PMATH 340: Elementary Number Theory

Felix Zhou*

Winter 2019
University of Waterloo

*from Michael Rubinstein's lectures

Contents

Introduction

From the University of Waterloo's website: an elementary approach to the theory of numbers; the Euclidean algorithm, congruence equations, multiplicative functions, solutions to Diophantine equations, continued fractions, and rational approximations to real numbers.

1 Primes

1.1 Divisibility

Definition 1.1.1
let $d, n \in \mathbb{Z}$
If $d|n$, then we say d divides n ,or n is a multiple of d if there is some $m \in \mathbb{Z}$, $n = md$.

Proposition 1.1.1

1. $a|b, b|c \implies a|c$
2. $a|b, a|c \implies a|bx + cy \quad \forall x, y \in \mathbb{Z}$
3. $a|b, b|a \implies a = \pm b$
4. $a|b, b \neq 0 \implies |a| \leq |b|$

Proof
Trivial

1.2 Prime Numbers

Definition 1.2.1 (Prime)
$p \in \mathbb{Z}^+$ is prime if and only if $a|p \implies |a| \in \{1, p\}$

Definition 1.2.2 (Composite)
any integers that are not primes (include negative integers!)

Lemma 1.2.1
for $n \in \mathbb{Z}^+$, there is some prime p that divides n.

Proof
induction

Lemma 1.2.2
$n \in \mathbb{Z}^+$ is either prime or a product of primes.

Proof
induction

Theorem 1.2.3
There are an infinite number of primes

Proof
Suppose that there are finite primes p_i
Then consider $1 + \prod p_i$, it must be prime!
Else there some prime which divides it, meaning that prime would divide 1 as well! Contradiction

1.3 Greatest Common Divisors and Euclid's Algorithm

Definition 1.3.1 (Greatest Common Divisor)
$\gcd(a, b), a, b \in \mathbb{Z}$ is literally its name above
Note $\gcd(0, a) = a$ for every non-zero integer a.
Note $\gcd(0, 0)$ is not defined but most things work out if we define that to be 0.

Theorem 1.3.1 (Euclidean Algorithm)
$|a| \geq |b| \in \mathbb{Z}$, then $\gcd(a, 0) = a \wedge \gcd(a, b) = \gcd(a \pmod b, b)$

Proof
The proof hinges on the fact that and common divisor of integers a, b will divide the linear combinations of a, b.

Theorem 1.3.2 (Division Algorithm)
For $0 \neq |a| < |b|$, there are unique integers r, q such $b = qa + r$ with $0 \leq r < |a|$

Corollary 1.3.2.1
Let $a, b \in \mathbb{Z}$, Then there exists $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

Proof
By Euclidean Algorithm with Back Substitution

1.4 Unique Factorization

Lemma 1.4.1
$a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Proof
since $\gcd(a, b) = 1$, $1 = ax + by$ for some integers x, y.

So $c = cax + cby$.
Now, we have both $a|cax$ and $a|cby$, the second by assumption.
So it must be true that a divides their linear combination ie $a|c$.

Lemma 1.4.2
If a prime q divides a product of primes $\prod p_i$. Then it is equivalent to one of the primes.

Proof
By previous lemma

Theorem 1.4.3 (Fundamental Theorem of Arithmetic)
Every integer $n > 1$ is either prime or can be uniquely expressed as a product of primes, up to permutation.

Proof (contradiction)
Let n be smallest number with no unique factorization.
divide by a common prime, which is possible by previous lemma.
We have a smaller non-unique factorization which is a contradiction.

1.5 Applications of Unique Factorization

Theorem 1.5.1 (Pythagoras)
$\sqrt{2}$ is irrational

Proof
Suppose it is not. Express as a fraction $\sqrt{2} = \frac{a}{b}$.
So $2b^2 = a^2$
This clearly contradicts unique factorization as number of twos differ on both sides.
Note that the proof may be adapted to a variety of cases.

Theorem 1.5.2 (Euler's Proof of Infinitude of Primes)
Assuming unique factorization, we have the identity

$$\sum_{n=1}^{\infty} n^{-s} = \sum_{p} \left(1 + p^{-s} + p^{2-s} + \dots\right) = \sum_{p} \left(1 - p^{-s}\right)^{-1}$$

Let $s \to 1^+$, The LHS diverges but RHS is bounded if there are only finitely many primes which is a contradiction.

1.6 Divisors

Proposition 1.6.1
Let $n \in \mathbb{Z}^+$. Write $n = \prod p_i^{\alpha_i}$
define $d(n)$ to be the number of divisors of n.
We have

$$d(n) = \prod (\alpha_i + 1)$$

Proof
By inspection

Proposition 1.6.2
Let $n \in \mathbb{Z}^+$. Write $n = \prod p_i^{\alpha_i}$
define $\sigma(n)$ to be the sum of divisors of n.
We have

$$\sigma(n) = \prod \left(1 + p_i^1 + p_i^2 + \cdots + p_i^{\alpha_i}\right)$$

Proof
By inspection

Proposition 1.6.3
If $m, n \in \mathbb{Z}^+$, then $\sigma(mn) = \sigma(m)\sigma(n)$
We say such a function is **multiplicative**.

Proof
By inspection

1.7 Perfect Numbers

Definition 1.7.1
A Perfect Number is an integer $n \in \mathbb{Z}^+$ that is equal to the sum of its proper divisors (or two times its divisors).
So $\sigma(n) = 2n$.

Theorem 1.7.1
Let p be a prime of the form $p = \sum_{i=0}^{q-1} 2^i$.
Then $n = 2^{q-1}p$ is perfect.

Proof
Note that p is odd.
So $n = 2^{q-1}p$ has two distinct primes appearing in its prime factorization (2 and p).

So $\sigma(n) = (1 + 2 + \cdots + 2^{q-1})(1 + p) = p \cdot 2^q = 2n$

Definition 1.7.2 (Mersenne Prime)
Primes of the form $2^q - 1$ are called Mersenne Primes.
It is an open problem whether there are infinite Mersenne Primes and therefore infinite Perfect Numbers.

Theorem 1.7.2
If $2^q - 1$ is prime then so is q.

Proof
Suppose $q = a, b \in Z^+$ with $a, b > 1$.
Then

$$2^q - 1 = 2^{ab} - 1 = (2^a - 1)\left(1 + 2^a + \cdots + 2^{(b-1)a}\right) = (2^a - 1)\left(\frac{2^{ba} - 1}{2^a - 1}\right)$$

There do not seem to be odd perfect numbers, but no proof exists as of today.

Proposition 1.7.3
If p is an odd prime and $\alpha \in \mathbb{Z}^+$, then p^α is not perfect.

Proof

$$\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1}}{p-1} < p^\alpha \frac{p}{p-1}$$

But $\frac{p}{p-1}$ is at most $\frac{3}{2}$, so $\sigma(p^\alpha) < 2p^\alpha$.

Theorem 1.7.4 (Euler's Converse for Even Perfect Numbers)
$n \in \mathbb{Z}^+$ is a positive even integer and perfect means that n is of the form

$$2^k(2^{k+1} - 1)$$

Where $2^{k+1} - 1$ is a Mersenne prime.

Proof
If n is even, write it as $2^k m$ Where m is odd, $k \in \mathbb{Z}^+$.
Now, n is perfect implies $\sigma(2^k m) = 2^{k+1} m$.
So $2^{k+1} m = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m)$.
Since $\gcd(2^k, 2^{k+1} - 1) = 1$, we must have $2^{k+1} | \sigma(m)$.

Write $\sigma(m) = 2^{k+1}c$ for some $c \in \mathbb{Z}^+$.
Then $2^{k+1}m = (2^{k+1}-1)2^{k+1}c$.
But that indicates that $m = (2^{k+1}-1)c$.
We need to show that $c = 1$ and $2^{k+1}-1$ is prime.
To see the first note that $\sigma(m) = \sigma((2^{k+1}-1)c) = 2^{k+1}c$.
If $c > 1$, then $m = (2^{k+1}-1)c$ has at least three distinct divisors $1, c, (2^{k+1}-1)c$.
But then $\sigma(m) \geq 1 + c + (2^{k+1}-1)c = 2^{k+1}c + 1$ since $2^{k+1}-1 \geq 1$.
However, we showed $\sigma(m) = 2^{k+1}c$! This is clearly a contradiction.
So $c = 1$.
We have $\sigma(2^{k+1}-1) = 2^{k+1}$.
So the only divisors are $2^{k+1}-1$ and 1 which is the definition for $2^{k+1}-1$ being prime, completing the proof.

2 Congruences

2.1 Gauss' Notation

Definition 2.1.1
$a, b, m \in \mathbb{Z}$ with $m \geq 1$, then $a \equiv b \pmod{m}$ if $m|a-b$
Note that this is an equivalence relationship!
We say b is a **residue** of a modulus m.

Theorem 2.1.1
$a = q_1 m + r_1, b = q_2 m + r_2 \implies a \equiv b \pmod{m} \iff r_1 = r_2$

Proof
This is a direct consequence of the definition

Definition 2.1.2
A **Complete set of Residues** for the modulus m is any set of m integers such that any integer is congruent, modulo m to exactly one integer in the set.
ie $\mathbb{Z}_m := \{0, 1, 2, \ldots, m-1\}$
We can compute which element in $\mathbb{Z}_m$ is it congruent to by computing the remainder of a when divided by m, we call this *reducing a modulo m*.

2.2 Congruence Arithmetic

Proposition 2.2.1
for $a \equiv a' \pmod{m} \wedge b \equiv b' \pmod{m}$

1. $a + b \equiv a' + b' \pmod{m}$
2. $ab \equiv a'b' \pmod{m}$

Proof
1. This is trivial
2. $m|a-a' \wedge m|b-b'$ so $mc_1 = a - a', mc_2 = b - b'$
   Then $a = mc_1 + a', b = mc_2 + b'$ so $ab = m^2 c_1 c_2 + a' m c_2 + b' m c_1 + a'b'$
   Rearranging, we see $ab - a'b' = m(mc_1c_2 + a'c_2 + b'c_1)$, so we have $m|ab - a'b'$

2.3 Inverses modulo m

Definition 2.3.1 (invertible)
An integer a is invertible or has an inverse mod m if there is an integer b such that $ab \equiv 1 \pmod{m}$.

Proposition 2.3.1
We can calculate the inverse of a mod m if $\gcd(a, m) = 1$ by Bezout's Lemma.

Proof
Trivial

2.4 Sun Zi's Theorem

Theorem 2.4.1 (Sun Zi / Chinese Remainder Theorem)
Let m_1, m_2 be positive integers with $\gcd(m_1, m_2) = 1$. Let $0 \leq r_1 < m_1 - 1, 0 \leq r_2 < m_2 - 1$.
Then any pair of congruences mod m_1 and mod m_2 with:

$$x \equiv r_1 \pmod{m}_1$$
$$x \equiv r_2 \pmod{m}_2$$

is equivalent to one congruence mod mn, i.e. there exists a unique $0 \leq c \leq mn$ such that $x \equiv c \pmod{mn}$

Proposition 2.4.2
Let b_1, b_2 be congruent to m_1^{-1}, m_2^{-1} respectively mod m_2, m_1. Note the swap.
The integer $m_1 b_1 r_2 + m_2 b_2 r_1$ is one desired solution.

Proof
By inspection

Example 2.4.3
We have $x \equiv 2 \pmod{3}, x \equiv 4 \pmod{5} \iff x \equiv 14 \pmod{15}$
To arrive at this, we set set an equality for one of the two congruences and solve in terms of the other congruence.

2.5 Fermat's Little Theorem

Theorem 2.5.1 (Fermat's Little Theorem)
$a, p \in \mathbb{Z}$ with p prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof
Consider $\{a, 2a, \ldots, (p-1)a\} \pmod p$, we have $a^{p-1}[1 \cdot 2 \cdot \ldots (p-1)] \pmod p$, and each $1, \ldots, (p-1)$ is distinctly congruent to one of $\{1, 2, \ldots, p-1\}$.
If $ai \equiv aj \pmod p$, then $p|(i-j)a$.
But $\gcd(p, a) = 1$, so $p|i-j$, so $i \equiv j \pmod p$.

2.6 Euler's Generalization and his phi-function

Definition 2.6.1 (Euler Phi/Totient Function)
$n \in \mathbb{Z}$
$\phi(n) =$ number of $1 \leq x \leq n$ such that $\gcd(x, n) = 1$

Example 2.6.1
$\phi(7) = 6$
$1, 2, 3, 4, 5, 6$
In general $\phi(p) = p - 1$ for p prime

Example 2.6.2
$\phi(3^2) = p^2 - p$
In general $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for p prime
$(p, 2p, 3p, \ldots, p^{k-1}p)$

Proposition 2.6.3
If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$
So the Euler Phi function is multiplicative

Proof

Theorem 2.6.4 (Euler)
let $m \in \mathbb{Z}^+, a \in \mathbb{Z}, \gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod m$
note that if m is prime, this is simply the specialization to Fermat's Little Theorem

Proof
This is similar to the proof of Fermat's Little Theorem, but restricted to invertible residue classes mod m (ie the ones with inverses mod m).
Let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be the $\phi(m)$ representatives of of the invertible residue classes mod m $(1 \leq r_i \leq m)$.
Consider $\{ar_1, \ldots, ar_{\phi(m)}\}$. They are a permutation of the residue classes mod m.
So $\prod ar_i \equiv \prod r_i \pmod m$.
In other words, $m|(a^{\phi(m)} - 1) \prod r_i$.
But $\gcd(\prod r_i, m) = 1$, thus $m|a^{\phi(m)} - 1$, which by definition implies $a^{\phi(m)} \equiv 1 \pmod m$.

Theorem 2.6.5
If $n \in \mathbb{N}, n = p_1^{\alpha_1} \cdot \dots \dots \cdot p_k^{\alpha_k}$ then

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

2.7 The Divisor Sum

Theorem 2.7.1 (Divisor Sum of ϕ)

$$\sum_{d|n} \phi(d) = \prod_{i=1}^{k}(1 + \phi(p_i) + \cdots + \phi(p_i^{\alpha_i})) = \prod_{i}^{k} p_i^{\alpha_i}$$

Proof
telescoping sum

2.8 Wilson's Theorem

Theorem 2.8.1 (Wilson's Theorem)
p is prime $\iff (p-1)! \equiv -1 \pmod{p}$

Proof
Suppose p is prime.
Each $1 \leq a \leq p-1$ is invertible mod p.
Consider a when a is its own inverse mod p.

$$a^2 \equiv 1 \pmod{p} \implies p|a^2 - 1 \implies p|a-1 \vee p|a+1 \implies a \equiv 1, -1 \pmod{p}$$

Thus, with the exception of ± 1, we know that the other numbers can be arranged into pairs such that the product of each pair is 1, so their product comes out as -1.

For the converse, suppose $(p-1)! \equiv -1 \pmod{p}$ with p being composite.
Then there is some $1 < d \leq p$ such that $d|p$, so $d|(p-1)!$.
But we have $d|p|(p-1)!+1$ by assumption, so

$$d|\left((p-1)!+1\right)-(p-1)! = 1$$

which contradicts $d > 1$.

2.9 Polynomials in mod p

p prime
$\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$
arithmetic in the $\mathbb{F}_p$ mod p.
All non-zero residue classes mod p are invertible.
Can consider polynomials with coefficients in $\mathbb{F}_p$

Theorem 2.9.1 (division algorithm in modular field)
p prime, let $f(x), g(x) \in \mathbb{F}_p[x]$, with $g(x) \neq 0$ in $\mathbb{F}_p[x]$.
$f(x) = q(x)g(x) + r(x)$
with $\deg r(x) < \deg g(x) \vee r(x) = 0$

Proof
we apply highschool division by reducing $f(x)$ repeatedly by a max factor of $g(x)$

Theorem 2.9.2 (Lagrange's Theorem)
p prime, $f(x) \in \mathbb{F}_[x]$ with degree n.
Then there are at most n solutions $x \in \mathbb{F}_[x]_p$ to $f(x) \equiv 0 \pmod{p}$

Proof (by induction)
The result holds for $n = 0$. IF $f(x) \equiv x \neq 0$ in $\mathbb{F}_p$, then there are no solutions to $f(x) \equiv 0 \pmod{p}$
Suppose now inductively, the result holds for degree $k < n$.
If there are no solution for $0 \pmod{p}$, we are done for $f(x)$ with degree $n \geq 1$.
Else say $x_1 \in \mathbb{F}_p$ is a solution to $f(x_1) \equiv 0 \pmod{p}$.
divide $f(x)$ by $(x - x_1)$, $f(x) = q(x)(x - x_1) + r(x)$ with $\deg r(x) < \deg(x - x_1) = 1$, so r is a constant polynomial.
So $f(x) = q(x)(x - x_1) + a$, but $f(x_1) = q(x_1)0 + a \equiv 0 \pmod{p}$ so $a = 0$!
But $\deg q(x) = \deg f(x) - 1$, so we can apply the induction hypothesis to $q(x)$ (has at most $n-1$ solutions)
Note that we used $f(x_2) \equiv 0 \pmod{p} \implies (x_2 - x_1)q(x_2) \equiv 0 \pmod{p}$ Since p is prime and thus must divide either one of the two

Example 2.9.3
$x^3 + x \equiv 0 \pmod 5$ has 3 solutions $x = 0, 2, 3$

Example 2.9.4
$x^3 + x \equiv 0 \pmod 7$ has 1 solutions $x = 0$

Example 2.9.5
$x^7 + 6x + 1 \equiv 0 \pmod 7$ has no solutions since $f(x) \equiv 1 \mod p \quad \forall x \in \mathbb{F}_p$

3 Primitive Roots and Quadratic Reciprocity

3.1 Primitive Roots

Definition 3.1.1 (order)
$m \geq 1, a \in \mathbb{Z}$.
m is said to have (finite) order l mod m if l is the smallest positive integer:

$$a^l \equiv 1 \pmod{m}$$

Note a has finite order if and only if $\gcd(a, m) = 1$.

Proposition 3.1.1
If a has order l mod m, then a^j has order

$$\frac{l}{\gcd(j, l)}$$

Proof
Let $d = \gcd(j, l), l = dl_0, j = dj_0, \gcd(l_0, j_0) = 1$.
What is the smallest integer such that

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

Now, $a^{jk} \equiv 1 \pmod{m}$ so

$$a^{dj_0k} \equiv 1 \pmod{m} \implies l|dj_0k \implies dl_0|dj_0k \implies l_0|j_0k \implies l_0|k$$

So the smallest positive integer k is $k = l_0$.

Definition 3.1.2 (primitive root)
$m \geq 2, a \in \mathbb{Z}$ is said to be a primitive root mod m if a has order $\phi(m)$

Theorem 3.1.2 (Primitive Root Theorem)
The only moduli which have primitive roots are $2, 4, p^\alpha, 2p^\alpha$ where p is prime $\alpha \geq 1$.

Lemma 3.1.3
Let n be an odd modulus. There are primitive roots modulo n if and only if there are primitive roots modulo $2n$

Proof (Lemma)
Note that $\phi(2n) = \phi(n)$ since n is odd.
Then
$$g^k \equiv 1 \pmod{2n} \iff g^k \equiv 1 \pmod{n} \wedge g^k \equiv 1 \pmod{2}$$
for g an (necessarily odd) invertible residue class of $2n$.
So an primitive root mod $2n$ is necessarily an invertible root mod n, and an primitive root h mod n generates a (possibly different) primitive root mod $2n$ $(h + n)$.

Lemma 3.1.4
Suppose that $p|n$ for some odd prime p. If there is a primitive root modulo n, then either $n = p^k$ or $n = 2p^k$ for some integer $k \geq 1$

Proof (Lemma)
Write $n = mp^k$ for some $p \not| m$. We show that if $m \geq 3$ then primitive roots modulo n do not exist.
First not that $\phi(n) = \phi(m)\phi(p^k)$ Where both are even integers since $m \geq 3$.
for any a coprime to n, we have
$$a^{\phi(n)/2} = (a^{\phi(m)})^{\phi(p^k)/2} \equiv 1 \pmod{m}$$
And
$$a^{\phi(n)/2} = (a^{\phi(p^k)})^{\phi(m)/2} \equiv 1 \ (\text{mod } p)^k$$
So by the Chinese Remainder Theorem, $a^{\phi(n)/2} \equiv 1 \pmod{n}$ so we cannot have any primitive roots mod n.

Lemma 3.1.5
Let $n = 2^k$ with $k \geq 3$. Then there are no primitive roots modulo n.

Proof
We proceed by induction so show that $a^{2^{k-2}} \equiv 1 \pmod{2^k}$.
The case $k = 3$ is trivial to check.
For the induction step we note that
$$a^{2^{k-1}} = 1 + m2^{k+1} + m^2 2^{2k} \equiv 1 \pmod{2^{k+1}}$$
for some integer m
So we cannot have primitive roots mod 2^{k+1} either and all of $k \geq 3$ by induction.

Lemma 3.1.6
Let g be a primitive root modulo an odd prime p such that $g^{p-1} \not\equiv 1 \pmod{p^2}$.
Then $g^{\phi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$ for all $k \geq 1$.

Proof
Write $g^{\phi(p^k)} = 1 + mp^k$ for some integer m by Euler's Generalization.
We have $p \not| m$ by supposition.
Since $\phi(p^{k+1}) = p^{k+1} - p^k = \phi(p^k) \times p$, the binomial expansion gives us

$$g^{\phi(p^{k+1})} = (1 + mp^k)^p \equiv 1 + mp^{k+1} \not\equiv 1 \pmod{p^{k+2}}$$

Lemma 3.1.7
Let g be a primitive root modulo an odd prime p. Then either g or $g+p$ is a primitive root modulo p^k for all $k \geq 1$.

Proof
Case I, $g^{p-1} \not\equiv 1 \pmod{p^2}$.
We argue by induction that $ord_{p^k}(g) = \phi(p^k) = p^{k-1}(p-1)$.
The base case clearly holds.
Now, write $m = ord_{p^{k+1}}(g)$.
Since $g^m \equiv 1 \pmod{p}^k$, so $p^{k-1}(p-1)|m$.
We also have $m|\phi(p^{k+1}) = p^k(p-1)$. So either $m = \phi(p^{k+1})$ or $m = p^{k-1}(p-1) = \phi(p^k)$.
But the second is impossible by the second lemma. So we are done.
Case II, $g^{p-1} \equiv 1 \pmod{p^2}$.
We will consider $g + p$.
It is still a primitive root modulo p and by the binomial theorem, satisfies

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 - g^{p-2}p \not\equiv 1 \pmod{p^2}$$

But $p \not| g \implies$ we can use the same argument as above to show that $g + p$ is a always a primitive root mod p^k

Proof (Primitive Roots Theorem, Case: p odd prime)
Let $1 \leq a < p$.
Consider $f_p(p)$ for $l|\phi(p-1)$.
Where $f_p(l)$ denotes the number of invertible residue classes mod p with order l
We claim $f_p(l) = \phi(l), 0$ for all $l|p-1$ and furthermore, $f_p(l) = \phi(l)$. In particular, $f_p(p-1) = \phi(p-1) \geq 1$
Now, to see proof of our first claim. We show that if $f_p(l) = \phi(l)$ if $f_p(l) \neq 0$.
Since $f_p(l) \neq 0$ there is at least one $1 \leq a < p$ of order l mod p.
Let a have order l mod p. So it is a solution to $x^l \equiv 1 \pmod{p}$.
By Legendre's Theorem, the system has at most l solutions mod p.
However, $a^k, 1 \leq k \leq l$ are the l distinct solutions mod p to $x^l \equiv 1 \pmod{p}$ by minimality of orders.
But how many of a^k have order l mod p?
a^j has order $l \iff \gcd(j, l) = 1$.
Among $j = 1, \ldots, l$, $\phi(l)$ has $\gcd(j, l) = 1$.

Given our first claim, then $f_p(l) \leq \phi(l)$ for all $l|p-1$.
Hence
$$p - 1 = \sum_{l|p-1} f_p(l) \leq \sum_{l|p-1} \phi(l) = p - 1$$
Note the RHS uses the divisor sum.
with equality if and only if $f_p(l) = \phi(l)$ for all $l|p-1$.

3.2 Quadratic Residues

Definition 3.2.1
p prime, $a \in \mathbb{Z}, a \not\equiv 0 \pmod{p}$,
a is said to be a quadratic residue mod p if there is some $x \in \mathbb{Z}$ such that
$$x^2 \equiv a \pmod{p}$$
otherwise, a is said to be a quadratic non-residue (or non-quadratic residue).

Note that we may study quadratic residues mod p in terms of a primitive root mod p.

Proposition 3.2.1
p, odd, prime.
We have a quadratic residue mod p if and only if it is an even power of a primitive root mod p.

Proof ($\Longleftarrow$)
Let $a \equiv g^\alpha \pmod{p}$ for g a primitive root.
If $\alpha = 2\alpha_0$, take $x \equiv g^{\alpha_0}$ and we are done.

Proof ($\Longrightarrow$)
Write x, a in terms of g.
Let $a \equiv g^\alpha \pmod{p}$. $x \equiv g^\lambda \pmod{p}$.
Note both $a, x \not\equiv 0 \pmod{p}$ so the above is valid.
Hence
$$x^2 \equiv a \pmod{p} \implies g^{2\lambda} \equiv g^\alpha \pmod{p}$$
By the definition of the order, $p-1|2\lambda - \alpha$
So we have $2|2\lambda - \alpha$.
Now, p is odd so $2|p-1$.
Thus we must have $2|\alpha$!

Corollary 3.2.1.1
p is and odd prime.
The number of quad residues amongst $1 \leq a < p$ in equal to $\frac{p-1}{2}$.

To see this note that half the powers $1 \leq \alpha < p-1$ are even.

Theorem 3.2.2 (Mutiplicative Law for Quadratic Residues / Non-Residues)
If a is a quadratic residue mod p, and b is a quadratic residue mod p.
Then $ab \equiv g^{\alpha+\beta}$ with the power and even number and thus ab is a quadratic residue mod p.
By similar logic the product of two quadratic non-residue is a quandratic residue by parity.
Finally the product of a quadratic residue and quadratic non-residue is a quadratic non-residue.

Definition 3.2.2 (Legendre's Symbol)
p an odd prime. $a \in \mathbb{Z}$.
Define

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a \equiv 0 \pmod{p} \\ 1, & a \text{ is a quadratic residue} \\ -1, & a \text{ is a quadratic non-residue} \end{cases}$$

Proposition 3.2.3 (multiplication law in terms of Legendre Symbols)
For all $a, b \in \mathbb{Z}$.

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

Proof
Trivial

Theorem 3.2.4 (Euler's Criterion)
p an odd prime. $a \in \mathbb{Z}$.

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

Proof
If $a \equiv 0 \pmod{p}$, both sides are 0.
Else, let g be primitive so we can write

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

case I: $\left(\frac{a}{p}\right) = 1 \implies 2|\alpha$

Thus

$$a^{\frac{p-1}{2}} \equiv (g^{2\alpha_0})^{\frac{p-1}{2}} \equiv g^{(p-1)\alpha} \equiv 1 \pmod p$$

case II: $2 \not| \alpha$ So

$$a^{\frac{p-1}{2}} \equiv \left(g^{2\alpha_0+1}\right)^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Theorem 3.2.5 (Gauss' Lemma)
p and odd prime, $a \in \mathbb{Z}$.
Consider the numbers $a, 2a, \ldots, \frac{p-1}{2}a$.
Reduce these $\pmod p$ to lie in the interval $(-\frac{p}{2}, \frac{p}{2})$.
Let ν be the number of reductions that end up negative.
Then

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

Proof
Let

$$\begin{aligned} a &\equiv r_1 \pmod p \\ 2a &\equiv r_2 \pmod p \\ &\ldots \\ \frac{p-1}{2} &\equiv r_{\frac{p-1}{2}} \pmod p \end{aligned}$$

with

$$-\frac{p}{2} < r_i < \frac{p}{2}$$

for all i.
We claim that

$$\{|r_i|\} = \left\{1, \ldots, \frac{p-1}{2}\right\}$$

Indeed, note the bounds of each r_i and none are zero.
Case I: $r_i = r_j$.
$ai \equiv aj \pmod p \implies p|a(i-j)$ so $p|i-j$.
But that means $i - j = 0$ or $i = j$.
Case II: $r_i = -r_j$.
$ai \equiv -aj \pmod p \implies p|(i+j)$
But for $1 \leq i, j \leq \frac{p-1}{2}$.
$0 < i + j \leq p - 1$
There is no $0 < i + j < p$ with $p|i + j$ so $r_i = -r_j$ does not occur.
So

$$a \cdot 2a \cdot \ldots \frac{p-1}{2} a \equiv (-1)^\nu r_1 \cdot r_2 \cdot \ldots r_{\frac{p-1}{2}} \pmod p$$

Next, multiplying by inverses result in

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

But $a^{\frac{p-1}{2}} \equiv (-1)^{\nu} \pmod{p}$ by Euler's Criterion, so

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

Hence

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

Corollary 3.2.5.1

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p = 4k+1 \\ -1, & p = 4k+3 \end{cases}$$

Corollary 3.2.5.2
Note $1 \cdot 2, \ldots \frac{p-1}{2} \cdot 2 = p-1$.
To determine the value of Legendre's symbol, we must count how many even numbers $2x$ satisfy $\frac{p}{2} < 2x < p$ to get ν.
Equivalently, we count the number of integers x in the range

$$\frac{p}{4} < x < \frac{p}{2}$$

Let $p = 8k + r$ for $r = 1, 3, 5, 7$.
So

$$\frac{p}{4} < x < \frac{p}{2} \iff 2k + \frac{r}{4} < x < 4k + \frac{r}{2}$$

Since we are only concerned with the parity of ν, if suffices to claculate the number of integers x with

$$\frac{r}{4} < x < \frac{r}{2}$$

All in all

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & r = 1, 7 \\ -1, & r = 3, 5 \end{cases}$$

Lemma 3.2.6
let a be an integer and p an odd prime with $a \equiv 0 \pmod{p}$.
The value of $\left(\frac{a}{p}\right)$ is determined by $p \pmod{2a}$.

Proof (lemma)
We show the case $a > 0$ and note that the other cases are handled in a similar fashion. Consider $a, 2a, \ldots, \frac{p-1}{2}a$ and reduce them modulo p so they lie in the interval $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$. Note that each $i \cdot a$ lies in some interval

$$\left(0, \frac{p}{2}\right), \left(\frac{p}{2}, \frac{3p}{2}\right), \ldots, \left((b - \frac{1}{2})p, bp\right)$$

with $b = \frac{a}{2}$ since

$$\frac{a}{2}(p-1) < \frac{a}{2}p < \frac{a}{2}(p+1)$$

Note we do not omit any values by taking open intervals as none of them are multiples of p or $\frac{p}{2}$.
Let $i \cdot a \equiv r_i \pmod{p}$ with each $r_i \in \left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$.
Note that the negative r_i lie in the intervals of the form $\left((n - \frac{1}{2})p, np\right)$ for $n \in \mathbb{N} \setminus \{0\}$.
Now, the number of ax with $x \in \mathbb{Z}$ satisfying $(n - \frac{1}{2})p < ax < np$ is the same as the number of x satisfying

$$\left(n - \frac{1}{2}\right)\frac{p}{a} < x < n\frac{p}{a}$$

Let $p \equiv r \pmod{4}a$ so $p = 4ak + r$ with $0 \leq r < 4a$. ν is the number of integers in the intervals:

$$\left(2k + \frac{r}{2a}, 4k + \frac{r}{a}\right), \left(6k + \frac{3r}{2a}, 8k + \frac{2r}{a}\right), \ldots, \left((2c-1)2k + \frac{(2c-1)r}{2a}, 4ck + \frac{cr}{a}\right)$$

with

$$c = \begin{cases} b, & b \in \mathbb{Z} \\ b - \frac{1}{2}, & \text{else} \end{cases}$$

Since we are again only concerned with the parity of ν, we count the integers in the intervals

$$\left(\frac{r}{2a}, \frac{r}{a}\right), \left(\frac{3r}{2a}, \frac{2r}{a}\right), \ldots, \left(\frac{(2c-1)r}{2a}, \frac{cr}{a}\right)$$

So the parity of ν depends only on a, r but not k! In other wirds, we have shown that the legendre's symbol depends only on $p \pmod{4a}$.

Theorem 3.2.7 (Quadratic Reciprocity)
Let p, q be distinct odd primes, then

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

Proof (Quadratic Reciprocity)
Let p, q be as in the statement.
We will show the equivalent statement that

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

If $p \equiv q \pmod 4$ then $4 | p - q$ so $p = 4a + q$ for some integer a.

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)$$

By Fermat's Little Theorem.
Similarly,

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

So the conjecture certainly holds when $p \equiv q \pmod 4$.
Now, if $p \not\equiv q \pmod 4$, then $p \equiv -q \pmod 4$.
So $4 | p + q$ and $p + q = 4a$ for some integer $a > 0$.

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right)$$

Also,

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

Having considered both cases, we conclude the proof.

4 Pythagorean Triple

4.1 Pythagorean Triple

Definition 4.1.1 (Pythagorean Triple)
$x, y, z \in \mathbb{Z}$ solutions to

$$x^2 + y^2 = z^2$$

We say it is primitive if $\gcd(x, y, z) = 1$

Theorem 4.1.1 (Classification of Primitive Pythagorean Triples)
$z, y, z \in \mathbb{Z}$ are primitive Pythagorean Triples if and only if

$$\begin{aligned} z &= \frac{A+B}{2} = U^2 + V^2 \\ x &= \frac{B-A}{2} = V^2 - U^2 \\ y &= \sqrt{AB} = 2UV \end{aligned}$$

with $\gcd(U, V) = 1, V > U > 0$ and U, V having opposite parity.
Note if $x^2 + y^2 = z^2$ and $\gcd(x, y, z) = 1$ then $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$
Recall that if x, y, z is a primitive pythagorean triple, without loss of generality x, y are odd, even respectively.

Proof
Now $x^2 + y^2 = z^2 \implies y^2 = z^2 - x^2 = (z - x)(z + x) = AB$ with A, B both even since x, z are both odd.
Let $d = \gcd(A, B)$ so $2|d$ as both A, B are even. So write $d = 2d_0$
But

$$\begin{aligned} d|A, d|B &\implies d|A + B \wedge d|B - A \\ &\implies d_0|z \wedge d_0|x \end{aligned}$$

However, $\gcd(x, z) = 1 \implies d_0 = 1 \implies d = 2$

$$
\begin{aligned}
A &= 2A_0 \\
B &= 2B_0 \\
y^2 &= AB \\
&= (2A_0)(2B_0) \\
\left(\frac{y}{2}\right)^2 &= A_0B_0 \\
\gcd(A_0, B_0) &= 1 \\
\implies A_0 &= U^2 \\
B_0 &= V^2
\end{aligned}
$$

So $A = 2U^2, B = 2V^2, \gcd(U, V) = 1, 0 < U < V$
And so

$$
\begin{aligned}
z &= \frac{A+B}{2} = U^2 + V^2 \\
x &= \frac{B-A}{2} = V^2 - U^2 \\
y &= \sqrt{AB} = 2UV
\end{aligned}
$$

with $\gcd(U, V) = 1, V > U > 0$ and U, V having opposite parity.
Note the converse if trivial to check for validity of Pythagorean Triple.
let $b = \gcd(x, y, z)$ with x, y, z specified by the above.
So

$$
\begin{aligned}
b|x &\implies b|x + z = zV^2 \\
b|z &\implies b|z - x = 2U^2
\end{aligned}
$$

But $\gcd(2, b) = 1$ since $x = V^2 - U^2$ is odd.
So by Euclid's Proposition, $b|V^2 \wedge b|U^2 \implies b = 1$ as $\gcd(U, V) = 1$
Hence $\gcd(x, y, z) = 1$.

Theorem 4.1.2 (Fermat's Last Theorem)
Let $n \geq 3 \in \mathbb{Z}$.
There are no positive integer solutions x, y, z to

$$x^n + y^n = z^n$$

Proof (General Case)
in 1995 by Andrew Wiles and Richard Taylor

Proof (Fermat's Case, $n = 4$)
We consider
$$x^4 + y^4 = z^2$$
and show that it has no positive integer solution.
We will apply a minimality argument.
Let x, y, z be a solution with z minimal.
We will then show that there is a smaller solution for $x', y', z' < z$, contradicting the minimality of z.
We have $\gcd(x, y) = 1$, otherwise there would be a smaller solution.
Hence x^2, y^2, z is a Primitive Pythagorean triple, as
$$\gcd(x, y) = 1 \implies \gcd(x^2, y^2, z) = 1$$
Thus, by the classification of Primitive Pythagorean triples,
$$\begin{aligned} x^2 &= V^2 - U^2 \\ y^2 &= 2UV \\ z &= U^2 + V^2 \end{aligned}$$
Now, $x^2 \equiv 1 \pmod 2 \implies x^2 \equiv 1 \pmod 4$.
Thus $V^2 \equiv 1 \pmod 4, U^2 \equiv 0 \pmod 4$.
In other words, V is odd, U is even.
But U is even implies that $U = 2r, 0 < r \in \mathbb{Z}$. Substituting into our previous work shows that
$$x^2 = V^2 - 4r^2$$
as well as
$$y^2 = 4rV \implies \left(\frac{y}{2}\right)^2 = rV$$
But $\gcd(r, V) = 1$ as $\gcd(U, V) = 1$ hence $r = t^2, V = S^2$ as rV is a square.
Note that $V > 0 \implies S > 0$.
Substituting again, we see that
$$x^2 = S^4 - 4t^4$$
So $x, 2t^2, S^2$ form a Primitive Pythagorean Triple as
$$\gcd(r, V) = 1 \implies \gcd(S^2, t^2) = 1 \implies \gcd(x, 2t^2, S^2) = 1$$
Now then, there is some U', V' such that
$$\begin{aligned} x &= V'^2 - U'^2 \\ 2t^2 &= 2U'V' \\ S^2 &= U'^2 + V'^2 \end{aligned}$$

with $\gcd(U', V') = 1$, U', V' having opposite parity and $V' > U' > 0$.
But then $t^2 = U'V'$ so

$$U' = X^2, V' = Y^2$$

since $U'V'$ is a square and they are coprime.
Now, substituting, we have

$$X'^4 + Y'^4 = S^2$$

with $U', V' > 0 \implies X, Y, S > 0$.
But then X', Y', s is a solution to our original equation with $S < z$ which contradicts the minimality of z.

5 Sums of Two Squares

Let $A, B, a, b, c, d \in \mathbb{Z}$

$$A = a^2 + b^2$$
$$B = c^2 + d^2$$

Note, by cancellation

$$AB = (ac - bd)^2 + (ad + bc)^2$$

5.1 Complex Numbers

Definition 5.1.1 (Complex Exponential)

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

Where $e^u + v = e^u \cdot e^v$, for all $u, v \in \mathbb{C}$.

Theorem 5.1.1 (Euler's Identity)

$$e^{i\varphi} = \cos\varphi + i\sin\varphi$$

Proof
By definition

$$e^{i\varphi} = 1 + (i\varphi) + \frac{(i\varphi)^2}{2!} + \dots = \left(1 - \frac{\varphi^2}{2!} + \frac{\varphi^4}{4!} + \dots\right) + i\left(\varphi - \frac{\varphi^3}{3!} + \frac{\varphi^5}{5!}\right) = \cos\varphi + i\sin\varphi$$

5.2 Primes that are Sums of Squares

Proposition 5.2.1
Let $p \equiv 3 \pmod 4$ be prime.
Then p is not a sum of squares.

$$\neg\exists a, b \in \mathbb{Z}, p = a^2 + b^2$$

Theorem 5.2.2 (Euler)
If $p \equiv 1 \pmod 4$ is prime, then p is a sum of squares.

$$p = a^2 + b^2, a, b \in \mathbb{Z}$$

with a, b unique up to order and sign.

Proof (existence)
$p \equiv 1 \pmod 4 \implies \exists z \in \mathbb{Z}$ such that

$$z^2 \equiv -1 \pmod p$$

since $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod 4$.
So $p | z^2 + 1$, which by definition means $z^2 + 1 = mp < \frac{p^2}{4} + 1$, which means $m < p$.
Note $m \geq 1$ since $z^2 + 1$ is positive.
We can take $\frac{-p}{2} < z < \frac{p}{2}$, hence $z^2 + 1 < \frac{p^2}{4} + 1$
Now, we show that if $mp = x^2 + y^2$ and if $m > 1$, then there is some $r, x', y' \in \mathbb{Z}$ such that

$$rp = (x')^2 + (y')^2$$

with $1 \leq r < m$.
If so, the repeat until we get

$$p = X^2 + Y^2$$

so $r = 1$.
Assume $m > 1$, otherwise we are done.
Let $\frac{-m}{2} < u, v \leq \frac{m}{2}$ such that

$$u \equiv x \pmod m$$
$$v \equiv y \pmod m$$

Thus $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod m$
So there is some $r \in \mathbb{Z}, u^2 + v^2 = rm$.
if $r = 0$, then $u = v = 0 \implies x \equiv y \equiv 0 \pmod m$.
But $mp = x^2 + y^2$ so if $x \equiv y \equiv 0 \pmod m$

$$m^2 | x^2 + y^2 = mp \implies m | p$$

But $1 \leq m < p$, contradicting primality of p.
Furthermore,

$$r = \frac{u^2 + v^2}{m} \leq \frac{2\left(\frac{m}{2}\right)^2}{m} = \frac{m}{2} < m$$

in other words, $r < m$.

Next,
$$mp \cdot mr = (x^2+y^2)(u^2+v^2) = (xu+yv)^2 + (xv-yu)^2$$
with $xu+yv \equiv x^2+y^2 \equiv 0 \pmod m$ so $m|xu+yv$
Also, $xv-yu \equiv xy-yx \equiv 0 \pmod m$ so $m|xv-yu$.
Thus dividing by m^2, we have
$$rp = \left(\frac{xu+yv}{m}\right)^2 + \left(\frac{xv-yu}{m}\right)^2$$
both being integers.
So we have reached our goal and we are done.

Proof (uniqueness)
Say $p = x^2+y^2 = X^2+Y^2$, where $x, y, X, Y \in Z$.
Then we wish to show $x = \pm X, y = \pm Y$ or $y = \pm X, x = \pm Y$.
We have by assumption
$$p \equiv 1 \pmod 4 \implies \exists h \in \mathbb{Z}, h^2 \equiv -1 \pmod p$$
So
$$p = x^2+y^2 = (x+hy)(x-hy) \pmod p \implies p|(x+hy)(x-hy) \implies p|x+hy \vee p|x-hy$$
as $x^2 - h^2y^2 \equiv x^2+y^2 \pmod p$.
We have $x \equiv \pm hy \pmod p$.
Also
$$p = X^2+Y^2 \equiv (X+hY)(X-hY) \implies \cdots \implies X \equiv \pm hY \pmod p$$
If $p = x^2+y^2$, then $p = (\pm x)^2 + (\pm y)^2$.
So we can assume $x \equiv hy \pmod p$ (if not, we replace b $y \to -y$, etc) and $X \equiv hY \pmod p$.
Thus
$$p^2 = (x^2+y^2)(Y^2+X^2) = (xY-yX)(xX+yY)$$
but $xY - yX \equiv hyY - hyY \equiv 0 \pmod p$ and $xX + yY \equiv h^2yY + yY \equiv 0 \pmod p$.
Thus $\frac{xY-yX}{p}, \frac{xX+yY}{p} \in \mathbb{Z}$.
dividing by p^2 gives
$$1 \equiv (xY-yX)^2 + (xX+yY)^2$$
Therefore either $xY - yX = \pm 0$ and $xX + yY = 1$ or vice versa.
Note $\gcd(x,y) = \gcd(X,Y) = 1$.
But $x|xY$, so $x|yX$ and by Euclide $x|X$.
Likewise, $X|x$ so $x = \pm X$.
Similarly, $y = \pm Y$.
In the other case, $xX = -yY$.
But $x|xX$ so $x|-yY$ and by Euclide $x|Y$.
Likewise $Y|x$.
Repeating gets us $x = \pm Y$.

6 Continued Fractions

6.1 Continued Fractions

Let $\alpha \in \mathbb{R}$, we can write

$$\alpha = q_0 + \alpha'$$

where $q_0 \in \mathbb{Z}, 0 \leq \alpha' < 1$, if $\alpha' > 0$.
Let $\alpha' = \frac{1}{\alpha}$ with $\alpha_1 > 1$.
Hence

$$\alpha = q_0 + \frac{1}{\alpha_1}, \alpha_1 > 1$$

We can repeat on α to get a continued fraction, note this process terminates if and only if α is rational.
This is due to the Euclidean Algorithm.

6.2 General Continued Fraction

Then general, finite continued fraction is in the form

$$q_0 + \frac{1}{q_1 +} \frac{1}{q_2 +} \dots \frac{1}{q_n}$$

Note for $n = 1$, we have

$$q_0 + \frac{1}{q_1} = \frac{q_0 q_1 + 1}{q_1}$$

If $n = 2$ we have

$$\begin{aligned} q_0 + \frac{1}{q_1 +} \frac{1}{q_2} &= q_0 + \frac{q_2}{q_1 q_2 + 1} \\ &= \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1} \end{aligned}$$

Continuing forwards, $n = 3$

$$\begin{aligned} q_0 + \frac{1}{q_1 +} \frac{1}{q_2 +} \frac{1}{3} &= q_0 + \frac{q_2 q_3 + 1}{q_1 q_2 q_3 + q_1 + q_3} \\ &= \frac{q_0 q_1 q_2 q_3 + q_0 q_1 + q_0 q_3 + q_2 q_3 + 1}{q_1 q_2 q_3 + q_1 + q_3} \end{aligned}$$

Definition 6.2.1

$$[q_0, \dots, q_n]$$

denote the numerator of

$$q_0 + \frac{1}{q_1 + \cdots + \frac{1}{q_n}}$$

So inductively, we have that

$$\begin{aligned}
[q_0] &= q_0 \\
[q_0, q_1] &= q_0 q_1 + 1 \\
[q_0, q_1, q_2] &= q_0 q_1 q_2 + q_0 + q_2 \\
[q_0, q_1, q_2, q_3] &= q_0 q_1 q_2 q_3 + q_0 q_1 + q_0 q_3 + q_2 q_3 + 1
\end{aligned}$$

Lemma 6.2.1
The denominator of the above is

$$[q_1, \dots q_n]$$

Proof (Induction)
True for $n = 1$: $[q_0, q_1] = q_0 q_1 + 1$, $[q_1] = q_1$.
Inductively

$$\begin{aligned}
q_0 + \frac{1}{q_1 +} \cdots \frac{1}{q_n} &= q_0 + \frac{1}{\frac{[q_1, \dots, q_n]}{[q_2, \dots, q_n]}} \\
&= \frac{q_0 [q_1, \dots, q_n] + [q_2, \dots, q_n]}{[q_1, \cdots q_n]}
\end{aligned}$$

Theorem 6.2.2 (Euler's Rule)
$[q_0, \dots q_n]$ is equal to a sum of all possible products obtained from $q_0 q_1 \dots q_n$ by omitting no terms, omitting consequetive pairs of terms, two pairs of consequetive terms, and so on.

Proof (Induction)
True for $n = 0, 1$.
$[q_0] = q_0$.
$[q_0, q_1] = \underbrace{q_0 q_1}_{\text{erase nothing}} + \underbrace{1}_{\text{erase first pair of terms}}$
Inductively,

$$[q_0, \ldots, q_n] = \underbrace{q_0[q_1, \ldots, q_n]}_{\text{sum of products with } q_0} + \underbrace{[q_2, \ldots, q_n]}_{\text{sum of products omitting } q_0, q_1}$$

The first term, we never erase $q_0 q_1$ while the second one we definitely do.

Note that

$$[q_0, \ldots, q_n] = [q_n, \ldots, q_0]$$

Corollary 6.2.2.1 (forwards recursion)

$$[q_0, \ldots, q_n] = [q_n, \ldots, q_0] = q_n[q_{n-1}, \ldots, q_0] + [q_{n-2}, \ldots, q_0] = q_n[q_0, \ldots, q_{n-1}] + [q_0, \ldots, q_{n-2}]$$

6.3 Convergents to a Continued Fraction

Definition 6.3.1
Let

$$\frac{A}{B} = q_0 + \frac{1}{q_1 + \ldots} \in \mathbb{Q}$$

be a finite continued fraction.
The fraction that one gets by stopping at q_m rather than q_n, $0 \leq m \leq n$ is called the m-th convergent to $\frac{A}{B}$ and is given by

$$\frac{A_m}{B_m}$$

with $A_m = [q_0, \ldots, q_m]$, $B_m = [q_1, \ldots, q_m]$.

Proposition 6.3.1 (forwards recursion for $q_0, \ldots, q_m$)

$$A_m = q_m A_{m-1} + A_{m-2}$$

and also

$$B_m = q_m B_{m-1} + B_{m-2}$$

we can take $m \geq 0$ by taking

$$\frac{A_0}{B_0} = \frac{q_0}{1}$$

Theorem 6.3.2

$$A_m B_{m-1} - B_m A_{m-1} = (-1)^{m-1}, m \geq -1$$

Proof (induction)
true for $m = -1$.

$$A_{-1}B_{-2} - B_{-1}A{-2} = 1 = (-1)^{-2}$$

Next, assume the result holds for $m-1$, consider the m case:

$$\begin{aligned} A_m B_{m-1} - B_m A_{m-1} &= (q_m A_{m-1} + A_{m-2})B_{m-1} - (q_m B_{m-1} + B_{m-2})A_{m-1} \\ &= A_{m-2}B_{m-1} - B_{m-2}A_{m-1} \\ &= -(A_{m-1}B_{m-2} - B_{m-1}A_{m-2}) \\ &= (-1)^{m-1} \end{aligned}$$

6.4 Infinite Continued Fractions

$\alpha \in \mathbb{R} \setminus \mathbb{Q}$, the procedure

$$\alpha = q_0 + \frac{1}{\alpha_1}, \alpha_1 > 1$$

repeated produces a continued fraction for α.

$$\alpha = \frac{[q_0, \ldots, \alpha_{n+1}]}{[q_1, \ldots, q_n \alpha_{n+1}]}$$

Forward Recursion gives

$$[q_0, \ldots q_n, \alpha_{n+1}] = \alpha_{n+1}[q_0, \ldots q_n] + [q_0, \ldots q_{n-1}]$$

and

$$[q_1, \ldots, q_n, \alpha_{n+1}] = \alpha_{n+1}[q_1, \ldots, q_n] + [q_1, \ldots, q_{n-1}]$$

As before, we have convergents $\frac{A_m}{B_m}$.

$$\frac{A_0}{B_0} = \frac{q_0}{1}, \frac{A_1}{B_1} = \frac{q_0 q_1 + 1}{q_1}, \ldots$$

where $A_{-2} = 0, B_{-2} = 1, A_{-1} = 1, B_{-1} = 0$.
By our work above

$$\alpha = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}, n \geq -1, \alpha_0 = \alpha$$

Theorem 6.4.1

$$\left|\alpha - \frac{A_n}{B_n}\right| < \frac{1}{B_n B_{n+1}}$$

Proof

$$\begin{aligned}\alpha - \frac{A_n}{B_n} &= \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} - \frac{A_n}{B_n} \\ &= \frac{B_n A_{n-1} - A_n B_{n-1}}{B_n(\alpha_{n+1}B_n + B_{n-1})} \\ &= \frac{(-1)^n}{B_n(\alpha_{n+1}B_n + B_{n-1})}\end{aligned}$$

Note that $\alpha_{n+1} = q_{n+1} + \frac{1}{\alpha_{n+2}}$.
Taking absolute value

$$\begin{aligned}|\alpha - \frac{A_n}{B_n}| &= \frac{1}{B_n(\alpha_{n+1}B_n + B_{n-1})} \\ &< \frac{1}{B_n(q_{n+1}B_n + B_{n-1})} \\ &= \frac{1}{B_n B_{n+1}}\end{aligned}$$

Futhermore,

$$\begin{aligned}B_{n+1}(\alpha_{n+2}B_{n+1} + B_n) &> B_n(\alpha_{n+1}B_n + B_{n-1}) \\ &= B_n\left(B_{n+1} + \frac{B_n}{\alpha_{n+2}}\right)\end{aligned}$$

We need

$$\alpha_{n+2}(B_{n+1})^2 > \frac{B_n^2}{\alpha_{n+2}}$$

which is true as $\alpha_{n+2} > 1, B_{n+1} > B_n$.
So these differences are monotonically decreasing.

Corollary 6.4.1.1
Note that

$$B_0 = 1, B_1 = q_1, B_2 = q_2 q_1 + q_0 > q_1$$

continued, we see

$$B_m = q_m B_{m-1} + B_{m-2} \geq B_{m-1} + B_{m-2} > B_{m-1}$$

So B_m is strictly increasing.
It follows that $\frac{A_n}{B_n} \to \alpha$.

6.5 Purely Periodic Continued Fractions

We can recursively define the continued fraction in terms of itself, and even better with forwards recursion.

$$\alpha = \frac{\alpha A_n + A_{n-1}}{\alpha B_n + B_{n+1}}$$

Definition 6.5.1 (Quadratic Irrational)
$\alpha \in \mathbb{R}$ is a Qudratic Irrational if it is an irrational root of a polynomial

$$ax^2 + bc + c$$

with $a, b, c \in \mathbb{Z}, a \neq 2$.

Definition 6.5.2 (Conjugate)
$\alpha \in \mathbb{R}$ a Quadratic Irrational, then

$$\alpha'$$

is the other root and defined to be the Conjugate

Definition 6.5.3 (Reduced)
α is said to be reduced if $\alpha > 1$ and

$$-1 < \alpha' < 0$$

Theorem 6.5.1 (Galois)
α has a purely periodic continued fraction representation if and only if α is reduced.

Proof ($\implies$)
Say α is purely periodic.

$$\alpha = \frac{\alpha A_n + A_{n-1}}{\alpha B_n + B_{n-1}}$$

So

$$B_n\alpha^2 + \alpha(B_{n-1} - A_n) - A_{n-1} = 0$$

We have

(i) $\alpha > 1$ since $q_0 > 1$, as the first partial quotient appears repeatedly

(ii) α is irrational due to periodicity

Consider

$$\begin{aligned}
\beta &= q_n + \cfrac{1}{q_{n-1}\cfrac{1}{\ddots + \cfrac{1}{q_0 + \beta}}} \\
&= \frac{\beta[q_n, \dots, q_0] + [q_n, \dots, q_1]}{\beta[q_{n-1}, \dots, q_0] + [q_{n-1}, \dots, q_1]} \\
&= \frac{A_n\beta + B_n}{A_{n-1}\beta + B_{n-1}} \\
&\implies \\
A_{n-1}\beta^2 + \beta(B_{n-1} - A_n) - B_n &= 0
\end{aligned}$$

Hence, if α is one solution of

$$B_nX^2 + X(B_{n-1} - A_n) - A_{n-1} = 0$$

then $\frac{-1}{\beta}$ is the other solution.
Note $\beta > 1$ since $q_n > 1$, hence the expression above gives the desired other root, ie α is reduced.

6.6 Application to $\sqrt{N}$

Theorem 6.6.1
Let $N \in \mathbb{Z}^+$ be a positive integer, but not a perfect square.
Then $\sqrt{N}$ is irrational.
Let $q_0 = \lfloor\sqrt{N}\rfloor$ be the integer part of $\sqrt{N}$.
Then $\sqrt{N} + q_0$ is reduced and hence has a purely periodic continued fraction.

Proof
First, note $\sqrt{N} + q_0$ is the root of

$$(x - q_0)^2 - N = x^2 - 2q_0x + q_0^2 - N$$

Furthermore, $\sqrt{N} + q_0$ is irrational.

> Then $\alpha = \sqrt{N} + q_0 > 1$ and
> $$\alpha' = -\sqrt{N} + q_0 < 0$$
> So α is reduced.

Note palindriomic nature.

6.7 Pell's Equation

$N \in \mathbb{Z}+$ not a square.
Find positive $x, y \in \mathbb{Z}^+$ with
$$x^2 - Ny^2 = 1$$
Solutions can be found via continued fractions for $\sqrt{N}$.
$$x - \sqrt{N}y = \frac{1}{x + \sqrt{N}y} \iff \left(\frac{x}{y} - \sqrt{N}\right) = \frac{1}{y(x + \sqrt{N}y)}$$
Note that
$$\frac{1}{y(x + \sqrt{1}y)} < \frac{1}{2y^2\sqrt{N}}$$
this suggests that $\frac{x}{y}$ is a continued fraction approximation to $\sqrt{N}$.
Take advantage of large $2q_0$'s. Indeed, let $\frac{A_n}{B_n}, \frac{A_{n-1}}{B_{n-1}}$ occuring before the $2q_0$ partial quotient.
$$\sqrt{N} = \frac{(\sqrt{N} + q_0)A_n + A_{n-1}}{(\sqrt{N} + q_0)B_n + B_{n-1}}$$
clearing denominator
$$\sqrt{N}\left((\sqrt{N} + q_0)B_n + B_{n-1}\right) = (\sqrt{N} + q_0)A_nA_{n-1}$$
collecting terms
$$NB_n + \sqrt{N}\,(q_0B_n + B_{n-1}) = q_0A_n + A_{n-1} + \sqrt{N}A_n$$
If $a + b\sqrt{N} = c + d\sqrt{N}$ with integer variables, and N is not a square, then $a = c, b = d$ otherwise N is rational.
Hence comparing integer and $\sqrt{N}$ components:
$$NB_n = q_0A_n + A_{n-1} \implies A_{n-1} = NB_n - q_0A_n$$
$$q_0B_n + B_{n-1} = A_n \implies B_{n-1} = A_n - q_0B_n$$
But
$$A_nB_{n-1} - A_{n-1}B_n = (-1)^{n-1}$$

So

$$A_n(A_n - q_0 B_n) - (NB_n - q_0 A_n)B_n = A_n^2 - NB_n^2$$

Thus

$$A_n^2 - NB_n^2 = \begin{cases} 1, & n \equiv 1 \pmod 2 \\ -1, & n \equiv 0 \pmod 2 \end{cases}$$

We can take A_{2n+1}, B_{2n+1} which reverses parity and would guarantee a solution.