MATH3301 Summary Notes

Stanley Li

November 3, 2022

Contents

1 Foundations

Definition (Divisibility): We write $d \mid n$ (read "d divides n") if there is an integer a such that $n = ad$.

Equivalently, we say that d is a divisor or factor of n, or that n is a multiple of d.

Lemma (Properties of divisibility): For all n, we have

1. $1, -1 \mid n$
2. $n \mid 0$, and $0 \mid n$ iff $n = 0$
3. $n \mid n$
4. If $d \mid m$ and $m \mid n$, then $d \mid n$
5. If $d \mid n$ then $d \mid mn$ for any m
6. If $d \mid n$ and $d \mid m$, then $d \mid m + n$

Definition (Unit): *A number u is a unit if it has a multiplicative inverse v.*

The units of $\mathbb{Z}$ are ± 1.

Definition (Prime and composite): An integer $n > 1$ is said to be *prime* if for all $d > 0$, $d \mid n$ implies $d = 1$ or $d = n$. We say that n is *composite* if it is not prime.

Negative integers are not classified as prime or composite.

Lemma (Composite numbers): $n > 1$ is a composite number if and only if there exist a and b with $1 < a, b < n$ and $n = ab$.

Definition (Indecomposable): A non-zero, non-unit integer n is said to be indecomposable if whenever $n = ab$ for some a and b, one of a and b are a unit.

Lemma (Prime decomposition): Any integer $n > 0$ can be written as a product of primes, i.e. $n = p_1 \dots p_k$ for $k \geq 0$.

Lemma (Existence of a prime divisor): If $n > 1$ is an integer, either n is prime or it has a prime divisor $p < n$.

Theorem (Infinitude of primes): There are infinitely many primes.

Definition (Prime counting): For $n > 1$, write $\pi(n) = |\{p \in \mathbb{N} \mid p < n, m \text{ is prime}\}|$.

Theorem (Prime Number Theorem): $\pi(n) \sim \frac{n}{\ln(n)}$, that is,

$$\lim_{n \to \infty} \frac{\pi(n)}{\left(\frac{n}{\ln(n)}\right)} = 1$$

2 Linear Diophantine Equations

Definition (GCD): The greatest common divisor $\gcd(a, b)$ of two integers a and b is the largest positive integer d such that $d \mid a$ and $d \mid b$.

Lemma: Suppose that there are integers n, m such that $an + bm = \gcd(a, b)$. Then $ax + by = c$ has an integer solution if and only if $\gcd(a, b) \mid c$.

Lemma (The division algorithm): Given positive integers a and b, there are unique integers q and r with $0 \leq r < a$ such that $b = aq + r$.

Proposition (Transitivity of GCDs): Let a and b be positive integers satisfying $b = aq + r$. Then $\gcd(a, b) = \gcd(r, a)$. In particular, if $r = 0$, then $\gcd(a, b) = a$.

Computing GCDs: Using the Euclidean algorithm, given non-negative integers $a < b$, apply the following

1. If $a \neq 0$, write $b = aq + r$.
2. If $r = 0$, the gcd of the original two integers is a.
3. Otherwise, repeat step 1 with (r, a) in place of (a, b).

By following through the steps of the Euclidean algorithm in reverse

Theorem (Solution to Linear Diophantine Equations in 2 variables): Let a, b, c be integers. Then there are $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $\gcd(a, b) \mid c$.

Definition (Coprime): We say that a and b are *coprime* (or *relatively prime*) if $\gcd(a, b) = 1$.

Equivalently, if there are n, m with $an + bm = 1$.

Lemma (Coprimality and primes): If p is prime, then p and a are coprime if and only if $p \nmid a$.

Proposition (Key property of primes): Let p be prime. Then if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Corollary (Extension of key property of primes): Let p be prime and $p \mid a_1 \dots a_k$. Then $p \mid a_i$.

Theorem (Fundamental Theorem of Arithmetic): Every integer has a unique decomposition as a product of primes.

Definition (Multiplicity): The *multiplicity* of a prime p in a number n is the number of times that p appears in the prime decomposition of n.

Corollary (Orders and divisibility):

1. $d \mid n$ if and only if $\mathrm{ord}_p(d) \leq \mathrm{ord}_p(n)$ for all primes p.
2. For all primes p, $\mathrm{ord}_p(\gcd(a, b)) = \min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$

3 Modular Arithmetic

Definition (Modular congruence): If $a, b, m > 0$ are integers, we say that a is congruent to b modulo m if $m \mid a - b$, written $a \equiv b \mod m$.

Equivalently, $a \equiv b \mod m$ if and only if the remainders on division by m are equal. $\equiv$ is an equivalence relation, and if $n \mid m$, $a \equiv b \mod m$ implies $a \equiv b \mod n$.

Proposition (Addition and multiplication): If $a \equiv a', b \equiv b' \mod m$, then

1. $a + b \equiv a' + b' \mod m$
2. $ab \equiv a'b' \mod m$

Proposition (Divisibility tests):

1. For $n = 3, 9$, $n \mid a$ if and only if $n \mid \sum_{k=0}^{n} a_k$, where a_k are the digits of a in base 10.
2. $11 \mid a$ if and only if $11 \mid \sum_{k=0}^{n} (-1)^k a_k$

Definition (Congruence class): The congruence class of a modulo m is the set of all integers congruent to $a \mod m$

$$[a]_m = \{b \mid b \equiv a \mod m\}$$

Equivalently, these are the equivalence classes of $\equiv \mod n$.

Theorem (Linear congruences in one variable): The equation $ax \equiv b \mod m$ has solutions if and only if $\gcd(a, m) \mid b$.

Lemma (Solutions modulo m): Suppose $d = \gcd(a, m)$ and n is a solution of $ax \equiv b \mod m$. Then

$$n, n + \frac{m}{d}, n + \frac{2m}{d}, \ldots, n + \frac{(d-1)m}{d}$$

are all solutions to this equation, and pairwise incongruent modulo m.

Lemma (Reducing modular congruences): For $d \neq 0$, $a \equiv b \mod m$ if and only if $da \equiv db \mod dm$.

Lemma (Reducing to coprime integers): If $a, b \in \mathbb{Z}$, then $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are coprime.

Lemma (A property of divisibility): If a, b are coprime and $a \mid bc$, then $a \mid c$.

Proposition (Solutions to linear congruences): If n and n' are solutions to $ax \equiv b \mod m$, then $n \equiv n' \mod \left(\frac{m}{\gcd(a,b)}\right)$.

Definition (Modular inverses): We say that b is a modulo m inverse for a if $ab \equiv 1 \mod m$.

Inverses are unique, and we write a^{-1} for the inverse of a modulo m.

Corollary: The integer a has a modulo m inverse if and only if $\gcd(a, m) = 1$.

4 Fundamental Number Theory Results

4.1 Foundational results

Theorem (Chinese Remainder Theorem): Let $m_1, \ldots, m_k$ be pairwise coprime integers. Then the system

$$\begin{aligned} x &\equiv b_1 \mod m_1 \\ x &\equiv b_2 \mod m_2 \\ &\vdots \\ x &\equiv b_k \mod m_k \end{aligned}$$

has a unique solution modulo $M = m_1 \ldots m_k$, namely $x = b_1 M_1 s_1 + \ldots b_k M_k s_k$ where $M_i = M/m_i$ and s_i is a modular m_i inverse for M_i.

Lemma (Divisibility and coprimality): If a, b are coprime, and $a, b \mid n$, then $ab \mid n$.

Corollary (Arbitrary products and divisibility): If a_i pairwise coprime, $a_i \mid n$, $\prod_{i=1}^{k} a_i \mid n$.

Lemma (Self-inverses modulo p): Let p be a prime and $a^2 \equiv 1 \mod p$. Then $a \equiv \pm 1 \mod p$.

Lemma (Multiplication as a bijection): Let a, n be relatively prime. Then the map $[x] \mapsto [ax]$ on congruence classes is a bijection.

4.2 Number theoretic identities

Theorem (Wilson's Theorem): An integer n is prime if and only if $(n-1)! \equiv -1 \mod n$.

Theorem (Fermat's Little Theorem): If p is a prime and a is an integer with $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$. Equivalently, $a^p \equiv a \mod p$ for all a.

Definition (Euler's Totient Function): Euler's totient function ϕ is defined by

$$\phi(n) = \left|\left\{a \in \mathbb{Z}^+ \mid \gcd(a, n) = 1, a \leq n\right\}\right|$$

Lemma (Counting congruence classes): There are exactly $\phi(n)$ congruence classes modulo n whose elements are coprime to n.

Definition (Reduced residue system): A *reduced residue system* modulo n is a set of $\phi(n)$ integers coprime to n that are parwise incongruent modulo n.

Lemma (RRS condition): $\{r_1, \ldots, r_k\}$ is a reduced residue system modulo n if and only if the respective classes enumerate all congruence classes modulo n coprime to n. There are thus exactly $\phi(n)$ elements.

Corollary (Uniqueness of RRS): A reduced residue system is unique up to congruence modulo n and permutation of its elements.

Corollary (Equality of products across RRS): If $\left\{r_1, \ldots, r_{\phi(n)}\right\}$ and $\left\{s_1, \ldots, s_{\phi(n)}\right\}$ are two

reduced residue systems, then

$$\prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} s_i \mod n$$

Proposition (Permuting an RRS): If $\{r_1, \ldots, r_n\}$ is a reduced residue system and $\gcd(a, n) = 1$, then so is $\{ar_1, \ldots, ar_n\}$.

Theorem (Euler): If a and n are coprime, then

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

Lemma (ϕ of a prime power): Let p be prime and $k > 0$. Then $\phi(p^k) = (p-1)p^{k-1}$.

Proposition (Totient is multiplicative): If m and n are coprime, then $\phi(mn) = \phi(m)\phi(n)$.

Corollary (Formula for the totient): If $n = p_1^{r_1} \ldots p_k^{r_k}$, then

$$\phi(n) = (p_1 - 1)p_1^{r_1 - 1} \ldots (p_k - 1)p_k^{r_k - 1} = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

5 Factoring and primality tests

5.1 Pollard's $p-1$ algorithm

Algorithm: (Factoring n) Want to find k such that $p-1 \mid k!$ for some $p \mid n$

1. Pick a coprime to n - if n is odd, take $a = 2$.
2. Compute $a^{k!} \mod n$ for $k = 1, \ldots$, until the first k with $\gcd(a^{k!} - 1, n) \neq 1$.
3. If $\gcd(a^{k!} - 1, n) \neq n$, we have a non-trivial factor of n, otherwise try a different a.

5.2 Primality testing

Definition (Pseudoprime base b): A pseudoprime base b is a non-prime number n such that $b^{n-1} \equiv 1 \mod n$.

Lemma: If $d \mid n$, $b^d - 1 \mid b^n - 1$.

Proposition (Infinitude of pseudoprimes): If n is a base 2 pseudoprime, then so is $2^n - 1$.

Corollary: There are infinitely many base 2 pseudoprimes.

Definition (Absolute pseudoprime): We say that n is an absolute pseudoprime (or a Carmichael number) if $b^{n-1} \equiv 1 \mod n$ for all bases $0 < b < n$ coprime to n.

Theorem (Korselt's criterion): An integer n with prime composition $n = p_1 \ldots p_k$ (for $k \geq 2$) is a Carmichael number if and only if

1. $p_1, \ldots, p_k$ distinct primes
2. $p_i - 1 \mid n - 1$ for all $i = 1, \ldots, k$

Proposition (Roots of $x^2 - 1$ modulo p): If p is an odd prime, $x^2 \equiv 1 \mod p$ has exactly 2 congruence classes

$$x \equiv \pm 1 \mod p$$

as solutions.

Definition (Miller's test): Let $n > 2$ be an odd integer, and write $n - 1 = 2^k m$ where m is odd. We say that n *passes Miller's test* for the base a if $a^m \equiv 1 \mod n$, or $a^{2^j m} \equiv -1 \mod n$ for $0 \leq j < k$.

Lemma (Primes and Miller's test): If p is prime then it passes Miller's test for any coprime base a.

Proposition (Success of Miller's Test): Any odd composite $n > 2$ fails Miller's test for some coprime base a.

Theorem (Probability of Miller's Test failure): For any odd composite $n > 2$, Miller's test fails for at least $\frac{3}{4}$ of the bases up to (but excluding) n.

Primality test: Let $n > 2$ be a positive integer.

1. Pick k different integers $1 \leq a_1, \ldots, a_k \leq n-1$ **at random**.
2. Run Miller's test for each a_i.
3. If one of these tests fails, n is composite. Otherwise, if all pass, the probability that n is *not prime* is at most $\left(\frac{1}{4}\right)^k$.

This is proven later, after developing the theory for primitive roots. We have the following definition from after looking at primitive roots.

Definition (Strong pseudoprime): We say that n is a strong pseudoprime base b if it is not prime but it passes Miller's test in base b.

Unlike the previous primality test, there are no bases n for which every $0 < b < n$ coprime to n is a strong pseudoprime.

Lemma (Number of k^{th} roots of unity modulo p^e): Let p be an odd prime, and $e, k \in \mathbb{Z}_{>0}$. Then the number of solutions to

$$x^k \equiv 1 \mod p^e$$

is exactly $\gcd(k, \phi(p^e))$.

Proposition (Number of primitive $2k^{\text{th}}$ roots of unity modulo p): Let p be an odd prime. Then the number of solutions to

$$x^k \equiv -1 \mod p$$

is exactly $\gcd(2k, p-1) - \gcd(k, p-1)$. If $k = 2^j u$ and $p - 1 = 2^s t$ for $(2, u) = (2, t) = 1$, then

$$\gcd(2k, p-1) - \gcd(k, p-1) = \begin{cases} \gcd(k, p-1) & \text{if } j \leq s-1 \\ 0 & \text{otherwise} \end{cases}$$

We prove slightly weaker versions of the probability bound as above, namely

Theorem (Probability bound, case 1): Let $n = p_1^{e_1} \ldots p_k^{e_k}$, where some $e_i \geq 1$. Then

$$\frac{\left|\left\{b \mid 1 \leq b \leq n, b^{n-1} \equiv 1 \mod n\right\}\right|}{n} \leq \frac{2}{9}$$

That is, Miller's test fails for at most $\frac{2}{9}$ of integers modulo n.

Theorem ((Weaker) probability bound, case 2): Let $n = p_1 \ldots p_k$ where p_i are distinct odd primes and $k \geq 2$. Then

$$\frac{|\{b \mid 1 \leq b \leq n-1, n \text{ passes Miller's test in base } b\}|}{\phi(n)} \leq \frac{7}{12}$$

6 Cryptography

Definition (Cryptosystem): A cryptosystem consists of 3 sets

$$\begin{aligned}\mathcal{P} &= \{\text{plain text messages}\}\\ \mathcal{C} &= \{\text{cipher text messages}\}\\ \mathcal{K} &= \{\text{keys}\}\end{aligned}$$

and two functions $E_k : \mathcal{P} \to \mathcal{C}$ and $D_K : \mathcal{C} \to \mathcal{P}$ for each $k \in \mathcal{K}$, such that $D_k \circ E_k = \mathrm{id}_{\mathcal{P}}$.

Public key cryptography: *Key idea:* Make a cryptosystem where the keys are asymmetric. That is, encryption is significantly easier than decryption.

Lemma (Key result of RSA): Let p, q be distinct primes and $n = pq$. If $\gcd(e, \phi(n)) = 1$ and $de \equiv 1 \mod \phi(n)$, then

$$a^{de} \equiv a \mod n$$

6.1 The RSA cryptosystem

We set

$$\begin{aligned}\mathcal{P} &= \{\text{strings of alphabet digits}\}\\ \mathcal{C} &= \{\text{strings of digits}\}\\ \mathcal{K} &= \{(e, n) \mid n = pq \text{ for } p, q \text{ prime}, \gcd(e, \phi(n)) = 1\}\end{aligned}$$

We keep p and q private, and make e, n public. The encryption and decryption is as follows:

Encryption:

1. Convert letters to 2 digit integers (with a becoming 00 and z becoming 25)
2. Group integers into blocks of identical size such that each block is less than n.
3. For each block integer B_i, set C_i to be the integer obtained by reducing $B_i^e \mod n$.
4. Concatenate these integers C_i together to give the block integer B_i.

We decrypt by using the fact that $C_i^d \equiv B_i \mod n$ for each i (and d can be computed from e and $\phi(n)$).

In practice: In a setting with multiple people, each person picks 2 large primes p and q, and computes $n = pq$, $\phi(n)$, e and d. They then each publish n and e, and keep $p, q, \phi(n)$ and d to themselves.

Note that computing $\phi(n)$ is as computationally difficult as finding the primes p and q, as $\phi(n) = n - (p + q) + 1$, and so $p + q = n - \phi(n) + 1$ and $p - q = \sqrt{(n - \phi(n) + 1)^2 - 4n}$.

Definition (Fast, slow algorithms): We say that an algorithm is *fast* if it requires at most cn^k bit operations for some $c \in \mathbb{R}$ and $k \in \mathbb{Z}$. An algorithm is *slow* if it is not fast.

The process of finding primes p and q is a fast algorithm, while factoring an integer is not known to be a fast algorithm.

7 Power Equations

7.1 Basic properties of orders

Proposition (Existence of solutions to power equations): $a^x \equiv 1 \mod m$ has a non-zero solution if and only if $\gcd(a, m) = 1$.

Definition (Order): Let a, m be such that $\gcd(a, m) = 1$. The order of a modulo m, denoted $\text{ord}_m(a)$, is the least positive x with $a^x \equiv 1 \mod m$.

(This is slightly bad notation, as multiplicity was also given effectively the same notation.)

Proposition: Let $\gcd(a, m) = 1$ and $n \in \mathbb{Z}^+$. Then $a^n \equiv 1 \mod m$ if and only if $\text{ord}_m(a) \mid n$.

Corollary: If $\gcd(a, m) = 1$, $\text{ord}_m(a) \mid \phi(m)$.

Corollary: If $\gcd(a, m) = 1$, $a^i \equiv a^j \mod m$ if and only if $\text{ord}_m(a) \mid i - j$.

Proposition: Let $\gcd(a, m) = 1$. If there is n such that $a^n \equiv b \mod m$, then $\gcd(b, m) = 1$.

7.2 Primitive roots

Definition (Primitive root): We say that a is a primitive root modulo m if $\text{ord}_m(a) = \phi(m)$.

Definition (Multiplicative function): We say that a function $f : \mathbb{N} \to \mathbb{N}$ is multiplicative if for all m, n with $\gcd(m, n) = 1$, $f(mn) = f(m)f(n)$.

Proposition (Totient is multiplicative): If m and n are coprime, then $\phi(mn) = \phi(m)\phi(n)$.[1]

Proposition (Totients and sums): For any integer n,

$$\sum_{d|n} \phi(d) = n$$

Proposition (Multiplicativity and sums): If $f : \mathbb{N} \to \mathbb{N}$ is multiplicative, then so is

$$\tilde{f}(n) = \sum_{d|n} f(d)$$

7.3 Counting elements of a given order

For notation, we may denote $\gcd(a, b)$ as (a, b).

Proposition (Order of a power): Let $d = \text{ord}_m(a)$. Then

$$\text{ord}_m(a^k) = \frac{d}{(d, k)}$$

Proposition (Elements of the same order): If $\text{ord}_p(a) = \text{ord}_p(b)$, then there is some k with $(k, p - 1) = 1$ and

$$b \equiv a^k \mod p$$

[1] This has appeared previously, namely at the end of section 4

Lemma (Polynomials in $\mathbb{Z}/p\mathbb{Z}$): If f is a degree n polynomial with $\mathbb{Z}$-coefficients with leading term $p \nmid a_n$, then f has at most n roots modulo p.

Theorem (Counting elements of given orders): Let p be an odd prime. Then

$$\phi(d) = |a \mid 1 \leq a \leq p-1, \mathrm{ord}_p(a) = d|$$

In particular, the number of primitive roots modulo p is exactly $\phi((p-1)) = \phi(\phi(p))$.

7.4 Existence of primitive roots

The main theorem is that there is a primitive root modulo n if and only if $n = 1, 2, 4, p^k$ or $2p^k$ for some odd prime p.

Proposition (Non-existence of primitive roots modulo 2^k): Let a be an odd integer and $k \geq 3$. Then

$$a^{2^{k-2}} \equiv 1 \mod 2^k$$

In particular, as $\phi(2^k) = 2^{k-1}$, there are no primitive roots modulo k for $k \geq 3$.

Lemma (Computing lifts and primitive roots): Let a be a primitive root modulo p. Then $\mathrm{ord}_{p^2}(a)$ is either $p-1$ or $p(p-1)$.

Thus to compute whether a lifts to a primitive root modulo p^2, it suffices to check that $a^{p-1} \not\equiv 1 \mod p^2$.

Theorem (Existence of primitive roots modulo p^2): Let p be an odd prime. If a is a primitive root modulo p, then either a or $a+p$ is a primitive root modulo p^2.

Theorem (Existence of primitive roots modulo p^k): Let p be an odd prime. If a is a primitive root modulo p^2, then it is a primitive root modulo p^k for all $k \geq 3$.

The following results are from assignment 4, and complete the proof of the main theorem of this section.

Lemma (Orders and the Chinese Remainder Theorem): Let $n = de$ with $(d, e) = 1$, and $(a, n) = 1$. Then $\mathrm{ord}_n(a) = \mathrm{lcm}(\mathrm{ord}_d(a), \mathrm{ord}_e(a))$.

Theorem (Non-existence of primitive roots):

1. If n has two distinct odd prime factors p and q, then there are no primitive roots modulo n.
2. If $4 \mid n$, then there are no primitive roots modulo n.

(Part 2 of the above theorem was not proven in the assignment, but the same reasoning for why part 1 is true also shows part 2)

Theorem (Classification of integers with primitive roots): Let n be a positive integer. Then there is a primitive root modulo n if and only if $n = 1, 2, 4, p^k$ or $2p^k$ for some odd prime p and positive integer k.

8 Continued fractions

8.1 Finite continued fractions

Definition (Finite continued fraction): Let $a_i \in \mathbb{Z}$ for $0 \leq i \leq n$ and $a_1, \ldots, a_n > 0$. Then

$$[a_0, \ldots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

and we refer to $a_0, \ldots, a_n$ as the partial quotients of a.

Theorem (Existence of rational continued fraction expansions): Every rational number $\frac{a}{b}$ can be expressed as a finite continued fraction. Namely, if $(a, b) = 1$, the Euclidean algorithm gives

$$\begin{aligned}
a &= q_1 b + r_1 & \frac{a}{b} &= q_1 + \frac{r_1}{b} \\
b &= q_2 r_1 + r_2 & \frac{b}{r_1} &= q_2 + \frac{r_2}{r_1} \\
&\vdots & & \\
r_{i-1} &= q_{i+1} r_i + r_{i+1} & \frac{r_{i-1}}{r_i} &= q_{i+1} + \frac{r_{i+1}}{r_i} \\
&\vdots & & \\
r_{k-1} &= q_{k+1} r_k + 1 & \frac{r_{k-1}}{r_k} &= q_{k+1} + \frac{1}{r_k}
\end{aligned}$$

Then $\frac{a}{b} = [q_1, \ldots, q_{k+1}, r_k]$.

8.2 Infinite continued fractions

Definition (Convergents): If $[a_0, \ldots, a_n]$ is a finite continued fraction, the k^{th} convergent of $[a_0, \ldots, a_n]$ is $[a_0, \ldots, a_k]$. If $a_0, a_1, \ldots,$ is a sequence with $a_i > 0$ for $i \geq 1$, the k^{th} convergent of this sequence is $[a_0, \ldots, a_k]$.

Theorem (Computing convergents): Let $a_0, a_1, \ldots$ be a sequence with $a_i > 0$ for $i \geq 1$. Define p_i and q_i by the recurrence relations

$$\begin{aligned}
p_0 &= a_0 & q_0 &= 1 & \\
p_1 &= a_1 p_0 + 1 & q_1 &= a_1 & \\
p_i &= a_i p_{i-1} + p_{i-2} & q_i &= a_i q_{i-1} + q_{i-2} & \text{for } i \geq 2
\end{aligned}$$

Then $[a_0, \ldots, a_k] = \frac{p_k}{q_k}$.

Lemma: Let $a_0, a_1, \ldots$ be a sequence with $a_i > 0$ for $i \geq 1$, and p_i, q_i as above. Then

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$$

Corollary (Convergence of convergents): Let $a_0, a_1, \ldots$ be a sequence of integers with $a_i > 0$ for $i \geq 1$, and let p_k, q_k be defined as previously. Then

1. $p_i, q_i \in \mathbb{Z}$, and $(p_k, q_k) = 1$.
2. q_i are positive with $q_k \geq k$.
3. Writing $C_k[a_0, \ldots, a_k]$ we have
$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$
$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}$$
4. The limit $\lim_{k\to\infty} C_k$ exists.

Definition (Infinite continued fraction): Let $a_0, a_1, \ldots$ be a sequence of integers with $a_i > 0$ for $i > 1$. Then
$$[a_0, a_1, \ldots] := \lim_{k\to\infty} [a_0, a_1, \ldots, a_k]$$

Theorem (Computing infinite continued fractions): Let $\alpha \in \mathbb{R}$. Define sequences (α_n) and (a_n) by

$$\alpha_0 = \alpha \qquad a_0 = \lfloor \alpha_0 \rfloor$$
$$\alpha_i = \frac{1}{\alpha_{i-1} - a_{i-1}} \qquad a_i = \lfloor \alpha_i \rfloor \qquad \text{for } i \geq 1$$

Then $\alpha = \lim_{k\to\infty}[a_0, a_1, \ldots, a_k] = [a_0, a_1, \ldots]$.

Corollary (Closeness of convergents): If $\alpha \in \mathbb{R}$ and p_k, q_k are as defined previously, then
$$\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}}$$

Proposition (Uniqueness of continued fraction expansion): Let $[a_0, a_1, \ldots] = [b_0, b_1, \ldots]$. Then $a_i = b_i$ for all $i \geq 0$.

Lemma (Distance between rational numbers): Let $\frac{r}{s}, \frac{p}{q}$ be distinct rational numbers with $s, q > 0$. Then
$$\left|\frac{r}{s} - \frac{p}{q}\right| \geq \frac{1}{sq}$$

Theorem (Convergents and rational approximation): Let $\alpha \in \mathbb{R}$ and $\frac{p_k}{q_k}$ be the k^{th} convergent of the continued fraction expansion of α. If
$$\left|\alpha - \frac{r}{s}\right| \leq \left|\alpha - \frac{p_k}{q_k}\right|$$
Then $s \geq q_k$. That is, $\frac{p_k}{q_k}$ is the best rational approximation to α with denominator at most q_k.

Theorem (Dirichlet's Theorem): Let $\alpha \in \mathbb{R}$. Then α is irrational if and only if there are infinitely many numbers p/q such that
$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

8.3 Solutions to Pell's equation

Definition (Pell's equation): Let d be a non-square integer. Pell's equation for d is of the form
$$x^2 - dy^2 = 1$$

Theorem (Existence of solutions to Pell's equation): The smallest positive solution (x, y) to Pell's equation for d is of the form (p_k, q_k) for some convergent $\frac{p_k}{q_k}$ of $\sqrt{d}$.

Theorem (Characterisation of all integer solutions to Pell's equation): Let (x_0, y_0) be the smallest positive solution to Pell's equation for d. Then (x, y) is a positive solution to Pell's equation if and only if $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^n$ for some $n \in \mathbb{Z}_{>0}$.

9 Quadratic residues

9.1 Basics

Definition (Quadratic residue): We say that a is a quadratic residue modulo m if $m \nmid a$ and there is a solution to $x^2 \equiv a \mod m$.

Theorem (Counting quadratic residues modulo p): Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ quadratic residues modulo p.

9.2 The Legendre symbol

Definition (Legendre symbol): Let p be an odd prime and $a \in \mathbb{Z}$ be such that $(a, p) = 1$. We define the *Legendre symbol* by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{otherwise} \end{cases}$$

Lemma (Legendre symbol is multiplicative): If $(a, p) = (b, p) = 1$, then

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

Lemma (Formula for the Legendre symbol): If $(a, p) = 1$, then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

Proposition (First supplementary law of quadratic reciprocity): For any odd prime p,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Definition (Least modulus residue): If $a \in \mathbb{Z}$, the lesat modulus residue of a modulo p is the unique integer b with $|b| \leq \frac{p-1}{2}$ and $a \equiv b \mod p$.

Lemma (Gauss): Let p be an odd prime, and $a \in \mathbb{Z}$ with $(a, p) = 1$. Consider the least modulus residues of ia, $1 \leq i \leq \frac{p-1}{2}$. If l of them are negative, then

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

Theorem (Second supplementary law of quadratic reciprocity): For any odd prime p, we have

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

Or equivalently

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$$

Lemma (Alternate formula for the Legendre symbol): Let p be an odd prime and $p \nmid a$ an odd integer. Then

$$\left(\frac{a}{p}\right) = (-1)^{L(a,p)}$$

where

$$L(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$$

Theorem (Law of quadratic reciprocity): For distinct odd primes p, q, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = \begin{cases} 1 & \text{if } p \text{ or } q \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \mod 4 \end{cases}$$

10 Miscellaneous results

10.1 Formulae

10.1.1 Modular arithmetic

If p is a prime and a is any integer:

$$(p-1)! \equiv -1 \mod p$$
$$a^p \equiv a \mod p$$

If $(a, n) = 1$, $a^{\phi(n)} \equiv 1 \mod n$.

[[The Chinese Remainder Theorem]]

[[Euclid's algorithm for GCDs and linear Diophantine equations]]

If $d = \gcd(a, n)$ and $d \mid b$, then

$$ax \equiv b \mod n \iff \left(\frac{a}{d}\right) x \equiv \frac{b}{d} \mod \left(\frac{n}{d}\right)$$

When $d \nmid b$, the former equation has no solutions.

10.1.2 Totients

For any $n = p_1^{e_1} \dots p_r^{e_r}$,

$$\phi(n) = (p_1 - 1)p_1^{e_1 - 1} \dots (p_r - 1)p_r^{e_r - 1}$$

We have

$$\sum_{d|n} \phi(d) = n$$

10.1.3 Discrete logarithms

If a, b are coprime to n, m is an integer and r is a primitive root modulo n, then

$$\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r(a) + \operatorname{ind}_r(b) \mod \phi(n)$$
$$\operatorname{ind}_r(a^m) \equiv m \operatorname{ind}_r(a) \mod \phi(n)$$

10.1.4 Continued fractions

If $\frac{a}{b}$ is a rational number in lowest form, its continued fraction is $[q_1, \dots, q_{k+1}, r_k]$, where

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$\vdots$$
$$r_k = q_{k+1} r_{k-1} + 1$$

10.2 Workshop 1

Proposition (Cycle lengths of decimal expansions): The decimal cycle length of a non-integer fraction $\frac{a}{b}$ in lowest terms (with $b = 2^{n_1}5^{n_2}b'$ and $(10, b') = 1$) is $\mathrm{ord}_{10}(b')$.

10.3 Assignment 1

We have $\mathrm{lcm}(a, b)\gcd(a, b) = ab$.

10.4 Workshop 3

Lemma (Divisibility and totients): If $a \mid b$, then $\phi(a) \mid \phi(b)$.

10.5 Assignment 2

Proposition (Infinitude of primes): If q is an odd prime and p is a prime factor of $2^q - 1$, then $p \equiv 1 \mod q$.

10.6 Workshop 5

Proposition (Power sums modulo p): Let p be a prime and mk be an integer. Then

$$\sum_{a=1}^{p-1} a^k = \begin{cases} -1 & \text{if } p-1 \mid k \\ 0 & \text{otherwise} \end{cases}$$

10.7 Assignment 4

Proposition (Estimating totients): For any integer n, we have $\phi(n) \leq n - 1$, with equality if and only if n is prime. If n is composite, $\phi(n) \leq n - \sqrt{n}$.

10.8 Workshop 10

Proposition (Cubes modulo p): Let p be a prime. If $p \equiv 1 \mod 3$, there are $(p-1)/3$ cubic residues modulo p, and otherwise there are $p - 1$ cubic residues modulo p.