MATH342 Review Notes

By Jack 'jryzkns' Zhou

1 The division Algorithm

If $a, b \in \mathbb{Z}$ with $b > 0$, then $\exists!(q, r) \in \mathbb{Z}$[1] s.t.

$$a = bq + r; \quad 0 \leq r < b$$

2 Divisibility and Primes

If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say that a *divides* b if $\exists c \in \mathbb{Z}$ s.t. $b = ac$. We write this relationship as $a \mid b$. If a *does not divide* b, we write $a \nmid b$.
Below are some properties of divisibility, using $a, b, c \in \mathbb{Z}$ and $m, n \in \mathbb{Z}$:

- $a \mid b \wedge b \mid c \rightarrow a|c$
- $c \mid a \wedge c \mid b \rightarrow c|(ma + nb)$

An integer n is said to have *odd* parity when $n \nmid 2$, and otherwise *even* parity when $n \mid 2$. Often times an odd number can be written in the form $n = 2k + 1$ for some integer k, and $n = 2k$ for even numbers.
A *prime* is an integer greater than 1 thatis divisible by no positive integers other than 1 and itself. Otherwise, a number is said to be a *composite*. Note that by this definition. The number 2 is a prime. Often times there will be indications to exclude 2 from primes by specifying odd primes.
Here are some facts about prime numbers, where $n \in \mathbb{Z}$:

- when $n > 1$, $p \mid n$ for some prime $p \leq n$
- There are infinitely many primes
- If n is composite, then $p \mid n$ for some prime $p \leq \sqrt{n}$

The function $\pi(x)$ where x is a positive real number denotes the number of primes not exceeding x.

Dirichlet's Theorem in Arithmetic Progressons

Suppose that $a, b \in \mathbb{N}$ where $(a, b) = 1$. Then the arithmetic progression $an + b, n \in \mathbb{N}$ contains infinitely many primes.

3 Greatest Common Divisors

The *greatest common divisor* (GCD) of $a, b \in \mathbb{Z}$ is the largest divisor d such that $d \mid a$ and $d \mid b$. The GCD of a and b are often written as $\gcd(a, b)$ or (a, b).
One way to describe the GCD is that a positive integer d is a GCD iff:

- $d \mid a$ and $d \mid b$
- if $c \in \mathbb{Z}$ s.t. $c \mid a$ and $c \mid b$, then $c \mid d$

Some facts about GCD's:

- Two integers $a, b \in \mathbb{Z}$ are said to be *relatively prime* if $(a, b) = 1$
- Suppose $d = (a, b)$, then $(\frac{a}{d}, \frac{b}{d}) = 1$
- A fraction $\frac{p}{q}$ is in lowest terms when $(p, q) = 1$
- suppose $(a, b) = 1$ and $a|bc$, then $a|c$
- The notion of GCD's applies to multiple values too, suppose $a_1, a_2, \cdots, a_n \in \mathbb{Z}$, then

  $$(a_1, a_2, \cdots, a_n) = (a_1, a_2, \cdots, (a_{n-1}, a_n))$$

  Note that simply with the above definition, $(a_1, a_2, \cdots, a_n) = 1$ means that these numbers are *mutually relatively prime*. A stronger statement is *pairwise relatively prime*, where for any pair of the numbers a_i and a_j with $i \neq j$, $(a_i, a_j) = 1$.

Bezout's Theorem

If $a, b \in \mathbb{Z}$, then $\exists m, n \in \mathbb{Z}$ s.t.

$$ma + nb = (a, b)$$

Where m, n are denoted the bezout coefficients to a, b. Furthermore, $(a, b) = 1 \Leftrightarrow ma + nb = 1$.
The set of linear combinations of a, b is the set of integer multiples of (a, b).

Euclidean Algorithm (+Backtracking)

The Euclidean Algorithm computes (a, b). It proceeds by heavily using a property of GCD's:
Let $b, q, r \in \mathbb{Z}$,

$$(bq + r, b) = (b, r)$$

Suppose $a = bq + r$ (by the division algorithm), we have $(a, b) = (b, r)$. As $0 \leq r < b$, the RHS will always be in lower terms: each time we apply this property, we will get smaller computations to carry out until a base case of $(b, 0)$ is reached, in which case $(b, 0) = b$.
Once the series of division algorithms are applied, the results can be used in reverse with substitution to find the bezout coefficients.
As a side note, suppose we have f_{n+1}, f_{n+2} be successive terms of the Fibonacci Sequence with $n > 1$, then the Euclidean algorithm takes exactly n divisions to show that $(f_{n+1}, f_{n+2}) = 1$.

[1]The symbol $\exists!$ indicates that the existence is unique

4 Continued Fraction Expansions

Given the sequence $a_0, a_1, a_2, \cdots$ (may be infinite), a continued fraction is a fraction of the following form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

A fraction of this form can also be written as $[a_0, a_1, a_2, \cdots]$. If the sequence is infinite and has repeating elements, we denote one instance of the repeating values with a line drawn over it.
The numbers $a_1, a_2, \cdots, a_n$ are called *partial quotients* of the continued fraction, and if all a_i's are integers, the continued fraction is said to be a *simple* continued fraction. We are only concerned with *simple* continued fractions and unless otherwise stated, all continued fractions under discussion are simple.

Finite Continued Fractions

For a rational number that can be expressed as $\frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $p > q$. Its continued fraction expansion is finite. The way to generate the expansion is to consider the division algorithms applies when computing (p, q). For each row, it will be of the form $a = q \cdot b + r$. We apply the following transformation:

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

The $\frac{b}{r}$ term will correspond to the LHS on the next row, recall that the next row would be computing b divided by r, and thus a substitution can be made. We can continuously apply these substitutions until a continued fraction is formed.

Infinite Continued Fractions

For an irrational number n, its continued fraction expansion is computed in the following manner:

$$\alpha_0 = n$$
$$a_i = [\alpha_i] \quad \alpha_{i+1} = (\alpha_i - a_i)^{-1}$$

It's good to note that a_i is the integral component to α_i, and that $\alpha_i - a_i$ is the fractional component to α_i.

Convergents

Given a continued fraction

$$C = [a_0; a_1, a_2, \cdots, a_n]$$

and $C_k = [a_0; a_1, a_2, \cdots, a_k]$ with $0 < k \leq n$, C_k is called the kth convergent of C. Given C, we can compute all of the convergents of C as follows:

$$\begin{aligned}
&p_0 = a_0 && q_0 = 1 && \\
&p_1 = a_0 a_1 + 1 && q_1 = a_1 && C_1 = \frac{p_1}{q_1} \\
&p_k = a_k p_{k-1} + p_{k-2} && q_k = a_k q_{k-1} + q_{k-2} && C_k = \frac{p_k}{q_k}
\end{aligned}$$

5 Linear Diophantine Equations

A linear diophantine equation in two variables is an equation of the follow form

$$ax + by = c$$

where $a, b, c \in \mathbb{Z}$ and an integer solution (x, y) is sought for. In general, an equation that is linear in the coefficients to the polynomial powers would be considered a diophantine equation. We will focus on linear diophantine equations in two variables. Much of the results we find here applies to diophantine equations of more than two variables.
Let $d = (a, b)$. If $d \nmid c$, then the diophantine equation in question has no integral solutions. If $d \mid c$, then there are infinitely many solutions (granted that there are no restrictions on the solution space). Indeed, once we have an initial solution (x_0, y_0), the rest of the solutions will all be of the form

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n$$

for any integer n. Notice the minus sign on y.

Systems of Linear Diophantine Equations

When there is a system of linear diophantine equations (most commonly two equations in 3 variables), the ideal approach is to substitute one equation into another, to reduce the system into a single equation. From there, solve as intended and substitute back for a full solution.

6 The Fundamental Theorem of Arithmetic

Every positive integer greater than 1 is *uniquely* expressible as a product of primes, with the prime factors in non decreasing order:

$$n = \prod_i p_i^{a_i}$$

The sequence of a_i's denote the exponents to each of the prime factors. If a prime factor $p_i \nmid= n$, then $a_i = 0$.
Using this prime factorization form, we can describe the GCD and LCM (least common multiple) as follows, letting $a = \prod_i p_i^{a_i}$ and $b = \prod_i p_i^{b_i}$:

$$(a, b) = \prod_i p_i^{\min(a_i, b_i)} \quad [a, b] = \prod_i p_i^{\max(a_i, b_i)}$$

As $\max(a_i, b_i) + \min(a_i, b_i) = a_i + b_i$, we can see from above that $(a, b) \cdot [a, b] = ab$

7 Congruences

Let m be a positive integer. If $a, b \in \mathbb{Z}$, we say that a is *congruent* to b modulo m if $m \mid (a-b)$. Furthermore, we can write $a \equiv b \pmod{m}$ iff $a = b + km$ for some integer k. Here are some properties about arithmetic in modulo m:

- $a + c \equiv b + c \pmod{m}$
- $a - c \equiv b - c \pmod{m}$
- $ab \equiv bc \pmod{m}$

The congruence relation over a modulus forms an *equivalence class*, which satisfies the following properties:

- Reflexitivity: $a \equiv a \pmod{m}$
- Symmetricity: $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$
- Transitivity: $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

A number in a modulo number system itself is referred to as a residue. If a, b are congruent mod m, then their residues $a \pmod{m}$ and $b \pmod{m}$ have to be the same as well.
A complete system of residues modulo m is a set of integers such that every integer is congruent to exactly one integer of the set. Of which, the least non-negative residues modulo m is the set

$$\{0, 1, \cdots, m-1\}$$

When m is odd, the absolute least residues modulo m is the set

$$\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \cdots, -1, 0, 1, \frac{m-3}{2}, \frac{m-1}{2}\right\}$$

If $a, b, c, m \in \mathbb{Z}^+$ with $d = (c, m)$ and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{\frac{m}{d}}$. In the case that $(c, m) = 1$, we simply have $a \equiv b \pmod{m}$.
If we have $a \equiv b \pmod{m_i}$ for several values of i and each m_i are pairwise coprime, then $a \equiv b \pmod{\prod_i m_i}$.
For a given integer $a \in \mathbb{Z}/m\mathbb{Z}$, a is either *invertible* or a *zero-divisor*. We focus on the case of invertibility. For an invertible a, its *inverse* is a quantity a^{-1} such that $a^{-1}a \equiv 1 \pmod{m}$.
For a prime p and $(a, p) = 1$,

$$a \equiv a^{-1} \pmod{p} \Leftrightarrow a \equiv \pm 1 \pmod{p}$$

8 Linear Congruences

A linear congruence in one variable is of the form

$$ax \equiv b \pmod{m}$$

It can be similarly seen as a linear diophantine equation of the form $ax - my = b$. Analoguous to the study of linear diophantine equations, we can see that with $(a, m) = d$, if $d \mid b$, then $ax \equiv b \pmod{m}$ has d incongruent solutions. The way to find these solutions follow from solutions of linear diophantines of the same kind.
In particular, if $(a, m) = 1$, then there is one unique solution, which can by found by $x \equiv a^{-1}b \pmod{m}$.

9 Chinese Remainder Theorem

Let $m_1, m_2, \cdots, m_r$ be pairwise coprime positive integers. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = \prod_i^r m_i$. The solution will be a sum where each term will turn to 0 for all modulo's except one. That term will be focused on solving specifically that congruence. It's important to take a mod M at the end.
If $a, b \in \mathbb{Z}^+$, then the least positive residue of $2^a - 1$ modulo $a^b - 1$ is $2^r - 1$, where r is the least positive residue of $a \pmod{b}$.
If $a, b \in \mathbb{Z}^+$, then $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$. With this we can also see that $(2^a - 1, 2^b - 1) = 1 \Leftrightarrow (a, b) = 1$.
Suppose we have a polynomial $f(x)$ and we want to solve the congruence $f(x) \equiv 0 \pmod{m}$. We can obtain its solution by splitting m into its prime factors and create a system of congruences. From there, we can proceed by applying the chinese remainder theorem.

10 Wilson's Theorem

If $n \geq 2$, then n is prime iff

$$(n-1)! \equiv -1 \pmod{n}$$

11 Fermat's Little Theorem

If p is prime and a is an integer with $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

This theorem can take on multiple forms, such as

$$a^p \equiv a \pmod{p}$$

and for finding inverses,

$$a^{p-2} \equiv a^{-1} \pmod{p}$$

12 Pseudoprimes

Let b be a positive integer. If n is a composite positive integer and $b^n \equiv b \pmod{n}$, then n is called a pseudoprime to the base b. Note that this shows that the converse of FLT does not hold. Generally pseudoprimes are composites that pass a certain primality condition, such as the converse of FLT.

If d, n are positive integes s.t. $d \mid n$, then $2^d - 1 \mid 2^n - 1$. There are also infinitely many pseudoprimes to the base 2.

A composite number n is said to be a *Carmichael* number if

$$b^{n-1} \equiv 1 \pmod{n}$$

for any natural b where $(b, n) = 1$. If n is of the form $n = p_1 \cdot p_k$, where each p_i are distinct primes and $p_i - 1 \mid n - 1$ for any i, then n is a Carmichael number.

13 Euler Totient

The function $\phi(n)$ is defined to be the number of positive integers not exceeding n, which are relatively prime to n. For a value n with the prime power factorization $n = \prod_i p_i^{a_i}$, $\phi(n)$ has many properties:

- $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$
- $\phi(n) = \prod_i p_i^{a_i - 1}(p_i - 1)$
- For a prime p, $\phi(p) = p - 1$
- For a prime p, integer $a > 0$, $\phi(p^a) = p^a - p^{a-1}$
- $a \mid b \Rightarrow \phi(a) \mid \phi(b)$
- $(m, n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$
- $\phi(n)$ is even when $n > 2$

To get point 1 on above, consider point 4 above and carry out the following manipulations:

$$\begin{aligned}
\phi(n) &= \phi(\prod_i p_i^{a_i}) \\
&= \prod_i \phi(p_i^{a_i}) \\
&= \prod_i (p_i^{a_i} - p_i^{a_i - 1}) \\
&= \prod_i p_i^{a_i}(1 - p_i^{-1}) \\
&= n \prod_i (1 - p_i^{-1}) \\
&= n \prod_{p|n} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

The Euler Totient is considered a *multiplicative* function, which will be described in greter detail later on.

With knowledge of the Euler totient, we can present a more generalized version of FLT:

Euler's Theorem

If m is a positive integer and a is an integer with $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

14 Multiplicative Functions

A *arithmetic* function is a function that is defined for all positive integers. An arithmetic function is *multiplicative* when if $(m, n) = 1$, $f(mn) = f(m)f(n)$. A *totally-multplicative* function ignores the coprimality condition. One example of a multiplicative function is the Euler Totient function.

A multiplicative function is easy to compute when it can be broken down into calls with smaller arguments.

Let f be an arithmetic function, then

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

is called the *summatory* function of f. A function f is multiplicative iff its summatory function F is multiplicative as well.

Let n be a positive integer, then $n = \sum_{d|n} \phi(d)$.

Sum and Number of divisors

The sum of divisors function σ is defined as the sum of all positive divisors of n, including n itself. The number of divisors function τ is defined as the number of positive divisors of n, including n itself:

$$\sigma(n) = \sum_{d|n} d \quad \tau(n) = \sum_{d|n} 1$$

Both σ and τ are multiplicative.

Let p be a prime and a be a positive integers, we have

$$\sigma(p^a) = p^0 + p^1 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1} \quad \tau(p^a) = a + 1$$

Generalizing to non-primes, if we have $n = \prod_i p_i^{a_i}$,

$$\sigma(n) = \prod_i \frac{p_1^{a_i + 1} - 1}{p_i - 1} \quad \tau(n) = \prod_i (a_i + 1)$$

15 Perfect and Mersenne Numbers

A positive integer n is said to be a *perfect* number if $\sigma(n) = 2n$. At the moment we only know of even perfect numbers and there aren't any know odd perfect numbers. An even number is perfect iff

$$n = 2^{m-1}(2^m - 1)$$

where $m \geq 2$ is an integer and $2^m - 1$ is prime.
If m is a positive integer, then $M_m = 2^m - 1$ is called the mth *Mersenne Number*. If p is prime and $M_p = 2^p - 1$ is also prime, then M_p is called a *Mersenne Prime*. If m is a positive integer and M_m is prime, then m must be prime.
If p is an odd prime, then any divisor of M_p is of the form $2kp + 1$, where k is a positive integer.

16 Mobius Inversion

To invert a summatory function, we can proceed as follows:

$$f(n) = \sum_{d|n} \mu(d)F(n/d)$$

where μ is a multiplicative Mobius function defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ (-1)^r & \text{if } n = p_1p_2\cdots p_r, \text{where } p_i \text{ are primes;} \\ 0 & \text{otherwise.} \end{cases}$$

The summatory function of μ satisfies

$$F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1. \end{cases}$$

Because σ and τ are summatory functions to $f(n) = n$ and $f(n) = 1$, we can apply mobius inversion to get

$$\sum_{d|n} \mu\left(\frac{n}{d}\right)\sigma(d) = n, \quad \sum_{d|n} \mu\left(\frac{n}{d}\right)\tau(d) = 1$$

17 RSA Cryptography

RSA is a public key encryption/decryption scheme that relies on the difficulty in factoring large numbers. The setup involves the following:

- Let $n = pq$, with p, q being distinct primes
- Encryption exponent $e \in \mathbb{Z}$ s.t. $(e, \phi(n)) = (e, \phi(pq)) = (e, \phi(p)\phi(q)) = (e, (p-1)(q-1)) = 1$
- Decryption exponent $d \in \mathbb{Z}$ s.t. $de \equiv 1 \pmod{\phi(n)}$

Letting P be the plaintext and C be the ciphertext, we define our encryption function E and decryption function D as follows:

$$C = E(P) = P^e \pmod{n}$$

$$P = D(C) = C^d \pmod{n}$$

Taking a closer look at how D works,

$$\begin{aligned} D(C) &\equiv D(E(P)) && \pmod{n} \\ &\equiv (P^e)^d \equiv P^{ed} && \pmod{n} \\ &\equiv P^{1+k\phi(n)} && \pmod{n} \\ &\equiv P(P^{\phi(n)})^k && \pmod{n} \\ &\equiv P && \pmod{n} \end{aligned}$$

Suppose there are two parties A, B, and A wants to send B a message. B will start with generating two primes p, q to compute n, $\phi(n) = (p-1)(q-1)$, and exponents e and d. B can now make n, e public. Given n, e, A can compute $C = E(P) = P^e \pmod{n}$ to send to B.
The security in this cryptosystem lies in the fact that given e and n, it is difficult factoring n to determine d.
One important fact to note is that if $\phi(n)$ was made public, it is easy to factor n based off of that:

$$\begin{aligned} \phi(n) &= \phi(pq) \\ &= \phi(p)\phi(q) \\ &= (p-1)(q-1) \\ &= pq - (p+q) + 1 \end{aligned}$$

Therefore, $p + q$ is a known quantity. As an aside we observe that $(p-q)^2 = (p+q)^2 - 4pq = (p+q)^2 - 4n$. With $p - q = \sqrt{(p+q)^2 - 4n}$, so we can know $p + q$ and $p + q$. Therefore, p, q can be obtained.

18 Order of an integer

Let $a, nin\mathbb{Z}$ with $(a, n) = 1$, $a \neq 0$, $n > 0$. The least positive $x \in \mathbb{Z}$ s.t. $a^x \equiv 1 \pmod{n}$ is called the *order* of a modulo n, denoted as $\text{ord}_n a$. In other words

$$a^{\text{ord}_n a} \equiv 1 \pmod{n}$$

A positive integer x is a solution to $a^x \equiv 1 \pmod{n}$ iff $\text{ord}_n a \mid x$.
It follows from Euler's Theorem that for any a that is coprime to the modulo n, $\text{ord}_n a \mid \phi(n)$.
If $(a, n) = 1$, $a^i \equiv a^j \pmod{n}$ iff $i \equiv j \pmod{\text{ord}_n a}$.

Primitive Roots

If $r, n \in \mathbb{Z}$ with $(r, n) = 1$, and if $\text{ord}_n r = \phi(n)$, then r is called a *primitive root* of n. Every prime has a primitive root.
If $(r, n) = 1$ and r is a primitive root of n, then the integers $r^1, r^2, \cdots, r^{\phi(n)}$ form a reduced residue system modulo n. We can see that when r is a primitive root and $(a, n) = 1$, $a \equiv r^x \pmod{n}$ for some x.
Suppose we have an exponent $u \in \mathbb{Z}^+$, then

$$\text{ord}_n(a^u) = \frac{\text{ord}_n a}{(\text{ord}_n a, u)}$$

We can see above that if a is a primitive root, then a^u is a primitive root iff $(\text{ord}_n a, u) = (\phi(n), u) = 1$.
If a positive integer n has a primitive root, then it has a total of $\phi(\phi(n))$ incongruent primitive roots.

19 Discrete Logarithms

When $(a, n) = 1$ and r is a primitive root, the x in $a \equiv r^x \pmod{n}$ is called the *index* or *discrete logarithm* of a to base r, denoted as $\text{ind}_r a$. Note that the modulus n is absent from the notation. We observe a few properties of discrete logarithms, note the typical continuous logarithm rules apply:

- $r^{\text{ind}_r a} \equiv a \pmod{n}$
- $\text{ind}_r 1 \equiv 0 \pmod{\phi(n)}$
- $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(n)}$
- $\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(n)}$, $k \in \mathbb{Z}^+$

Suppose n has a primitive root, if we have an integer a s.t. $(a, n) = 1$, then $x^k \equiv a \pmod{n}$ has a solution. Similarly, $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n}$ where $d = (k, \phi(n))$. Furthermore, if there are solution of $x^k \equiv a \pmod{n}$, then there are exactly d incongruent solutions mod n. A way to interpret such results is that if an integer a is a kth power residue iff $a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}$.

20 Distribution Of Primes

A function $\pi(n)$ counts the number of primes up to n. It is importantly used in the following theorem:

Prime Number Theorem

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

In other words, $\frac{x}{\ln x}$ and $\pi(x)$ are asymptotic. This is often written as $\pi(x) \sim \frac{x}{\ln x}$. When $a(x) \sim b(x)$, $\lim_{x\to\infty} \frac{a(x)}{b(x)} = 1$.
Let p_n be the nth prime, then $p_n \sim n \log n$.
For any $n > 0$, there are at least n consecutive composite positive integers.

21 Quadratic Residues

If $m \in \mathbb{Z}^+$, we said that an integer a is a *quadratic residue* of m if $(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution. If this congruence has no solutions, then a is a *quadratic nonresidue.*
Given a prime p and $a \nmid p$, the congruence $x^2 \equiv a \pmod{p}$ has either no solutions or exactly two incongruent solutions mod p. For the case where we have two incongruent solutions, x_0 is a solution, then $-x_0$ is a solution as well.
If p is an odd prime, then there are exactly $\frac{p-1}{2}$ quadratic residues of p and similarly $\frac{p-1}{2}$ quadratic nonresidues among $1, 2, \cdots, p-1$.
Let p be a prime and let r be a primiive root of p. If $a \nmid p$, then a is a quadratic residue if $\text{ind}_r a$ is even, and a quadratic nonresidue otherwise. When $ind_r a$ is even, we have an even exponent which can easily be written as a square, which is by definition a quadratic residue.
Let p be an odd prime and $a \nmid p$, The *Legendre Symbol* $\left(\frac{a}{p}\right)$ is equal to 1 when a is a quadratic residue of p, and -1 otherwise. Below are some properties of Legendre Symbols:

- $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
- $\left(\frac{a^2}{p}\right) = 1$ (duh)

Euler's Criterion

Let p be an odd prime and $a \nmid p$, then

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

We can verify one direction by supposing that a solution $x = x_0$ exists for $x^2 \equiv a \pmod{p}$. So $\left(\frac{a}{p}\right) = 1$ and $x_0^2 \equiv a$: $a^{\frac{p-1}{2}} = (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1}$. As $\phi(p) = p - 1$, by FLT $x_0^{p-1} \equiv 1 = \left(\frac{a}{p}\right)$.

Gauss's Lemma

Let p be an odd prime and a an integer with $(a, p) = 1$. If s is the number of least positive residues of the integers $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$, then $\left(\frac{a}{p}\right) = (-1)^s$.

When is -1 a Quadratic Residue

If p is an odd prime, then

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

The proof proceeds by seeing that $p \equiv 1 \pmod 4$ makes p of the form $4k+1$ and directly applying Euler's Criterion. The same goes for the $p \equiv -1 \pmod 4$ case.

When is 2 a Quadratic Residue

If p is an odd prime, then

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

So, 2 is a quadratic residue of all primes $p \equiv \pm 1 \pmod 8$ and a quadratic nonresidue of all primes $p \equiv \pm 3 \pmod 8$.

22 The Law of Quadratic Reciprocity

Let p, q be distinct odd primes, Then

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

Suppose p is an odd prime and a is an integer where $a \nmid p$. If q is a prime with $q \equiv \pm q \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

23 The Jacobi Symbol

Let n be an positive integer with prime factorization $n = \prod_{i=1}^{m} p_i^{a_i}$, and let a be an integer s.t. $(a, n) = 1$. The *Jacobi Symbol* is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{\prod_{i=1}^{m} p_i^{a_i}}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{a_i}$$

Each of $\left(\frac{a}{p_i}\right)$'s on the RHS are Legendre Symbols. Note that if a Jacobi symbol $\left(\frac{a}{n}\right)$ evaluates to 1, it does not imply anything about if a is a quadrati residue of n. Additionally, when $(a, n) \neq 1$, $\left(\frac{a}{n}\right) = 0$.

24 Sum of Squares

If m, n are both sums of two squares, then mn is also the sum of two squares.
If p is a prime of the form $p = 4k + 1$, then there exists x, y such that $x^2 + y^2 = lp$ for some integer $l < p$.
If p is a prime not of the form $4k + 3$, then there are integers x, y such that $x^2 + y^2 = p$
The integer $n > 0$ is the sum of two squares iff each prime factor of n of the form $4k + 3$ occurs to an even power in the prime factorization of n.

25 Infinimality of primes of the form $4k + 3$

Before the actual proof can take place, we note that primes can only either be of the form $4k + 1$ or $4k + 3$, which are the odd numbers in mod 4.

Also we note that if two numbers a, b are both of the form $4k + 1$, then ab will also be of the form $4k + 1$ (proof omitted for brevity).

To begin the actual proof, suppose we have a finite amount of primes of the form $4k + 3$, Namely, all in the sequence $\{p_i\}$ starting with $p_0 = 3$. We construct the following:

$$Q = 4 \prod_{i=1} p_i + 3$$

Note that $p_0 = 3$ is omitted from the expression.

Clearly, Q is a composite value of the form $4k+3$ by construction. It needs to have a factor that is of the form $4k+3$, as we have established that multiplication between numbers of the form $4k+1$ is closed. Therefore, for some i, $p_i \mid Q$. However, none of the p_i's can divide Q by construction. Therefore, Q is another prime of the form $4k + 3$, a contradiction to the assumption that there are only a finite amount of them.