d)$. d can be written uniquely as $d = d_1 d_2$ with $d_1 | m$, $d_2 | n$. $\Rightarrow h(mn) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2)\, g\left(\frac{mn}{d_1 d_2}\right)$.
But, $f(d_1 d_2) = f(d_1) f(d_2)$, $g\left(\frac{mn}{d_1 d_2}\right) = g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right)$
So $h(mn) = \left(\sum_{d_1|m} f(d_1)\, g(m/d_1)\right)\left(\sum_{d_2|n} f(d_2)\, g(n/d_2)\right) = h(m)\, h(n)$.

Corollary: $\sigma_k = n^k * \mathbb{1}$. $n = p_1^{a_1} \cdots p_k^{a_k}$, p_i distinct primes.

$$\sigma_k(n) = \prod \sigma_k(p_i^{a_i}) = \prod \left(1 + p_i^k + \cdots + p_i^{a_i k}\right) = \begin{cases} \prod (a_i + 1), & k = 0 \\ \prod \left(\frac{p_i^{(a_i+1)k} - 1}{p_i^k - 1}\right), & k \neq 0 \end{cases}$$

3.1.2. Generating Functions.

Definition: For $f: \mathbb{N}_+ \to \mathbb{C}$, define its generating function: $Z_f(s) = F(s) = \sum_{n=1}^{\infty} f(n)/n^s$.

View as either a formal expression, or as a function of $s \in$ region of $\mathbb{C}$ if convergent.

Note: $Z_f = Z_g \iff f = g$.

Proposition: (i) If f is multiplicative then $F(s) = \prod_{p \text{ prime}} \left(1 + f(p)/p^s + f(p^2)/p^{2s} + \cdots\right)$
(ii) If f is strongly multiplicative then $F(s) = \prod_{p \text{ prime}} (1 - f(p)/p^s)^{-1}$

Proof: (i) Writing $n = p_1^{a_1} \cdots p_k^{a_k}$, term on RHS with denominator n^s is $\left(f(p_1^{a_1})/p^{a_1 s}\right) \cdots \left(f(p_k^{a_k})/p^{a_k s}\right) = f(n)/n^s$ - on LHS.
(ii) Here, $\sum_{k=0}^{\infty} f(p^k)/p^{ks} = \sum_{k \geq 0} \left(f(p)/p^s\right)^k = \left(1 - f(p)/p^s\right)^{-1}$

Example: Riemann Zeta-Function. Let $f = \mathbb{1}$. $Z_{\mathbb{1}}(s) = \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$
Proposition $\Rightarrow \zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$, by Euler.

Lemma: $Z_{f*g}(s) = Z_f(s)\, Z_g(s)$
Proof: LHS $= \sum_{n=1}^{\infty} \left(\sum_{d|n} f(d)\, g(n/d)\right) \frac{1}{n^s} = \sum_{d=1}^{\infty} \sum_{e=1}^{\infty} \frac{f(d)}{d^s} \cdot \frac{g(e)}{e^s} =$ RHS, writing $e = n/d$.

Corollary: $f * g = g * f$, $f * (g * h) = (f * g) * h$.
Proof: $F.G = G.F$, $F.(G.H) = (F.G).H$

Examples: (o) $Z_\delta(s) = 1$

(i) $n^k \longleftrightarrow \sum_{n=1}^{\infty} \frac{n^k}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^{s-k}} = \zeta(s-k)$.

(ii) $k=0$: $\mathbb{1} \longleftrightarrow \zeta(s)$.

(iii) $\sigma_k = n^k * \mathbb{1} \overset{\text{Lemma}}{\longleftrightarrow} \zeta(s-k)\zeta(s) = \sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s}$.

(iv) $\varphi(n)$. Fact: $\sum_{d|n} \varphi(d) = n$ $(\varphi * \mathbb{1} = n)$. For each of $\{\frac{1}{n}, \dots, \frac{n}{n}\}$, write as $\frac{a}{d}$ where $d|n$ and $(a,d)=1$, and for fixed d there are $\varphi(d)$ of them.

Lemma $\Rightarrow Z_\varphi(s)\zeta(s) = \zeta(s-1) \Rightarrow \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \zeta(s-1)/\zeta(s)$.

3.1.3. Möbius Inversion Formula.

Theorem: (i) $\sum_{n=1}^{\infty} \mu(n)/n^s = 1/\zeta(s)$.

(ii) $\sum_{d|n} \mu(d) = \delta(n) = \begin{cases} 1, & n=1 \\ 0, & n>1 \end{cases}$

(iii) (MIF): If $g(n) = \sum_{d|n} f(d)$ $\forall n \geq 1$, then $f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) = \sum_{d|n} g(d)\mu(n/d)$

Proof: (i) $1/\zeta(s) \overset{\text{Euler}}{=} \prod_{p \text{ prime}} (1 - 1/p^s) = \sum_{\substack{n=p_1\cdots p_k \\ p_i \text{ distinct}}} (-1)^k/n^s = \sum_{n\geq 1} \mu(n)/n^s$.

(ii) Arithmetic function , Generating Function

$\mu \longleftrightarrow 1/\zeta(s)$

$\mathbb{1} \longleftrightarrow \zeta(s)$

$\mu * \mathbb{1} \longleftrightarrow 1/\zeta(s) \cdot \zeta(s) = 1$ (by proposition)

$\delta \longleftrightarrow 1$

$\Rightarrow \mu * \mathbb{1} = \delta \Rightarrow (\mu * \mathbb{1})(n) = \sum_{d|n} \mu(d) = \delta(n)$.

(iii) $f \longleftrightarrow F(s)$, $g \longleftrightarrow G(s)$. $g = f * \mathbb{1} \Rightarrow G(s) = F(s)\zeta(s) \Leftrightarrow F(s) = G(s)/\zeta(s)$

$g * \mu \longleftrightarrow G(s) \cdot 1/\zeta(s) = F(s) \Rightarrow g * \mu = f$.

Application: $f(n) = \varphi(n) \Rightarrow g(n) = \sum_{d|n} \varphi(d) = n$.

MIF: $\varphi(n) = \sum_{d|n} \mu(d) g(n/d) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} (1 - 1/p)$

3.2. Prime Numbers.

Notation: Enumerate the primes: $2, 3, 5, 7, \dots \longleftrightarrow p_1, p_2, p_3, \dots$ $(p_i < p_j \Leftrightarrow i<j)$

Let $\pi(x) = \#\{p \leq x : p \text{ prime}\} = \max\{n : p_n \leq x\}$.

3.2.1. Facts.

Theorem A (Prime Number Theorem): $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$ $\left(\Leftrightarrow \lim_{n\to\infty} \frac{p_n}{n \log n} = 1\right)$

Theorem B (Euler): $\sum_{p \text{ prime}} \frac{1}{p} = \infty$. In fact, $\lim_{x\to\infty} \left(\sum_{\substack{p\leq x \\ p \text{ prime}}} \frac{1}{p} - \log(\log x) \right)$ exists and is finite.

Theorem C (Dirichlet): For any $a, m \geq 1$, $(a,m) = 1$, $\exists$ infinitely many primes $p \equiv a \bmod m$.

In fact, $\sum_{\substack{p \equiv a \pmod m \\ p \text{ prime}}} \frac{1}{p} = \infty$.

Theorem D (Bertrand Postulate): $p_{n+1} < 2p_n$. -proved by Chebyshev.

3.2.2. Ideas behind Theorems A $\to$ D.

$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$. This is (absolutely) convergent for $Re(s) < 1$
because $\sum_{n=1}^{\infty} \left|\frac{1}{n^s}\right| = \sum_{n=1}^{\infty} \frac{1}{n^{Re(s)}}$, and $\int_1^{\infty} \frac{dx}{x^{\sigma}} < \infty$ for $\sigma < 1$.

Riemann: - $\zeta(s)$ can be defined $\forall\, s \in \mathbb{C} \setminus \{1\}$, by analytic continuation.
- there is a relation between $\zeta(s)$ and $\zeta(1-s)$.

Example: $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \Rightarrow \zeta(-1) = \frac{-1}{12}$.

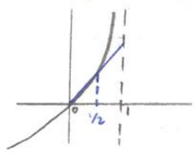
For "decent functions" one can express $\sum_{\substack{p \le x \\ p \text{ prime}}} f(p)$ as something involving $\zeta(s)$, f, integrals.
Roots of $\zeta(s) = 0$ - these appear in the formulae.
Riemann Hypothesis: if $\zeta(s) = 0$, then $s = -2, -4, -6, \dots$, or $s = \frac{1}{2} + it$, $t \in \mathbb{R}$.
If true, $p_{n+1} < p_n + c(\varepsilon)\, p_n^{\frac{1}{2}+\varepsilon}$ $\forall\, \varepsilon > 0$. $\pi(x) - \frac{x}{\log x}$ is "small".

Proof of Theorem B: $\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$. We want $s = 1$.

$\prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{n \le x} \frac{1}{n}$ + some other $\frac{1}{m} \geq \sum_{n \le x} \frac{1}{n}$. $\Rightarrow \sum_{p \le x} -\log\left(1 - \frac{1}{p}\right) \geq \log\left(\sum_{n \le x} \frac{1}{n}\right)$, $0 \le \frac{1}{p} \le \frac{1}{2}$.

Let $f(x) = -\log(1-x)$

$f'(x) = \frac{1}{1-x}$, $f''(x) = \frac{1}{(1-x)^2} > 0$, so f convex.



$\Rightarrow$ for $0 \le x \le \frac{1}{2}$, $f(x) \le 2f\left(\frac{1}{2}\right)x \Rightarrow \sum \frac{1}{p} = \infty$.

Elementary versions of theorem C.

Lemma: $\exists$ infinitely many primes of the form (i) $p \equiv 2 \pmod 3$, (ii) $p \equiv 1 \pmod 3$.

Proof: (i) $q_1, \dots, q_k \equiv 2 \pmod 3$, q_i primes, $k \geq 0$, let $N = \left(\prod_{i=1}^{k} q_i\right)^2 + 1 \equiv 2 \pmod 3$

$\Rightarrow$ if $\exists$ prime $p | N$, $p \equiv 2 \pmod 3$ (if $p = q_i \Rightarrow p | 1$ - absurd), so $p \neq q_1, \dots, q_k$

(ii) Given $q_1, \dots, q_k \equiv 1 \pmod 3$, let $N = \left(2 \prod_{i=1}^{k} q_i\right)^2 + 3 \equiv 1 \pmod 3$

If $p | N$, prime, then $p > 2$, and $x^2 \equiv -3 \pmod p$ has a solution ($x = 2 \prod q_i$).

QRL $\Rightarrow p \equiv 1 \bmod 3$, but, as before, $p \neq q_1, \dots, q_k$.

Dirichlet: uses. $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$ - χ strongly multiplicative, periodic (mod m).

3.2.3. Unknown Facts.

Are there infinitely many primes of the form n^2+1, 2^n+1, 2^n-1 ?
Are there infinitely many prime twins (ie, primes $p, p+2$), such as 17, 19 or 107, 109?
(It is known that $\sum_{p,\, p+2} \frac{1}{p} < \infty$)

Goldbach Conjecture: Is every number $n > 2$, $2 \mid n$ a sum of two primes?
(we know that every sufficiently big number is a sum of 3 primes)

Definition: Mersenne Numbers: $M_n = 2^n - 1$, Fermat Numbers: $F_n = 2 \quad + 1$.

Lemma: (i) M_n a prime $\Rightarrow$ n a prime.
(ii) F_n a prime $\Rightarrow$ $n = 2^k$

Proof: (i) $2^{a \cdot b} - 1 = (2^a - 1)(2^{a(b-1)} + \dots + 2^a + 1)$
(ii) Suppose $n = 2^k q$, q odd. $2^{2^k q} + 1 = (2^{2^k} + 1)(2^{2^k(q-1)} + \dots + 1)$

4. Continued Fractions, Approximations.

4.1. Continued Fractions.

4.1.1. Basic Setup.

$$\alpha \in \mathbb{R} \rightarrow \alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}, \quad a_i \in \mathbb{Z}.$$

Construction: $\alpha = \underbrace{[\alpha]}_{\text{integral part, } a_0 \in \mathbb{Z}} + \underbrace{\{\alpha\}}_{\text{fractional part, } 0 \le \{\alpha\} < 1}$.

If $\{\alpha\} \neq 0$, $\alpha_1 = \frac{1}{\{\alpha\}}$, $\alpha_1 = \underbrace{[\alpha_1]}_{= a_1 \in \mathbb{Z}} + \{\alpha_1\}$, and so on.

Ie, $\alpha_n = [\alpha_n] + \{\alpha_n\}$. If $\{\alpha_n\} = 0$, stop, else $\alpha_{n+1} = \frac{1}{\{\alpha_n\}}$ and continue.

Notation: $\alpha = [a_0, a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$

Fact: The continued fraction expression of α is finite $\Leftrightarrow$ $\alpha \in \mathbb{Q}$ (Euclid's algorithm.

Example: $\alpha = \frac{27}{4} = 6 + \frac{1}{4/3} = 6 + \frac{1}{1 + \frac{1}{3}} = [6, 1, 3]$
Think: $27 = 6 \cdot 4 + 3$, $4 = 1 \cdot 3 + 1$, $3 = 3 \cdot 1$

Example: $\alpha = \frac{1}{2}(1 + \sqrt{5})$, $\alpha^2 = \alpha + 1 \Rightarrow \alpha = 1 + \frac{1}{\alpha}$ $\therefore$ $\alpha = 1 + \cfrac{1}{1 + \frac{1}{\alpha}} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{\alpha}}} = \dots = [1, 1, 1, \dots]$

Definition: If $\alpha = [a_0, a_1, \dots]$, then $\frac{p_n}{q_n} = [a_0, \dots, a_n]$ are convergents to α.

Example: $\pi = [3, 7, 16, \dots]$, $\frac{3}{1}$, $3 + \frac{1}{7} = \frac{22}{7}$, $3 + \cfrac{1}{7 + \frac{1}{16}} = \frac{355}{113}$, ..

4.1.2. Formulae for p_n / q_n. (Take $\alpha \in \mathbb{R} \setminus \mathbb{Q}$)

Convergents: $\frac{p_0}{q_0} = \frac{a_0}{1}$, $\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$,

$$\frac{p_2}{q_2} = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}$$

Table:

a_n			a_0	a_1	a_2
p_n	0	1	a_0	a_0a_1+1	$a_2(a_0a_1+1)+a_0$
q_n	1	0	1	a_1	a_1a_2+1

Theorem: Put $\left.\begin{matrix} p_{-2}=0, \ p_{-1}=1 \\ q_{-2}=1, \ q_{-1}=0 \end{matrix}\right\}$ and define inductively: $\left\{\begin{matrix} p_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{matrix}\right.$ for $n \geq 0$.

Then, $\forall\, n \geq 0$, (A_n): $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$

(B_n): $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$

(C_n): $p_{n-2}q_n - p_n q_{n-2} = (-1)^{n-1} a_n$.

Proof: Induction on $n \geq 0$. $n=0 \Rightarrow (A_0)$: $p_0/q_0 = a_0/1$. Similarly for B_0, C_0.

So assume A_m, B_m, C_m true $\forall\, m \leq n$.

Consider $f(x) = [a_0, \ldots, a_n, x] = a_0 + \cfrac{1}{a_1 \cdots \cfrac{1}{a_n + \frac{1}{x}}} = \frac{Ax+B}{Cx+D}$, some $A,B,C,D \in \mathbb{Z}$.

Now, $\left.\begin{matrix} \frac{B}{D} = f(0) = [a_0, \ldots, a_{n-1}] \overset{(A_{n-1})}{=} p_{n-1}/q_{n-1} \\ \frac{A}{C} = f(\infty) = [a_0, \ldots, a_n] \overset{(A_n)}{=} p_n/q_n \end{matrix}\right\} \Rightarrow f(x) = \frac{p_n x + \lambda p_{n-1}}{q_n x + \lambda q_{n-1}}$, some λ.

But, $f(\frac{-1}{a_n}) = [a_0, \ldots, a_{n-2}] \overset{(A_{n-2})}{=} p_{n-2}/q_{n-2} \Rightarrow \frac{p_{n-2}}{q_{n-2}} = \left(\frac{-p_n}{a_n} + \lambda p_{n-1}\right) / \left(\frac{-q_n}{a_n} + \lambda q_{n-1}\right)$

$\Rightarrow \frac{1}{a_n}(p_{n-2}q_n - p_n q_{n-2}) = \lambda(p_{n-2}q_{n-1} - p_{n-1}q_{n-2}) \overset{(C_n)}{\Rightarrow} (-1)^{n-1} = \lambda(-1)^{n-1} \Rightarrow \lambda = 1$.

Hence, $f(x) = (p_n x + p_{n-1})/(q_n x + q_{n-1})$

Thus: (A_{n+1}): $[a_0, \ldots, a_{n+1}] = f(a_{n+1}) = (p_n a_{n+1} + p_{n-1})/(q_n a_{n+1} + q_{n-1}) = p_{n+1}/q_{n+1}$.

(B_{n+1}): $p_n(\overbrace{q_n a_{n+1} + q_{n-1}}^{=q_{n+1}}) - q_n(\overbrace{p_n a_{n+1} + p_{n-1}}^{=p_{n+1}}) = p_n q_{n-1} - p_{n-1} q_n \overset{(B_n)}{=} (-1)^{n+1}$

(C_{n+1}): $p_{n-1}(q_n a_{n+1} + q_{n-1}) - q_{n-1}(p_n a_{n+1} + p_{n-1}) = a_{n+1}(p_{n-1}q_n - p_n q_{n-1}) = (-1)^n a_{n+1}$.

Corollary of (B_n): (i) $p_{n-1}/q_{n-1} - p_n/q_n = (-1)^n / q_n q_{n-1}$

(ii) $(p_n, q_n) = 1 \ \forall\, n \geq 0$, as $p_{n-1}q_n - q_{n-1}p_n = \pm 1$

4.1.3. Approximations of α by p_n/q_n.

Proposition: (i) $\alpha - p_n/q_n = (-1)^n / q_n(q_n \alpha_{n+1} + q_{n-1})$, (ii) $|\alpha - p_n/q_n| < 1/q_n^2$

(iii) $\lim_{n\to\infty} (p_n/q_n) = \alpha$, (iv) $p_0/q_0 < p_2/q_2 < \ldots < \alpha < \ldots < p_3/q_3 < p_1/q_1$.

Proof: (i) $\alpha = [a_0, \ldots, a_n, \alpha_{n+1}] = f(\alpha_{n+1}) = (p_n \alpha_{n+1} + p_{n-1})/(q_n \alpha_{n+1} + q_{n-1})$

$\Rightarrow \alpha - p_n/q_n = (p_n \alpha_{n+1} + p_{n-1})/(q_n \alpha_{n+1} + q_{n-1}) - p_n/q_n = (p_{n-1}q_n - p_n q_{n-1})/q_n(q_n \alpha_{n+1} + q_{n-1}) = (-1)^n / q_n(q_n \alpha_{n+1} + q_{n-1})$

(ii) By (i), $|\alpha - p_n/q_n| = 1/|q_n| \cdot |q_n \alpha_{n+1} + q_{n-1}| < 1/q_n^2$

(iii) As $q_{n+1} > q_n$ we have $\lim_{n\to\infty} 1/q_n^2 = 0 \Rightarrow \lim_{n\to\infty} |\alpha - p_n/q_n| = 0$.

(iv) By (i), $p_{2k}/q_{2k} < \alpha < p_{2k-1}/q_{2k-1}$

But, $p_{n-2}/q_{n-2} - p_n/q_n = (p_{n-2}q_n - p_n q_{n-2})/q_{n-2}q_n \overset{(C_n)}{=} \frac{(-1)^{n-1} a_n}{q_{n-2}q_n} \begin{cases} < 0, & n \text{ even} \\ > 0, & n \text{ odd.} \end{cases}$

Theorem: For $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $n \geq 0$, then for at least one $k \in \{n, n+1\}$ we have $|\alpha - \frac{p_k}{q_k}| < \frac{1}{2q_k^2}$

Proof: By proposition, we know that α lies in between p_n/q_n, p_{n+1}/q_{n+1}.

$\Rightarrow |\alpha - p_n/q_n| + |\alpha - p_{n+1}/q_{n+1}| = |p_n/q_n - p_{n+1}/q_{n+1}| \overset{(\text{corollary})}{=} \frac{1}{q_n q_{n+1}} \leq \frac{1}{2}\left(\frac{1}{q_n^2} + \frac{1}{q_{n+1}^2}\right)$

(as $2xy \leq x^2 + y^2 \ \forall\, x, y \in \mathbb{R}$)

$\Rightarrow$ for at least one of $n, n+1$, $|\alpha - p_k/q_k| < \frac{1}{2q_k^2}$

4.1.4. Naive Approximation.

Lemma (Dirichlet): if $\alpha \in \mathbb{R}$, $Q > 1 \in \mathbb{Z}$, then $\exists\ p, q \in \mathbb{Z}$, $1 \le q < Q$ such that $|q\alpha - p| \le \frac{1}{Q} < \frac{1}{q}$.

Corollary: For $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\exists$ infinitely many $p/q \in \mathbb{Q}$ such that $|\alpha - p/q| < 1/q^2$.

Proof of Lemma: Take $[0,1]$ with "holes" $[0, \frac{1}{Q}], \dots, [\frac{Q-1}{Q}, 1]$ – Q holes
and "pigeons" $1, \{i\alpha\}$, $i = 0, \dots, Q-1$.
$\Rightarrow$ 2 in 1 hole $\Rightarrow |\{i\alpha\} - \{j\alpha\}| \le \frac{1}{Q} \Rightarrow |q\alpha - p| \le \frac{1}{Q}$.

4.1.5. Back to $|\alpha - p_n/q_n|$

As before, $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.

Proposition: $|q_{n+1}\alpha - p_{n+1}| < |q_n\alpha - p_n|$

Proof: We know that (by Proposition 4.1.3) $|q_n\alpha - p_n| = 1/(q_n\alpha_{n+1} + q_{n-1})$ – ⊛.
But $q_{n+1}\overbrace{\alpha_{n+2}}^{>1} + q_n > \overbrace{q_{n+1}}^{= a_{n+1}q_n + q_{n-1}} + q_n = q_n\overbrace{(a_{n+1} + 1)}^{> \alpha_{n+1}} + q_{n-1} > q_n\alpha_{n+1} + q_{n-1}$,
which, using ⊛, gives the result.

Theorem: If $1 \le q < q_{n+1}$, $p \in \mathbb{Z}$, then $|q\alpha - p| \geq |q_n\alpha - p_n|$, with equality iff $\begin{cases} p = p_n \\ q = q_n. \end{cases}$

Remark: $q \mapsto \text{distance}(q\alpha, \text{nearest integer})$.

Proof: Idea: express p, q in terms of $p_n, q_n, p_{n+1}, q_{n+1}$.
We solve $\begin{cases} p = up_n + vp_{n+1} \\ q = uq_n + vq_{n+1} \end{cases}$, $u, v \in \mathbb{Z}$. Can be close, as $\begin{vmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{vmatrix} = \pm 1$.
Clearly $u \neq 0$.

Case 1: $v = 0 \Rightarrow \left.\begin{matrix} p = up_n \\ q = uq_n \end{matrix}\right\} \Rightarrow |q\alpha - p| = \underset{\geq 1}{|u|} \cdot |q_n\alpha - p_n|$

Case 2: $v \neq 0 \Rightarrow uv < 0$ (as $0 < q < q_{n+1}$) $\therefore$ u, v have opposite signs.
So, $|q\alpha - p| = |\underbrace{u(q_n\alpha - p_n) + v(q_{n+1}\alpha - p_{n+1})}_{\text{have same sign, using Proposition 4.1.3.(i).}}| > |u| \cdot |q_n\alpha - p_n| \geq |q_n\alpha - p_n|$

Corollary: If $|\alpha - p/q| < \frac{1}{2q^2}$, then $\frac{p}{q} = \frac{p_n}{q_n}$ for some $n \geq 0$.

Proof: We assume that $q > 0 \Rightarrow q_n \le q < q_{n+1}$ for some $n \geq 0$.
Consider, $\frac{|pq_n - p_nq|}{qq_n} = \left|\frac{p}{q} - \frac{p_n}{q_n}\right| = \left|\left(\frac{p}{q} - \alpha\right) - \left(\frac{p_n}{q_n} - \alpha\right)\right| \le |\alpha - p/q| + |\alpha - p_n/q_n|$

$$= \frac{1}{q}|q\alpha - p| + \frac{1}{q_n}\underbrace{|q_n\alpha - p_n|}_{\le |q\alpha - p|} \le \underbrace{|q\alpha - p|}_{< \frac{1}{2q}}\underbrace{\left(\frac{1}{q} + \frac{1}{q_n}\right)}_{\le \frac{2}{q_n}} < \frac{1}{qq_n}.$$

$\Rightarrow$ LHS $= 0 \Rightarrow \frac{p}{q} = \frac{p_n}{q_n}$.

4.2. Continued Fractions of Quadratic Irrationals.

4.2.1. Quadratic Irrationals.

Definition: $\alpha \in \mathbb{R}$ is a *quadratic irrational* if $\alpha = x + y\sqrt{\Delta}$, $x, y \in \mathbb{Q}$, $\Delta > 0 \in \mathbb{Z}$, $\sqrt{\Delta} \notin \mathbb{Z}$.
Or, identically, α is a root of $ax^2 + bx + c = 0$, $a, b, c \in \mathbb{Z}$, $a \neq 0$, $\Delta = b^2 - 4ac > 0$, $\sqrt{\Delta} \notin \mathbb{Z}$.

Notation: For $\alpha = x + y\sqrt{\Delta}$, let $\bar{\alpha} = x - y\sqrt{\Delta}$ (also a root of $ax^2 + bx + c = 0$).
$N(\alpha) = \alpha\bar{\alpha} = x^2 - \Delta^2 y^2$ – the *norm*.

Basic Facts: (i) $\alpha = 0 \iff x = y = 0$
(ii) $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$
(iii) $N(\alpha\beta) = N(\alpha)N(\beta)$
(iv) $\alpha \neq 0 \Rightarrow \frac{1}{\alpha} = \bar{\alpha}/N(\alpha)$

Examples: $\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \dots}}}}$ $\qquad \alpha_1 = \frac{1}{\sqrt{3} - 1} = \frac{1}{2}(\sqrt{3} + 1)$

$\alpha_2 = \frac{1}{\alpha_1 - 1} = \frac{2}{\sqrt{3} - 1} = \sqrt{3} + 1 = \alpha + 1.$

$\sqrt{3} = [1, 1, 2, 1, 2, \dots]$, $\sqrt{3} + 1 = [2, 1, 2, 1, \dots]$
$\sqrt{5} = [2, 4, 4, 4, \dots]$, $\sqrt{5} + 2 = [4, 4, 4, \dots]$

4.2.2. Periodic Continued Fractions.

Definition: $\alpha = [a_0, a_1, \dots]$ has a *periodic continued fraction* if $a_{n+m} = a_n$, m fixed $\forall n \geq k$.
It is *purely periodic* if $a_{n+m} = a_n$ $\forall n \geq 0$.

Examples: $\sqrt{5} + 2$, $\sqrt{3} + 1$ – purely periodic. $\sqrt{3}, \sqrt{5}$ – periodic.

Theorem: α has a periodic continued fraction $\iff$ α is a quadratic irrational.

Proof: $(\Rightarrow)$: $\alpha = [a_0, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+m-1}}]$, ie, $a_k, \dots, a_{k+m-1}$ repeats itself.
Let $\beta = \alpha_k = [\overline{a_k, \dots, a_{k+m-1}}]$ – purely periodic. Ie, $\beta = [b_0, \dots, b_{m-1}, b_0, \dots]$ so $\beta_m = \beta$.
$\therefore \beta = \frac{p_{m-1}\beta_m + p_{m-2}}{q_{m-1}\beta_m + q_{m-2}} = \frac{p_{m-1}\beta + p_{m-2}}{q_{m-1}\beta + q_{m-2}}$ $\Rightarrow$ quadratic equation for β. $\Rightarrow \beta$ a quadratic irrational.

But $\alpha = \frac{p_{k-1}\beta + p_{k-2}}{q_{k-1}\beta + q_{k-2}}$ $\Rightarrow$ α is a quadratic irrational, or $\alpha \in \mathbb{Q}$ (assumed not at start)

$(\Leftarrow)$: α a root of $P(x) = Ax^2 + Bx + C = 0$, $\Delta = B^2 - 4AC > 0$, $\sqrt{\Delta} \notin \mathbb{Z}$.
We want $\alpha_n = \alpha_{n+m}$ for some $m < n$. Idea – produce equations for α_m.
We know $\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$ $\Rightarrow$ equation: $A(p_{n-1}\alpha_n + p_{n-2})^2 + B(p_{n-1}\alpha_n + p_{n-2})(q_{n-1}\alpha_n + q_{n-2}) + C(q_{n-1}\alpha_n + q_{n-2})^2 = 0$
Ie, $A_n\alpha_n^2 + B_n\alpha_n + C_n = 0$, where $A_n = Ap_{n-1}^2 + Bp_{n-1}q_{n-1} + Cq_{n-1}^2$; $C_n = A_{n-1}$. (by inspection).
Discriminant, $\Delta_n = B_n^2 - 4A_nC_n = B^2 - 4AC$. Claim: $|A_n| \leq$ const. $\forall n$.
If true $\Rightarrow$ $|C_n|, |B_n| \leq$ const. $\Rightarrow$ finitely many α_n's $\Rightarrow$ $\alpha_n = \alpha_{n+m}$, some $m < n$.
Now, $A_n/q_{n-1}^2 = A\left(\frac{p_{n-1}}{q_{n-1}}\right)^2 + B\left(\frac{p_{n-1}}{q_{n-1}}\right) + C - (A\alpha^2 + B\alpha + C) = \left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right)\left(A\left(\frac{p_{n-1}}{q_{n-1}} + \alpha\right) + B\right)$
We know $\left|\frac{p_{n-1}}{q_{n-1}} - \alpha\right| < \frac{1}{q_{n-1}^2} \leq 1 \Rightarrow \left|\frac{p_{n-1}}{q_{n-1}} + \alpha\right| \leq 2|\alpha| + 1 \Rightarrow |A_n| \leq |A|(2|\alpha| + 1) + |B| =$ const.

Theorem: $\alpha = x + y\sqrt{D}$ has a purely periodic continued fraction $\Leftrightarrow \begin{cases} \alpha > 1 \\ -1 < \bar{\alpha} \end{cases}$

Corollary: For $d > 1$, $\sqrt{d} \notin \mathbb{Z}$, $\alpha = \sqrt{d} + [\sqrt{d}]$ has purely periodic continued fraction.

Proof of Theorem: $(\Rightarrow)$ If $\alpha = [\overline{a_0, \dots, a_{m-1}}]$ then $\alpha_m = \alpha \Rightarrow \alpha > a_0 = a_m \geq 1$.

So, $\alpha = \frac{p_{m-1}\alpha + p_{m-2}}{q_{m-1}\alpha + q_{m-2}} \Rightarrow \alpha$ (and thus $\bar{\alpha}$) root of $P(T) = q_{m-1}T^2 + (q_{m-2} - p_{m-1})T - p_{m-2} = 0$.

Now, $P(-1) = (q_{m-1} - q_{m-2}) + (p_{m-1} - p_{m-2}) > 0 > -p_{m-2} = P(0)$, so $\exists$ root in $(-1, 0)$.

It cannot be α as $\alpha > 1$, so $\bar{\alpha} \in (-1, 0)$.

$(\Leftarrow)$: Assume $\alpha > 1$, $-1 < \bar{\alpha} < 0$. Now, $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$, so $\bar{\alpha}_n = a_n + \frac{1}{\bar{\alpha}_{n+1}} \geq 1 + \frac{1}{\bar{\alpha}_{n+1}}$

So, $\bar{\alpha}_n - 1 \geq \frac{1}{\bar{\alpha}_{n+1}}$. Induction: if $-1 < \bar{\alpha}_n < 0$ then we get $-2 < \bar{\alpha}_n - 1 < -1$,

so $\frac{1}{\bar{\alpha}_{n+1}} < -1 \Rightarrow -1 < \bar{\alpha}_{n+1} < 0$. Ie, $-1 < \bar{\alpha}_n < 0$ $\forall n$.

Substituting into $\bar{\alpha}_n = a_n + \frac{1}{\bar{\alpha}_{n+1}} \Rightarrow a_n = \left[-\frac{1}{\bar{\alpha}_{n+1}}\right]$ $\forall n \geq 0$. – $\circledast$

By previous theorem, know that $\alpha_n = \alpha_{n+m}$, some m, $\forall n \geq$ some k.

$\circledast \Rightarrow a_{k-1} = \left[-\frac{1}{\bar{\alpha}_k}\right] = \left[-\frac{1}{\bar{\alpha}_{k+m}}\right] = a_{k+m-1}$. So $\alpha_n = \alpha_{n+m}$ $\forall n \geq k-1$.

Continue until $k = 0$.

4.3. Pell's Equation.

4.3.1. $x^2 - dy^2 = \pm 1$ and Continued Fractions.

Idea: $\frac{x}{y}$ is close to $\sqrt{d}$.

Notation: $d \in \mathbb{Z}$, $d > 1$, $\sqrt{d} \notin \mathbb{Z}$. Looking for $\alpha = x + y\sqrt{d}$, $x, y \in \mathbb{Z}$.

Write $N(\alpha) = x^2 - dy^2 = \pm 1$

Note: α a solution $\Rightarrow \alpha^n$ a solution (as $N(\alpha^n) = N(\alpha)^n$).

Lemma: If $x^2 - dy^2 = \pm 1$, $x, y > 0$, then $\frac{x}{y} = \frac{p_n}{q_n}$, a convergent to $\sqrt{d}$.

Proof: It is sufficient to show that $\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2}$, and apply corollary 4.1.5.

Case 1: $x^2 - dy^2 = 1 \Rightarrow \left(\frac{x}{y} - \sqrt{d}\right)\left(\frac{x}{y} + \sqrt{d}\right) = \frac{1}{y^2} \Rightarrow \frac{x}{y} > \sqrt{d}$. $\Rightarrow \frac{x}{y} + \sqrt{d} > 2\sqrt{d}$

$\Rightarrow \left|\frac{x}{y} - \sqrt{d}\right| = \frac{1}{y^2|x/y + \sqrt{d}|} < \frac{1}{2\sqrt{d}\,y^2} < \frac{1}{2y^2}$.

Case 2: $x^2 - dy^2 = -1 \Rightarrow \left(\frac{x}{y} - \sqrt{d}\right)\left(\frac{x}{y} + \sqrt{d}\right) = \frac{-1}{y^2} \Rightarrow \frac{x}{y} < \sqrt{d}$. $\Rightarrow \frac{2x}{y} < \frac{x}{y} + \sqrt{d}$

$\Rightarrow \left|\frac{x}{y} - \sqrt{d}\right| = \frac{1}{y^2|x/y + \sqrt{d}|} < \frac{1}{y^2 . 2x/y} = \frac{1}{2xy} \leq \frac{1}{2y^2}$ (as clearly $x \geq y$)

We have $\alpha = \sqrt{d} = [a_0, \dots]$, $[\sqrt{d}] = a_0$. By corollary of theorem 4.2.2, $\sqrt{d} + a_0 = [\overline{2a_0, a_1, \dots, a_{m-1}}]$ has purely periodic continued fraction.

Definition: Let this m be the length of the period.

<u>Proposition</u>: If $p_n^2 - dq_n^2 = \pm 1$, then n is $\left\{\begin{matrix}\text{odd}\\ \text{even}\end{matrix}\right\}$ and $n = km-1$, some $k \geq 1$.

<u>Proof</u>: $\left(\frac{p_n}{q_n} - \sqrt{d}\right)\left(\frac{p_n}{q_n} + \sqrt{d}\right) = \pm 1/q_n^2 \Rightarrow$ sign on RHS is $(-1)^{n-1}$, as $\left(\frac{p_n}{q_n} - \sqrt{d}\right)$ has sign $(-1)^{n-1}$, (proposition 4.1.3)

$\sqrt{d} = \frac{p_n \alpha_{n+1} + p_{n-1}}{q_n \alpha_{n+1} + q_{n-1}} \Rightarrow (p_n - \sqrt{d}\, q_n)\alpha_{n+1} = -p_{n-1} + \sqrt{d}\, q_{n-1}$.

Now multiply by $p_n + \sqrt{d}\, q_n$: $\underbrace{(p_n^2 - dq_n^2)}_{=(-1)^{n-1}}\alpha_{n+1} = \sqrt{d}\underbrace{(p_n q_{n-1} - p_{n-1} q_n)}_{=(-1)^{n-1}} + (\text{integer})$

So, $\alpha_{n+1} = \sqrt{d} + (\text{integer})$

$\Rightarrow \{\alpha_{n+1}\} = \{\sqrt{d}\} \Rightarrow \alpha_{n+2} = \alpha_1 \Rightarrow n+2 = 1+km \Rightarrow n = km-1$.

<u>Theorem</u>: If $n = km-1$ then (i) $p_n^2 - dq_n^2 = (-1)^{n-1}$

(ii) $p_n + q_n\sqrt{d} = (p_{m-1} + q_{m-1}\sqrt{d})^k$.

<u>Proof</u>: (i) $n = km-1$, so $\alpha_{n+1} = \alpha_{km} = \alpha_m = a_0 + \sqrt{d}$, by periodicity, since $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_m}]$.

Hence, $\sqrt{d} = \frac{p_n\alpha_{n+1} + p_{n-1}}{q_n\alpha_{n+1} + q_{n-1}} = \frac{p_n(a_0 + \sqrt{d}) + p_{n-1}}{q_n(a_0+\sqrt{d}) + q_{n-1}} \Rightarrow \begin{cases} dq_n = a_0 p_n + p_{n-1} & ① \\ p_n = a_0 q_n + q_{n-1} & ② \end{cases}$ (equating rational and irrational parts)

So, $① \times (-q_n) + ② \times (p_n) \Rightarrow p_n^2 - dq_n^2 = p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$.

(ii) Induction on k. $k=1$, true. Assume true for $n = km-1$.

Set $x = [a_{n+1}, \ldots, a_{n+m}] = [a_m, a_1, \ldots, a_{m-1}] = a_0 + [a_0, \ldots, a_{m-1}] = a_0 + \frac{p_{m-1}}{q_{m-1}}$. $-\circledast$

Thus, $\frac{p_{n+m}}{q_{n+m}} = [a_0, \ldots, a_n, x] = \frac{p_n x + p_{n-1}}{q_n x + q_{n-1}} = \frac{p_n(a_0 + p_{m-1}/q_{m-1}) + dq_n - a_0 p_n}{q_n(a_0 + p_{m-1}/q_{m-1}) + p_n - a_0 q_n}$, using $\circledast$ and ①, ②.

$= \frac{p_n p_{m-1} + dq_n q_{m-1}}{q_n p_{m-1} + p_n q_{m-1}}$

Now, $(p_{n+m}, q_{n+m}) = 1 \Rightarrow q_n p_{m-1} + p_n q_{m-1} = \lambda q_{n+m}$, $p_n p_{m-1} + dq_n q_{m-1} = \lambda p_{n+m}$.

$\Rightarrow \lambda(p_{n+m} + \sqrt{d}\, q_{n+m}) = p_n p_{m-1} + dq_n q_{m-1} + (q_n p_{m-1} + p_n q_{m-1})\sqrt{d} = (p_n + \sqrt{d}\, q_n)(p_{m-1} + \sqrt{d}\, q_{m-1})$

$= (p_{m-1} + \sqrt{d}\, q_{m-1})^{k+1}$, by induction.

Now, $\lambda(p_{n+m} - \sqrt{d}\, q_{n+m}) = p_n p_{m-1} + dq_n q_{m-1} - (q_n p_{m-1} + p_n q_{m-1})\sqrt{d} = (p_n - \sqrt{d}\, q_n)(p_{m-1} - \sqrt{d}\, q_{m-1})$.

Multiplying together $\Rightarrow \lambda^2 \underbrace{(p_{n+m}^2 - dq_{n+m}^2)}_{=(-1)^{n+m-1}} = \underbrace{(p_n^2 - dq_n^2)}_{=(-1)^{n-1}}\underbrace{(p_{m-1}^2 - dq_{m-1}^2)}_{=(-1)^{m-2}} \Rightarrow \lambda^2 = 1$.

But everything is positive, so $\lambda = 1$.

<u>Theorem</u>: Let $d \in \mathbb{Z}$, $d > 1$, $\sqrt{d} \notin \mathbb{Z}$, let $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_m}]$. Then, all solutions $x, y > 0$ of $x^2 - dy^2 = \pm 1$ are of the form: $x + y\sqrt{d} = (p_{m-1} + q_{m-1}\sqrt{d})^k$, $k \geq 1$, $x^2 - dy^2 = (-1)^{mk}$.

<u>Proof</u>: Combine previous two results.

In particular, if m is even, then there are no solutions of $x^2 - dy^2 = -1$.

<u>Examples</u>: $d = 3$. $\sqrt{3} = [1, \overline{1, 2}]$, $m = 2$. Convergents: $\frac{1}{1}, \frac{2}{1}$. $x + y\sqrt{3} = (2+\sqrt{3})^k$

$d = 5$. $\sqrt{5} = [2, \overline{4}]$, $m = 1$. Convergents: $\frac{2}{1}$. $x + y\sqrt{5} = (2+\sqrt{5})^k$

$d = 7$. $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$, $m = 4$. Convergents: $\frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3}$. $x + y\sqrt{7} = (8 + 3\sqrt{7})^k$

When is m even?

<u>Proposition</u>: Let $p > 2$, prime. (i) If $p \equiv 3 \pmod 4$, $p \mid d$, then $x^2 - dy^2 = -1$ has no solutions $x, y \in \mathbb{Z}$.

(ii) If $p \equiv 1 \pmod 4$, then $x^2 - py^2 = -1$ has a solution.

<u>Proof</u>: (i) $x^2 - dy^2 = -1 \Rightarrow x^2 \equiv -1 \pmod p \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod 4$ $-\!\!\!\not\!\!\times$

(ii) Take solution of $x^2 - py^2 = 1$ with $x, y > 0$, x minimal. Now, $x^2 - y^2 \equiv 1 \pmod 4$.

So, x odd, y even $\Rightarrow (x-1, x+1) = (x+1, 2) = 2$. $x^2 - 1 = (x+1)(x-1) = py^2 \Rightarrow \left(\frac{x+1}{2}\right)\left(\frac{x-1}{2}\right) = p\left(\frac{y}{2}\right)^2$.

$\left(\frac{x+1}{2}, \frac{x-1}{2}\right) = 1$, so fundamental theorem of arithmetic $\Rightarrow$ (i) $\frac{x-1}{2} = pu^2$, $\frac{x+1}{2} = v^2 \Rightarrow v^2 - pu^2 = 1$, $v < x$ $-\!\!\!\not\!\!\times$

or (ii) $\frac{x-1}{2} = u^2$, $\frac{x+1}{2} = pv^2 \Rightarrow u^2 - pv^2 = -1$, as required.

Example: $x^2 - 13.17\,y^2 = -1$ has no solutions $x, y \in \mathbb{Z}$.

4.4. Approximation of Algebraic Numbers.

4.4.1. Algebraic and Transcendental Numbers.

Definition: $\alpha \in \mathbb{C}$ is algebraic if $P(\alpha) = 0$ for some $P(T) = a_0 T^n + \dots + a_n$, $a_i \in \mathbb{Z}$, $a_0 \neq 0$.

If true, there is a minimal degree polynomial (this is the degree of α) which can be normalised so that $(a_0, \dots, a_n) = 1$, $a_0 > 0$. In this case, P is the minimal polynomial of α (irreducible over $\mathbb{Q}$).

Example: $n = 1 \iff \alpha \in \mathbb{Q}$, $\alpha = p/q$ - root of $qT - p$.
$\alpha = x + y\sqrt{d}$, $\sqrt{d} \notin \mathbb{Q}$, $x, y, d \in \mathbb{Q} \Rightarrow \alpha$ is of degree 2.

Definition: $\alpha \in \mathbb{C}$ is transcendental if it is not algebraic.

4.4.2. Liouville's Theorem.

Theorem: If $\alpha \in \mathbb{C}$ is an algebraic number of degree $n > 1$, then $\exists\, c > 0$ such that $|\alpha - p/q| > c/q^n \quad \forall\, p, q \in \mathbb{Z}, q \neq 0$.

Proof: if $\alpha \notin \mathbb{R} \Rightarrow |\alpha - p/q| \geq \operatorname{Im}(\alpha) > 0$ - okay.
Let $\alpha \in \mathbb{R}$, algebraic of degree n, with minimal polynomial $P(T) = a_0 T^n + \dots + a_n$.
Idea: relate $|\alpha - p/q|$ to $|P(\alpha) - P(p/q)|$.
Mean value theorem: $|P(\alpha) - P(p/q)| = |\alpha - p/q| \, |P'(\xi)|$, some $\xi \in (\alpha, p/q)$
$P(\alpha) = 0$ by definition, and $P(p/q) \neq 0$ as P irreducible over $\mathbb{Q}$.
So, $\frac{1}{q^n}(a_0 p^n + a_1 p^{n-1} q + \dots + a_n q^n) = (\text{integer} \neq 0)/q^n \Rightarrow |P(p/q)| \geq 1/q^n$.
Case 1: $|\alpha - p/q| > 1$ - can take $c = 1$ $\left(1 \geq 1/q^2_n\right)$.
Case 2: $|\alpha - p/q| < 1$, so $p/q \in [\alpha - 1, \alpha + 1]$. $\Rightarrow d = \max_{\xi \in [\alpha-1, \alpha+1]} |P'(\xi)|$ exists, $d < \infty$.
So $d(\alpha - p/q) \geq 1/q_n$, so take $c = \min(1, 1/d)$.

4.4.3. Liouville Numbers.

Definition: $\alpha \in \mathbb{R}$ is a Liouville number if $\forall\, c > 0, n \geq 1$, $\exists\, p/q \in \mathbb{Q}$ such that $|\alpha - \frac{p}{q}| < \frac{c}{q^n}$.

Corollary: Every Liouville number is transcendental.

Warning: There are many transcendental numbers which are not Liouville numbers.
For example: π, e.

Proposition: $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is a Liouville number.

Proof: $\alpha \notin \mathbb{Q}$ - clear as its decimal expansion is not periodic.

Take $\frac{p_m}{q_m} = \sum_{n=1}^{m} \frac{1}{10^{n!}}$, with $q_m = 10^{m!}$; $p_m = \sum_{n=1}^{m} 10^{m!-n!}$, $q_m, p_m \in \mathbb{Z}$.

So, $|\alpha - p_m/q_m| = \frac{1}{q_m^{m+1}} \left| 1 + \frac{1}{10^{\text{something}}} + \frac{1}{10^{\text{something bigger}}} + \dots \right| < \frac{1}{q_m^{m+1}} \left| 1 + \frac{1}{10} + \frac{1}{10^2} + \dots \right| = \frac{10}{9} \cdot \frac{1}{q_m^{m+1}}$.

Given $c > 0$, $n \geq 1$, we want $|\alpha - p_m/q_m| < c/q_m^n$, for suitable m.

By above, all we need is $\frac{10}{9} \cdot \frac{1}{q_m^{m+1}} < \frac{c}{q_m^n}$, ie, $\frac{10}{9c} < q^{m+1-n}$.

But this is true for $m \gg 1$, because both $q_m \to \infty$, $m+1-n \to \infty$ as $m \to \infty$.

Remark: The same method shows that $\sum_{k=1}^{\infty} \frac{1}{a^{n_1 \dots n_k}}$ is Liouville if $a > 1$, $a \in \mathbb{Z}$, and $1 \leq n_1 < n_2 < \dots$ - integers.

Liouville's Theorem for $n = 2$.

α a quadratic irrational $\Rightarrow \alpha = [a_0, a_1, \dots]$. $a_n \leq A$, some A, $\forall n$.

$\Rightarrow |q_n \alpha - p_n| = 1/(q_n \alpha_{n+1} + q_{n-1}) > 1/q_n(a_{n+1}+2) \geq 1/(A+2)q_n$. $\Rightarrow |\alpha - p_n/q_n| > 1/(A+2)q_n^2$

As $\frac{1}{A+2} < \frac{1}{2}$, by corollary 4.1.5, if $|\alpha - p/q| \leq 1/(A+2)q^2 < \frac{1}{2q^2}$, then $\frac{p}{q} = \frac{p_n}{q_n}$. - *.

So, $|\alpha - \frac{p}{q}| > 1/(A+2)q^2$ $\forall p, q$.

4.4.4. Diophantine Equations and Approximations.

What about $x^3 - 7y^3 = 18$?

Theorem [Thue-Siegel-Roth]: If α is an algebraic number of degree $n > 1$, then $\forall \varepsilon > 0$ $\exists c(\varepsilon)$ such that $|\alpha - p/q| > c(\varepsilon)/q^{2+\varepsilon}$ $\forall p/q \in \mathbb{Q}$.

Corollary: Let $P(T) = a_0 T^n + \dots + a_n$ be the minimal polynomial of α. ($a_i \in \mathbb{Z}$, $a_0 > 0$, $(a_0, \dots, a_n) = 1$).

Then $P(T) = a_0 (T - \alpha_1) \cdots (T - \alpha_n)$, with $\alpha_1 = \alpha$.

Consider $a_0 x^n + a_1 x^{n-1} y + \dots + a_n y^n = m$ — ⊗ (Eg: for $\alpha = \sqrt[3]{7}$, $P(T) = T^3 - 7$)

If $n > 2$, then ⊗ has only finitely many solutions $x, y \in \mathbb{Z}$ ($\forall m$).

Theorem $\Rightarrow$ corollary: If $x, y \in \mathbb{Z}$, solution of ⊗ $\Rightarrow |P(\frac{x}{y})| = |\frac{m}{y^n}| = a_0 \prod_{i=1}^{n} |\frac{x}{y} - \alpha_i|$.

If x/y is close to α_1, then $|\frac{x}{y} - \alpha_i| \geq \text{const.} > 0$, $i > 1$.

So, $c(\varepsilon)/|y|^{2+\varepsilon} < |\frac{x}{y} - \alpha| \leq \text{const.}/|y|^n \Rightarrow |y| \leq \text{const.}$ (as $2 + \varepsilon < n$).

5. Algorithms.

5.1 Primality Testing.

Want: given $n > 1 \to$ TEST $\to$ n is/isn't prime - without factorising n.

In reality, some composite numbers slip through - "probabilistic algorithms".

5.1.1. Pseudoprimes

Idea: Use Fermat: p prime $\Rightarrow b^{p-1} \equiv 1 \pmod p$ $\forall\, p \nmid b$.

Definition: $n>1$, odd, composite, is called a pseudoprime wrt base b if $b^{n-1} \equiv 1 \pmod n$, $(b,n)=1$.

Example: $b=2$, $n = 11.31 = 341$.

Primality Test (probabilistic): Given $n>1$ odd:

(i) choose at random b, $1 \le b < n$.
(ii) compute $d=(b,n)$, (Euclid). If $d>1$, n is composite.
(iii) if $d=1$, compute $a \equiv b^{n-1} \pmod n$ (use binary expansion of the exponent $n-1$)
(iv) if $a \not\equiv 1 \pmod n$, n is composite.
(v) if $a \equiv 1 \pmod n$ then go to step (i), if you are not tired. If you are tired, deduce that n is probably a prime.

Note on step (iii): "binary expansion". Compute $a \equiv x^{20} \pmod n$. $20 = 2^4 + 2^2$.

$$x \pmod n \mapsto x^2 \pmod n \mapsto \underset{\uparrow a_2}{x^4} \pmod n \mapsto x^8 \pmod n \mapsto \underset{\uparrow a_1}{x^{16}} \pmod n.$$

$a \equiv a_1 a_2 \pmod n$

Problem - there are composite n's such that $b^{n-1} \equiv 1 \pmod n$ - ⊛ holds $\forall\, b$, $(b,n)=1$.

Remark: If n fails ⊛ for at least one b, $(b,n)=1$, then it fails for at least half of the b's, $1 \le b < n$, $(b,n)=1$.

Proof: If ⊛ is true for $b_1, \dots, b_k$ (distinct mod n) but fails for b, then it also fails for $bb_1, \dots, bb_k$. For, $b_i^{n-1} \equiv 1 \pmod n$, $b^{n-1} \not\equiv 1 \pmod n \Rightarrow (bb_i)^n \not\equiv 1 \pmod n$.

5.1.2. Carmichael Numbers.

Definition: An odd composite $n>1$ is a Carmichael number if $b^{n-1} \equiv 1 \pmod n$ $\forall\, b$, $(b,n)=1$.

Fact: There are infinitely many of them.

Proposition: Let $n>1$ be odd and composite. Then,

(i) If $d^2 \mid n$ for some $d>1$, then n is not Carmichael.
(ii) $n = p_1 \cdots p_k$ (p_i distinct primes >2) is Carmichael iff $(p_i - 1) \mid (n-1)$, $1 \le i \le k$.
(iii) $n = p_1 \cdots p_k$ is Carmichael $\Rightarrow k \geq 3$.
(iv) n Carmichael $\Rightarrow b^n \equiv b \pmod n$ $\forall\, b \in \mathbb{Z}$.

Example: $n = 561 = 3.11.17$, $n-1 = 560 = 2^4.5.7$.
$n = 1105 = 5.13.17$, $n-1 = 1104 = 2^4.3.23$.
$n = 1729 = 7.13.19$, $n-1 = 2^6.3^3$

Proof: (i) If $p^2 \mid n$, $p>2$ prime, then $n = p^a m$, $p \nmid m$, $a \geq 2$. Take a primitive root $g \pmod{p^a}$ (such exists). CRT: $\exists\ b \in \mathbb{Z}$ such that $\begin{cases} b \equiv g \pmod{p^a} \\ b \equiv 1 \pmod{m} \end{cases} \Rightarrow (b,n)=1$.
Claim $b^{n-1} \not\equiv 1 \pmod{n}$.
If $b^{n-1} \equiv 1 \pmod n$ then $n-1$ is a multiple of order of $b \pmod n$
$\Rightarrow$ $n-1$ a multiple of order of $g \pmod{p^a} = \varphi(p^a) = p^{a-1}(p-1)$.
$\Rightarrow$ $p^{a-1}(p-1) \mid (n-1)$ – impossible, as $p \mid n$.

(ii) CRT: $b^{n-1} \equiv 1 \pmod n \Leftrightarrow b^{n-1} \equiv 1 \pmod{p_i}$, $1 \leq i \leq k$.
($\Leftarrow$): If $n-1 = (p_i - 1)A_i$ then $b^{n-1} = (b^{p_i - 1})^{A_i} \equiv 1 \pmod{p_i}$, by Fermat.
($\Rightarrow$): If n is Carmichael, take b = primitive root $\pmod{p_i}$ (fix i)
$b^{n-1} \equiv 1 \pmod{p_i} \Rightarrow n-1$ divisible by the order of $b \pmod{p_i} = p_i - 1$.

(iii) If $n = pq$ is Carmichael, (ii) $\Rightarrow$ $(p-1) \mid (n-1)$, $n-1 = pq - 1 = (p-1)q + (q-1)$.
(Say, wlog, $p>q$). So we have $(p-1) \mid (q-1)$ – ✱.

(iv) By CRT, we have to check $b^n \equiv b \pmod{p_i}$, $1 \leq i \leq k$. By (ii), $n = p_1 \cdots p_k$.
If $p_i \nmid b$, then $b^{n-1} \equiv 1 \pmod{p_i} \Rightarrow b^n \equiv b \pmod{p_i}$
If $p_i \mid b$, then $b^n \equiv b \equiv 0 \pmod{p_i}$.

5.1.3. Euler Pseudoprimes.

Fermat: $x^{p-1} \equiv 1 \pmod p$, p prime, $p \nmid x$.
Euler: $x^{\frac{1}{2}(p-1)} \equiv \left(\frac{x}{p}\right) \pmod p$, p prime >2.

Definition: An odd composite $n>1$ is called an Euler Pseudoprime ✱ wrt base b if $b^{\frac{1}{2}(n-1)} \equiv \left(\frac{b}{n}\right) \pmod n$ – ⊛, where $(b,n)=1$ and $\left(\frac{b}{n}\right)$ is the Jacobi symbol.

Remarks: (i) n is an Euler pseudoprime wrt b $\Rightarrow$ n is a pseudoprime wrt b.
(Squaring ⊛ $\Rightarrow$ $b^{n-1} \equiv 1 \pmod n$).
(ii) n an Euler pseudoprime wrt b_1, b_2 $\Rightarrow$ n an Euler pseudoprime wrt $b = b_1 b_2$.

Solovay – Strassen Test (probabilistic): Given $n>1$, odd:
(i) choose at random $1<b<n$
(ii) compute $d = (b,n)$ (Euclid). If $d>1$, n is not prime.
(iii) if $d=1$, compute $a \equiv b^{\frac{1}{2}(n-1)} \pmod n$, compute $\left(\frac{b}{n}\right) = \pm 1$ (reciprocity law, Euclid).
(iv) if $a \not\equiv \left(\frac{b}{n}\right) \pmod n$ then n is not prime.
(v) if $a \equiv \left(\frac{b}{n}\right) \pmod n$ and we are not tired, go to (i)
If we are tired, declare n is probably a prime.

Proposition: $\forall$ odd composite $n>1$, the congruence $b^{\frac{1}{2}(n-1)} \equiv \left(\frac{b}{n}\right) \pmod n$ fails for at least half of b's, $1 \leq b \leq n$, $(b,n)=1$.

Remark: If n passes k tests (ie, $\exists\ k$ b's), we expect n to be not a prime with probability $\leq \frac{1}{2^k}$

Proof of Proposition: It is sufficient to find one b such that $b^{\frac{1}{2}(n-1)} \not\equiv \left(\frac{b}{n}\right) \pmod n$

(Then use same argument as in §5.1.1 $\Rightarrow$ half are bad).

Suppose $\left(\frac{b}{n}\right) \equiv b^{\frac{1}{2}(n-1)} \pmod n \quad \forall\, b,\ (b,n)=1. \Rightarrow 1 \equiv b^{n-1} \pmod n \quad \forall\, b.$

$\Rightarrow n$ is Carmichael $\Rightarrow n = p_1 \cdots p_k$, distinct primes. Select one.

$\exists\ b'$ such that $b' \equiv b \pmod{p_i}$, $2 \le i \le k$. Ie, $b' = b + A p_2 \cdots p_k$.

Since $(p_1, p_2 \cdots p_k) = 1$, may select A so that $\left(\frac{b'}{p_1}\right) = -\left(\frac{b}{p_1}\right)$

Now, $(b, p_i) = 1\ \forall i$, so $(b', p_i) = 1\ \forall i$, so $(b', n) = 1$. And, $\left(\frac{b'}{p_i}\right) = \left(\frac{b}{p_i}\right)\ \forall\, i > 1$.

So, $\left(\frac{b'}{n}\right) = \prod_{i=1}^{k} \left(\frac{b'}{p_i}\right) \ne \left(\frac{b}{n}\right)$, but $(b')^{(n-1)/2} \equiv b^{(n-1)/2} \pmod{p_2}$

$\Rightarrow (b')^{\frac{1}{2}(n-1)} \not\equiv \left(\frac{b'}{n}\right) \pmod{p_2} \Rightarrow (b')^{\frac{1}{2}(n-1)} \not\equiv \left(\frac{b'}{n}\right) \pmod n$, as required.

Example: $n = 15$.

b	± 1	± 2	± 4	± 8
$\left(\frac{b}{15}\right)$	± 1	± 1	± 1	± 1
$b^{\frac{1}{2}(15-1)} \pmod{15}$	± 1	± 8	± 4	± 2

5.1.4. Strong Pseudoprimes.

Observe, $p > 2$ prime, $x^2 \equiv 1 \pmod p \Rightarrow x = \pm \pmod p$.

Write $p - 1 = 2^s . t$, $2 \nmid t$. Take $p \nmid y$, put $z = y^t \pmod p$. $1 \equiv y^{p-1} \equiv z^{2^s}$

The first number in the sequence $z^{2^s}, z^{2^{s-1}}, \ldots, z^2, z \pmod p$ which is not $\equiv 1 \pmod p$ must be $\equiv -1 \pmod p$

Definition: $n > 1$, odd, composite, is a strong pseudoprime wrt base b, $(b,n) = 1$ if the first $\not\equiv 1 \pmod n$ among $b^{2^s . t}, b^{2^{s-1} . t}, \ldots, b^{2t}, b^t \pmod n$ is $\equiv -1 \pmod n$, and obviously $b^{n-1} \equiv 1 \pmod n$. (This also includes the case when they are all $\equiv 1 \pmod n$).

Lemma: For $n \equiv 3 \pmod 4$, n is a strong pseudoprime (wrt b) iff it is an Euler pseudoprime (wrt b).

Proof: $n - 1 = 2.t$, $2 \nmid t$. $b^{n-1} = b^{2t}$, $b^t = b^{\frac{1}{2}(n-1)}$.

n an EPP $\Leftrightarrow b^t = \left(\frac{b}{n}\right) \pmod n$, n an SPP $\Leftrightarrow b^t = \pm 1 \pmod n$.

$E \Rightarrow S$: obvious.

$S \Rightarrow E$: Suppose that $b^t \equiv \pm 1 =: c \pmod n$. As $n \equiv 3 \pmod 4$, we have

$\left(\frac{-1}{n}\right) = -1$, $\left(\frac{1}{n}\right) = 1$, so $\left(\frac{c}{n}\right) = c$. We want $\left(\frac{b}{n}\right) = c$.

$\left(\frac{b}{n}\right) = \left(\frac{b(b^2)^{\frac{1}{4}(n-3)}}{n}\right) = \left(\frac{b^{\frac{1}{2}(n-1)}}{n}\right) = \left(\frac{b^t}{n}\right) = \left(\frac{c}{n}\right) = c.$

Example: $n = 65 = 5.13$, $n - 1 = 64 = 2^6$, $t = 1$, $s = 6$. n is an SPP wrt $b = 8, 18$, but n is not an SPP wrt $b = 8 \times 18$.

$8^2 = 64 \equiv -1 \pmod n$, $8^4 \equiv 1 \pmod n$.

$18^2 = 324 \equiv -1 \pmod n$, $18^4 \equiv 1 \pmod n$.

So, $(8.18)^2 \equiv 1 \pmod n$, but $8.18 \equiv 14 \not\equiv 1 \pmod n$.

Theorem: If $n>1$, odd, composite, $(b,n)=1$, then:

(i) n an SPP wrt $b \Rightarrow n$ an EPP wrt b.

(ii) n an SPP wrt b for at most 25% of b's, $1 \le b \le n$.

* Proof: See Koblitz, pp. 130-133. *.

Miller-Rabin Test (probabilistic): Given $n>1$, odd, write $n-1 = 2^s \cdot t$, $2 \nmid t$.

(i) choose at random b, $1<b<n$.

(ii) compute $d=(b,n)$. If $d>1$, n is composite.

(iii) if $d=1$, compute $y=b^t \pmod n$.

(iv) if $y \equiv \pm 1 \pmod n$, goto (vii)

(v) if $y \not\equiv \pm 1 \pmod n$, compute successive squares: $y^{2^s}, \dots, y^2, y$. If, at some stage, we get $y^a \equiv -1 \pmod n$, goto (vii)

(vi) if none of these is $\equiv -1 \pmod n$ $\Rightarrow$ n composite.

(vii) if not tired, goto (i), else declare n is probably prime.

Theorem: If n passes the test $\forall b < 2(\log n)^2$, then n is a prime. (provided Generalised Riemann Hypothesis holds).

5.2. Factorisation.

Problem: given $n>1$, odd, composite, want a divisor $d \mid n$, $d \neq 1, n$.

5.2.1. Pollard's $p-1$ Method.

This finds a prime number $p \mid n$, provided we know some multiple, k, of $p-1$. We can take $k = B!$, or $k = \mathrm{lcm}(1, \dots, B)$, for some "small" B. (This works only if all prime divisors dividing B are small).

Algorithm: (i) Choose B. Compute $k = \mathrm{lcm}(1, \dots, B)$.

(ii) Choose $1<a<n-2$, comp... $b \equiv a^k \pmod n$.

(iii) Compute $d = \gcd(n, b-1)$ (Euclid). If $d \neq 1, n$, have a non-trivial factor.

(iv) If $d=1, n$, and you are tired, go to (i)

(v) If tired, stop.

5.2.2. Fermat Factorisation.

Idea: If $s \not\equiv \pm t \pmod n$ - ⊗, but $t^2 \equiv s^2 \pmod n$. $\Rightarrow$ Factorisation $(t+s)(t-s) = t^2 - s^2 = kn$.

$\Rightarrow$ $d = \gcd(t+s, n)$, divisor of n, $d \neq 1, n$ by ⊗.

How do we find t, s, k?

Trial and Error - try small $k = 1, 2, 3, \dots$, and for each k try $t = [\sqrt{kn}]+1, [\sqrt{kn}]+2, \dots$
If $t^2 - kn$ is a square, we are done. If not, try the next value.
(See Koblitz, p144 for examples).

5.2.3. Factor Bases.

Aim: Find t, s such that $t^2 \equiv s^2 \pmod{n}$
Idea: Find several numbers t_i such that $t_i^2 \equiv$ product of small primes $\pmod{n}$.
Find some combination $t = t_1 \dots t_k$ such that $t^2 \equiv (\text{small primes}\dots)^2 \pmod{n}$.

Example: $n = 4633$. $67^2 \equiv -144 \equiv -2^4 . 3^2 \pmod{n}$, $68^2 \equiv -9 \equiv -3^2 \pmod{n}$.
$\Rightarrow (67.68)^2 \equiv (2^2 . 3^2)^2 \pmod{n} \Rightarrow$ Factorisation for n.

Definition: A factor base is a set $B \subseteq \{p_1, \dots, p_k\}$, with p_i distinct prime numbers, although we ~~add~~ allow $p_1 = -1$.

In above example, $B = \{-1, 2, 3\}$.

Definition: A B-number is an integer x such that $x \equiv b \pmod{n}$, $|b| < n/2$, and $b =$ product of elements of B.

Aim: Want t_i's such that t_i^2 are B-numbers.

Algorithm: Given $n > 1$, odd, composite:
(i) Choose $B = \{-1, 2, 3, 5, 7, \dots\} = \{p_1, \dots, p_k\} = \{-1\} \cup \{\text{all primes} \in C\}$, some $C \in \mathbb{N}$.
(ii) Generate many numbers t_i such that $t_i^2 \equiv p_1^{\alpha_{i1}} \dots p_k^{\alpha_{ik}} \pmod{n}$, $1 \leq i \leq N$. (Either by trial and error, or by method in §5.2.4).
(iii) Write $\alpha_{ij} = 2\beta_{ij} + \varepsilon_{ij}$, where $\varepsilon_{ij} \in \{0, 1\} \Rightarrow t_i^2 = p_1^{\varepsilon_{i1}} \dots p_k^{\varepsilon_{ik}} (p_1^{\beta_{i1}} \dots p_k^{\beta_{ik}})^2$.
Want to eliminate the non-square part of RHS.
Want $t = t_1^{\gamma_1} \dots t_N^{\gamma_N}$, $\gamma_i \in \{0, 1\}$, such that $t^2 \equiv (\text{square}) \pmod{n}$.
But $t^2 \equiv (\prod_{j=1}^{k} p_j^{\gamma_1 \varepsilon_{1j} + \dots + \gamma_N \varepsilon_{Nj}}) . (\text{square}) \pmod{n}$.
So we need $\gamma_1 \varepsilon_{1j} + \dots + \gamma_N \varepsilon_{Nj} \equiv 0 \pmod{2}$ $\forall j = 1, \dots, k$.
If we can solve these equations for $\gamma_1, \dots, \gamma_N$, we have $t^2 \equiv s^2 \pmod{n}$
(iv) Compute $\gcd(t+s, n)$. If $d \neq 1, n$, have non-trivial factor $d | n$.
(v) If $d = 1, n$, try another $(\gamma_1, \dots, \gamma_N)$.

Examples: (See Koblitz, p.158). $n = 1829$, $B = \{-1, 2, 3, 5, 7, 11, 13\}$.
Try t_i close to $[\sqrt{kn}]$ for $k = 1, 2, 3, 4$. Compute $t_i^2 \pmod{n}$
For example: $t_1^2 \equiv p_1 p_4 p_7 \pmod{n}$, $t_2^2 \equiv p_2^2 p_4 \pmod{n}$, etc.
Need a combination of lines with all entries even.
(See table...)

p_j		-1	2	3	5	7	11	13
t_i	42	1	0	0	1	0	0	1
	43	0	2	0	1	0	0	0
	61	0	0	2	0	1	0	0
	74	1	0	0	0	0	1	0
	85	1	0	0	0	1	0	1
	86	0	4	0	1	0	0	0

$(t_2 t_6)^2 \equiv (2^3 . 5)^2 \pmod{n} \Rightarrow 40^2 \equiv 40^2 \pmod{n}$ - useless.

$(t_1 t_2 t_3 t_5)^2 \equiv (2.3.5.7.13)^2 \pmod{n} \Rightarrow 1459^2 \equiv 901^2 \pmod{n}$.

$d = (1459 + 901, n) = 59 \Rightarrow 1829 = 31 . 59.$

5.2.4 Continued Fraction Method.

We want to generate t_i such that $t_i^2 \equiv$ (something small) $\pmod{n}$.

Proposition: Let $n \in \mathbb{N}$, $n > 1$, $\sqrt{n} \in \mathbb{Z}$. Let $\frac{p_i}{q_i}$ be a convergent to $\sqrt{n}$. Then $p_i^2 \equiv a \pmod{n}$ with $|a| < 2\sqrt{n}$.

Proof: $\sqrt{n}$ lies between $\frac{p_i}{q_i}$ and $\frac{p_{i+1}}{q_{i+1}}$. $|p_i/q_i - p_{i+1}/q_{i+1}| = \frac{1}{q_i q_{i+1}}$.

$\Rightarrow |p_i/q_i - \sqrt{n}| < 1/q_i q_{i+1}$. $|p_i/q_i + \sqrt{n}| < 2\sqrt{n} + 1/q_i q_{i+1}$.

$\Rightarrow |p_i^2 - n q_i^2| = q_i^2 \, |p_i/q_i - \sqrt{n}| . |p_i/q_i + \sqrt{n}| < \frac{1}{q_{i+1}^2} + 2\sqrt{n} . \frac{q_i}{q_{i+1}}$.

$$\Rightarrow |p_i^2 - n q_i^2| < 2\sqrt{n} \underbrace{\left(\frac{q_i}{q_{i+1}} + \underbrace{\frac{1}{2\sqrt{n}\, q_{i+1}^2}}_{< 1/q_{i+1}} \right)}_{< \frac{q_i + 1}{q_{i+1}} \leq 1} < 2\sqrt{n}$$

$\Rightarrow p_i^2 \equiv a \pmod{n}$, $|a| < 2\sqrt{n}$. So we can take $t_i = p_i$.