3701 Theory of Numbers I Notes

Based on the 2012 spring lectures by Dr I Strouthos

Theory of Numbers

Our basic object of study will be the set of natural numbers
$\mathbb{N} = \{1, 2, \ldots\}$

We will often imagine this as lying in the set of intergers,
$\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$
and we will use the set of rational numbers $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$
directly and indirectly.

We first consider $\mathbb{N} = \{1, 2, 3, \ldots\}$
There are two kinds of basic of operations on $\mathbb{N}$:

Addition: $a, b \in \mathbb{N}$, $a+b$ is the sum of a and b
Some properties: $a+b = b+a$
$a+(b+c) = (a+b)+c$
We can generate $\mathbb{N}$ additively using only the number 1.

Multiplication: Given $a, b \in \mathbb{N}$ we can form the product
$ab = \underbrace{b+b+\ldots+b}_{a \text{ copies of } b}$
Properties: $ab = ba$
$a(bc) = (ab)c$
Multiplicatively, we may generate $\mathbb{N}$ using 1 and prime numbers.

Some questions involving primes

1) How many primes are there? infinitely many

2) can we write down any natural number uniquely as a products of primes? Basically yes.

3) How are the primes spread out? Is there any formula giving us the nth prime.

Many interesting problems arise when we 'suppose' additive and multiplicative ideas.

1) Do there exist consecutive odd numbers that are both prime?
If so how many? Unknown.

2) Can we get every natural number of a sum of primes? Yes.

Famous unsolved problems

- Every even number can be written as the sum of at most two primes (?)
- Every odd number can be written as the sum of at most three primes numbers (?).

We may also combine addition and multiplication in other ways.

How many squares do we need to add to obtain every number? If every natural number can be obtained as a sum of n squares, what is the least n?

Using at most

1 square	2 squares	3 squares	4 squares
1	1	1	1
4	2	2	2
9	4	3	3
16	5	4	4
⋮	8	5	5
	9	6	6
	10	8	7
	13	9	8
	16	10	9
	⋮	⋮	⋮

Chapter 1 : Review of Basic Ideas

Given natural numbers m, n where $n > m$ say, it is always possible to find $q \in \mathbb{N}$ st $n = m + q$.

However it is not always possible to find $q \in \mathbb{N}$ st $n = mq$.
If there exists such a number q, we say that m divides n, or m is a divisor of n and we write $m \mid n$
Otherwise m does not divide n and we write $m \nmid n$
eg. $3 \mid 3$, $3 \mid 6$, $6 \nmid 3$, $5 \nmid 8$, $1 \mid n$ for any n.

Note: If $m \mid n$ then $m \leq n$

Some of the main properties of 'division' are

- If $r \mid n$ then $r \mid kn$ for any $k \in \mathbb{N}$.

Proof: $r \mid n \Leftrightarrow n = ar$ for some $a \in \mathbb{N}$
Then $kn = kar = (ka)r$
so $r \mid kn$.

- If $r \mid m$ and $r \mid n$ then $r \mid m+n$

Proof: $r \mid m \Leftrightarrow m = ar$
$r \mid n \Leftrightarrow n = br$
Then $m + n = ar + br$
$= (a+b)r$
so $r \mid m+n$.

In general if $r \mid m$ and $r \mid n$ then $r \mid am + bn$ for any $a, b \in \mathbb{N}$.

Note: We can extend these ideas and results to the set of intergers $\mathbb{Z}$.

In for two numbers m, n ($n \geq m$ say) it is not true that $m \mid n$, we can try to 'approximate' division
This leads to Euclidean Algorithm

Proposition:

Suppose that $m, n \in \mathbb{N}$ and that $n \geq m$. Then there exists natural numbers q and r such that $n = qm + r$ for $0 \leq r \leq m-1$ (the numbers q and r are unique in this case).

'Proof': Subtract as many copies of m from n as possible.

By repeatedly using the proposition we will always arrive at a computation with zero remainder

$n = q_1 m + r_1$

$m = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

$\vdots$

$r_k = q_k r_{k+1} + 0$

eg. $n = 38 \quad m = 7$

$38 = 5 \cdot 7 + 3$

$7 = 2 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$.

This process must terminate with zero remainder, after a finite number of steps, since the remainders are getting strictly smaller and smaller.

$m > r_1 > r_2 > r_3 > \dots > 0$.

eg. $n = 38 \quad m = 8$

$38 = 4 \cdot 8 + 6$

$8 = 1 \cdot 6 + 2$

$6 = 3 \cdot 2 + 0$

Crucially the final non-zero remainder in the process divides both of the original numbers. In fact, it is the greatest number that divides them both.

Definition:

A natural number d is the greatest common divisor of numbers m and n if:

- d is a common divisor of m and n ie $d|m$ and $d|n$
- For any common divisor r, of m and n, r divides d ie $r|m, r|n \Rightarrow r|d$

In such a case we may write $d = \gcd(m, n)$.

In general the greatest common divisor exist and we can find

it using the Euclidean algorithm.
Let us work back up the algorithm

$n = q_1 m + r_1$

$m = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

$\vdots$

$r_{k-2} = q_k r_{k-1} + r_k$

$r_{k-1} = q_{k+1} r_k + 0$

Then since $r_{k-1} = q_{k+1} r_k$, $r_k | r_{k-1}$

$r_{k-2} = q_k r_{k-1} + r_k$ $\quad r_k | r_{k-2}$

~~ie In fact by substituting through the algorithm, we can ex~~

ie r_k is a common ~~factor~~ divisor of n and m.
In fact by substituting through the algorithm, we can express r_k as a combination of m, n
There are intergers a, b such that $r_k = am + bn$

eg. ~~7/2/4~~ $7 = 2 \cdot 3 + 1$

$1 = 7 - 2 \cdot 3$

$1 = 7 - 2(38 \cdot 5 \cdot 7)$

$1 = 7 - 2 \cdot 38 + 10 \cdot 7$

$1 = 11 \cdot 7 - 2 \cdot 38$

In fact r_k is the greatest common divisor of m, n : $r_k = \gcd(m, n)$
Let us show that if r is any other common divisor of m, n, then x must divide r_k.
$r | m$ so $r | am$. Also $r | n$ so $r | bn$
Therefore $r | am + bn$ ie $r | r_k$
So $r_k = \gcd(m, n)$

Note: If there is no non-zero ~~dv~~ remainder in the Euclidean algorithm then $\gcd(m, n) = m$

$n = q_1 m + 0$

eg. $\gcd(12, 4) = 4$ $\quad 12 = 2 \cdot 4 + 0$

The relationship between the Euclidean algorithm and the greatest common divisor is a key idea that may be used to factorise numbers (into primes)

Definition:

A prime number is a natural number greater than 1, whose only divisors are 1 and itself.

Note: This means that if p is a prime and n is any natural numbers then $\gcd(p,n)=1$ or $\gcd(p,n)=p$.

In general if $\gcd(m,n)=1$, then we say that m and are coprime. (In this case we can find $a,b \in \mathbb{Z}$ st $am+bn=1$).
Prime numbers have a crucial property.

Proposition:

If $m,n \in \mathbb{N}$ and p is a prime number the $p|mn \Rightarrow p|m$ or $p|n$ (or both)
(Note: the opposite direction is satisfied by all natural numbers, not just primes)

Proof: Suppose $p|mn$. If p also divides m, we are done
If p does not divide m, let us show that p divides n
Well $\gcd(p,m)=1$ (it cannot be p, since $p \nmid m$ and it has to be 1 or p)
So using an earlier idea, we can find intergers a,b such that
$1=ap+bm$
Multiply through by n: $n=apn+bmn$
But $p|apn$ and $p|bmn$ (since $p|mn$), so $p|apn+bmn$
ie $p|n$ $\square$.

Using this proposition we can factorise any number as a product of primes, essentially uniquely.
Start with a number n — either n is prime
or $n=a_1a_2$
Look at each a_1,a_2: either what we have is prime or it can be factorised further.
Carry on further. This process will end with only primes being present.

Let us show the uniqueness of a factorisation defined as above
Suppose that we have two different factorisations, of a number

into primes: $p_1 \dots p_r = q_1 \dots q_m$ (with possible repetitions)

Consider p_1: $p_1 | p_1 \dots p_r$ so $p_1 | q_1 \dots q_m$

Using the earlier proposition $p_1 | q_j$ for some q_j

The only divisors of q_j are 1 and q_j (it cannot be 1) so $p_1 = q_j$

Similarly each p_i is one of the q_j's

q_j is one of the p_i's

So the factorisations are essentially ~~unique~~ the same, there is a unique prime factorisation, upto reordering

The existance and uniqueness of a prime factorisation for any natural number greater than 1 is the Fundemental Theorem of Arithmetic

We may use this theorem to show that there are infinitely many primes

Let's show that there is a prime number greater than any given prime number.

Consider a prime number p. Multiply all the primes upto and including p and add 1, ie consider $2 \cdot 3 \cdot 5 \cdots p + 1$

This number has no prime factors upto and including p, so its prime factors must be larger than p, ie there is prime larger than p.

This works for any p.

Lets multiply all the primes up to p (with an extra 2) and subtract 1

$2 \cdot 2 \cdot 3 \cdot 5 \cdots p - 1$

This number is of the form $4n - 1$

ie of the form $4(n-1) + 3$ ...

For some arithmetic progressions of numbers like $4n+3$, $6n+5$ we can relatively easily prove that they contain infinitely many primes

In fact any sensibly defined arithmetic sequences contains infintely many primes.

Dirichlet's Theorem:

The sequence $an+b$ contains infinitely many primes, if a, b coprime

In fact it is also true that within the primes, we can find arithmetic progressions

Green-Tao Theorem:

Within the prime numbers we can find a finite sequence of primes in an arithmetic progression, for any number of primes.

Some remarks regarding the Euclidean algorithm and prime factorisation:

We can find certain sets of numbers where 'addition' and 'multiplication' are defined, and where there are 'primes', but where there is no unique factorisation into primes

eg. consider $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a,b \in \mathbb{Z}\}$

We can add and multiply 'numbers' in $\mathbb{Z}[\sqrt{-5}]$ and even find 'numbers' that do not properly factorise further within $\mathbb{Z}[\sqrt{-5}]$

For example $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are 'primes' in $\mathbb{Z}[\sqrt{-5}]$

However $2 \cdot 3 = 6$, $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$

So 6 can not be uniquely factorised into 'primes' in $\mathbb{Z}[\sqrt{-5}]$.

Searching for unique factorisation within 'systems of numbers' like $\mathbb{Z}[\sqrt{-5}]$ lead to concept of ideal numbers (Kummer) and later on the concept of an ideal (Dedekind)

We can specialise the proof that there infinitely many primes to subsets of the prime numbers that satisfy a common property:

eg. Consider numbers of the form $4k+3$ (for $k \in \mathbb{N}$).

Key property: For each $k \in \mathbb{N}$, $4k+3$ is an odd number. So it has odd prime factors.

Any such factor (in fact any ~~such~~ odd number) has one of the forms $4k+1$, $4k+3$.

$(4k+1)(4k+1) = 16k^2+8k+1 = 4(4k^2+2k)+1$ of the form $4m+1$

$(4k+3)(4k+1) = 16k^2+16k+3 = 4(4k^2+4k)+3$ $4m+3$

$(4k+1)(4k+3) =$ "

$(4k+3)(4k+3) = 16k^2+24k+9 = 4(4k^2+6k+2)+1$ $4m+1$

So a number of the form $4m+3$ must have a divisor of the form $4k+3$

Then we can show;

Proposition:

There are infinitely many primes of the form $4k+3$

Proof: Suppose that $3, 7, 11, \dots, p$ are all the prime numbers of the form $4k+3$, $(k \geq 0)$

Consider $N = 4 \cdot 3 \cdot 7 \cdot 11 \cdots p - 1$

Then N is of the form $4k+3$ (in fact $N = 4((3 \cdot 7 \cdot 11 \cdots p) - 1) + 3$)

None of the primes $3, 7, 11 \cdots p$ divides N.

But N must have a prime factor of the form $4k+3$.

So there must be a prime number of the form $4k+3$ that is greater than p.

Perhaps this has revealed a pattern in primes: "there are infinitely many of the form $4k+3$, but only finitely many of the form $4k+1$"

This does not hold!

In fact there are also infinitely many primes of the form $4k+1$ even though we cannot prove it in the same way as $4k+3$.

In general: If a, b are coprime natural numbers, then there are infinitely many prime numbers of the form $ak+b$ $(k \in \mathbb{N})$

(Dirichlet's Theorem)

Above we considered arithmetic sequences of natural numbers and to try to find prime numbers.

We can also find 'arithmetic sequence' patterns within the primes.

eg. 2 prime numbers, 2 away from each other: $3, 5$, $5, 7$.

3 primes numbers following an arithmetic sequence pattern: $3, 5, 7$

4 prime numbers following an arithmetic sequence pattern: $11, 17, 23, 29$

In general it might not be easy to find examples, but ...

For any k, we can find k prime numbers in arithmetic progression.

Green - Tao Theorem.

~~Informally, solving what is known as the Riemann hypothesis would give us~~

~~understanded at Moebius~~

We may not know of a simple pattern in the prime numbers, but we have a sense of how they are spread out.

On average the proposition of natural numbers that are prime, up to and including a number x is $1/\ln x$. This is an approximate answer.

eg it suggests that there are around 22 primes less than 100, there actually 25.

informally, solving what is known as the Riemann hypothesis would give us a better sense of how this approximation works.

Congruences and modular form.

Basic idea: in the Euclidean process of dividing n by m, $n = qm + r$

Fix m and divide every natural number n by m

In this case, the only possible remainder are $0, 1, \ldots, m-1$

Then, identify numbers that give the same remainder when divided by m, or the same remainder modulo m, or mod m

eg. (we may even suppose $n \in \mathbb{Z}$).

These classes of 'modular numbers' inherit addition and multiplication from $\mathbb{N}$ (or $\mathbb{Z}$)

Notation: we refer to the class (set of numbers) containing n as $n \bmod m$ or $\bar{n}$

eg. $3 \equiv 8 \bmod 5$, $3 \equiv 13 \bmod 5$, $0 \equiv 5 \bmod 5$

or in $\mathbb{Z}_5$ $\bar{3} = \bar{8}$, $\bar{3} = \overline{13}$, $\bar{0} = \bar{5}$

Addition and multiplication are both well defined as operations here:

eg. In $\mathbb{Z}_5$: $\bar{2} = \bar{7}$ $\quad \bar{2} + \bar{4} = \bar{6} = \bar{1}$ $\quad \bar{2} \cdot \bar{4} = \bar{8} = \bar{3}$

$\bar{7} + \bar{4} = \overline{11} = \bar{1}$ $\quad \bar{7} \cdot \bar{4} = \overline{28} = \bar{3}$

In general: For any $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $a \equiv b \bmod m$ if a, b have the same 'Euclidean remainder' when divided by m

ie if $a = qm + r$, $b = q'm + r$

$a \equiv b \bmod m \iff m$ divides $a - b$.

Lets check that addition and multiplication are well defined in general (ii)

Suppose that $a \equiv b \bmod m$ ie $m \mid a-b$

$c \equiv d \bmod m$ ie $m \mid c-d$

Lets show that $a+c \equiv (b+d) \bmod m$ ie $m \mid (a+c)-(b+d)$

But $(a+c)-(b+d) = (a-b)+(c-d)$

From $m \mid a-b$ and $m \mid c-d$, we deduce $m \mid (a+c)-(b+d)$ as required

Lets show that $ab \equiv bd \bmod m$ ie $m \mid ac-bd$

But $ac-bd = ac-bc+bd-bd = (a-b)c+(c-d)b$

From $m \mid a-b$, $m \mid c-d$, we can deduce that $m \mid (a-b)c$, $m \mid (c-d)b$

and so $m \mid (a-b)c+(c-d)b$

So addition and multiplication is well defined in $\mathbb{Z}_n$.

What is the additive structure of numbers modulo m?

Associativity: $\bar{x}+(\bar{y}+\bar{z}) = (\bar{x}+\bar{y})+\bar{z}$

Identity: $\bar{x}+\bar{0} = \bar{0}+\bar{x}$ for any $\bar{x}$

Inverse: $\bar{x}+(\bar{m}-\bar{x}) = 0 \bmod m$ for any $\bar{x}$

So, additively, $\mathbb{Z}_m$ forms a group it is a cyclic group with generator $\bar{1}$.

What is the multiplicative structure of numbers modulo m?

Associativity: $\bar{x}\cdot(\bar{y}\cdot\bar{z}) = (\bar{x}\cdot\bar{y})\cdot\bar{z}$

Identity: $\bar{1}\cdot\bar{x} = \bar{x} = \bar{x}\cdot\bar{1}$ for any $\bar{x}$

Inverse: We do not necessarily have inverses.

eg. Does $\bar{2}$ have inverse in modulo 6?

If α inverse of $\bar{2}$ $\quad 2\alpha = 1 \bmod 6 \Rightarrow 6 \mid 2a-1$

$\Rightarrow 2a-6n = 1$. But $2 \mid 2a-6n = 1$. contradiction.

In general: Consider $\bar{n} \in \mathbb{Z}_m$. $\bar{n}$ has a multiplicative inverse (in $\mathbb{Z}_m$) precisely when n, m are coprime.

Proof: Suppose $\exists$ $\bar{a} \in \mathbb{Z}_m$ st $\bar{n}\bar{a} = \bar{1}$ ie st $na \equiv 1 \bmod m$

Then $na = 1+bm$, ie $an-bm = 1$ (for some $b \in \mathbb{Z}$)

(i) If m, n are coprime, then using Bezout's identity, $\exists$ $a, b \in \mathbb{Z}$ st $an+bm = \gcd(m,n) = 1$

Then $an \equiv 1 \bmod m$

ii) If m, n are not coprime then $GCD(m,n) = d > 1$ and for any $a, b \in \mathbb{Z}$ $d \mid an - bm$.
So it is not possible for $an - bm = 1$ ie. there is no inverse for $\bar{n}$ in $\mathbb{Z}_m$.

(Note: The congruence class of $\bar{0}$ does not have a multiplicative inverse modulo any $m \in \mathbb{N}$ eg. 0 is the same congruence class as m and m is not coprime to m).

Using the above result, and the fact that $GCD(a, p) = 1$ for p, prime and $a \in \{1, 2, \ldots, p-1\}$ we deduce that in mod p every non-zero class has an inverse.

eg. In $\mathbb{Z}_5$ $\bar{1} \cdot \bar{1} = \bar{1}$ $\bar{2} \cdot \bar{3} = \bar{1}$ $\bar{4} \cdot \bar{4} = \bar{1}$

Even for a composite number we can collect the invertible elements together and form a group
Last time we checked that for any m, the set $\mathbb{Z}_m$ was associative wrt to multiplication and there was an identity element, $\bar{1}$

If m is a prime every element in $\mathbb{Z}_m^* = \{1, 2, \ldots, m-1\}$ is invertible
ie $\mathbb{Z}_m^*$ is a group under multiplication.

If m is not prime then the invertible elements form a group.
Lets check that the set of invertible elements, is closed under multiplication
Suppose $\bar{x}, \bar{y}$ are invertible in $\mathbb{Z}_m$
Then $\bar{x} \cdot \bar{y}$ is also invertible with inverse $\overline{y^{-1}} \cdot \overline{x^{-1}}$

In general, it is useful to know the number of numbers less than m, which are coprime to m.
This is Euler's totient function: $\phi : \mathbb{N} \longrightarrow \mathbb{N}$
$m \longmapsto$ number of elements $\{1, 2, \ldots m-1\}$ which are coprime to m.

Examples

m	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(m)$		1	2	2	4	2	6	4	6	4	10	4

Note :
- If p is prime $\phi(p) = p-1$
- If p is prime $\phi(p^2) = p^2 - p$

$$\phi(p^3) = p^3 - p^2$$
$$\phi(p^n) = p^n - p^{n-1}$$

In general ϕ is a multiplicative function, in a certain sense:
$\phi(mn) = \phi(m)\phi(n)$ precisely when m and n are coprime
In one way this allows us to calculate $\phi(m)$ for any m, by seperating and different prime factors.

eg. $\phi(120) = \phi(2^3 \cdot 3 \cdot 5) = \phi(2^3)\phi(3)\phi(5)$
$= (2^3 - 2^2) \cdot 2 \cdot 4$
$= 4 \cdot 2 \cdot 4$
$= 32$.

Note: congruence classes mod m are also known as residues mod m.
$\{a \in \mathbb{N} : 1 \leq a \leq m-1, \ GCD(a,m) = 1$

The size of this set is denoted by $\phi(m)$

Note: This is also the size of the set $\{a \in \mathbb{N} : 1 \leq a \leq m, \ GCD(a,m) = 1\}$.

Then using the following correspondence
For $a \in \mathbb{N}$: $GCD(a,m) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z} : ax + my = 1$
$\Leftrightarrow \exists x \in \mathbb{Z} : ax \equiv 1 \bmod m$
ie a is invertible mod m
$\bar{a}$ is invertible in $\mathbb{Z}_m$.

Then the set of classes mod m corresponds to
$U(\mathbb{Z}_m) = \{\bar{a} \in \mathbb{Z}_m : \bar{a}$ invertible in $\mathbb{Z}_m\}$
This is the set of units mod m, or units of $\mathbb{Z}_m$.
The fact that inverses exist in $U(\mathbb{Z}_m)$ leads to cancellation law mod m :

Proposition :

If $\bar{x}, \bar{y} \in \mathbb{Z}_m$ and $\bar{n} \in U(\mathbb{Z}_m)$, then :

i) $\bar{n}\bar{x} = \bar{n}\bar{y} \Rightarrow x = y$ in $\mathbb{Z}_m$
ii) $\bar{x}\bar{n} = \bar{y}\bar{n} \Rightarrow x = y$ in $\mathbb{Z}_m$.

Proof: i) Since $\bar{n} \in U(\mathbb{Z}_n)$, there is an element $\bar{p} \in U(\mathbb{Z}_n)$ st $\bar{n}\bar{p} = 1 = \bar{p}\bar{n}$. Then if $\bar{n}\bar{x} = \bar{n}\bar{y} \Rightarrow \bar{p}(\bar{n}\bar{x}) = \bar{p}(\bar{n}\bar{y}) \Rightarrow (\bar{p}\bar{n})\bar{x} = (\bar{p}\bar{n})\bar{y}$ $\Rightarrow \bar{x} = \bar{y}$ in $\mathbb{Z}_m$.
ii) Similarly.

Using this cancellation law we may prove the following:

Theorem:

If $\bar{a} \in U(\mathbb{Z}_m)$, then $\bar{a}^{\phi(m)} \equiv \bar{1}$

(This result known as the Fermat-Euler Theorem)

Proof: Let $U(\mathbb{Z}_m) = \{\bar{u}_1, \bar{u}_2, \dots \bar{u}_{\phi(m)}\}$ $\phi(m) = |U(\mathbb{Z}_m)|$
For any $\bar{a} \in U(\mathbb{Z}_m)$, multiply '$U(\mathbb{Z}_m)$ through by a' to obtain $\{\bar{a}\bar{u}_1, \bar{a}\bar{u}_2, \dots, \bar{a}\bar{u}_{\phi(m)}\} = S$
Multiplying a unit by unit leads to a unit.
S contains $\phi(m)$ distinct terms: If $\bar{a}\bar{u}_i = \bar{a}\bar{u}_j$, then by cancellation law $\bar{u}_i = \bar{u}_j$
So, S contains $\phi(m)$ distinct units, ie $S = U(\mathbb{Z}_m)$
Then since $\{\bar{u}_1, \bar{u}_2, \dots, \bar{u}_{\phi(m)}\} = \{\bar{a}\bar{u}_1, \bar{a}\bar{u}_2, \dots \bar{a}\bar{u}_{\phi(m)}\}$. we obtain
$\bar{u}_1 \cdot \bar{u}_2 \cdot \dots \cdot \bar{u}_{\phi(m)} = (\bar{a} \cdot \bar{u}_1)(\bar{a}\bar{u}_2) \cdot \dots \cdot (\bar{a}\bar{u}_{\phi(m)})$ in $\mathbb{Z}_m$
ie $(\bar{u}_1 \cdot \bar{u}_2 \dots \bar{u}_{\phi(m)}) = \bar{a}^{\phi(m)}(\bar{u}_1 \cdot \bar{u}_2 \cdot \dots \cdot \bar{u}_{\phi(m)})$ in $\mathbb{Z}_m$
By cancellation laws $\bar{a}^{\phi(m)} = \bar{1}$ in $\mathbb{Z}_m$.

Example: In $\mathbb{Z}_{12}$, $U(\mathbb{Z}_{12}) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$
$\bar{1}^4 = \bar{1}$, $\bar{5}^4 = \bar{1}$, $\bar{7}^4 = \bar{1}$, $\bar{11}^4 = \bar{1}$

Note: When p is prime, every non-zero congruence class is invertible mod p: $\phi(p) = p-1$
In this special case we obtain:
Fermats Little Theorem: $\bar{a}^{p-1} = 1 \bmod p$ if $\gcd(a,p) = 1$

Note: We have not proved that $U(\mathbb{Z}_m)$ contains elements of order $\phi(m)$

ie. the theorem does not show that there exists $a \in U(\mathbb{Z}_m)$ st

the smallest positive number k satisfying $\bar{a}^k = \bar{1}$ is $\phi(m)$

This may or may not be true.

eg. $U(\mathbb{Z}_{12}) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

$\bar{1}^4 = \bar{1}, \quad \bar{5}^4 = \bar{1}, \quad \bar{7}^4 = \bar{1}, \quad \bar{11}^4 = \bar{1}$

However $\bar{1}^2 = \bar{1}, \ \bar{5}^2 = \bar{1}, \ \bar{7}^2 = \bar{1}, \ \bar{11}^2 = \bar{1}$.

So no element in $U(\mathbb{Z}_{12})$ has order $\phi(12) = 4$.

eg. $U(\mathbb{Z}_5) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

$\bar{1}^4 = \bar{2}^4 = \bar{3}^4 = \bar{4}^4 = \bar{1}$

$\bar{4}^2 = \bar{1}$, $\bar{4}$ has order 2 in $\mathbb{Z}_5$

$\bar{2}^2 = \bar{4}, \quad \bar{2}^3 = \bar{3}, \quad \bar{2}^4 = \bar{1}$

$\bar{3}^2 = \bar{4}, \quad \bar{3}^3 = \bar{2}, \quad \bar{3}^4 = \bar{1}$

So in $\mathbb{Z}_5$ there exist elements of order $\phi(5) = 4$.

$U(\mathbb{Z}_5)$ is a cyclic group

So $U(\mathbb{Z}_5)$ may be written as $\{x, x^2, x^3, x^4\}$ for $\bar{x} = 2$ or $\bar{x} = 3$.

In general: If p is prime : $U(\mathbb{Z}_p)$ is cyclic

ie there does exist an element $x \in U(\mathbb{Z}_p)$ of order $p-1$

Let's study $\phi(m)$ a bit more:

Proposition: p prime, $\phi(p^n) = p^n - p^{n-1}$

Proof: The only prime factor of p^n is p (by the Fundamental Theorem of Arithmetic) so if a number, b say, is not coprime to p^n the must have a common factor of p.

So out of p^n numbers $1, 2, \dots, p^n$ the following p^{n-1} numbers are not coprime to p^n: $p, 2p, 3p, \dots (p^{n-1})p$

So $\phi(p) = p^n - p^{n-1}$

Let us now try to see how we may work out $\phi(m)$ (and the structure of $U(\mathbb{Z}_m)$) for any number m, using our results on primes and prime powers.

Key Idea: Suppose that m, n are coprime numbers and consider the set of all linear combinations:

$$am + bn \quad \text{mod } mn$$

for $0 \le a \le n-1$, $0 \le b \le m-1$
These give us mn numbers and they are all distinct.
ie they give every number modmn.

eg. Set $m=3$, $n=4$
We obtain the following linear combinations

$0 \cdot 3 + 0 \cdot 4 = 0 \equiv 0 \bmod 12$
$0 \cdot 3 + 1 \cdot 4 = 4 \equiv 4 \bmod 12$
$0 \cdot 3 + 2 \cdot 4 = 8 \equiv 8 \bmod 12$
$1 \cdot 3 + 0 \cdot 4 = 3 \equiv 3 \bmod 12$
$1 \cdot 3 + 1 \cdot 4 = 7 \equiv 7 \bmod 12$
$1 \cdot 3 + 2 \cdot 4 = 11 \equiv 11 \bmod 12$
$2 \cdot 3 + 0 \cdot 4 = 6 \equiv 6 \bmod 12$
$2 \cdot 3 + 1 \cdot 4 = 10 \equiv 10 \bmod 12$
$2 \cdot 3 + 2 \cdot 4 = 14 \equiv 2 \bmod 12$
$3 \cdot 3 + 0 \cdot 4 = 9 \equiv 9 \bmod 12$
$3 \cdot 3 + 1 \cdot 4 = 13 \equiv 1 \bmod 12$
$3 \cdot 3 + 2 \cdot 4 = 17 \equiv 5 \bmod 12$.

Theorem:

Suppose that m, n are coprime natural number
Then the following set includes all congruence classes modmn
$\{am + bn \bmod mn : 0 \le a \le n-1,\ 0 \le b \le m-1\}$.

Proof: The set given above contains mn numbers modmn, so it is enough to check that different choices for a, b lead to different elements modmn:
Suppose $am + bn \equiv a'm + b'n \bmod mn$
Then mod m: $bn \equiv b'n \bmod m$ (m, n coprime)
$b \equiv b' \bmod m$
Similarly mod n: $am \equiv a'm \bmod n$
$a \equiv a' \bmod n$
ie $am + bn \equiv a'm + b'n \bmod mn$ precisely when $a \equiv a' \bmod m$
$b \equiv b' \bmod n$.
So the set represents mn distinct congruence classes, modmn
ie it includes (representations of) all congruence classes modmn.

From this we may deduce that units modmn are obtained when we combine units mod$m$ and mod n.

Proposition:

For $0 \le a \le n-1$, $0 \le b \le m-1$, $\gcd(am+bn, mn) = 1 \iff \gcd(a,n)=1$ and $\gcd(b,m)=1$ (m,n coprime.)

Proof: $\gcd(am+bn, mn)=1$ if and only if $\gcd(am+bn, m)=1$ and $\gcd(am+bn, n)=1$
$\iff \gcd(bn, m)=1$ and $\gcd(am, n)=1$
$\iff \gcd(b,m)=1$ and $\gcd(a,n)=1$

Check online proof

Let us think about this result in terms of Euler ϕ-function
If m, n coprime, then we obtain the $\phi(mn)$ units mod mn by taking linear combinations of the $\phi(m)$ units mod m and the $\phi(n)$ units mod n.
So we obtain:

Theorem:

Suppose that m, n are coprimes.
Then $\phi(mn) = \phi(m)\phi(n)$

eg. $\phi(12) = \phi(3)\phi(4)$ note $\phi(12) \neq \phi(6)\phi(2)$.
$= (3-1)(4-2)$
$= 4$

$\phi(200) = \phi(8)\phi(25)$
$= \phi(2^3)\phi(5^2)$
$= (2^3-2^2)(5^2-5^1)$
$= 4 \cdot 20$
$= 80$

The euler-totient function has another special property, which is related to the 'multiplicativity' $\phi(mn) = \phi(m)\phi(n)$ for coprime m, n.
As an example consider 8. It's divisors are 1, 2, 4, 8
~~is written as~~ $\phi(1)+\phi(2)+\phi(4)+\phi(8) = 1+1+2+4 = 8$.
So written ~~concise~~ concisely $\sum_{d \mid 8} \phi(d) = 8$
This works in general for any prime prower

Proposition:

If p, prime then $\sum_{d|p^n} \phi(d) = p^n$ for any natural number n.

Proof: The divisors of p^n are $1, p, p^2, \ldots, p^{n-1}, p^n$

$$\sum_{d|p^n} \phi(d) = \phi(1) + \phi(p) + \ldots + \phi(p^n)$$
$$= \cancel{1} + (\cancel{p} - \cancel{1}) + (p^2 - \cancel{p}) + \ldots + (p^{n-1} - p^{n-2}) + (\cancel{p^n} - \cancel{p^{n-1}}) = p^n$$

Does something similar for composite numbers?

Consider 12. Divisors are $1, 2, 3, 4, 6, 12$

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1+1+2+2+2+4 = 12.$$
$$= \phi(1) + \phi(2) + \phi(3) + \phi(2^2) + \phi(2)\phi(3) + \phi(2^2)\phi(3)$$
$$= \underbrace{(\phi(1) + \phi(2) + \phi(2^2))}_{=4}\underbrace{(\phi(1) + \phi(3))}_{=3} = 12.$$

This holds in general.

Theorem:

For any positive interger m, $\sum_{d|m} \phi(d) = m$

Proof: Consider the prime factorisation of m: $m = p_1^{n_1} \cdots p_k^{n_k}$ for, $p_1, \ldots, p_n$ distinct primes.

Then the divisors of m have the form $p_1^{r_1} \cdots p_k^{r_k}$ $\quad 0 \leq r_i \leq n_i$

For each such divisor $\phi(p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}) = \phi(p_1^{r_1})\phi(p_2^{r_2}) \ldots \phi(p_k^{r_k})$

$$\sum_{d|m} \phi(d) = \sum_{0 \leq r_i \leq n_i} \phi(p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}) = \sum_{0 \leq r_i \leq n_i} \phi(p_1^{r_1}) \ldots \phi(p_k^{r_k})$$
$$= \sum (\phi(1) + \phi(p_1) + \ldots + \phi(p_1)^{n_1}) \cdots (\phi(1) + \phi(p_k) + \ldots + \phi(p_k)^{n_k})$$
$$= p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$$
$$= m$$

So far the ~~tool~~ ~~that~~ tools we have seen, allows us to solve linear equations, mod m.

For example consider the general linear congruence

$ax + b \equiv 0 \bmod m$, $a \not\equiv 0 \bmod m$.

We may rewrite this as $ax \equiv -b \bmod m$.

A congruence of this form may have, zero, one unique or ~~infinitely~~ many solutions

eg. • $3x \equiv 1 \bmod 12$ $10x \equiv 9 \bmod 12$, have no solutions mod 12.
• $5x \equiv 2 \bmod 12$, $7x \equiv 7 \bmod 12$ have a unique solution mod 12.
• $3x \equiv 3 \bmod 12$, $10x \equiv 8 \bmod 12$.
$x = 1, 5, 9 \bmod 12$ $x \equiv 2, 8 \bmod 12$
$(x \equiv 1 \bmod 4)$. $(5x \equiv 4 \bmod 6)$.

In general: The congruence $ax \equiv b \bmod m$ has:
a unique solution if $GCD(a,m) = 1$
has no solutions if $GCD(a,m) > 1$, $GCD(a,m) \nmid b$.
has more than one solution if $GCD(a,m) > 1$, $GCD(a,m) \mid b$.

Further more, our earlier theorem on 'linear combinations' ~~addisis~~ essentially allows us to solve simultaneous linear congruences. From that result, we may deduce the following:

Theorem:

If m, n are coprime, there is ~~an~~ unique congruence class mod mn, x say. satisfying: $x \equiv a \bmod m$, $x \equiv b \bmod n$, for any given a, b.

eg. $x \equiv 2 \bmod 6$, $x \equiv 9 \bmod 23$
$x = 9 + 23k \quad k \in \mathbb{Z}$

$9 + 23k \equiv 2 \bmod 6$
$23 \equiv 2 - 9 \bmod 6$
$5k \equiv 5 \bmod 6$
$k \equiv 1 \bmod 6$

So we may choose $y = 9 + 23 \cdot 1 = 32$
If $x \equiv 32 \bmod 138$, then $x \equiv 2 \bmod 6$, $x \equiv 9 \bmod 23$.

This result can be generalised to:

Chinese Remainder Theorem:

Suppose that $m_1, m_2, \ldots, m_k$ are pairwise coprime natural numbers. Then modulo ~~$m_1m_2\cdots m_k$~~ $m_1 m_2 \cdots m_k$, there is a unique solution, x say, to the following set of congruences:

$x \equiv a_1 \bmod m_1$

$x \equiv a_2 \bmod m_2$ for any $a_1, a_2, \ldots a_k$ relevant congruence classes.

$\vdots$

$x \equiv a_k \bmod m_k$

Quadratic Residues

Suppose that we wish to solve a general quadratic congruence

$ax^2 + bx + c \equiv 0 \bmod m$, where $a \not\equiv 0 \bmod m$.

We will concentrate on the case where m is prime

eg. consider $3x^2 + 2x + 5 \equiv 0 \bmod 7$.

We will not use the ordinary 'quadratic formula', which ~~can~~ involves divison and square roots, but will try to complete the square.

Lets first make the leading coeff 1 by multiplying by 5 ~~mod~~ 7.

$5\cdot 3x^2 + 5\cdot 2x + 5\cdot 5 \equiv 5\cdot 0 \bmod 7$

$x^2 + 3x + 4 \equiv 0 \bmod 7$.

$(x+5)^2 - 25 + 4 \equiv 0 \bmod 7$

$(x+5)^2 - 21 \equiv 0 \bmod 7$

$(x+5)^2 \equiv 0 \bmod 7$.

unique solution $x \equiv -5 \bmod 7$

$x \equiv 2 \bmod 7$.

Example $3x^2 + 4x + 4 \equiv 0 \bmod 7$

Multiply through by 5

$x^2 + 6x + 6 \equiv 0 \bmod 7$

$(x+3)^2 - 9 + 6 \equiv 0 \bmod 7$

$(x+3)^2 - 3 \equiv 0 \bmod 7$

$(x+3)^2 \equiv 3 \bmod 7$

There is no number that squares to $3 \bmod 7$

The quadratic congruence class has no solutions

Example: $3x^2+4x+1 \equiv 0 \bmod 7$

multiply by 5 $\quad x^2+6x+5 \equiv 0 \bmod 7$

$$(x+3)^2-9+5 \equiv 0 \bmod 7$$

$$(x+3)^2 \equiv 4 \bmod 7$$

so $x+3 \equiv 2 \bmod 7$ or $x+3 \equiv 5 \bmod 7$

$\therefore x \equiv 6 \bmod 7$ or $x \equiv 2 \bmod 7$

OR $\quad 3x^2+4x+1 \equiv 0 \bmod 7$

$6x^2+6x+5 \equiv 0 \bmod 7$

$(x+5)(x+1) \equiv 0 \bmod 7$

$x \equiv -5 \bmod 7 \qquad x \equiv -1 \bmod 7$

$x \equiv 2 \bmod 7 \qquad x \equiv 6 \bmod 7.$

As the examples show, a quadratic congruence (mod p) may have 0, 1, or 2 solutions (in terms of congruence classes)

In general, by ~~[illegible]~~ completing the square, we can reduce such congruences to the form

$$z^2 \equiv n \bmod p, \text{ where } z = x + s.$$

So it seems that understanding quadratic equations mod p is equivalent to understanding which numbers can occur as squares mod p.

*A trivial case is when $n=0$: $z^2 \equiv 0 \bmod p \Leftrightarrow z \equiv 0 \bmod p$

Note that in general $ab \equiv 0 \bmod p \Leftrightarrow a \equiv 0 \bmod p$, $b \equiv 0 \bmod p$.

Proof: $ab \equiv 0 \bmod p$ is equivalent to $ab = kp \quad k \in \mathbb{Z}$. $\Leftrightarrow p \mid ab$

$\Leftrightarrow p \mid a$ or $p \mid b$ (shown previously) $\Leftrightarrow a \equiv 0 \bmod p$, $b \equiv 0 \bmod p$.

Apart from $0 \bmod p$, numbers mod p fall into two ~~[illegible]~~ classes:

Definition:

Consider a non-zero congruence class, a, mod p.

- If there exists a congruence class x, st $x^2 \equiv a \bmod p$, then ~~this~~ we say that a is a quadratic residue mod p.
- If the equation $x^2 \equiv a \bmod p$ has no solutions (mod p) then we say that a is a quadratic non residue, mod p.

Eg. Say for example the congruence classes of 1, 2, 4 are quadratic residues mod 7, whereas the congruence classes of, 3, 5, 6 are quadratic nonresidues mod 7.

It seems that half of the non-zero classes mod p $(p \neq 2)$ are residues, while the other half are not.

~~It is easy to see that at most $\frac{p-1}{2}$~~

There are at most $p-1/2$ quadratic residues mod p $(p \neq 2)$ since $a^2 \equiv (-a)^2 \bmod p \equiv (p-a)^2 \bmod p$.
~~$a^2 \equiv (p-a)^2 \bmod p$~~.

Lets confirm that we obtain exactly $p-1/2$ residues.

Proposition:

Suppose that p, odd prime and suppose that $x^2 \equiv y^2 \bmod p$
Then either $x \equiv y \bmod p$ or $x \equiv -y \bmod p$ (iff).

Proof: $x^2 \equiv y^2 \bmod p$
$\iff x^2 - y^2 \equiv 0 \bmod p$
$\iff (x+y)(x-y) \equiv 0 \bmod p$
$\iff x \equiv y \bmod p$ or $x \equiv -y \bmod p$

In general: $x^2 \equiv 0 \bmod p \Rightarrow x \equiv 0 \bmod p$
For $a \not\equiv 0 \bmod p$ $x^2 \equiv a \bmod p$ may have no solutions mod p or exactly two solutions mod p (of the form $x, -x$).
If $x^2 \equiv a \bmod p$, then $(-x)^2 \equiv a \bmod p$
Also $x^2 \equiv y^2 \bmod p \Rightarrow x \equiv y \bmod p$ or $x \equiv -y \bmod p$.

Lets introduce the notation we will use to work with quadratic residues.

Definition:

Consider a prime p (odd) and let a be a natural number
The Legandre symbol (a/p) is defined as follows

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \bmod p \\ +1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is not a quadratic residue mod } p. \end{cases}$$

eg. $p=7$ $\left(\frac{0}{7}\right)=0$ $\left(\frac{1}{7}\right)=1$ $\left(\frac{2}{7}\right)=1$ $\left(\frac{3}{7}\right)=-1$ $\left(\frac{4}{7}\right)=1$ $\left(\frac{5}{7}\right)=-1$

$\left(\frac{6}{7}\right)=-1$

$\left(\frac{18}{7}\right)=\left(\frac{4}{7}\right)=1.$

Let us try to describe some ways that may be used to determine whether or not numbers are residues

Consider residues mod 7 : residues 1, 2, 4, nonresidues 3, 5, 6

Note that $a^6 \equiv 1 \bmod 7$ for any $a \not\equiv 0 \bmod 7$.

ie $a^3 \equiv 1 \bmod 7$ or $a^3 \equiv -1 \bmod 7$. for any $a \not\equiv 0 \bmod \cancel{p}$.

$1^3 \equiv 1 \bmod 7$ $\quad$ $4^3 \equiv 1 \bmod 7$

$2^3 \equiv 1 \bmod 7$ $\quad$ $5^3 \equiv (-2)^3 \equiv -1 \bmod 7$

$3^3 \equiv -1 \bmod 7$ $\quad$ $6^3 \equiv (-1)^3 \equiv -1 \bmod 7$

So if a ~~residue~~ is a residue mod 7 then $a^3 \equiv 1 \bmod 7$ and if a is not a residue mod 7 then $a^3 \equiv -1 \bmod 7$.

ie $\left(\frac{a}{7}\right) = a^3 \bmod 7$.

In general the following holds : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Wilson's Theorem :

For any prime p : $(p-1)! \equiv -1 \bmod p$.

Proof : mod p, each congruence class has an inverse. So for each non zero congruence class x, there exists a non-zero congruence class y such that $xy \equiv 1 \bmod p$.

Let's identify which classes are their own inverses :

$x \cdot x \equiv 1 \bmod p$ iff $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p \equiv p-1 \bmod p$.

Now consider $(p-1)! \bmod p = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \bmod p$

If x is any class not congruent to 1 or $p-1 \bmod p$, its inverse will also be in this product, so that they will

'cancel out'
ie we may rearrange this product so that all classes except 1, -1 mod p, 'cancel out' in pairs

$1\cdot 2\cdot 3\cdots(p-1) \overset{\text{mod } p}{=} 1\cdot(\ldots)\cdot(\ldots)\cdots(p-1) \bmod p$

$= 1(p-1) \bmod p$

So $(p-1)! \equiv -1 \bmod p$ QED.

eg. $p=7$: $6! \equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 \bmod 7$

$\equiv 1\cdot(2\cdot 4)\cdot(3\cdot 5)\cdot 6 \bmod 7$

$\equiv 1\cdot 1\cdot 1\cdot 6 \bmod 7$

$\equiv -1 \bmod 7.$

Theorem : (Euler's Criterion) :

Let p be a prime. Then $(a/p) = a^{\frac{p-1}{2}} \bmod p$.

Proof : if $a \equiv 0 \bmod p$, then $(a/p) = 0$ by definition and $a^{\frac{p-1}{2}} = 0^{\frac{p-1}{2}} \equiv 0 \bmod p$, so the result holds.
Mod p, each non-zero congruence class is invertible
So for each non-zero congruence class x, there exists a non zero congruence class y such that

$xy \equiv a \bmod p$ (choose $y \equiv x^{-1} a \bmod p$) for $a \not\equiv 0 \bmod p$.

Let's try to describe any class x satisfying $x^2 \equiv a \bmod p$
There are two cases to consider :
Case 1 : The class a is a residue mod p, so there does exists an x satisfying $x^2 \equiv a \bmod p$
In fact the equation $x^2 \equiv a \bmod p$ has two solutions, x and $-x \equiv p - x \bmod p$, ~~say~~.
In this case for every non-zero congruence class b, $b \not\equiv x \bmod p$, $b \not\equiv -x \bmod p$, we can find a different congruence class c say, such that $(b\cdot c) \equiv a \bmod p$.
We may then rearrange the product $(p-1)!$ to 'cancel out' such classes :

$1\cdot 2\cdot 3\cdots(p-1) \equiv x\cdot -x\cdot a\cdot a\cdots\cdot a \bmod p$

$\equiv -x^2\, a^{p-3/2} \bmod p$

$\equiv -a\cdot a^{\frac{p-3}{2}} \bmod p$

$\equiv -a^{\frac{p-1}{2}} \bmod p$

But $(p-1)! \equiv -1 \bmod p$ so if a is a quadratic residue mod p.
$a^{\frac{p-1}{2}} \equiv 1 \bmod p$
So $(a/p) \equiv a^{\frac{p-1}{2}} \bmod p$

Case 2 a is not a quadratic residue mod p
so no congruence class $x \bmod p$ satisfies $x^2 \equiv a \bmod p$.
But for each $x \bmod p$, there does exist a class $y \bmod p$ such that $xy \equiv a \bmod p$, choose $y \equiv x^{-1} a \bmod p$.
Therefore for each class $x \bmod p$ there is a different class $y \bmod p$ such that $xy \equiv a \bmod p$
Then consider the product $(p-1)! \bmod p$: $1 \cdot 2 \cdot \ldots (p-2) \cdot (p-1) \bmod p$
We may rearrange this product so that pairs $x, y \bmod p$ that multiply to give $a \bmod p$ 'cancel out' accordingly

$$1 \cdot 2 \ldots (p-1) \equiv \underset{a}{(\;)} \cdot \underset{a}{(\;)} \ldots \underset{a}{(\;)}$$

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

At the same time $(p-1)! \equiv -1 \bmod p$ by Wilson's Theorem
So $a^{\frac{1}{2}(p-1)} \equiv -1 \bmod p$ and by definition of a, a is not a quadratic residue mod p: $(a/p) \equiv -1$
Hence $(a/p) \equiv a^{\frac{1}{2}(p-1)} \bmod p$.

Example: Let us determine if 2, 3 are quadratic residues mod 11 using Euler's Criterion.

$p = 11$ $\quad 2^{\frac{1}{2}(p-1)} = 2^5 = 32$
$\equiv -1 \bmod 11$. So 2 is not a quadratic residue

$3^{\frac{1}{2}(p-1)} = 3^5 = 27 \cdot 9$
$\equiv 5 \cdot 9 \bmod 11$
$\equiv 1 \bmod 11$. So 3 is a quadratic residue mod 11

From Euler's Criterion we may define a very useful property of the Legandre symbol.

Proposition:

For an odd prime, p and intergers a, b: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof : Using euler's criterion

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

$\left(\frac{b}{p}\right) \equiv b^{\frac{1}{2}(p-1)} \bmod p$

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

Another way of stating this result is :
suppose a, b intergers , $a, b \not\equiv 0 \bmod p$ (p odd prime)
Then mod p : • If a and b are both quadratic residues the so is ab $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1 \cdot 1 = 1$

• If ~~much~~ neither a, b are quadratic residues then ab is a quadratic residue $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -1 \cdot -1 = 1$

• If exactly one of of a, b is a quadratic residue then ab is not a quadratic residue $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -1 \cdot 1 = -1$

Furthermore the 'multiplicatively' of the Legandre symbol, shows that in order to calculate $\left(\frac{a}{p}\right)$ for any interger a and any odd prime p it is sufficent to know the value of (q/p) for a prime q

eg. $\left(\frac{60}{67}\right) = \left(\frac{2^2 \cdot 3 \cdot 5}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{2}{67}\right)\left(\frac{3}{67}\right)\left(\frac{5}{67}\right)$

Next ~~mmm~~ step : To find a relatively simple way of computing $\left(\frac{a}{p}\right)$ by ~~raha~~ relating it to $\left(\frac{p}{q}\right)$

To show how $\left(\frac{p}{q}\right)$ relates to $\left(\frac{q}{p}\right)$, as well as other related results, we will give another way of calculating Legandre symbols (other than Euler's criterion)
This works by condensing the least residue of a number mod p (p odd)

Definition:

The least residue of an interger m mod p is the element of the congruence class of m mod p with the smallest absolute value.

eg. the least residue of 2 mod 7 is 2
4 mod 7 is -3
19 mod 7 is -2

So modulo an odd prime p, the ~~least~~ possible least residues are $-\frac{1}{2}(p-1), \dots, -2, -1, 0, 1, 2, \dots, \frac{1}{2}(p-1)$

eg. the least residues mod 7 are $-3, -2, -1, 0, 1, 2, 3$.

Lets see how we may use the least residues to calculate $\left(\frac{m}{p}\right)$ with odd prime p.
We first multiply m by each of $1, 2, \dots, \frac{1}{2}(p-1)$ and then find the least residue of the resulting answers.
The number of negative least residues reveals the answers to $\left(\frac{m}{p}\right)$.

Example: Compute $\left(\frac{2}{7}\right)$

Consider $\underset{2}{\underset{\shortparallel}{2\cdot 1}}, \underset{-3}{\underset{\shortparallel}{2\cdot 2}}, \underset{-1}{\underset{\shortparallel}{2\cdot 3}}$

$(2\cdot 1)(2\cdot 2)(2\cdot 3) \equiv (-1)^2(2)(3) \bmod 7$

$2^{\frac{1}{2}(7-1)} = 2^3 \equiv (-1)^2 \bmod 7$

This is congruent to $\left(\frac{2}{7}\right) \bmod 7$

so $(-1)^2 \equiv \left(\frac{2}{7}\right) \bmod 7$.

Example: compute $\left(\frac{2}{11}\right)$

$(2\cdot 1)(2\cdot 2)(2\cdot 3)(2\cdot 4)(2\cdot 5) = 2^5(5!)$

$\;\;\;\;\underset{2}{\shortparallel}\;\;\;\;\underset{4}{\shortparallel}\;\;\;\;\underset{-5}{\shortparallel}\;\;\;\;\underset{-3}{\shortparallel}\;\;\;\;\underset{-1}{\shortparallel} \;\; = (-1)^3(5!)$

$\Rightarrow \left(\frac{2}{11}\right) \equiv 2^{\frac{1}{2}(11-1)} = 2^5 \equiv (-1)^3 \bmod 11$.

In general:

Theorem: Gauss' Lemma

Let p be an odd prime, and m interger, $m \not\equiv 0 \bmod p$.
Then consider the least residues of $1\cdot m, 2\cdot m, \dots \frac{1}{2}(p-1)\cdot m$
If u is the number of negative least residues: $\left(\frac{m}{p}\right) = (-1)^u$

Proof: Lets first consider absolute values of $m, 2m, \dots \frac{1}{2}(p-1)m$.
These absolute values a precisely all positive numbers from 1 to $\frac{p-1}{2}$, as we show below.
Since p prime, none of $m, 2m, \dots \frac{1}{2}(p-1)m$ is zero.
There are $\frac{p-1}{2}$ numbers in $\{m, 2m, \dots \frac{1}{2}(p-1)m\}$ and there are

$\frac{p-1}{2}$ possible absolute values of least residues, so it is enough to check that no two absolute values are equal.

Suppose $|am| = |bm| \mod p$

Either $am \equiv bm \mod p$, ie $a \equiv b \mod p$

OR $am \equiv -bm \mod p$ ie ~~am+bm~~ $am + bm \equiv 0 \mod p$

ie $a + b \equiv 0 \mod p$.

This is not possible since, $1 \leq a \leq \frac{1}{2}(p-1)$

$1 \leq b \leq \frac{1}{2}(p-1)$

So $2 \leq a+b \leq p-1$

So $a+b \not\equiv 0 \mod p$

So the absolute values of least residues of $m, 2m, \ldots, \frac{1}{2}(p-1)m$ are $1, 2, \ldots, \frac{1}{2}(p-1)$ in some order.

So $m \cdot 2m \cdot \ldots \cdot \frac{1}{2}(p-1)m \equiv (-1)^u \, 1 \cdot 2 \cdot \ldots \cdot \frac{1}{2}(p-1) \mod p$

ie $m^{\frac{1}{2}(p-1)}(1 \cdot 2 \ldots (\frac{1}{2}(p-1))) \mod p$

Therefore $m^{\frac{1}{2}(p-1)} \equiv (-1)^u \mod p$

By Eulers Criterion: $\left(\frac{m}{p}\right) \equiv m^{\frac{1}{2}(p-1)} \mod p$

Therefore, as required, $\left(\frac{m}{p}\right) \equiv (-1)^u \mod p$. QED.

Example: Lets use Gauss' Lemma to compute $\left(\frac{2}{17}\right), \left(\frac{3}{17}\right), \left(\frac{4}{17}\right)$ $\left(\frac{3}{17}\right)$ $p = 17$, $\frac{p-1}{2} = 8$

Consider $2, 4, 6, 8, 10, 12, 14, 16$

$\downarrow \mod 17 \downarrow$

$2, 4, 6, 8, \underbrace{-7, -5, -3, -1}_{\text{4 negative least residues}}$

$\left(\frac{2}{17}\right) = (-1)^u = (-1)^4 = 1$

$\left(\frac{3}{17}\right)$ Consider $3, 6, 9, 12, 15, 18, 21, 24$

$3, 6, -8, -5, -2, 1, 4, 7$

$\left(\frac{3}{17}\right) = (-1)^3 = -1$

$\left(\frac{4}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{2}{17}\right) = 1$

$\left(\frac{6}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right) = 1 \cdot -1 = -1.$

Lets try, to use what we have proven so far to obtain some general results about $\left(\frac{m}{p}\right)$ for some choices of m.

eg consider $m=-1$

By eulers criterion $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)} \bmod p$

So $\left(\frac{-1}{p}\right) = 1$ if $\frac{1}{2}(p-1)$ is even ie $\frac{1}{2}(p-1) = 2k$

ie $p-1 = 4k$ ie $p = 4k+1$ for some $k \in \mathbb{Z}$.

$\left(\frac{-1}{p}\right) = -1$ if $\frac{1}{2}(p-1)$ is odd ie $\frac{1}{2}(p-1) = 2k+1$

ie $p-1 = 4k+2$ ie $pk = 4k+3$.

So we have shown:

Proposition:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 4k+1 \quad k \in \mathbb{Z}. \\ -1 & \text{if } p = 4k+3 \end{cases}$$

eg. $-1 \equiv 12 \bmod 13$ is a square mod 13 $(13 = 4\cdot 3+1)$

$-1 \equiv 22 \bmod 23$ is not square mod 23 $(23 = 4\cdot 8+2)$.

Is there are a similar result for $\left(\frac{2}{p}\right)$? $(p \neq 2)$.

Eulers Criterion: $\left(\frac{2}{p}\right) \equiv 2^{\frac{1}{2}(p-1)} \bmod p$.

not so easy to compute this. Lets use Gauss Lemma instead.

p	2, 4, ..., p-1
3	$\underline{2}$
5	2 $\underline{4}$
7	2 $\underline{4}$ $\underline{6}$
11	2 4 $\underline{6\ 8\ 10}$
13	2 4 6 $\underline{8\ 10\ 12}$
17	2 4 6 8 $\underline{10\ 12\ 14\ 16}$

— negative residue.

Lets try to work out a general rule, by using Gauss Lemma:

Consider 2, 4, ..., p-1

We wish to count the number of negative residues

There are two cases to consider

$\frac{1}{2}(p-1)$ is even

In this case the number of negative residues is $\frac{1}{2}\left(\frac{p-1}{2}\right) = \frac{1}{4}(p-1)$

$\frac{1}{2}(p-1)$ is odd

Number of -ve residues $\frac{1}{4}(p+1)$

Gauss' Lemma converts the problem of determining $\left(\frac{m}{p}\right)$ to an exercise in counting, in some cases.

A particularly simple case is where $m=2$.

Proposition:

For an odd prime p $\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p = 1, 7 \bmod 8 \\ -1 & \text{if } p = 3, 5 \bmod 8. \end{cases}$

Proof: We will use Gauss' Lemma:

Consider the numbers $2, 4, 6, \ldots, 2\frac{1}{2}(p-1) = (p-1) \bmod p$

We need to find the classes corresponinding to negative least residues and count.

In this case the numbers with negative least residue are precisely those corresponding to multiples of 2 greater than $\frac{p}{2}$.

So lets count how many such residues exist.

Case 1: $\frac{1}{2}(p-1) = 2 \times \frac{1}{4}(p-1)$ is an even number

Then there are $\frac{1}{4}(p-1)$ positive least residues in this list

$2 \cdot 1, 2 \cdot 2, \ldots, 2 \cdot \frac{1}{2}(p-1)$

So there are $\frac{1}{2}(p-1) - \frac{1}{4}(p-1) = \frac{1}{4}(p-1)$

Then. $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{4}(p-1)}$ using Gauss Lemma

Hence: $\left(\frac{2}{p}\right) = 1$ if $\frac{1}{4}(p-1)$ is even

ie $\frac{1}{4}(p-1) = 2K \quad K \in \mathbb{Z}$

$p-1 = 8K$

$p = 8K+1$

$p \equiv 1 \bmod 8$

While $\left(\frac{2}{p}\right) = -1$ if $\frac{1}{4}(p-1)$ is odd

ie if $p \equiv 5 \bmod 8$.

Case 2 : $\frac{1}{2}(p-1) = 2 \times \frac{1}{4}(p-1)$ is an odd number

Then there are $\frac{1}{4}(p-3)$ positive least residues in the list
$2\cdot 1, 2\cdot 2, \ldots, 2\cdot\frac{1}{2}(p-1)$
So there are $\frac{1}{2}(p-1) - \frac{1}{4}(p-3) = \frac{1}{4}(p+1)$ negative least residues
Then $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{4}(p+1)}$ using Gauss' Lemma.
Here : $\left(\frac{2}{p}\right) = 1$ if $\frac{1}{4}(p+1)$ is even
ie $\frac{1}{4}(p+1) = 2k \quad k \in \mathbb{Z}$
$p+1 = 8k$
$p = 8k-1$
$p \equiv 7 \bmod 8$
While : $\left(\frac{2}{p}\right) = -1$ if $\frac{1}{4}(p+1)$ is odd
~~ie $\frac{1}{4}(p+1)$~~ ie $p \equiv 3 \bmod 8$. QED.

We could try to apply the same idea, and Gauss' Lemma, to determine $\left(\frac{m}{p}\right)$ for cases other than $m \equiv 2 \bmod p$.
But in such cases, counting the ~~least~~ negative least residues is not as simple.

eg. $p = 11$, $m = 3$: $3\times1, 3\times2, 3\times3, 3\times4, 3\times5$
$3 \quad 6 \quad 9 \quad 12 \quad 15$
$3 \quad -5 \quad -2 \quad 1 \quad 4 \mod 11$

Another way of computing $\left(\frac{3}{11}\right)$
Consider the multiples of 3 up to $3 \times \frac{1}{2}(11-1) = 3\times 5$
$3, 6, 9, 12, 15$
Lets count the number of times 11 divides each of these multiples
ie compute : $\left\lfloor \frac{3}{11} \right\rfloor, \left\lfloor \frac{6}{11} \right\rfloor, \left\lfloor \frac{9}{11} \right\rfloor, \left\lfloor \frac{12}{11} \right\rfloor, \left\lfloor \frac{15}{11} \right\rfloor$
$0 \quad 0 \quad 0 \quad 1 \quad 1$

Let u' be the sum of the resulting answers : $u' = 0+0+0+1+1 = 2$ here
Then $\left(\frac{3}{11}\right) = (-1)^{u'} = +1$

Lets also apply this process to $\left(\frac{5}{11}\right)$
$\left\lfloor \frac{5}{11} \right\rfloor + \left\lfloor \frac{10}{11} \right\rfloor + \left\lfloor \frac{15}{11} \right\rfloor + \left\lfloor \frac{20}{11} \right\rfloor + \left\lfloor \frac{25}{11} \right\rfloor = 0+0+1+1+2 = 4.$

This holds in general, for an odd prime p, and an odd m

Proposition:

Let p be an odd prime, and m be an odd natural number, $m \not\equiv 0 \bmod p$.

Then $\left(\frac{m}{p}\right) = (-1)^{u'}$ where $u' = \sum_{k=1}^{\bar{p}} \left\lfloor \frac{km}{p} \right\rfloor$ $\quad \bar{p} = \frac{1}{2}(p-1)$

Proof: Consider the congruence classes of $m, 2m, \dots, \frac{1}{2}(p-1)m = \bar{p}m \bmod p$ and apply the euclidean algorithm (once) to each km $(1 \leq k \leq \bar{p})$ and p:

$$km = \left\lfloor \frac{km}{p} \right\rfloor p + \begin{cases} r_k & \text{if remainder is less than } p/2 \\ s_k & \text{if remainder is greater than } p/2 \end{cases}$$

(r_k have positive least residue, s_k have negative least residue).

Lets consider the sum of these Euclidean processes from $k=1$ to $k=\bar{p}$

$$\sum_{k=1}^{\bar{p}} km = \sum_{k=1}^{\bar{p}} \left\lfloor \frac{km}{p} \right\rfloor p + \sum r_k + \sum s_k$$

ie $m \sum_{k=1}^{\bar{p}} k = p \sum_{k=1}^{\bar{p}} \left\lfloor \frac{km}{p} \right\rfloor + \sum r_k + \sum s_k$ (1)

We also know that the absolute values of the least residue remainders give $1, 2, \dots, \frac{1}{2}(p-1) = \bar{p}$ in some order

For a remainder of the type r_k, the least residue is r_k and the absolute value of this is $|r_k| = r_k$

For a remainder of the type s_k, the least residue is $s_k - p$ and the absolute value for this is $|s_k - p| = p - s_k$

The sum of the absolute values is $1 + 2 + \dots + \bar{p}$

~~ie $|\sum r_k + \sum (p - s_k)|$~~

ie $\sum_{k=1}^{\bar{p}} k = \sum (p - s_k) + \sum r_k$ (2)

Subtracting (2) from (1) gives:

$$(m-1) \sum_{k=1}^{\bar{p}} k = p \sum_{k=1}^{\bar{p}} \left\lfloor \frac{km}{p} \right\rfloor + \underbrace{\sum s_k - \sum (p - s_k)}_{\sum 2s_k - \sum p}$$

$$(m-1) \sum_{k=1}^{\bar{p}} k = p \sum_{k=1}^{\bar{p}} \left\lfloor \frac{km}{p} \right\rfloor + 2 \sum s_k - pu$$ where u is the number of negative least residues

Consider the resulting equation mod 2.

$$0 = \sum_{k=1}^{\bar{p}} \left\lfloor \frac{km}{p} \right\rfloor + u$$

ie $\sum_{k=1}^{\bar{p}} \left\lfloor \frac{km}{p} \right\rfloor \equiv u \bmod 2$

By Gauss' Lemma $\left(\frac{m}{p}\right) = (-1)^{u}$

So $\left(\frac{m}{p}\right) = (-1)^{u'}$ where $u' = \sum_{k=1}^{\bar{p}} \left\lfloor \frac{km}{p} \right\rfloor$ QED.

We will use this to prove a special connection between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for odd primes p and q.

Consider $p=3,\ q=5$: $\left(\frac{3}{5}\right) = -1$, $\left(\frac{5}{3}\right) = -1$

$p=5,\ q=11$: $\left(\frac{5}{11}\right) = +1$ $\left(\frac{11}{5}\right) = +1$

$p=5,\ q=7$: $\left(\frac{5}{7}\right) = -1$ $\left(\frac{7}{5}\right) = -1$

$p=3,\ q=7$: $\left(\frac{3}{7}\right) = -1$ $\left(\frac{7}{3}\right) = +1$!

In general the following holds.

Theorem: Law of Quadratic Reciprocity

Let p, q be distinct odd primes. Then:

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

ie if $\frac{p-1}{2}$ is even, ie $p \equiv 1 \bmod 4$ then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$

$\frac{q-1}{2}$ is even ie $q \equiv 1 \bmod 4$ then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$

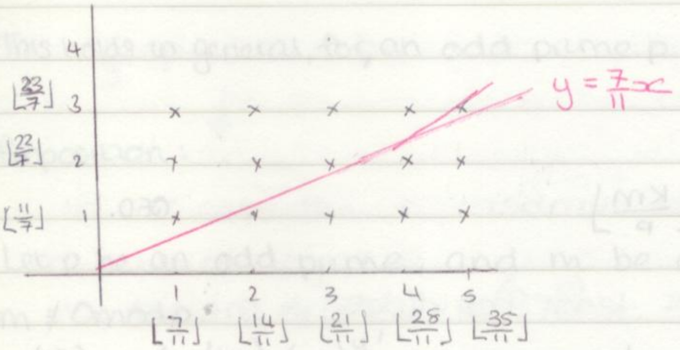
$(-1)^{\bar{p}\bar{q}}$ is odd precisely when $p \equiv 3 \bmod 4$ and $q \equiv 3 \bmod 4$ then $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

Example: $p=11,\ q=7$

Using a result from last time: $\left(\frac{7}{11}\right) = (-1)^{\sum_{k=1}^{5} \left\lfloor \frac{7k}{11} \right\rfloor}$ and $\left(\frac{11}{7}\right) = (-1)^{\sum_{k=1}^{3} \left\lfloor \frac{11k}{7} \right\rfloor}$

Therefore $\left(\frac{7}{11}\right)\left(\frac{11}{7}\right) = (-1)^{\sum_{k=1}^{5} \left\lfloor \frac{7k}{11} \right\rfloor + \sum_{k=1}^{3} \left\lfloor \frac{11k}{7} \right\rfloor}$

So we need to show $\sum_{k=1}^{5} \left\lfloor \frac{7k}{11} \right\rfloor + \sum_{k=1}^{3} \left\lfloor \frac{11k}{7} \right\rfloor = 5 \cdot 3$



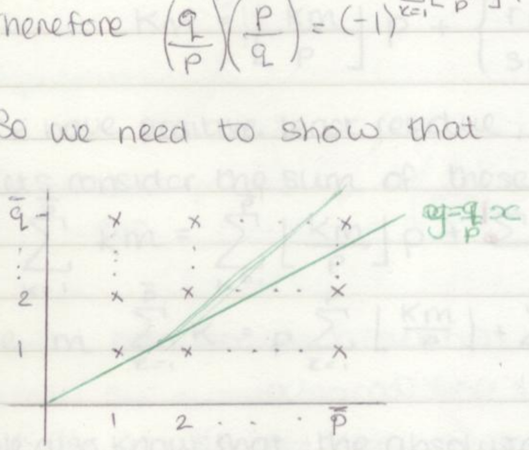
Consider the line $y=\frac{7}{11}x$.

Proof: Lets suppose wlog, that $p>q$.

Using result from last time: $\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\bar{p}}\lfloor\frac{kq}{p}\rfloor}$, $\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\bar{q}}\lfloor\frac{kp}{q}\rfloor}$

Therefore $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\bar{p}}\lfloor\frac{kq}{p}\rfloor + \sum_{k=1}^{\bar{q}}\lfloor\frac{kp}{q}\rfloor}$

So we need to show that $\sum_{k=1}^{\bar{p}}\lfloor\frac{kq}{p}\rfloor + \sum_{k=1}^{\bar{q}}\lfloor\frac{kp}{q}\rfloor = \bar{p}\cdot\bar{q}$



Lets consider the line $y=\frac{q}{p}x$

The number of integers points on the line $x=k$ below $y=\frac{q}{p}x$ is equal to $\lfloor\frac{kq}{p}\rfloor$.

The number of integer points on the line $y=k$, to the left of $y=\frac{q}{p}x$ is equal to $\lfloor\frac{kp}{q}\rfloor$

So the total number of points below the line $y=\frac{q}{p}x$ (for $1\leq x\leq\bar{p}$) is $\sum_{k=1}^{\bar{p}}\lfloor\frac{kq}{p}\rfloor$, while the total number to the left of the line $y=\frac{q}{p}x$ (for $1\leq y\leq\bar{q}$) is $\sum_{k=1}^{\bar{q}}\lfloor\frac{kp}{q}\rfloor$.

Furthermore there are no integer points on the line $y=\frac{q}{p}x$ for $0<x\leq\bar{p}$ (if $y=\frac{q}{p}x$ for $x,y\in\mathbb{N}$ then $yp=qx$ so since p,q coprime, y is a multiple of q and x is a multiple of p).

Also if we substitute the largest x-coordinate of the region we are considering, $x=\bar{p}$, we obtain $y=\frac{q}{p}\bar{p}$

We can check that $\bar{q}<\frac{q}{p}\bar{p}<\bar{q}+1$

So the sum of the numbers of points below and to the left of $y=\frac{q}{p}x$ (for $1\leq x\leq\bar{p}$) is precisely the number of integer points, within the region defined by $1\leq x\leq\bar{p}$, $1\leq y\leq\bar{q}$.

ie $\sum_{k=1}^{\bar{p}}\lfloor\frac{kq}{p}\rfloor + \sum_{k=1}^{\bar{q}}\lfloor\frac{kq}{p}\rfloor = \bar{p}\cdot\bar{q}$ QED

Computing 'quadratic residues'/problems involving quadratic residues

Lets see how we may use some of the results related to quadratic residues in order to try to compute particular Legendre symbols and try to solve problems involving residues.

First we summerise some of the results we have seen:

- If p is an odd prime: $\left(\frac{m}{p}\right) \equiv m^{\frac{1}{2}(p-1)} \bmod p \rightsquigarrow \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv -1 \bmod 4 \end{cases}$

  Eulers criterion.

- $\left(\frac{m}{p}\right) = (-1)^{u}$ where u is the number of negative residues in $\{m, 2m, \dots, \frac{1}{2}(p-1)m\}$ Gauss Lemma

  $\rightsquigarrow \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \bmod 8 \\ -1 & \text{if } p \equiv 3, 5 \bmod 8 \end{cases}$

- If p, q distinct odd primes $\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\left(\frac{p}{q}\right)$

  Law of quadratic reciprocity.

Example: Lets try to compute quadratic residues mod 59 Legendre symbols.

Firstly, we determine the legendre symbol $\left(\frac{p}{59}\right)$ for any prime p less than or equal to 59.

eg. $\left(\frac{2}{59}\right) = -1$ (since $59 \equiv 3 \bmod 8$).

$\left(\frac{3}{59}\right) = (-1)^{1\cdot 29}\left(\frac{59}{3}\right) = -\left(\frac{59}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = +1$

$\left(\frac{7}{59}\right) = -\left(\frac{59}{7}\right) = -\left(\frac{3}{7}\right) = -(-1) = 1$

$\left(\frac{11}{59}\right) = -\left(\frac{59}{11}\right) = -\left(\frac{4}{11}\right) = -1$

It might also be useful to compute $\left(\frac{-1}{59}\right)$: $\left(\frac{-1}{59}\right) = -1$ since $p \equiv -1 \bmod 4$.

We may then use the general rule $\left(\frac{ab}{59}\right) = \left(\frac{a}{59}\right)\left(\frac{b}{59}\right)$ to compute any other Legendre symbol.

eg. $\left(\frac{6}{59}\right) = \left(\frac{2}{59}\right)\left(\frac{3}{59}\right) = -1\cdot 1 = -1$

$\left(\frac{8}{59}\right) = \left(\frac{2}{59}\right)^3 = (-1)^3 = -1$

$$\left(\frac{48}{59}\right)=\left(\frac{2}{59}\right)\left(\frac{2}{59}\right)\left(\frac{2}{59}\right)\left(\frac{2}{59}\right)\left(\frac{3}{59}\right)=1$$

Here we used the fact that, since, for any $m \not\equiv 0 \bmod p$ $\left(\frac{m}{p}\right)=1$ or -1 the following always holds: $\left(\frac{m^2}{p}\right)=1$

$$\left(\frac{30}{59}\right)=\left(\frac{2}{59}\right)\left(\frac{3}{59}\right)\left(\frac{5}{59}\right)=-1\cdot 1\cdot 1=-1.$$

In some cases it might be useful to also 'introduce' a negative congruence class and use the result for $\left(\frac{-1}{p}\right)$.

eg. $\left(\frac{58}{59}\right)=\left(\frac{2}{59}\right)\left(\frac{29}{59}\right)\ldots$ and $\left(\frac{58}{59}\right)=\left(\frac{-1}{59}\right)=-1$

$\left(\frac{53}{59}\right)$ note 53 is prime.

One way: $\left(\frac{53}{59}\right)=(-1)^{26\cdot 29}\left(\frac{59}{53}\right)=\left(\frac{6}{53}\right)=\left(\frac{2}{53}\right)\left(\frac{3}{53}\right)$

Possibly quicker method: $\left(\frac{53}{59}\right)=\left(\frac{-6}{59}\right)=\left(\frac{-1}{59}\right)\left(\frac{2}{59}\right)\left(\frac{3}{59}\right)=-1\cdot -1\cdot 1=1$

We can generalise this last ~~result~~ 'trick' of using negative congruence classes to compute, for example $\left(\frac{p-2}{p}\right)$ p odd prime.

Proposition:

$$\left(\frac{p-2}{p}\right)$$

Proof: $\left(\frac{p-2}{p}\right)=\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$

$\left(\frac{-1}{p}\right)=\begin{cases}1 & p\equiv 1 \bmod 4\\ -1 & p\equiv 3 \bmod 4\end{cases}$ ie $p\equiv 1$ or $5 \bmod 8$, $p\equiv 3$ or $7 \bmod 8$

$\left(\frac{2}{p}\right)=\begin{cases}1 & p\equiv 1 \text{ or } 7 \bmod 8\\ -1 & p\equiv 3 \text{ or } 5 \bmod 8.\end{cases}$

So if $p\equiv 1 \bmod 8$: $\left(\frac{p-2}{p}\right)=(1)(1)=1$

$\equiv 3 \bmod 8$: " $(-1)(-1)=1$

$\equiv 5 \bmod 8$: " $(1)(-1)=-1$

$\equiv 7 \bmod 8$: " $(-1)(1)=-1$

Other exercises involving residues:

Determine whether or not the following congruences have solutions.

1 $x^2 + 2x \equiv 0 \bmod 59$

2 $x^2 + 2x \equiv 2 \bmod 59$

3 $x^2 - 6x + 7 \equiv 0 \bmod 59$.

1. $\Leftrightarrow (x^2 + 2x + 1) - 1 \equiv 0 \bmod 59 \Leftrightarrow (x+1)^2 \equiv 1 \bmod 59$

There are solutions $x + 1 \equiv 1 \bmod 59$ $\quad x + 1 \equiv -1 \bmod 59$

$x \equiv 0 \bmod 59$ or $x \equiv -2 \bmod 59$.

2. $\Leftrightarrow (x^2 + 2x + 1) \equiv 3 \bmod 59 \Leftrightarrow (x+1)^2 \equiv 3 \bmod 59$

Does have solutions since $\left(\frac{3}{59}\right) = +1$

3. $\Leftrightarrow (x^2 - 3) \equiv 2 \bmod 59$,

has no solutions since $\left(\frac{2}{59}\right) = -1$.

We may also generalise results involving specific congruences, eg. lets determine for which odd primes p we have solutions for $x^2 - 6x + 7 \equiv 0 \bmod p$.

$x^2 - 6x + 7 \equiv 0 \bmod p \Leftrightarrow (x-3)^2 - 9 + 7 \equiv 0 \bmod p$

$\Leftrightarrow (x-3)^2 \equiv 2 \bmod p$.

For which values of p is 2 a square mod p?

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

So 2 is a quadratic residue (or ~~'square~~ 'square') mod p precisely when $p \equiv 1 \bmod 8$ or $p \equiv 7 \bmod 8$.

ie. the original equation has a solution for an odd prime p, precisely when $p \equiv 1 \bmod 8$ or $p \equiv 7 \bmod 8$.

Primality Testing

Suppose that we are given a number n and we wish to determine whether or not n is prime.

Definite ways:

1. Check whether or not any number $1 < m < n$ divides n.
2. Check whether or not any prime $1 < p < n$ divides n
3. Check whether or not any prime $1 < p \leq \sqrt{n}$ divides n

There are more sophisticated methods, but even these take 'too long' to check primality of large numbers.

Instead of checking directly and trying to verify conclusively the primality of a number, we may try to find a more indirect method, involving some properties of prime numbers. (inconclusive).

We will use Fermats Little Theorem to try to identify primes:

If p is prime then $m^{p-1} \equiv 1 \bmod p$ for any $m \not\equiv 0 \bmod p$.

This leads to the following algorithm for primality testing.

- ~~Consider $m^{n-1} \not\equiv 1 \bmod n$ then n is definitely not~~
- Consider a natural number n and a number m less than n.
  If $m^{n-1} \not\equiv 1 \bmod n$ then n definitely isn't prime.
  If $m^{n-1} \equiv 1 \bmod n$, then try a different value of m.

eg. Consider $n=5$

$1^4 \equiv 1 \bmod 5$
$2^4 \equiv 1 \bmod 5$
$3^4 \equiv 1 \bmod 5$
$4^4 \equiv 1 \bmod 5$

$n=6$

$1^5 \equiv 1 \bmod 6$
$2^5 \equiv 2 \bmod 6$
$3^5 \equiv 3 \bmod 6$
$4^5 \equiv 4 \bmod 6$
$5^5 \equiv 5 \bmod 6$.

Note that in general $m^{\phi(n)} \equiv 1 \bmod n$
$\phi(6) = 2 \quad m^2 \equiv 1 \bmod 6$.

So the algorithm works very well for 6. Apart from $m=1$, $m^5 \not\equiv 1 \bmod 6$

However this does not hold in general, ~~sometimes it will be~~

Definition:

Consider natural numbers, n and m, n, m coprime.

Then n is pseudoprime for the base m if $m^{n-1} \equiv 1 \bmod n$

eg. ~~For example~~ $n=21$, $m=8$

$(8)^{20} = (8^2)^{10} \equiv 64^{10} \bmod 21 \equiv 1^{10} \bmod 21$

So since $8^{20} \equiv 1 \bmod 21$, 21 is pseudoprime base 8.

Note that, in such a case m must be coprime to n.

If $m^{n-1} \equiv 1 \bmod n$, then $m(m^{n-2}) \equiv 1 \bmod n$

ie if m is invertible mod n

ie if m is coprime to n.

So when looking for pseudoprime bases for n, we only need to consider numbers coprime to n.

Example: Lets find all bases for which 21 is pseudoprime, try to find values of m(mod 21) satisfying $m^{20} \equiv 1 \bmod 21$.

$\phi(21) = \phi(3)\phi(7) = 2 \cdot 6 = 12$.

Numbers coprime to 21: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20.

Lets find $m^{20} \bmod 21$ for $m = 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20 \bmod 21$

We could compute $m^{20} \bmod 21$ in each case by:

i) computing $m, m^2, m^3, \ldots, m^{20} \bmod 21$

ii) using $m^{\phi(21)} \equiv 1 \bmod 21$ ie $m^{12} \equiv 1 \bmod 21$

Because of this, $m^{20} = m^{12} \cdot m^8$
$\equiv m^8 \bmod 21$

So we need only calculate m^8 in each case

$1^8 \equiv 1 \bmod 21$

$2^4 \equiv 16 \bmod 21$, $2^4 \equiv -5 \bmod 21$

$2^8 \equiv (-5)^2 \bmod 21$

ie $2^8 \equiv 4 \bmod 21$

$(19)^8 \equiv (-2)^8 \bmod 21$
$\equiv 2^8 \bmod 21$
$\equiv 4 \bmod 21$

$(20)^8 \equiv (-1)^8 \bmod 21$
$\equiv 1 \bmod 21$

ii) is slightly easier/better than i) but in general we may use the following method.

iii) $m^{20} \equiv 1 \bmod 21$ if and only if

$m^{20} \equiv 1 \bmod 3$

Mod 3: $m^2 \equiv 1$ for any $m \not\equiv 0 \bmod p$

$m \equiv 1 \bmod 3$ or $m \equiv -1 \bmod 3$

$m^{20} \equiv 1 \bmod 7$

Mod 7: $m^6 \equiv 1 \bmod 7$ for any $m \not\equiv 0 \bmod 7$

So $m^{20} = m^{18} m^2$
$\equiv m^2 \bmod 7$

So $m^{20} \equiv 1 \bmod 7$ iff $m^2 \equiv 1 \bmod 7$
$m \equiv \pm 1 \bmod 7$.

So it is enough to write down all numbers mod 21 that are congruent to $\pm 1 \bmod 3$ and $\pm 1 \bmod 7$:

For '$\pm 1 \bmod 7$', have: 1, 6, 8, 13, 15, 20

Of these, each of $m = 1, 8, 13, 20$ also satisfy $m \equiv \pm 1 \bmod 3$.

So these must be the 'pseudoprime'

ie $1^{20} \equiv 1 \bmod 21$
$8^{20} \equiv 1 \bmod 21$

$13^{20} \equiv (-8)^{20} \bmod 21$
$\equiv 1 \bmod 21$

$20^{20} \equiv (-1)^{20} \bmod 21$
$\equiv 1 \bmod 21$

So out of 20 'numbers' mod 21, 4 of them (1, 8, 13, 20) make 21 look like a prime.

in general the proposition of pseudoprime bases may vary considerably.

There are three general cases:

1. n is a prime number
   Then $m^{n-1} \equiv 1 \bmod n$ for any m coprime to n (Fermat's little theorem)

2. n is a composite number such that $m^{n-1} \equiv 1 \bmod n$ for some values of m (coprime to n) and $m^{n-1} \not\equiv 1 \bmod n$ for others values of m

3. n is a composite number such that $m^{n-1} \equiv 1 \bmod n$ for any m coprime to n. Such numbers are called Carmichael numbers
   eg 561

Definition:

A composite natural number n is a Carmichael number if $m^{n-1} \equiv 1 \bmod n$ for any integer m coprime to n
(or equivalently, if $\bar{m}^{n-1} = \bar{1}$ for any $\bar{m} \in U(\mathbb{Z}_n)$)

eg. 561 is a carmichael number, $m^{560} \equiv 1 \bmod 561$ for any integer m coprime to 561.

Proof: Consider the prime factorisation of 561: $561 = 3 \times 11 \times 17$.

If m is coprime to; 3 $m^2 \equiv 1 \bmod 3$, then $m^{560} \equiv (m^2)^{280} \equiv 1 \bmod 3$
11 $m^{10} \equiv 1 \bmod 11$, then $m^{560} = (m^{10})^{56} \equiv 1 \bmod 11$
17 $m^{16} \equiv 1 \bmod 17$, then $m^{560} = (m^{16})^{35} \equiv 1 \bmod 17$

But $a \equiv 1 \bmod 561$ if and only if $a \equiv 1 \bmod 3$, $a \equiv 1 \bmod 11$, $a \equiv 1 \bmod 17$
$\Rightarrow m^{560} \equiv 1 \bmod 561$ for any m coprime to 561.

In general the following holds:

Proposition:

Suppose that a composite number n is a product of distinct primes $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ (where $p_i \neq p_j$, $i \neq j$).
and $p_1 - 1, p_2 - 1, \ldots, p_k - 1$ are all divisors of $n-1$, then n is a Carmichael number

Proof: consider an interger m coprime to $n = p_1 p_2 \dots p_k$
Then m is also coprime to $p_1 \dots p_k$.
Therefore using Fermats Little Theorem:
$m^{p_1 - 1} \equiv 1 \bmod p_1$ then $m^{n-1} \equiv 1 \bmod p_1$ since $p_1 - 1 \mid n-1$
$\vdots$
$m^{p_k - 1} \equiv 1 \bmod p_k$ then $m^{n-1} \equiv 1 \bmod p_k$ since $p_k - 1 \mid n-1$.
Then using the chinese remainder theorem, the unique congruence class of $m^{n-1} \bmod n$ is 1: $m^{n-1} \equiv 1 \bmod n$
So n is a carmicheal number as required.

Lets now consider the case where n is not a prime number or a carmichael number, then for some interger m coprime to n
$m^{n-1} \not\equiv 1 \bmod n$
What is the proportion of such values of m?
To determine this we need to study the structure of the set
$S = \{\bar{m} \in U(\mathbb{Z}_n) : \bar{m}^{n-1} = \bar{1}\}$.
It turns out S is a subgroup of $U(\mathbb{Z}_n)$.

Proposition:

For any natural number n, greater than 1, the set $S = \{\bar{m} \in U(\mathbb{Z}_n) : \bar{m}^{n-1} = \bar{1}\}$ is a (multiplicative) subgroup of $U(\mathbb{Z}_n)$

Proof: Let's check that the 'closure', 'identity' and 'inverse' conditions are satisfied.
i) Suppose that $\bar{a}, \bar{b} \in S$ ie that $\bar{a}^{n-1} = \bar{1}$ and $\bar{b}^{n-1} = \bar{1}$.
Then $(\bar{a}\bar{b})^{n-1} = \bar{a}^{n-1}\bar{b}^{n-1} = \bar{1} \cdot \bar{1} = \bar{1}$.
So $\bar{a}\bar{b} \in S$
ii) The identity in $U(\mathbb{Z}_n)$ is $\bar{1}$: $\bar{1}^{n-1} = \bar{1}$ so $\bar{1} \in S$.
iii) Suppose that $\bar{a} \in S$, $\bar{a}^{n-1} = \bar{1}$
Then $(\bar{a}^{-1})^{n-1} = (\bar{a}^{n-1})^{-1} = (\bar{1})^{-1} = \bar{1} \Rightarrow \bar{a}^{-1} \in S$
$\bar{a}\bar{a}^{-1} = \bar{1}$
$\Rightarrow S$ is a subgroup of $U(\mathbb{Z}_n)$

Note that $S = U(\mathbb{Z}_n)$ if $\bar{m}^{n-1} = \bar{1}$ for every $\bar{m} \in U(\mathbb{Z}_n)$
ie $S = U(\mathbb{Z}_n)$ if and only if n is prime or a carmichael number.

For any other number, S is a proper subgroup of $U(\mathbb{Z}_n)$
Then by Legrange's Theorem: $|U(\mathbb{Z}_n)| = k|S|$ for $k \geq 2$ ie $\frac{|S|}{|U(\mathbb{Z}_n)|} \leq 1/2$.

So suppose that n is not a prime number or a carmichael number
The probability that for a randomly choosen interger m (coprime to n) satisfies $m^{n-1} \equiv 1 \bmod n$ is less than 1/2
So given a large number n, we may try to compute $m^{n-1} \bmod n$ for various values of m:
Say we try it for 20 randomly choosen values of m.
If n is not a carmichael number, the probability that $m^{n-1} \equiv 1 \bmod n$ for each of these 20 values is less than $\underbrace{\frac{1}{2} \cdots \frac{1}{2}}_{20 \text{ times}} = \frac{1}{2^{20}} < \frac{1}{10^6}$

So primality testing using this algorithm seems "quite good" - Rabin-Miller algorithm.

~~Continued Fractions and Approximation~~.

Continued Fractions and Approximation

Definition:

A regular continued fraction is a (finite or infinite) expression of the form:

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \ddots}}}}$$

where for each $i \geq 1$ a_i is a non-negative interger and for each $i \geq 2$, a_i is positive.

Examples

1) $1 + \cfrac{1}{2 + 1/3}$ $a_1 = 1,\ a_2 = 2,\ a_3 = 3$

2) $1 + \cfrac{1}{1 + \cfrac{1}{1 + 1/2}}$ $a_1 = 1,\ a_2 = 1\ a_3 = 1\ a_4 = 2$

3) $1/7$ $a_1 = 0\ a_2 = 7$

4) 4 $a_1 = 4$

5) $1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}$ $a_i = 1$ for $i \in \mathbb{N}$.

We say that a continued fraction terminates if it is finite continued fraction

eg. 1, 2, 3, 4 above.

In such cases we may simplify a continued fraction to obtain a rational number.

We may work out continued fractions corresponding to $m/n \in \mathbb{Q}$ by applying the Euclidean algorithm to m and n.

eg. Try to express $10/7$ as a continued fraction.

$10 = 1 \cdot 7 + 3$ $\quad$ $10/7 = 1 + 3/7$ $\quad$ 1

$7 = 2 \cdot 3 + 1$ $\quad$ $\underrightarrow{\text{dividing}}$ $\quad$ $7/3 = 2 + 1/7$ $\quad$ 2

$3 = 3 \cdot 1 + 0$ $\quad$ $a = b \cdot c + d$ by c $\quad$ $3 = 3 \cdot 1$ $\quad$ 3.

By back substitution in the 'rational version' of the Euclidean algorithm we may obtain a continued fraction for $10/7$:

$$\frac{10}{7} = \underset{\uparrow_{1}}{1} + \frac{3}{7} = 1 + \frac{1}{7/3} \underset{\uparrow_{2.}}{=} 1 + \frac{1}{2 + 1/3}$$

Notice that even if we ~~move~~ start with an 'equivalent form' of $10/7$, we could obtain the same continued fraction.

eg. Start with $30/21$

$30 = 1 \cdot 21 + 9$ $\qquad 30/21 = 1 + 9/21$

$21 = 2 \cdot 9 + 3$ $\qquad 21/9 = 2 + 3/9 = 2 + 1/3$.

$9 = 3 \cdot 3 + 0$ $\qquad 9/3 = 3$.

$$30/21 = 1 + 9/21$$
$$= 1 + 1/21/9$$
$$= 1 + \frac{1}{2 + 1/3}.$$

In this way, ~~we~~ every finite continued fraction corresponds to a rational number, we will also show that only rational numbers may be written as continued fractions.

Let us now describe an algorithm that may be used to obtain a continued fraction for any (non-negative) real numbers by extending the 'scope' of the Euclidean algorithm:

Method:

Let r be a non-negative real number.

- We may express r as follows: $r = a_1 + r_1$
  where a_1 is a non-negative interger and r_1 is a real number satisfying $0 \leq r < 1$.
  If $r_1 = 0$ then $r = a_1$ is a non-negative interger, represented by the continued function a_1.
  Otherwise if $0 < r_1 < 1$, we consider $1/r_1$. This is a real number > 1 and we may express $1/r_1$ as follows:
  $1/r_1 = a_2 + r_2$ where a_2 is a positive interger and $0 \leq r_2 < 1$
  If $r_2 = 0$ then the process terminates: $1/r_1 = a_2$ and r may be expressed as $r = a_1 + \frac{1}{a_2}$

In general if $0 < r_n < 1$ then $1/r_n = a_{n+1} + r_{n+1}$ ($a_{n+1} \in \mathbb{N}$, $r_{n+1} \in \mathbb{R}$ $0 \leq r_{n+1} \leq 1$)
Then if $r_{n+1} = 0$, the process terminates, we express r as $a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}$

If $r_{n+1} \neq 0$ we proceed as above: $\frac{1}{r_{n+1}} = \ldots$

eg. $\frac{8}{5} = 1.6$

$1.6 = 1 + 0.6$ $\quad \frac{1}{0.6} = 1 + 0.\dot{6}$ $\quad \frac{1}{0.\dot{6}} = 1 + 0.5$ $\quad \frac{1}{0.5} = 2 + 0$,

$1.6 = 1 + \frac{1}{1 + \frac{1}{1 + 1/2}}$

It is obvious that if a continued fraction terminates, it corresponds to a rational number

ie if $r = a_1 + \frac{1}{a_2 + \frac{1}{\ddots\, a_{n-1} + \frac{1}{a_n}}}$ then since $a_{n-1}, a_n \in \mathbb{Q}$, $a_n \neq 0$: $a_{n-1} + \frac{1}{a_n} \in \mathbb{Q} \neq 0$

since $a_{n-1} + 1/a_n$, $a_{n-2} \in \mathbb{Q}$, $a_{n-1} + \frac{1}{a_n} \neq 0$:

$\Rightarrow a_{n-2} + \frac{1}{a_{n-1} + 1/a_n} \in \mathbb{Q} \neq 0$.

$r \in \mathbb{Q}$.

Lets try to show that, if r is a rational number, then the process described above terminates so that r is represented by a finite continued fraction.

Proposition:

If r is a rational number the above process terminates

Check online proof.

Proof: We will prove this by induction on the denominator of r.
Suppose that $r = p/q$, p non-negative interger, $q \in \mathbb{N}$.
If $q = 1$, then $r = p$ is a non-negative interger, represented by the continuous fraction p. (process terminates immediatly).
Lets now suppose that $q = n$ and that the result holds for all denominaters less than n.
$r = \frac{p}{n}$, $\frac{p}{n} = a + r_1$ where $r_1 \in \mathbb{R}$, $0 \leq r_1 \leq 1$.

ie $p = an + r_1 n$ where $r_1 n < n$
(note that p, a, n are intergers so p, an are intergers so $r_1 n$ is an interger).
Then at the next step we start with $1/r_1 n$, a rational number with a denominator less than n, so by induction $1/r_1 n$ may be expressed as a finite continued fraction.
So the whole process terminates, $\frac{p}{n}$ may be expressed as a finite continued fraction.

Preview: Consider $x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \dots}}}$ which number is this?

$x = 1 + 1/x$. $x^2 - x - 1 = 0$.

We will now try to identify the number corresponding to infinite continued fractions.
We starty by trying to introduce a, prehaps convient, way of computing continued fractions step by step.

Definition:

Consider a continued fraction, ~~of~~ finite or infinite, of the form
$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}$$

Then the number we obtain if we truncate the continued fraction at the n^{th} step (at a_n) is the n^{th} convergent of the continued fraction.

Example: Consider $2 + \cfrac{1}{3 + 1/5}$

first convergent is 2
second convergent is $2 + 1/3 = 7/3$
third convergent is $2 + \cfrac{1}{3 + 1/5} = 2 + \cfrac{1}{16/5}$
$$= \frac{37}{16}.$$

Example: Consider the infinite continued fraction: $1 + \cfrac{1}{1+\cfrac{1}{1+\cdots}}$

first convergent is $1/1$

Second convergent is $\cancel{1+\frac{1}{1}}$ $1+1/1 = 2/1$

third convergent is $\cancel{1+\frac{1}{1+\frac{1}{1}}}$ $= 1 + \frac{1}{1+1/1} = 3/2$

fourth convergent is $1 + \cfrac{1}{1+\cfrac{1}{1+1/1}} = 1 + \frac{1}{3/2} = \frac{5}{3}$.

fifth convergent is . . . . $8/5$.

We obtain sucessive ratios of consecutive Fibonacci numbers.
Let us try to show this holds in general, by first describing a different way of obtaining convergents.

Lets try to spot a pattern in the convergents; they are all rational numbers
suppose that the nth convergent is represented by the rational p_n/q_n

consider $a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}$

Then $\frac{p_1}{q_1} = a_1 = \frac{a_1}{1}$ so we may set $p_1 = a_1$ $q_1 = 1$

$\frac{p_2}{q_2} = a_1 + \frac{1}{a_2} = \frac{a_1a_2+1}{a_2}$ $p_2 = a_1a_2+1$ $q_2 = a_2$

$\frac{p_3}{q_3} = a_1 + \cfrac{1}{a_2+\cfrac{1}{a_3}} = a_1 + \cfrac{1}{\cfrac{a_2a_3+1}{a_3}}$

$= a_1 + \frac{a_3}{a_2a_3+1} =$ $p_3 = a_1a_2a_3 + a_1 + a_3$

$q_3 = a_2a_3+1$.

$= \frac{a_1a_2a_3+a_1+a_3}{a_2a_3+1}$

In this way the ~~general~~ 'formula' for general p_n, q_n may be quite complicated. However the following recursive equations hold in general.

$p_n = a_np_{n-1} + p_{n-2}$ $q_n = a_nq_{n-1} + q_{n-2}$. for $n \geq 3$.

eg $p_3 = a_3p_2 + p_1$ $q_3 = a_3q_2 + q_1$
$= a_1a_2a_3 + a_3 + a_1$ $= a_2a_3 + 1$.

Note that in our previous example, $a_i = 1$ for all i
ie the formula become $p_n = p_{n-1} + p_{n-2}$ $q_n = q_{n-1} + q_{n-2}$
leading to Fibonacci numbers.

Lets use these formula to retrieve the convergents of $1 + \cfrac{1}{1+\cfrac{1}{1+\ddots}}$

K	a_k	p_k	q_k
1	1	1	1
2	1	2	1
3	1	3	2
4	4	5	3
5	1	8	5
6	1	13	8
7	1	21	13
8	1	34	21

$\frac{p_1}{q_1} = 1 = \frac{1}{1}$ $\quad \frac{p_2}{q_2} = 1 + \frac{1}{1} = 2.$

Example: Similarly, lets try to compute some convergents of $1 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\ddots}}}$

K	a_k	p_k	q_k	p_k/q_k
1	1	1	1	1
2	2	3	2	1.5
3	2	7	5	1.4
4	2	17	12	$1.41\dot{6}$
5	2	41	29	1.41379 (5dp)
6	2	99	70	1.41429 (5d.p).

$\frac{p_1}{q_1} = \frac{1}{1}$

$\frac{p_2}{q_2} = 1 + \frac{1}{2} = \frac{3}{2}$

We may verify that the continued fraction given 'converges to' $\sqrt{2}$* by using the fact that we are dealing with a periodic continued fraction.

in general each such fraction is a solution of a quadratic equation.

For example in this case: Let $\theta = 1 + \cfrac{1}{2+\cfrac{1}{2+\ddots}}$

Let's 'isolate' the 'periodic part' say $x = \cfrac{1}{2+\cfrac{1}{2+\ddots}}$ $\quad (\theta = x+1)$

Then the continued fraction for x is 'self-similar': $x = \frac{1}{2+x}$

ie $2x + x^2 = 1$

$x^2 + 2x - 1 = 0$

Then $x = \frac{-2 \pm \sqrt{8}}{2}$

$= \frac{-2 \pm 2\sqrt{2}}{2}$

$= -1 \pm \sqrt{2}$

x is a positive number so here, $x = -1 + \sqrt{2}$. and $\theta = 1 - 1 + \sqrt{2} = \sqrt{2}$.

Example: Let us consider a slightly more 'complicated' periodic continued fraction $\vartheta = 1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{4 + \cdots}}}}$

$a_1 = 1$
$a_2 = 2 \quad a_3 = 4$
$a_4 = 2 \quad a_5 = 4$
$a_6 = 2 \quad a_7 = 4$
$\vdots \qquad \vdots$

$x = \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{4 + \cdots}}}}$ x is 'self similar': $x = \cfrac{1}{2 + \cfrac{1}{4 + x}}$

ie $x = \cfrac{1}{\frac{9 + 2x}{4 + x}} = \dfrac{4 + x}{9 + 2x}$

$9x + 2x^2 = 4 + x$

$2x^2 + 4x - 2 = 0$

$x = \dfrac{-4 \pm \sqrt{24}}{2}$

$x = -2 \pm \sqrt{6}$

x corresponds to positive number so here $x = -2 + \sqrt{6}$

So $\vartheta = 1 - 2 + \sqrt{6} = -1 + \sqrt{6}$.

Lets now prove that formulae ~~given~~ for convergents given earlier are valid.

Proposition:

Let p_n/q_n be the nth convergent for the continued fraction $a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}$

$n \geq 3$.

Then we may set $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$

Proof: By induction on n.

$n = 3$ $\quad \dfrac{p_1}{q_1} = \dfrac{a_1}{1} \quad \dfrac{p_2}{q_2} = \dfrac{a_2 a_1 + 1}{a_2}, \quad \dfrac{p_3}{q_3} = \dfrac{a_1 a_2 a_3 + a_1 + a_3}{a_2 a_3 + 1}$

$p_3 = a_3(a_2 a_1 + 1) + a_1 \qquad q_3 = a_2 a_3 + 1$
$\quad = a_3 p_2 + p_1 \qquad\qquad\quad = a_3 q_2 + q_1$

holds for $n = 3$.

Assume result holds for n: $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$

$\dfrac{p_{n+1}}{q_{n+1}} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \, a_n + \cfrac{1}{a_{n+1}}}}} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \, a_{n-1} + \cfrac{1}{b}}}$

$b = a_n + \dfrac{1}{a_{n+1}}$

So $\frac{p_{n+1}}{q_{n+1}}$ has the form of the nth convergent

So by inductive assumption $\frac{p_{n+1}}{q_{n+1}} = \frac{b p_{n-1} + p_{n-2}}{b q_{n-1} + q_{n-2}}$

$$= \frac{(a_n + \frac{1}{a_{n+1}}) p_{n-1} + p_{n-2}}{(a_n + \frac{1}{a_{n+1}}) q_{n-1} + q_{n-2}}$$

$$= \frac{(a_n a_{n+1} + 1) p_{n-1} + p_{n-2} a_{n+1}}{(a_n a_{n+1} + 1) q_{n-1} + q_{n-2} a_{n+1}}$$

$$= \frac{a_n a_{n+1} p_{n-1} + p_{n-1} + p_{n-2} a_{n+1}}{a_n a_{n+1} q_{n-1} + q_{n-1} + q_{n-2} a_{n+1}}$$

$$= \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}}$$

$$= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}}$$

$p_n = a_{n+1} p_n + p_{n-1}$ $\quad q_n = a_{n+1} q_n + q_{n-1}$ as required QED.

Today, we will try to show that the sequence of convergents $p_1/q_1, p_2/q_2 \dots$ converges.

Lets try to identify some relationship between nearby convergents.

For example consider $1 + \frac{1}{1 + \frac{1}{1 + \dots}}$ Then $\frac{p_1}{q_1} = \frac{1}{1}$ $\frac{p_2}{q_2} = \frac{2}{1}$ $\frac{p_3}{q_3} = \frac{3}{2}$ $\frac{p_4}{q_4} = \frac{5}{3}$ $\frac{p_5}{q_5} = \frac{8}{5} \dots$

Lets look at the difference between sucessive convergents:

$p_2/q_2 - p_1/q_1 = 1$

$p_3/q_3 - p_2/q_2 = -1/2$

$p_4/q_4 - p_3/q_3 = 1/6$ $\quad$ In general it seems that $|p_{n+1} q_n - p_n q_{n+1}| = 1$

$p_5/q_5 - p_4/q_4 = -1/15$

Also note that the sequence $p_1/q_1, p_2/q_2 \dots$ 'alternates' (bigger smaller).

Lets try to show that:

Proposition:

For any $n \in \mathbb{N}$ $p_{n+1} q_n - p_n q_{n+1} = (-1)^{n-1}$ for any continued fraction

Proof: Consider a general continued fraction and its n^{th} convergent p_n/q_n.

Let us prove this result by induction on n.

$n=1$ Consider: $p_2q_1 - p_1q_2$ where we may set $p_1 = a_1$ $p_2 = a_2a_1+1$
$q_1 = 1$ $q_2 = a_2$

Then $p_2q_1 - p_1q_2 = (a_2a_1+1)\cdot 1 - a_1\cdot a_2$
$= 1$
$= (-1)^2$

Lets now assume that the result holds for $n-1$

ie $p_nq_{n-1} - p_{n-1}q_n = (-1)^n$

Consider $p_{n+1}q_n - p_nq_{n+1} = (a_{n+1}p_n + p_{n-1})q_n - p_n(a_{n+1}q_n + q_{n-1})$
$= p_{n-1}q_n - p_nq_{n-1}$
$= -(p_nq_{n-1} - p_{n-1}q_n)$
$= -(-1)^n$
$= (-1)^{n+1}$

Using this we may obtain a 'formula' for the difference succesive ~~congeergents~~ convergents.

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^{n+1}}{q_nq_{n+1}}$$

From this we may deduce that the sequence of convergents alternates in the sense $\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \begin{cases} >0 & \text{if } n \text{ is odd} \\ <0 & \text{if } n \text{ is even.} \end{cases}$

In order to show convergence, we will consider the odd and even subsequences of $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3} \dots$

$$\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} = \frac{p_{n+2}q_n - p_nq_{n+2}}{q_{n+2}q_n} = \frac{(-1)^{n+1}a_{n+2}}{q_{n+2}q_n}$$ exercise.

This shows that the sequence of odd convergents is increasing

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \dots$$

and that the sequence of ~~odd~~ even convergents is decreasing

$$\frac{p_2}{q_2} > \frac{p_4}{q_4} > \dots$$

In fact we have an increasing sequence bounded above by p_2/q_2 and a decreasing sequence bounded below by p_1/q_1

Explanation: $\frac{p_{2n}}{q_{2n}} = a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_{2n}}} > a_1 = \frac{p_1}{q_1}$

$$\frac{p_{2n+1}}{q_{2n+1}} = a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{2n+1}}} < a_1 + \frac{1}{a_2} = \frac{p_2}{q_2}.$$

From here it ~~is easy to sho~~ may be shown that the sequence $p_1/q_1, p_2/q_2 \ldots$ converges.

~~The final~~

Representing Numbers as Sums of Squares.

In this final part of the course, we will try to obtain some results indicating which numbers can be written as sums of squares.

In the case where we are searching for numbers represented as squares, we obtain the square numbers 1, 4, 9, 16, 25, ...

In general: a natural number n may be expressed as a square number precisely when any prime factor of n has an even exponent in the prime factorisation of n.

Definition:

A natural number n may be expressed as a sum of two squares if there exists non-negative intergers x, y such that $n = x^2 + y^2$

eg. $25 = 5^2 + 0^2 = 3^2 + 4^2$ $\quad$ $5 = 1^2 + 2^2$, 7 may not be represented as sum of two squares.

$20 = 4^2 + 2^2$

$73 = 8^2 + 3^2$

71 may not be represented as a sum of two squares.

Lets now try to determine which numbers may be represented as sums of two squares.

We start with the simpler problem of trying to determine which prime numbers can be represented in this way.

$2 = 1^2 + 1^2$

3 $\times$

$5 = 1^2 + 2^2$

7 $\times$

11 $\times$

$13 = 3^2 + 2^2$

Note that 3, 7, 11 are all congruent to 3mod4

In general the following holds:

~~Proposition:~~

Proposition:

Let p be a prime number congruent to 3mod4. Then p cannot be represented as a sum of two squares.

Proof: Suppose that p satisfies $a^2+b^2=p$, for some non-negative integers a, b. Note that in such a case, since p is prime, neither of a, b can be zero.

Lets consider the equation mod p: $a^2+b^2 \equiv 0 \bmod p$.

Note: neither a, b can be congruent to 0 mod p.

Since $a \not\equiv 0 \bmod p$ the congruence class $\bar{a}$ has a multiplicative inverse mod p, a^{-1} say.

We deduce that $(a^{-1})^2(a^2+b^2) \equiv 0 \bmod p$

$$1+(a^{-1}b)^2 \equiv 0 \bmod p$$

$$(a^{-1}b)^2 \equiv -1 \bmod p.$$

Then -1 is a quadratic residue mod p.

This contradicts a result from earlier in the course, which shows that if $p \equiv 3 \bmod 4$, then -1 is not a quadratic residue mod p.

This contradiction implies that p cannot be expressed as the sum of two squares.

We may extend the above argument in order to prove the following result:

Proposition:

~~Let n be a natural number~~

Let p be a prime number ~~satisfying~~ congruent to 3 mod 4 and n be a natural number satisfying $n=p^{2k+1}m$, where p does not divide m. Then n cannot be represented as the sum of two squares.

Proof: By contradiction

Let n be a natural number satisfying $n=p^{2k+1}m$ $(p \equiv 3 \bmod 4,\ p \nmid m)$.

Suppose that $n=a^2+b^2$

Note that, since n is not a square number, neither of a and b is zero.

Lets suppose that n is the smallest number of the form $p^{2k+1}m$ that may be represented as a sum of two squares.

We first show that neither of a, b are multiples of p.

Lets assume that $a \equiv 0 \bmod p$ ie $a=a'p$

Then considering $n=a^2+b^2 \bmod p$, $0 \equiv 0+b^2 \bmod p$

$\Rightarrow b \equiv 0 \bmod p$

So if $a \equiv 0 \bmod p$ then $b \equiv 0 \bmod p$.

So $a=a'p$, $b=b'p$ for $a', b' \in \mathbb{N}$.

In this case we can find a smaller number that can be represented as a sum of two squares:

Dividing $p^{2k+1}m = a^2+b^2$ through by p^2

$$p^{2k-1}m = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 = (a')^2 + (b')^2$$

This contradicts the minimality of $n = p^{2k+1}m$.

So we can deduce neither of a or b are congruent to 0 mod p.

(As previously) $a^2+b^2 \equiv 0 \bmod p$

So $(a^{-1})^2(a^2+b^2) \equiv 0 \bmod p$

$1 + (a^{-1}b)^2 \equiv 0 \bmod p$

$(a^{-1}b)^2 \equiv -1 \bmod p$.

This contradicts that -1 is not a quadratic residue and proves the result.

Crucially the converse of this proposition holds in general.

Theorem:

A natural number n may be represented as a sum of two squares if and only if any prime number congruent to 3 mod 4 appears an even number of times in the prime factorisation of p.

A key component in our proof of this will be the following:

Proposition

Suppose that each of the natural numbers n, m may be represented as a sum of two squares: $n = a^2+b^2$, $m = c^2+d^2$.

Then the product mn may also be represented as a sum of two squares

Proof: Let $n = a^2+b^2$ $m = c^2+d^2$ for non-negative intergers a, b, c, d

$$\begin{aligned}\text{Then } (ad-bc)^2 + (ac+bd)^2 &= a^2d^2 - 2abcd + b^2c^2 + a^2c^2 + 2abcd + b^2d^2 \\ &= a^2d^2 + b^2c^2 + a^2c^2 + b^2d^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= mn.\end{aligned}$$

2 other ways of expressing this calculation:

1) use matrices to express result. $n = \det\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ $m = \begin{pmatrix} d & -c \\ c & d \end{pmatrix}$ ...

2) use complex numbers to express the result. $n = a^2+b^2 = (a+ib)(a-ib)$

ie $n = |a+ib|^2$

$m = |d+ic|^2$

Using the setting of complex numbers shows that there is a geometrical interpretation of sums of squares:

a natural number may be represented as a sum of two squares if and only if it is the square of the length of a complex vector with integer coeffs.

The previous proposition is useful in yielding representations of numbers as sums of squares

eg. $5 = 1^2+2^2$ $41 = 4^2+5^2$

Lets try to obtain representations of $5 \times 41 = 205$ as a sum of two sequences, using the previous result.

$5 = a^2+b^2$ $41 = c^2+d^2$

a	b	c	d	$\lvert ad-bc\rvert$	$\lvert ac+bd\rvert$
2	1	4	5	6	13
1	2	4	5	3	14

So we have found two ways of representing 205 as a sum of two squares

$205 = 6^2+13^2$

$205 = 3^2+14^2$

eg. $325 = 25 \times 13$

$25 = 5^2+0^2$ $13 = 3^2+2^2$

$= 3^2+4^2$

a	b	c	d	$\lvert ad-bc\rvert$	$\lvert ac+bd\rvert$	
5	0	2	3	15	10	$325 = 10^2+15^2$
0	5	2	3	10	15	$325 = 1+18^2$
3	4	2	3	1	18	$325 = 6^2+17^2$
4	3	2	3	6	17	

Note: We would obtain the same representations if we used other factorisations of 325.

$L(\Pi, \Omega)$ - structure consists of

- a non empty set U
- For each predicate symbol P of arity n in Π a relation or predicate of arity n in U denoted P_U.
- For each n-arity functional symbol F, an operation or functional in U, F_U say $F_U : U \to U$