Math 4400

$\mathbb{N} = \{0, 1, 2, \dots\}$

§1: Induction

A very useful tool in mathematics! It has a few guises.

- 'Weak induction': ~~let~~ for each natural number n, let $P(n)$ be a proposition (ie sentence) depending on n. If
  - $P(0)$ is true, and
  - For all k in $\mathbb{N}$, if $P(k)$ is true then so is $P(k+1)$,

  Then $P(n)$ is true for all natural #s n.

Think: dominos! If each domino knocks down the next, and if I knock down the first domino, then all the dominos will be knocked down.

E.g. For all n, The sum of the first n odd numbers is n^2. I.e. $\sum_{j=1}^{n} (2j-1) = n^2$

$$\sum_{j=1}^{n}(2j-1) = 1+3+5+\dots+2n-1$$

<u>Proof</u>: Let's use induction! Here the proposition that we want to show is true for all n is:

$$P(n) = \text{"} \sum_{j=1}^{n} (2j-1) = n^2 \text{"}$$

"base case"

start w/ 1?

$$P(0): \quad \sum_{j=1}^{0} (2j-1) = \text{empty sum} = 0.$$

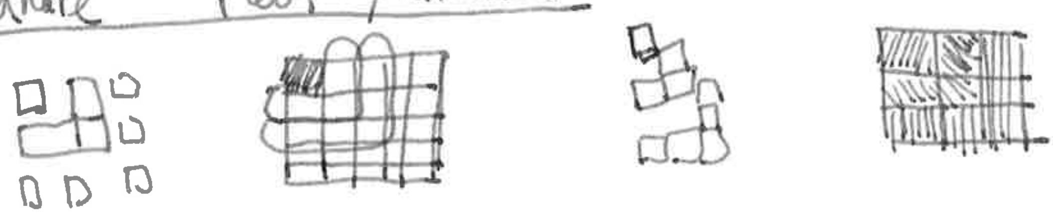
"induction step"

Now, suppose $P(k)$ is true for some natural number k. We need to show (NTS) $P(k+1)$ holds.

Well
$$\sum_{j=1}^{k+1} (2j-1) = \sum_{j=1}^{k} (2j-1) + 2(k+1) - 1$$
$$\overset{P(k)}{=} k^2 + 2(k+1) - 1$$
$$= k^2 + 2k + 2 - 1 = k^2 + 2k + 1$$
$$= (k+1)^2 \quad \checkmark \quad \blacksquare$$

Qs?

<u>Alternate "proof"/intuition</u>



Your turn! Show $n < 2^n$ for all natural #s n.

<u>Pf</u>: induction step: $n+1 < 2^n + 1 \leq 2^n + 2^n$

$$= 2 \cdot 2^n = 2^{n+1}$$

<u>Note</u>: diff base case like knocking down a diff domino at the start.

<u>I.E.</u>: If $a \in \mathbb{N}$, $P(a)$ true, and $P(k) \Rightarrow P(k+1)$ for all $k \geq a$, then $P(n)$ true for all $n \geq a$.

(often induction starts @ 1 and not 0).

<u>Strong induction</u>

If $\boxed{P(0) \text{ true}}$ and $\forall k \in \mathbb{N}$: If $P(j)$ true for all $j \in \mathbb{N}$, $j \leq k$, then $P(k+1)$ true

Then $P(k)$ is true for all natural #s k.

By the way, here's some notation:

"$\in$" means "in"

"$\forall$" means "for all"

"$\exists$" means "there exists"

$\mathbb{N}$ = natural #s = $\{0,1,2,\ldots\}$, $\mathbb{Z}$ = integers = $\{\ldots,-2,-1,0,1,2,\ldots\}$

$\mathbb{Q}$ = rational #s, eg $5/3$, $-2/7$

$\mathbb{R}$ = real #s, eg $\sqrt{2}$, π

$\mathbb{C}$ = complex #s, eg $\pi + 2i$

If A and B are sets, then $A \cap B$ = intersection
$A \cup B$ = union

$A \setminus B$ = set difference, or relative complement
= stuff in A and not B

Eg. $5/6 \in \mathbb{Q} \setminus \mathbb{Z}$, but $2 \notin \mathbb{Q} \setminus \mathbb{Z}$, since $2 \in \mathbb{Z}$.

"Example of strong induction:"

Postage problem: any amount of postage $\geq 12¢$ can be made from 4¢ and 5¢ stamps

weird proof, save for later.

Strong ind

<u>Example</u> : Nim!

Nim is a game. Start with two piles of stones:

Two players take turns taking whatever # ~~[illegible]~~ of stones they like from one of the piles (have to take at least 1, though!) Last player to take a stone wins.

<u>Prop</u> If the two piles have same # of stones, player 2 can always win!

<u>Pf</u> Suppose # stones in piles $= 1$ ✓.

Induct on # stones.

Suppose true for $1, \ldots, k$ stones.

<u>NTS</u> true for $k+1$ stones!

Suppose P1 ~~[illegible]~~ takes j stones from a pile.

~~If $j = k+1$: ✓~~

~~If $j < k+1$: P~~

If $j = k+1$: ✓

If $j < k+1$:

P2 takes same # stones from other pile.

~~N~~ Now both piles have same # stones. Induction hypothesis: ✓

5

~~Strong~~ Weak induction

example: Fibonacci #s: $F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Sequence: 1, 1, 2, 3, 5, 8, ...

Then $\sum_{i=1}^{n} F_i = F_{n+2} - 1$ for all $n \geq 1$.

Pf: $n=1$: $1 = 2-1$ ✓

Induction step: Suppose it's true for $1, 2, \ldots, k$.

NTS: it's true for $k+1$.

$$\sum_{i=1}^{k+1} F_i = \sum_{i=1}^{k} F_i + F_{k+1} \underset{P(k)}{=} F_{k+2} - 1 + F_{k+1} = F_{k+3} - 1.$$

Math 4400 (Lecture 2) (3-17-17)

Outline

- Well-ordering principle
- What's the axiom? Maybe prove weak induction using WOP.
  - doesn't matter which we assume...

• WOP $\Rightarrow$ Wk Ind $\Rightarrow$ Strong Ind $\Rightarrow$ WOP.

- From now on: prove everything we use!
- Euclidean algo: sketch idea, then prove
  - Divis algo.
  - Does it stop?
  - Much of NT is divis. problems.
  - One way: factor into primes. Hard! Basis of crypto.

• Define $a|b$, $a|b, a|c \Rightarrow a|b+c$.

$\mathbb{Z}, \exists, \forall$

Question: how do we prove the principle of induction?

- Francesco Maurolico (1575): ¯_(ツ)_/¯
- Giuseppe Peano (1888): it's an axiom!
- Zermelo / Fraenkel (1908): by definition of the natural #s!

So basically, it's an axiom — one of our starting points. Of course, there are lots of starting points one can choose. For instance:

<u>Well-ordering principle</u>: Let $S \subseteq \mathbb{N}$. If S is nonempty, then S has a smallest element.

<u>Theorem</u> TFAE:

1. Well ordering
2. Weak induction
3. Strong induction

I.e., if you choose any to be an axiom, you can prove the other two.

<u>Proof</u> I'll show $1 \Rightarrow 2$: Let $P(n)$ be a proposition for each n. Set $S = \{a \in \mathbb{N} \mid P(a) \text{ not true.}\}$.

Suppose $P(0)$ true, and $\forall k$, if $P(k)$ then $P(k+1)$

WTS $P(n)$ true for all n

WTS $S = \emptyset$.

Proof by contradiction: suppose, for contradiction, $S \neq \emptyset$, Then Well ordering $\Rightarrow$ S has a smallest element, say b. Then $b \neq 0$, so $b-1 \in \mathbb{N}$.

But $b-1 < b$, so $b-1 \notin S$

$\Leftrightarrow P(b-1)$ true

$\Rightarrow P(b)$ true Contradiction.

$\Leftrightarrow b \notin S$ #.

Euclidean algo (1.1)

Given two #s $a, b \in \mathbb{N}$, what's their greatest common divisor?

$\mathbb{Z}$ = integers = $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

<u>Def</u> let $a, b \in \mathbb{Z}$. a <u>divides</u> b if there exists $c \in \mathbb{Z}$ such that $a \cdot c = b$.

<u>Def</u> Let $a, b \in \mathbb{Z}$, $a \neq 0$, $\gcd(a,b)$ = "greatest common divisor"
= largest $c \in \mathbb{Z}$ s.t. $c | a$ and $c | b$.

<u>Note</u>: $\gcd(a,b)$ always exists! and is unique! You should always make sure definitions make sense

Why does it exist? (Exercise — hw problem!)
↳ "Show any finite set of integers has largest elt"

So how can we compute gcd of two #s?

E.g. 657 & 123?

$657 = 3^2 \cdot 73$, $123 = 3 \cdot 41$

Can list factors of each, but that's hard!
(The basis of RSA encryption)

Alternate: use a lemma.

<u>Lemma</u> if $c|a$, $c|b \Rightarrow c | a+b$

<u>Pf</u> $\exists a_1, b_1$: $ca_1 = a$, $cb_1 = b \Rightarrow c(a_1+b_1) = a+b$ ✓

<u>Note</u> if $c \mid b$, then $c \mid -b$.

So if $c \mid a, c \mid b$, then $c \mid a, c \mid -b \Rightarrow c \mid a-b$ by lemma.

Also, if $c \mid a$, $c \mid b-a$, then $c \mid b$.

We have shown:

$*$ <u>Lemma</u> $(c \mid a$ and $c \mid b) \iff (c \mid a$ and $c \mid b-a)$

So $\{$divisors of 657 and $123\}$

$= \{$divisors of $657-123$ & $123\}$

$$\gcd(657, 123) = \gcd(534, 123) = \gcd(\underset{534-4\cdot 123}{\overset{\shortparallel}{42}}, 123)$$

$$= \gcd(42, 39) = \gcd(3, 39) = 3.$$

This process is called the Euclidean algo.

Let's prove it works! First, we need to formalize the notion of "subtract b from a until you get something smaller than b"

<u>Thm</u> (Division algo) Let $a, b \in \mathbb{Z}$, $a > 0$. Then $\exists!\ q, r \in \mathbb{Z}$ with $b = qa + r$ and $0 \leq r < a$

<u>Proof</u> First existence, then uniqueness

Let $A = \{b - u \cdot a \mid u \in \mathbb{Z}\}$. Claim: $A \cap \mathbb{N} \neq \emptyset$.

Pf of claim: • if $b \geq 0$, choose $u = -1$, Then

$b - ua = b + a \geq 0$, so $b + a \in A \cap \mathbb{N}$.

• If $b < 0$, choose $u = b$. Then $b - ua = b(1-a) \geq 0$.

By WOP, $A \cap \mathbb{N}$ has min'l element, say $r = b - u_0 a$

Then $b = u_0 a + r$, $0 \leq r$.

<u>Claim</u> $r < a$. Suppose $r \geq a$. Then

$r - a = b - (u_0 + 1) a \in A \cap \mathbb{N}$ is smaller than r!

<u>Uniqueness</u>

Suppose $b = qa + r = q'a + r'$ with $0 \leq r, r' < a$.

WTS $q = q'$ & $r = r'$.

If $q < q'$: then $q' \geq q + 1$.

$\leadsto r' = b - q'a \leq b - (q+1) a = r - a < 0$.

Similarly, if $q > q'$: $r < 0$

$r = b - qa \leq b - (q'+1) a = r' - a < 0$.

∎

Euclidean algo (b,a)

Input: $a, b \in \mathbb{N}$; $b \geq a > 0$

Output: $\gcd(b,a)$

Write $b = qa + r$ using divis algo.

If $r = 0$: return a

Else: return EuclidAlgo(a, r)

Thm It terminates and gives correct answer

Pf Induction on a. Base case: $a = 1$. ✓

Induction step: $\gcd(b,a) = \gcd(a,r)$ by lemma.

More concretely:

$$b = q_1 a + r_1$$
$$a = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_1$$
$$\vdots$$
$$r_{n-1} = q_{n+1} r_n \rightsquigarrow r_n = \gcd.$$

Exercise use Euclid algo to find

$\gcd(204, 595)$

$\gcd(105, 270)$

Math 4400 Lecture 3

Induction: • if cont. frac terminates, then rat'l.
• if $p \mid a_1 \cdots a_n$, $p \mid a_i$ some i

5/19/17

12

Outline: • Euclidean algo ex.
• continued fracs (of rat'l(s) of quadratics)
• continued fracs of irrational #s.
• Groupwork (?) cont frac periodic $\Longleftrightarrow$ quadratic
• Diophantine eqns? Pythag triples ??

• Last time: euclidean algo for finding $\gcd(a,b)$.

Concretely, we do divis algo a bunch:

$a = q_1 b + r_1$, $b = q_2 r_1 + r_2$, $r_1 = q_3 r_2 + r_3$, ...,

$r_{n-1} = q_{n+1} r_n$

$r_n = \gcd(a,b)$.

<u>E.g.</u> $\gcd(84, 116) = ?$

$116 = 1 \cdot 84 + 32$,
$84 = 2 \cdot 32 + 20$
$32 = 1 \cdot 20 + 12$
$20 = 1 \cdot 12 + 8$
$12 = 1 \cdot 8 + 4$
$8 = 2 \cdot \boxed{4}$

$\gcd(206, 5280)$

$5280 = 25 \cdot 206 + 130$
$206 = 1 \cdot 130 + 76$
$130 = 1 \cdot 76 + 54$
$76 = 1 \cdot 54 + 22$
$54 = 2 \cdot 22 + 10$
$22 = 2 \cdot 10 + 2$
$10 = 5 \cdot \boxed{2}$

<u>Def</u> "a and b are rel. prime" if $\gcd(a,b) = 1$.

13

Eg gcd (265, 98) = 1:

$265 = 2\cdot 98 + 67$, $98 = 1\cdot 67 + 31$, $67 = 2\cdot 31 + 5$,

$31 = 6\cdot 5 + 1$, $5 = 5\cdot \boxed{1}$

keep!

Let's talk about "rational approximations!

What's a good rational approx for π?

$\pi = 3.14159265\ldots$

"3" is a good start!

$\pi = 3 + 0.14159265\ldots = 3 +$ "a bit"

$= 3 + 1/\left(1/0.14159\ldots\right) = 3 + 1/7.0625\ldots$

repeat!

$$= 3 + \cfrac{1}{7 + \cfrac{1}{1/0.0625\ldots}} = 3 + \cfrac{1}{7 + \cfrac{1}{15.996\ldots}} = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \ldots}}}$$

"continued fraction expansion" of π

Better notation: $\pi = [3; 7, 15, 1, \ldots]$

"Convergents" are rational #s you get by stopping early. E.g.

$$3 + \frac{1}{7} = \frac{22}{7} = \underbrace{3.14}29\ldots, \quad 3 + \cfrac{1}{7 + \frac{1}{15}} = \frac{333}{106} = \underbrace{3.1415}09\ldots, \quad 3 + \cfrac{1}{7 + \cfrac{1}{15 + \frac{1}{1}}} = \frac{355}{113} = \underbrace{3.141592}9\ldots$$

Next step: $[3; 7, 15, 1, 292] = \dfrac{103993}{33102} = \underbrace{3.141592653}01$

get 3 more digits instead of 2! b.c. 292 is "big"

What if we did this to a # that's already rational?

E.g. $\frac{265}{98} = 2 + 0.704\ldots = 2 + \frac{1}{1.46\ldots}$

$$= 2 + \cfrac{1}{1 + \cfrac{1}{2.\!\!.61\ldots}} = \boxed{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6 + \frac{1}{5}}}}}$$

these are the q_i appearing in the euclidean algo!

Why? $265 = 2 \cdot 98 + 67 \rightsquigarrow \frac{265}{98} = 2 + \frac{67}{98} = 2 + \frac{1}{98/67}$

$98 = 1 \cdot 67 + 31 \rightsquigarrow 98/67 = 1 + 31/67$

So $265/98 = 2 + \cfrac{1}{1 + \frac{1}{67/31}} \quad \ldots$

Thm If Euclidean algo is

$a = q_1 b + r_1, \; b = q_2 r_1 + r_2, \ldots, \; r_{n-1} = q_{n+1} r_n,$

then $\frac{a}{b} = [q_1; q_2, \ldots, q_{n+1}]$ (note: $q_i \neq 0$ if $i \geq 2$; $b > r_1 > r_2 > \cdots > r_n$.)

Pf HW exercise (induction on $n =$ length of Euclid algo -1)

Corollary Let $\alpha \in \mathbb{R}$. Continued fraction expansion of α terminates iff α is rational.

Pf If terminates, α is rational.

[If you like, induction on n: if $\alpha = [q_1]$ ✓.

induction: if $\alpha = [q_1; q_2, \ldots, q_{n+1}]$

$\alpha = q_1 + \frac{1}{[q_2; \ldots]} = q_1 + \frac{1}{\text{rat'l}} = \text{rat'l}.$]

Pf, continued

it rational, then terminates: $\alpha = \frac{a}{b}$. Then Euclidean algo ^on a,b terminates. Use theorem above. ■

Continued fracs of irrational #s

Continued fraction of $\sqrt{2}$: $[1; 2, 2, 2, \ldots]$

$\sqrt{3}$: $[1; 1, 2, 1, 2, \ldots]$

$\sqrt{4}$: $[2]$

$\sqrt{5}$: $[2; 4, 4, 4, \ldots]$

$[a_1; a_2, \ldots, a_i = 0, \ldots]$

$= [a_1; a_2, \ldots, a_{i-1} + a_{i+1}, a_{i+2}, \ldots]$

By the way, are continued frac. expansions unique? Certainly not, if they're finite:

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

What if they're infinite? (Yes)

(Do exercises on p. 16)

Aside #2: we said if a large # appears in continued frac expansion, cutting off there gives a good approx.

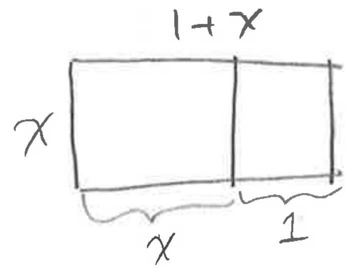
$\rightsquigarrow$ "Hardest" # to approximate w/ a rational # is $1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}$

What is this #? Call it "x". Then

$$x = 1 + \frac{1}{x} \rightsquigarrow x^2 - x - 1 = 0 \rightsquigarrow x = \frac{1 + \sqrt{5}}{2}$$

not $-$ b.c. $x > 0$.

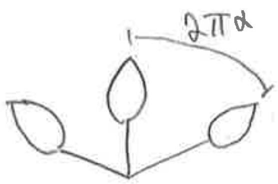
$\frac{x}{1} = \frac{x+1}{x} \rightsquigarrow$



$x =$ golden ratio!

if $\frac{a+b}{a} = \frac{a}{b}$, then $\frac{a}{b} = \varphi$

This is why φ appears in nature:



Plant growing, trying to maximize sunlight on each leaf.

if α = rational $= \frac{a}{b}$, b^{th} leaf is on top of 1st leaf!

To optimize sunlight, need α to be far from rational $\rightsquigarrow$ use $\alpha = \varphi$.

<u>Thm</u> Continued fractions give <u>best</u> rational approximation:

If $\alpha \in \mathbb{R}$, $\frac{p}{q} = i^{th}$ convergent of α, and $a, b \in \mathbb{Z}$, $0 < b \leq q$

Then $$\left|\alpha - \frac{p}{q}\right| \leq \left|\alpha - \frac{a}{b}\right|,$$ equality iff $\frac{p}{q} = \frac{a}{b}$

Pf: Maybe later

Group work: prove $\sqrt{2} = [1; 2, 2, \ldots]$

Compute: $[a; b, b, \ldots]$

Answer: $\frac{2a-b}{2} + \frac{\sqrt{b^2+4}}{2}$

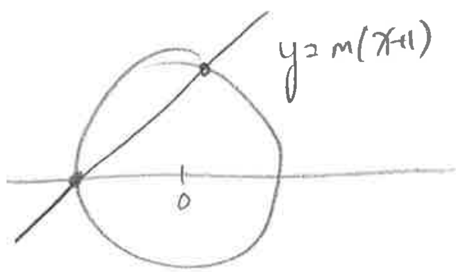
Diophantine equations

Given a polynomial w/ integer coefficients, does it have any integer / rational roots? What are they?

Eg. $x^2 - 2$: no! (using continued fractions!)

Perhaps the oldest one : $x^2 + y^2 = z^2$

Answer: Find rat'l sol'ns to $x^2 + y^2 = 1$.



$$y = m(x+1),$$
$$x^2 + y^2 = 1$$
$$x^2 + m^2(x+1)^2 = 1$$

$$(m^2+1)x^2 + 2m^2 x + (m^2-1) = 0$$

divide by $(x+1)$: $(m^2+1)x + (m^2-1)$

$$\rightsquigarrow (x,y) = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2} \right) \quad m \in \mathbb{Q},$$

$$= \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2} \right) \quad u, v \in \mathbb{Z}.$$

$m = \frac{v}{u}$, simplify

- Continued fracs give best rat'l approx (p. 16)
  Hardest # to approximate w/ a rat'l is φ. (p. 15)
- Diophantine eqns: pythagorean triples.
  Simplest ones: linear diophantine equations!
- eg $a, b \in \mathbb{Z}$, x a variable. When does $ax = b$ have an integer solution? What is it?
- Next simplest: $a, b, c \in \mathbb{Z}$, x and y variables.
  When does $ax + by = c$ have a solution?
  Well, if $d \mid a$ and $d \mid b$, then definitely we need $d \mid c$.

  E.g $9x + 6y = 5$ has no integer solutions.

- What about the other way?
  $9x + 6y = 3$ has a solution ($x = 1$, $y = -1$).

Lemma (Bezout's lemma)

Let $a, b \in \mathbb{Z}$, $a, b \geq 1$. Then $\exists\, x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$

E.g. $\gcd(27,20)=1$, so $27x+20y=1$ has a solution.

$27 = 1\cdot 20 + 7, \quad 20 = 2\cdot 7 + 6, \quad 7 = 1\cdot 6 + 1$

$\leadsto \; 7 - \underbrace{6}_{20-2\cdot 7} = 1 \;\Rightarrow\; 3\cdot\underbrace{7}_{27-20} - 20 = 1$

$\leadsto \; 3(27-20) - 20 = 1 \;\leadsto\; 3\cdot 27 - 4\cdot 20 = 1.$

$(x,y) = (3,-4)$ is our solution.

Pf (Bezout's lemma).

(strong) Induction on $n = \min(a,b)$.

Base case: $\min(a,b) = 1$. Then WLOG $a=1$, $\gcd(a,b) = 1$, and $c=1$, $d=0$ works ✓

Induction step: Suppose lemma is true whenever $\min(a,b) \leq n$, and suppose $\min(a,b) = n+1$.

WLOG, $a = n+1$. Then apply divis algo:

$b = qa + r, \quad 0 \leq r < a$. If $r=0$, then $\gcd(a,b) = a$ and $(x,y) = (1,0)$ works.

Else, by induction, $\exists\, x', y'$: $ax' + ry' = \gcd(x,r)$.

$\Rightarrow ax' + ry' = \gcd(a,r) = \gcd(a, b-qa) = \gcd(a,b)$

$\Rightarrow ax' + (b-qa)y' = \gcd(a,b) \Rightarrow a(x'-qy') + by' = \gcd(a,b)$ ∎

Savin, p.11: relationship to continued fracs.

Corollary: if $c|a$, $c|b$, then $c \mid \gcd(a,b)$. HW.

Pf $\exists x, y$: $ax + by = \gcd(a,b)$. c divides left-hand side.

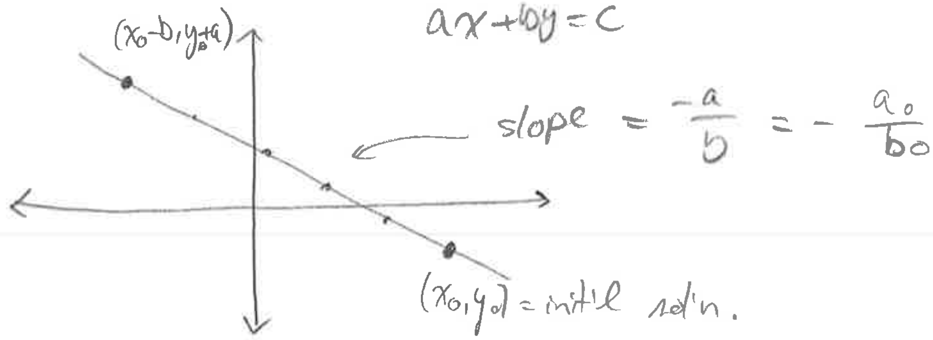
Cor. $ax + by = c$ has an integer solution iff $\gcd(a,b) \mid c$. (Important!)

Pf. If $\gcd(a,b) \mid c$, then $\exists d$ st $d \cdot \gcd(x,y) = c$.

Also $\exists x_0, y_0$: $ax_0 + by_0 = \gcd(a,b)$. Multiply each side by d; (dx_0, dy_0) is an integer solution to $ax + by = c$.

Other way: if $ax + by = c$ has sol'n, then $\gcd(a,b)$ divides left side, so it divides c.

• We've figured out when the linear diophantine has a solution. Now we ask, what are all the solutions?



<u>Thm</u> If (x_0, y_0) a solution to $ax+by=c$, where $c=\gcd(a,b)$, then every other solution is of the form $x=x_0+k\frac{b}{c}$, $y=y_0-k\frac{a}{c}$.

<u>Pf</u> Let (x_1,y_1) be another sol'n.

$$\begin{aligned} ax_0+by_0&=c \\ ax_1+by_1&=c. \end{aligned} \quad \rightsquigarrow \quad \begin{aligned} &ax_0y_1+by_0y_1=cy_1, \quad ax_0x_1+by_0x_1=cx_1 \\ &ax_1y_0+by_1y_0=cy_0, \quad ax_1x_0+by_1x_0=cx_0 \end{aligned}$$

$$\Rightarrow \quad a(x_0y_1-x_1y_0)=c(y_1-y_0), \qquad b(y_0x_1-y_1x_0)=c(x_1-x_0)$$

set $k=-x_0y_1+x_1y_0$. Then

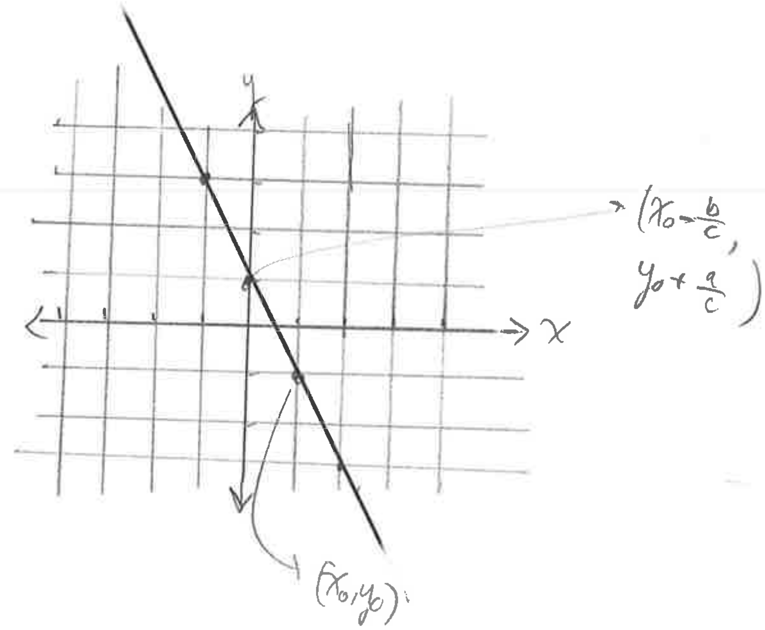
$$-ak=c(y_1-y_0), \qquad bk=c(x_1-x_0)$$

$$\rightsquigarrow \quad y_1=y_0-\frac{a}{c}k, \qquad x_1=x_0+\frac{b}{c}k.$$

Geometric intuition

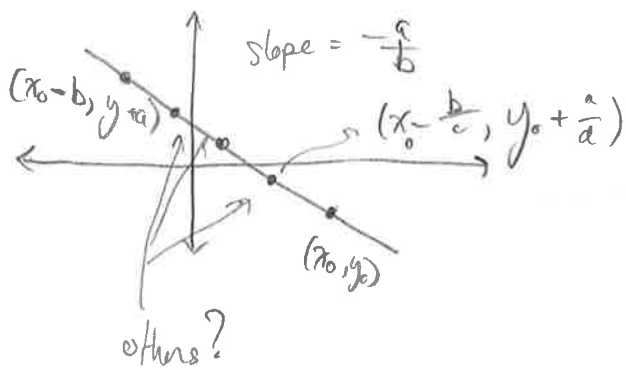
Solutions to $ax+by=c$ give a line in $\mathbb{R}^2$. We want to know which ones happen to lie in $\mathbb{Z}^2$.

E.g. $4x+2y=2$:



More generally

$ax+by=c=\gcd(a,b)$.



Write slope $-\frac{a}{b}$ in lowest terms

$$\Rightarrow \quad -\frac{a/c}{b/c}$$

Math 4400 5/24/17

Uniqueness of factorization!

<u>Def</u> Let $p > 1$ be an integer. We say p is <u>prime</u> if $\forall a \in \mathbb{N}: \ a | p \Rightarrow (a=1 \text{ or } a=p)$

First thing to know about primes: they are the "building blocks" or "atoms" of the integers.

<u>Theorem</u> Every positive integer can be factored uniquely, up to ordering of the factors, into primes ($1 :=$ empty product)

<u>I.e.</u> $\forall n \in \mathbb{Z}, \ n>0, \ \exists \underbrace{p_1, \ldots, p_r}_{\text{primes}} : \ n = p_1 \cdots p_r$. If $q_1, \ldots, q_s$ are also primes with $n = q_1 \cdots q_s$, then $r=s$, and we can rearrange the q's so that $p_1 = q_1, \ldots, p_r = q_r$.

(Not an obvious fact! See Silverman's notes abt "$\mathbb{E}$-zone")

First we need a lemma:

<u>Lemma</u> Let $p \in \mathbb{Z}$ be prime, $a, b \in \mathbb{Z}$. If $p | ab$ then $p | a$ or $p | b$.

<u>Proof</u> If $p|a$ we're done. So suppose $p \nmid a$. Then, since p prime, $\gcd(a,p) = 1$.

By Bezout, $\exists\, c,d \in \mathbb{Z}$: $ac + pd = 1$

$\Rightarrow abc + pbd = b \Rightarrow p \mid b$ ∎

Proof of theorem

Let's show existence first.

~~Suppose $\exists$ some $n \in \mathbb{Z}$ s.t. n can't be factored into primes.~~

Suppose existence part of thm is false. Then the set $S = \{ n \in \mathbb{N},\ n > 0 \mid n \text{ can't be factored into primes} \}$ is not empty. Using well-ordering, let n be its minimal element.

Then n is not prime, so $\exists\, a, b \in \mathbb{N}$, $a \neq 1, n$ such that $ab = n$. Then $1 < a < n$, and $1 < b < n$, so we can write $a = p_1 \cdot \ldots \cdot p_r$ and $b = q_1 \cdots q_s$ for some primes $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$.

$\Rightarrow n = p_1 \cdots p_r \cdot q_1 \cdots q_s$. Contradiction!

Uniqueness use lemma.

Oops, we actually need a corollary of the lemma:

Cor (of lemma) if $r \geq 2$, $a_1, \ldots, a_r \in \mathbb{Z}$, and $p \mid a_1 \cdots a_r$,
then $p \mid a_i$ for some i

Pf Induction on r.

maybe discuss the idea first.

Proof of uniqueness: let $n \in \mathbb{N}$ and let
$S = \{ s \in \mathbb{N} \mid n$ can be factored into s primes$\}$.

S is nonempty, by existence, so it has a min'l element r.

Prove uniqueness by induction on r.

Base case $r=1$: $n = p_1 = q_1 \cdots q_s \Rightarrow$ each $q_i = 1$ or p_1
(p_1 prime)
$\Rightarrow$ each $q_i = p$ (q_i prime)
$\Rightarrow s = 1$, $q_1 = p_1$.

Induction step

$n = p_1 \cdots p_{k+1} = q_1 \cdots q_s$. Then p_{k+1} divides some q_i. WLOG p_{k+1} divides q_s (reorder the q_i)

$\Rightarrow p_{k+1} = q_s$ (since q_s is prime & $p_{k+1} \neq 1$).

$\Rightarrow p_1 \cdots p_k = q_1 \cdots q_{s-1}$

By induction, $k = s-1$, and we can reorder the q's s.t.
$p_1 = q_1, \ldots, p_k = q_k$ ∎

Math 4400 5/26/17

Theorem $\forall n > 0$, $n \in \mathbb{N}$, $\exists r \geq 0$ and primes $p_1, \ldots, p_r \in \mathbb{N}$ s.t. $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Unique up to ordering.

Remark What about $n=1$? That's the empty product.

Pf Existence: well-ordering princ. (p.23)

Uniqueness: need our lemma: if p prime, and $p \mid a_1 \cdot \ldots \cdot a_n$, then $p \mid a_i$ for some i. (p.24)

Idea: $p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$. Lemma $\Rightarrow p_1 \mid q_i$ (WLOG $i=1$)

$\Rightarrow p_1 = q_1$

$\Rightarrow p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s$ Keep going!

Protip if the idea behind your pf is "keep doing this thing over & over, then you're secretly using induction! (Probably)

$P(k)$ = "if n can be written as a product of k primes, then it's unique (up to ordering)"

Number theorists love to talk about prime #s. Lots of open Qs!

Goldbach: every even number > 2 is the sum of two primes. 250-year-old question!

Known up to 4×10^{18}

Helfgott '13: can do it w/ 4 primes.

Thm: Infinitely many primes

Pf (Euclid) Suppose fin. many, $p_1, \ldots, p_n$. By our theorem, $a = p_1 \cdot \ldots \cdot p_n + 1$ has a prime factorization.

But! If $p_i \mid a$ for any i, then $p_i \mid a - p_1 \cdot \ldots \cdot p_n$

$\Rightarrow p_i \mid 1$. #.

(Alternatively, divis algo shows remainder after dividing by $p_i = 1$)

Def Let p_1, p_2 be prime #s. If $|p_2 - p_1| = 2$, then p_1 & p_2 are called "twin primes".

E.g. 3 & 5, 5 & 7, 11 & 13, ...

Twin primes conjecture

There are infinitely many pairs of twin primes.

Zhang, '13: $\exists$ inf. many pairs p_1, p_2 s.t. $|p_1 - p_2| < 7 \times 10^7$

Polymath project: (Maynard, Tao) $|p_1 - p_2| < 246$ "

Aside $\sqrt{2}$ is irrational.

Pf Suppose $\sqrt{2} = \frac{a}{b}$. Then $a = p_1 \cdots p_r$, $b = q_1 \cdot \ldots \cdot q_s$

$\Rightarrow 2 \cdot q_1^2 \cdot \ldots \cdot q_s^2 = p_1^2 \cdot \ldots \cdot p_r^2$

But 2 appears odd # times on left and even # times on the right! Contradicts uniqueness. $\blacksquare$

Congruences & Modular Arithmetic

Let $a,b,m \in \mathbb{Z}$. We say "a is congruent to b modulo m"

if $m \mid (a-b)$.

Note $a \equiv 0 \mod m$ iff $m \mid a$.

It's like doing math on a clock! Or a circle.

3 hours past 11 pm is 2am ($3+11 \equiv 2 \mod 12$).

Basic facts if $a \equiv b \mod m$, $b \equiv c \mod m$, then $a \equiv c \mod m$.

If $a \equiv c$, $b \equiv d$, then $a+b \equiv c+d$ and $a \cdot b \equiv c \cdot d$.

Congruences / Modular arith. 5/31/17

Recall: if $a, b, n \in \mathbb{Z}$, we say "$a \equiv b \mod n$" if $n \mid a-b$.

E.g. $28 \equiv 2 \mod 13$, $2 \equiv -6 \mod 8$, $1000007 \equiv 7 \mod 10$.

Note if $a_1 \equiv a_2 \mod n$ and $b_1 \equiv b_2 \mod n$, then

$a_1 + b_1 \equiv a_2 + b_2 \mod n$ and $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod n$.

Special case: $a \equiv b \Rightarrow a+c \equiv b+c$, $a \cdot c \equiv b \cdot c$

$\boxed{\text{We can do algebra!}}$

$a \equiv 0 \mod n \Leftrightarrow n \mid a$.

Thus, when we're doing calculations "mod n", we can simplify ~~the~~ the numbers first.

E.g. What's $16253 \cdot 8754 \pmod{10}$?

$16253 \equiv 3 \mod 10$ and $8754 \equiv 4 \mod 10$,

so $16253 \cdot 8754 \equiv 3 \cdot 4 \equiv 12 \equiv 2 \pmod{10}$

E.g. What's $(25)^{100} \mod 12$? $25 \equiv 1 \mod 12$,

so $(25)^{100} \equiv 1^{100} \equiv 1 \mod 12$

Note If $a = qn + r$, then $qn = a - r$, so $a \equiv r \mod n$.

Thus, by divis algs, each integer is congruent to exactly one of $0, 1, 2, \ldots, n-1 \mod n$.

Note If $a \in \mathbb{Z}$, a odd, then $a \equiv 1 \mod 2$.

Prop an odd # + odd # = even #
odd # times odd # = odd #.

Pf if $x, y \in \mathbb{Z}$ both odd, then $x \equiv 1 \mod 2$, $y \equiv 1 \mod 2$,

$x + y \equiv 1 + 1 \equiv 0 \mod 2 \Rightarrow x+y$ even

$x \cdot y \equiv 1 \cdot 1 \equiv 1 \mod 2 \Rightarrow x \cdot y$ odd. ∎

Alternatively: $x = 2k+1$, $y = 2l+1$,

$$x+y = 2(k+l)+2 = 2(k+l+1) = \text{even}$$

$$x \cdot y = 4kl + 2k + 2l + 1 = 2(2kl+k+l)+1. = \text{odd}.$$

But! This is a lot like the proof that $a_1 + b_1 \equiv a_2 + b_2$ if $a_1 \equiv a_2$, $b_1 \equiv b_2$. We did the messy calculation once, and now we never have to do it again! This is sort of the point of math — find general principles that give elegant proofs, and also connect seemingly disparate facts. General principles give context to and deeper understanding of the facts. Abstraction simplifies proofs and distills ideas.

<u>Caution</u>: you can't divide "mod n".

Eg. $2 \cdot 12 \equiv 2 \cdot 17 \mod 10$ but $12 \not\equiv 17 \mod 10$!

$2 \cdot 12 \to 24$, $2 \cdot 17 \to 34$

In fact, sometimes $a \cdot b \equiv 0 \mod n$ when $a \not\equiv 0$ and $b \not\equiv 0 \mod n$! Examples???

Can you think of other things that you can multiply but not divide?/ Other things w/ this behavior? $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

This is, philosophically, "why" we can't divide: $2\cdot 17 \equiv 2\cdot 12 \mod 10 \Leftrightarrow 2\cdot(17-12)\equiv 0 \mod 10.$

but $2 \not\equiv 0$ and $17-12 \not\equiv 0$.

we can rewrite one fact as the other.

Solving equations mod n

- Solve $x+12 \equiv 5 \mod 8. \Rightarrow x \equiv -7 \mod 8$
  or $x \equiv 1 \mod 8$

  Same thing! When we ask to solve equations mod n, we mean "find incongruous solutions".

- Solve $4x \equiv 5 \mod 19.$
  Can't divide by 4! But notice: $5\cdot 4x \equiv 5\cdot 5 \mod 19$
  $\rightsquigarrow 20x \equiv 25 \mod 19 \rightsquigarrow 1\cdot x \equiv 6 \mod 19.$

- Solve $x^2+2x-1 \equiv 0 \mod 7$
  Try 7 options!

  $0^2+0-1 \not\equiv 0$
  $1^2+2-1 \not\equiv 0$
  $2^2+4-1 \equiv 0$ ✓
  $3^2+2.3-1 \equiv 2+6-1 \equiv 0$ ✓
  etc.

- Some equations don't have solutions, eg
  $x^2 \equiv 3 \mod 7$

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

  $x^2 \equiv 2$ does!!!

Solving linear congruences $a, c, m \in \mathbb{Z}$.

When does $ax \equiv c \pmod m$ have a solution? What are they?

Try some examples:
$10x \equiv 3 \mod 11$, $(x \equiv 8)$
$5x \equiv 0 \mod 10$ $(x \equiv 0, 2, 4, 6, 8)$
$5x \equiv 1 \mod 10$ (no sol'ns!)
$7x \equiv 1 \mod 10$ $(x \equiv 3)$
$8x \equiv 1 \mod 10$ (none)
$9x \equiv 1 \mod 10$ $(x \equiv 9)$
$2x \equiv 7 \mod 20$ (none!)

Weird behavior if $\gcd(a,c) \neq 1$!

Note: $ax \equiv c \pmod m \Leftrightarrow \exists k : mk = ax - c$
$\Leftrightarrow \exists k : ax - mk = c$

So a solution exists iff $\gcd(a,m) \mid c$, by Bezout!
The solutions are $x = x_0 + \ell \frac{\gcd(a,m)}{m}$, $\ell \in \mathbb{Z}$,
where x_0 is any initial solution.

E.g. Solve $128x = 2 \mod 506$

Is it possible? Find $\gcd(128, 506)$:

- ~~1140 ≠ 2·506 + 128~~
- $506 = 3 \cdot 128 + 122$
- $128 = 1 \cdot 122 + 6$
- $122 = 20 \cdot 6 + 2$
- $6 = 3 \cdot 2$

$2 \mid 2$ so we're good.

Initial solution?

By prop, start by solving
$128x = 2 \mod 506$.

Solve for 2 first.

$122 - 20 \cdot 6 = 2$, so $x_0 \equiv -83$ is our initial sol'n.

$21 \cdot 122 - 20 \cdot 128 = 2$, or $x_0 \equiv 45$

$21 \cdot 506 - 83 \cdot 128 = 2$ $\Rightarrow$ $x \equiv 45 + k \cdot \frac{506}{2} = 45 + k \cdot 253$

$\rightsquigarrow x \equiv 45, 298, 551 = 45 + 506, \ldots$ (only 2 incongruous solutions)

What if we wish to solve $128x = 4 \bmod 506$?

<u>Fact</u> if (x_0, y_0) is a solution to $ax + by = c$, with $\gcd(a,b) \mid c$, then all others are $x_0 + k\frac{b}{\gcd(a,b)}$, $y_0 - k\frac{a}{\gcd(a,b)}$

<u>Pf</u> Basically the same as before.

So we start with initial solution $x_0 = 90$, and get $x_0 = 90$, $x \equiv 90, 343$.

Later: prop abt all the solutions to $ax \equiv c \bmod m$.

<u>Homework hint</u> Show $9 \mid n$ iff sum of digits of n is divisible by 9.

Digits of n are $a_0, a_1, \ldots a_d$ if $0 \leq a_i < 10$ $\forall i$, and

$$n = \sum_{i=0}^{d} a_i 10^i.$$

Math 4400 6/2/17

Last time: Fact: if $\gcd(a,b) \mid c$, and $ax_0 + by_0 = c$, then the set of (x,y) s.t. $ax+by=c$ is $\left\{\left(x_0 + k\frac{b}{\gcd(a,b)},\ y_0 - k\frac{a}{\gcd(a,b)}\right) \,\middle|\, k \in \mathbb{Z}\right\}$

Also, $ax \equiv c \mod n \iff \exists l.\ ax + nl = c$.

So, $ax \equiv c \mod n$ has solutions iff $\gcd(a,n) \mid c$, by Bezout, and they are $\left\{x_0 + k\frac{n}{\gcd(a,n)} \,\middle|\, k \in \mathbb{Z}\right\}$

Some of these are really the same mod n!

Eg $x_0 \equiv x_0 + n \equiv x_0 + 2n \ldots$

$x_0 + 1\cdot\frac{n}{\gcd(a,n)} \equiv x_0 + (1+\gcd(a,n))\frac{n}{\gcd(a,n)} \equiv x_0 + (1+2\gcd(a,n))\frac{n}{\gcd(a,n)}$

$\vdots$

$x_0 + (\gcd(a,n)-1)\frac{n}{\gcd(a,n)} \equiv \ldots$

So there are <u>at most</u> $\gcd(a,n)$-many distinct solutions mod n.

<u>Prop</u> There are exactly $\gcd(a,n)$-many incongruent solutions mod n.

<u>Pf</u> It suffices to check: if $0 \le r, s < \gcd(a,n)$ and $r \ne s$, then $x_0 + r\frac{n}{\gcd(a,n)} \not\equiv x_0 + s\frac{n}{\gcd(a,n)}$

Suppose $x_0 + r\frac{n}{\gcd(a,n)} \equiv x_0 + s\frac{n}{\gcd(a,n)}$. WLOG: $r > s$.

$\Rightarrow n \mid r\frac{n}{\gcd(a,n)} - s\frac{n}{\gcd(a,n)} \Rightarrow n \mid (r-s)\frac{n}{\gcd(a,n)}$

But $0 < r-s < \gcd(a,n)$, so $0 < (r-s)\frac{n}{\gcd(a,n)} < n$. Contradiction!
(Easy lemma: if $n, m \in \mathbb{N}$, $n | m$, then $m = 0$ or $m \geq n$)

Eg. Solve $128x \equiv 4 \mod 506$ (p. 31).

answer: $x \equiv 90, 343$.

Note if $\gcd(a,n) = 1$, $\exists x$: $ax \equiv 1 \mod n$. Inverse of a!

~~Next let's solve $a^x \equiv b \mod n$ for $a, b, n \in \mathbb{Z}$!~~
~~Well, that's too hard. Let's work~~

Let's think about $a^m \mod n$ for various m:

eg.

a	a^2	a^3	a^4	a^5
0	0	0	0	0
1	1	1	1	1
2	0	0	0	0
3	1	3	1	3

mod 4

a	a^2	a^3	a^4	a^5
0	0	0	0	0
1	1	1	1	1
2	4	3	1	2
3	4	2	1	3
4	1	4	1	4

mod 5

Fermat's little theorem

Let p be prime, $a \not\equiv 0 \mod p$. Then $a^{p-1} \equiv 1 \mod p$

First, a lemma

$1, 2, 3, \ldots, (p-1) \mod p$ is the same as
$a, 2a, 3a, \ldots, (p-1)a$ (in a different order). ← do example, mod 5.

Pf Clearly $a, 2a, \ldots, (p-1)a \not\equiv 0 \mod p$, since
$p | na \Rightarrow p | n$ or $p | a$
Also, if $ra \equiv sa$, then $(r-s)a \equiv 0$.
Hw problem $\Rightarrow$ $p | r-s$, since $\gcd(a,p) = 1$

Now, if $0 < r < s < p$, then $p \nmid (r-s)$

$\Rightarrow ra \not\equiv sa$. So each element in $\{a, 2a, \ldots, (p-1)a\}$ is congruent to a different nonzero # mod p.

Proof of Fermat:

$$\underbrace{a \cdot 2a \cdot \ldots \cdot (p-1)a}_{= a^{p-1} \cdot (p-1)!} \equiv \underbrace{1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)}_{= (p-1)!} \mod p$$

Note: $p \nmid (p-1)!$ since $p \nmid n \ \forall n: 2 \leq n \leq p-1$.

Thus $\exists x$ s.t. $(p-1)! \, x \equiv 1 \mod p$.

$$\Rightarrow \underbrace{a^{p-1} (p-1)! \, x}_{\equiv a^{p-1}} \equiv \underbrace{(p-1)! \, x}_{\equiv 1} \mod p \qquad \blacksquare$$

Math 4400, 6/5/17

- $\gcd(a,n)=1 \iff a$ is invertible mod n.
- define "equiv class mod n"
- Lemma for Fermat
- Fermat

Important remark

Let $a,n \in \mathbb{Z}$. Then $ax \equiv 1 \bmod n$ has a solution iff $\gcd(a,n)$. It's unique! The solution, x_0, is called the (multaplicative) inverse of a mod n.

To "divide by a", just multiply by x_0.

i.e. $ab \equiv c \implies x_0 ab \equiv x_0 c \implies b \equiv x_0 c$.

and vice-versa.

Def let $a,n \in \mathbb{Z}$. The (equivalence) class of a mod n is the set of all integers congruent to a mod n. Denoted $[a]_n$ or $a+n\mathbb{Z}$

$[a]$ if n is clear from context.

E.g. $[1]_{10} = \{\ldots, -9, 1, 11, 21, \ldots\}$

$[2]_{10} = \{\ldots, -8, 2, 12, 22, \ldots\}$

The set of all equivalence classes mod n is $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$.

Fermat's Little Theorem

Studying patterns of $a^m \mod n$.

a	a^2	a^3	a^4	a^5
0				
1				
2				
3				

mod 4

a	a^2	a^3	a^4	a^5	a^6

mod 5

(see p. 34)

Striking thing: $a^4 \equiv 1 \pmod 5$ if $a \not\equiv 0$,
$a^5 \equiv a$ for all a.

Fermat's little theorem

Let p = prime, $a \not\equiv 0 \mod p$. Then $a^{p-1} \equiv 1 \mod p$.

Lemma $\{[a]_p, [2a]_p, \ldots, [(p-1)a]_p\} = \{[1]_p, \ldots, [p-1]_p\} = (\cancel{\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}})$ everything but 0.

Pf. If $[na] = [0]$, i.e. $na \equiv 0$, then $p \mid na$. Since p is prime,

$p \mid na \implies p \mid n$ or $p \mid a$. Since $\gcd(p,a)=1$, $p \nmid a$.

Thus, if $[na] \equiv [0]$, must have $p \mid n$.

Contrapositive $\implies$ $[a], [2a], \ldots, [(p-1)a]$ are all nonzero.

Thus: it's enough to show $[ra] \neq [sa]$ if $0 < r < s < p$.
(if $|S| < \infty$, $|T| < \infty$, $S \subseteq T$, and $|S| = |T|$, then $S = T$)

But if $ra \equiv sa$, then $(s-r)a \equiv 0$. Contradiction. ∎
$(0 < s-r < p)$

Proof of Fermat's little thm: see p. 35.

Eg. Solve $x^{43} + 3 \equiv 0 \mod 7$.
Note $x^6 \equiv 1$, so $x^{43} = x^{7\cdot 6+1} = (x^6)^7 \cdot x \equiv x$.

$\Rightarrow$ $x \equiv -3 \equiv 4$ is the solution.

Eg. 1234567 isn't prime.

$2^{1234566} \equiv 89957 \mod 1234567$

$\uparrow$ easy for computers

$\uparrow$ hard to factor.

Euler's formula

Let $a, n \in \mathbb{Z}$, n not necessarily prime. How can we solve $a^x \equiv 1 \mod n$?

Note $n-1$ doesn't work: $3^7 \equiv 3 \mod 8$.

Note if $a^x \equiv 1$, then $(a^{x-1})\, a \equiv 1$, so a^{x-1} is the inverse of a. Thus $\gcd(a,n) = 1$.

This suggests we study #s rel. prime to n.

Def Euler's φ function: $\varphi(n) =$ the number of integers a, $0 < a < n$, s.t. $\gcd(a,n) = 1$.

$\varphi(n) = \# \{a \in \mathbb{Z} \mid 0 < a < n, \quad \gcd(a,n) = 1\}$

size of a set, "Cardinality"

Let's try to apply proof of Fermat's little theorem.

For that: we needed a lemma: $\{a, 2a, \dots, (p-1)a\} = \{1, 2, \dots, p-1\}$.

Note what happens if we restrict our attn to #s rel. prime to n:

<u>Eg.</u> $n = 10$. Relatively prime #s: $1, 3, 7, 9$.

$\Rightarrow \varphi(n) = 4$.

Notice:
$$\begin{array}{cccc} 1\cdot 7, & 3\cdot 7, & 7\cdot 7, & 9\cdot 7 \\ \equiv & \equiv & \equiv & \equiv \\ 7 & 1 & 9 & 3. \end{array}$$

$$\begin{array}{cccc} 1\cdot 3, & 3\cdot 3, & 7\cdot 3, & 9\cdot 3 \\ \equiv & \equiv & \equiv & \equiv \\ 3 & 9 & 1 & 7 \end{array}$$
same thing with 3.

Thus, $(1\cdot 7)(3\cdot 7)(7\cdot 7)(9\cdot 7) \equiv 1\cdot 3\cdot 7 \cdot 9 \mod 10$,

$$\| $$

$$7^4 \cdot (1\cdot 3\cdot 7\cdot 9)$$

But $\underbrace{\gcd(1\cdot 3\cdot 7\cdot 9, 10)}_{\text{consider prime \#s.}} = 1$, so we can cancel.

[$\gcd(a,b) = 1 \iff$ no primes divide both a and b.]

$7^4 \equiv 1 \mod 10$.

Euler's formula $\forall a,n \in \mathbb{Z}$, if $\gcd(a,n)=1$, then $a^{\varphi(n)} \equiv 1 \mod n$.

Pf Same idea as Fermat.

Math 4400 6/7/17

- If S is a set, $\# S$ or $|S|$ denotes size of S.
- Define φ.

Eg $\varphi(10) = 4$. $\varphi(p) = p-1$.

- Lemma if $\gcd(a,b)=1$ and $\gcd(a,c)=1$, then $\gcd(a,bc)=1$.

Pf Let $d \in \mathbb{N}$, $d|a$, $d|bc$. $d|a \Rightarrow \{x \mid x|d$ and $x|b\} \subseteq \{x \mid x|a$ and $x|b\}$, so $\gcd(d,b)=1$. Similarly, $\gcd(d,c)=1$.

Since $d|bc$, hw problem $\Rightarrow$ $d|c \Rightarrow \gcd(d,c)=d$.

But $\gcd(d,c)=1$, so $d=1$.

- Proof of Euler's formula

Let $1 = b_1 < b_2 < b_3 < \dots < b_{\varphi(n)} < n$ be all the nat. #s $< n$ rel prime to n.

Claim $\{[b_1]_n, [b_2]_n, \dots, [b_{\varphi(n)}]_n\} = \{[ab_1]_n, \dots, [ab_{\varphi(n)}]_n\}$.

Note: $\supseteq$ is easy. Why?

Ugh, we need another lemma ...

Lemma if $\gcd(a,n)=1$ and $a = qn + r$, then $\gcd(a,n) = \gcd(n,r)$.

(Actually, we already know this from our Euclidean Algo lectures!)

Ok, so write $ab_i = qn + r$ using divis algo.
Then $0 \le r < n$ and $\gcd(r,n) = \gcd(ab_i, n) = 1$
(using lemma before proof).

Then $r = b_j$ for some j, and $ab_i \equiv r \mod n$ ✓

Just like before, it now suffices to check $ab_i \not\equiv ab_j$ if $i \ne j$. So suppose $ab_i \equiv ab_j$. wlog $i \geq j$
Then $n \mid a(b_i - b_j)$, but $\gcd(a,n)=1$, so
$n \mid b_i - b_j$. But $0 \le |b_i - b_j| < n$, so $b_i - b_j = 0$ ✓

$\Rightarrow ab_1 \cdots ab_{\varphi(n)} \equiv b_1 \cdots b_{\varphi(n)} \mod n$

$\Rightarrow a^{\varphi(n)} \underbrace{b_1 \cdots b_{\varphi(n)}}_{\text{rel prime to } n, \text{ by our lemma.}} \equiv b_1 \cdots b_{\varphi(n)} \mod n$

$\Rightarrow a^{\varphi(n)} \equiv 1 \mod n$ ∎

Ask: Can anyone guess what comes next?

Our next order of business: computing $\varphi(n)$

Easy for primes: $\varphi(p) = p-1$.

For powers of primes: $\gcd(a, p^k) = 1 \iff p \nmid a$.

So $\varphi(p^k) = \#\{a \mid 1 \le a \le p^k\} - \#\{a \mid 1 \le a \le p^k,\ p \mid a\}$

$$= p^k - \#\{p, 2p, \ldots, (p^{k-1}-1)p, p^k = p^{k-1}\cdot p\}$$

$$= p^k - p^{k-1}$$

Other #s?

n	$\{a \mid \gcd(a,n)=1\}$	$\varphi(n)$
6	$\{1, 5\}$	2
12	$\{1, 5, 7, 11\}$	4 $= \varphi(4)\cdot\varphi(3)$
14	$\{1, 3, 5, 9, 11, 13\}$	6 $= \varphi(2)\cdot\varphi(7)$
21	$\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$	12 $= \varphi(3)\cdot\varphi(7)$

n	$\varphi(n)$
2	1
4	2
8	4
7	6
3	2

Notice $\varphi(p^j q^k) = \varphi(p^j)\,\varphi(q^k)$

In fact: if $\gcd(m,n) = 1$, then $\varphi(m)\varphi(n) = \varphi(mn)$.
(Prove later.)

How can we use this to compute $\varphi(m)$?

First, factorize m: $m = p_1^{k_1} \cdots p_n^{k_n}$

$$\Rightarrow \varphi(m) = \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_n^{k_n}) = (p_1^{k_1} - p_1^{k_1-1}) \cdot \ldots \cdot (p_n^{k_n} - p_n^{k_n-1})$$

Note: $(p^k - p^{k-1}) = p^k\left(1-\frac{1}{p}\right)$

Thus $\varphi(m) = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n} \left(1-\frac{1}{p_1}\right) \cdots \left(1-\frac{1}{p_n}\right)$

$= m \cdot \left(1-\frac{1}{p_1}\right) \cdot \ldots \cdot \left(1-\frac{1}{p_n}\right)$

Corr $\forall m > 0$, $\varphi(m) = m \cdot \prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1-\frac{1}{p}\right)$

E.g. $\varphi(100) = \varphi(2^2 5^2) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = \frac{100 \cdot 4}{10}$

$= 40.$

To prove our formula, we need the Chinese Remainder theorem, which deals with systems of linear congruences.

E.g. Solve $x \equiv 8 \mod 11$ and $x \equiv 2 \mod 9$.

First eq $\Rightarrow$ $x = 11y + 8$. So, solve $11y + 8 \equiv 2 \mod 9$.

$\rightsquigarrow$ $2y \equiv 3 \mod 9$. One solution is $y = 6$.

(use modular inverse, etc).

$\Rightarrow x = 11 \cdot 6 + 8 = 74$ works. (Verify!)

Math 4460 §2.5 of Savin 6/9/17

- We wanna show $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $\gcd(m,n)=1$.

- First, some facts: $\forall a,b,n$ if $a \equiv b \mod n$, then $\gcd(a,n) = \gcd(b,n)$. because $\gcd(a,n) = \gcd(a-nk, n)$ $\forall k$.

- Also, $\forall a,m,n$ if $\gcd(a,n)=1$ and $\gcd(a,m)=1$, then $\gcd(a,mn)=1$.

  <u>Pf</u> If $d|a$, $d|mn$, $d>1$, then $\exists$ some prime number p st. $p|a$ and $p|mn$. Then $p|m$ or $p|n$.
  First case: $\gcd(a,m) \geq p$. Contradiction.

- Theorem: if $m,n \in \mathbb{Z}$ w/ $\gcd(m,n)=1$, then $\varphi(m)\varphi(n) = \varphi(mn)$.

  <u>Proof</u> Think about what $\varphi(mn)$ is counting:

  $$\varphi(mn) = \#\{x \mid 1 \leq x \leq mn \;\&\; \gcd(x, mn)=1\} = \#S$$

  $$\varphi(m)\varphi(n) = \#\left\{(a,b) \;\middle|\; \begin{array}{l} 1 \leq a \leq m, \; \gcd(a,m)=1 \\ 1 \leq b \leq n, \; \gcd(b,n)=1 \end{array}\right\} = \#T$$

We want to show these sets have the same size.

To do so, we need the <u>Chinese Remainder Thm</u>

$\boxed{\text{CRT: } \forall a,b,m,n \in \mathbb{Z} \text{ w/ } \gcd(m,n)=1 \ \exists!\, x,\ 0 \le x < mn \text{ Solving } x \equiv a \bmod m,\ x \equiv b \bmod n.}$

Prove later!

switch order.

Define a function $f: S \longrightarrow T$, $f(x) = (x \bmod m, x \bmod n)$

Want: $\forall y \in T\ \exists! x \in S: f(x) = y$ (i.e. f a bijection)

(One way to show two sets have the same size is to find a bijection)

CRT: for all $(a,b) \in T$ $\exists!\, x \in \{1, 2, \ldots, mn\}$ s.t. $a \equiv x \bmod m$, $b \equiv x \bmod m$. So we just need to show $\gcd(x, mn) = 1$.

But Fact 1 $\Rightarrow$ $\gcd(x,m) = \gcd(x,n) = 1$,

Fact 2 $\Rightarrow$ $\gcd(x, mn) = 1$. $\blacksquare$

CRT example: solve $x \equiv 8 \bmod 11$, $x \equiv 5 \bmod 10$.

Well, $x = 8 + 11n$. $\rightsquigarrow$ $8 + 11n \equiv 5 \bmod 10$

$\Rightarrow 11n \equiv -3 \bmod 10$. ($\exists!$ sol by rel. prime).

$\Rightarrow n \equiv -3 \bmod 10$.

i.e. $n \equiv 7 \bmod 10$, $x = 8 + 77 = 85$

Check: $85 \equiv 8 \bmod 11$ $85 \equiv 5 \bmod 10$.

Proof of CRT

(There's a more slick pf in Savin's notes)

Set up: m, n rel prime, $a, b \in \mathbb{Z}$

Want to show $\exists!\, x$: $0 \le x < mn$ s.t.

$x \equiv a \mod m$, $x \equiv b \mod n$.

First: we may assume $0 \le a < m$, $0 \le b < n$.

Well, since $\gcd(m,n) = 1$, $\exists!\, k$, $0 \le k < n$, s.t.

$mk \equiv b - a \mod n$. Set $x = mk + a$. Then

$x \equiv a \mod m$, $x \equiv b \mod n$, and

$0 \le mk + a \le m(n-1) + m - 1 = mn - 1$ Existence ✓

Uniqueness? If $0 \le x_2 < mn$ and

$x_2 \equiv a \mod m$, $x_2 \equiv b \mod n$, then

$x_2 = k_2 m + a$, some k_2, $0 \le k_2 \le n-1$ since $0 \le x_2 < mn$

(if $k_2 \le -1$, $x_2 \le -m + a < 0$).

So $0 \le k_2 < n$ and $k_2 m \equiv b - a \mod n$.

$\Rightarrow k_2 = k$ and $x_2 = x$.

Math 4400 6/12/17

- Give my little spiel on "the point" of modular arithmetic from p. 29
- Whenever you want to say "n is either even or odd," replace it with "n is either 0 mod 2 or 1 mod 2"
- Modular arithmetic is a generalization of the idea of even #s vs. odd #s.
- So proving $a^2 \not\equiv 2 \mod 5$ is a lot like proving "even · odd = even"

//

Groups §2.1

Recall: if A and B are sets,

$A \times B$ = "cartesian product" = $\{(a,b) \mid a \in A, b \in B\}$

Def Let S be a set. A binary operation on S is a function $S \times S \longrightarrow S$.

E.g. addition is a binary op. on $\mathbb{Z}$:

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a,b) \longmapsto a+b$$

"infix notation"

we could just as well write $+(a,b)$, but that's awkward

E.g. $$\mathbb{Z} \times \mathbb{Z} \xrightarrow{f} \mathbb{Z}$$
$$(a,b) \longmapsto 3a+b$$

E.g. $M_{2\times 2}(\mathbb{R}) = \{ 2\times 2 \text{ matrices w/ real entries} \}$.

Then
$$M_{2\times2}(\mathbb{R}) \times M_{2\times2}(\mathbb{R}) \xrightarrow{\ \bullet\ } M_{2\times2}(\mathbb{R})$$
$$(A, B) \longmapsto A \cdot B$$

E.g. Subtraction is <u>not</u> a binary operation on $\mathbb{N}$, since $\exists\, a, b \in \mathbb{N}$ s.t. $a - b \notin \mathbb{N}$.

However, subtraction <u>is</u> a binary op. on $\mathbb{Z}$.

Here's a new example:

this triangle is symmetric, right? each altitude is a line of symmetry.

Also: rotations!

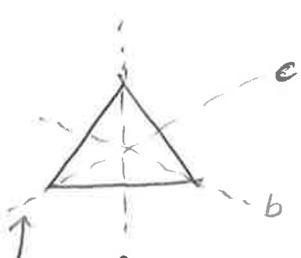
"Def": a symmetry of the triangle is a way to pick it up, move it around, and put it back down over itself.

"Rigid motions"

D_6 = set of symmetries of $\triangle$

$= \{ I, R, T, a, b, c \}$

- R: rotate 120° CW
- T: rotate 240° CW
- a: Flip over "a"
- b: Flip over b
- c: Flip over c.



These lines live on the chalkboard, not on $\triangle$.

Binary operation on D_6:

$D_6 \times D_6 \xrightarrow{\cdot} D_6$, $(a,b) \longmapsto$ "do b, then a". Denoted $a \cdot b$, or just ab.

E.g. $a \cdot R =$ 

$= b$.

$R \cdot a =$ 

$= c$

Do a worksheet!?

Ask each group to give a couple answers.

<u>Def</u> A <u>group</u> is a set, G, along w/ a binary op $G \times G \xrightarrow{\cdot} G$, satisfying 3 properties ("axioms")

- Identity: $\exists e \in G$ s.t. $\forall g \in G$, $e \cdot g = g \cdot e = g$. e is called the identity element of G.
- Associativity: $\forall a,b,c \in G$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- Inverses: $\forall g \in G$ $\exists h \in G$: $hg = gh = e$ — h is inverse of g. denoted g^{-1}, usually.

<u>E.g.</u> $(\mathbb{Z}, +)$ is a group (ie set $= \mathbb{Z}$, bin op $= +$)

<u>Pf</u> We should check $+$ really is a bin op, and also the group axioms.

E.g. (continued)

- $+$ is a binary op ✓
- id: $0+a = a+0 = a$ for all $a \in \mathbb{Z}$ ✓
- assoc: $a+(b+c) = (a+b)+c$ ✓
- inverses: $\forall a \in \mathbb{Z}, -a \in \mathbb{Z}$, and $-a+a = a+(-a) = 0$.

E.g. D_6 with $\cdot$ operation is a group, "Dihedral group of order 6"

If $(G, \cdot)$ is a group, the <u>order</u> of G is $\#G$.

<u>Note</u>: $aR \neq Ra$. The operation doesn't commute!

<u>Def</u> A group $(G, \circ)$ is said to be <u>Abelian</u> if, $\forall g, h \in G$, $g \circ h = h \circ g$.

E.g. $(\mathbb{Z}, +)$ is abelian, $(D_6, \cdot)$ isn't.

<u>Surprising fact</u>
Any group of order ≤ 5 is abelian.

Notation: $g^n = \underbrace{g \circ \cdots \circ g}_{n \text{ times}}$ ($n \geq 0$), $g^0 = e$, $g^{-n} = \underbrace{g^{-1} \circ \cdots \circ g^{-1}}_{n \text{ times}}$

Then: $g^m g^n = g^{m+n}$, $(g^m)^n = g^{mn}$ $\forall m, n \in \mathbb{Z}$.

<u>Def</u> Let $(G,\circ)$ be a group. A subset $H \subseteq G$ is called a subgroup if $(H,\circ)$ is also a group (with the same binary op).

<u>Prop</u> Let $(G,\cdot)$ be a group and H a subset of G. Then H is a subgroup iff $\forall h,g \in H$, $hg^{-1} \in H$.

<u>Pf</u>. $\Rightarrow$ is obvious.

$\Leftarrow$ Let $h \in H$. Then $h \cdot h^{-1} \in H$, so $e \in H$.

Then $e \cdot h^{-1} \in H$, so $h^{-1} \in H$.

Let $g \in H$ as well. Then $g(h^{-1})^{-1} = gh \in H$.

Let $f \in H$. Then $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ because $f,g,h \in G$ and the group op of G is associative.

$\blacksquare$

<u>E.g.</u> $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z},+)$

(Check 4 things: $+$ still a binary op? id? assoc.? inverses?)

Let $g \in G$. Then define $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. This is a subgroup of G, called the <u>cyclic subgp generated by g</u>.

If $G = \langle g \rangle$ for some $g \in G$, then G is called a <u>cyclic group</u>.

Math 4400 6/14.

- $\mathbb{Q}^\times$ eg.
- Add vs. Mult.
- Cyclic gps / order of an element.
- Lagrange's thm.
- Cosets.

Notes cyclic gps, $\mathbb{Q}^\times$, $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^\times$, Lagrange's theorem. full generality..?? cosets, $hH = H$ if $h \in H$.

- Question: is $(\mathbb{Q}, \cdot)$ a gp? No, $\mathbb{Q}^\times$ is.

- Notation: if $g \in G$, $g^n = \underbrace{g \circ \cdots \circ g}_{n \text{ times}}$ $g^{-n} = \underbrace{g^{-1} \circ \cdots \circ g^{-1}}_{n \text{ times}}$ $g^0 = e$.

Usual rules of exponents apply: $g^n \circ g^m = g^{n+m}$

$(g^n)^m = g^{nm}$

- $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. "Cyclic subgp" (always a subgp!) $g^m (g^n)^{-1} = g^{m-n}$. G is cyclic if $\exists g : G = \langle g \rangle$.
- Eg. $\mathbb{Z} = \langle 1 \rangle$
- Additive vs. mult. notation: The group operation is usually denoted by $+$ or $\cdot$
  $+$ for ab. gps, $\cdot$ for others. If using $+$, write ng instead of g^n.

- Eg. in D_6, $\langle R \rangle = \langle e, R, T \rangle$

Powerful theorem: Lagrange's theorem: Let G be a finite group, $H \subseteq G$ a subgroup. Then $\# H$ divides $\# G$.

Important consequences!

Let $g \in G$. The <u>order</u> of g is smallest positive n such that $g^n = e$. $o(g)$. $o(g) = \infty$ if no such n. (cf: order of a group).

<u>Note</u>: if G is finite, $o(g) < \infty$ for all $g \in G$;

Write $\{g, g^2, g^3 \ldots\} \subseteq G$. This set is finite,

So $\exists\ m > n$: $g^m = g^n$. Then $\underbrace{g^m g^{-n}}_{= g^{m-n}} = \underbrace{g^n g^{-n}}_{= e}$.

$m-n$ is positive since $m > n$.

<u>Prop</u> Let $(G, \cdot)$ be a group, $g \in G$.

Suppose $o(g) = k < \infty$. Then $\langle g \rangle = \{e, g, g^2, \ldots, g^{k-1}\}$.

<u>Proof</u> Divis algo. Clearly, $\{e, g, \ldots, g^{k-1}\} \subseteq \langle g \rangle$.

WTS $\langle g \rangle \subseteq \{e, g, \ldots, g^{k-1}\}$. Let $n \in \mathbb{Z}$. Then

$\exists\ q, r$: $n = qk + r$, $0 \le r < k$.

$\rightsquigarrow$ $g^n = g^{qk+r} = (g^k)^q g^r = e^q \cdot g^r = g^r \in \{e, g, \ldots, g^{k-1}\}$. ∎

<u>Corr</u> $o(g) = \# \langle g \rangle$.

§ $\mathbb{Z}/n\mathbb{Z}$ is a group.

$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

Group operation: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{+} \mathbb{Z}/n\mathbb{Z}$.

$[a], [b] \longmapsto [a+b]$.

(Need to check: this is well-defined!).

- Id: $[0]$,
- $-[a] = [-a]$,
- assoc: $([a]+[b])+[c]$
$= [a+b] + [c]$
$= [(a+b)+c] = [a+(b+c)]$
$= \ldots$

<u>note</u>: $m[a] = [ma]$.

- <u>E.g.</u> in $\mathbb{Z}/10\mathbb{Z}$, $o([5]) = 2$.
$o([3]) = 10$ $o([2]) = 5$ $o([4]) = 5$

HW problem.

<u>Prop</u> If $a, n \in \mathbb{Z}$, $n \neq 0$, then $o([a])$ in $\mathbb{Z}/n\mathbb{Z}$ is $n/\gcd(a,n)$.

<u>Pf</u>. $\operatorname{lcm}(a,n) = \dfrac{a \cdot n}{\gcd(a,n)}$

- $\mathbb{Z}/n\mathbb{Z}$ <u>not</u> a gp under mult.
- But, $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \mid \gcd(a,n)=1\}$.
- Binary op? "Fact 2" from last Friday (6/9/17).

- (State Lagrange)
- Consequences: if $g \in G$, then $o(g) \mid \# G$, (G finite.)
- What's $\# (\mathbb{Z}/n\mathbb{Z})^\times$? It's $\varphi(n)$!
- So $\forall x \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\exists k : \varphi(n) = k \cdot o(g)$ $\Rightarrow x^{\varphi(n)} = e = 1$
- Euler's formula is a quick consequence! And a small part of a larger picture.
- Cosets: show $h \cdot H = H$.
- Pf of Lagrange: $x_i^{-1} x_j \in H \Rightarrow x_i H = x_i (x_i^{-1} x_j H) = x_j H$.

Math 4400, 6/19/17

- Restate Lagrange's thm.

§ Cosets Let $S \subseteq G$ (subset), $x \in G$. Define $xS = \{xs \mid s \in S\}$

- Let $H \subseteq G$ be a subgroup, $x \in G$. xH is called a **left coset** of H. Sim, right coset.
- No longer a subgp! Eg. $3\mathbb{Z} \subseteq \mathbb{Z}$. $1 + 3\mathbb{Z}$ is a coset. $1 + 3\mathbb{Z} = \{\ldots, -2, 1, 4, 7, 10\} = [1]_3$
- Note: if $h \in H$, then $hH = H$.

  Pf
  - Clearly $hH \subseteq H$, since H is a group.
  - Let $h' \in H$. Then $h' = h \cdot (h^{-1} h') \in hH$. So $H \subseteq hH$.
- Note: $x \cdot (yH) = \{xz \mid z \in yH\} = \{xyh \mid h \in H\} = (xy)H$.

- Let $x_1, x_2 \in G$. If $x_1H \cap x_2H \neq \emptyset$, then $x_1H = x_2H$.

Pf let $y \in x_1H \cap x_2H$. Then $\exists h_1, h_2 \in H$ s.t.

$y = x_1h_1 = x_2h_2$. $\Rightarrow h_1 = x_1^{-1}x_2h_2 \Rightarrow h_1h_2^{-1} = x_1^{-1}x_2$,

so $x_1^{-1}x_2 \in H$.

Thus $x_1H = x_1(x_1^{-1}x_2H) = (x_1x_1^{-1}x_2)H = x_2H$. ■

- Note: if H finite, $\#(xH) = \#H$. Pf: $H \xrightarrow{\cdot x} xH$ is a bijection
- Proof of Lagrange's theorem:

  G finite, $H \leq G$ a subgroup.

  - If $H = G$, ✓ otherwise, $\exists x_1 \in G \setminus H$. Then

    $x = xe \in xH$, but $x \notin H$. So $xH \neq H$. So $xH \cap H = \emptyset$.

  - If $H \cup xH = G$, then $\#G = \underbrace{2 \cdot \#H}_{\text{because } H, xH \text{ disjoint}}$, so we're done.

    Otherwise, $\exists x_2 \in G : x_2 \notin H \cup x_1H$

    Then $x_2H \neq H$, $x_2H \neq x_1H$, so $x_2H \cap H = \emptyset$, $x_2H \cap x_1H = \emptyset$.

  - Continue the process, until we get

    $G = x_0H \cup x_1H \cup \dots \cup x_nH$, where $x_iH \cap x_jH = \emptyset$ whenever $0 \leq i < j \leq n$.
    $(x_0 = e)$

$\Longrightarrow \#G = (n+1)\,\#H$.

Note: the process terminates since G is finite: $n+1 \leq \#G$.

- Another application: let p = prime, G a group of order p. Then G is cyclic.

<u>Pf</u> let $g \in G$, $g \neq e$ (possible, since $\# G \geq 2$!)

Then Lagrange $\Rightarrow$ $\# \langle g \rangle$ divides p, so $\# \langle g \rangle = 1$ or $\# \langle g \rangle = p$.

If $\# \langle g \rangle = 1$, then $g^2 = g \Rightarrow g^2 g^{-1} = g g^{-1} \Rightarrow g = e$.

So $\# \langle g \rangle = p$, and $G = \langle g \rangle$. $\boxtimes$

<u>Note</u>: if G a group, $\{e\} \leq G$ is a subgp. Called the trivial group/subgroup.

- Eg of Lagrange: $\mathbb{Z}/12\mathbb{Z}$ has the following subgroups: $\{[0]\}$, $\{[0], [3], [6], [9]\}$, $\{[0], [4], [8]\}$, $\{[0], [2], [4], [6], [8], [10]\}$, $\{[0], [6]\}$

Rings / Fields

- Most of our examples of groups have more than one binary operation:

  $\mathbb{Z}$ has $+, \cdot$, $M_{n\times n}(\mathbb{R})$ has $+, \cdot$, $\mathbb{Z}/n\mathbb{Z}$.

  Just one op: D_6, $GL_n(\mathbb{R})$

Def (Noether)

- A ring is a set R with two binary ops, denoted $+$ and $\cdot$ (called "addition" and "mult") satisfying four properties:
  - $(R,+)$ is an abelian group. Id element denoted 0.
  - mult. is associative
  - R has a multiplicative identity: $\exists r\in R: \forall s\in R:$
    $r\cdot s = s\cdot r = s$.

    Usually denoted 1, or 1_R
  - Distributive prop: $\forall a,b,c\in R$: $a\cdot(b+c) = a\cdot b + a\cdot c$.
    and $(b+c)a = b\cdot a + c\cdot a$

E.g. $\mathbb{Z}$ is a ring, $\mathbb{Z}/n\mathbb{Z}$, $M_{n\times n}(\mathbb{R})$. E.g. $\mathbb{Z}[\sqrt{D}]$, $D\in\mathbb{Z}$.

Note $(R,\cdot)$ almost a group, but might not have inverses; Let $R^\times = \{r\in R \mid \exists s\in R: rs=sr=1\}$.

Claim $(R^\times,\cdot)$ is a group.

Binary op? Let $a,b\in R^\times$. Then $\exists c,d\in R: ac=ca=1$
$bd=db=1$.

$\Rightarrow (ab)(dc) = (dc)(ab) = 1$, so $ab\in R^\times$

• id ✓ • assoc: ✓ • inverses: ✓

Note: $\forall r \in R$, $r \cdot 0 = 0$: **Note** $1 \in R^\times$ $\forall$ rings.

$$r\cdot 0 \underset{\substack{\uparrow \\ \text{add. id}}}{=} r\cdot(0+0) \underset{\substack{\uparrow \\ \text{distrib}}}{=} r\cdot 0 + r\cdot 0;$$

Then $r\cdot 0$ has additive inverse, since $(R,+)$ a gp.

$$\Rightarrow \quad r\cdot 0 + (-r\cdot 0) = r\cdot 0 + r\cdot 0 + -r\cdot 0$$

$$\Rightarrow \quad 0 = r\cdot 0$$

Note: if $1=0$, then $R=\{0\}$:

Pf Let $r\in R$. Then $0 \underset{\substack{\uparrow \\ \text{above}}}{=} r\cdot 0 \underset{\substack{\uparrow \\ 1=0}}{=} r\cdot 1 \underset{\substack{\uparrow \\ \text{def of } 1}}{=} r$.

From now on: our rings will satisfy a fifth axiom, $1\neq 0$. Equiv: $\{0\}$ is not a ring

(Kinda like saying $0! = 1$; done for convenience)

• **Def** a ring is <u>commutative</u> if $a\cdot b = b\cdot a$ $\forall a,b\in R$.

• **Note**: if $1\neq 0$, then $\forall r$: $r\cdot 0 = 0 \neq 1$, so 0 is not invertible.

Eg. $M_{2\times 2}(\mathbb{R})$ <u>not</u> comm. $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ are.

• **Def** A comm. ring is called a <u>field</u> if $R^\times = R\setminus\{0\}$.

E.g. $M_{n\times n}(\mathbb{R})$ not comm.

$\underset{\substack{\| \\ \mathbb{F}_p}}{\mathbb{Z}/p\mathbb{Z}}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all fields.

- pp 58, 59.

- Usual notation: if $r \in R$, its additive inverse denoted $-r$. If mult. inverse exists, it's denoted r^{-1}.
  r^2, $2r$, etc.
- Maybe a hw question? $(-1)\cdot r = -r \quad \forall r \in R$.
- Define fields, give examples..

$$(a+b)^2 = a^2 + ab + ba + b^2$$
$$= a^2 + 2ab + b^2$$
if R comm.

$\rightsquigarrow a^2 - b^2 = (a+b)(a-b)$

- **Def** if $a \in R$, $a \neq 0$, then a is called a zero divisor if $\exists b \in R \setminus \{0\}$ such that $a \cdot b = 0$.
- Eg in $\mathbb{Z}/10\mathbb{Z}$, 5 is a zero-divisor.

Prop Fields don't have zero-divisors.

Pf if $a \cdot b = 0$, and $a \neq 0$, then $a^{-1} \in R$.

Thus: $a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$

$$a^{-1}\cdot a\cdot b = 1 \cdot b = b.$$

Cor Let F be a field and $r \in F$. If $r^2 = 1$, then $r = 1$ or $r = -1$.

Proof: $r^2 = 1 \Rightarrow r^2 - 1 = 0 \Rightarrow (r+1)(r-1) = 0$

No zero-divisors! So $r+1 = 0$ or $r - 1 = 0$
$\Rightarrow r = -1$ $r = 1$.

- Cor: Wilson's theorem: $(p-1)! \equiv -1 \mod p$, whenever p is a prime.

- Eg. $6! \mod 7 \equiv ?$

  Note: $6 \equiv -1$, $1 \equiv 1$, $2\cdot 4 \equiv 1$, and $3 \cdot 5 \equiv 1$.

  So $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv -1$.

  Each # but 6, 1 can be paired with its inverse mod 7.

Pf (Wilson) Let $x \in (\mathbb{Z}/p\mathbb{Z})^\times = \{[1],[2],\ldots,[p-1]\}$.

Then $x^{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times$. If $x = x^{-1}$, then $\underset{\overset{\|}{1}}{xx^{-1}} = x^2$

$\Rightarrow x = [1]$ or $x = -[1] = \cancel{[-1]} = [p-1]$.

Thus, each number in $\{[2], \ldots, [p-2]\}$ can be paired with its inverse, so

$(p-1)! \equiv (p-1)\cdot(p-2)\cdots 1 \equiv (p-1)\cdot 1 \equiv -1$.

§ Characteristic & Frobenius (3.2)

Let F be a field, $1_F \in F$ mult. id.

Then, for $n \in \mathbb{N}$, $n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ times}}$.

NOTE if $n\cdot 1 = 0$, then $n \cdot r = \underbrace{r + \cdots + r}_{n} = \underbrace{(1 + \cdots 1)}_{n} \cdot r = 0$.

Thus: if $n, m \in \mathbb{N}$, $(n+m)\cdot 1 = n\cdot 1 + m \cdot 1$,
$(nm)\cdot 1 = (n\cdot 1)\cdot(m \cdot 1)$.

Def $\min\{n \in \mathbb{N} \mid n \neq 0,\ n\cdot 1 = 0\}$ is the characteristic of F. If that set is empty, $\operatorname{char} F = 0$.

- Note: If $\text{char } F \neq 0$, then $\text{char } F =$ order of 1_F in the group $(F, +)$

- <u>Note</u> if $\text{char } F \neq 0$, then $\text{char } F$ is a prime number.

<u>Pf</u> by contradiction. Let $\text{char } F = n$, where $n \in \mathbb{N}$ not prime, Then $\exists\, a, b \in \mathbb{N}$: $a \cdot b = n$ and $1 < a, b < n$.

Then $0 = n \cdot 1_F = (a \cdot b) \cdot 1_F = (a \cdot 1_F) \cdot (b\, 1_F)$.

Fields have no zero-divisors, so either $a \cdot 1_F = 0$
or $b \cdot 1_F = 0$.

Either way, contradicts minimality of n.

<u>Eg.</u> $\text{char } \mathbb{Q}$, $\text{char } \mathbb{R}$, $\text{char } \mathbb{C} = 0$,
$\text{char } \mathbb{F}_p = p$.

<u>Def</u> Let F be a field of char p for some prime p. The <u>Frobenius map</u> on F is the function $F \xrightarrow{Fr} F$ defined by $x \longmapsto x^p$.

<u>Note</u>: $Fr(ab) = Fr(a) \cdot Fr(b)$: $(ab)^p = ab \cdot ab \cdot \_ \cdot ab$
$= a^p b^p$ since fields are comm.

More surprisingly:

<u>Prop (3.13)</u> $Fr(a+b) = Fr(a) + Fr(b)$.

Proof $(a+b)^p = \sum \binom{p}{i} \cdot a^i \, b^{p-i}$

If $i=0$ or p, $\binom{p}{i} = 1$.

If $0<i<p$: $\binom{p}{i} = \dfrac{p\cdot(p-1)\cdots(p-i+1)}{i\cdot(i-1)\cdots 1} \in \mathbb{Z}$

p appears in numerator, but can't divide anything in denom, since $i<p$. So $\binom{p}{i} = p\cdot k$, some $k \in \mathbb{N}$.

Thus $\binom{p}{i}\cdot a^i b^{p-i} = pk \cdot a^i b^{p-i} = 0$, when $0<i<p$.

- Next time: Gaussian ints, Gaussian ints mod p, Homomorphs / Isoms, polynomials over a ring, divis. thereof, $\mathbb{F}_p$ - fixed field of Frob.

Math 4460 6/23/17

§ Quadratic integers

Define later, if at all...
- A quadratic integer is root of x^2+Bx+C, where $B, C \in \mathbb{Z}$
- A quadratic rational is " " " " " $B, C \in \mathbb{Q}$

E.g. $\sqrt{3}$ is a root of x^2-3,

$\frac{1+\sqrt{5}}{2}$ is a root of x^2-x-1

Let $B, C \in \mathbb{Z}$. Then $\dfrac{-B \pm \sqrt{B^2-4C}}{2}$ is a root of

$\sqrt{-1}$ = root of $x^2+1=0$.

Let ω be a quadratic integer. Then the set $\mathbb{Z}[\omega] := \{a+b\omega \mid a,b\in\mathbb{Z}\}$ is a ring, w/ usual $+$, mult of cx numbers.

Pf First, let's check $+$ and $\cdot$ are binary operations.

By assumption, $\exists B, C \in \mathbb{Z}$ s.t. $\omega^2 + B\omega + C = 0$

Let $a+b\omega,\ c+d\omega \in \mathbb{Z}[\omega]$. Then $a+b\omega + c+d\omega = (a+c)+(b+d)\omega \in \mathbb{Z}[\omega]$.

$$(a+b\omega)\cdot(c+d\omega) = ac + ad\omega + bc\omega + bd\boxed{\omega^2} \longrightarrow \text{problem!}$$

$$= ac + (ad+bc)\omega + bd[-C + B\omega]$$

$$= ac - bdC + (ad+bc+bdB)\omega \in \mathbb{Z}[\omega]$$

Need to check: $0 \in \mathbb{Z}[\omega]$ ✓, if $a+b\omega \in \mathbb{Z}[\omega]$, then $-[a+b\omega] = -a-b\omega \in \mathbb{Z}[\omega]$, mult of cx #s is assoc ✓
$1 \in \mathbb{Z}[\omega]$, mult is assoc, distributive prop holds for cx #s ✓

Eg Gaussian ints, $\mathbb{Z}[i]$.

Similarly, $\mathbb{Q}[\omega]$ is a ring. In fact, it's a field! whenever ω a $\underline{\underline{\text{ratl}}}$ q

Pf Let ω be a root of $x^2+px+q=0$, where $p, q \in \mathbb{Q}$.

Then $\omega = \dfrac{-p \pm \sqrt{p^2-4q}}{2}$. Let $a+b\omega \in \mathbb{Q}[\omega]$ be non zero. Note: if $\sqrt{p^2-4q} \in \mathbb{Q}$, then $\omega \in \mathbb{Q}$, so $\mathbb{Q}[\omega] = \mathbb{Q}$ ✓ So assume $\sqrt{p^2-4q} \notin \mathbb{Q}$.

Skip, for space

Then $a+b\omega = \underbrace{a + b\cdot\frac{-p}{2}}_{\alpha} \pm \underbrace{\frac{b}{2}}_{\beta}\underbrace{\sqrt{p^2-4q}}_{D} = \alpha + \beta\sqrt{D}$.

- Since $\sqrt{D} \notin \mathbb{Q}$, $\alpha - \beta\sqrt{D} \neq 0$.

$$\Rightarrow \frac{1}{\alpha+\beta\sqrt{D}} = \frac{\alpha-\beta\sqrt{D}}{\alpha^2-\beta^2 D} = \frac{\alpha}{\alpha^2-\beta^2 D} + \frac{-\beta}{\alpha^2-\beta^2 D}\sqrt{D} \quad \blacksquare$$

E.g. $\mathbb{Q}[\sqrt{3}]$ is a field: if $a+b\sqrt{3} \neq 0$, then
$b \neq 0$

$$\frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-b^2 3} = \frac{a}{a^2-3b^2} + \frac{-b}{a^2-3b^2}\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$$

If $b=0$, $\frac{1}{a} \in \mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}]$ ✓.

Note: $a^2-3b^2 \neq 0$. O.w., $\sqrt{3} = \frac{a}{b}$, contradiction!

Pf $\sqrt{3}$ is irrational. o.w. $\sqrt{3} = \frac{a}{b}$, $a, b \in \mathbb{Z}$.
Let $a = p_1^{e_1} \cdots p_r^{e_r}$, $b = q_1^{f_1} \cdots q_s^{f_s}$ prime factorizations.
$3 q_1^{2f_1} \cdots q_s^{2f_s} = p_1^{2e_1} \cdots p_r^{2e_r}$. 3 appears odd # times on left and even # times on right. # uniqueness of factorization.

Start here. 6/26/17

Def $a^2-b^2 3$ is the norm of $a+b\sqrt{3}$, in $\mathbb{Z}[\sqrt{3}]$.

More generally: Def if $D \in \mathbb{Z}$, and $\alpha = a+b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$,
then $\bar{\alpha} := a-b\sqrt{D}$ = conjugate of α.

Norm of α := $N(\alpha) := \alpha \cdot \bar{\alpha} = a^2-b^2 D$.

§ Mod p

We can still do modular arithmetic in $\mathbb{Z}[\sqrt{3}]$:
say $a+b\sqrt{3} \equiv c+d\sqrt{3} \mod n$ if $a \equiv c \mod n$ and $b \equiv d \mod n$.

Equiv: if $\exists\, e+f\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ s.t. $n(e+f\sqrt{3}) = (a-c)+(b-d)\sqrt{3}$.

$\mathbb{Z}[\sqrt{D}]/_{n}\mathbb{Z}[\sqrt{D}]$ = set of equivalence classes of elements in $\mathbb{Z}[\sqrt{D}]$ mod n.

Eg. Let $a+b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, Then $a \equiv 0$ or 1 mod 2
$b \equiv 0$ or 1 mod 2.

So $a+b\sqrt{3} \equiv$ one of: $0+0\sqrt{3}$, $1+0\sqrt{3}$
$0+1\sqrt{3}$, $1+1\sqrt{3}$.

mod 2.

Thus: $\mathbb{Z}[\sqrt{3}]/2\mathbb{Z}[\sqrt{3}] = \{[0], [1], [\sqrt{3}], [1+\sqrt{3}]\}$

In general: if $\sqrt{D} \notin \mathbb{Z}$, then $\mathbb{Z}[\sqrt{D}]/_{n}\mathbb{Z}[\sqrt{D}]$ has n^2 elements. (What if $\sqrt{D} \in \mathbb{Z}$?)

What are the invertible elements of $\mathbb{Z}[\sqrt{3}]/p\mathbb{Z}[\sqrt{3}]$? ($p$ prime).

Fact: • α invertible mod p iff $N(\alpha) \not\equiv 0$ mod p.
• if $N(\alpha) \equiv 0$, α is a zero-divisor. (obv)

Eg $5+3\sqrt{3}$ mod 7: $N(5+3\sqrt{3}) = -2$.

$(-2)^{-1}$ mod 7 is 3.

$3 \cdot (5-3\sqrt{3}) \cdot (5+3\sqrt{3}) \equiv (1-2\sqrt{3})(5+3\sqrt{3}) \equiv 5-7\sqrt{3}-18$
$\equiv 1$ mod 7.

More generally, in $\mathbb{Z}[\sqrt{D}]$, if $N(\alpha) \not\equiv 0 \mod p$,

then $\exists$ inverse $N(\alpha)^{-1}$, Then $N(\alpha)^{-1} \cdot \bar{\alpha} \cdot \alpha = N(\alpha)^{-1} \cdot N(\alpha) = 1$

So $N(\alpha)^{-1} \bar{\alpha}$ is the inverse of α.

* (Start here, 6/28)

<u>Prop</u> Let $R = \mathbb{Z}[\sqrt{D}]$, where $\sqrt{D} \notin \mathbb{Z}$. Let p be an odd prime not dividing D.

- If D not a square mod p, then $\#(R/pR)^{\times} = p^2 - 1$
- If D is, then $\#(R/pR)^{\times} = (p-1)^2$.

<u>Q</u> When is D a square mod p? (Ch. 6!)

<u>Pf</u> If $\alpha = x + y\sqrt{D} \not\equiv 0$, and $N(\alpha) \equiv 0 \mod p$, then

$x^2 - y^2 D \equiv 0$, so $D \equiv (xy^{-1})^2$ and $y \not\equiv 0$, is a square mod p.

<u>Idea</u> if D not a sq mod p, then all nonzero elt's are invertible!

If D is a square mod p, then $D \equiv s^2$. If

$N(\alpha) = x^2 - y^2 D \equiv 0$, then $(x+ys)(x-ys) \equiv 0$

$\Rightarrow x + ys \equiv 0$ or $x - ys \equiv 0$.

p pairs $\left\{ \begin{array}{l} \Rightarrow x \equiv 0, y \equiv 0, \text{ or} \\ x \not\equiv 0, y \equiv -xs^{-1} \end{array} \right.$ $\qquad$ $\left. \begin{array}{l} x \equiv 0 \text{ and } y \equiv 0, \text{ or} \\ x \not\equiv 0, y \equiv xs^{-1} \not\equiv -xs^{-1} \end{array} \right\}$ p pairs.

since $p \neq 2$.

\# sols to $x^2 - y^2 D \equiv 0$ is $2p - 1$.

$\Rightarrow \#(R/pR)^{\times} = p^2 - 2p + 1 = (p-1)^2$

If $p = 2$: D <u>is</u> a square, and $\#(R/pR) = p^2 - p$.

$\Rightarrow$ another example of a finite field!!

E.g. $\mathbb{Z}[i]/3\mathbb{Z}[i]$ is a field w/ 9 elements:

$\{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$.

- Next: homomorphs, isoms, polynomials over a ring/field.

§ Loose ends

Polynomial rings: first, define, give examples. two main things to know

- they exist!
- Polynomials over a field behave like we're used to.

Tying up Loose Ends

Math 4400, Summer 2017

These notes are meant to supplement the course text. They discuss some basic ring/group theory that is used later in the book, but not really discussed anywhere in detail.

1 Polynomial rings

Let R be a ring. For simplicity's sake, we'll assume always assume that R is commutative in these notes. We can use R to build a new ring, called the ***ring of polyonomials over R***, and denoted $R[X]$. As a set, $R[X]$ is defined to be:

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; n \in \mathbb{N}, \text{ and } a_i \in R \text{ for all } i \right\}$$

Addition and multiplication in $R[X]$ are defined in the usual way that we define addition and multiplication of polynomials: if $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{i=0}^{m} b_i X^i$, then

$$f + g = \sum_{i=0}^{\max(m,n)} (a_i + b_i) X^i \qquad f \cdot g = \sum_{i=0}^{m+n} \sum_{j=0}^{i} a_j b_{i-j} X^i$$

(we define $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$)

If $f = \sum_{i=0}^{n} a_i X^i$ is an element of $R[X]$, then the ***degree*** of f is defined to be $\max\{i \in \mathbb{N} \mid a_i \neq 0\}$. If $a_i = 0$ for all i, then $f = 0_R$, and the degree of f is defined to be $-\infty$. The degree of f is denoted $\deg f$. If $n = \deg f \geq 0$, then a_n is called the ***leading coefficient*** of f.

Example. $\mathbb{Z}[X]$ is the set of polynomials with integer coefficients. Elements include $3X^5 - 6$ and $X + 1$. As usual,

$$(3X^5 - 6) + (X + 1) = 3X^5 + X - 5$$

and

$$(3X^5 - 6) \cdot (X + 1) = 3X^6 + 3X^5 - 6X - 6$$

□

Example. Let $R = \mathbb{Z}/5\mathbb{Z}$. Then $R[X]$ is the set of polynomials with coefficients in $\mathbb{Z}/5\mathbb{Z}$. For instance, $[1]X^2 + [2]$ and $[3]X^3 + [4]X^2 + [1]X$ are elements of $R[X]$. In this ring,

$$([1]X^2 + [2]) + ([3]X^3 + [4]X^2 + [1]X) = [3]X^3 + [5]X^2 + [1]X + [2]$$

But $[5] = [0]$ in $\mathbb{Z}/5\mathbb{Z}$, so

$$([1]X^2 + [2]) + ([3]X^3 + [4]X^2 + [1]X) = [3]X^3 + [0]X^2 + [1]X + [2]$$

It's a little silly to write things this way, though. Usually we omit the "$[0]X^2$" and the $[1]$s:

$$(X^2 + [2]) + ([3]X^3 + [4]X^2 + X) = [3]X^3 + X + [2]$$

Proof. By Lemma 1.2, there exist $g, r \in k[X]$ such that

$$f = g \cdot (X - \alpha) + r \tag{1}$$

and $\deg r < \deg(X - \alpha) = 1$. Thus $\deg r = 0$ or $\deg r = -\infty$. In either case, we know $r \in k$. Then, evaluating both sides of equation 1 at α, we get

$$f(\alpha) = g(\alpha)(\alpha - \alpha) + r(\alpha) = g(\alpha) \cdot 0 + r = r$$

But α is a root of f, so $f(\alpha) = 0$. Thus $r = 0$ and $f = g \cdot (X - \alpha)$. □

Lemma 1.4. *Let $f, g \in k[X]$. Then* $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Proof. We define $n \cdot -\infty = -\infty \cdot n$ for all $n \in \mathbb{N}$, and this takes care of the case that $f = 0$ or $g = 0$. So assume $f \neq 0$ and $g \neq 0$. So let $\deg f = n \geq 0$ and $\deg g = m \geq 0$. Then we can write $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{i=0}^{m} b_i X^i$ for some $a_i, b_i \in R$. Then $f \cdot g = \sum_{i=0}^{m+n} c_i X^i$, where

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

for all i. Thus $c_{n+m} = a_n b_m \neq 0$, since $a_n \neq 0$, $b_m \neq 0$, and fields don't have zero-divisors. This proves the lemma. □

Skip

Caution. This lemma doesn't hold for polynomials over an arbitrary ring. For instance, let $R = \mathbb{Z}/6\mathbb{Z}$. If $f = 2X^2 + 1$ and $g = 3X$ are elements of $R[X]$, then $fg = 3X$, so $\deg(fg) = 1 < \deg f + \deg g$. In general, if R is any ring and f and g are any elements of $R[X]$, the most we can say is that $\deg(fg) \leq \deg f + \deg g$.

Proof of Theorem 1.1. We prove this by induction on the degree of f. If $\deg f = 0$, then f is some nonzero constant, so it has no roots. Now let $d \in \mathbb{N}$ and suppose the theorem is true for polynomials of degree d. Let f be a polynomial of degree $d + 1$. We wish to show that f has at most $d + 1$ roots. If f has no roots, then we're done since $0 \leq d + 1$. Otherwise, f has some root r. By Lemma 1.3, we can write $f = g \cdot (X - r)$ for some polynomial g. By Lemma 1.4, we have $\deg g + 1 = \deg f$, so $\deg g = d$. Now suppose that s is a root of f. That means $f(s) = g(s) \cdot (s - r) = 0$. Since k is a field, this means either $g(s) = 0$ or $s - r = 0$. In other words, either s is a root of g or $s = r$. Thus the set of all roots of f is $\{\text{roots of g}\} \cup \{r\}$. But, by the inductive hypothesis, g has at most d roots. Thus f has at most $d + 1$ roots □

Sketch?

2 Groups, rings, and functions

Our next object of study is the set of functions between two groups. Consider the groups $(\mathbb{Z}/3\mathbb{Z}, +)$ and $(\mathbb{Z}/9\mathbb{Z}, +)$. There are many functions from one set to the other. For instance, we could define a function $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ by setting $f([0]_3) = [4]_9$, $f([1]_3) = [7]_9$, and $f([2]_3) = [2]_9$. However, most functions, like the one above, are not very interesting—they have nothing to do with the group structures on $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$! On the other hand, some functions are nice. For instance, the following function,

$$f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}, \ [n]_3 \mapsto [3n]_9$$

2.1 Isomorphisms

Sometimes two groups can really be the same, even if they look different. For instance, consider the following two groups: one group is $\mathbb{Z}/4\mathbb{Z}$ under addition, and the other is the set, $G = \{I, A, B, C\}$ under matrix multiplication, where

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Clearly, $\mathbb{Z}/4\mathbb{Z}$ and G are two different sets, so $\mathbb{Z}/4\mathbb{Z}$ and G are not literally the same group. However, they have quite a similar structure:

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\cdot$	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

These two tables are basically the same table but labeled differently: if you take the table on the left and replace each [0] with an I, each [1] with A, each [2] with B, and each [3] with C, then you get the table on the right. In this sense, the groups G and $\mathbb{Z}/4\mathbb{Z}$ have exactly the same "structure." This leads to the following deinitions:

Definition 3. *Let G and H be two groups. A function $f : G \to H$ is called a* **group isomorphism** *if:*

- *f is a group homomorphism, and*
- *f is a bijection*

We define ring isomorphisms in exactly the same way: just replace each instance of "group" in the definition above with "ring". Two groups/rings are said to be ***isomorphic*** if there exists an isomorphism from one to the other. This means they have the same structure.

Example. In the example above (right before the definition), the function $f : \mathbb{Z}/4\mathbb{Z} \to G$ defined by $f([0]) = I, f([1]) = A, f([2]) = B, f([3]) = C$ is an isomorphism. Thus, $\mathbb{Z}/4\mathbb{Z}$ and G are isomorphic. We usually use the symbol $\cong$ to mean "isomorphic". So we write $\mathbb{Z}/4\mathbb{Z} \cong G$. $\square$

Example. Let $\mathbb{R}$ be the group of real numbers under addition, and let $\mathbb{R}^+$ be the group of positive real numbers under multiplication. Then the function $\exp : \mathbb{R} \to \mathbb{R}^+$ is an isomorphism. This function is a homomorphism, since $\exp(a + b) = \exp(a) \cdot \exp(b)$ for all $a, b \in \mathbb{R}$, so we just have to show exp is a bijection. In other words, given any $y \in \mathbb{R}^+$, we must show there exists a unique $x \in \mathbb{R}$ such that $\exp(x) = y$. This unique x is given by $\ln(y)$, so we're done. $\square$

Math 4400

- Last week: $\#\left(\mathbb{Z}[\sqrt{D}]/p\,\mathbb{Z}[\sqrt{D}]\right)^{\times} = \begin{cases} p^2-1, & D \text{ not a square mod } p \\ (p-1)^2 & D \text{ is.} \end{cases}$

- Question: when is D a square mod p?
Old questions: Fermat, 1600's: -1 is a square mod p iff $p \equiv 1 \mod 4$.

- Euler, Legendre attacked the general problem w/o completely answering it.

- Gauss: answers the question w/ his "quadratic reciprocity" law: (1797)
  Let $p \neq q$ be odd primes.
  - if $p \equiv 1$ or $q \equiv 1 \mod 4$, then p is a square mod q iff q is square mod p.
  - if $p \equiv q \equiv 3 \mod 4$, p is a square mod q iff q is <u>not</u> a square mod p.

- We'll see later how computations reduce to this.

- For now: chapter 5.1: let $m, k > 0$ be integers. $a \in \mathbb{Z}$.

Solve: $x^k \equiv a \mod m$.

If m small, we can just try everything

• More systematic way: use group theory!

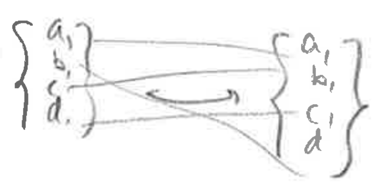
• (Proposition 19) Let G be a finite group of order n, let $k \in \mathbb{Z}$ with $\gcd(k,n) = 1$.
~~(Using Bezout's lemma, let $u,v \in \mathbb{Z}$ s.t. $ku+nv=1$)~~
Let u be the inverse of k mod n. Then "$x = a^u$" is the <u>unique</u> solution to "$x^k = a$" for all $a \in G$.

<u>Proof</u> $ku \equiv 1 \mod n$, so $\exists v \in \mathbb{Z}$: $ku = 1 + nv$.
Thus $(a^u)^k = a^{uk} = a^{1+nv} = a \cdot (a^n)^v$. By Lagrange, $o(a)$ divides n. In p'tic, $a^n = e$.

$$a^n = \left(a^{o(a)}\right)^{n/o(a)}$$

$$\Rightarrow (a^u)^k = a \cdot e^v = a.$$

We have shown a^u is a solution. Why is it unique? Well, we just proved that the function $G \xrightarrow{f} G$, $x \overset{f}{\longmapsto} x^k$ is onto: $\forall a \in G$, $f(a^u) = a$. Since G is finite, that means any onto function $G \longrightarrow G$ is automatically one-to-one! <u>E.g.</u>



every onto function is automatically 1-1.

So a^u is <u>unique</u> preimage of a, <u>i.e.</u> <u>unique</u> sol'n to $x^k = a$. ∎

- How to solve $x^k \equiv a \mod m$?

Apply the above theorem to the group $(\mathbb{Z}/m\mathbb{Z})^\times$:

- if $\gcd(a,m) = 1$, and
- $\gcd(k, \varphi(m)) = 1$, then

$x = a^u$ is the unique sol'n, where $k \cdot u \equiv 1 \mod \varphi(m)$.

- Eg. Solve $x^7 \equiv 13 \mod 100$.

$\varphi(100) = 100 \cdot (1-\frac{1}{2}) \cdot (1-\frac{1}{5}) = 40$.

$\gcd(13, 100) = 1$ ✓ $\gcd(7, 40) = 1$ ✓.

So the answer is 13^u where $7 \cdot u \equiv 1 \mod 40$.

$u = ?$ Euclidean algo! $40 = 5 \cdot 7 + 5$, $7 = 5 + 2$, $5 = 2 \cdot 2 + 1$

$\Rightarrow 5 - 2 \cdot 2 = 1 \Rightarrow 5 - 2(7-5) = 1 \Rightarrow 3 \cdot 5 - 2 \cdot 7 = 1$

$\Rightarrow 3(40 - 5 \cdot 7) - 2 \cdot 7 = 1 \Rightarrow 3 \cdot 40 - 17 \cdot 7 = 1$,

So -17, equiv $-17 + 40 = 23$ is the inverse of $7 \mod 40$.

$\Rightarrow$ $\boxed{13^{23} \text{ is the answer!}}$

(What's $13^{23} \mod 100$ though?)

Trick for computing large powers:

- start by writing 23 in binary, i.e. as a sum of powers of 2:

$23 = 16 + 4 + 2 + 1$

$\Rightarrow 13^{23} = 13^{16} \cdot 13^4 \cdot 13^2 \cdot 13^1$

$13^2 \equiv 69 \mod 100$

$13^4 \equiv (69)^2 \equiv 61 \mod 100$

$13^8 \equiv (61)^2 \equiv 21 \mod 100$

$13^{16} \equiv (21)^2 \equiv 41 \mod 100$

$\Rightarrow 13^{23} \equiv 41 \cdot 61 \cdot 69 \cdot 13 \equiv 97 \mod 100$

$\equiv -3 \mod 100$

Check: $(-3)^7 = -2187 \equiv 13 \mod 100$ ✓

Two questions: what if $\gcd(a, m) \neq 1$?

what if $\gcd(k, \varphi(m)) \neq 1$?

First one: chinese remainder thm!

Eg $x^4 \equiv 6 \mod 10 = 5 \cdot 2$

First solve $x^4 \equiv 6 \mod 5$,

$y^4 \equiv 6 \mod 2$

$\Rightarrow x \equiv 1 \mod 5$, $y \equiv 0 \mod 2$

CRT: $\exists! z \in \mathbb{Z}/10\mathbb{Z}$ s.t. $z \equiv 1 \mod 5$, $z \equiv 0 \mod 2$

This z is the answer.

- Solving $x^k \equiv a \mod m$ when $\gcd(k, \varphi(m)) \neq 1$?

Very difficult!

- Simplest case: m an odd prime; $k=2$

($\varphi(m) = m-1$ = even, in this case)

$\Rightarrow$ when does $x^2 \equiv a \mod m$ have a solution?? Quadratic reciprocity!

"

7/5/17

- one more example of solving $x^k \equiv a \mod n$.
- $\sum_{d|n} \varphi(d) = n$
- Primitive roots: they give all the other ones.

One more example:

Solve $x^7 \equiv 3 \mod 17$

- $\varphi(17) = 16$, and $\gcd(7, 16) = 1$
- $\gcd(3, 17) = 1$

So the answer is 3^u where $7 \cdot u \equiv 1 \mod \varphi(17)$

$16 = 2 \cdot 7 + 2$, $7 = 3 \cdot 2 + 1$

$\Rightarrow 7 - 3 \cdot 2 = 1 \Rightarrow 7 - 3(16 - 2 \cdot 7) = 1$

$\Rightarrow 7 \cdot 7 - 3 \cdot 16 = 1$

$\Rightarrow 3^7 \mod 17.$

$3^7 = ?$ $\qquad 3^2 = 9, \quad 3^3 = 27 \equiv 10, \quad 3^4 \equiv 30 \equiv 13$

$\Rightarrow 3^7 = 3^4 \cdot 3^3 \equiv 130 \equiv 11 \mod 17$

$\Rightarrow x \equiv 11 \mod 17$ is the unique sol'n.

- Recall from the midterm: if $n \in \mathbb{Z}$, $n > 0$, and $d | n$, then $\varphi\left(\frac{n}{d}\right) = \#\{x \in \mathbb{Z} \mid 1 \leq x \leq n,\ \gcd(x,n) = d\}$

WTS $\displaystyle\sum_{e|n} \varphi(e) = n.$

Pf. $n = \#\{x \in \mathbb{Z} \mid 1 \leq x \leq n\} = \displaystyle\sum_{d|n} \#\{x \in \mathbb{Z} \mid 1 \leq x \leq n,\ \gcd(x,n) = d\}$

$$= \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{e|n} \varphi(e)$$

$e = n/d$

as d ranges thru $\{x \mid x|n\}$, $\frac{n}{d}$ ranges thru $\{x \mid x|n\}$ as well.

ie if $e|n$, $e = \frac{n}{d}$, for some unique d s.t. $d|n$.

§5.3 Primitive roots

$n \in \mathbb{Z}$, positive

Let F be a field. An element $\alpha \in F$ is called an nth root of unity if $\alpha^n = 1$.

Set of all such $:= \mu_n(F)$.

- Note: $\mu_n(F) \subseteq F^\times = F \setminus \{0\}$.
- if $x, y \in \mu_n(F)$, $xy^{-1} \in \mu_n(F)$? $(xy^{-1})^n = x^n y^{-n} = 1 \cdot 1^{-1} = 1$.

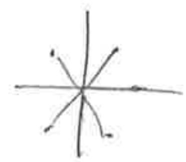
So $\mu_n(F)$ is a subgroup of $F^\times$

- Note: $\mu_n(F)$ is the set of all solutions to $x^n - 1 = 0$ in F. So $\# \mu_n(F) \leq n$.

- E.g. $F = \mathbb{C}$ complex #s.

$\mu_4(\mathbb{C}) = \{1, i, -1, -i\}$

$\mu_5(\mathbb{C}) = \{1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}\}$



$\mu_n(\mathbb{C}) = \{ e^{2\pi i \cdot k/n} \mid \underset{k \in \mathbb{Z}}{0 \leq k < n} \}$

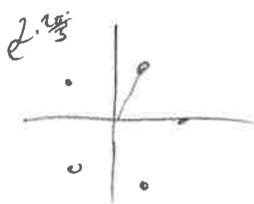
- Let $\alpha \in \mu_n(F)$. Then $o(\alpha) \leq n$ (thinking of α as an element of the group $F^\times$)

<u>Def</u> $\alpha \in F$ is called a <u>primitive</u> n^{th} root of unity if $\alpha \in \mu_n(F)$ and $o(\alpha) = n$.

- These are important since primitive roots give all the other ones!

- General fact: if G a group, $g \in G$, and $o(g) = n$, then $g, g^2, \dots, g^n = e$ are all distinct. (iff!)
- So if F a field and $\alpha \in F$ a primitive nth root, then $\alpha, \alpha^2, \dots, \alpha^n = 1$ are all distinct elements of $\mu_n(F)$. But we already knew $\# \mu_n(F) \leq n$. So $\mu_n(F) = \{\alpha^j \mid 1 \leq j \leq n\}$, $\rightsquigarrow$ $\mu_n(F)$ is cyclic!
- E.g. In $\mu_4(\mathbb{C})$: $i, -i$ are primitive 4th roots of unity.

  What are the primitive 5th roots of unity?



all of 'em! Except 1. 1 is never a primitive nth root if $n > 1$.

- Q: how many primitive roots?

<u>Prop 20</u>: If $\# \mu_n(F) = n$, then $\#$ primitive roots $= \varphi(n)$.

E.g. in $\mathbb{C}$: $e^{\frac{2\pi i}{n} j} = e^{\frac{2\pi i}{n} j'}$ iff $j \equiv j' \bmod n$.

So $\left\{ e^{\frac{2\pi i}{n} j}, \left(e^{\frac{2\pi i}{n} j}\right)^2, \dots, \left(e^{\frac{2\pi i}{n} j}\right)^n \right\}$ distinct iff

$\{ [j]_n, [2j]_n, \dots, [n \cdot j]_n \}$ all distinct.

$\Rightarrow$ $e^{\frac{2\pi i}{n} j}$ a primitive iff $o([j]_n) = n$ in $\mathbb{Z}/n\mathbb{Z}$.

- But $o([j]) = \frac{n}{\gcd(j,n)} = n$ iff $\gcd(j,n) = 1$.

Pf prop 20: Strong induction on n.

7/7/17 Last time, defined: • n^{th} root of unity,
• primitive root.

- In $\mathbb{C}$, # primitive n^{th} roots $= \varphi(n)$. Argued via modular arithmetic: $\left(e^{2\pi i/n}\right)^j = \left(e^{2\pi i/n}\right)^k \iff j \equiv k \bmod n$.
In fact, $\mu_n(\mathbb{C}) \cong \mathbb{Z}/n\mathbb{Z}$ as groups.
- Q: in a given field, how many primitive roots?
- Prop 20: Let F be a field, $n \in \mathbb{Z}$, $n > 0$. If $x^n - 1$ has n solutions, then # primitive roots is $\varphi(n)$
- Two ingredients: one is the formula

$$(x^n - 1) = (x-1)(x^{n-1} + x^{n-2} + \dots + 1)$$
$$= (x^n + x^{n-1} + \dots + x) + (-x^{n-1} - x^{n-2} \dots - 1)$$

- The other: if $g \in G$, $o(g) = n$, and $g^d = e$, then $n | d$. Pf: divis algo. Write $d = qn + r$, $0 \le r < n$.
$\Rightarrow e = g^d = g^{qn+r} = (g^n)^q \cdot (g^r) = g^r$
But $r < o(g)$, so $r = 0$.

Pf (prop 20): Strong induction!

- If $n=1$: # primitive 1^{st} roots of unity $= 1$ ✓
- Suppose $n \in \mathbb{N}$, $n>0$, and it's true $\forall k<n$.

Let $\alpha \in \mu_n(F)$. Then $o(\alpha) \mid n$. Note, by def, if $d = o(\alpha)$, ~~then~~ α is a primitive d^{th} root.

So # primitive n^{th} roots $= n - \sum_{\substack{d \mid n \\ d<n}}$ (# primitive d^{th} roots)

Now, let $d \mid n$, so $d\ell = n$, some $\ell \in \mathbb{N}$, $\ell \geq 1$.

$$\underbrace{x^n - 1}_{h(x)} = x^{d\ell} - 1 = (x^d)^\ell - 1 = \underbrace{(x^d - 1)}_{f(x)} \underbrace{(x^{d(\ell-1)} + x^{d(\ell-2)} + \dots + 1)}_{g(x)}$$

roots $h(x) \leq$ # roots $f(x)$ + # roots $g(x)$. ($<$ if f, g share roots)

But # roots $h(x) = n$ by assumption, and

roots $f \leq d$, # roots $g(x) \leq d\ell - d = n - d$. (for degree reasons)

Only possibility is # roots $f = d$.

$\Rightarrow$ by induction hyp., # primitive d^{th} roots $= \varphi(d)$ $\forall d \mid n$.

$\Rightarrow$ # primitive n^{th} roots $= n - \sum_{\substack{d \mid n \\ d<n}} \varphi(d) = \sum_{d \mid n} \varphi(d) - \sum_{\substack{d \mid n \\ d<n}} \varphi(d)$

$= \varphi(n)$ ∎

§5.5 : Cyclotomic polynomials

Let $n \in \mathbb{N}$. Then $\#\mu_n(\mathbb{C}) = n$. Define the n^{th} cyclotomic polynomial as

$$\Phi_n(x) = \prod_{\substack{\alpha \text{ primitive} \\ \text{root order} \\ n}} (x-\alpha)$$

Then $\deg \Phi_n = \varphi(n)$

E.g.

$$\Phi_1(x) = x-1$$
$$\Phi_2(x) = x+1$$
$$\Phi_3(x) = (x-e^{\frac{2\pi i}{3}})(x-e^{\frac{4\pi i}{3}})$$
$$= x^2+x+1$$

Alternatively: $x^3-1 = (x-1)(x-e^{\frac{2\pi i}{3}})(x-e^{4\pi i/3})$

$$\Rightarrow \Phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1.$$

$$\Phi_4(x) = (x-i)(x+i) = x^2+1$$

$$\Phi_5(x) = (x^5-1)/(x-1) = x^4+x^3+x^2+x+1$$

$$\Phi_6(x) = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2-x+1.$$

Note: always integer coefficients!

Note: coeffs always ± 1!

Except: $\Phi_{105}(x) : x^{48}+x^{47}+\ldots-x^{42}-2x^{41}-x^{40}$

Why integer coefficients?

Well, $x^n - 1 = \prod_{\alpha \in \mu_n(\mathbb{C})} (x - \alpha)$, Each $\alpha \in \mu_n(\mathbb{C})$ has

$o(\alpha) = d$, for some $d | n$. Thus

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \quad \text{or} \quad \Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}$$

Proceed by induction: $\Phi_1(x) = x - 1$ has integer coeffs, leading coeff $= 1$.

If true $\forall k < n$: Then $\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$ also has integer coeffs, leading coeff $= 1$.

Thus, it's clear leading coeff of $\Phi_n(x) = 1$.

Why are they all integers though?

Enough to prove the following fact:

If $f, g \in \mathbb{Z}[X]$, with g monic (ie leading coeff $= 1$), then $\exists!\, q, r \in \mathbb{Z}[x]$ w/ $f = qg + r$, $\deg r < \deg g$

Not to hard to convince yourself:

$$\begin{array}{r|l} & x^5 + x^4 + \cdots \\ \hline x - 1 & x^6 - 1 \\ & x^6 - x^5 \\ \hline & +x^5 - 1 \end{array} \qquad \begin{array}{r|l} & \frac{1}{2}x^5 + \cdots \\ \hline 2x - 1 & x^6 - 1 \\ & x^6 - \frac{1}{2}x^5 \\ \hline & \frac{1}{2}x^5 - 1 \end{array}$$

(Rigorous pf found in notes on polynomials)

Thus: $$x^n-1 = \prod_{\substack{d|n \\ d\neq n}} \Phi_d(x) \cdot \Phi_n(x)$$

$$= q \cdot \prod_{\substack{d|n \\ d\neq n}} \Phi_d(x) + r, \quad \deg r < \deg \prod \Phi_d(x)$$

Plug in any β s.t. β a primitive d^{th} root for some $d|n$: $\cancel{\beta^n - 1} = q(\beta) \cdot \cancel{\prod \Phi_d(\beta)} + r(\beta)$

$\Rightarrow \quad 0 = r(\beta)$.

$\Rightarrow \quad (x-\beta) \mid r(x) \quad \forall$ such β.

$\Rightarrow \quad \prod_{\substack{d|n \\ d\neq n}} \Phi_d(\beta) \mid r(x) \quad \Rightarrow \quad r = 0$ for degree reasons.

So $$\Phi_n(x) \cdot \prod_{\substack{d|n \\ d\neq n}} \Phi_d(x) = q \cdot \prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)$$

$$\Rightarrow \quad \Phi_n(x) = q \in \mathbb{Z}[x].$$

Math 4400 7/13/17 §6.1

- Let p = prime, $p \neq 2$ for whole lecture.
- HW problem: $\forall$ p prime, $\exists$ primitive $(p-1)^{st}$ root of unity in $\mathbb{Z}/p\mathbb{Z}$. Usually called a primitive root mod p. Let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be primitive root for whole lec.

- Q: which #s in $\mathbb{Z}/p\mathbb{Z}$ are squares? $p \neq 2$, prime.
- First Q: how many? Consider real #s:

  $\mathbb{R}^\times \xrightarrow{f} \mathbb{R}^\times$, $f(x) = x^2$. Each $a \in \mathbb{R}^2$ has 1 or 2 preimages / sq. roots

- $(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ works the same!

  $x \longmapsto x^2$

  Let $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ w/ $d \equiv a^2$. Then $d \equiv (-a)^2$

  $-a \not\equiv a$: o.w. $p \mid 2a$. But $p \nmid 2$, $p \nmid a$.

  If $a^2 \equiv b^2$, then $a^2 - b^2 = 0$, $\rightsquigarrow (a+b)(a-b) = 0$

  $\Rightarrow (a+b) = 0$ or $a-b = 0$ ($\mathbb{Z}/p\mathbb{Z}$ is a field).

  $\Rightarrow b = \pm a$

  So each $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ has 0 or 2 sq. roots.

  HW: half the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are squares, i.e. congruent to d^2, some $d \in \mathbb{Z}/p\mathbb{Z}$.

- Let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be primitive root mod p.

Then, $\forall \alpha \in (\mathbb{Z}/p\mathbb{Z})^\times \ \exists!\ n \in \{1, 2, \dots, p-1\}$ st. $\alpha = g^n$. (HW)

$\Rightarrow (\mathbb{Z}/p\mathbb{Z})^\times = \{g^1, g^2, \dots, \underset{1}{\underset{\shortparallel}{g^{p-1}}}\}$. Above work shows

<u>g^n a square iff n even</u>. Indeed, if n even, then $g^n = (g^{n/2})^2$. $\exists \frac{p-1}{2}$ even #s in the set $\{1, 2, \dots, p-1\}$, so $\exists \frac{p-1}{2}$ squares of the form $g^{(\text{even } \#)}$.

But there are only $\frac{p-1}{2}$ squares total! ∎

§ Euler's criterion

First some notation: The Legendre symbol. $\forall n \in (\mathbb{Z}/p\mathbb{Z})^\times$, define

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & n \text{ a square mod } p. \\ -1, & n \text{ not} \end{cases}$$

* It's not a fraction!! That — is just a symbol.

V. useful notation. E.g:

<u>Prop 22 (Euler's criterion)</u> Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then

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

<u>Pf</u> Let $a = g^n$. $\Rightarrow a^{\frac{p-1}{2}} \equiv (g^n)^{\frac{p-1}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)^n$

$\Rightarrow$ a square iff n even.

- What's $g^{\frac{p-1}{2}}$? Well $\left(g^{\frac{p-1}{2}}\right)^2 \equiv 1$.

But 1 has only two sq. roots mod p: $1, -1$.

$g^{\frac{p-1}{2}} \neq 1$, since g <u>primitive</u> $(p-1)^{\text{st}}$ root of 1.

$\Rightarrow$ $\boxed{g^{\frac{p-1}{2}} \equiv -1.}$ useful fact!

$\Rightarrow$ $a^{\frac{p-1}{2}} \equiv (-1)^n \equiv \begin{cases} 1, & n \text{ even} \Leftrightarrow a \text{ square mod } p. \\ -1, & n \text{ odd} \Leftrightarrow a \text{ isn't} \end{cases}$

Example: $p = 17$. Primitive roots: no great way to find them. Just try everything in $(\mathbb{Z}/17\mathbb{Z})^\times$.

Primitive roots: $\{3, 5, 6, 7, 10, 11, 12, 14\}$

Squares:

1	2	3	4	5	6	7	8	9	10	11
1	4	9	16	8	2	...				

$= \{1, 4, 9, 16, 8, 2, 15, 13\} = \{1, 2, 4, 8, 9, 13, 15, 16\}$

-1 a square!

Take any prim root raised to odd #: got non-square. eg $11^5 \equiv 10$, not sq.

Prim root to even #: $7^8 \equiv 16$

Try at home: compute a^8 for $a \in \mathbb{Z}$. Confirm Euler's formula.

<u>Note</u>: Generalized artin conj: if $a \neq \pm 1$, $a \neq d^2$, $\forall d \in \mathbb{Z}$, then $\exists$ inf. many p: a sq. mod p. Need GRH!

Consequences of Euler:

Prop 23: -1 a square mod p iff $p \equiv 1 \bmod 4$.

Ie $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv 3 \bmod 4 \end{cases}$ explain why only these 2 options.

Pf $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$. If $p = 4k+1$, $\frac{p-1}{2} = 2k$.

$\Rightarrow \left(\frac{-1}{p}\right) \equiv (-1)^{2k} = 1$. If $p \equiv 4k+3$, $\frac{p-1}{2} = 2k+1$.

$\Rightarrow \left(\frac{-1}{p}\right) \equiv (-1)^{2k+1} = -1$.

Properties of Legendre symbol: if $a \equiv b \bmod p$,

$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ (by def).

$\forall\ a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

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

But LHS $= \pm 1$, RHS $= \pm 1$. Congruent mod $p \Rightarrow =$.

Note: $x \longmapsto \left(\frac{x}{p}\right)$ is homomorph $(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}^\times$.

Note: $\left(\frac{n}{p}\right) = \left(\frac{q_1}{p}\right)^{e_1} \cdots \left(\frac{q_n}{p}\right)^{e_n}$, $n = q_1^{e_1} \cdots q_n^{e_n}$ $\longrightarrow$ So need: $\left(\frac{q}{p}\right) = ?$ p, q prime.

§6.3 When is 2 a square mod p?

Alternate pf: use Lagrange's thm. Suppose $-1 = a^2 \bmod p$.

($\Rightarrow a$ = prim 4th root) $\Longrightarrow$ $o(a) = 4$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ $\Longrightarrow$ $4 \mid p-1$. $\Rightarrow p \equiv 1 \bmod 4$.

$(a \neq 1,\ a^2 \neq 1)$

OTOH, if $p \equiv 1 \bmod 4$, then $\left(g^{\frac{p-1}{4}}\right)^2 = g^{\frac{p-1}{2}} = -1$

[I'm telling you how to find the sq root of 1)

- Prop 26: 2 is a square mod p iff $p \equiv 1$ or $p \equiv 7$ mod 8.

7/14/17: Recall: $\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ square} \\ -1, & a \text{ not square.} \end{cases}$

How to use QR.

Defined for $p \neq 2$ prime, $a \not\equiv 0$ mod p.

"Jacobi symbol" if p not prime.

E.g. Squares mod 5:

x	1	2	3	4
x^2	1	4	4	1

$$\Rightarrow \left(\frac{1}{5}\right) = 1, \quad \underset{\left(\frac{-1}{5}\right)}{\left(\frac{4}{5}\right)\overset{}{\shortparallel}} = 1, \quad \left(\frac{2}{5}\right) = -1, \quad \left(\frac{3}{5}\right) = -1$$

Note: $\left(\frac{4}{5}\right)\cdot\left(\frac{2}{5}\right) = -1 = \left(\frac{8}{5}\right)$, as predicted.

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \forall\, a,b \in (\mathbb{Z}/p\mathbb{Z})^*$

- Want to know: what is $\left(\frac{d}{p}\right)$ for arbitrary $d \in \mathbb{Z}$?

- Start by factoring d into primes: $d = \pm q_1^{e_1} \cdots q_n^{e_n}$

$$\Rightarrow \left(\frac{d}{p}\right) = \left(\frac{\pm 1}{p}\right)\cdot\left(\frac{q_1}{p}\right)^{e_1} \cdots \left(\frac{q_n}{p}\right)^{e_n}$$

- Euler's criterion takes care of the ± 1 case: $\left(\frac{1}{p}\right) = 1$; $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1$ mod 4.

- Notice: we can ignore q_i term if e_i is even.

As is often the case, we treat the case $p=2$ differently from the others.

Prop 26: $\left(\frac{2}{p}\right)=1$ iff $p \equiv 1$ or $-1 \mod 8$.

Book has proof using complicated field theory; we'll do sthg. else.

Recall: since $\left(\frac{2}{p}\right)=\pm 1$, and $1 \not\equiv -1 \mod p$, it's enough to show that $\left(\frac{2}{p}\right) \equiv 1 \mod p$ iff $p \equiv 1$ or $-1 \mod 8$.

Recall: euler's criterion, $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \mod p$.

Let $s = \frac{p-1}{2}$. We'll use our favorite trick: compute $s! \mod p$ in two different ways.

Note: $s+1 = \frac{p+1}{2}$

Start with:

$$\left.\begin{aligned} 1 &= (-1)(-1)^1 \\ 2 &= 2\cdot(-1)^2 \\ 3 &= (-3)\cdot(-1)^3 \\ &\vdots \\ s &= (\pm s)\cdot(-1)^s \end{aligned}\right\}$$

i.e. $n = ((-1)^n \cdot n)\cdot(-1)^n$ for $1 \le n \le s$.

Claim $\prod_{n=1}^{s} (-1)^n n \equiv \prod_{k=1}^{s} 2k$ (here's the hard part!)

$\prod_{n=1}^{s}(-1)^n n = (-1)\cdot 2\cdot(-3)\cdot 4 \cdots (\pm s)$, $\prod_{k=1}^{s} 2k = 2\cdot 4\cdot 6 \cdots \underbrace{2s}_{p-1} = \prod_{\substack{1\le k\le p-1 \\ k \text{ even}}} k$

Break each product into two parts:

$$\prod_{n=1}^{s}(-1)^n n = \boxed{\prod_{\substack{1\le n\le s \\ n \text{ even}}} n} \cdot \prod_{\substack{1\le n\le s \\ n \text{ odd}}} (-n)$$

same!

$$\prod_{\substack{1\le k\le p-1 \\ k \text{ even}}} k = \boxed{\prod_{\substack{1\le k\le s \\ k \text{ even}}} k} \cdot \prod_{\substack{s+1\le k\le p-1 \\ k \text{ even}}} k$$

- Note: if n odd, then $-n \equiv p-n$ and $p-n$ even. If $1 \le n \le s$, then $p-s \le p-n \le p-1$.

- Similarly, if k even and $p-s \le k \le p-1$, then $p-k$ odd, and $1 \le p-k \le s$.

- Also, $k = p-(p-k)$.
- Conclusion: $\forall k \in [p-s, p-1]$, k even, $k = p-n \equiv -n$ for some unique $n \in [1, s]$, n odd.

$$\Rightarrow \prod_{\substack{1 \le n \le s \\ n \text{ odd}}} (-n) \equiv \prod_{\substack{p-s \le k \le p-1 \\ k \text{ even}}} k \quad . \quad \text{Note: } p-s = p - \frac{p-1}{2} = \frac{p+1}{2} = s+1. \quad \blacksquare$$

So: $\displaystyle\prod_{n=1}^{s} (-1)^n n \equiv \prod_{k=1}^{s} 2k = 2^s \prod_{k=1}^{s} k \equiv 2^s s!$

Also: $\displaystyle\prod_{n=1}^{s} (-1)^n = (-1)^{\sum_{n=1}^{s} n} = (-1)^{s\cdot(s+1)/2}$

$$\frac{s\cdot(s+1)}{2} = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8}$$

Upshot: $1 = (-1)(-1)^1$, $2 = 2\cdot(-1)^2$, etc.

$$\Rightarrow \quad s! \equiv \prod (-1)^n n \cdot \prod (-1)^n \equiv 2^s s! \cdot (-1)^{\frac{p^2-1}{8}}$$

$\Rightarrow \quad 1 \equiv 2^s (-1)^{\frac{p^2-1}{8}}$. Since $\left((-1)^{\frac{p^2-1}{8}}\right)^2 = 1$,

$(-1)^{\frac{p^2-1}{8}} \equiv 2^s \equiv \left(\frac{2}{p}\right)$. Check: $\frac{p^2-1}{8}$ even iff $p \equiv 1, 7 \mod 8$ $\blacksquare$

– What about other primes? I.e. $\left(\frac{q}{p}\right)$ for q odd prime?

———————— " ————————

Oh, first an example: 2 is a square mod 7, $(2 \equiv 3^2)$ and mod 17 $(2 \equiv 6^2)$, but not a square mod 5: $\frac{1\ 2\ 3\ 4}{1\ 4\ 4\ 1}$ 11: $\frac{1\ 2\ 3\ 4\ 5}{1\ 4\ 9\ 5\ 3\ 3 \cdots}$

Application: $\mathbb{Z}[\sqrt{2}]/p\mathbb{Z}[\sqrt{2}]$ a field iff $p \equiv 3, 5 \bmod 8$

———————— " ————————

Other primes? We have the following beautiful theorem:

$\boxed{\text{\underline{Thm} (QR) Let } p, q \in \mathbb{N} \text{ be odd primes. Then } \left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}}$

I.e. if $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. If $p \equiv q \equiv 3 \bmod 4$, then $\left(\frac{p}{q}\right) \equiv -\left(\frac{q}{p}\right)$

Applications: is 85 a square mod 101?

Factor 85: $85 = 5 \cdot 17$. Note: 101 is an odd prime!

$$\Rightarrow \left(\frac{85}{101}\right) = \left(\frac{5}{101}\right)\cdot\left(\frac{17}{101}\right) \underset{\substack{\uparrow \\ 101 \equiv 1 \bmod 4}}{=} \left(\frac{101}{5}\right)\cdot\left(\frac{101}{17}\right) = \left(\frac{1}{5}\right)\cdot\left(\frac{16}{17}\right)$$

$$= \left(\frac{1}{5}\right)\cdot\left(\frac{4}{7}\right)^2 = \underline{1}.$$

Yes!

- Is -26 a square mod 67?

Check: 67 is prime, congruent to 3 mod 4.

$$\left(\frac{-26}{67}\right) = \left(\frac{-1}{67}\right)\cdot\left(\frac{2}{67}\right)\cdot\left(\frac{13}{67}\right)$$

$$= \underset{\substack{\uparrow \\ 3 \bmod 4}}{-1} \cdot \underset{\substack{\uparrow \\ 3 \bmod 8}}{-1} \cdot \underset{\substack{\uparrow \\ 13 \equiv 1 \bmod 4.}}{\left(\frac{67}{13}\right)} = \left(\frac{2}{13}\right) = 1$$

Yes!

- ~~Is 37063 a square mod 48611?~~

~~Well... I don't really want to factor 37063...~~ I don't wanna mess w/ Jacobi symbol...

~~Note: if p_1, p_2, q odd primes, can we write $\left(\frac{p_1p_2}{q}\right) = (-1)\left(\frac{q}{p_1p_2}\right)$~~

- $$\left(\frac{55}{179}\right) = \left(\frac{5}{179}\right)\cdot\left(\frac{11}{179}\right) = \left(\frac{179}{5}\right)\cdot(-1)\left(\frac{179}{11}\right) = \left(\frac{4}{5}\right)\cdot(-1)\cdot\left(\frac{3}{11}\right)$$

$$= \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Proof of QR: There are > 200 published proofs!

None are v. easy: it took 3 generations of mathematicians to originally figure out!

- Simplest proof is due to Rousseau, '91
- Ingredients: Chinese Remainder theorem and that multiplication trick.
- Restatement: $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$ where $p^* = \begin{cases} p, & p \equiv 1 \bmod 4 \\ -p, & p \equiv 3 \bmod 4 \end{cases}$.
- Let's talk about cryptography now!

- The goal of (PK) cryptography: to allow two people to exchange confidential info even when adversaries are eavesdropping <u>on every word.</u>
- <u>E.g.</u> sending messages over the internet: it's kind of like sending a post-card. You rely on a bunch of other people to deliver your message and they can all read what you're saying.
- So how do I buy stuff on amazon w/o someone else stealing my CC #?
- The first answer to this question was discovered in the 1970s: Diffie-Helman and RSA.

§ ~~Diffie-Hellman key exchange~~

- ~~The point of DH is to establish a shared secret between the two parties that can be used for later encryption.~~ say later.

§ Old way:

- E.g. one of the simplest/easiest forms of encryption is a Caesar cipher / shift cipher.
- You and your friend start by establishing a secret key, $k \in \mathbb{Z}$. Don't tell anyone else!!
- Encrypt by shifting each letter in the alphabet forward by k. $\left(\frac{A}{D} \middle| \frac{B}{E} \middle| \frac{C}{F} \middle| \frac{D}{G} \middle| \frac{E}{H} \middle| \frac{F}{I} \cdots \; k=3 \right)$
- E.g. Jon Snow wants to send secret messages to Dany Targaryen. They agree, in private, to use Caesar cipher w/ secret key $k=2$.

To encrypt the message "GO NORTH", replace each letter w/ the one that's 2 letters later in the alphabet: $G \mapsto I$, $O \mapsto Q$, $N \mapsto P$ etc.

"GO NORTH" $\longrightarrow$ "IQ PQTVJ"

- D receives the message "IQ PQTVJ"
- To decrypt, she shifts each letter <u>backwards</u> by k

- The downside (well, one of many): they need to agree on the secret key! How can they do this w/ eavesdroppers around?
- Diffie – Hellman to the rescue!

1) Choose a prime # p and a primitive root g. This is broadcast publicly.
2) J chooses a random # $x \in [1, p-1]$ and D chooses a random # $y \in [1, p-1]$. The x and y are secret; they don't tell those to anyone!
3) J computes $X = g^x \bmod p$ and sends it to D. D computes $Y = g^y \bmod p$ and sends it to J.
4) Then J computes $k = Y^x$ — This is their shared secret!

   D computes $k = X^y$. Note: $X^y = (g^x)^y = g^{xy} = (g^y)^x = Y^x$

Concrete example:

Step #	J's private info	Public info	D's private info
1)		"J: Let's do DH. $p=23$, $g=10$" "D: ok"	
2)	$x=4$ $g^x \equiv 10^4 \equiv 18 \mod 23$		$y=17$ $g^y \equiv 10^{17} \equiv 17 \mod 23$
3)		"J: $X=18$" "D: $Y=17$"	
4)	$k = Y^x = 17^4 \equiv 8$		$k = X^y = 18^{17} \equiv 8$

Note: you can use any group for Diffie-Hellman and any element $g \in G$ of large order.

Note: security depends on strangers not being able to find x, y given g, p, X, Y. "Discrete log problem": compute disc. log of X w.r.t. g in $\mathbb{Z}/p\mathbb{Z}$.

The point: computing disc. log takes exponentially longer than computing g^x. (as far as we know!)

Note You don't get to decide what the shared secret, k, is.

Math 4400, 7-19-17

Assumptions for crypto:

- It's feasible to: multiply #s mod n, raise a # to a power mod n, Euclidean algo
- Unfeasible: if $m \in \mathbb{Z}$ product of large primes,
  - factoring m, find $\varphi(m)$ w/o factorizations
  - Given p large and g a primitive root, compute discrete log of $X \in \mathbb{Z}/p\mathbb{Z}$.
- Have a nice way to convert messages to #s (encoding)

Diffie–Hellman: establishing a shared secret.

<u>Example</u>: Alice and Bob want to establish shared secret. (see table p. 94)

They use their shared secret to encrypt later comms.

- <u>Note</u>: no one can predict what the shared secret will be! Don't get to choose.
- <u>Note</u>: In principle, instead of saying "here's p," Alice can say "here's a group G and an element $g \in G$". Just need discrete logs to be hard to compute.

§6.2, RSA

- What about actual encryption?
- Caesar cipher sucks. Also it's symmetric: anyone who can encrypt the message can decrypt.
- Asymmetric encryption: one key for encrypting (public key) and a different one for decrypting (private key)
- Think: a safe w/ a slot. Anyone can drop messages into the slot, but only one person can retrieve them

RSA is an example of this. Here's the algo:

- Setup: Alice wants anyone to be able to send her encrypted messages.
  - Chooses two large prime #s p, q.
    (e.g. $p=43$, $q=71$)
  - computes $m = p \cdot q$, $\varphi(m) = (p-1)(q-1)$
    ($m = 3053$, $\varphi(m) = 2940$)
  - chooses some $e \in (\mathbb{Z}/m\mathbb{Z})^\times$. (eg $e=11$).
    note: $\frac{2940}{3053} = 96\%$ of #s in $[1,m]$ are rel. prime. Randomly pick one, do euclid algo to check coprime.
  - find $d \equiv e^{-1} \mod m$ ($d = 1871$)

- Alice publicly anounces (m, e). This is her public key. $(13053, 11)$

Encryption process

- Bob takes message N, breaks it into pieces w/ fewer digits than m. $x_0, x_1, \dots, x_r$

e.g. $N = 123\,456 \longrightarrow \underbrace{123}_{x_0} \; \underbrace{456}_{x_1}$

- encrypted vers: $X_0 \equiv x_0^e$, $X_1 \equiv x_1^e \mod m$.

$(X_0 = 123^{11} \equiv 7 \mod 3053, \; X_1 \equiv 456^{11} \equiv 2943 \mod m)$

- Bob sends $(X_0, X_1, X_2, \dots, X_r)$

$(7, 2943)$.

Decryption: Alice receives $X_0, X_1, \dots, X_r$

Alice needs to solve

$$x_0^e \equiv X_0 \mod m,$$
$$\vdots$$
$$x_r^e \equiv X_r \mod m.$$

We know how to do this! Just find $d \equiv e^{-1} \mod \varphi(n)$ [Eucld. algo]. Then

find it once and for all.

$x_0 \equiv X_0^d, \dots, x_r \equiv X_r^d$

(note: we don't know $\gcd(X_0, m) = 1$... but CRT says we can do this anyway, since $m = p \cdot q$.)

e.g. $x_0 \equiv X_0^d \equiv 7^{1871} \equiv 123 \mod 3053$

$x_1 \equiv (2943)^{1871} \equiv 456 \mod 3053.$

Private key: (m, d) $[(3053, 1871)]$

- Note: it's important that hackers can't figure out $\varphi(m)$. This is called the "RSA problem"

Digital signatures

- How do you know you're talking to who you think you're talking to?
- RSA / asymmetric crypto helps us know!
- The idea is: if Alice encrypts ~~sthg~~ with her private key, Bob can decrypt w/ public key.

i.e. if Alice sends $y = x^d$ to Bob, Bob can recover x by computing $y^e = x^{de} = x$.

- So if Alice wants to send a message, x, and prove it's from her, she can send $(x, \underbrace{y}_{x^d})$

Receiver checks: is $y^e = x$?

If so, sender has proven they have A's priv. key (priv. key corresp. to e).

- Note: this only works if Bob is certain that e really is Alice's pubkey!

Math 4400 Wednesday, July 26, 2017.

- Recall, RSA: to construct key pair, choose large primes p, q. Set $m = pq$, choose e relprime to $\varphi(m)$. Find $d \equiv e^{-1} \bmod \varphi(m)$.

Pub key: (m, e) Private key: (m, d).

Uses: $(x^e)^d \equiv x \mod m$.

Note: $(x^d)^e \equiv x \mod m$ as well! i.e. can encrypt w/ priv. key! This allows us to use RSA for <u>digital</u> <u>signatures</u>.

- So, if Bob wants to confirm other person is Alice, he can ask her to send her ~~message~~ message M along with the same message encrypted by her private key. (eg. if message $M < m$, she sends $(M, N = M^d)$)

- Bob receives (M, N). Decrypts N using e, compares w/ M. If $M = N^e$, then presumably other person has Alice's private key!

- Note: technically, all it shows is the other person has priv. key corresp. to the public key (m, e).
- How do we know e really is Alice's pub key? (CA, web of trust)

El Gamal (§10.3)

- Idea: Diffie–Hellman to establish shared secret.
- Multiply/divide by secret mod p to encrypt/decrypt.

Eg. Alice wants to receive messages encrypted via El Gamal. She chooses a prime p, and prim root g

Q: next step?

Chooses a random $x \in [2 \to p-2]$ (or $[1, p]$. whatever)

Anounces publicly $p, g, X = g^x$

[Eg: $p = 131$, $g = 2$; $x = 37$, so $X = 2^{37} \equiv 76 \mod 131$]

Bob wants to send a message M to Alice. He chooses random y, sets $Y = g^y$

M: 123456

[Eg $y = 19$, $Y = 2^{19} \equiv 26 \mod 131$]

Then the shared secret is $X^y = 76^{19} \equiv 116 \mod 131$.

To encrypt: break up M into pieces smaller than p.

Eg. $123456 \to 12 \quad 34 \quad 56$ or $123 \quad 4 \quad 56$

$12 \to 12 \cdot k \mod p = 82$ $\qquad 56 \cdot 116 \equiv 77 \mod 131$.

$34 \to 34 \cdot k \mod p = 14$

multiply each piece by k mod p.

Decryption:

So Bob sends to Alice his # Y, along with encrypted message. Eg $Y=26$; 82, 14, 77

Alice uses Y to compute $k = Y^x = 26^{37} \equiv 116 \mod 131$

To decrypt, Alice must solve the equations:

$$x_1 \cdot 116 \equiv 82 \mod 131$$
$$x_2 \cdot 116 \equiv 14 \mod 131$$
$$x_3 \cdot 116 \equiv 77 \mod 131$$

Sol'n: find $116^{-1} \mod 131$. via Euclidean algo.

$116^{-1} = 96$.

$\Longrightarrow \quad x_1 = 82 \cdot 96 \equiv 12 \mod 131$

(etc).

Q: why can't an adversary decrypt? Finding inverses is easy! A: They don't know what to find the inverse of!

Q How do we find these large prime #s?

A Guess! Eg. Say we want to find a prime in the interval $[2^{100}, 2^{101}]$. Then we pick a random # x in this interval.

Q $P(x \text{ is prime}) = ?$

Prime number theorem: let $\pi(n) = \#\text{primes} \le n$.

Thm (PNT) $\pi(n) \sim \frac{n}{\log(n)}$ asymptotically.

ie $\lim_{n\to\infty} \frac{\pi(n)}{n/\log(n)} = 1$ $\log = \log_e$

$\Rightarrow$ # primes in $[2^{100}, 2^{101}]$ is $\pi(2^{101}) - \pi(2^{100})$, which is approx $\frac{2^{101}}{101 \log 2} - \frac{2^{100}}{100 \log 2} \sim \frac{2^{101} - 2^{100}}{100 \log 2}$

$$\sim \frac{2^{100}}{100 \log 2}$$

$\Rightarrow$ probability x is prime $\sim \frac{2^{100}/100\log 2}{2^{100}} = \frac{1}{100 \log 2} = 1.4\%$

$\Rightarrow$ but all the primes are odd! If we choose x odd, our chances are $\frac{2}{100 \log 2} = 2.8\%$

$\Rightarrow$ So, we guess a random odd #, check if it's prime, If not, guess again.

$\Rightarrow$ How many tries will this take? Geometric distrib. On average, $\frac{100 \log 2}{2} = \underline{\underline{35}}$ tries. Only 35!!!

But wait, how do we quickly check if it's prime?

<u>Probabilistic Miller-Rabin test.</u> (§11.1)

Idea: If n prime, then $\forall \underset{\in [1,n-1]}{a}$, $a^{n-1} \equiv 1 \mod n$.

$\Rightarrow$ If $\exists a \in [1, n-1]$ with $a^{n-1} \not\equiv 1 \mod n$, then n isn't prime!

Note: this isn't very good though! $\exists$ Carmichael #s, ie numbers n s.t. $a^{n-1} \equiv 1$ for all a with $\gcd(a,n)=1$

Further, if $n = p \cdot q$ for large p, q, then chances of finding something not rel. prime are slim!

Miller–Rabin criterion: Let n be odd, $n-1 = 2^k q$ (q odd) $k \geq 0$.

Then n is composite if $\exists a \in \mathbb{Z}/n\mathbb{Z}$ s.t.

1) $a^q \not\equiv 1 \mod n$, and
2) $a^{2^i q} \not\equiv -1 \mod n$ for all $i = 0, 1, \ldots, k-1$ (such a is called 'witness')

Pf Prove contrapositive: if n prime, one of these fails. We have $a^{2^i q} = 1$ for some i by FLT. One case or the other fails depending on smallest such i: If it's $i=0$, first fails. if $i > 0$, second fails. ∎

Note: if n composite, 75% of $\mathbb{Z}/n\mathbb{Z}$ is a witness

---

Next time: Chinese Remainder Thm?

Math 4400 7/28/17 Solving polynomials w/ CRT

Q Who can state the CRT?

A If $\gcd(m,n)=1$, then $\forall a \in \mathbb{Z}/m\mathbb{Z}$, $b \in \mathbb{Z}/n\mathbb{Z}$ $\exists!\, x \in \{0,1,2,\dots,mn-1\}$
(or $x \in \mathbb{Z}/mn\mathbb{Z}$)

s.t. $[x]_m = a$, $[x]_n = b$.

i.e. $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\mu} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a bijection.
$[x]_{mn} \longmapsto ([x]_m, [x]_n)$

E.g. $\exists!\, x \in \mathbb{Z}/21\mathbb{Z}$ s.t. $x \equiv 0 \bmod 3$, $x \equiv 4 \bmod 7$.
How do we find it? Well, $x \equiv 4 \bmod 7 \Rightarrow x = 4 + 7k$
for some k. Two options:

1) Write all #s of the form $4+7k \in \{0,1,\dots,20\}$:
$4, 11, 18$
Check to see which one $\equiv 0 \bmod 3$.

2) More systematic: solve $4+7k \equiv 0 \bmod 3$
$\Rightarrow k \equiv -1 \bmod 3$. Choose smallest $k \in \mathbb{N}$, st $k \equiv -1 \bmod 3$
$\Rightarrow k = 2$
$\Rightarrow x = 4 + 7 \cdot 2 = 18$.

Note $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a ring!
$(a,b) + (c,d) \overset{\text{def}}{=} (a+c, b+d)$, $(a,b) \cdot (c,d) \overset{\text{def}}{=} (a \cdot c, b \cdot d)$.

Check @ home: $[x]_{mn} \overset{\mu}{\longmapsto} ([x]_m, [x]_n)$ is a ring homomorph!

Thus, we can rephrase CRT: the map $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\mu} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is an isomorphism of rings!!! (Again, if $\gcd(m,n)=1$)

Thus most questions we ask abt $\mathbb{Z}/mn\mathbb{Z}$ can be answered by working in $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

Eg. Is 2 a square mod 15? If $2 \equiv a^2$ mod 15, then $\mu(2) = \mu(a^2) = \mu(a)^2$ $\mu : \mathbb{Z}/15 \to \mathbb{Z}/3 \times \mathbb{Z}/5$

$\Rightarrow ([2]_3, [2]_5) = ([a]_3^2, [a]_5^2)$

$\Rightarrow 2 \equiv a^2$ mod 3, $2 \equiv a^2$ mod 5.

Not a square! 2 is not a square mod 3.

What abt 6? ~~If $6 \equiv a^2$ mod 15~~ Solve:

$\Rightarrow 6 \equiv a^2$ mod 3, $6 \equiv a^2$ mod 5

$\Rightarrow a \equiv 0$ mod 3 and $a \equiv 1$ or 4 mod 5.

So, yes! In prac, if $x \in \mathbb{Z}/15$ w/ $x \equiv 0$ mod 3, $x \equiv 1$ mod 5

Then $\mu(6) = \mu(x)^2 = \mu(x^2) \Rightarrow 6 = x^2$
μ is injective

"Whatever gets sent to a solution in $\mathbb{Z}/3 \times \mathbb{Z}/5$ is a solution in $\mathbb{Z}/15\mathbb{Z}$"

Here: $x=6$ and $x=9$ work.

$6 \in \mathbb{Z}/15$ is the unique elt $\equiv 0 \bmod 3$ and $1 \bmod 5$

$9 \in \mathbb{Z}/15$ " " " " " " $4 \bmod 5$

$6^2 \equiv 9^2 \equiv 6$ ✓

Also note: $105 = 3 \cdot 5 \cdot 7$

$\Rightarrow \mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/35 \cong \mathbb{Z}/3 \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

If $n = p_1^{e_1} \cdots p_r^{e_r}$, then $\mathbb{Z}/n \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$

Solving polynomial eqns.

Note: if $f(x) \in \mathbb{Z}[X]$, and $a \equiv b \bmod n$, then

$f(a) \equiv f(b) \bmod n$.

E.g. $f(x) = 3x^2+x+1 \Rightarrow 3 \cdot 8^2 + 8 + 1 \equiv 3 \cdot 2^2 + 2 + 1 \bmod 6$

$n=6$

Let $n = n_1 n_2$, n_1 & n_2 rel. prime. $f(x) \in \mathbb{Z}[X]$,

Want to solve: $f(x) \equiv b \bmod n$. $b \equiv b_i \bmod n_i$,

Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ s.t.

$f(a_i) \equiv b_i \bmod n_i \quad (i=1,2)$

CRT: $\exists!\ a \in \mathbb{Z}/n_1n_2\mathbb{Z}$ s.t. $a \equiv a_i \bmod n_i$

Then $f(a) \equiv f(a_i) \bmod n_i$
$\equiv b_i$

$\boxed{\text{Claim } a \text{ is soln to } f(x) \equiv b \bmod n.}$

$\Rightarrow$ So $f(a)$ and $b \in \mathbb{Z}/n\mathbb{Z}$ both $\equiv b_i \bmod n_i$

CRT: $f(a) \equiv b \bmod n$, by uniqueness! ∎

E.g. Solve $x^5 \equiv 9 \mod 21 = 3 \cdot 7$

$\gcd(9, 21) \neq 1$. Oh no!

$\rightsquigarrow$ break it up: work mod 3 and mod 7.

$x_1^5 \equiv 9 \mod 3$, $\quad x_2^5 \equiv 9 \mod 7$.

$\Rightarrow x_1 \equiv 0 \mod 3$. $\quad x_2 \equiv ?$ now $\gcd(9,7)=1$, $\gcd(5, \varphi(7)) = 1$

So: find $5^{-1} \mod 6$: it's 5.

$\Rightarrow x_2 \equiv 2^5 \mod 7 \equiv 4$.

So: sol'n to original eqn, $x^5 \equiv 9 \mod 21$, is whatever's $\equiv 0 \mod 3$ and $\equiv 4 \mod 7$ in $\mathbb{Z}/21\mathbb{Z}$.

$\rightsquigarrow x \equiv 18 \mod 21$.

Doesn't always work, though:

$x^{17} \equiv 15 \mod 175 = 5^2 \cdot 7 \qquad x \equiv ?$

$\rightsquigarrow x_1^{17} \equiv 15 \mod 25$, $\quad x_2^{17} \equiv 15 \mod 7$

$x_1 \equiv ?$ $\quad \rightsquigarrow x_2 \equiv 1$.

Nothing we can do abt $\gcd(15, 25) \neq 1$.

However, if $x_1^{17} \equiv 15 \mod 25$, then $5 \mid 15 - x_1^{17} \Rightarrow 5 \mid x_1^{17}$
$\Rightarrow 5 \mid x_1$
$\Rightarrow x_1^{17} \equiv 0$, so no sol'n!

- However, all is fine and dandy if $n = p_1 \cdots p_r$, $p_i \neq p_j$
- "n is square-free." Not divisible by any square #s.
- Finally: Prop If $n = pq$, $p \neq q$ primes, then Sol'n to $x^k \equiv a \mod n$ is $x \equiv a^u$ where $k \cdot u \equiv 1 \mod \varphi(n)$. [no matter what a is!] [if $\gcd(k, \varphi(n)) = 1$].

Pf if $\gcd(a, n) = 1$, ok. If $a \equiv 0$, ok.

So WLOG $\gcd(a, n) = p$, $q \nmid a$.

$$\Rightarrow \quad x^k \equiv a \Rightarrow x^{k \cdot u} \equiv x^{\ell\varphi(n)+1} \equiv a^u$$

ETP $x^{\ell\varphi(n)+1} \equiv x \quad \forall x \in \mathbb{Z}/n\mathbb{Z}$.

USE CRT: $x_1^k \equiv a \mod p \Rightarrow x_1 \equiv 0$. $\equiv a^u$

$x_2^k \equiv a \mod p$.

$$\Rightarrow x_2^{k \cdot u} \equiv a^u \mod p. \Rightarrow x^{\ell\varphi(n)+1} \equiv a^u$$

Note: $\varphi(p) \mid \varphi(n)$. So $x^{\ell\varphi(n)+1} \equiv \left(x^{\varphi(p)}\right)^{\ell'\varphi(q)} \cdot x \equiv x$

So $x \equiv a^u$ works mod p & mod q

$\Rightarrow$ works mod n.

Math 4400 7/31/17

- Method of descent.

- Q When is a prime # a sum of two squares? (SOTS)

- HW: p a SOTS $\Rightarrow p \equiv 1 \mod 4$

- Thm if $p \equiv 1 \mod 4$, then p is SOTS

- Idea: method of descent!

Given $A^2 + B^2 = Mp$, $M > 1$,
find a, b, m with $a^2 + b^2 = mp$, $1 \leq m < M$.

Repeat this process a finite ($< M$) # of times, and get $\alpha^2 + \beta^2 = p$.

Details

- Key ingredient: (SOTS) $\cdot$ (SOTS) = SOTS
in ptic, $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (bc-ad)^2$

- Also, if $p \equiv 1 \mod 4$, then $\exists A$, $0 \leq A \leq p-1$,
s.t. $A^2 \equiv -1 \mod p \Rightarrow A^2 + 1 = Mp$, some $M \in \mathbb{Z}$.

Note: $M = \dfrac{A^2+1}{p} \leq \dfrac{(p-1)^2+1}{p} = \dfrac{p^2-2p+2}{p} = p - 2 + \frac{2}{p} < p$.

Algorithm

- Start with $A^2+B^2=Mp$, $1<M<p$.

- Choose $u,v \in [-\frac{1}{2}M, \frac{1}{2}M]$ with

  $A \equiv u \mod M$, $B \equiv v \mod M$.

  (Note: can't have $u=0$ and $v=0$)

- **Note:** $u^2+v^2 \equiv A^2+B^2 \equiv 0 \mod M$.

$\Longrightarrow \exists r: \ u^2+v^2 = rM$.

Claim $1 \leq r < M$. (this r will be the new M)

Pf: • for $r<M$, note

$$u^2+v^2 \leq \frac{1}{4}M^2 + \frac{1}{4}M^2 = \frac{M}{2}\cdot M \quad (\text{so } r \leq \tfrac{M}{2})$$

• for $1 \leq r$: enough to show $u^2+v^2 \neq 0$.

If $u^2+v^2=0$, then $u=0$, $v=0$ $\Rightarrow M \mid A, B$.

$\Longrightarrow M^2 \mid A^2+B^2 = Mp \Longrightarrow M \mid p$ $\#$.

but $M<p$. $\square$

- $\Longrightarrow (u^2+v^2)(A^2+B^2) = rpM^2$

  $\| $ formula!

  $(uA+vB)^2+(vA-uB)^2$

- claim: $M \mid uA+vB$ and $M \mid vA-uB$

$\equiv A^2+B^2 \equiv 0 \mod M$ $\qquad\qquad$ $\equiv BA - AB \equiv 0 \mod M$. magic!!!

$$\Longrightarrow \left(\frac{uA+vB}{M}\right)^2 + \left(\frac{vA-uB}{M}\right)^2 = rp.$$

Eg $p = 881$

$387^2 + 1^2 = 170 \cdot 881$

$387 \equiv 47 \mod 170,$
$1 \equiv 1 \mod 170$

$47^2 + 1^2 = 13 \cdot 170$

$\Rightarrow \quad (47^2+1^2)(387^2+1^2) = 13 \cdot 170 \cdot 881$

$\quad \| $

$(47 \cdot 387 + 1)^2 + (387 - 47)^2$

$\quad \|$

$18190^2 + 340^2$

$18190 = 170 \cdot 107, \quad 340 = 170 \cdot 2$

$\Rightarrow \quad 170^2 + 2^2 = 13 \cdot 881$

repeat! get $25^2 + 16^2 = 881$.

Another application: Fermat's Last Theorem

If $n > 2$, then $x^n + y^n = z^n$ has no nontrivial solutions in $\mathbb{Z}$.

To prove the case where $n = 4$, Fermat used the method of descent.

Fermat showed: whenever $X^4+Y^4=Z^4$, $X, Y, Z > 0$,
there exists X_2, Y_2, Z_2 with $0 < Z_2 < Z$
and $X_2^4 + Y_2^4 = Z_2^4$

Thus you get infinitely many sol'ns (X_i, Y_i, Z_i)
with $Z_1 > Z_2 > Z_3 > \dots$ can't be! ...

Idea of proof: X^2, Y^2, Z^2 a pythag triple
$\Rightarrow \exists s,t \in \mathbb{Z}$ with $X^2 = st$, $Y^2 = \frac{s^2-t^2}{2}$, $Z^2 = \frac{s^2+t^2}{2}$

Do some clever computations:

- Show $\exists u, v$: $s+t = 2u^2$, $s-t = 4v^2$
- $\Rightarrow$ $X^2 + 4v^4 = u^4$

$\Rightarrow \exists S, T$ s.t. $X = ST$, $2v^2 = \frac{S^2-T^2}{2}$, $u^2 = \frac{S^2+T^2}{2}$

$S+T = 2x^2$, $S-T = 2y^2$

$\Rightarrow$ (x, y, u) is new sol'n.