# Notes - Math 115B

May 6, 2014

## 1/5

### Continuation of Math 115A

Some goals:

1. Theorem that every prime, $p$, has a primitive root.
2. quadratic residues. Theorem (Guass) whether $p$ is a quadratic $\mod q$ determined by whether $q$ is a quadratic $\mod p$. ($x$ is a quadratic $\mod p$ means $x \equiv y^2 \mod p$ for some $y$). Quadratic reciprocity.
3. Polynomial equations in integers and $\mod p$.

Some review: What primitive roots do for you.
Knowing that $\mod p$ arithmetic $(\mathbb{Z}/p)$ has a primitive root, $r$ (an element of order $p-1$) makes $(/p)^x \cong \mathbb{Z}/(p-1)$, a renaming or bijection that preserves important things.

| | | |
|---|---|---|
| $(\mathbb{Z}/p)^x$ | $\leftrightarrow$ | $\mathbb{Z}/(p-1)$ |
| $r^x$ | $\leftarrow$ | $x$ |
| $a$ | $\mapsto$ | $ind_r a$ |
| multiplication $ab$ | $\leftrightarrow$ | addition $x+y$ |
| exponentiation $a^y$ | $\leftrightarrow$ | multiplication $xy$ |
| addition | $\leftrightarrow$ | eh.... nothing simple |
| order of $a$, $ord_p a$ | $\leftrightarrow_{a \equiv r^x}$ | additive order, 1st $y$ such that $xy \equiv 0 \mod p-1$ or $y = \frac{p-1}{gcd(x, p-1)}$ |
| primitive root $b$ | $\leftrightarrow_{b \equiv r^y}$ | prime residue$y$ |

Therefore, $\exists \phi(p-1) = \phi(\phi(p))$ primitive roots.
Recall $\phi(n)$ = number of prime residues $\mod n$.
An example: 2 is a primitive root $\mod 11$.
$1, 2, 4, 8, 5, -1, -2, -4, -8, -5$
This corresponds to $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.
What does this mean?
$-1 \leftrightarrow \frac{p-1}{2}$ if $p$ is odd.
In this case, $r^{\frac{p-1}{2}} \equiv -1$ for any primitive root.
The equation $x^2 \equiv -1$, i.e. $x^4 \equiv 1$ and $x \not\equiv 1$ or $-1$, i.e. $x$ has order 4.
($x$ is like $i$, $i^2 \equiv -1$. It is fair to say $x \equiv i$.)
$\pm i \leftrightarrow \frac{p-1}{4}$ and $\frac{3(p-1)}{4}$ exists iff $\equiv 1 \mod 4$. primitive root theorem thus implies that if $p \equiv 3 \mod 4$, $p \not| n^2 + 1$. If $p \equiv 1 \mod 4$, $\exists n$ such that $p \equiv 1 \exists p | n^2 + 1$

# 1/7

We looked at consequences of the primitive root theorem.

Theorem:

1. If $p \equiv 1 \mod 4$, then $\mathbb{Z}/p$ has $i$ or solution to $x^2 \equiv -1 \mod p$.
2. If $p \equiv -1 \mod 4$, then $\mathbb{Z}/p$ does not have $i$.

(1) eventually gets you $p = a^2 + b^2$ if $p \equiv 1 \mod 4$ (and prime).
Note: $n = 21 \neq a^2 + b^2$.
part (1) of the theorem also says that $p|n^2 + 1$ for some $n$.
(2) $\implies$ theorem below.

Theorem: $\exists \infty$ many primes that are $1 \mod 4$.

Theorem: $\infty$ many primes

Proof: Suppose that there only exists $k$, a finite number, primes with $p_k$ being the largest prime..
Let $n = p_1 p_2 \dots p_k$. Then, $3 \leq n+1$ has some prime factors since $n+1 > p_k$, so CONTRADICTION!!!!

Theorem: $\infty$ many primes that are equivalent to $3 \mod 4$

Proof: Suppose that there only exists $k$, a finite number, primes that are equivalent to $3 \mod 4$ with $p_k$ being the largest.
Let $n = p_1 p_2 \dots p_k$.
Let's look at $4n - 1$. Of course, it's equivalent to $3 \mod 4$, so not all its prime factors are $1 \mod 4$ and none are $p_1, \dots, p_k$
Pretty much the same as the one above.

Not a Proof: For primes that are equivalent to $1 \mod 4$.
Let $n = p_1 p_2 \dots p_k$.
Looking at $4n+1$ or $n+1$ does not imply that that any of their factors are $1 \mod 4$, although happily their factors aren't $p_1, \dots p_k$
Real Proof: Let $n = p_1 p_2 \dots p_k$
Look at $4n^2 + 1$. None of its prime factors, $q$, are among $p_1, \dots, p_k$ want at least one $q$ to be $1 \mod 4$. Even better, they all are $q \neq 2$.
$q \not\equiv 3 \mod 4$ because as we said by part (2) of the theorem, if it were, then $q \not| (2n)^2 + 1 \implies \infty$ many primes equivalent to $1 \mod 4$.

Theorem: (prime number theorem) If $\pi(n)$ is the number of primes les than $n$, then $\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)}$

Let $\pi_{a_b}$ be the number of primes less than $n$ that are equivalent to $a \mod b$.
For each $b$, there are $phi(b)$ interesting choices of $a$, namely $a \perp b$.

Theorem(Dirichlet): If $a \perp b$, then $\lim_{n\to\infty} \frac{\pi_{a,b}(n)}{\pi(n)} = \frac{1}{\phi(b)}$
I have heard that $\pi_{i,j+1}(n)$ and $\pi 3, 4(n)$ are "unbalanced" in the sense $\pi_{3,4}(n) > \pi_{1,4}(n)$ usually or always.

Theorem: $\exists$ a primitive root $\mod p$

# 1/9

Theorem (Langrange): If $p$ is prime, $\alpha(x)$ is a integer polynomial of degree $n$, then $\alpha(x) \equiv \mod p$ has $\leq n$ incongruent solutions. ($\alpha(x) \neq 0$)

Compare with, In $\mathbb{Q}$ or $\mathbb{R}$, $\alpha(a) = 0$ has $\leq n$ solutions. In $\mathbb{C}$, $\alpha(x) = 0$ has exactly $n$ solutions counting repeats.

## Polynomials mod $p$ in general

If we say that $\alpha(x) \equiv \beta(x) \mod n$, it could mean that the coefficients are equivalent or the values are congruent.
They're not congruent situations. The former is the usual meaning and is stronger. The former implies the latter.
Example: $n = 2$. Let's claim that $x^2 + x \equiv 0 \mod 2$
There are only 2 cases, $0, 1$.
$0^2 + 0 \equiv 0$ and $1^2 + 1 \equiv 0$, so it's true.
They're not equivalent as polynomials.

## Proof of Lagrange's theorem

Uses induction on degree of $a$ and Primality Lemma
Primality Lemma - If $p|ab$, then $p|a$ or $p|b$.
Base case: Let $\deg(a) = 0$ where $a \not\equiv 0$.
We want to know that $a$ has at most 0 roots mod $p$.
This is true because $a(x) = b \mod c$ where $b \not\equiv 0$ has no solution since no matter what $x$ is, $a(x) \not\equiv 0$ since it is $\equiv b$.
Inductive case: We have $a(x)$, say $x = r$ is $a \mod p$ roots. Otherwise, if there is no $r$, we're done.
Then, $a(r) = b$, say I mean $=$ in $\mathbb{Z}$, $b \equiv 0 \mod p$ or $p|b$. We can change $a(x)$ to $\hat{a}(x) = a(x) - b$, doesn't change the situation. $r$ is an ordinary root of $\hat{a}(x)$.
$\hat{a}(x) = (x - r)c(x)$
$a(x) \equiv (x - r)c(x) \mod p$.
I claim that if $(s - r)c(s) \equiv 0 \mod p$ where $s \neq r$, then $c(s) \equiv 0 \mod p$.
Yes, this is true because $p \not| s - r$, so $p|c(s)$ or $\frac{1}{s-r}$ exists mod $p$.
$a(x) \equiv (x - r)c(x)$, so $\deg(a) = n$, $\deg(c) = $ n -1, $c(x)$ has $\leq n - 1$ roots.
Claim says $a(x)$ has the roots that $c(x)$ does. $p$ is at most one more, so $a(x)$ has $\leq n$ roots.

Theorem: A polynomial with coefficients in any field factors uniquely into irreducible polynomials.

Proof is similar to the unique factorication of integers last quarter. It's a bit more abstract, but the idea is still the same.

Recall, we will care about $x^k \equiv 1 \mod p$.
In general, $a(x) \equiv 0 \mod p$ is hard to solve when $p$ is big.
The $\leq \deg(a)$ solutions is only easy part.
What about $a(x) \equiv 0 \mod n$ where $n$ is not prime?
Example: $x^3 + x + 5 = 0 \mod 21$

From the chinese remainder theorem, $a(x) \equiv 0 \mod n \Leftrightarrow a(x) \equiv 0 \mod$ prime power factors of $n$
That still leaves $a(x) \equiv 0 \mod p^k$.
Note: mod 49 $\not\Leftarrow$ mod 7, BUT mod 49 $\implies$ mod 7.
So, from our example, $x^3 + x + 5 \equiv 0 \mod 49 \implies x^3 + x + 5 \equiv 0 \mod 7$.
So, our plan: solve mod $p^{k-1}$. First say $x \equiv r \mod p^k$. Then, lift $x \equiv r + tp^{k-1} \mod p^k$. $t$ exists mod $p$. This is called "Hensel lifting".

| Theorem(Hensel): the equation for $t$ is linear and uses $\frac{d}{dx}a(x)$. |
|---|

# 1/12

## Hensel lifting

We're looking at $a(x) \equiv 0 \mod p^k$ ($n$ to $p^k$ by the Chinese Remainder Theorem)
First, look at $a(x) \equiv 0 \mod p$ which could be hard. (when $p$ is small, it's not hard)
Lagrange says there is less than degree,a, solutions.
Then, work, by induction on k. The set from $k-1$ to $k$ is called "Hensel listing"
Suppose $a(r) \equiv 0 \mod p^{k-1}$
If we know $r \mod p^{k-1}$, pick some choice mod $p^k$, then all choices mod $p^k$ are $r + tp^{k-1}$ where $t$ exists for matters of mod $p$.
I'm thinking of some $a + b * 100 \mod 1000$. Then, $b$ exists for matters mod 10.
In general, if I have $b * k \mod n$ where $k, n$ are fixed, then $b$ exists for matters mod $\frac{n}{gcd(k,n)}$.
$b$ matters for mod 10 because $1000/100 = 10$

Example: $x^2 \equiv -1 \mod 5$, e.g. x = 2 works
Now, $x^2 \equiv -1 \mod 25$, Is $x \equiv 2 \mod 5$? Maybe.
If so, $x \equiv 2 + 5t \mod 25$. $t$ exists mod 5.
Despite the fact that we started with non-linear equation, $t$ is still linear even when lifting.
$x^2 \equiv (2 + 5t)^2 \equiv 4 + 20t + 25t^2 \equiv_? -1 \equiv 24 \mod 25$
Then, because 2 works mod 5, 5| constant parts of the equation.
Therefore,

$$\begin{aligned} 20t &\equiv -5 \mod 25 \\ 4t &\equiv -1 \mod 5 \\ t &\equiv -\frac{1}{4} \equiv 1 \mod 5 \end{aligned}$$

So, $x \equiv 7 \mod 25$ works.
Ok... so... what about mod 125?, mod $5^4$?

| part of Hensel's Lemma: $a(r + tp^{k-1}) - a(r) \equiv tp^{k-1}a'(r) \mod p^k$ |
|---|

In calculus, derivatives follows from sum and product rules and from $c' = 0$ and $x' = 1$ and induction.
Claim is $b(t, r) \equiv a(r + tp^{k-1}) - a(r) \mod p^k$ is "psuedo calculus" in the sense that the derivatives holds with a factor of $tp^{k-1}$
If $a(x) = c$, $b(x) = c - c = 0$.

If $a(x) = x$, $b(x) = x + tp^{k-1} - x = tp^{k-1}$
Product rule: We have $a_1(x), a_2(x), b_1(t,x), b_2(t,x)$.
Then, say $a_3(x) = a_1(x)a_2(x)$ and $b_3(t,x) =?$

$$\begin{aligned} a_1(x + tp^{k-1}a_2(x + tp^{k-1}) &\equiv (a_1(x) + tp^{k-1}a_1'(x))(a_2(x) + tp^{k-1}a_2'(x)) \\ &\equiv a_1(x)a_2(x) + tp^{k-1}(a_1'(x)a_2(x) + a_1(x)a_2'(x)) \end{aligned}$$

So, Hensel's lemma 1st form is true.
The second form is how you use this to solve things.
Have $a(r) \equiv 0 \mod p^{k-1}$, where $r$ is some lift, not necessarily $0 \mod p^k$
$a(r + tp^{k-1}) \equiv a(r) + tp^{k-1}a'(r) \equiv_? 0 \mod p^k$, so $a'(r)t \equiv_? -\frac{a(r)}{p^{k-1}} \mod p$
Hensel's lemma says the solution $\mod p^k$ amounts to $a'(r)t \equiv -\frac{-a(r)}{p^{k-1}} \mod p$
There are three cases:

1. $a'(r) \not\equiv 0 \mod p$, there is a unique solution for $t$. You can keep lifting forever from $p$ to $p^2$ to ...
2. $a'(r) \equiv 0$ and $a(r) \not\equiv 0 \mod p^k$. there is no solution.
3. both $\equiv 0$, $t$ can be anything.

Example: $x^2 \equiv -1 \mod 5$
$a(x) = x^2 + 1$ and $a'(x) = 2x$
$x \equiv 2 \mod 5$, $a'(2) = 4 \not\equiv 0 \mod 5$, so $\exists$ a unique lift $\mod 25, 125, \ldots$
Hensel also defined $p$-adic numbers, which are numbers in base $p$ with infinitely many digits to the left.

# 1/16

Ordinary numbers in $\mathbb{R}$ have finitely many digits to left, infinitely many digits to the right, carry rules for $+, -, \times$, optional minus sign, and different bases, $b$ represent the same $\mathbb{R}$.
We know that $\pi = 3.14159\ldots$
Definition: If $p$ is prime, $p$-adict number has infinitely many base $p$ digits to the left and finitely many to the right, and carries to the left set of all of those us written $\mathbb{Q}_p$, p-adic numbers
Those that have no digits to the right are $p$-adic integers, $\mathbb{Z}_p$
Note: $\mathbb{Z}_p \neq \mathbb{Z}/p$. $|\mathbb{Z}_p|$ is uncountable. $|\mathbb{Z}/p| = p$.

Example: $\mathbb{Z}_5$
$\ldots 0000_5 = 0$
$\ldots 0000034_5 = 34_5 = 19$
Let's say I have $\ldots 4444_5 + \ldots 0_5 = \ldots 0_5$. that means that $\ldots 444444 = 0$.
Can subtract anything from $\ldots 000_5$ in $\mathbb{Z}/p$
Therefore, minus signs are optional.
Another definition/explanation of $x \in \mathbb{Z}_p$ is that it's any consistant sequence of residues mod $p^k$ as $k \to \infty$

Example: I want $x \equiv 2 \mod 5, \equiv 22_5 \mod 25 \equiv 12, 222_5 \mod 125 \equiv 62$.
$x \in \mathbb{Z}$ is sometimes. $\mathbb{Z} \subseteq \mathbb{Z}_p$
This $x \equiv -\frac{1}{2}$ because $x \equiv -\frac{1}{2} \mod 5^k \ \forall k$
Jesus said $x^2 \equiv -1 \mod 5^k$ has two solutions for all $k$.

Therefore, it has two 5-adic solutions, so $x = \ldots 12_5$ solutions to $x^2 = -1 \in \mathbb{Z}_5$

**Theorem 1.** *$\mathbb{Z}_p$'s are all inequivalent rings, all inequivalent to $\mathbb{R}$ or $\mathbb{C}$*

Example: $\mathbb{Z}_5 \not\equiv \mathbb{R}$ because $i \in \mathbb{Z}$

**Theorem 2.** *$\mathbb{Q}_p$ is closed under division*

Actually, everything $\mathbb{Z}_p$ can divide by any $x$ such that $p \not| x$.
Can make $\mathbb{Z}_n$ for composite $n > 1$ too, but they don't add much to $\mathbb{Z}_p$'s.

# 1/21

$x \in \mathbb{Z}_p$ is like an integer except when it has infinitely digits to the left in base $p$.
Example: $\ldots 444_5 + \ldots 001_5 = \ldots 000_5$
As we can see, $\ldots 444_5 = -1$, $\ldots 001_5 = 1$, and $\ldots 000_5 = 0$

Example: $\ldots 12_5 * \ldots 12_5 = \ldots 44_5$
there exists a way to fill remaining digits, so that $x^2 = -1 \in \mathbb{Z}_5$
A $p$-adic integer, $x \in \mathbb{Z}_p$ is the same as any consistent set of residues $\mod p$, $\mod p^2$, ...
$x = \ldots 12_5$

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 7 \mod 25 \\ &\vdots \end{aligned}$$

Hensel lifting $p$-adically base $p$.
Lift $x^2 \equiv -1 \mod 5$

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 7 \mod 25 \end{aligned}$$

To get to $\mod 125$, as in the book, $x \equiv 7 + t25 \mod 125$

Recall, $\bar{n}$ has used for $\mod k$ value of $n$
$\ldots t12_5 \times \ldots t12_5 = \ldots \bar{2}t24_5 + \ldots t12_5 + \ldots t$ or $t + 1\bar{2}t$. Confusing? Yea... We end up ignoring the t's at the end anyway, since we only have three digits.
So, we have $4t \bar{+} 144_5$

If we wanted, $x^2 \equiv -1 \in \mathbb{Z}_5$, got $4t + 1 \equiv 4 \mod 5$
$t \equiv 2$.
Remember, $\ldots 44_5 \equiv -1$, which is why we wanted the digit, $4t + 1$ to be 4.

Other fun facts,

1. $\mathbb{Z}_n$, $n$ not prime
   $\mathbb{Z}_{p^k} \cong \mathbb{Z}_p$
   i.e. 2-adicts, and 8-addics are equivalent

2. Every $\mathbb{Z}_n$ is a commutative ring

3. $\mathbb{Q}_p$ is a field

4. If $n$ is not $p^k$, say $n = p_1^{k_1} p_2^{k_2} \dots p_a^{k_a}$, then by the Chinese Remainder Theorem, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1} \times \dots \times \mathbb{Z}_{p_a}$

Example: $\mathbb{Z}_{10} \cong \mathbb{Z}_5 \times \mathbb{Z}_2$ by the Chinese Remainder Theorem

$$\begin{array}{rcl} \text{a 10-adic integer} & \leftrightarrow & \text{a pair consisting of a 5-addic integer and 2-addict integer} \\ x \mod 1000 & \leftrightarrow & (x \mod 125, x \mod 8) \end{array}$$

## Mobius inversion

Leading to existence of primitive roots

Recall that $\mu(n) = \begin{cases} (-1)^{\text{number of prime divisors of } n} & \text{if } n \text{ is square-free} \\ 0 & \text{otherwise} \end{cases}$

Let $f(n)$ be some function.
Let $F(n) = \sum_{d|n} f(d)$ where $f(d)$ is a summatory function.
If we know $F(n)$, what's $f(n)$ for all $n$?
i.e. $f(9) = F(9) - F(3)$
i.e. $f(12) = F(12) - F(6) - F(4) + F(2)$. This is inclusion-exclusion with two subsets divisible by 6 and 4.

General inclusion-exclusion formula for sets:
Number of elements in $U$ not in $A_i$'s where $A_i$ is each subset of $U = \sum |A_i| - \sum |A_i \bigcap A_j| + \sum |A_i \bigcap A_j \bigcap A_k| - \dots$.
Mobius inversion is an adaptation of that.

$$\begin{aligned} f(n) &= F(n) - \sum_{p|n} F(\frac{n}{p}) + \sum_{p,q|n, \text{ but } p \neq q} F(\frac{n}{pq}) - \sum F(\frac{n}{pqr}) + \dots \\ &= \sum_{d|n \text{ and is square free}} (-1)^{\text{number of prime factors of } d} F(\frac{n}{d}) \end{aligned}$$

Back to the example,

$$f(12) = F(12) - F(6) + 0F(3) - F(4) + F(2) + 0F(1)$$

# 1/23

## More Mobius inversions

$f(n)$ is some function and $F(n)$ is the $f(n)$'s summatory function.
$F(n) = \sum_{d|n} f(d)$
You can also find $f(n)$ from $F(d)$ too. $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$
Most important point: You have a bijection between $f$ and $F$.

Example: Last quarter, we learn the following:

- $\tau(n)$ is the number of divisors of $n$
- $\sigma(n)$ is the sum of divisors of $n$
- $\phi(n)$ is the number of prime residues $\mod n$

$\tau(n)$ is the summatory function of $f(n) = 1$ ($\tau(n) = \sum_{d|n} 1$) , so $1 = \sum_{d|n} \mu(\frac{n}{d})\tau(d)$

$\sigma(n) = \sum_{d|n} d$, so $\sigma(n)$ is the summatory function of $f(n) = n$ making $n = \sum_{d|n} \mu(\frac{n}{d})\sigma(d)$.

What about $\phi(n)$?

**Theorem 3.** *The summatory function of $\phi(n)$ is $F(n) = n$, so $\phi(n) = \sum d|n\mu(\frac{n}{d})$*

example and idea: Let $n = 10$. The plan is to assemble $\mathbb{Z}/10$. From $\mathbb{Z}/d)^x$ for $d|a$.

*Proof.* If $a \in \mathbb{Z}/n, gcd(a, n) = d$ for $d|n$
Segregate $a$'s by this value. For each of them, there are $f(\frac{n}{d})$ choices for $a$ because $a = db$, $b \in (\mathbb{Z}/\frac{n}{d})^x$, so $n = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d)$ □

**Theorem 4.** *Primitive root theorem If $p$ is prime, then $\mathbb{Z}/p$ has a primitive root, $r$, an element of order $p - 1$.*
*Then, the elements of $\mathbb{Z}/p$ are powers of $r$.*
*Then, there are $\phi(p - 1)$ primtive roots, $r^x$ where $x \in (\mathbb{Z}/(p - 1))^x$.*

Actually, we'll go straight to this.
What we need for this proof:

1. Lagrange's theorem: We have $\leq$ degree of $a(x)$ solutions to $a(x) \equiv 0 \mod p$
2. Number of solutions to $x^{p-1} \equiv 1 \mod p$ is $p - 1$
3. The defintion of $f_p(n)$ and $F_p(n)$
4. The lemma that will be introduced later

**Definition 5.**
- *$f_p(n)$ is the number of residues of order $n \mod p$*
- *$F_p(n)$ is the number of solutions to $x^n \equiv 1 \mod p$ where $ord_p x|n$*

If you let $d = ord_p x$, definitions give us $F_p(n) = \sum_{d|n} f_p(d)$
Our goal is to show $(\mathbb{Z}/p)^x$ are a big circle, i.e.

$$\begin{aligned} F_p(n) = n \text{when } n|p-1 &\Leftrightarrow f_p(n) = \phi(n) \text{ when } n|p-1 \\ &\Leftarrow \text{Today's lemma} \\ &\Rightarrow \text{Mobius inversion} \end{aligned}$$

**Lemma 6.** *If $n|p - 1$, then $x^n \equiv 1 \mod p$ has exactly $n$ solutions.*

*Proof.* $x^{p-1} - 1 = (x^n - 1) \times a(x)$
On the left side, we have $p - 1$ solutions.
$x^n - 1$ has at least $n$ solutions.
degree of $a(x)$ is $p - 1 - n$
We know that $x^{ab} - 1 = (x^a - 1)(x^{ab-a} + x^{ab-2a} + x^{ab-3a} + \ldots + x^a + 1)$

□

Recall, $a$ is a quadratic residue $\mod p$ means that it's a square $\mod p$.

**Definition 7.** $\left(\frac{a}{p}\right) = \textit{Legendre symbol} = \begin{cases} 1 & \textit{if } a \textit{ is a quad residue and } a \not\equiv 0 \mod p \\ -1 & \textit{if } a \not\equiv 0 \mod p \textit{ and not quad residue} \\ 0 & a \equiv 0 \mod p \end{cases}$

# 1/26

## Quadratic residues

If $p$ is prime (and a large one), most $a(x) \equiv 0 \mod p$ are hard to solve or even to count solutions for computer with known algorithms.
$x^n \equiv 1 \mod p$ is a special and easy to count solutions.
The number is the $gcd(n, p-1)$. It is easy to find them too if you obtain a primitive root, $r$.
$x^n \equiv c \mod p$ is hard again even for most small $n$, i.e. $n = 3$.
Even counting solutions , even (I think) if you have a primitive root and can factor $p-1$.

How you use primitive roots.

$$\begin{aligned} (\mathbb{Z}/p)^x &\cong \mathbb{Z}/(p-1) \\ r^x &\leftarrow x \\ a &\mapsto ind_{r,p}a \end{aligned}$$

Why not take discrete logs?
$ind_{r,p}x^n \equiv n \times ind_{r,p}x \equiv ind_{r,p}c \mod p-1$
But this is hard to find! "Discrete logarithm problem"

BUT, $n = 2^m$ where $m \in \mathbb{N}$ is the big exception.
You can count solution to $x^2 \equiv c \mod p$ and even find them (Shanks - Tonelli).
Traditional and convenient form for two types of $c$ ($x^2 \equiv c$ has or doesn't have solutions) is Legendre symbol.
$\left(\frac{c}{p}\right) = \begin{cases} 1 & \text{if } c \perp p \text{ and two solutions} \\ -1 & \text{if } c \not\perp p \text{ and 0 solutions} \end{cases}$
In the former case, $c$ is quadratic residue. In the latter case, $c$ is non-quadratic residue. If $p|c$, we have two conventions.
$\left(\frac{c}{p}\right)$ is undefined or it's 0.

First properties

1. $\left(\frac{a}{b}\right)$ depends only on $a \mod p$. The real point: $f(a) = \left(\frac{a}{b}\right)$ is either a function on $\mathbb{Z}/p$ or an $\mathbb{Z}$. Both interpretations are important.

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. So, it's completely multiplicative in $a$.

For the second property, Not so hard if $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ are $1, 1$ or $1, -1$ or -1, 1. But, -1, -1?
If $a \equiv x^2$ and $b \equiv y^2$, then $ab \equiv (xy)^2$.
Interesting case, $a \not\equiv x^2$ and $b \not\equiv y^2$ (for any $x$ or $y \Rightarrow ab \equiv z^2$.

*Proof.* For the second property
Say we have primitive roots and $p$ is odd.
Then, $a \equiv x^2 \mod p$. Take logs and you get $j \equiv 2k \mod p-1$ where $a \equiv r^j$ and $x \equiv r^k$
If $a \equiv r^j$, then $(\frac{a}{p}) \equiv \begin{cases} 1 & \text{when } z|j \\ -1 & \text{when } z \not| j \end{cases}$
So, $(\frac{ab}{p}) \equiv (\frac{a}{p})(\frac{b}{p})$.
Then, just becomes addition of exponents $\mod 2$
So, $(\frac{a}{p}) = 1$ $\frac{p-1}{2}$ times.
This is also true because $x \mapsto x^2$ is 2-to-1 □

Back to the first property, $(\frac{a}{p})$ depends on $a \mod p$.
For example, $(\frac{10000}{31})$. You can divide and take the remainder.
Can you relate $(\frac{a}{p})$ to $\frac{p}{a}$?
Then, it would be step 1 towards an Euclidean type algorithm to compute $(\frac{a}{p})$

**Theorem 8.** *From Gauss.*
*If $p$ and $q$ are odd primes, then* $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
*I.e.* $(\frac{p}{q}) = (\frac{q}{p})$ *if at least 1 of $p$ and $q$ is* $1 \mod 4$
$(\frac{p}{q}) \neq (\frac{q}{p})$ *if* $p \equiv q \equiv 3 \mod 4$

# 1/28

Computational Context (Corrected)

1. Discrete logartihms are hard. If $a \equiv r^x \mod p$, solving for $x$.
2. Solving $a(x) \equiv 0 \mod p$ is not hard where degree of $a$ is low. i.e. For each fixed $k$, if degree($a$) $\leq k$ (*) gets harder only slowly as $p$ increases. It does polynomial time in number of digits of $p$, but it gets harder much faster as degree of polynomial increase.
   $x^2 \equiv c \mod p$, it's fast to count or find solutions.
   $x^3 \equiv c \mod p$, too and so is any $x^a \equiv c$.
   $x^k - c$ is moreever a special polynomial.
   Finding solutions is "Shanks-Tonelli". Counting solutions to these equations is due to Euler.

**Theorem 9.** *Euler*
$(\frac{a}{b}) \equiv a^{\frac{p-1}{2}} \mod p$

*Proof.* Take logarithms!
$a \equiv r^x \mod p$ where $r$ is a primitive root
We know that $(\frac{a}{p}) = \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd} \end{cases}$
$\frac{1}{2} = 1^2 \mod 2d$. Trivial case since we are looking at large prime numbers (which are odd).
$x$ exists $\mod p-1 = n$
$(x \mod 2)\frac{n}{2} = \frac{xn}{w} \times n$
So, $(r^x)^{\frac{n}{2}} = -1$ iff $x$ is odd.

Example: $r = 2$ and $mod 11$
$(2^x)^5$ is 180 degee times $x$ way around the circle. so, you get to top = 1 if $x$ is even and bottom = -1 if $x$ is odd.

□

By some type of argument, if $k|p-1$, then $a$ has a $k$th root $mod p$ iff $a^{\frac{p-1}{k}} \equiv 1 \mod p$.
What were curious about with $(\frac{a}{b})$, quadratic residues.
What digits can $n^2$ end in? $0, 1, 4, 5, 6, 9$ and not the others in base 10.

I.e. For what $p$ is $(\frac{2}{p}) = 1$?

| mod | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|---|
| $(\frac{2}{p})$ | -1 | -1 | 1 | -1 | -1 | 1 | -1 |

$6^2 \equiv 2 \mod 17$. Gauss amazing 1st step to replace exponents in Euler by products, products by sums.

**Lemma 10.** *Say $p$ is odd and $a \perp p$. Then, $(\frac{a}{p} = 1$ if an even number of least prime residues of $a, 2a, \ldots, \frac{p-1}{2}a$ are between 1(?) and $\frac{p-1}{2}$*
$(\frac{a}{p}) = (-1)^{\text{number of } aj\text{'s that are "2nd half" mod } p \text{ when } j \text{ is "1st half" mod } p}$

Example: $a = 3$, $p = 13$

| j | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $aj$ | 3 | 6 | 9 | 12 | 2 | 5 | 8 | 11 | 1 | 4 | 7 | 10 |

so... $(\frac{3}{13}) = (-1)^2 = 1$. Take the first $\frac{p-1}{2}$ $j$'s. Find all the residues of $aj$. Count all the number of residues of these that are $> \frac{p-1}{2}$.
Idea of the proof: Compare $1 * 2 * 3 * \ldots * \frac{p-1}{2} \equiv s$ and $a * 2a * 3a * \ldots * a\frac{p-1}{2} \equiv t$.

# 1/30

Quadratic reciprocity thm:
1st criterion and definition

"$a$ on $p$" $(\frac{a}{p}) = \begin{cases} 1 & \text{if there exists } x, \text{ a solution to } x^2 \equiv a^e \\ -1 & \text{if not} \\ 0 & \text{if p — a} \end{cases}$

2nd criterion is Euler's lemma: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \mod p$
3rd criterion is Gauss' lemma: $(\frac{a}{p}) = (-1)^s$ where $s$ is the number of left-half residues, $1 \leq j \leq \frac{p-1}{2}$, such that $a_j$ is the right half, $\frac{p+1}{2} \leq a_j \mod p \leq p-1$

*Proof.* Compare two products mod $p$.
$x \equiv 1 \times 2 \times \ldots \times \frac{p-1}{2} \mod p$
$y \equiv a \times (2a) \times (3a) \times \ldots \times ((\frac{p-1}{2})a) \mod p$
$\frac{y}{x}$ is, 1st of all, defined on mod $p$ ($p \not| x$).
$\frac{y}{x} \equiv a \times a \times \ldots \times a \equiv a^{\frac{p-1}{2}} \equiv (\frac{a}{p})$
$s$ is the number of left-half $j$'s with $a_j$ is the half.
Let $G = \{a, 2a, \ldots, \frac{p-1}{2}a\}$, all of which has a different equivalence mod $p$.
$|G| = \frac{p-1}{2}$. No two elements of $G$ are negatives either. $a_j \equiv -ak$, then $j \equiv -k$ can't happen if $j, k$ are left half.
this happens $s$ times, so $\frac{y}{x} \equiv (-1)^s$ also.
$(\frac{a}{p} \equiv \frac{y}{x} \equiv (-1)^s$ □

Example: $a = 3$, $p = 11$.
$x \equiv 1 \times 3 \times 3 \times 4 \times 5$

$y \equiv 3 \times 6 \times 9 \times 1 \times 4 \equiv 3 \times (-5) \times (-2) \times 1 \times 4 \equiv x \times (-1)^s$ with $s = e$ in this case.

**Theorem 11.** *Using Gauss's Lemma,*
$(\frac{2}{p}) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \mod 8 \\ -1 & \text{otherwise} \end{cases}$
$(\frac{-1}{p}) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$

*Proof.* $(\frac{-1}{p}) = (-1)^s$ where $s$ is $s = \frac{p-1}{2}$ in this case $= (-1)^{\frac{p-1}{2}}$

$(\frac{2}{p}) = (-1)^s$
i.e. $(\frac{2}{11}) =$ number of $1 \leq j \leq \frac{p-1}{2}$, such that $2j | \frac{p-1}{2}$ and $2j < p$
Let $s$ be the number of $\frac{p}{2} < 2j < p$ where $p$ is odd.
Then, the number of $2j < p$ is $\frac{p-1}{2}$ which is even if $p \equiv 1 \mod y$ and odd if $p \equiv 3 \mod 4$
Then, the number of $2j < \frac{p-1}{2}$ is $\lfloor \frac{p-1}{4} \rfloor$ which is even if $p \equiv$ odd $\mod 8$ and odd otherwise.
$s \equiv 0$ if $p \equiv 1$ or $7 \mod 8$ and 1 if $p \equiv 3$ or $5 \mod 8$ □

**Lemma 12.** *: Gauss Lemma*
$(\frac{a}{p}) = (-1)^s$ *where* $s \equiv \sum_{j=1}^{p-1} \lfloor \frac{2a_j}{p} \rfloor \mod 2$

# 2/2

## Gauss' Lemma

$(\frac{a}{b}) = (-1)^s$ where

$$\begin{aligned} s &= \text{number of left-half residues } j \text{ such that } a_j \text{ is right half} \\ &= \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{a_j}{p/2} \rfloor \mod 2 \end{aligned}$$

## Geometric Interpretation

Let $t = \lfloor \frac{a_j}{p/2} \rfloor$ be the number of lattice points inside of a triangle. (Lattice points are points with integer coordinates, $(x, y)$)
The triangle has vertices, $(0,0)$, $(\frac{p}{2}, a)$, $(\frac{p}{2}, 0)$
The slope of the line is $\frac{a}{p/2}$. The points on the hypotenuse is $\frac{a_j}{p/2}$.
The number of dots inside the column of $a_j$ is $\lfloor \frac{a_j}{p/2} \rfloor$ where $p \not| 2, a_j$.

**Lemma 13.** *Also, if $a$ is odd,* $s \equiv \sum_{j=1} \frac{p-1}{2} \lfloor \frac{a_j}{p} \rfloor \mod 2$

Want to show: $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.
Let $t_1 = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{qj}{p} \rfloor$
$t_2 = \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{pj}{q} \rfloor$
Then, $(\frac{p}{q}) = (-1)^{t_1}$ and $(\frac{q}{p}) = (-1)^{t_2}$ by Eisenstein's Lemma.
$(\frac{p}{q})(\frac{q}{p}) = (-1)^{t_1+t_2} =_? (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$

Using the geometric Interpretation again...
Think of a rectangle with x-length, $\frac{p}{2}$, and y-length, $\frac{q}{2}$. Let there be a diagonal of the rectangle with slope $\frac{q}{p}$. Count the lattice points. Bottom triangle has $t_1$ lattice points and upper triangle has $t_2$ lattice points.
The total number of lattice points in the rectangle is $\frac{p-1}{2}\frac{q-1}{2}$. The reason is because there is $\lfloor \frac{qj}{p} \rfloor$ on the columns of bottom triangle with endpoint on hypotenuse and $\lfloor \frac{pj}{q} \rfloor$ dots in row.

The only thing missing is a proof of Eisenstein's lemma itself.

**Lemma 14.** *Also, if $a$ is odd, $s \equiv \sum_{j=1} \frac{p-1}{2} \lfloor \frac{a_j}{p} \rfloor \mod 2$*

Conjecture: number of $j$'s such that $\lfloor \frac{aj}{p} \rfloor$ is odd. Working $\mod 2$
$a \equiv p \equiv 1$. Also, "$+ \equiv -$"
Following book, write $aj = p\lfloor \frac{aj}{p} \rfloor$ + remainder.
The remainder is either $1 \leq u \leq \frac{p-1}{2}$
What the remainders do: $r = aj\%p$, so as in Gauss' lemma, get each $u$ once.
Get $p$ $s$ times
So, let's sum $aj = p\lfloor \frac{aj}{p} +$ remainder over $1 \leq j \leq \frac{p-1}{2}$
$\sum_1^{\frac{p-1}{2}} aj = p\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{a_j}{p} \rfloor + p \times s + \sum_{u=1}^{\frac{p-1}{2}} u \mod 2$
You are then left with $\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{aj}{p} \rfloor + s \equiv 0 \mod 2$, so $s \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{aj}{p} \rfloor =$ Eisenstein's sum $\mod 2$.

So, where now?
Want Euclidean-style algorithm to compute $(\frac{a}{p})$, but what if $a$ isn't prime? Then, $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$, so if you can factor top, you're ok.

**Definition 15.** *$(\frac{a}{n})$, the Jacobi symbol is by definition $(\frac{a}{n}) = \Pi_k (\frac{a}{p_k})^{l_k}$ if $n = p_1^{l_1} \dots p_m^{l_m}$*

Not really comming from $\mod n$ arithmetic. Doesn't solve $a \equiv x^2 \mod n$ or count solutions.
It is defined, so that $(\frac{a}{b})(\frac{b}{a}) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$ when $a, b$ both are odd, even if composite

# 2/4

## The Jacobi symbol

If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, then $(\frac{a}{n}) = (\frac{a}{p_1})^{e_1} (\frac{a}{p_2})^{e_2} \dots (\frac{a}{p_k})^{e_k}$
Right hand side is the Legendre symbol and left side is the Jacobi symbol.
Legendre is only defined for odd primes.
If $gcd(a, n) > 1$, let it be 0. There is no particular interpretation at first.
This is set up so that quadratic reciprocity is still true and the laws for $(\frac{-1}{n})$ and $(\frac{2}{n})$

| Easier | Harder |
|---|---|
| Easy 1) $(\frac{ab}{c}) = (\frac{a}{c})(\frac{b}{c})$ | |
| Easy 2) $(\frac{a}{bc}) = (\frac{a}{b})(\frac{a}{c})$ | |
| $(\frac{a}{b})$ is completely multiplicative in $a$ and separately in $b$.A lot like dot products | |
| | Hard 1)$(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$ for odd $n$. |
| | Hard 2)$(\frac{2}{n}) = (-1)^{\frac{n-1}{8}}$ for odd $n$. |
| | Hard 3)Jacobi's reciprocity: $(\frac{a}{b})(\frac{b}{a}) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$ |

Why is Easy 2 true?
It's engineered by definition.
Prime factors of gc = (prime factors of b)(prime factors of c), so expanding ($\frac{a}{bc}$ gives same thing as expected: $(\frac{a}{b})$ and $(\frac{a}{c})$.

Why is Easy 1 true?
$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ is true for legendre symbol, so and these are factors of $(\frac{ab}{p})$, $(\frac{a}{p})$ and $(\frac{b}{bp})$.
So, let's check in $\mathbb{Z}$

| $p$ | $\frac{p^2-1}{8}$ | $(-1)^{\frac{p^2-1}{8}}$ |
|---|---|---|
| 1 | 0 | 1 |
| 3 | 1 | -1 |
| 5 | 3 | -1 |
| 7 | 6 | 1 |

$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ and $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ are other versions of the same trick. $p, q$ only matter $\mod 4$.

*Proof.* Hard 3
$(\frac{a}{b})$ by Easy 1 and Easy 2 is "bimultiplicative", just like an inner products is bilinear. $\langle ab\rangle = (\frac{a}{b})(\frac{b}{a})$ is also bimultiplicative just like an $i, p$ is determined by its values on a basis (which you make into a matrix).
$\langle\frac{a}{b}\rangle$ is determined by its values on primes.
$\langle\frac{p}{q}\rangle = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
So, $\langle\frac{a}{b}\rangle = \left[\frac{a}{b}\right]$ if $\left[\frac{a}{b}\right]$ is 1) bimultiplicative too and 2) has the same matrix.
Let $\left[\frac{a}{b}\right] = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$
Same matrix when $a = p$, $b = q$? Yes!
Is it bimultiplicative?
Is it true that $\left[\frac{ab}{c}\right] = \left[\frac{a}{c}\right]\left[\frac{b}{c}\right]$ and some on the other side? Yes, just check all eight cases $\mod 4$

□

This is really a proof by induction that $\langle\frac{a}{b}\rangle = (\frac{a}{b})(\frac{b}{c}) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$ using easy 1 and easy 2.
$\langle\frac{ab}{c}\rangle = \langle\frac{a}{c}\rangle\langle\frac{b}{c}\cdots$

$(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$ is the same plan: Both sides are multiplicative in $n$ and when $n$ is prime.

$\frac{a}{n}$ vs. Is $a$ a square mod n?
Say $n = p^2$ where $(\frac{a}{p^2}) = (\frac{a}{p})^2 = 1$, so... $a$ is not involved at all and we don't know whether $a$ is a quadratic residue or not.

Let's say that $n$ is square-free
$n = p_1 p_2 \dots p_k$ with all primes being different.
$a \equiv x^2 \mod n$ iff $(\frac{a}{p_j}) = 1$ for each prime factor.
$(\frac{a}{n} = 1$ iff $(\frac{a}{p_j} = -1$ for an even number of prime factors.

# 2/6

Why $(\frac{a}{b})(\frac{b}{a}) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$ when $a, b$ are odd and positive.

1. Both sides are bimultiplicative. The left side comes from defintion. The right side are cases mod 4
2. Equal when $a, b$ are prime, quadratic reciprocity

Likewise, $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$ and $(-1)^{\frac{n^2-1}{8}}$

1. Both sides are completely multiplicative
2. $=$ when $n$ is prime $\Leftarrow$ Gauss' Lemma, and in $(\frac{a}{n})$, $a$ only matters $\mod n \Rightarrow$ algorithm to compute Jacobi symbol $\Rightarrow$ Legendre symbol

According to the book $(\frac{a}{n})$ is defined when $n > 0$, $a < 0$, or $a > 0$
I disagree. Let $(\frac{a}{-1}) = 1$. Then, $(\frac{a}{-n}) = (\frac{a}{n})$ to make all of the laws still work.

Example: $(\frac{23}{101}) = (\frac{101}{23}) = (\frac{9}{23})$
The second step is bcause 101 is 1 $\mod 4$ and so is 9.
Now, $(\frac{9}{23}) = (\frac{23}{9}) = (\frac{5}{9}) = (\frac{9}{5}) = (\frac{4}{5}) = (\frac{-1}{5}) = (-1)^{\frac{s-1}{2}} = 1$

$(\frac{a}{b})$ what if $a$ or $b$ is even?
$(\frac{26}{101}) = (-\frac{75}{100}) = (\frac{-1}{100})(\frac{72}{100}) = \ldots$
Also, $(\frac{26}{100}) = (\frac{2}{101})(\frac{13}{1001}) = -(\frac{13}{101}))$
Since $(\frac{a}{b}) = \pm\frac{b}{a}$ when both odd, can reduce a mod b in $(\frac{a}{b})$, and $(-\frac{a}{b}) = (\frac{-1}{b})(\frac{a}{b})$ and $(\frac{2}{10}$ is known and $(\frac{2a}{b}) = \frac{2}{b} \Rightarrow$ a version of Euler's algorithm

Miller-Rabin is Miller's test choosing at random. It exposes that $n$ is composite of at least 3 quarters of the time. Then, $n$ is probably prime or is is definitely composite.

Special cases: Fermat numbers/primes.
Is $2^n + 1$ prime? If it is, either $n = 0$ or $n = 2^k$

Mersenne primes: Primes that are $2^n - 1$

**Theorem 16.** *If $f_k = 2^{2^k} + 1$ as fermat and $k > 0$.*
*Then, $a = 2$ is not interesting.*
*Then, $a = 3$ exposes composite $f_k$ for sure.*
*Then, in fact, $3^{\frac{f_k-1}{2}} \equiv -1 \mod f_k$ iff $f_k$ is prime.*

Why is $3^{\frac{f_k-1}{2}} \equiv -1$ when $f_k$ is prime. (if direction)

*Proof.*

$$\begin{aligned} 3^{\frac{f_k-1}{2}} &= (\frac{3}{f_k}) \text{ ( by euler's lemma)} \\ &= (\frac{f_k}{3}) \text{ (Quadratic reciprocity)} \\ &= (\frac{2^{2^k}+1}{3}) \\ &= (\frac{4^{2^{k-1}}}{3}) \end{aligned}$$

□

# 2/9

Jacobi symbol and primality tests for $n$.
Let's say $n$ odd.
If $n$ is prime,$p$, there are two ways to compile $(\frac{a}{n}) = (\frac{a}{p})$,

1. Euler's lemma, $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \mod p$
2. Extension of Euclidean algorithm, using quadratic residues of $p$

But if $n$ is composite, only have part 2 to compute $(\frac{a}{n})$.
Thus, a primality test (Solovay-Skossen).
If $n$ is prime, then $(\frac{a}{n}) \equiv a^{\frac{n-1}{2}} \mod n$
These could happen even if $n$ is not prime for some $a$.
If it happens (and $n$ is composite) $n$ is an "Euler pseudoprime".
Fact: If $a^{\frac{n-1}{2}} \equiv (\frac{a}{n}) \mod n$, then $a^{n-1} \equiv (\frac{a}{n})^2 \equiv 1 \mod n$.
Euler psuedoprime $\Rightarrow$ vanilla a-psuedoprime.
Miller's Test is stronger than Euler's test.

**Theorem 17.** *If $a$ is a Miller a-pseudoprime, then $a$ is a Euler a-pseudoprime.*

Let $2^j | n-1$ such that $\frac{n-1}{2}$ is odd.
Then, if $n$ is prime, $a^{\frac{n-1}{2^j}}, a^{\frac{n-1}{2^{j-1}}} \dots a^{n-1}$ is either all 1s or $\dots, -1, 1$.

The strategy for either test is chosen at random to make $n$ either composite for sure or probably prime.

**Theorem 18.** *(Miller-Rabin) At least $\frac{3}{4}$ of reults reveal $n$ to be completely by Miller's test.*

**Theorem 19.** *(Solovay-Strassen) At least $\frac{1}{2}$ of reults reveal $n$ to be completely by Euler's test.*

**Theorem 20.** *(Baby Solovay Strassen) If $n$ is composite, $\exists a \perp n$ such that $a^{n-1} \not\equiv (\frac{a}{n}) \mod n$*

*Proof.* say it wasn't so for some $n$.
$a^{n-1} \equiv 1 \mod n \ \forall a \perp n$, so $n$ is Carmichael.
$n$ is square-free and $p-1 | n-1$ when $p|n$
Say $p|n$, we supposed $a^{\frac{n-1}{2}} \equiv \pm 1 \mod p$.
Let $k = \frac{n-1}{p-1}$.
$a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$
$(a^{\frac{p-1}{2}})^k \equiv a^{\frac{n-1}{2}}$ and $k$ is odd because $a^{p-12}$.
So, where we are, $a^{\frac{n-1}{2}} \equiv a^{p-1}2 \mod p$ when $p|n$
By hypothesis, $a^{\frac{n-1}{2}} = (\frac{a}{n})$ and $(\frac{a}{p})$ by fact.
Therefore, $(\frac{a}{n}) = (\frac{a}{p}) \Rightarrow$ If $p, q | n$,then $(\frac{a}{p}) = (\frac{a}{q})$. This can't happen because $a$ is $\mod p$ of a $\mod q$. □

Example: Let $n = 561 = 3 \times 11 \times 17$. If this passed Euler's test, then $\forall a \perp n$, then 1) $n-1 = (p-1)k$ $\forall p | \overline{n \text{ and } 2)}$ $(\frac{a}{p}) = (\frac{a}{q})$.

## Rational and irrational numbers

We'll be doing this in $\mathbb{Q} \subseteq \mathbb{R}$ and in $\mathbb{Q}_p$.

**Theorem 21.** *$\alpha \in \mathbb{R}$ is rational iff it's a repeating decimal.*

*Proof.* Depends on how long division works. The algorithm determines by the remainder. If the remainder ever repeats, when you're pulling down 0s, then the whole algorithm repeats after that. Repeats must happen because there is only finite choices of remainders.

The converse.
If digits of $\alpha$ repeats, then $\alpha = \frac{a}{b}$.
2 cases:
1) Terminating decimals: Yes! Ex) 7.215 = 7215 / 1000 2) Repeating from start. $.99999999\ldots = 1$, $.001001\ldots = \frac{1}{999}$, and $.237237\ldots = \frac{237}{999}$ □

# 2/11

## Repeating decimals and fractions

fractions $\implies$ repeating decimal
Now, repeating decimal $\implies$ fraction

1. A terminating decimal is a fraction $\frac{a}{10^n}$ where $n$ is the number of digits. OR in base $d$, $\frac{a}{d^n}$
   Note: decimal points can be used to express $\alpha \in \mathbb{R}$ in any base.

2. Pure reptition, $0 < \alpha < 1$ and repeats from beginning.
   $\alpha = .$digits of some $k$, e.g., $\alpha = .237\overline{237}$, so $\frac{\alpha}{k} = .\overline{000\ldots1} = \frac{1}{10^n - 1}$

Finally, every $\alpha =$ terminating repeats from beginning.

Another argument that fraction implies repeating decimal is based on converse direction:
If $\frac{a}{b} = \frac{c}{99\ldots9} = \frac{c}{10^n - 1}$, then yes.
Claim is, this is possible if $b \perp 10$.
Another claim: $\exists n$ such that $b | 10^n - 1$, $10^n \equiv 1 \mod b$
Yes, $n = ab$, for instance, Euler's theorem.
In base $d$ $b \perp d$, then $d^{\phi(b)} \equiv 1 \mod b$, $(\frac{a}{b}) = (\frac{c}{d^n - 1})$.
What if $gcd(b, 10) > 1$ or $gcd(b, d) > 1$? Can we fix that by multiplying and dividing by the base.
Example: $\frac{1}{14} = \frac{1}{10}(\frac{10}{14}) = \frac{1}{10}(\frac{5}{7})$
A general, $\frac{a}{b} = \frac{1}{10^k}(\frac{b^k a}{b})$ if $k$ is big enough $\frac{10^k a}{b} = \frac{c}{d}$
All of this still works in $p$-adic number $\mathbb{Q}_p$ or even in $n$-adic number $\mathbb{Q}_n$.
$\mathbb{Q}_p$ is $\mathbb{Z}_p$ except with dividing by $p$ allowed and realized by finitely many digits to the right of the decimal.

Example: $\ldots444_3 = -1$
$\ldots111_5 = -\frac{1}{4}$
$\ldots334_5 = \frac{1}{4}$
$\frac{1}{4}\frac{1}{25} = \frac{1}{100} = \ldots333.34_5$
$\frac{1}{5} = .1_5$

**Theorem 22.** *In $\mathbb{Q}_p$ or even $\mathbb{Q}_n$. fraction $\Leftrightarrow$ repeating digits.*

$\mathbb{Q}_p$ is a field $\mathbb{Q}_{p^k} = \mathbb{Q}_p$
$\ltimes$ where $p, q|n$ has "zero division". $ab = 0$, $a, b \neq 0$. In $\mathbb{R}$, in base $p$, $\frac{1}{7} = .\overline{142857}$ and $-\frac{1}{7} = \ldots 142857$.

# 2/18

## Midterm question 1

$\ldots 777000_{10} = 1000 * \ldots 777_{10}$

## $p$-addic/$n$-addic convergence

of sequences or series
$\lim_{k\to\infty} x_k = x$ and $x_k, x \in \mathbb{Z}_p$ or $\mathbb{Z}_n$ means $\lim_{k\to\infty} d(x_k, x) = 0$ where $d(a, b) = 2^{-l}$ where $p^l$ or $n^l | a - b$ and $p^{l+1}$ or $n^{l+1} \nmid a - b$.

Example:
$\overline{a = 2375}008$
$b = 1375008$
$d_{\mathbb{R}}(a, b) = 10^6 =$ a lot
$d_{10}(a, b) = 2^{-6} =$ small. It converges 10-addicly.

## Geometryic series formula

$\sum_{k=0}^{\infty} ba^k = \frac{b}{1-a}$
Why don't we just test it out in 10-addictly?
$\sum_{k=0}^{\infty} 7 * 10^k = \frac{7}{1-10} = -\frac{7}{9}$, which is what it is! 10-adically right n-addic criterion is $d_n(a, 0) = a \ \forall a$.

**Theorem 23.** *: e is irrational where $e = 2 + \frac{1}{2} + \frac{1}{6} + \ldots = \sum_{n=0}^{\infty} \frac{1}{n!}$*

*Proof.* Use "factorial base": $xxxxxxxxxxxx.xxxxxxxx\ldots$
Everything to the left of the decimal point is base 10.
First place right of decimal point is base 2, next is base 3, next is base 4.
On the other hand, $e = 2.11111\ldots = 2 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \ldots$
On the other hand, if $\frac{a}{b}$ is rational, then $\frac{a}{b} = \frac{c}{b!}$ which terminates. e.g. $\frac{1}{5} = \frac{24}{120} = .0104_{fac}$.
Assume that an estimate. Let $\alpha \in \mathbb{R}$ and consider approximating $\alpha$ by $\frac{a}{b}$ except for $\alpha = \frac{a}{b}$
$\alpha \approx \frac{a}{b}$, but $\alpha \neq \frac{a}{b}$

□

**Theorem 24.** *If $\alpha \in \mathbb{Q}$, then $|\alpha - \frac{a}{b} > \frac{c}{b}$ depends on $\alpha$, but not b.*
*$|\alpha - \frac{a}{b}| =$ small with b not too big is called diophantine approximation.*
*In our case, $|\alpha - \frac{a}{b}| = \Omega(\frac{1}{b})$ where $\Omega(f(n))$ means $\geq cf(n)$.*

*Proof.* $\alpha = \frac{x}{y}$

$$\begin{aligned} |\frac{x}{y} - \frac{a}{b}| &= \frac{|xb - ay|}{yb} \\ &\geq \frac{1}{yb} \\ &= \Omega(\frac{1}{b}) \end{aligned}$$

□

Back to the proof

*Proof.* How well does $e$ work in $|\alpha - \frac{a}{b}|$?
To well
$S_n = \sum_{k=0}^{n} \frac{1}{k!} = \frac{a_n}{n!}$ is a close rational.
$e - s_n| = \frac{1}{(n+1)!} + \frac{(n+2)!}{+} \ldots < \frac{2}{n-1}! \neq \Omega(\frac{1}{n!})$, so $e \notin \mathbb{Q}$. □

**Theorem 25.** *If $\alpha$ is algebraic of degree $n$, then $|\alpha - \frac{a}{b}| = \Omega(\frac{1}{b^n})$*

# 2/20

## Irrational and transcendental numbers

$\alpha \in \mathbb{R}$ is algebraic means $f(\alpha) = 0$ for some polynomial with integer coefficients.
This generalizes root constructions.

**Theorem 26.** *If $f(\alpha) = 0$ where coefficients of $f$ are algebraic, then $g(\alpha) = 0$ where coefficients are integers.*

interesting ideas: $\pi$ is not algebraic. Even though it's from a circle, you use calculus to get the perimeter of the circle and areas of the circle.
$\alpha$ is transcendental if it is not algebraic.

**Theorem 27.** *Transcendental exists.*

**Theorem 28.** *$e$ and $\pi$ are transcendental.*

Proving $e$ and $\pi$ are irrational is very difficult, so we won't...

**Theorem 29.** *$2^\pi$ is irrational and transcendental.*

No one can prove this.
Let's say that $\alpha = \frac{a}{b}$. Then, $f(\alpha) = 0$ where $f(\alpha) = a - bx$, so rational numbers are algebraic.

Proof 1 of transcendental existence: Set $A$ of algebraic numbers is countable, but $\mathbb{R}$ is uncountable.
Computer Science approach to countability:
If $S$ is a set of elements described by finite words by a finite alphabet, then it's countable.
Order $s$ as words of length 1 in alphabetical order, then words of length 2 in alphbetical order, ....
If $x \in S$ has many names, just use the first one.

Example: $\mathbb{Q}$ is countable.
Alphabet: 0, 1, ..., 9, /, -.
Just use lowest term.
My dictionary: 0, 1, 2, 3, ..., 9, 10, 11, ..., 99, -1, ..., -9, 100, ..., 199, 1/2, ..., 1/9, 200, ..., ...

$\alpha \in \mathbb{R}$, algebraic, described by a word with alphabet: 0, 1, ..., 9, x, +, -, ;
For the polynomials, $\sqrt{2}$ is described by $xx-2;2$ where ; is the separator. The last 2 is the kth root from smallest to largest.
$xx-2;2$ means 2nd root of $x^2-2=0$.

Proof 2: If $\alpha \in \mathbb{Q}$, $|\alpha - \frac{a}{b}| > \frac{c}{b} = \Omega(\frac{1}{b})$ when $\alpha \neq \frac{a}{b}$
Let $\alpha = \frac{x}{y}$. $|\frac{x}{y} - \frac{a}{b}| = \frac{|xb-ya|}{by} \geq \frac{1}{by}$

**Theorem 30.** *If $\alpha$ is algebraic number of degree $n$, $|\alpha - \frac{a}{b}| \geq \frac{c}{b^n}$, so if we choose $\alpha$ very close to $\frac{a}{b}$, it's transcendental.*

**Theorem 31.** $x = .1100010000\ldots010\ldots01$
*Say fourth 1 is on the 24th digit and fifth one is at 120th.*
*Well...* $x = \sum_{n=1}^{\infty} 10^{-n!}$.
*Let* $x = \frac{a}{b}$ *where* $b = 10^{n!}$.
*Then,* $|\alpha - \frac{a}{b}| \approx 10^{-(n+1)!} \leq 2 \times 10^{-(n+1)!}$
$|\alpha - \frac{a}{b}| \geq \frac{c}{b^n}$

*Proof.* Idea is, if $f(x)$ is a polynominal of degree $n$, with coeffcients $\in \mathbb{Z}$ can bound $|f(\frac{a}{b})|$
$f(x) = x^3 - x + 1$, $|\frac{a^3}{b^3} - \frac{a}{b} + 1| = \frac{integer}{b^3} \geq \frac{1}{b^3}$.

□

# 2/23

## Prove that $e$ is irrational

$$e = 2 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \ldots$$

converges quickly.
The tail ¡ 1/ (denominator of partial sum)
In fact, The tail $< \frac{2}{n+1} \times 1/$ denominator of partial sum.

## 2nd proof of $e$ is irrational

If $\alpha \in \mathbb{Q}$, but $\alpha \neq \frac{a}{b}$.
$|\alpha - \frac{a}{b}| > \frac{constant}{b}$ contradicts tail $< \frac{2}{n+1}\frac{1}{b}$.

**Theorem 32.** *$\pi$ is irrational*

**Lemma 33.** *If $f(x)$ is a polynomial of degree $n$ with integer coefficients and $f(\frac{a}{b})$, then $|f(\frac{a}{b})| \geq \frac{1}{p^n}$*

*Proof.* Proof of the Lemma
Combine denomiators! Get some integer over $b^n$

i.e.$|3(\frac{a}{b})^3 - 2(\frac{a}{b}) + 7| = \frac{|3a^3+2ab^2+7b^3|}{b^3} \geq \frac{1}{b^3}$
Now, let $I_n = \int_0^\pi \frac{x^n(\pi-x)^n}{n!}\sin(x)$.
We know that $I_n > 0$, but less than $\frac{(\frac{\pi}{2})^{2n}}{n!}$
$I_n < \frac{\pi(\frac{\pi}{2})^2 n}{n!}$ as $n \to \infty$ goes to 0.
In fact, it goes very fast.

| $n$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $I_n$ | 2 | 4 | $24 - 2\pi^2$ | ... | ... |

□

**Lemma 34.** *$I_n$ is an integer polynomial in $\pi$. In fact, in $\pi^2 \Rightarrow \pi^2$ is irrational*

## Continued fraction

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

is called the continued fraction expansion of $\alpha$.

## Various theorems

All continued fractions converges to different $\alpha \in \mathbb{R}$ and every $\alpha \in \mathbb{R}$ is reached and c.f.e of $\alpha$ is finite iff $\alpha \in \mathbb{Q}$.

# 2/25

## Continued Fraction

A nice corollary to continued fraction

**Theorem 35.** *(by Dirchlet)*
*If $\alpha \notin \mathbb{Q}$ and $\alpha \in \mathbb{R}$, then $|\alpha - \frac{a}{b}| < \frac{1}{b^2}$ for infinitely many $\frac{a}{b}$*

**Theorem 36.** *If $\alpha \in \mathbb{Q}$, then $\exists C$ (depends on $\alpha$ only) such that $|\alpha - \frac{a}{b}|$ either is 0 or greater than $\frac{C}{b}$.*

Examples: $|\pi - \frac{22}{7}| = .00012\ldots < \frac{1}{49}$
$|\sqrt{2} - \frac{3}{2}| = .08\ldots < \frac{1}{4}$, not good enough
$|\sqrt{2} - \frac{7}{5}| = .014\ldots < \frac{1}{25}$.

Dirchlet's theorem is proven by continuous fractions.
Say that $\frac{a}{b}$ is a record setting approximation to $\alpha$ if $|\alpha - \frac{a}{b}| < |\alpha - \frac{c}{d}| \forall d < b$ and $\frac{a}{b} \neq \frac{c}{d}$.

Example: $\sqrt{2} \approx \frac{7}{5}$
$\frac{6}{4}$, $\frac{4}{3}$, $\frac{3}{2}$, and $\frac{1}{1}$ are still good approximation.

**Theorem 37.** *All record setting $\frac{a}{b}$ comes from continuous fraction expansion of $\alpha$.*

A continuation fraction is denoted by $[a_0; a_1, \ldots, a_n]$ (finite) or $[a_0; a_1, \ldots]$ (infinite).
Both means that

$$[a_0] = a_0$$

and

$$[a_0; a_1, \ldots] = a_0 + \frac{1}{[a_1, a_2, \ldots]}$$

More rigorously, if you chop a continuous fraction to $c_k = [a_0, a_1, \ldots, a_k]$.
Then, $[a_0, a_1, \ldots]$ is by definition $\lim_{k\to\infty} c_k$.

**Theorem 38.** *1.* $\lim_{k\to\infty} c_k$ *always exists*

*2. limits differ for two different continuous fractions*

*3. Every* $\alpha \in \mathbb{R}$ *is reached.*

Let's suppose all that. Take $\alpha \in \mathbb{R}$. Then,

$$\alpha = [a_0, a_1, \ldots] = a_0 + \frac{1}{a_1 + \ldots}$$

Say $\alpha = \sqrt{7} = 2.6\ldots$
$a_0 = 2$
Rules: $a_i > 0$ for all $i$. In $[a_0, \ldots, a_n]$, $a_n > 2$.
In fact, this shows part 2 by induction.

By this relation, if $\alpha = [a_0; a_1, a_2, \ldots]$, then $\frac{1}{1-\alpha_0} = [a_1; a_2, \ldots]$
Not a convergent. We chopped off head, not tail, so they're all unique.

$$\begin{aligned} \left\lfloor \sqrt{2} \right\rfloor &= 1 \\ \left\lfloor \frac{1}{\sqrt{2}-1} \right\rfloor &= 2 \\ \left\lfloor \frac{1}{\frac{1}{\sqrt{2}-1} - 2} \right\rfloor &= 2 \end{aligned}$$

**Theorem 39.** *If* $\alpha = \sqrt{n}$*, tne remainders in continued fraction expansion of* $\alpha$ *eventually reach* $\sqrt{n}+k$ *or* $\frac{\sqrt{n}+k}{2} \Rightarrow$ *continued fraction expansion repeats.*

**Theorem 40.** *Converse is true. If continuous fraction expansion of* $\alpha$ *repeats, then a is a root of* $ax^2 + bx + c = 0$*,* $a, b, c \in \mathbb{Z}$*.*
$\alpha = \frac{\sqrt{n}+d}{e}$

*Proof.* Suppose $\alpha = \frac{a}{b}$ is rational, then by the theorem, continued fraction expansion of $\alpha$ terminates. In fact, it's just the euclidean algorithm to compute $gcd(a, b)$. Max(a,b) in remainders keep decreasing.

$$\begin{aligned} \frac{a}{b} &= q + \frac{r}{b} \\ &= \frac{1}{\frac{b}{r}} \end{aligned}$$

where $q = \lfloor \frac{a}{b} \rfloor$.
Therefore, continued fraction expansion of $\frac{a}{b}$ terminates. □

# 2/27

## Continued fractions

Example:

$$[1; 1, 1, 1, 1, \ldots]$$

Estimates:

$$\begin{aligned} 1 + \frac{1}{1} &= 1 \\ 1 + \frac{1}{2} &= \frac{3}{2} \\ 1 + \frac{1}{\frac{3}{2}} &= \frac{5}{3} \\ 1 + \frac{1}{\frac{5}{3}} &= \frac{8}{5} \\ &\vdots \end{aligned}$$

This follows the fibonnaci sequence.

$$1 + \frac{1}{\frac{a}{b}} = \frac{b+a}{a}$$

Let's derive the limit independently.
If $[1; 1, 1, 1, \ldots] = x$, then $x = 1 + \frac{1}{x}$ and $x > 1$, then $x^2 = x + 1$.
Therefore, $\frac{1+\sqrt{5}}{2}$

Two important lessons from the example:

1. Always fibbonacci like recurrence for numerical denomination of $C_k$
2. If continued fraction of $c$ is periodic, then it is a quadratic equation for $x$.

**Definition 41.** *$[a_0, a_1, \ldots]$ is a simple continued fractions means $a_k \in \mathbb{Z}$. You can write it down for any values.*

Example: Not simple

$$e + \frac{1}{\pi + \frac{1}{\sqrt{2}}} = [e; \pi, \sqrt{2}]$$

**Lemma 42.** *(Fibbonaccish theorem) Let $s_{-1} = 1$, $s_0 = a_0$, $s_k = a_k s_{k-1} + s_{k-2}$, $t_{-1} = 0$, $t_0 = 1$, $t_k = a_k t_{k-1} + t_{k-2}$ where $k \geq 1$. Then, $C_k = [a_0; a_1, \ldots, a_k] = \frac{s_k}{t_k}$.*
*$C_k$ may not be a simple continued fraction and the fraction is sustanominal fraction.*

**Theorem 43.** *If $[a_0; a_1, \ldots, a_k]$ is simple, $\frac{s_k}{t_k}$ is lowest term and $s_k$ and $t_k$ are integers.*

*Proof.* By induction on $k$.
Suppose we know this for some $k$.

$$C_{k+1} = [a_0, a_1, \ldots, a_{k+1}] = [a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}]$$

Let $C'_k$ be the $k$th term of in the continued fraction.

$$\begin{aligned} C'_k &= \frac{a'_k s_{k-1} + s_{k-2}}{a'_k t_{k-1} + t_{k-2}} = \frac{s'_k}{t'_k} \\ &= \frac{(a_k + \frac{1}{a_{k+1}})s_{k-1} + s_{k-2}}{(a_k + \frac{1}{a_k+1})t_{k-1} + t_{k-2}} \\ &= \frac{a_k s_{k-1} + s_{k-2} + \frac{s_{k-1}}{a_{k+1}}}{a_k t_{k-1} + t_{k-2} + \frac{t_{k-1}}{a_{k+1}}} \\ &= \frac{a_{k+1}s_k + s_{k-1}}{a_{k+1}t_k + t_{k-1}} \\ &= \frac{s_{k+1}}{t_{k+1}} \end{aligned}$$

We just need the base case and we proved this. □

**Theorem 44.**

$$s_k t_{k-1} - s_{k-1} t_k = (-1)^{k-1}$$

*if* $[a_0, a_1, \ldots, a_k]$ *is simple.*

From this theorem, we know that $gcd(s_k, t_k) = 1$ where $gcd s_k t_k = 1$, $gcd(s_k, s_{k-1} i_= 1$, $gcd(t_k, t_{k-1}) = 1$.
The proof of this theorem is done by induction too.

One of the goals we're after, all simple continued fractions converge. We need the following lemma to prove it.

**Lemma 45.**

$$c_0 < c_2 < c_4 < \ldots < \ldots < c_5 < c_3 < c_1$$

*always happens in simple continuous fractions.*

The proof of this lemma is done with the previous theorem.

# 3/2

## Continued fraction

$\alpha = [a_0, a_1, a_2, \ldots]$
$c_k = \frac{s_k}{t_k}$. Somehow, found a recurrence for $s_k$, $t_k \Rightarrow s_k t_{k-1} - s_{k-1} t_k = (-1)^{k-1} \Rightarrow gcd(s_k, t_k) = 1$

## Matrix/slope point of view

A linear map or matrix on $\mathbb{R}^2$ takes lines to lines. Let's take the lines through 0 and so, it takes slopes to slopes.
Say

$$M = \begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix}$$

$M$ takes slope $x$ to $\frac{c+dx}{a+bx}$

$$\begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} \begin{bmatrix} 1 \\ \text{x} \end{bmatrix} = \begin{bmatrix} \text{a + bx} \\ \text{c + dx} \end{bmatrix}$$

A bit more standard:

$$M = \begin{bmatrix} \text{d} & \text{c} \\ \text{b} & \text{a} \end{bmatrix} \mapsto \frac{ax+b}{cx+d}$$

This kind of function of $X$ is called a Mobius transformation.
A fractional functions is linear transformation or mapping.
When you compose two Mobius function, $f_1$, $f_2$, you should multiply their matrices, you will get another Mobius function, $f_3$.
Note: You can throw in the slope, $\infty$

Note: Just so we don't confuse ourselves, we'll just have the matrices $\begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix}$ map to the fractional linear equation, $\frac{ax+b}{cx+d}$.

If

$$f(x) = \frac{ax+b}{cx+d}$$

then $f(\infty) = \frac{a}{c}$ and

$$\begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \text{a} \\ \text{c} \end{bmatrix}$$

In other words, it is still included in the map.

So, how is this related to continued fractions?
Say,

$$\alpha = [a_0; a_1, a_2, \ldots]$$
$$C_k = [a_0; a_1, a_2, \ldots, a_k]$$

Let

$$D_k = [a_1; a_2, a_3, \ldots, a_k]$$

which is basically $C_k$ with $a_0$ chopped off and $a_i$ moved to $a_{i-1}$ or in other words,

$$C_k = a_0 + \frac{1}{D_k} = \frac{a_0 D_k + 1}{1 D_k + 0}$$

In other words, it's a fractional linear transformation with matrix,

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix}$$

$C_k$ is then the slope of

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_2 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix}$$

These matrices multiply to

$$\begin{bmatrix} s_k & s_{k-1} \\ t_k & t_{k-1} \end{bmatrix}$$

The determinant are all -1, so the determinant of $C_k$ is $(-1)^{k+1}$ or $(-1)^{k-1}$.
Therefore, $s_k t_{k-1} - s_{k-1} t_k = (-1)^{k-1}$
The book's recurrence is

$$\begin{bmatrix} s_k & s_{k-1} \\ t_k & t_{k-1} \end{bmatrix} = \begin{bmatrix} s_{k-1} & s_{k-2} \\ t_{k-1} & t_{k-2} \end{bmatrix} \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix}$$

This implicitly uses that matrix multiplication is associative.

## Convergence of Convergents

$$\alpha = [a_0, a_1, \ldots]$$

except does the right side always converge?

$$\begin{aligned} C_0 &= a_0 \\ C_1 &= a_0 + \frac{1}{a_1} \\ C_2 &= a_0 + \frac{1}{a_1 + \frac{1}{a_2}} \\ &\vdots \end{aligned}$$

$C_0 <$ all subsequent numbers in the sequence.
$C_1 >$ every subsequent numbers because $a_1 < [a_1, \ldots]$ $C_0 <$ all subsequent numbers in the sequence.
To summarize, $C_0 < C_2 < \ldots < \ldots < C_5 < C_3 < C_1$
$\lim C_{2k}$ exists and $\lim C_{2k+1}$ exists. Are they equal?
They are equal iff $|C_k - C_{k+1}| \to 0$.

Let $C_k = \frac{s_k}{t_k}$

$$|C_k - C_{k-1}| = \frac{|s_k t_{k-1} - t_k s_{k-1}|}{t_k t_{k-1}} = \frac{1}{t_k t_{k-1}} \to 0$$

$\alpha$ is between two consecutive partial continued fractions, so

$$\alpha - C_k| < \frac{1}{t_k t_{k+1}} < \frac{1}{t_k^2}$$

So, we just got Dirchlet's thoerem.

# 3/4

$\alpha \approx \frac{a}{b}$ is "best" means that $\alpha - \frac{a}{b}| > |\alpha - \frac{c}{d}| \Rightarrow d > b$.

**Theorem 46.** *If $C_k = \frac{s_k}{t_k}$ is a convergent of $\alpha$, then it is the best. In fact, if there exists $\frac{a}{b}$ is better, $b \geq t_{k+1}$*

An even better theorem

**Theorem 47.** $|t_k \alpha - s_k| > |b\alpha - a| \Rightarrow b \geq t_{k+1}$
*If $b < s_k$ and $|t_k \alpha - s_k| > |b\alpha - a|$, then this is weaker than $\frac{a}{b}$ being closer*

## Periodic continued fractions

Suppose $\alpha = [a_0; a_1, a_2, \ldots, \overline{b_1, \ldots, b_l}]$.
Then, what can $\alpha$ be? The right side does converge can use this solve for $\alpha$.

**Lemma 48.** *$f(x) = [a_0; a_1, \ldots, x]$ is a fractional linear transformation.*

*Proof.*

$$a_k + \frac{1}{x} = \frac{a_k x + 1}{bx + 0}$$

□

Is 1 over a fractional linear transformation a fractional linear transformation? Yes
Is $a+$ fractional linear transformation a fractional linear transformation? Yes

$$\begin{aligned} a + \frac{jx+k}{lx+m} &= \frac{a(lx+m)+jx+k}{lx+m} \\ &= \frac{x(al+j)+(am+k)}{lx+m} \end{aligned}$$

Case 1: $\alpha = [b_0; b_1, \ldots, b_l]$, so

$$\alpha = b_0 + \cfrac{1}{b_1 + \cfrac{1}{1 + \ddots + \cfrac{1}{b_l + \cfrac{1}{\alpha}}}} = \frac{a\alpha + b}{c\alpha + d}$$

by the lemma.
$\alpha$ is a root of $x = \frac{ax+b}{cx+d}$, which is approximate to a quadratic equation.

General case: If $[b_0; b_1, \ldots, b_l] = \frac{a+b\sqrt{n}}{c}$.
Let $\alpha = [a_0, a_1, \ldots, a_k, \frac{a+b\sqrt{n}}{c}]$.

**Lemma 49.** *$\alpha$ is then also a quadratic irrational.*

*Proof.* $\frac{a+b\sqrt{n}}{c}$ is a quadratic irrational.
Then, is $d+$ a quadratic irrational = a quadratic irrational?

$$d + \frac{a + b\sqrt{n}}{c} = \frac{(a + cd) + b\sqrt{n}}{c}$$

Is $\frac{1}{\text{quadratic irrational}}$ = quadratic irrational?

$$\frac{c}{a + b\sqrt{n}} = \frac{(a - b\sqrt{n})c}{a^2 - b^2 n}$$

Yes! Therefore, by induction... □

## Diophantine equations

Have some polynomial equations, in some variables.
$x^2 + y^2 = z^2$, $x^2 + y^2 = z$, $x^3 + y^3 = z^3$, $x^2 + y^2 + z^2 = w$, $x^2 + y^2 + z^2 + w^2 = t$

**Theorem 50.** *It is impossible to analyze a general Diophantine equation.*

*Proof.* The difficulty of this problem is too much for us. □

**Theorem 51.** *If $A$ is a formal math conjecture, then there exists a polynomial, $p_A(x_1, \dots x_k) = 0$, computable directly from $A$ that has solutions in $\mathbb{Z}$ iff $A$ is true.*

**Theorem 52.** *If $A$ is a formal computer program, then there exists a $p_A(x_1, \dots x_n)$ whose positive values, $x_1, \dots, x_n \in \mathbb{Z}$ are the output of $A$.*

We have $x^2 + y^2 = z^2$ where $x, y, z \in \mathbb{Z}$. These are called Pythagorean triples.
Without loss of generality, let's just consider $x, y, z > 0$.
We want $gcd(x, y, z) = 1$ because otherwise, this is just trivial. The triples with $gcd(x, y, z) = 1$ are called primitives.

A plan:

$$(n+1)^2 - n^2 = 2n + 1$$

sometimes that odd number on the right are squares.
Examples: $4^2 + 3^2 + 5^2$
$5^2 + 5^2 + 13^2$
$24^2 + 7^2 + 25^2$
$40^2 + 9^2 + 41^2$

General formula: $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 + n^2$ where $gcd(m, n) = 1$

# 3/6

## Pythagorean triples

$x^2 + y^2 = z^2$ was studied by various ancient civilizations.
Formulae for Pythagorean triples:

$$x = m^2 - n^2$$
$$y = 2mnz = m^2 + n^2$$

Now, Fermat proposed $x^n + y^n = z^n$.
For each fixed $n$, it's Diophantine.
Very different behavior for different $n$ with something in common.

**Theorem 53.** *Fermat's Last "Theorem"*
*There are no non-trivial integer solutions to $x^n + y^n = z^n$.*

Have fun with the proof...

**Theorem 54.** *Fermat did solve this though*
*$x^4 + y^4 = z^4$ has no non-trivial solutions.*

If $n = 1$, $x + y = z$, then that's easy.
If $n = 2$, $x^2 + y^2 = z^2$, that's doable. Just Pythagorean triples
Let $n = ab$. Then, $(x^a)^b + (y^a)^b = (z^a)^b$. This is a special case of $x^b + y^b = z^b$.
This reduces the cases to primes of power 4 and $n$ is prime.

No solutions to $a^2 + b^2 + c^2 = 7$
There's also no solutions to $\mod 8 \Rightarrow$ no solutions.
Let's look at $x^2 + y^2 = z^2$ and $gcd(x, y) = 1$.
Quadratic solutions of $\mod 4$ is $0, 1$.
With $0 + 0 = 0$ and $1 + 1 = 2$, they aren't interesting.
$1 + 0 = 1 = 0 + 1$
Without loss of generality, $x$ is odd and $y$ is even.

Using the formulae of pythagoren triples:

$$\begin{aligned} x^2 &= (m^2 - n^2)^2 \\ &= m^4 - 2m^2n^2 + n^4 \\ y^2 &= 4m^2n^2 \\ z^2 &= (m^2 + n^2)^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= x^2 + y^2 \end{aligned}$$

If $gcd(m, n) = d$, then $d^2|(x, y)$. We want $gcd(m, n) = 1$, then $gcd(x, y) = 1$.

Say $gcd(m, n) = 1$.
Say $p|y = 2mn$
If $p = 2$, then $p \not| x = m^2n^2$ and $x \equiv 1 \mod 2$.
If $p|m$, then $p \not| n$, so $x \equiv n^2 \not\equiv 0 \mod p$.

**Theorem 55.** *If $x^2 + y^2 = z^2$ with $gcd(x, y) = 1$ and $2|y$, then $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$.*

*Proof.* Let $y^2 = z^2 - x^2 = (z + x)(z - x)$.
Claim: $gcd(z - x, x + z) = 2$.
First of all, we know that $2 \not| x, z$, so it is at least 2.

$$gcd(x + z, z - x) = gcd(x + z, 2z)$$

If $p$ is odd — $2z$, then $p|z$. Then, $p \not| x$.
Then, $p \not| x + z$.

$$\begin{aligned} y^2 &= (x + z)(z - x) \\ &= 4\frac{x + 2}{2})\frac{z - x}{2} \end{aligned}$$

$$(\frac{y}{2})^2 = (\frac{x + z}{2})(\frac{z - x}{2})$$

By unique factorization, $\frac{x+z}{2} = m^2$ and $\frac{z-x}{2} = n^2$.
So, we have the following three equations:
$(\frac{y}{2})^2 = m^2n^2$
$\frac{z+x}{2} = m^2$
$\frac{z-x}{2} = n^2$

First equation gets you $y$ If we add the latter two equations, you get $z$ If we subtract the latter two equations, you get $x$ □

# 3/9

## Pythagorean triples and Fermat's last theorem

The solution: $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, $gcd(m, n) = 1$, $m$ and $n$ are not both odd, and $gcd(x, y) = 1$.

If $d|m, n$, then let $m' = \frac{m}{d}$, $n' = \frac{n}{d}$, $x' = \frac{x}{d^2}$, $y' = \frac{y}{d^2}$, and $z' = \frac{z}{d^2}$.

If $m, n$ are both odd, $m' = \frac{m+n}{2}$, $n' = \frac{m-n}{2}$, $x' = \pm\frac{y}{2}$, $y' = \pm\frac{x}{2}$, and $z' = \frac{z}{2}$.
Suggestive alternate formula:

$$x + iy = (m + in)^2$$
$$z = |m + in|^2 = (m + in)(m - in)$$

Official (lame) full solution:

$$x = k(m^2 - n^2), y = 2kmn, z = k(m^2 + n^2)$$

Another proof:

*Proof.* $x^2 + y^2 = z^2$ is a homogenous Diophantine equations.
Solutions in $\mathbb{Z} \leftrightarrow$ solutions in $\mathbb{Q} \leftrightarrow$ solutions to $x^2 + y^2 = 1$. □

## Open Problem

Are $\mathbb{Q}$ Diophantine equations computationally universal and/or mathematically universal? (like $\mathbb{Z}$ diophantine equations are)

Example:

$$\begin{aligned} x^2 + y^2 = z^2 &\leftrightarrow x^2 + y^2 = 1 \\ 3^2 + 4^2 = 5^2 &\leftrightarrow \left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1 \end{aligned}$$

What is the solution to $x^2 + y^2 = 1$? A unit circle centered at the origin.
Suppose that $x$ and $y$ are rational. Suppose I form a line between $(0, 1)$ and $(x, y)$, is the slope of the line rational? Yes! In fact, the slope, $s$, is $\frac{y-1}{x}$.

If $s \in \mathbb{Q}$, then $(x, y) \in \mathbb{Q}^2$ because you have a quadratic equation such that one solution, $(0, 1)$, is rational.
$x^2 + y^2 = 1$ and $y = xs + 1$, so
$x^2 + (sx + 1)^2 = 1$, $x^2 + s^2x^2 + 2sx + 1 = 1$
We then have $(1 + s^2)x + 2s = 0$, so $x = \frac{-2s}{1+s^2}$.
Then, $y = sx + 1 = \frac{1-s^2}{1+s^2}$.
Let $s = \frac{n}{m}$, then $x = \frac{-2mn}{n^2+m^2}$ and $y = \frac{m^2-n^2}{m^2+n^2}$. Although a few cosmetic errors, we can fix it to look like what we're looking for.

This is the same idea that works for any diophantine equations. with any quadratic(x,y,z) = 0, which is homogenous and such that you know one solution.
Example: $3x^2 + 4y^2 = 7z^2$. A solution, $(1, 1, 1)$ and this is homogenous since all the terms are quadratic.

$3x^2 + 4y^2 = 7$ forms the ellipse. $s \in \mathbb{Q} \leftrightarrow (x, y) \in \mathbb{Q}^2$.

## A case of Fermat's last theorem

$x^4 + y^4 = z^4$ has a no non-trivial solutions. Proved by "infinite descent." Solution $\Rightarrow$ a smaller solution. This is a contradiciton with a form of induction.

What we actually show by induction is $x^4 + y^4 = z^2$ and $4yx^4 + y^2 = z^4$ have no solutions.

# 3/11

**Theorem 56.** *$x^4 + y^4 = z^4$ has no non-trivial solutions.*

Hard to prove alone.

**Theorem 57.** *$x^4 + y^4 = z^2$ and $4x^4 + y^2 = z^4$ has no trivial solutions.*

Proof is by "infinite descent", i.e. solution implies a smaller solution.
Basically, it's a contraction in the form of an induction or "attack the smallest counterexample."

These are Pythagorean tripes, $(x^2, y^2, z)$ and $(2x^2, y, z^2)$.
In $x^4 + y^4 = z^2$, can we make $(x^2, y^2, z)$ a primitive triple?
$gcd(x^2, y^2) = 1 \leftrightarrow gcd(y^2, z) = 1 \leftrightarrow gcd(x^2, z) = 1 \leftrightarrow$ primitive.

If $gcd(x^2, y^2) = d^2$, then $x' = \frac{x}{d}$, $y' = \frac{y}{d}$, and $z' = \frac{z}{d^2}$.
Therefore, $(x^2, y^2, z)$ is primitive.
All primitive pythagoren triples are $odd^2 + even^2 = odd^2$.
Let's switch $x, y$ if necessary.

$$\begin{aligned} x^2 &= m^2 - n^2 \\ y^2 &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $gcd(m, n) = 1$ and one of $m, n$ is odd, the other even and $x$ is odd.
We also know that $n^2 + x^2 = m^2$ is another pythagorean triple, so $n$ has to be even and $m$ is odd.

Then, $y^2 = 2mn$. That means that $m \perp 2n$. This implies $m = s^2$ and $n = 2t^2$.
Combining them, I get $4t^2 + x^2 = s^4$ where $min(x, t, s) < min(x, y, z)$.

Say we have $4x^4 + y^2 = z^4$
Could $z$ be even and $x$ be odd? Let's say no.

If $gcd(x, z) = d > 1$, then let $x' = \frac{x}{d}$, $z' = \frac{z}{d}$, and $y' = \frac{y}{d^2}$ by induction, so $x \perp z$, so $x^2 \perp z^2$ and $2x^2 \perp z^2$.

So, $(2x^2, y, z^2)$ is primitive by induction.
Now, we know that

$$\begin{aligned} 2x^2 &= 2mn \\ y &= m^2 - n^2 \\ z &= m^2 + n^2 \end{aligned}$$

Then, $x^2 = mn$. If $m \perp n$, then $m = s^2$ and $n = t^2$, so $z^2 = s^2 + t^2$.

## Gaussian integers

Motivation: If $x^2 + y^2 = z^2$, then $(x + iy)(x + iy) = z^2$.
If we could say $x+iy \perp x-iy$, then presumably $x+iy = (m+in)^2$, which is the formula for Pythagorean triples.

What does the relative prime for complex integers mean?

**Definition 58.** *Let $\mathbb{Z}$ be the set of integers.*
*Let $\mathbb{C} \cong \mathbb{Z}[i]$ be the Gaussian integers. Gaussian integers are $\{x + iy | x, y \in \mathbb{Z}\}$.*

$5 = (2 + i)(2 - i)$ in $\mathbb{Z}[i]$. 5 is not a Guassian prime.
$3 = i(-3i)$ is not a reasonable factorization. 3 does not factor to "shorter" numbers. It is a Gaussian prime.

**Definition 59.** *1, -1, $i$, $-i$ are called units.*
*If $z \in \mathbb{Z}[i]$ does not factor except as $z = u \cdot z'$, then it is a Gaussian prime.*

**Theorem 60.** *1. $\mathbb{Z}[i]$ have unique factorization*

*2. The primes are $p \in \mathbb{Z}$ such that $p = 3 \mod 4$ and $a + it$ where $a^2 + b^2 = p \equiv 1 \mod 4$*

# 3/13

## Gaussian integers

**Definition 61.** *If $u \in \mathbb{Z}[i]$ has a reciprocal $u^{-1} \in \mathbb{Z}[i]$, then it's a unit.*

So, which elements is that?

**Definition 62.** *If $z \in \mathbb{Z}[i]$, $N(z) = |z|^2 = x^2 + y^2 \in \mathbb{Z}$ where $z = x + iy$.*

Note: $N(z)$ is the number theorists norm and $|z|$ is the analyst norm.
Note: $N(z) = 0 \Leftrightarrow z = 0$.
Note: $z|N(z)$ as Gaussian integers because $N(z) = z \cdot \overline{z} = (x + iy)(x - iy)$.
Note: $z \in \mathbb{Z}[i] \Leftrightarrow \overline{z} \in \mathbb{Z}[i]$.
Note: $N(z_1 z_2) = N(z_1)N(z_2)$

**Theorem 63** (Unique Factorization of Gaussian integers)**.** $\mathbb{Z}[i]$ *have unique factorization into Gaussian primes.*

In fact, if $u$ is a unit, $z \approx uz$. $z$ and $uz$ are associates.

Associate primes are equivalent in the sense of factorization.
Example: Is 2 square free in $\mathbb{Z}[i]$?
$2 = (1+i)(1-i)$
Are there repeats? Yes! $(1-i) = -i(1+i)$
Therefore, $2 = i(1+i)^2$
Therefore, 2 is not square free.

Why are we caring about units? In the past, we can just restrict everything to positive numbers. Now, we can't.

## Why $\mathbb{Z}$ has unique factorization?

For uniqueness, division with remainders, which led to euclidean algorithm, which led to primality lemma, which led to unique factorization.
All of our implications are inevitably provided, you get it started.

As for the existence, you have this if elements have a size which decreases when you factor.

Does $N(z)$ have a positive integer size such that if $z = ab$ where $a, b$ are not units, so that $N(a), N(b) < N(z)$? Yes!
$N(z) = N(a)N(b)$ and $N(a), N(b) \geq z$.

Example: $2 = (1+i)(1-i)$ where $N(2) = 4$ and $N(1+i) = 2$.

## Division with remainders

We want the following: Given $a, b \in \mathbb{Z}[i]$, $a = qb + r$ such that $N(r) < N(b)$.
In the Cartesian coordinates, multiplying by $b$ dilates by $|b|$ and rotates by the angle of $b$, which is known as $Arg(b)$.

Example: $b = 2 + i$.

# 3/16

$\mathbb{Z}[i]$ has division with "good" remainders.
$a = qb + r$ with $N(r) < N(b)$.
$q, r$ are not unique, but that's ok.

## A systematic way of finding Gaussian factors

Let $a = 7$ and $b = 2 + i$.
$\frac{7}{2+i} = \frac{7(2-i)}{5} = \frac{14-7i}{5}$.
Round up for $\frac{14}{5}$ since it's closer and round up for $\frac{-7i}{5}$ since it's closer to that area, so we have $3 - i$.
So, $7 = (3 - i)(2 + i) - (i)$.

Division implies Euclidean algorithm.
"$\mathbb{Z}[i]$ is a Euclidean domain"
This implies strong gcd. Given $a, b$, $\exists c, d$ such that $ac + bd = gcd(a, b)|a, b$
If $p$ is prime, $p|ab \Rightarrow p|a$ or $p|b$.

*Proof.* Suppose $p \not| a$ and $p \not| b$.
And so, $c_1p + d_1a = 1$ and $c_2p + d_2b = 1$.
Multiply by each other and you get something like...
stuff $\cdot p + d_1d_2ab = 1$. □

This then implies unique factorization.
What are Gaussian primes?

1. When $z$ is Gaussian primes, $z \approx \overline{ez}$

2. If $z$ is a Guassian prime (or any Gaussian integer), then $z|N(z) = z\overline{z}$
   Number of $\mathbb{Z}$ less than the number of $\mathbb{Z}[i]$ factors.
   So, $N(z) = p$, a vanilla prime and $p = (a + ib)(a - ib) = a^2 + b^2$ or $N(z) = p^2 = p$.
   So, finding Gaussian primes, amounts to $p = a^2 + b^2$.
   If $p \equiv 3 \mod$ , then $p \neq a^2 + b^2$, so $p$ is a Gaussian prime if $p \equiv 3 \mod 4$.

**Theorem 64.** *If $p \equiv 1 \mod 4$, then $p = a^2 + b^2$.*

*Proof.* Recall that if $-1 \equiv n^2 \mod p$ if $p \equiv 1 \mod 4$.
$p|n^2 + 1 = (n + i)(n - i)$
Does $p|n + i$. No! $p \not| 1$. □

**Theorem 65.** *$n = a^2 + b^2$ iff $\forall p \equiv 3 \mod 4$, number of factors of $p \cdot n$ is even.*