MA3265 Notes

Lou Yi

Last Edited by: April 17, 2024

Contents

1 Congruence

Lemma 1.1 *Suppose $a, b, k, n \in Z$, and $ka \equiv kb \mod n$, then $a \equiv b \mod \frac{n}{\gcd(k,n)}$.*

Proof: Suppose $ka \equiv kb \mod n$, then $n|(ka - kb) \Rightarrow n|k(a-b)$, then $\frac{n}{\gcd(k,n)}|a - b$. □

Corollary 1.1.1 *Suppose $a, b, k, n \in Z$, and $\gcd(k, n) = 1$. Then $ka \equiv kb \mod n$ implies $a \equiv b \mod n$.*

Lemma 1.2 *If $a \equiv b \mod n$, then $\gcd(a, n) = \gcd b, n$.*

Proof: $n|a - b$, then $a = b + nq$, so $(a, n) = (b + nq, n) = (b, n)$. □

Definition: set of integers $\{0, 1, 2, ..., n-1\}$ is called the least residue system modulo n. Any set of n integers, no two of which are congruent modulo n, is called a complete residue system modulo n.
Definition: a subset R of the integers is called a reduced residue system modulo n if the following holds:

1. $\gcd(r, n) = 1$ for each r in R;
2. R contains $\varphi(n)$ elements, where $\varphi(n)$ is the number of nonnegative integer less than n that is also coprime to n;
3. no two elements of R are congruent modulo n.

Lemma 1.3 *Fix $n > 0$. Suppose $S = \{r_1, \cdots, r_n\}$ is a CRS modulo n. Pick $a, b \in \mathbb{Z}$, s.t., $\gcd(a, n) = 1$. Then*

$$S' = \{ar_1 + b, ar_2 + b, \cdots, ar_n + b\}$$

is also an CRS modulo n.

Proof: Suppose $ar_i + b \equiv ar_j + b \mod n$, then $r_i \equiv r_j \mod n$, so $i = j$. □

Definition: fix $n > 0$. Then an multiplicative inverse of a modulo n is a solution to the equation $ax \equiv 1 \mod n$.

Theorem 1.4 *a has an inverse iff $(a, n) = 1$.*

Proof: $ax = 1 \mod n$ has a solution iff $\exists b \in \mathbb{Z}$, s.t., $ax + bn = 1$. By Bezout's Lemma, this can only happen iff $\gcd(a, n) = 1$. □

Remark 1.4.1 *This gives an algorithmic way to compute the multiplicative inverse of an element (if it exists). Using Euclid's Algorithm, we can find x and b such that $ax + bn = 1$, then x ($x \mod n$) is an inverse of a.*

Theorem 1.5 (Wilsom's Theorem) *Let p be a prime, then $(p-1)! \equiv -1 \mod p$.*

Proof: If $p = 2$ or 3, then the result is trivial, so let $p > 2$. Consider the RRS modulo p: $R = \{1, 2, \cdots, p-1\}$. For any $b \in R$, there is an unique element $b \in r$, s.t., $ab = 1 \bmod p$. Note that if $a \neq 1, -1$, then the inverse of a is not itself. Hence $(p-1)! = 1 \cdot (p-1) = -1 \bmod p$. □

Theorem 1.6 (Fermat's Little Theorem) *Let p be a prime, $a \in \mathbb{Z}$. If $(a, p) = 1$, then $a^{p-1} = 1 \bmod p$. In general, if a is arbitrary, then $a^p = a \bmod p$ for all a.*

Proof: Consider $R = \{1, 2, \cdots, p-1\}$ which is an RRS module p. Since $(a, p) = 1$, note $aR = \{a, 2a, \cdots, (p-1)a\}$ is also an RRS, so it contains the same elements as R. Then $\cdot 2 \cdots (p-1) = a \cdot (2a) \cdots (p-1)a \bmod p$, hence $a^{p-1} = 1 \bmod p$ by Wilson's Theorem. □

Some Primality Test:

Lemma 1.7 (Converse of Wilson's Theorem) *If $n \geq 2$, and $(n-1)! \equiv -1 \bmod n$, then n is a prime.*

Proof: We claim that if n is a composite number, then it has a factor $\leq \sqrt{n}$. Since $n = ab$ for some ab, and if $a, b > \sqrt{n}$, then $ab > n$ contradiction.
Next suppose $(n-1)! \equiv -1 \bmod n$. For any $1 \leq a \leq n-1$, there is a b, s.t., $a \cdot b \equiv -1 \bmod b$, so every number between $1 \leq a \leq n-1$ has a multiplicative inverse mod n. But recall the criterion for having an multiplicative inverse, this implies that all numbers between 1 to $n-1$ are coprime to n, which implies n is a prime. □

Suppose we want to check whether n is a prime: if we can find $1 \leq a \leq n-1$ for which $a^{n-1} \neq 1 \bmod n$, then n is not a prime by Fermat's Theorem. However, there are composite numbers n, s.t., $a^{n-1} = 1 \bmod n$ for all $1 \leq a \leq n-1$ with $(a, n) = 1$. If $a^{n-1} = 1 \bmod n$ for all $1 \leq a \leq n-1$, we say n passes the test. Such numbers are called Carmichel's Numbers.

Theorem 1.8 *Let p be a prime, then $n^2 = -1 \bmod p$ if and only if $p = 2$ or $p = 1 \bmod 4$.*

Proof: $\Rightarrow$: Assume p is not 2, then we show that p must be 1 mod 4. Suppose $\exists n$, s.t., $x^2 = (-1) \bmod p$. Then by Fermat's theorem, we have

$$(-1)^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = 1 \bmod p.$$

But this can only happen iff $\frac{p-1}{2}$ is even, i.e., $p = 1 \bmod 4$.
$\Leftarrow$: If $p = 2$, then $n = 1$ solves the system. Now suppose $p = 1 \bmod 4$, by Wilson's, we know under modulo p,

$$-1 = (p-1)! = \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \cdots (p-2)(p-1).$$

Note we can group the terms, so

$$(p-1)! = \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)\left[\left(-\frac{p-1}{2}\right) \cdots (-2)(-1)\right] = (-1)^{\frac{p-1}{2}}\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 = \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2.$$

Hence $n = \left(\frac{p-1}{2}\right)!$, is a solution to $n^2 = -1 \bmod p$. □

Fun application: we can use this theorem to prove a special case of Dirichilet's theorem. Let $\mathfrak{P}_{1,4} = \{1 + 4m : m \in \mathbb{Z}\}$, then $\mathfrak{P}_{1,4}$ contains infinitely many primes. Suppose $\{p_1, \cdots, p_r\}$ are all the primes in $\mathfrak{P}_{1,4}$, then $N = 4(p_1 \cdots p_r)^2 + 1$ is composite and does not have $2, p_1, \cdots, p_r$ as its prime factors. N must have some other prime p as its factors, i.e., $p|N$, then

$$4(p_1 \cdots p_r)^2 + 1 = 0 \Rightarrow (2p_1 \cdots p_r)^2 = 0 \mod p.$$

Then it must follows $p = 2$ or $p = 1 \mod 4$. But p is not 2, hence $p = 1 \mod 4$, so p must be in $\mathfrak{P}_{1,4}$ which is a contradiction.

Definition: we define the Euler-Totient function $\varphi(n)$ by $\varphi(1) := 1$, and for $n > 1$, $\varphi(n) :=$ the number of elements in the RRS modulo n, which is also the number of positive integers less than n and is coprime to n.

Theorem 1.9 (Euler's Theorem) *Let $n > 1$ be an integer, $a \in \mathbb{Z}$, then $a^{\varphi(n)} = 1 \mod n$ if $(a, n) = 1$*

Proof: Given $n > 1$, consider the RRS R of n, which has $\varphi(n)$ elements. Then aR is still the same set, since $a \in R$ and R is a group under multiplication. So the product of elements R is equal to the product of aR, hence $a^{\varphi(n)} = 1$. □

Remark 1.9.1 *The $|RRS| = |CRS| - 1$ if and only if n is a prime.*

Properties of the Euler Phi function:

- $\varphi(0) = 1$. This is by convention.
- $\varphi(1) = 1$. This is by convention/definition.
- $\varphi(p) = p - 1$. p is only divisible by p if it is a prime.
- $\varphi(p^k) = p^k - p^{k-1}$. Proof: there are p^k positive integers not greater than p^k, and $gcd(m, p^k) \neq 1$ if and only if $p|m$, hence there are $p^k/p = p^{k-1}$ such m.
- If $\gcd(m, n) = 1$, then $\varphi(m)\varphi(n) = \varphi(mn)$.
  Proof: Let M and N be the set of numbers $\leq m$ or n and coprime to m or n respectively, and U be the set of numbers coprime to mn and not greater than mn. We show $|M||N| = |K|$, if $\gcd(m, n) = 1$. If $(b, m) = (b, n)$, then $(a, mn) = 1$. So if $a' \in M$, $a'' \in N$, then $a = a'a'' \in K$. On the other hand, if $a \in N$, $(a, mn) = 1$, and then $(a \bmod m, m)$=1, and $(a \bmod n, n)$=1, so for every a in K, it corresponds to a distinct element in $M \times N$, i.e., $(a \bmod m, a \bmod n)$.
- If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then $\varphi(n) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1})$. This follows directly from the previous property.
- $\varphi(n) = \prod_{p|n} (1 - \frac{1}{p})$.
- $\varphi(n)\varphi(m)\frac{\gcd(m,n)}{\varphi(\gcd(m,n))} = \varphi(mn)$.
- $\varphi(2m) = 2\varphi(m)$ if m is even; $\varphi(2m) = \varphi(m)$ if m is odd.
- $\varphi(n^m) = n^{m-1}\varphi(n)$.

- If $a|b$, then $\varphi(a)|\varphi(b)$.
- $m|\varphi(a^m - 1)$.
- $\varphi(\text{lcm}(m,n)) \cdot \varphi(\gcd(m,n)) = \varphi(m) \cdot \varphi(n)$.

2 Solving Equations in Congruence Systems

2.1 Solving Linear Equations

Definition: an equation of the form $a_1x_1 + \cdots + a_kx_k = b \bmod n$ has an unique solution mod n if the following happens:

- $(x_1', \cdots, x_k')$ is a solution.
- If $(x_1'', \cdots, x_k'')$ is another solution, then $x_i' = x_i'' \bmod n$, for $i = 1, \cdots, k$.

Theorem 2.1 *Fix $n > 0$; let $d = \gcd(a, n)$, then $ax = b$ mod n has a solution if and only if $d|b$. In this case, this solution is unique mod $\frac{n}{d}$.*

Proof: $ax + ny = b$ has a solution iff $\gcd a, n | b$. The rest follows. □

Remark 2.1.1 *Module n, there are d solutions. Namely, if x_0 is a solution mod $\frac{n}{d}$, then all the solution mod n are*

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \cdots, x_0 + (d-1)\frac{n}{d}.$$

Next we have move onto a system of linear equations. Note given any linear system $ax = b \bmod n$, we can convert it into a more standard form, namely $x = c \bmod n'$ by the previous theorem.

Theorem 2.2 (Chinese Remainder Theorem) *Fix $n_1, \cdots, n_k > 0$ which are pairwise coprime. Then the system of linear congruence equation,*

$$\begin{cases} x = a_1 \ mod \ n_1, \\ x = a_2 \ mod \ n_2, \\ \quad \vdots \\ x = a_k \ mod \ n_k \end{cases}$$

Has a unique solution mod $n_1 n_2 \cdots n_k$.

Proof: For $i = 1, \cdots, k$, consider $A_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$, then $\gcd n_i, A_i = 1$, because the $n_j's$ are pairwise coprime. Then exists an inverse of $A_i \bmod n_i$, denote it y_i, and let $z_i = a_i y_i A_i$. Then $x = \sum_{i=1}^{k} z_i$ is a solution to the system. As $x \bmod n_i = a_i y_i A_i \bmod n_i = a_i$.
Next, suppose x' is another solution to the system. Then $x' - x = 0 \bmod n_i$, $i = 1, 2, \cdots, k$. So $n_i | x' - x$, since the numbers $n_j's$ are pairwise coprime, then $n_1 \cdots n_k | x' - x$, i.e. the solution is unique mod $n_1 \cdots n_k$. □

Remark 2.2.1 *The CRT shows that $\mathbb{Z}/n_1 \cdots n_k\mathbb{Z} \cong \mathbb{Z}/n_1/\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$ if $n_1, \cdots, n_k$ are pairwise coprime.*

Remark 2.2.2 *Suppose $n_1, \cdots, n_k$ is not pairwise coprime, we can break the equation involving $n_i's$ that are not pairwise coprime down. And if the system is consistent we will have a solution, otherwise we will not have a solution.*
I.e., if $x = a \mod pq$, then $x = a \mod p$, $x = a \mod q$.
Example: Solve $x = 34 \mod 36$ and $x = 7 \mod 15$ and $x = 2 \mod 40$. Then equivalent to solve $x=2 \mod 4$, $x= 7 \mod 9$, $x = 2 \mod 5$, $x=1 \mod 3$, $x= 2 \mod 5$, $x=2 \mod 8$. But then $x = 2 \mod 8$ implies $x = 2 \mod 4$ and similarly for the others. So we just need to solve $x=2 \mod 4$, $x=2 \mod 5$, $x=1 \mod 3$.

2.2 Monomial Equation / Discrete Logs

Definition: fix $n > 0$; if $a^{\varphi(n)} = 1 \mod n$ and φ is the smallest such exponent, then a is a primitive root mod n.

Theorem 2.3 *There is a primitive root modulo n if and only if n is of the form $1, 2, 4, p^k$, $2p^k$ for odd prime p.*

Lemma 2.4 *If a is a primitive root modulo n, then the reduced residue system of n is $\{a_i : 1 \leq i \leq \varphi(n)\}$.*

Proof: Follows from the definition of the primitive roots. □

Corollary 2.4.1 *If U_n has one primitive root, then it has $\phi(\phi(n))$ many primitive roots.*

How to use primitive root:
Suppose we want to solve a congruence equation of the form $x^d = c \mod n$, where n is a prime. We can first find a primitive root of n. Suppose a is such a primitive root, then $c = a^p$ for some $p \in \mathbb{Z}$. And not x must also be in the RRS of n, so $x = a^q$ for some $q \in \mathbb{Z}$. Hence we can turn this congruence equation into a linear one, i.e., $dq = p \mod \varphi(n)$.

Lemma 2.5 *Suppose a is a primitive root mod n. Then $a^k = a^j \mod n$ if and only if $k = j \mod \varphi(n)$.*

Proof: Group theory. □

Corollary 2.5.1 *In general, for general a (not necessarily primitive root, but still invertible). $a^k = a^j \mod n$, if and only if $k = j \mod ord(a)$, where $ord(a)$ is the smallest positive number such that $a^{ord(a)} = 1$.*

Next, for the general case, if we want to solve $x^m = c \mod n$, where n is not a prime. We do the following:

- Break this equation into several equations mod the prime powers that are factors of n.
- Solve the ones corresponding to odd primes using primitive roots (they exists).
- For modulo 2^k: use Theorem 2.6.
- "Glue" the result for each equation together by Chinese Remainder Theorem.

Theorem 2.6 *If $k \geq 3$, then*

$$RRS(2^k) = \{\pm 3^i \ : \ 0 \leq j < 2^{k-2}\} = \{\pm 5^j \ : \ 0 \leq j < 2^{k-2}\}.$$

I.e., this is generated by $\{-1, 3\}$, or $\{-1, 5\}$.

El Gammal Scheme (An encryption scheme):
Alice chooses

1. a "large" prime.
2. a primitive element of a RRS
3. an integer $1 \leq d \leq p-1$.

And computes

1. a^d modulo p, call the residue b.

The public key (p, a, b) is sent to every one, and the private key (d) is kept private.
Bob encrypts a message $M < p$ and sends to Alice as follows:

1. chooses random integer k
2. computes $a^k \mod p = \text{r}$, $b^k M \mod p = \text{t}$.

Bob sends to Alice these two numbers (r, t).
To decrypt it, Alice computes $tr^{-d} \mod p$. Note $a^d = b$, then

$$tr^{-d} = b^k M (a^k)^{-d} = (a^d)^k M (a^k)^{-d} = M.$$

2.3 Quadratic Reciprocity

Given $a \in \mathbb{Z}$, find n such that $x^2 = a \mod n$ has a solution?

Algebraic structure of U_n (=RRS(n)). We know that for which n, the primitive roots exists, i.e., U_n is cyclic. To understand the relationship between $\mathbb{Z}_l$ =CRS(l) and $\mathbb{Z}_n$, where $l|n$. Consider the map $\varphi_{n,z} : \mathbb{Z}_n \to \mathbb{Z}_l$, $[a]_n \mapsto [a]_l$. Note $\varphi_{n,z}$ is a group homomorphism. In fact, $[a]_l = [a]_n \cup [a+l]_n \cup \cdots \cup [a+(m-1)l]$, where $m = \frac{n}{l}$. Since $\varphi_{n,z} : \mathbb{Z}_n \to Z_l$ is also a ring homomorphism, it sends units in $\mathbb{Z}_n$ to the units in $\mathbb{Z}$. Then $\varphi_{n,z} : U_n \to U_l$ is also a group homomorphism. We can even have group homomorphism sending to the direct group. When $n = lm$, $\varphi = (\varphi_{n,1}, \varphi_{n,m}) : \mathbb{Z}_n \to \mathbb{Z}_l \oplus \mathbb{Z}_m$, $[a]_n \mapsto ([a]_l, [a]_m)$. The Chinese remainder theorem tells us that the map is surjective if $\gcd(l, m) = 1$, hence bijective (as the domain and codomain have the same cardinality), so φ is a ring isomorphism. Then as before, we have $U_n \cong U_l \oplus U_m$ under the group isomorphism φ. Comparing cardinality, we have $\varphi(n) = \varphi(l)\varphi(m)$, whenever $\gcd(l, m) = 1$ and $n = lm$.

Theorem 2.7 *If $n = p_1^{e_1} \cdots p_k^{e_k}$, then*

$$Z_n \cong \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$$

as rings, and

$$U_n \cong U_{p_1^{e_1}} \oplus \cdots \oplus U_{p_k^{e_k}}.$$

Definition: suppose G is a group that acts on a set X, then $X^G := \{x \in X : gx = x, \text{ for all g} \in G\}$.

Theorem 2.8 *If $|G| = p^n$, and G acts on X, then $|X| = |X^G|$ mod p.*

Proof: Since $X = O(x_1) \cup O(x_2) \cdots \cup O(x_n)$, the union of disjoint orbits. X^G is the union of singleton orbits. Note that for any orbit that is not a singleton, it is divisible by p, as it is equal to $|G : \text{stab}(x_i)|$, and the stabilizer of x_i is a proper subgroup of G so $|G : \text{stab}(x_i)|$ is divisible by p. Then the order of the singleton orbits $= |X^G| = |X|$ mod p. □

Question: which primes $p = x^2 + y^2$?
Question: when does $-1 = z^2$ mod p have a solution? (We already know the answer).
Note suppose $p = x^2 + y^2$, then $p \nmid x, y$, otherwise if $p|x, y$, then $p^2|x^2, y^2$, so $p^2|x^2 + y^2$. Mod p, $0 = x^2 + y^2$, so $(y^{-1})^2 = x^2 \cdot (y^{-1})^2 + 1 \Rightarrow z^2 = -1$ mod p. Then p must be 1 mod 4.
Suppose X is a set, $\sigma_1, \sigma_2 : X \to X$ are automorphisms, and $\sigma_1^2 = \sigma^2 = 1$, then

$$|\{x \in X : \sigma_1(x) = x\}| = |\{x \in X : \sigma_2(x) = x\}| \mod 2.$$

Remark: $G_1 = \{\sigma_1, 1\}$, $G_2 = \{\sigma_2, 1\}$ are groups acting on X. Then $|X^{G_1}| = |X| = |X^{G_2}|$.
Definition: an involution is a map $\sigma : X \to X$ such that $\sigma \circ \sigma = id$.
Now back to our first problem:
Let $X = \{(x, y, z) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} : x^2 + 4yz = p\}$ (Note X is finite). Define involution $\sigma_1(x, y, z) = (x, z, y)$. Note $\sigma_1(x, y, z) = (x, y, z)$ if and only if $y = z$. I.e., $(x, y, y) \in X$ such that $x^2 + 4yy = p$, so $p = x^2 + (2y)^2$. So if the fix point of $\sigma_1 \neq \emptyset$, then the problem has a solution.
Next, we define another involution $\sigma_2 : X \to X$, by

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z), & \text{if } x < y - z \\ (2y - x, y, x + z - y), & \text{if } y - z < x < 2y \\ (x - 2y, x + z - y, y), & \text{if } x > 2y \end{cases}.$$

One can check that σ_2 is well defined, and $\sigma_2^2 = 1$. Note the fixed points of σ_2 cannot come from case 1 and case 3, but only case 2. In this case $(x, y, z) = (2y - x, y, x + z - y)$, so $x = y$, which implies $x^2 + 4xz = p \Rightarrow x|p$, so $x = 1$. So $1 + 4z = p$, then $z = \frac{p-1}{4}$. Since $p = 1 \mod 4$. So the fixed points of $\sigma_2 \neq$, in particular it has one fixed point $(1, 1, \frac{p-1}{4})$. Then σ_1 has an odd number of fixed points, so it must have at least one fixed point.
Remark: if $p = x^2 + ny^2$, then mod p, we have $0 = x^2 + ny^2 \Rightarrow 0 = z^2 + n$, where $z = xy^{-1}$. So $-n$ is a square mod p. (Converse is not true; but do have an extra hypothesis to go in reverse direction).

Next we want to solve any quadratic polynomial mod n. By Chinese Remainder Theorem, we can solve mod p^e's and combine the solutions together.

Lemma 2.9 (Hensel's Lemma) *If polynomial $f(x)$ has integer coefficients; $f(a) = 0 \mod p^e$ and $f'(a) \neq 0 \mod p$. Then there is a unique k (modulo p), s.t., $f(a + kp^e) = 0 \mod p^{e+1}$.*

By previous steps, suffices to solve any quadratic polynomial modulo p : $f(x) = ax^2 + bx + c = 0 \mod p$. We complete the square and get

$$4af(x) = (2ax + b)^2 + (4ac - b^2) = 0 \mod p.$$

Since $a \neq 0 \mod p$ (otherwise it will not be a quadratic polynomial). Further, if $p \neq 2$ (if $p = 2$, then the equation is trivial), then $4a$ is a unit. Let $y = 2ax + b$, and $D = b^2 - 4ac$, so we just need to solve $y^2 = D \mod p$.

Definition: if a is a unit modulo n ($n \in \mathbb{Z}^*$), then a is called quadratic residue (QR) if $x^2 = a \mod n$ has solution, otherwise it is called a quadratic nonresidue (QNR).

Theorem 2.10 *Let $p > 2$ be a prime, then:*

1. *Let $e > 1$; a is a QR mod p iff a is QR mod p^e.*
2. *QR mod $p = \{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\}$ mod p. I.e., exactly half are QR.*
3. *If u is a primitive root, then QR mod $p = \{u^{2k} : k \in \mathbb{Z}\}$ mod p. The QNR mod $p = \{u^{2k+1} : k \in \mathbb{Z}\}$.*

Proof:

1. If $x^2 = a \mod p^e$ has a solution, then $x^2 = a \mod p$ has a solution, as $p | p^e$. For the converse, say $b^2 = a \mod p^d$, then $b^2 = a + rp^d$; define $k := -r \cdot (2b)^{-1}$, i.e., $(2b)k = -r$. Check $b' = b + kp^d$ satisfies $(b')^2 = a \mod p^{d+1}$.

$$(b')^2 = (b + kp^d)^2 = a + rp^d + 2bkp^d + k^2p^{2d} = a + rp^d - rp^d + k^2p^{2d} = a \mod p^{d+1}.$$

2. the units mod p are $\{1, 2, \cdots, p-1\}$, then the quadratic residues mod p are $\{1^2, 2^2, \cdots, (p-1)^2\}$ but one can verify this set is just $\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\}$ modulo p.

3. This is clear, as every unit is of the form u^k, $k \in \mathbb{Z}$. We also show that u^{2k+1} cannot equal to $u^{2k'}$, as otherwise, we would have $2k + 1 = 2k' \mod \phi(p)$, which is not possible as $\phi(p)$ is even.

□

Definition: suppose p is an odd prime; $a \in \mathbb{Z}_p$, we define the Legendre Symbol:

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & a = 0 \mod p \\ 1, & a = \square \\ -1, & a \neq \square \end{cases}.$$

Then $\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p \to \{0, \pm 1\}$ is a function.
Remark: instead, if we define $\left(\frac{\cdot}{p}\right) : U_p \to \{\pm 1\}$, we would get a group homomorphism.

Note: $\#\{x \in \mathbb{Z}_p : x^2 = a \mod p\} = 1 + \left(\frac{a}{p}\right)$. This only works if p is a prime.

Theorem 2.11 *If p is odd, then $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$.*

Proof: It is clear that if $a = 0 \mod p$, then the statement holds trivially. By Fermat's theorem, if $a \neq 0 \mod p$, then $(a^{\frac{p-1}{2}})^2 = a^{p-1} = 1 \mod p$, then $a^{\frac{p-1}{2}} = \pm 1$. If $a = \square$, then $a = u^{2k}$, where u is a primitive root. Then $a^{\frac{p-1}{2}} = u^{k(p-1)} = (u^{p-1})^k = 1^k = 1$ as desired. If $a \neq \square$, then $a = u^{2k+1}$, then

$$a^{\frac{p-1}{2}} = (u^{2k} \cdot u)^{\frac{p-1}{2}} = (u^{2k})^{\frac{p-1}{2}} \cdot u^{\frac{p-1}{2}} = 1 \cdot u^{\frac{p-1}{2}}.$$

Now u is primitive, then $P - 1$ is the smallest exponential k for which $u^k = 1$, so $u^{\frac{p-1}{2}} \neq 1 \Rightarrow u^{\frac{p-1}{2}} = -1$. $\square$

Corollary 2.11.1 *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, i.e., $\left(\frac{\cdot}{p}\right) : U_p \to \{\pm 1\}$ is a homomorphism.*

Proof: Since

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

$\square$

Remark: this gives a way to compute $\left(\frac{n}{p}\right)$, one can factorize $n = p_1^{e_1} \cdots p_k^{e_k}$ and apply the corollary. But then we want to develop a theorem of computing $\left(\frac{q}{p}\right)$.

Notation: let Q_n denote the set of quadratic residues mod n.
Recall: that if G is a group acting on a set X and $|G| = p^n$ for some n. Then $|X| = |X^G| \mod p$ where $|X^G|$ is all the fixed point of X under G.
Notation: Let $S_n^p(a)$ denote the set

$$S_n^p(a) := \{(x_1, \cdots, x_n) \in \mathbb{Z}_p^n : x_1^2 + \cdots + x_n^2 = a\}.$$

Remark: $S_1^p(a) = \{x \in \mathbb{Z}_p : x^2 = a\}$, then $|S_1^p(a)| = 1 + \left(\frac{a}{p}\right)$.

Theorem 2.12 (Gauss)

1. *(Reciprocity Law) If p, q are distinct odd primes, then*

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

Equivalently,

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

I.e., $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ are equal whenever p, q are not both 3 mod 4.

2. *$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, i.e., $2 = \square$ iff $p = 1, 7$ mod 8.*

3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$*, i.e.,* -1 *is a square iff* $p = 1 \mod 4$.

Proof: Fix two odd primes p, q, then

$$S_q^p(1) = \{(x_1, \cdots, x_q) \in \mathbb{Z}_p^q \,:\, x_1^2 + \cdots + x_q^2 = 1\}$$

Note $\mathbb{Z}_p$ acts on $s_q^p(1)$ by cyclic shift, to give $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(s_q^p(1))$ we just need to define $\varphi(1)$, which is defined by

$$\varphi(1) \cdot (x_1, \cdots, x_q) := (x_q, x_1, x_2, \cdots, x_{q-1}).$$

By Theorem 2.8, we have $|S_q^p(1)| = |\text{Fixed points}| \mod q$. But if $(x_1, \cdots, x_q)$ is fixed by the action, then $x_1 = \cdots = x_q$. So $x_1^2 + \cdots + x_q^2 = 1 \Rightarrow qx^2 = 1$, i.e., $q = \square$, $(x, \cdots, x)$ is fixed if $q = x^{-2} \mod p$. So the number of fixed points is $1 + \left(\frac{p}{q}\right)$. So $|S_q^p(1)| = 1 + \left(\frac{q}{p}\right) \mod q$.

Now we try to count $|S_q^p(1)|$ via recursion and we would get $\left(\frac{p}{q}\right)$ somewhere. Express $|S_n^p(a)|$ in terms of $|S_{n-2}^p(a)|$, then $|S_{n-4}^p(a)|$ and so on. To make this recursive formula effective, need to know $|S_1^p(a)|$ and $|S_2^p(a)|$.
We know $|S_1^p(a)| = 1 + \left(\frac{a}{p}\right)$. We claim

$$|S_2^p(a)| = |\{(x_1, x_2) \in \mathbb{Z}_p^2 \,:\, x_1^2 + x_2^2 = a\}| = \begin{cases} p - (-1)^{\frac{p-1}{2}}, & \text{if } a \neq 0, \\ p + (-1)^{\frac{p-1}{2}}(p-1) & \text{if } a = 0 \end{cases}.$$

For the case $a = 0$,

$$|S_2^p(0)| = \begin{cases} 2p - 1, & \text{if } p = 1 \mod 4 \\ 1, & \text{if } p = 3 \mod 4 \end{cases}$$

The case where $p = 3 \mod 4$ is clear. If $p = 1 \mod 4$. $x = y = 0$ contributes to one solution, if $x, y \neq 0$, then $(y^{-1}x)^2 + 1 = 0 \mod p \Rightarrow y^{-2}x^2 = -1 \mod p$, but $-1 = k^2 \mod p$ for two values of k. Hence there would be $x = yk$ can take $2(p-1)$ values. Then in total there are $2p - 1$ solutions.
We show that $|S_2^p(a)| = |S_2^p(1)|$ whenever $a \neq 0$. Note $|S_2^p(a)| =$ the number of solutions $x^2 + y^2 = a$. This is equal to

$$\begin{aligned} &= \sum_{\alpha \in \mathbb{Z}_p, \beta \in \mathbb{Z}_p, \alpha + \beta = p} |S_1^p(\alpha)||S_1^p(\beta)| \\ &= \sum_{\alpha+\beta=a} \left(1 + \left(\frac{\alpha}{p}\right)\right)\left(1 + \left(\frac{\beta}{p}\right)\right) \\ &= p + \sum_{\alpha \in \mathbb{Z}_p} \left(\frac{\alpha}{p}\right) + \sum_{\beta \in \mathbb{Z}_p} \left(\frac{\beta}{p}\right) + \sum_{\alpha+\beta=\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right) \\ &= p + 0 + 0 + \sum_{\alpha+\beta=\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right) \end{aligned}$$

Whenever $a \neq 0$, we show

$$\sum_{\alpha+\beta=\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right) = \sum_{\alpha+\beta=1} \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right).$$

Since $a \neq 0$, then a^{-1} exists in $\mathbb{Z}_p$, let $\alpha' = a^{-1}\alpha$, and $\beta' = a^{-1}\beta$, then $\alpha' + \beta' = 1$. Furthermore,

$$\left(\frac{\alpha'}{p}\right)\left(\frac{\beta'}{p}\right) = \left(\frac{a^{-1}\alpha}{p}\right)\left(\frac{a^{-1}\beta}{p}\right) = \left(\frac{a^{-1}}{p}\right)^2\left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right) = \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right).$$

Now we formulate a recursive formula:

$$x_1^2 + \cdots + x_n^2 = a \Leftrightarrow x_1^2 + \cdots + x_{n-2}^2 = a - x_{n-1}^2 - x_n^2 = a'.$$

Here

$$a' = a - x_{n-1}^2 - x_n^2 = \begin{cases} a, & \text{for } p + (p-1)(-1)^{\frac{p-1}{2}} \text{ values} \\ \text{other arbutrart values}, & \text{for } p - (-1)^{\frac{p-1}{2}} \text{ values} \end{cases}.$$

Since

$$|S_n(a)| = \sum_{x_n=0}^{p-1}\sum_{x_{n-1}=0}^{p-1} |S_{n-2}(a')|.$$

Then

$$|S_n(a)| = \left[p + (p-1)(-1)^{\frac{p-1}{2}}\right]|S_{n-2}(a)| + \left[p - (-1)^{\frac{p-1}{2}}\right]\sum_{b=0,\, b\neq a}^{p-1} |S_{n-2}(b)|$$

Note $\sum_{b=0}^{p-1} |S_{n-2}(b)| = p^{n-2}$,

$$\begin{aligned} |S_n(a)| &= \left[p + (p-1)(-1)^{\frac{p-1}{2}}\right]|S_{n-2}(a)| + \left[p - (-1)^{\frac{p-1}{2}}\right]\left[p^{n-2} - |S_{n-2}(a)|\right] \\ &= \left(p - (-1)^{\frac{p-1}{2}}\right)\cdot p^{n-2} + p\cdot(-1)^{\frac{p-1}{2}}|S_{n-2}(a)| \end{aligned}$$

Repeat this process we get

$$\begin{aligned} S_n(a) &= p^{n-1} - (-1)^{\frac{p-1}{2}\cdot 2}p^{n-3} + p^2|S_{n-4}(a)|(-1)^{\frac{p-1}{2}\cdot 2} \\ S_n(a) &= p^{n-1} - (-1)^{\frac{p-1}{2}\cdot k}p^{n-1-k} + p^k|S_{n-2k}(a)|(-1)^{\frac{p-1}{2}\cdot k} \qquad (*) \end{aligned}$$

Specialize to $n = q = 2k+1$, $a = 1$, where $S_1(1) = 1$:

$$(*) \Longrightarrow S_q(1) = p^{2k} + p^k(-1)^{\frac{p-1}{2}\cdot k}.$$

Apply modulo q, by Fermat, we have $p^{2k} = p^{q-1} = 1$ and by Euler's criterion, $p^k = p^{q-1} = \left(\frac{p}{q}\right)$. So $S_q^p(1) = 1 + (-1)^{\frac{p-1}{2}\cdot k}\cdot\left(\frac{p}{q}\right) \mod q$. But since $S_q^p(1) = 1 + \left(\frac{q}{p}\right) \mod q$, so

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

Since $q \neq 2$, then

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

Lastly, we show that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Consider $S_2(a)$. Like before:

$$S_2(1) = p - (-1)^{\frac{p-1}{2}} = \begin{cases} 0, & p = 1 \mod 8 \\ 4, & p = 3 \mod 8 \\ 4, & p = 5 \mod 8 \\ 0, & p = 7 \mod 8 \end{cases}$$

Now if $x^2 + y^2 = 1$, so is $(\pm x, \pm y)$ and $(\pm y, \pm x)$, i.e., if the solutions are in packets of 8 unless it is of the form (x, x), $(x, 0)$, $(0, y)$ or $(x, -x)$:

- $(x, 0) \implies x^2 = 1$, so 2 solutions;
- $(0, y) \implies y^2 = 1$, so 2 solutions;
- $(x, x) \implies 2$ is QR mod p, so $1 + \left(\frac{2}{p}\right)$
- $(x, -x) \implies 1 + \left(\frac{2}{p}\right)$ solutions.
- So $6 + 2\left(\frac{2}{p}\right)$ solutions in total.

Consider modulo 8, we have

$$6 + 2\left(\frac{2}{p}\right) = \begin{cases} 0, & p = 1 \mod 8 \\ 4, & p = 3 \mod 8 \\ 4, & p = 5 \mod 8 \\ 0, & p = 7 \mod 8 \end{cases}$$

Then we can see the supplementary law holds. □

2.4 Jacobi Symbol

Definition: if b is an odd positive integer with prime factorization $b = p_1 \cdots p_k$ (repetition allowed) and a is any integer, the Jacobi symbol $\left(\frac{a}{b}\right)_J$ is defined by setting

$$\left(\frac{a}{b}\right)_J := \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right).$$

Where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Proposition 2.13 *The following are easy to verify:*

1. *If* $x =$ mod b, *then* $(\frac{x}{b})_J = (\frac{y}{b})_J$.

2. $(\frac{a}{b})_J$ *is always* 0 *or* ± 1*, and it will only be* 0 *if and only if* $\gcd(a,b) > 1$.

3. *The Jacobi symbol is multiplicative on top and bottom:* $(\frac{x}{b})_J(\frac{y}{b})_J = (\frac{xy}{b})_J$ *and* $(\frac{x}{a})_J(\frac{x}{b})_J = (\frac{x}{ab})_J$.

4. *If* a *is a quadratic residue modulo* b *and is relative prime to* b*, then* $(\frac{a}{b}) = 1$.

Lemma 2.14 *Let* $b = p_1 \cdots p_k$ *be a product of odd prime, then*

- $\sum_{i=1}^k \frac{p_i - 1}{2} = \left[\left(\prod_{i=1}^k p_i\right) - 1\right]/2 \mod 2$.
- $\sum_{i=1}^k \frac{p_i^2 - 1}{8} = \left[\left(\prod_{i=1}^k p_i^2\right) - 1\right]/8 \mod 2$.

Proposition 2.15 *Suppose* b *is an odd integer, then*

1. $(\frac{-1}{b})_J = (-1)^{\frac{b-1}{2}}$.

2. $(\frac{2}{b})_J = (-1)^{\frac{b^2-1}{8}}$.

3. *If* a *is another odd positive integer with* $\gcd(a,b) = 1$*, then*

$$\left(\frac{a}{b}\right)_J \left(\frac{b}{a}\right)_J = (-1)^{\frac{(a-1)(b-1)}{4}}.$$

2.5 Two Interesting Problems

Mcnugget Problem: given two relatively prime positive integer, m, n. What is the biggest number than cannot be represented as non-negative linear combination of m, n?
Ans: $mn - m - n$.
Proof: Given $N \in \mathbb{N}^+$, find $a, b \geq 0$, s.t., $am + bn = N$. Define $X_N = \{(a,b) \in \mathbb{Z}^2_{\geq 0} : am + bn = N\}$. Note X_N is a strict subset of $Y_N = \{(a,b) \in \mathbb{Z}^2 : am + bn = N\}$.

Theorem 2.16 *Fix a solution* (x_0, y_0)*, i.e.,* $(x_0, y_0) \in Y_n$*, then* $Y_N = \{(x_0 + kn, y_0 - km) : k \in \mathbb{Z}\}$.

Proof: Clear. □

Observation 1: $\exists! x \in \mathbb{Z}$ and $y \in \{0, 1, \cdots, m-1\}$, s.t., $xm + yn = N$.
Observation 2: N is representable nonnegatively iff $x \geq 0$. Proof: $x > 0$, then $N = xm + yn$ is a viable representation. Conversely, if $x < 0$, then the solution set is of the form $(x_0 + kn, y_0 - km)$, so at least one component is negative.
Observation 3: Non representable set is the following:

$$\{mx + ny : x < 0, y \in \{0, 1, \cdots, m-1\}\}.$$

Then the maximum of the set happens when $x = -1$ and $y = m - 1$, i.e.,$-m + n(m-1) = mn - m - n$.

Problem 2: Given any positive integer N, describe whether its area of a Right-Angled Triangle having rational side length, i.e., $N = \frac{1}{2}ab$ and $a^2 + b^2 = c^2$, for some $a, b, c \in \mathbb{Q}$.
We can characterize a, b, c, i.e., Pythagorean triplets. Suppose $a, b, c \in \mathbb{Z}$, $a^2 + b^2 = c^2$, then scaling leaves the equation invariable. I.e., $(ka)^2 + (kb)^2 = (kc)^2$, $\forall k \in \mathbb{Z} \setminus \{0\}$ if and only if $a^2 + b^2 = c^2$. Call (a, bc) primitive, if a, b, c has no common divisor.

Theorem 2.17 *(a, b, c) is a primitive triple if and only if $(a, b, c) = (s^2 - t^2, 2st, s^2 + t^2)$ for some relatively prime integers, with $s > t$ and $s \neq t \mod 2$.*

Proof: Easy to see that a, b both cannot be even or odd ($\mod 4$). WLOG, let a be odd, b even, then c is odd.
Method 1: $a^2 + b^2 = c^2$ if and only if $b^2 = (c-a)(c+a)$, since b is even, then $\left(\frac{b}{2}\right)^2 = \frac{c-a}{2} \cdot \frac{c+a}{2}$.
Primitive condition implies $\gcd\left(\frac{c-a}{2}, \frac{c+a}{2}\right) = 1$. Note if we use a suitable substitution, then $xy = z^2$, $\gcd(x, y) = 1 \Rightarrow$ both x and y are perfect squares (By unique factorization in Z.) So $\frac{c-a}{2} = s^2$, $\frac{c+a}{2} = s^2$ for some $s, t \in \mathbb{Z}$, then $c = s^2 + t^2$, $a = s^2 - t^2$ and $b = 2st$. It is also clear that the extra conditions are also true.

Method 2: solve $a^2 + b^2 = c^2$ in $\mathbb{Z}$ is equivalent to solve $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$ in $\mathbb{Q}$, i.e., finding primitive triples is equivalent to finding rational points on $x^2 + y^2$.
Pick an (obvious) rational point on $\mathbb{C}$, draw secant line with rational slope passing through $\mathbb{C}$. Check that the other point on the intersection $x^2 + y^2 = 1$ and the previous line is also rational. Note all rational points can be obtained in this way. Then we would get

$$(x, y) = \left(\frac{s^2 - t^2}{s^2 + t^2}, \frac{2st}{s^2 + t^2}\right).$$

□

Congruent number problem: more generally, $N \in \mathbb{Q}_{\geq 0}$ is congruent if and only if $N = \frac{1}{2}ab$ and $a^2 + b^2 = c^2$, for some $a, b, c \in \mathbb{Q}$.
Remark: N is congruent if and only if $N \cdot \left(\frac{p}{q}\right)^2$ is also congruent, for any $\frac{p}{q}$, i.e., condition only depends on $\bar{N} \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.
Since we can always find suitable $\frac{p}{q}$ to make $N \cdot \left(\frac{p}{q}\right)^2 \in \mathbb{Z}_{>0}$ and square-free, so we only interested in characterizing square-free N as congruent numbers.

2.6 Negative Results For Diophantine Equations

Example 1: $x^2 + y^2 + z^2 = 4^a(8b + 7)$, for some fixed $a, b \in \mathbb{Z}_{\geq 0}$ has no integer solutions.

We show this using induction on a:
Suppose $a = 0$, then $x^2 + y^2 + z^2 = 8b + 7$, taking $\mod 8$ on both sides, we can see that $x^2 + y^2 + z^2 = 8b + 7$ has

no solutions.
Next assume there is no solution for a, we show that $x^2+y^2+z^2=4^{a+1}(8b+7)$ has no solutions. Reduce $\mod 4$, we have $x^2+y^2+z^2=0$, $x^2=y^2=z^2=0 \mod 4$, then 2 is a divisor of x,y,z. So we can divide 4 on both sides of the equation, we have $\left(\frac{x}{2}\right)^2+\left(\frac{y}{2}\right)^2+\left(\frac{z}{2}\right)^2=4^a(8b+7)$, which has no solutions. Hence $x^2+y^2+z^2=4^{a+1}(8b+7)$ must have no solution as well.

Remark: for any integer n not of the form $4^a(8b+7)$, $x^2+y^2+z^2=n$ has a solution.

Let S_2 denote the set of numbers n, s.t., $x^2+y^2=n$ has a solution, then S_2 is closed under multiplication. I.e., if $m\in S_2$ and $n\in S_2$, then $mn\in S_2$.

Example 2: $y^2=x^3+7$ has no integer solution, however, it has a solution $\mod n$ for every $n\in\mathbb{Z}_{>0}$.

If x is even, then $x=2k$, so $y^2=8xk^3+7$, and taking modular 3 on both sides, we have $y^2=3$ which is a contradiction. Hence x can only be odd. By adding 1 on both sides, we have $y^2+1=(x+2)(x^2-2x+4)$. We can see x cannot be negative (check -1) is enough, so $x+2$ is positive. We can also see $x=1 \mod 4$, as if $x=3 \mod 4$, then $y^2=2 \mod 4$.
Now we show that $y^2+1=(x+2)(x^2-2x+4)$ has no solution. If $p|y^2+1$, which happens when -1 is a QR mod p, that is when $p=1 \mod 4$. Since x is $1 \mod 4$, $x+2=3 \mod 4$, and is a positive divisor of y^2+1. Then $\exists$ a prime divisor of $x+2$ that is $3 \mod 4$. The divisor of $x+2$ that is $3 \mod 4$ is also a divisor of y^2+1 which is a contradiction, as if $q=3 \mod 4$ is a prime that divides y^2+1, then $y^2=-1 \mod q$, which cannot happen.

Example 3: Fermat's Last Theorem case $n=4$, i.e., $x^4+y^4=z^4$, $xyz\neq 0$, has no integer solution.

We can prove this using "descent" and parametrization and Pythagorean triples. Instead, we show $x^4+y^4=z^2$, $xyz\neq 0$ has no solution.
If $d=\gcd(x,y)$, then $d^4|x^4+y^4$, so $d^2|z$, then $\left(\frac{x}{d}\right)^4+\left(\frac{y}{d}\right)^4=\left(\frac{z}{d^2}\right)^2$. Hence WLOG, we can assume that $\gcd(x,y)=1$. Both x,y cannot be even and both cannot be odd, as otherwise we get $2=z^2 \mod 4$. WLOG, let x be even, y odd.
By Pythagorean Triple Parametrization, $(x^2)^2+(u^2)^2=z^2$, we have $x^2=2st$, $y^2=s^2-t^2$ and $z=s^2+t^2$, where $\gcd(s,t)=1$, $s>t$, $s\neq t \mod 2$. From $y^2=s^2-t^2$, we get s is odd, t is even, so let $t=2k$, then $x^2=4sk$, which yields $\left(\frac{x}{2}\right)^2=sk$. Since $\gcd(s,k)=1$, then both s and k are squares. So we can let $s=a^2$ and $k=b^2$, so $y^2=(a^2)^2-(2b^2)^2$.
Therefore, $(2b^2)^2+y^2=(a^2)^2$ which is again a Pythagorean triple $(y,2b^2,a^2)$. So $y=m^2-n^2$, $2b^2=2mn$ and $a^2=m^2+n^2$, for some $m,n\in\mathbb{Z}$, $\gcd(m,n)=1$, $m\neq n \mod 2$. Then $b^2=mn$, so m,n are squares. Let $m=v^2,n=w^2$, then $a^2=v^4+w^4$.
Note $a<z$, therefore start with a solution, we get a "smaller" solution. Then by "descent", no such solution exists.

2.7 Pell's Equation

Consider the diophantine equation of the form $x^2 - dy^2 = 1$, it will always have trivial solution of the form $(\pm 1, 0)$. Note if d is negative, then the equation becomes $x^2 + cy^2 = 1$, where $c \geq 1$, so it will have no non-trivial solutions. If d is a perfect square, i.e., $d = c^2$, then the equation becomes $(x - cy)(x + cy) = 1$, and we can easily get the solutions. Hence we consider the case where d is positive and not a perfect square. In this case, there is always a solution, in fact there are infinitely many solutions. The set of solutions form a group isomorphic to $\mathbb{Z}$. Then to get all the solution, it suffices to find the solution corresponding to 1 or -1 under this isomorphism. To do this, we must use Diophantine approximation, i.e., to get rational approximations to $\sqrt{d}$.

Finding solutions to $x^2 - dy^2 = 1$ is the same as studying $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \,|\, a, b \in \mathbb{Z}\}$ and find the elements in $\mathbb{Z}[\sqrt{d}]$ that has norm 1.
Observations:

1. $\mathbb{Z}[\sqrt{d}]$ is a ring.
2. $x + y\sqrt{d} = x' + y'\sqrt{d}$ if and only if $x = x'$ and $y = y'$.
3. If $x^2 - dy^2 = 1$ has a solution, $(a, b), (a', b')$. Then the coefficients of $(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + bb'd) + \sqrt{d}(ab' + a'b)$ gives another solutions. Then the norm one element of $\mathbb{Z}[\sqrt{d}]$ forms a subgroup.
4. If (a, b) is a solution, then coefficients of $(a + b\sqrt{d})^k$, $k \in \mathbb{Z}$ also gives a solution. If $k > 0$, then apply 3 repeatedly. If $k = 0$, we get the trivial solution. If $k < 0$: $(a + b\sqrt{d})^{-1} = a - b\sqrt{d}$ which clearly solves $x^2 - dy^2 = 1$.
5. We need to find a "generating solution" (a, b) such that procedure 4 gives all the solutions. Intuitively, find the" smallest positive solution", nonetheless in the ring $\mathbb{Z}[\sqrt{d}]$, it is not necessarily the case that $a + b\sqrt{d} \geq a' + b'\sqrt{d}$ if and only if $a \geq a'$ and $b \geq b'$.

Proposition 2.18 *Let (a, b) be a solution and $a + b\sqrt{d} > 1$. Then $a \geq 2, b \geq 1$. If $(x, y), (a, b)$ are two solutions, $x, y, a, b \geq 0$. Then $a + b\sqrt{d} < x + y\sqrt{d}$ if and only if $a < x$ and $b < y$, if and only if $a < x$ or $b < y$.*

Proof: $a + b\sqrt{d} > 1$ if $\frac{1}{a+b\sqrt{d}} = a - b\sqrt{d} < 1$. So $a + b\sqrt{d} > a - b\sqrt{d}$, so $2b\sqrt{d} > 0 \Rightarrow b \geq 1$. $a^2 - db^2 = 1$, $b \geq 1$, then $a^2 = 1 + db^2$, so $a \geq 2$.

If $a < x$ and $b < y$, then clearly $a + b\sqrt{d} < x + y\sqrt{d}$. Now suppose $x, y, a, b \geq 0$, we have $a, x \geq 1$. We have $a + b\sqrt{d} < x + y\sqrt{d}$, so $a - b\sqrt{d} > x - y\sqrt{d}$. Then $(a + x) + (b - y)\sqrt{d} < (a + x) + (y - b)\sqrt{d}$. So $y > b$. Then using the fact (a, b), (x, y) are solutions, then we get $a < x$. □

Theorem 2.19 *Assume $(x_1, y_1) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ is a solution with y_1 minimal, then all the solutions are coefficients of numbers of the form $\pm(x_1 + y_1\sqrt{d})^k : k \in \mathbb{Z}$.*

Proof: Suppose $(x, y) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ is a positive solution, then $x_1 + y_1\sqrt{d} > 1 \Rightarrow (x_1 + y_1\sqrt{d})^k \to \infty$ as $k \to \infty$. To show $x + y\sqrt{d} = (x_1 + y\sqrt{d})^k$ for some k, we argue via contradiction. That is we can find $k > 0$, s.t., $(x_1 + y_1\sqrt{d})^k < x + y\sqrt{d} < (x_1 + y_1\sqrt{d})^{k+1}$. Then divide $(x_1 + y_1\sqrt{d})^k$, we get $1 < x' + y'\sqrt{d} < x_1 + y_1\sqrt{d}$, which contradicts the minimality of y_1. Hence it must be the case that $x + y\sqrt{d} = (x - 1 + y_1\sqrt{d})^k$ for some k. Similarly, we can show for the negative case. □

Then it remains to obtain the "minimal solution". Earlier we saw $x^2 - dy^2 = 1$, then $x^2 = 1 + dy^2 \Leftrightarrow \frac{x}{y} = \sqrt{d + \frac{1}{y^2}} \approx \sqrt{d}$. So we need "good" rational approximation to the irrational number $\sqrt{d}$.

2.8 Continued Fractions and Rational Approximations

We can get rational approximation to irrationals (more specifically $\sqrt{a}$ in this case) via continued fraction.
Any rational number can be written in forms of

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots_{a_{k-1} + \frac{1}{a_k}}}}.$$

This expression can be calculated using Euclidean Algorithm and is essentially unique. Note the process will eventually terminate, so it can be denoted by $[a_1, a_2, \cdots, a_{k-1}, a_k]$, where $a_k > 1$. Since the expression is unique, then the tuple $[a_1, a_2, \cdots, a_k]$ is also unique.
Next, if we consider an irrational number, we can do the same process, its just that it will never end. For example $\sqrt{2} = [1, 2, 2, \cdots]$.

Definition: for an finite continued fraction $c = [a_0, a_1, \cdots, a_k]$, its truncation $c_n = [a_0, \cdots, a_n]$, $(n < k)$, is called a convergent.

Proposition 2.20 *$c = [a_0, \cdots, a_k]$, $a_i > 0$. Let $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$, and $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$. Then*

1. *$p_n > p_{n-1}$, $q_n > q_{n-1}$.*
2. *$c_n = \frac{p_n}{q_n}$.*
3. *$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$.*
4. *$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$.*
5. *$p_n q_{n-2} - p_{n-2} q_n = (-1)^{n-2} a_n$, $c_n - c_{n-2} = \frac{(-1)^{n-2} a_n}{q_n q_{n-2}}$.*
6. *$c_1 > c_3 > c_5 \cdots > \cdots > c_6 > c_4 > c_2$.*
7. *For $n < k$, we have $|c - c_n| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$.*

Proof:

1. Trivial.
2. Verify from the definition of c_n
3. $$\begin{aligned} p_nq_{n-1} - q_np_{n-1} &= (a_np_{n-1} + p_{n-2})q_{n-1} - (a_nq_{n-1} + q_{n-2})p_{n-1} \\ &= p_{n-2}q_{n-1} - q_{n-2}p_{n-1} \\ &= \cdots \\ &= (-1)^n(a_0 \cdot 0 - 1 \cdot 1) \\ &= (-1)^{n-1} \end{aligned}$$
4. This is by direct computation.
5. Similar to the previous two statements.
6. By 5, if n is even, then $c_n - c_{n-2} > 0$, hence $c_2 < c_4 < \cdots$. If n is odd, then $c_n - c_{n-2} < 0$, so $c_1 > c_3 > \cdots$. Also we want to show $c_{2n+1} > c_{2n}$, by 4, we have $c_{2n+1} - c_{2n} = \frac{(-1)^{2n}}{q_{2n+1}q_{2n}} > 0$.
7. If k is odd, then $c_1 > c_3 > \cdots > c = c_k > c_{even}$. Similarly, if k is even, then $c_{odd} > c = c_k > \cdots > c_4 > c_2$. If $n < k$, then $|c - c_n| \leq |c_{n+1} - c_n|$, since c is between c_n and c_{n-1}. So $|c - c_n| \leq \frac{1}{q_nq_{n+1}} < \frac{1}{q_n^2}$.

□

Definition: for a sequence $(a_0, a_1, \cdots)$, $a_i > 0$. Define the infinite continued fraction $a = [a_0, a_1, \cdots] := \lim_{n\to\infty}[a_0, a_1, \cdots, a_n]$. Similar to 2.20, we can check that both the even and odd terms converges to a limit. These two limits are equal since $|c_n - c_{n-1}| = \frac{1}{q_nq_{n-1}}$, then letting $n \to \infty$, we have the two limits are equal.

Proposition 2.21 *Different positive numbers have different continued fraction expression.*

Proof: Since the limit of the continuous fraction expression is unique. □

Fact: any recurring infinite continued fraction must be a quadratic irrational, i.e., it satisfies a degree 2 equation and irrational. The converse is also true (Not trivial).

Theorem 2.22 (Dirichlet) *For arbitrary irrational α, there exists infinitely many $\frac{p}{q}$, $p, q \in \mathbb{Q}$, such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2} \quad (*).$$

And if $(*)$ is true, then $\frac{p_n}{q_n}$ must be a convergent of the continued fraction for α.

Proof: Let $\frac{p_n}{q_n} = c_n$ be a convergent for c_n. Suppose that none of c_n, c_{n+1} satisfies $*$. $|c_n - c_{n+1}| = |c_n - \alpha| + |c_{n+1} - \alpha|$, since α is in between c_n and c_{n+1}. Then

$$(c_n - c_{n+1})^2 \geq 4|c_n - \alpha||c_{n+1} - \alpha|.$$

But equality cannot happen, because otherwise we have $|c_n - \alpha| = |c_{n+1} - \alpha|$, so α is rational, which is a contradiction. So we have

$$|c_n - c_{n+1}|^2 > 4\frac{1}{2q_n^2} \cdot \frac{1}{2q_{n+1}^2} = \frac{1}{q_n^2 q_{n+1}^2} \Rightarrow |c_n - c_{n+1}| > \frac{1}{q_n q_{n+1}}.$$

This contradicts with the fact that $|c - c_n| \leq \frac{1}{q_n q_{n+1}}$. □

Lemma 2.23 *If $\alpha \in \mathbb{R} - \mathbb{Q}$ and $\frac{p}{q}$ is a non-convergent that satisfies $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$. If $\frac{p_n}{q_n}$, $\frac{p_{n+1}}{q_{n+1}}$ are two continuous fraction convergent with $q < q_{n+1}$, then $|q_n\alpha - p_n| < |q\alpha - p|$.*

Proof: Suppose towards a contradiction $|q\alpha - p| \leq |q_n\alpha - p_n|$. Since

$$\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

Since the determinant of the matrix is ± 1, so invertible in $\mathbb{Z}$. So $p = xp_n + yp_{n+1}$, $q = xq_n + yq_{n+1}$. Since $q < q_{n+1}$, x, y have opposite signs (as $\frac{p}{q}$ is not a convergent). Recall, $\alpha - \frac{p_n}{q_n}$ and $\alpha - \frac{p_{n+1}}{q_{n+1}}$ have opposite signs. So $x(\alpha - \frac{p_n}{q_n})$ and $y(\alpha - \frac{p_{n+1}}{q_{n+1}})$ have the same sign. So,

$$\begin{aligned} |q\alpha - p| &= |(xq_n + yq_{n+1})\alpha - (xp_n + yp_{n+1})| \\ &= |x(q_n\alpha - p_n) + y(q_{n+1})\alpha - p_{n+1})| \\ &= |x||q_n\alpha - p_n| + |y||q_{n+1}\alpha - p_{n+1}| \qquad \text{(same sign)} \\ &> |q_n\alpha - p_n| \end{aligned}$$

However, this is a contradiction. Then it must be the case $|q_n\alpha - p_n| < |q\alpha - p|$. □

Proposition 2.24 *If $\alpha \in \mathbb{R} - \mathbb{Q}$ and $\frac{p}{q}$ is a rational number that satisfies $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, then $\frac{p}{q}$ has to be continuous fraction convergent of α.*

Proof: Suppose not, let $\left\{\frac{p_n}{q_n}\right\}_{n\geq 1}$ be the sequence of convergence. $p_n, q_n \to \infty$ as $n \to \infty$. Let n be such that $q_n \leq q < q_{n+1}$. Suppose $q_n < q < q_{n+1}$. Then applying Lemma 2.23, we have

$$|q_n\alpha - p_n| < q|\alpha - \frac{p}{q}| < q \cdot \frac{1}{2q^2} = \frac{1}{2q}.$$

Hence $|\alpha - \frac{p_n}{q_n}| < \frac{1}{2qq_n}$. But notice

$$\frac{1}{q_n q} \leq \left|\frac{p_n q - pq_n}{q_n q}\right| = \left|\frac{p_n}{q_n} - \frac{p}{q}\right| \leq \left|\frac{p}{q} - \alpha\right| + \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q^2} + \frac{1}{2qq^n} = \frac{q_n + q}{2q^2 q_n}.$$

Hence we have $2q < q_n + q$, but then we have $q < q_n$ contradicting $q_n < q$. So, it must be the case $q_n = q$. □

Remark: this shows that any solution to the Pell's Equation has to come from a convergent.

Theorem 2.25 *One of the three consecutive convergents satisfies*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{\sqrt{5}q_n^2}.$$

Proof: Suppose towards a contradiction, $|\alpha - \frac{p_i}{q_i}| \geq \frac{1}{\sqrt{5}q_i^2}$ for $i = n, n+1, n+2$.

$$\left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_n q_{n+1}}$$
$$\frac{1}{\sqrt{5}q_n^2} + \frac{1}{\sqrt{5}q_{n+1}^2} \leq \frac{1}{q_n q_{n+1}}$$
$$\frac{q_{n+1}}{q_n} + \frac{q_n}{q_{n+1}} \leq \sqrt{5}$$

Then $\frac{q_{n+1}}{q_n} < \frac{\sqrt{5}+1}{2}$, as $x \mapsto x + \frac{1}{x}$ is strictly increasing function on $(1, \infty)$, so if $x \geq \frac{\sqrt{5}+1}{2}$, then $x + \frac{1}{x} \geq \sqrt{5}$. But in this case $\frac{q_{n+1}}{q_n}$ cannot be irrational, so it cannot be $\frac{\sqrt{5}+1}{2}$.
Similarly,we have

$$\frac{q_{n+2}}{q_{n+1}} < \frac{\sqrt{5}+1}{2} \Rightarrow \frac{a_{n+2}q_{n+1} + q_n}{q_{n+1}} < \frac{\sqrt{5}+1}{2}.$$

Since $a_{n+2} > 1$, then $1 + \frac{q_n}{q_{n+1}} < \frac{\sqrt{5}+1}{2}$. So

$$\frac{\sqrt{5}+1}{2} > 1 + \frac{q_n}{q_{n+1}} > 1 + \frac{\sqrt{5}-1}{2}$$

Which is a contradiction. □

Remark: note the best approximation we can have is $\sqrt{5}$. That is That is if $\lambda > \sqrt{5}$, then $\alpha = \frac{\sqrt{5}+1}{2}$ and any number "equivalent" to it: $\alpha \sim \beta$ if CF of α and CT of β agrees after a finite stage only has finitely many $\frac{p}{q}'s$, s.t., $|\alpha - \frac{p}{q}| < \frac{1}{\lambda q^2}$.
Since a good enough approximation must be a convergent as $\frac{1}{\lambda q^2} < \frac{1}{2q^2}$, then CF of $\frac{1+\sqrt{5}}{2} = [1, \bar{1}]$. Then the convergent are $\frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \cdots$, which are ratio's of consecutive Fibonacci numbers.
To test this inequality, we can find the general formula for convergent,

$$F_n = \frac{\phi^n - \psi^n}{\phi - \psi}, \quad \text{where } \phi = \frac{\sqrt{5}+1}{2}, \ \psi = \frac{1-\sqrt{5}}{2}.$$

Compute

$$\lim_{n\to\infty} q_n^2 |\alpha - \frac{p_n}{q_n}| = \frac{1}{\sqrt{5}}.$$

This means, all but finitely many $\frac{p_n}{q_n}$ are such that

$$\left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{\lambda q_n^2}.$$

Proposition 2.26 *A real number α is approximable by infinitely many rational $\frac{p}{q}$ with $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$, then α is irrational.*

Proof: Suppose α is irrational, then the statement holds. Next, suppose $\alpha = \frac{a}{b}$, then

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \left|\frac{aq - bp}{bq}\right|.$$

If $b \leq q$, this can give at most finitely many solutions.
If $q > b$, then we need $|aq - bp| < 1$, i.e., $aq = bp$. But then $\frac{a}{b} = \frac{p}{q}$, which means at most 1 solution in this case. Hence combined, there can have at most finitely many such $\frac{p}{q}'s$. □

2.9 Transcendental Numbers

Criterion for testing Transcendence:
Note a rational number is a solution of a degree 1 equation with integer coefficient, that is $\frac{p}{q}$ satisfies $qx - p = 0$.
An algebraic number is one that is a solution of some polynomial with integer coefficient.
Transcendental numbers are real numbers that is not an algebraic numbers.

Theorem 2.27 (Liouville) *Suppose α is algebraic number of* $\deg d > 1$*, that is the minimal degree of a polynomial that the number satisfies is of degree d.Then there is a positive real constant A (depending on α), s.t.,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{A}{q^d} \quad \textit{for all } \frac{p}{q}.$$

Using this we can check that $\alpha = \sum_{n \geq 0} \frac{1}{10^{n!}}$ is not algebraic.
Say α is algebraic, then $|\alpha - \frac{p}{q}| > \frac{A}{q^d}$. If we can produce a sequence of $\frac{p_n}{q_n}$, s.t., $|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n^n}$. Then for any n, we must have, $\frac{1}{q_n^n} > \frac{A}{q_n^\alpha}$, but this is a contradiction, as d is fixed, and $n \to \infty$, so $\frac{1}{q_n^{n-d}} \to 0 < A$. And of course this can be done by taking the partial sums of α.

2.10 Solution of Pell's Equation

Algebraic Comment: The solutions of $x^2 - dy^2 = \pm 1$ are exactly the units of $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. This is seen using the norm map $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$, $a + b\sqrt{d} \mapsto a^2 - d^2b = (a + b\sqrt{d})(a - b\sqrt{d})$. Note N is multiplicative, that is $N(\alpha\beta) = N(\alpha)N(\beta)$. Then if α is a unit, then $\exists \beta \in \mathbb{Z}[\sqrt{d}]$, s.t., $\alpha\beta = 1$, so we must have $N(\alpha\beta) = N(1)$, $N(\alpha) = \pm 1$, i.e., $a^2 - db^2 = \pm 1$, so (a, b) is a solution to $x^2 - dy^2 = \pm 1$. Conversely, if $N(\alpha) = \pm 1$, then $\alpha\bar{\alpha} = \pm 1$, then one of $\pm\bar{\alpha}$ is the inverse of α.

Theorem 2.28 *Pell's Equation ($x^2 - dy^2 = 1$) has a non-trivial solution.*

Proof: Look into continuous fraction convergents of $\sqrt{d}$. Let $\frac{p}{q}$ be one such, then $|\sqrt{d} - \frac{p}{q}| < \frac{1}{q^2} < 1$. Also, $|\sqrt{d} + \frac{p}{q}| = |\frac{p}{q} - \sqrt{d}| + 2\sqrt{d} < 1 + 2\sqrt{d}$. So

$$|p^2 - dq^2| = q^2 \left| \frac{p^2}{q^2} - d \right| < q^2 \cdot \frac{1}{q^2} \cdot (1 + 2\sqrt{d}) \Rightarrow |p^2 - dq^2| < 1 + 2\sqrt{d}.$$

Since p, q, d are integers, then $|p^2 - dq^2|$ is also an integer, so there is some $0 \leq r < 1 + 2\sqrt{d}$, s.t., $p^2 - dq^2 = r$ for infinitely many convergent $\frac{p}{q}$. I.e., we have produced infinitely many $\alpha \in \mathbb{Z}[\sqrt{d}]$, s.t., $N(\alpha) = r$, where $r < 1 + 2\sqrt{d}$. We want to find α' with $N(\alpha') = 1$. Then for any two different α_1, α_2, s.t., $N(\alpha_1) = N(\alpha_2) = r$, we have $N(\frac{\alpha_1}{\alpha_2}) = \frac{N(\alpha_1)}{N(\alpha_2)} = 1$. So it suffices to find α_1, α_2 with the above condition, s.t., $\alpha' = \frac{\alpha_1}{\alpha_2}$ is in $\mathbb{Z}[\sqrt{d}]$.
Consider $p \mod r$, $q \mod r$, there are finitely many possibilities. Pick (p_1, q_1), (p_2, q_2) satisfying $x^2 - dy^2 = r$, s.t., $p_1 = p_2 \mod r$ and $q_1 = q_2 \mod r$. We claim $\frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}} = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ and (a, b) satisfies $x^2 - dy^2 = 1$. And by direct computation, we have

$$\frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}} = \frac{p_1p_2 - q_1q_2d + (q_1p_2 - p_1q_2)\sqrt{d}}{p_2^2 - q_2^2d}.$$

□

Remark: $x^2 - dy^2 = -1$ may not have a solution. Reduce modulo d, we have $x^2 = -1 \mod d$, and clearly this doesn't always have a solution. It only has a solution if primes $p = 3 \mod 4$ that divides d appears with even exponents.

Theorem 2.29

1. *$\sqrt{d} = [a_0, \overline{a_1, \cdots, a_{k-1}, 2a_0}]$ if d is positive and not a square.*
2. *All positive solution to $x^2 - dy^2 = \pm 1$ are of the form (p_n, q_n), where $\frac{p_n}{q_n}$ is a continuous fraction convergent of $\sqrt{d}$.*
3. *We define the period of d to be k. If k is even, then $x^2 - dy^2 = -1$ has no solution and all the positive solutions of $x^2 - dy^2 = 1$ are given by $x = p_{kr-1}$, $y = q_{kr-1}$, for $r = 1, 2, \cdots$. If k is odd, then $x^2 - dy^2 = -1$ has a solution, and all the positive solutions are (p_{kr-1}, q_{kr-1}), for $r = 1, 3, 5, \cdots$; and the positive solutions for $x^2 - dy^2 = 1$ are given (p_{kr-1}, q_{kr-1}), for $r = 2, 4, 6, \cdots$.*

Theorem 2.30 *Fix a solution $(a, b) \in \mathbb{Z}^2_{\geq 0}$ of $x^2 - dy^2 = 1$. Then for each $n \in \mathbb{Z} \setminus \{0\}$, every integer solution of $x^2 - dy^2 = n$ can be obtained from $(x' + y'\sqrt{d})(a + b\sqrt{d})^k$, where (x', y') is a solution of $x^2 - dy^2 = n$ with*

$$|x'| \leq \frac{\sqrt{|n|}}{2}(\sqrt{u} + \frac{1}{\sqrt{u}}), \quad |y'| \leq \frac{\sqrt{|n|}}{2\sqrt{d}}(\sqrt{u} + \frac{1}{\sqrt{u}}).$$

where $u = (a + b\sqrt{d})$. If $n > 0$, then we obtain a tighter bound, $|y'| \leq \frac{\sqrt{n}}{2\sqrt{d}}(\sqrt{u} - \frac{1}{\sqrt{u}})$.

3 Binary Quadratic Form

Prelude: which prime $p = x^2 + 2y^2$, for $x, y \in \mathbb{Z}$.
Answer: it happens if and only if $\left(\frac{-2}{p}\right) = 1$ or $p = 2$.
In general, we ask: what primes or numbers in general can be written as values of a given $ax^2 + bxy + cy^2$.

Definition:

1. We say $n \in \mathbb{Z}$ is represented by (a, b, c) form of $ax^2 + bxy + cy^2 = n$ has solutions in integers.
2. Discriminant $\Delta = b^2 - 4ac$.
3. f is definite if $f > 0$ or $f < 0$ for all values (x, y). It is semidefinite, if $f \geq 0$ or $f \leq 0$ for all values (x, y).

Remark: if Δ is a perfect square, then $f(x, y) = (\alpha x + \beta y)(\gamma x + \delta y)$ with

$$\Delta = \left[\det \begin{pmatrix} \alpha & \beta \\ \delta & \gamma \end{pmatrix}\right]^2.$$

Solving $f(x, y) = n$ amounts to factoring n and handle two linear equations. Hence in general, we do not consider the case when Δ is a perfect square.

Proposition 3.1 *f is definite iff $\Delta < 0$; In this case x is positive definite iff $a > 0$, negative definite iff $a < 0$.*

Proof: Calculus. □

To see whether n can be represented by f is equivalent to see whether $\frac{n}{d^2}$ can be properly represented (x, y are coprime) by $\frac{1}{d^2}f$, for any $d \in \mathbb{Z} \setminus \{0\}$.

Proposition 3.2 *Suppose $\Delta = 0$ or $1 \mod 4$, $n \in \mathbb{Z}$. There is a binary quadratic form of discriminant Δ, properly representing n, iff Δ is a quadratic residue mod n.*

Proof: $\Leftarrow$: $\Delta = b^2 \mod 4n$, then $b^2 - \Delta = 4nc$ for some c. So $f(x, y) = nx^2 + bxy + cy^2$ has the same discriminant as Δ and properly represents n, as $(1, 0)$ solves $f(x, y) = n$.
$\Rightarrow$: Suppose $ax^2 + bxy + cy^2 = n$ with $\gcd(x, y) = 1$. Then $4a^2x^2 + 4abxy + 4acy^2 = 4an$, completing the square, we have

$$(2ax + by)^2 + (4ac - b^2)y^2 = 4an \Rightarrow (2ax + by)^2 = \Delta \cdot y^2 \mod 4n \quad (*)$$

Since $(2ax + by^2) - \Delta y^2 = 4an$. So $a | \gcd(y, 4n)$, then multiplying y^{-2} on both sides of $(*)$, we have Δ is a quadratic residue mod $\frac{4n}{\gcd(y,4n)}$. Similarly, we get Δ is a quadratic residue mod $\frac{4n}{\gcd(x,4n)}$.
Notice $\operatorname{lcm}\left(\frac{4n}{\gcd(x,4n)}, \frac{4n}{\gcd(y,4n)}\right) = 4n$, because $(x, y) = 1$, then Δ is a quadratic residue mod $4n$. □

Corollary 3.2.1 *An odd prime p is (properly) represented by f if and only if $\left(\frac{\Delta}{p}\right) = 1$.*

Proof: $\Delta = 0, 1 \mod 4$; and a number is a quadratic residue mod p iff it is a quadratic residue mod $4p$. $\square$

It makes to collect all the binary quadratic forms with fixed discriminant Δ.
Observe: $f(x,y) = x^2 + y^2 [= g(x+y, y)]$, $g(x,y) = x^2 - 2xy + 2y^2 [= f(x-y, y)]$. Then n is representable by f if and only if n is representable by g. For representability purposes, can identify such forms that can be converted from one to another by integral linear change of variable.
$f = ax^2 + byx + cy^2$ is associated with the matrix $M = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$. Then $f(x,y) = v^T M v$, where $v = \begin{pmatrix} x \\ y \end{pmatrix}$. Then the change of variable above is via $v \mapsto Av$, so that $M_f = A^{-1} M_g A$. However, we need to ensure that $A \in GL_2(\mathbb{Z})$ and $A^{-1} \in GL_2(\mathbb{Z})$, that is $\det(A) = \pm 1$. For this specific case, we have $A = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.
In general, we will restrict that change of variables matrix A to have determinant 1. Observe that if $f(v)$ has discriminant Δ, then $f(Av)$ also has discriminant Δ. Hence we can define $SL_2(\mathbb{Z}) \curvearrowright$ the set of binary quadratic form having fixed discriminant Δ, $A \cdot f(v) := f(Av)$.

Notation: let S_Δ denote the set of all binary quadratic forms having fixed discriminant Δ.

Now consider $f = x^2 + y^2 \Rightarrow \Delta = -4$. Then p is represented by some form in S_Δ, iff $\left(\frac{-4}{p}\right)\left(\frac{-1}{p}\right) = 1$ if and only if $p = 2$ or $p = 1 \mod 4$. We claim without proving here that S_Δ has only one orbit under the action by $SL_2(\mathbb{Z})$, i.e., if $f, g \in S_\Delta$, then there exists an $A \in SL_2(\mathbb{Z})$, s.t., $A \cdot f = g$. Thus one can convert any form $f \in S_\Delta$ to $x^2 + y^2$, so $x^2 + y^2$ can represent any prime that is 1 mod 4, as well as 2.

Definition: we say $f = ax^2 + bxy + cy^2$ which is a BQF is reduced if

- $-|a| < b \leq |a| \leq |c|$;
- $|a| < |c|$ if $b = |a|$;
- $b \geq 0$ if $|a| = |c|$.

Theorem 3.3 *Fix $\Delta = 0$ or $1 \mod 4$; suppose f is reduced BQF in S_Δ. Then*

1. - *If $\Delta < 0$: a, c has the same sign, $|a| \leq \sqrt{-\frac{\Delta}{3}}$;*
   - *If $\Delta > 0$: a, c has opposite signs $|a| \leq \frac{\sqrt{\Delta}}{2}$.*

   In both cases, there are finitely many reduced in S_Δ.
2. *Every equivalence class in S_Δ have at least on reduced forms. But it may happen that two distinct reduced forms are equivalent (in fact, happens when $\Delta > 0$).*
3. *There are finitely many equivalence class in S_Δ.*

Proof:

2 To show any BQF in S_Δ can be converted to a reduced form. Fact: $SL_2(\mathbb{Z})$ is generated by $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We consider the effect of these generators acting on $f(x, y)$:

$$\begin{aligned} S \cdot f(x,y) &= cx^2 - bxy + ay^2 \\ S^2 \cdot f(x,y) &= f(x,y) \\ T^m \cdot f(x,y) &= ax^2 + (b+2am)xy + (am^2 + bm + c)y^2 \end{aligned}$$

Then we have a reduction algorithm:

- If $b \notin (-|a|, |a|]$, find the unique integer m¡ s.t., $b + 2am \in (-|a|, |a|]$. Then apply T^m to f.
- Now we have $b \in (-|a|, |a|]$. Test if $|a| = |c|$ and $|b| \geq 0$, in this case then f is already reduced. If $b < 0$ and $|a| = |c|$, then apply S and the new f is reduced; if $|c| < |a|$, then apply S and repeat the previous step.
- Eventually the process terminates, as $|a|$ gets smaller than smaller, it can only terminate if it is already reduced, or end by applying S, which would also mean f is reduced.

□

Definition: we define the class number $h(\Delta)$ as the number of orbits of S_Δ under the action of $SL_2(\mathbb{Z})$.
Example; $h(13) = 1$, as for any reduced form, we need to have $|a| \leq \frac{\sqrt{13}}{2} < 2$. So the only possible reduced forms are $f = (-1, 1, 3)$ and $g = (1, 1, -3)$. Next, we can check that f and g are equivalent by finding A, s.t., $g(x) = A \cdot f(x) = f(Ax)$, where $x \in \mathbb{R}^2$.
Example: $h(-4) = 2$, as it has two reduced forms $f = (1, 0, 1)$ and $g = (-1, 0, -1)$, and these two are not equivalent to each other.
Example: $h(-40) = 4$. There are 4 reduced forms with determinant -40: $(1, 0, 10)$, $(2, 0, 5)$, $(-1, 0, -10)$, $(-2, 0, -5)$, and none of them are equivalent to each other.

Proposition 3.4 *Suppose $f(x, y)$ and $g(x, y)$ are equivalent quadratic forms, then $f(x, y)$ and $g(x, y)$ properly represent the same set of numbers.*

Proof: Suppose $n \in \mathbb{Z}$ is properly represented by (x_0, y_0), then $\gcd(x_0, y_0) = 1$. Let $A \in SL_2(\mathbb{Z})$, s.t., $A \cdot f = g$, then $g\left((A \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right) = n$.
Let (a, b) be such that $ax_0 + by_0 = 1$, then $((a, b)A^{-1})A(x_0, y_0)^T = 1$, hence $A(x_0, y_0)^T$ is coprime. □

Lemma 3.5 *If f is a positive definite reduced from in S_Δ. Then the smallest positive values of f are $a, c, a + c - |b|$ (in ascending order).*

Proof: Direct computation. □

Theorem 3.6 *Suppose $\Delta < 0$ (i.e., the form is definite); $f, g \in S_\Delta$ reduced, then $f \sim g \Rightarrow f = g$.*

Proof: $f \sim g \Leftrightarrow (-f) \sim (-g)$ by the same matrix A. And clearly, a positive definite form cannot be equivalent to a negative definite form. So, WLOG, we prove the theorem for positive definite forms.
Now suppose $f \sim g$, then by Lemma 3.5, the smallest integers properly represented by f and g are the same. The smallest values for $f = (a, b, c)$ must be $a \leq c \leq a + c - |b|$; the smallest values of $g = (a', b', c')$ must be $a' \leq c' \leq a' + c' - |b'|$. Then it must follow that $a = a'$, $a' = c$ and $a + c - |b| = a' + c' - |b'|$. So we have $a = a'$, $c = c'$. Can use the inequalities in reduced forms to rule out the case $b = -b'$, so we must get $b = b'$. □

Corollary 3.6.1 *If $\Delta < 0$, then $h(\Delta)$ is equal to the number of reduced forms in S_Δ.*

For arbitrary Δ, $SL_2(\mathbb{Z})/S_\Delta :=$ the set of orbits can be made into a group. This group is isomorphic to "ideal class group" of $\mathbb{Q}_{\sqrt{\Delta}} = \{a + b\sqrt{\Delta} \ a, b \in \mathbb{Z}\}$.
Remark: Dirichilet's Theorem: if $p > 3$ is a prime and $p = 3 \mod 4$, then

$$h(-p) = -\frac{1}{p} \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) n.$$

Remark: $h(\Delta) = 1$ for $\Delta < 0$ happens 9 times, $-1, -2, -3, -7, -11, -19, -43, -67, -163$. For $\Delta > 0$, there is a conjecture that this happens for infinitely many Δ.

Previously, we have shown that odd prime p is represented by f iff $\left(\frac{\Delta}{p}\right) = 1$. If two forms in S_Δ are equivalent, then take the same values. So iff $h(\Delta) = 1$, and $\left(\frac{\Delta}{p}\right) = 1$, then any form in S_Δ will represent p. Note $x^2 + ny^2$ is always reduced in S_{-4n}.
When $n = 1$, $\Delta = -4$, $f = x^2 + y^2$ is reduced. Note $h(-4) = 2$, and there are only one positive definite form in S_{-4}. And $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = 1$ iff $p = 2$ or $p = 1 \mod 4$. Then $p = x^2 + y^2$ for some integers, iff $p = 2$ or $p = 1 \mod 4$.
When $n = -5$, then -20 is a QR of p iff $p = 1, 3, 7, 9 \mod 20$. If this is the case, then p is represented by some quadratic form in S_{-20}, but S_{-20} has two positive quadratic forms: $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$.

Theorem 3.7 *We can define an operation on the set of equivalent classes of S_Δ such that if two equivalence class e_1 and e_2 of S_Δ represents integers m_1 and m_2, then $e_1 * e_2$ represents $m_1 m_2$.*

Definition: let $f = (a, b, c)$ and $g = (a', b', c') \in S_\Delta$. Assume $\gcd(a, a', \frac{b+b'}{2}) = 1$, then the composition $f * g$ is $\left(aa', B, \frac{B^2 - \Delta}{4aa'}\right)$, where B is the unique solution to

$$\begin{cases} B = b \mod 2a \\ B = b' \mod 2a' \\ B^2 = \Delta \mod 4aa' \end{cases}$$

Remark:

1. $\Delta = b^2 - 4ac = (b')^2 - 4a'c'$, so b and b' have the same parity, which means $2|b+b'$.

2. Existence of B: The first two congruence gives $4aa' = 2a \cdot 2a' | (B-b)(B-b')$. So $B^2 - (b+b')B + b'b = 0 \mod 4aa'$. Then the third congruence is equivalent to $(\frac{b+b'}{2})B = \frac{bb'+\Delta}{2} \mod 2aa'$. The original equations are equivalent to
$$\begin{cases} a'B = a'b \mod 2aa' \\ AB = ab' \mod 2aa' \\ \frac{b+b'}{2}B = \frac{bb'+\Delta}{2} \mod 2aa' \end{cases}$$
Since $\gcd(a, a', \frac{b+b'}{2}) = 1$, then $1 = pa' + qa + r \cdot \frac{b+b'}{2}$ for some p, q, r. Hence $B = pa'b + qab' + r\frac{bb'+\Delta}{2}$.

3. If $\gcd(a, a', \frac{b+b'}{2}) = 1$ is not satisfied, then we need to find equivalent forms such that the condition holds (This can be done).

Theorem 3.8 *$S_\Delta / SL_2(\mathbb{Z})$ = the set of primitive equivalence classes of S_Δ, is a group with respect to the composition defined above.*

Proof: Well-definedness: Difficult.
Associativity: computationally tedious.
Identity:
$$f_0 = \begin{cases} (1, 1, \frac{1-\Delta}{4}), & \Delta \text{ odd} \\ (1, 0, -\frac{\Delta}{4}), & \Delta \text{ even} \end{cases}.$$
We check that f_0 is the identity, that is given $f \in S_\Delta$, then $f * f_0 = f_0 * f = f$.
Inverse: $(a, b, c)^{-1} = (a, -b, c)$. □

Next we consider how many solutions to $f(x, y) = n$?
E.g. if $p = 1 \mod 4 \Leftrightarrow p = x^2 + y^2$: $(x, y) \to (y, x)$, $(x, y) \to (\pm x, \pm y)$, hence there are eight solutions.
$\Delta > 0$: e.g. $x^2 - dy^2 = 1$, $(d > 0)$, then there is infinitely many solutions, the solution set is isomorphic to $\{\pm 1\} \times \mathbb{Z}$.
Or $x^2 - dy^2 = n$, then it has either no solution or infinitely many solutions.

Definition: $\mathcal{O}_\Delta = \{x + y\sqrt{p_\Delta} : x, y \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{d})$, where
$$p_\Delta = \begin{cases} \sqrt{\frac{\Delta}{4}}, & \Delta = 0 \mod 4 \\ \frac{1+\sqrt{\Delta}}{2}, & \Delta = 1 \mod 4 \end{cases}$$

And define $M_F = \{xa + y(b + \sqrt{\Delta}) : x, y \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{d})$.
Then $\mathcal{O}_\Delta \curvearrowright M_f$: $(u + vp_\Delta) \cdot (xa + y\frac{b+\sqrt{\Delta}}{2}) = x'a + y'\frac{b+\sqrt{\Delta}}{2}$.

Proposition 3.9 *If $\Delta > 0$ for a binary quadratic form $f(x, y)$, then*

1. *There is a bijection $\psi : \{(x, y) \in \mathbb{Z}^2 : f(x, y) = n\} \leftrightarrow \{\gamma \in M_f : N(\gamma) = an\}$, $(x, y) \mapsto ax + y\frac{b+\sqrt{\Delta}}{2}$, where $N(a + d\sqrt{b}) = \sqrt{a^2 - db^2}$.*

2. *$\mathcal{O}^x_{\Delta,1}$ = norm 1 units of Q_Δ = solutions of Pell's Equation. $\mathcal{O}^x_{\Delta,1} \curvearrowright$ the solution set of $f(x,y) = n$ by multiplication. Since $\mathcal{O}^x_{\Delta,1}$ is infinite, then the solution set $f(x,y) = n$ is either empty or infinite.*

3. *The number of orbits of $\mathcal{O}^x_{\Delta,1}$ acting on the solution set of $f(x,y) = n$ is finite and we can give explicit description of representatives in each orbit (in terms of bounds on $|y|$).*

If $\Delta < 0$: then by completing the square, $f(x,y) = n$ can only have finitely many solutions.

Proposition 3.10 *f properly represents n if and only if $f \sim (n, b, c)$.*

If this is the case, then $b^2 = \Delta \mod 4n$ and b can made such that $0 \leq b < 2n$.
Let $\mathcal{G}_f(n)$ = the set of all such $g = (n, b, c)$. Then a proper representation of n gives an element in $\mathcal{G}_f(n)$. If $A \cdot f = f$, then this gives a different representation of n by f.
Upshot: proper representations of n by f is in bijection with $|\mathcal{G}_f(n)||Aut(f)|$, where $Aut(f) = \{A \in SL_2(\mathbb{Z}) : A \cdot f = f\}$.
If $\Delta < 0$, then

$$|Aut(f)| = \begin{cases} 6, & a = b = c \\ 4, & a = c, b = 0 \\ 2, & \text{otherwise} \end{cases}.$$

To calculate $|Aut(f)|$, we note if $f \sim g$, then $Aut(f) \cong Aut(g)$, so $|Aut(f)| = |Aut(g)|$. So we only need to consider reduced form g.

If we denote $r_f(n) = \mathcal{G}_f(n)$, then

$$r_\Delta(n) = \sum_{f \in S_\Delta \text{ reduced}} r_f(n) = \#\{b \in \mathbb{Z} : b^2 = \Delta \mod 4n,\ 0 \leq b < 2n\}.$$

Class number formula: $d < -4$, with some conditions, then

$$h = \frac{\sqrt{-d}}{\pi} L(1, \chi_d),$$

where

$$\chi_d(n) = \left(\frac{d}{n}\right)$$

, where $(\frac{\cdot}{\cdot})$ is the generalization of the Jacobi symbol:

$$\left(\frac{a}{2}\right) = \begin{cases} 1, & \pm 3 \mod 8 \\ -1, & \pm 1 \mod 8 \\ 0 & 2|a \end{cases}.$$

Theorem 3.11 *If $\Delta < 0$, with some conditions then*

$$r_\Delta(n) = \begin{cases} 0 & \text{if } p^2|n \text{ for some prime factor } p \text{ of } \Delta \\ \prod\limits_{p|n,(p,d)=1} (1+\chi_d(p)), & \text{othwerise.} \end{cases}.$$