

\mathbb{Z} : set of integers

$\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \dots\}$ natural numbers

$\mathbb{N}_0 = \mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, \dots\}$

Fundamental Theorem of Arithmetic

\Rightarrow prime numbers are important

Fermat: $x^n + y^n = z^n$, $n \geq 3$

Twin primes: $(p, p+2)$ when both are primes

Are there infinitely many twin primes? (Open)

Goldbach's Conjecture: even numbers are sum of two primes (Open)

Main goal this week : Solving linear diophantine equations

finding all
integer solutions
 x, y .

a, b, c integer
 $ax + by = c$

- $x + y = 0 \quad \{ (n, -n) : n \in \mathbb{Z} \}$

- $2x - 4y = 0$.

Divide by 2 $\Rightarrow x - 2y = 0 \quad \{ (2n, n) : n \in \mathbb{Z} \}$

- $3x + 5y = 7$ This one is harder

- $4x + 6y = 3$. No solution because 2 divides $4x + 6y$, but not 3.

Definition: a, b are integers. We say " a divides b " or " b is a multiple of a " if $b = k \cdot a$ for an integer k . We write $a | b$ in that case and $a \nmid b$ otherwise

- $a | 0$ • $a | a$ • $a | -a$ • $1 | a$ for every a .

Next, we prove some properties

- $a|b$ and $b|c \Rightarrow a|c$

Proof: $a|b \Rightarrow b = k \cdot a, k \in \mathbb{Z}$

$$b|c \Rightarrow c = \ell \cdot b, \ell \in \mathbb{Z}$$

$$\Rightarrow c = \ell \cdot b = (\ell \cdot k) \cdot a \Rightarrow a|c.$$

- $a|b$ and $c|d \Rightarrow ac|bd$

Exercise.

Disprove $a|b \Leftrightarrow ma|mb$. (m integer)

We need a counter example: $a=2, b=1, m=0$

- $m \neq 0, a|b \Leftrightarrow ma|mb$

(\Rightarrow): If $a|b$, then $b = k \cdot a \Rightarrow mb = k \cdot (ma) \Rightarrow ma|mb$.

(\Leftarrow): If $ma|mb$, then $mb = k \cdot ma \Rightarrow b = k \cdot a \Rightarrow a|b$.

- $x|a$ and $x|b \Rightarrow x|ma + nb$

$x|a \Rightarrow a = k \cdot x \Rightarrow ma + nb = m \cdot kx + n \cdot lx = x(mk + nl)$

$x|b \Rightarrow b = \ell \cdot x \Rightarrow x|ma + nb$

Can generalize: $x|a, x|b, x|c \Rightarrow x|la+mb+nc$
etc.

- $a|b$ and $b|a \Rightarrow a = \pm b$
- $a|b \Rightarrow |a| \leq |b|$ unless $b=0$.

Division Algorithm: $b \neq 0$. There are unique integers k and r such that $a = k \cdot b + r$ and $0 \leq r < |b|$

Proof: Let's just focus on $b > 0$ because $b < 0$ is not very different: $24 = 4 \cdot 5 + 4$ and $24 = (-4) \cdot (-5) + 4$.

Two things to prove: existence, uniqueness

Existence: $S = \text{set of all non-negative integers}$ of the form $a - kb$ ($a, a \pm b, a \pm 2b, a \pm 3b, \dots$)

Obviously $S \neq \emptyset$, so it has a smallest element, say $r_0 = a - k_0 \cdot b$ (well-ordering principle)

$a - (k_0 + 1)b$ is smaller than $r_0 \Rightarrow a - (k_0 + 1)b \notin S$

$\Rightarrow a - (k_0 + 1)b < 0 \Rightarrow a < (k_0 + 1) \cdot b$

$\Rightarrow r_0 = a - k_0 b < b$.

Uniqueness: Say $a = k_0 b + r_0$ and $a = k_1 b + r_1$, with $0 \leq r_0, r_1 < b$.

$$k_0 b + r_0 = k_1 b + r_1 \Rightarrow r_0 - r_1 = k_1 b - k_0 b$$

$$\Rightarrow r_0 - r_1 = (k_1 - k_0) \cdot b \Rightarrow b | r_0 - r_1 \quad -b < r_0 - r_1 < b$$

$$\Rightarrow r_0 - r_1 = 0 \text{ or } |r_0 - r_1| \geq b \text{ (not possible)}$$

$$\Rightarrow r_0 = r_1$$

$$\text{Now } k_0 b + r_0 = k_1 b + r_1 \text{ and } r_0 = r_1$$

$$\Rightarrow k_0 b = k_1 b \Rightarrow k_0 = k_1.$$

We can partition the integers into several classes using Division Algorithms

- $\begin{matrix} 2k \\ \uparrow \\ \text{even} \end{matrix}, \begin{matrix} 2k+1 \\ \uparrow \\ \text{odd} \end{matrix}$
- $3k, 3k+1, 3k+2$

- $4k, 4k+1, 4k+2, 4k+3$

- $2k, 4k+1, 4k+3$

Question: what are the possible remainders when a square n^2 is divided by 8?

$$1^2 \rightarrow 1 \quad 5^2 \rightarrow 1 \quad 9^2 \rightarrow 1$$

$$2^2 \rightarrow 4 \quad 6^2 \rightarrow 4 \quad 10^2 \rightarrow 4$$

$$3^2 \rightarrow 1 \quad 7^2 \rightarrow 1 \quad 11^2 \rightarrow 1$$

$$4^2 \rightarrow 0 \quad 8^2 \rightarrow 0 \quad 12^2 \rightarrow 0$$

... continue

$$\text{Pattern: } (4k)^2 \rightarrow 0$$

$$(4k+1)^2 \rightarrow 1$$

$$(4k+2)^2 \rightarrow 4$$

$$(4k+3)^2 \rightarrow 1$$

$$\underline{\text{Proof: }} (4k)^2 = 16k^2 = (2k^2) \cdot 8 + 0$$

$$(4k+1)^2 = 16k^2 + 8k + 1 = (2k^2 + k) \cdot 8 + 1$$

$$(4k+2)^2 = 16k^2 + 16k + 4 = (2k^2 + 2k) \cdot 8 + 4$$

$$(4k+3)^2 = 16k^2 + 24k + 9 = (2k^2 + 3k + 1) \cdot 8 + 1$$

G.C.D and L.C.M

c is a common divisor of a and b if
 $c|a$ and $c|b$

d is a common multiple of a and b if
 $a|d$ and $b|d$.

We define

- $\gcd(a, b)$ (or simply (a, b)) as the greatest common divisor of a and b (except $a=b=0$)

- $\text{lcm}(a, b)$ (or simply $[a, b]$) as the smallest (positive) common multiple of a and b ($a \neq 0, b \neq 0$)

- $(10, 12) = 2$ and $[10, 12] = 60$
- $(5, 7) = 1$ and $[5, 7] = 35$.

Can generalize to define (a, b, c) , $[a, b, c]$ etc.

Back to the equation $ax + by = c$.

- (a, b) divides both a and b
 $\Rightarrow (a, b)$ divides $ax + by$
No solution unless $(a, b) \mid c$.

What about $c = (a, b)$?

Theorem: There are integers x, y such that

$$ax + by = (a, b)$$

Proof: We'll give an algorithm that finds (a, b) and integers x, y such that $ax + by = (a, b)$ (Euclid's algorithm)

By Division algorithm, we can write

$$\bullet a = k_0 \cdot b + r_0, \quad 0 \leq r_0 < |b| \quad \begin{matrix} \text{Lemma:} \\ (a, b) = (b, r_0) \end{matrix}$$

Then, continue using Division algorithm to find (b, r_0) (will prove later)

$$\begin{aligned} \bullet b &= k_1 \cdot r_0 + r_1, \quad 0 \leq r_1 < r_0 \quad \rightarrow (b, r_0) = (r_0, r_1) \\ \bullet r_0 &= k_2 \cdot r_1 + r_2, \quad 0 \leq r_2 < r_1 < r_0 \quad \rightarrow (r_0, r_1) = (r_1, r_2) \\ &\vdots && 0 \\ \bullet r_{n-2} &= k_n \cdot r_{n-1} + r_n \quad \text{because } r_0, r_1, r_2, \dots \text{ decreasing.} \end{aligned}$$

$$\Rightarrow (a, b) = (b, r_0) = (r_0, r_1) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) \\ = r_{n-1}.$$

Tracing back our steps, we can find x and y such that $ax + by = r_{n-1}$

- Begin with the equation (2^{nd} from last)
 $r_{n-3} = k_{n-1} \cdot r_{n-2} + r_{n-1} \Rightarrow r_{n-1} = r_{n-3} - k_{n-1} \cdot r_{n-2}$
- Replace r_{n-2} on RHS using the equation
 $r_{n-4} = k_{n-2} \cdot r_{n-3} + r_{n-2} \Rightarrow r_{n-2} = r_{n-4} - k_{n-2} \cdot r_{n-3}$

$$\text{Now, } r_{n-1} = r_{n-3} - k_{n-1} \cdot (r_{n-4} - k_{n-2} \cdot r_{n-3})$$

- Replace r_{n-3} similarly ...

:

Moving upward, we eventually get $ax + by = r_{n-1}$.

Lemma: $a = kb + r$, then $(a, b) = (b, r)$

Proof: $c|a$ and $c|b \Rightarrow c|a - kb = r$
 $\Rightarrow c|r$

$d|b$ and $d|r \Rightarrow d|kb + r$
 $\Rightarrow d|a$ and $d|b$

Same common divisors mean same gcd.

Example: $a = 600$ and $b = 136$

$$600 = 4 \cdot 136 + 56$$

$$136 = 2 \cdot 56 + 24 \Rightarrow (600, 136) = 8$$

$$56 = 2 \cdot 24 + 8$$

$$24 = 3 \cdot 8 + 0$$

$$8 = 56 - 2 \cdot 24 = 56 - 2 \cdot (136 - 2 \cdot 56)$$

$$= 5 \cdot 56 - 2 \cdot 136$$

$$= 5 \cdot (600 - 4 \cdot 136) - 2 \cdot 136$$

$$= 5 \cdot 600 - 22 \cdot 136.$$

Corollary: $ax + by = c$ has solution if and only if $(a, b) | c$.

$$ax + by = (a, b) \Rightarrow a \cdot kx + b \cdot ky = k \cdot (a, b)$$

An alternative definition for gcd: (a, b) is the smallest positive integer that can be written $ax + by$.

(Very useful to prove some properties)

- a, b not all zero.

$$a = 24 \quad b = 30$$

$$(a, b) = 6$$

$$c|a \text{ and } c|b \Leftrightarrow c|(a, b)$$

common divisors
 $\pm 1, \pm 2, \pm 3, \pm 6$

Common divisors are divisors of greatest common divisor

Proof: (\Leftarrow): obvious.

$$c|(a, b) | a \text{ and } c|(a, b) | b$$

$$(\Rightarrow): c|a \text{ and } c|b \Rightarrow c|ax + by$$

||
 (a, b)

- a, b not both zero

$$(a, b, c) = ((a, b), c)$$

$$\underbrace{x|a, x|b, x|c}_{\sim} \Rightarrow x|(a, b) \text{ and } x|c$$

$$y|(a, b) \text{ and } y|c \Rightarrow \underbrace{y|a \text{ and } y|b}_{\sim}, y|c$$

Same common divisors, same gcd.

- $m > 0$
- $(ma, mb) = m \cdot (a, b)$

$$(ma, mb) = \text{smallest pos. int. } ma + mb y$$

$$= \text{smallest pos. int. } m(ax + by)$$

= m · smallest pos. int. $ax + by$

= m · (a, b)

- $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1$
- $(a, b) = c \Rightarrow a = c \cdot a_1 \text{ and } b = c \cdot b_1$
such that $(a_1, b_1) = 1$.

Definition: We say a and b are relatively prime (or coprime) if $(a, b) = 1$.

- a, b coprime and $a \mid bc \Rightarrow a \mid c$.

$$\begin{aligned} a, b \text{ coprime} &\Rightarrow ax + by = 1 \text{ for some } x \text{ and } y. \\ &\Rightarrow acx + bcy = c \end{aligned}$$

$$a \mid acx \text{ and } a \mid bcy \mid acx + bcy \Rightarrow a \mid c.$$

Can generalize: $a \mid bc \Rightarrow a \mid (a, b) \cdot (a, c)$
(Proof is left as an exercise)

- $(a, b) = 1 \Rightarrow [a, b] = |ab| \quad (a, b \neq 0)$

Let c be a common multiple of a and b ,
i.e. $a \mid c$ and $b \mid c$.

$$\begin{aligned} b \mid c &\Rightarrow c = k \cdot b \text{ and we have } a \mid k \cdot b \Rightarrow a \mid k \\ &\Rightarrow k = \ell \cdot a \Rightarrow c = \ell \cdot ab \\ &\Rightarrow \text{A common multiple } c \text{ is at least } |ab| \end{aligned}$$

Also, clearly $|ab|$ is a common multiple of a and $b \Rightarrow [a, b] = |ab|$.

- $[a, b] = \frac{ab}{(a, b)}$

Let $(a, b) = c \Rightarrow a = c \cdot a_1$, and $b = c \cdot b_1$, such that $(a_1, b_1) = 1$

$$[a, b] = [c \cdot a_1, c \cdot b_1] = c \cdot [a_1, b_1] = ca_1b_1 = \frac{ab}{(a, b)}.$$

Exercise

Back to the equation $ax + by = c$ one last time.

Suppose $c = k \cdot (a, b)$, otherwise no solution.

We know how to find one solution:

- Euclid's algorithm finds x and y such that $ax + by = (a, b)$
- Then $a \cdot (kx) + b \cdot (ky) = k \cdot (a, b)$

Now using one solution, say (x_0, y_0) , we should find all solutions:

$$ax + by = c \iff ax + by = ax_0 + by_0$$

$$\iff a \cdot (x - x_0) = b \cdot (y_0 - y)$$

$$\Leftrightarrow \frac{a}{(a,b)} \cdot (x - x_0) = \frac{b}{(a,b)} \cdot (y_0 - y)$$

$$\frac{b}{(a,b)} \mid \frac{a}{(a,b)} \cdot (x - x_0) \quad \text{and} \quad \left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1$$

$$\Rightarrow \frac{b}{(a,b)} \mid x - x_0 \Rightarrow x - x_0 = m \cdot \frac{b}{(a,b)}$$

$$\Rightarrow y_0 - y = m \cdot \frac{a}{(a,b)}$$

$$\Rightarrow x = x_0 + m \cdot \frac{b}{(a,b)}, \quad y = y_0 - m \cdot \frac{a}{(a,b)}, \quad m \in \mathbb{Z}.$$

are all of the solutions.

Example: Find all integers (x, y) such that

$$\text{a) } 66x + 121y = 100 \quad \text{b) } 14x + 8y = 6$$

a) No solution because $(66, 121) = 11 \nmid 100$.

$$\begin{aligned} \text{b) } 14 &= 1 \cdot 8 + 6 & (14, 8) &= 2 \quad \text{and} \\ 8 &= 1 \cdot 6 + 2 & \Rightarrow & 2 = 8 - 1 \cdot 6 \\ 6 &= 3 \cdot 2 + 0 & & = 8 - (14 - 1 \cdot 8) \\ & & & = 2 \cdot 8 - 14 \end{aligned}$$

$\Rightarrow 6 = 6 \cdot 8 - 3 \cdot 14 \Rightarrow (x_0, y_0) = (-3, 6)$ is solution

All solutions: $x = -3 + m \cdot \frac{8}{(14, 8)} = 4m - 3$

$$y = 6 - m \cdot \frac{14}{(14, 8)} = -7m + 6$$

$\left\{ (4m-3, -7m+6) : m \in \mathbb{Z} \right\}$: set of solutions

$p \geq 2$ is called prime if 1 and p are its only positive divisors.

$n \geq 2$ is called composite if it is not prime.

- n is composite \Rightarrow it has a divisor $a | n$ such that $1 < a < n$
 $\Rightarrow n = a \cdot b$ with $1 < a, b < n$.

- p prime, n integer. What are the possible values of (n, p) ?

Since $(n, p) | p \Rightarrow (n, p) = 1$ or p

- $(n, p) = 1 \Rightarrow n$ and p are coprime, and $p \nmid n$.
- $(n, p) = p \Rightarrow p | n$.

- $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ (or both)

$$p \mid ab \Rightarrow p \mid (a, p) \cdot (b, p)$$

		\rightarrow	not possible
	p	\rightarrow	$p \mid b$
p		\rightarrow	$p \mid a$
p	p	\rightarrow	both

Can generalize: $p \mid a_1 a_2 \dots a_k \Rightarrow p \mid a_1$ or $p \mid a_2$ or... $p \mid a_k$.
 (Proof is exercise. Hint: induction on k).

A special case: $p \mid a^k \Rightarrow p \mid a$

Fundamental Theorem of Arithmetic: Every $n \geq 2$ has a prime factorisation $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ where p_i are distinct primes and α_i are positive integers. This factorisation is unique up to re-ordering.

e.g. $2^2 \cdot 3^5 \cdot 7^2$ same as $3^5 \cdot 7^2 \cdot 2^2$.

Proof: we prove "existence" first, by strong induction on n .

Base case: $n = 2 \rightarrow n = 2^1$ ✓

Assume $2, 3, \dots, k$ all have prime factorisations.

- Case I: $k+1$ is prime, then $(k+1)^1$ is a prime factorisation

- Case II : $k+1$ is composite , then $k+1 = ab$
such that $2 \leq a, b \leq k$. By assumption a and b
have prime factorisations . Combining them, we get
a prime factorisation of $k+1$

$$(2^2 \cdot 3^1 \cdot 7^1) \cdot (3^2 \cdot 5^3)$$

$$2^2 \cdot 3^3 \cdot 5^3 \cdot 7^1$$

Next, we show the uniqueness. Suppose not unique
for some integers and n be the smallest
of such integers.

Write $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} = n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_\ell^{\beta_\ell}$.

$$p_1 \mid LHS \Rightarrow p_1 \mid RHS \Rightarrow p_1 \mid q_i \text{ for some } i$$

$$\Rightarrow p_1 = q_i \text{ for some } i$$

Cancelling out p_1 from both sides , we have
two factorisations for $\frac{n}{p_1}$, contradiction

because n was the smallest such integer.

$$175 = 5^2 \cdot 7^1, 196 = 2^2 \cdot 7^2, 1001 = 7^1 \cdot 11^1 \cdot 13^1$$

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{and} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}$$

(They don't have to have same prime factors, but we can write p^0 if p is missing in one of them.)

$$\text{e.g. } 196 = 2^2 \cdot 7^2 \cdot 11^0 \cdot 13^0, \quad 1001 = 2^0 \cdot 7^1 \cdot 11^1 \cdot 13^1.$$

- $ab = p_1^{\alpha_1 + \beta_1} \cdot p_2^{\alpha_2 + \beta_2} \cdots p_k^{\alpha_k + \beta_k}$
- $\frac{a}{b} = p_1^{\alpha_1 - \beta_1} \cdot p_2^{\alpha_2 - \beta_2} \cdots p_k^{\alpha_k - \beta_k}$
- $a^m = p_1^{m\alpha_1} \cdot p_2^{m\alpha_2} \cdots p_k^{m\alpha_k}$

Questions: 1. When does a divide b ?

Answer: $\alpha_1 \leq \beta_1, \alpha_2 \leq \beta_2, \dots, \alpha_k \leq \beta_k$

2. What is $\gcd(a, b)$? What is $\text{lcm}[a, b]$?

Answer: $(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \cdots \cdot p_k^{\min(\alpha_k, \beta_k)}$

$[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot \cdots \cdot p_k^{\max(\alpha_k, \beta_k)}$

Can generalize to $(a, b, c), [a, b, c]$, etc.

We now have easier proofs for some properties we proved earlier:

$$\bullet (a, b) \cdot [a, b] = ab$$

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$$

$$\bullet (a, b, c) = ((a, b), c)$$

$$\min(\alpha, \beta, \theta) = \min(\min(\alpha, \beta), \theta).$$

In-person office hours:

- Wednesday 4-5 at 215 Huron 10th floor lounge or HU 1009
 - or by appointment
-

- $\sqrt{2}$ is not a rational number

Assume $\sqrt{2}$ is rational. $\Rightarrow \sqrt{2} = \frac{a}{b}$ for some positive integers a, b .

$$\sqrt{2} = \frac{a}{b} \Rightarrow b\sqrt{2} = a \Rightarrow 2b^2 = a^2.$$

Say a and b have prime factorizations
 $a = 2^x \cdot \dots$ and $b = 2^y \cdot \dots$

$$\Rightarrow 2b^2 = 2^{2y+1} \cdot \dots \text{ and } a^2 = 2^{2x} \cdot \dots$$

$$\Rightarrow 2y+1 = 2x, \text{ contradiction.}$$

Notation: We write $p^e \parallel a$ if $p^e \mid a$ but
 $p^{e+1} \nmid a$
fully divides

(p^e is the highest power of p contained in a)

$$\bullet p^\alpha \parallel a \text{ and } p^\beta \parallel b \Rightarrow p^{\alpha+\beta} \parallel ab, p^{\alpha-\beta} \parallel \frac{a}{b}.$$

Exercise: If $p^\alpha \parallel a$ and $p^\beta \parallel b$ and $\alpha < \beta$, then $p^\alpha \parallel a+b$. (If $\beta < \alpha$, then $p^\beta \parallel a+b$. If $\alpha = \beta$, $p^\alpha \mid a+b$ but not necessarily $p^\alpha \parallel a+b$).

4.9

Questions: Suppose $(a, b) = 1$ and ab is a square. What can we say further about a and b ?

$(a, b) = 1 \Rightarrow$ They have different prime factors.

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{and} \quad b = p_{k+1}^{\alpha_{k+1}} \cdots p_{k+l}^{\alpha_{k+l}}$$

$$\Rightarrow ab = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_{k+l}^{\alpha_{k+l}} \text{ is a square}$$

$\Rightarrow \alpha_1, \alpha_2, \dots, \alpha_{k+l}$ are all even.

$\alpha_1, \alpha_2, \dots, \alpha_k$ even $\Rightarrow a$ is a square

$\alpha_{k+1}, \dots, \alpha_{k+l}$ even $\Rightarrow b$ is a square

Can generalize: If a_1, a_2, \dots, a_k are mutually coprime and $a_1 a_2 \cdots a_k$ is an m^{th} power of an integer, then so are all of a_1, a_2, \dots, a_k .

Exercise: $n(n+1)$ is never a square, $n \geq 1$.

Theorem: There are infinitely many primes.

Proof: Suppose not and say p_1, p_2, \dots, p_n are all the primes. Consider $m = p_1 p_2 \dots p_n + 1$.

• m cannot be a prime. Because m is larger than all of the "finitely many" primes

$p_1, p_2, \dots, p_n \Rightarrow m$ composite *This part was unnecessary*

$\Rightarrow m$ has a prime divisor, say $p_i \mid m$

• $p_i \mid m$ and $p_i \mid p_1 p_2 \dots p_n \Rightarrow p_i \mid m - p_1 p_2 \dots p_n$

$\Rightarrow p_i \mid 1$, contradiction.

Integers have one the forms : $4k, 4k+1, 4k+2, 4k+3$

Are there infinitely many primes for each form?

• $4k$: no because there is no prime divisible by 4.

• $4k+2$: no because there is no prime divisible by 2, except $p=2$.

Dirichlet's Theorem: There are infinitely many primes of the form $ak+b$ if and only if $(a, b) = 1$.

We can give a proof for $4k+3$, but a general proof is beyond our level.

Lemma: We cannot have the form $4k+3$ by multiplying $4k, 4k+1, 4k+2$.

$$4k \cdot 4\ell = 4m \quad (4k+1) \cdot (4\ell+1) = 4m+1$$

$$4k \cdot (4\ell+1) = 4m \quad (4k+1) \cdot (4\ell+2) = 4m+2$$

$$4k \cdot (4\ell+2) = 4m \quad (4k+2) \cdot (4\ell+2) = 4m.$$

Infinitely many primes $4k+3$:

Proof: Suppose $3 = p_1, 7 = p_2, p_3, \dots, p_n$ are all the primes of the form $4k+3$.

$$m = 4(p_1 p_2 \dots p_n - 1).$$

- m is of the form $4k+3$

$$m = 4(p_1 p_2 \dots p_n - 1) + 3$$

- m has a prime divisor of the form $4k+3$, by the lemma.

- Say $p_i | m$.

$$p_i | 4(p_1 p_2 \dots p_n - 1) \Rightarrow p_i | 1, \text{ contradiction.}$$

- Pay attention to the differences between

the two proofs.

- Why the same argument doesn't work for $4k+1$?

Clarification / Correction: In the previous lecture, we said

$$p^{\alpha} \parallel a, p^{\beta} \parallel b \Rightarrow p^{\alpha-\beta} \parallel \frac{a}{b}.$$

This is true for every a and b , but you may want to have $p^e \parallel a$ as well because we didn't precisely define what does $p^e \parallel x$ mean for a rational number x .

For example, $5^2 \parallel \frac{75}{7}$ while $5^{-3} \parallel \frac{3}{125}$. Try figuring out the definition for the general case.

How can we check if a given integer n is prime?

• We can check the divisibility by $2, 3, 4, \dots, n-1$. If n is not divisible by any of them, then it is a prime. We can actually do better.

Lemma: If n is composite, then it must have a prime divisor $p \leq \sqrt{n}$.

Proof: n composite $\Rightarrow n = ab$ for some $1 < a, b < n$. We have $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ because otherwise $a > \sqrt{n}$, $b > \sqrt{n} \Rightarrow ab > \sqrt{n} \cdot \sqrt{n} = n$.

Say $a \leq \sqrt{n}$ and p be a prime divisor of a , then $p \leq a \leq \sqrt{n}$ and $p \mid a$ and $a \mid n \Rightarrow p \mid n$.

Thus, we only need to check the divisibility by primes $p \leq \sqrt{n}$.

e.g. 101 prime because it is not divisible by 2, 3, 5, 7.

Sieve of Eratosthenes : Find all primes less than or equal to 50. ($\sqrt{50} < 8$)

2	3	4	5	6	7	8	9	10	2
11	12	13	14	15	16	17	18	19	3
21	22	23	24	25	26	27	28	29	5
31	32	33	34	35	36	37	38	39	7
41	42	43	44	45	46	47	48	49	0

How can we check the divisibility by 2, 3, 4, 5, 8, 9?

Let $n = \overline{a_k a_{k-1} \dots a_0}$ (decimal representation)

$$\Rightarrow n = a_0 + 10a_1 + 10^2 \cdot a_2 + 10^3 \cdot a_3 + \dots + 10^K \cdot a_K. \left(\begin{array}{l} \text{base 10} \\ \text{expansion} \end{array} \right)$$

- Divisibility by 2: $n = a_0 + \underbrace{(10a_1 + 10^2a_2 + \dots + 10^K a_K)}_{\text{already divisible by 2}}$

$$so, 2|n \Leftrightarrow 2|a_0.$$

- Divisibility by 4: $n = a_0 + 10a_1 + (10^2a_2 + 10^3a_3 + \dots + 10^k a_k)$

$$\text{So, } 4|n \Leftrightarrow 4 \mid \underbrace{a_0 + 10a_1}_{\frac{1}{11}} \overline{a_1 a_0}$$

can generalize to divisibility
by 2^m

- Divisibility by 3:

$$n = a_0 + a_1 + a_2 + \dots + a_k + (\underbrace{9a_1 + 99a_2 + 999a_3 + \dots + (10^k - 1)a_k}_{\text{already divisible by 3}})$$

$$\text{So, } 3|n \Leftrightarrow 3|a_0 + a_1 + \dots + a_k.$$

- Divisibility by 11:

- observe that $10+1, 10^2-1, 10^3+1, 10^4-1, 10^5+1$
are divisible by 11.

$$n = a_0 - a_1 + a_2 - \dots + (-1)^k a_k + (\underbrace{(10^1+1)a_1 + (10^2-1)a_2 + \dots + (10^k-(-1))^k a_k}_{\text{divisible by 11}})$$

$$\text{So, } 11|n \Leftrightarrow 11|a_0 - a_1 + a_2 - \dots + (-1)^k a_k.$$

Next, we'll consider the primes of the form $2^m \pm 1$, but first recall:

- $x^a - 1 = (x-1) \cdot (x^{a-1} + x^{a-2} + x^{a-3} + \dots + x^1 + 1)$
- $x^{2a+1} + 1 = (x+1) \cdot (x^{2a} - x^{2a-1} + x^{2a-2} - \dots - x^1 + 1).$

$$x^3 - 1 = (x-1)(x^2 + x + 1) \quad x^3 + 1 = (x+1)(x^2 - x + 1).$$

Question: Suppose $2^m \pm 1$. What can we say about m ?

- m cannot be odd, because otherwise $2^m \pm 1 = (2+1)(\dots)$ cannot be prime.
- m is not divisible by any odd number, except 1.

If $m = \underbrace{(2a+1)}_{\text{odd divisor}} \cdot k$, then

$$2^m \pm 1 = (2^k)^{2a+1} \pm 1 = (2^k \pm 1)(\dots)$$

$\Rightarrow 2^k \pm 1$ divides $2^m \pm 1$.

For $2^m \pm 1$ to be prime, $2^k \pm 1 = 2^m \pm 1$
 $\Rightarrow k=m \Rightarrow (2a+1)=1$.

- no odd number > 1 divides $m \Rightarrow m = 2^n$ for some n .

Recall:

- $x^a - 1 = (x-1) \cdot (x^{a-1} + x^{a-2} + x^{a-3} + \dots + x^1 + 1)$
- $x^{2a+1} + 1 = (x+1) \cdot (x^{2a} - x^{2a-1} + x^{2a-2} - \dots - x^1 + 1)$.

We proved that if $2^m + 1$ is prime, then $m = 2^n$ for some n .

Suppose $2^m - 1$ is prime. What can we say about m ?

- m must be a prime, otherwise $m = ab$ with $1 < a, b < m$ and $2^m - 1 = (2^b)^a - 1$ is divisible by $2^b - 1$, cannot be prime ($1 < 2^b - 1 < 2^m - 1$)

$F_n = 2^{2^n} + 1$ are called Fermat numbers

$M_p = 2^p - 1$ (p : prime) are called Mersenne numbers.

A proof of infinitude of primes using Fermat numbers:

Lemma: If a_1, a_2, a_3, \dots is a sequence of integers bigger than 1 such that $(a_i, a_j) = 1$ for every $i \neq j$, then there are infinitely many primes dividing the terms of this sequence

Proof: Each term has different prime divisors.
 Infinitely many terms \Rightarrow Infinitely many prime divisors.

Lemma: $(F_i, F_j) = 1$ for all $i \neq j$.

Proof: Without loss of generality (WLOG) suppose $j > i$ and write $j = i + k$.

$$F_i = 2^{2^i} + 1 \mid 2^{2^{i+1}} - 1 \mid 2^{2^{i+k}} - 1 = F_j - 2$$

$$x = 2^{2^i} \quad x + 1 \mid x^2 - 1 \mid (x^2)^{2^{k-1}} - 1$$

$$\Rightarrow F_i \mid F_j - 2, \text{ i.e. } F_j - 2 = m \cdot F_i.$$

$$(F_i, F_j) = (F_i, F_j - m \cdot F_i) = (F_i, 2) = 1.$$



F_i is odd

This proves that n^{th} smallest prime p_n satisfies $p_n \leq 2^{2^{n-1}} + 1$. ($p_1 = 2, p_2 = 3, p_3 = 5, \dots$).

Modular Arithmetic

Recall that we can partition integers according to their remainders when divided by 4.

$$[0]_4 = \{ \dots, -8, 0, 4, 8, \dots \} \quad 4k$$

$$[1]_4 = \{ \dots, -7, -3, 1, 5, \dots \} \quad 4k+1$$

$$[2]_4 = \{ \dots, -6, -2, 2, 6, \dots \} \quad 4k+2$$

$$[3]_4 = \{ \dots, -5, -1, 3, 7, \dots \} \quad 4k+3$$

- The sum of an element of $[1]_4$ with an element of $[2]_4$ is always in $[3]_4$.
- The product of an element of $[3]_4$ with an element of $[2]_4$ is always in $[2]_4$.

Never depends on the element, the sets determine everything. That means we can do arithmetic with the sets: $[1]_4 + [2]_4 = [3]_4$ or $[2]_4 \cdot [3]_4 = [2]_4$.

There is an easy way to express the rules of summation and multiplication if we also allow using $[-8]_4$, $[12]_4$ etc. for $[0]_4$; $[7]_4$, $[11]_4$ etc for $[3]_4$ (different names for the same set)

$$\text{Now, } [a]_4 + [b]_4 = [a+b]_4$$

$$[a]_4 \cdot [b]_4 = [ab]_4.$$

Question: When $[a]_4$ and $[b]_4$ are the same set?

Answer: When they have same remainder after division by 4.

$a = 4k+r$ and $b = 4l+r \Rightarrow a-b = 4(k-l)$ is divisible by 4.

Alternative Answer: When $4 \mid a-b$.

When $[a]_4 = [b]_4$ we say a is congruent to b modulo 4 and we write $a \equiv b \pmod{4}$.

The general case : mod n $n \in \mathbb{N}$

- Integers are partitioned into n sets (congruence classes)

$\mathbb{Z}_n = \{ [0]_n, [1]_n, [2]_n, \dots, [n-1]_n \}$ and we can do basic arithmetic with the elements of \mathbb{Z}_n .

- $[a]_n = [b]_n \Leftrightarrow n | a - b$ (same remainder) and we'll say a is congruent to b modulo n and write $a \equiv b \pmod{n}$ in that case

- $[a]_n + [b]_n = [a+b]_n$; $[a]_n \cdot [b]_n = [ab]_n$.
Are these well-defined operations? We should prove

$$1. [a]_n = [c]_n \text{ and } [b]_n = [d]_n \Rightarrow [a+b]_n = [c+d]_n$$

$$2. [a]_n = [c]_n \text{ and } [b]_n = [d]_n \Rightarrow [ab]_n = [cd]_n.$$

Proof: $[a]_n = [c]_n \Rightarrow n | c-a$

$$[b]_n = [d]_n \Rightarrow n | d-b$$

$$1. n | c-a \text{ and } n | d-b \Rightarrow n | c-a+d-b \\ \Rightarrow n | (c+d)-(a+b) \Rightarrow [a+b]_n = [c+d]_n.$$

$$2. n|c-a \Rightarrow c-a = n \cdot k \Rightarrow c = n \cdot k + a$$

$$n|d-b \Rightarrow d-b = n \cdot \ell \Rightarrow d = n \cdot \ell + b$$

$$cd = (nk+a) \cdot (n\ell+b) = n^2k\ell + nk\ell b + nk a + ab$$

$$\Rightarrow cd - ab = n^2k\ell + nk\ell b + nk a = n \cdot (nk\ell + kb + la)$$

is divisible by n

$$\Rightarrow [cd]_n = [ab]_n$$

To summarize some important points.

Theorem: If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then

- $a+b \equiv c+d \pmod{n}$
- $ab \equiv cd \pmod{n} \quad (k \in \mathbb{N})$
- $a^2 \equiv c^2 \pmod{n}, a^3 \equiv c^3 \pmod{n}, \dots, a^k \equiv c^k \pmod{n}$

Also, we have

- $x \equiv x \pmod{n}$
- $x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$
- $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$

Remark: $a \equiv 0 \pmod{n}$ means a is divisible by n .

Why is modular arithmetic a useful tool?

Question: What is the remainder of $113 \cdot 114$ after dividing by 120?

Answer: $113 \equiv -7 \pmod{120}$ and $114 \equiv -6 \pmod{120}$

$$\Rightarrow 113 \cdot 114 \equiv (-7) \cdot (-6) \equiv \boxed{42} \pmod{120}$$

Question: What is the remainder of 5^{16} after dividing by 17?

Answer: $5^2 \equiv 25 \equiv 8 \pmod{17}$

$$5^4 \equiv (5^2)^2 \equiv 8^2 \equiv 64 \equiv -4 \pmod{17}$$

$$5^8 \equiv (5^4)^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$$

$$5^{16} \equiv (5^8)^2 \equiv (-1)^2 \equiv \boxed{1} \pmod{17}$$

Question: Prove that n^3 is of the form $7k$ or $7k+1$ or $7k+6$.

Solution: $0^3 \equiv 0 \pmod{7}$, $1^3 \equiv 1 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$

$$3^3 \equiv 27 \equiv 6 \pmod{7}, 4^3 \equiv (-3)^3 \equiv -3^3 \equiv -6 \equiv 1 \pmod{7}$$

$$5^3 \equiv -2^3 \equiv 6 \pmod{7}, 6^3 \equiv -1^3 \equiv 6 \pmod{7}$$

$n^3 \equiv 0^3, 1^3, 2^3, 3^3, 4^3, 5^3$ or $6^3 \pmod{7}$ and we are done.

Exercise: $n \in \mathbb{Z}$. Prove that $n \cdot (n+1) \cdot (n+2)$ is divisible by 6.

If $a \equiv b \pmod{n}$, then

- $3a \equiv 3b \pmod{n}$
- $2a^2 \equiv 2b^2 \pmod{n}$
- $a^3 \equiv b^3 \pmod{n}$

$$\Rightarrow a^3 + 2a^2 + 3a + 5 \equiv b^3 + 2b^2 + 3b + 5 \pmod{n}$$

More generally,

Theorem: Let $p(x)$ be a polynomial with integer coefficients, then
 $a \equiv b \pmod{n} \Rightarrow p(a) \equiv p(b) \pmod{n}$
(Lemma 3.5 of the textbook)

Recall: In the previous lecture, we've seen for a polynomial $p(x)$ with integer coefficients that

$$a \equiv b \pmod{m} \Rightarrow p(a) \equiv p(b) \pmod{m}$$

For example, let $p(x) = x^3 + 2x^2 + 3x + 5$. Then, we have $p(1) = 11$, $p(4) = 113$, and $11 \equiv 113 \pmod{3}$.

This is actually a very useful tool to prove that some equations have no solution in the integers.

Example: $x^3 - x + 1 = 42$ has no integer solution.

$$p(0) \equiv 1 \pmod{3}, \quad p(1) \equiv 1 \pmod{3}, \quad p(2) \equiv 7 \equiv 1 \pmod{3}$$

$$x \equiv 0, 1, \text{ or } 2 \pmod{3} \Rightarrow p(x) \equiv p(0), p(1), \text{ or } p(2) \pmod{3}$$

$$\Rightarrow p(x) \equiv 1 \pmod{3}, \text{ but } 42 \not\equiv 1 \pmod{3}.$$

An interesting problem: Is there a polynomial $p(x)$ with integer coefficients such that $p(n)$ is prime for every $n \in \mathbb{Z}$, except the constant polynomial?

The answer is no, see Theorem 3.6 for that.

Now, some properties of the congruences

- Suppose $d \geq 1$ and $d|m$, then

$$a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{d}$$

$$a \equiv b \pmod{m} \Rightarrow m|a-b \Rightarrow d|a-b \Rightarrow a \equiv b \pmod{d}.$$

e.g. $3 \equiv 19 \pmod{8} \Rightarrow 3 \equiv 19 \pmod{2}$

- Suppose $c > 0$, then

$$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{mc}$$

$$a \equiv b \pmod{m} \Rightarrow m|a-b \Rightarrow a-b = m \cdot k$$

$$\Rightarrow ac - bc = c \cdot (a-b) = (mc) \cdot k$$

$$\Rightarrow mc | ac - bc \Rightarrow ac \equiv bc \pmod{mc}.$$

The next property is similar to

$$m|ab \Rightarrow m|(m,a) \cdot b .$$

- $ax \equiv ay \pmod{m} \Rightarrow x \equiv y \left(\pmod{\frac{m}{(m,a)}} \right)$

$$ax \equiv ay \pmod{m} \Rightarrow m|ax - ay \Rightarrow m|a \cdot (x-y)$$

$$\Rightarrow m|(m,a) \cdot (x-y) \Rightarrow (m,a) \cdot (x-y) = m \cdot k$$

$$\Rightarrow x-y = \frac{m}{(m,a)} \cdot k \Rightarrow x \equiv y \left(\pmod{\frac{m}{(m,a)}} \right) .$$

Special case: $(m, a) = 1$, we say $x \equiv y \pmod{m}$

This property is useful solving linear congruences:

$$ax \equiv b \pmod{m}$$

find
/ | /
given

Example: which integers x satisfy $15x \equiv 30 \pmod{40}$?

$$15 \cdot x \equiv 15 \cdot 2 \pmod{40} \quad \text{and} \quad \frac{40}{(40, 15)} = 8$$

$$\Rightarrow x \equiv 2 \pmod{8}.$$

$$\text{Check: } x \equiv 2 \pmod{8} \Rightarrow x = 8k + 2$$

$$15x = 15(8k + 2) = 120k + 30 \equiv 30 \pmod{40}.$$

We'll solve $ax \equiv b \pmod{m}$ in general case (similar to linear diophantine equations).

$$ax \equiv b \pmod{m} \text{ means } m \mid ax - b, \text{ i.e. } ax - b = m \cdot k, \quad k \in \mathbb{Z}$$

$$\text{Rewrite it as } ax - m \cdot k = b.$$

- No solution unless $(a, m) \mid b$.
- When $(a, m) \mid b$: There is a solution, say (x_0, k_0) . Then the all solutions will have

$$x = x_0 - t \cdot \frac{m}{(a, m)} \quad \text{with} \quad t \in \mathbb{Z}.$$

$$\text{Set of all solutions} = \left\{ x \in \mathbb{Z} : x = x_0 - t \cdot \frac{m}{(a, m)}, t \in \mathbb{Z} \right\}.$$

$$= \left\{ x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{(a, m)}} \right\}.$$

Examples: Solve (a) $3x \equiv 7 \pmod{11}$

$$(b) 9x \equiv 6 \pmod{12} \quad (c) 66x \equiv 100 \pmod{121}$$

$$(d) 14x \equiv 1 \pmod{45}$$

$$(a) x_0 = 6 \text{ is a solution} \Rightarrow x \equiv 6 \pmod{11}$$

$$(b) 9x \equiv 6 \pmod{12} \Rightarrow 3 \cdot 3x \equiv 3 \cdot 2 \pmod{12} \text{ and } (12, 3) = 3$$

$$\Rightarrow 3x \equiv 2 \pmod{4}. \quad x_0 = 2 \text{ is a solution}$$

$$\Rightarrow x \equiv 2 \pmod{4}.$$

$$(c) (121, 66) = 11 \neq 100 \Rightarrow \text{no solution.}$$

$$(d) 14x \equiv 1 \pmod{45} \Rightarrow 14x = 45k + 1$$

$$\Rightarrow 14x - 45k = 1$$

$$\text{Euclidean algorithm: } 1 = 5 \cdot 45 - 16 \cdot 14.$$

$$\Rightarrow x_0 = -16 \text{ is a solution} \Rightarrow x \equiv -16 \pmod{45}.$$

Recall: The congruence $ax \equiv b \pmod{m}$ has a solution if and only if $(a, m) | b$. When $(a, m) | b$, the set of all solutions is $\left\{ x \in \mathbb{Z} : x_0 + t \cdot \frac{m}{(a, m)}, t \in \mathbb{Z} \right\}$ which is same as $\left\{ x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{(a, m)}} \right\}$, where x_0 is just one of the solutions.

We can find x_0 using Euclid's algorithm:

$$ax \equiv b \pmod{m} \Rightarrow ax = mk + b \Rightarrow ax - mk = b$$

Inverse in \mathbb{Z}_n : For an a , is there an x such that $ax \equiv 1 \pmod{n}$?

- Only when $(a, n) | 1$, i.e. $(a, n) = 1$. x is called the inverse of a modulo n , and we write $x \equiv a^{-1} \pmod{n}$.

To solve $ax \equiv b \pmod{n}$ with $(a, n) = 1$:

$$ax \equiv b \pmod{n} \Leftrightarrow a^{-1} \cdot a \cdot x \equiv a^{-1} \cdot b \pmod{n}$$

$$\Leftrightarrow x \equiv a^{-1} \cdot b \pmod{n}.$$

Exercise: $(a, n) = 1 \Rightarrow (a^{-1}, n) = 1$.

Also $(a^{-1})^{-1} \equiv a \pmod{n}$.

Some Terminology: In the previous lecture we solved $9x \equiv 6 \pmod{12}$.

$$\text{Answer: } \{x \in \mathbb{Z} : x = 2 + 4t, t \in \mathbb{Z}\}$$

$$= \{x \in \mathbb{Z} : x \equiv 2 \pmod{4}\}$$

Question: Solve $9x \equiv 6 \pmod{12}$ in \mathbb{Z}_{12} .

$$x \equiv 2 \pmod{4} : \dots, 2, 6, 10, 14, 18, 22, 26, \dots$$

$$\Rightarrow x \equiv 2, 6, 10 \pmod{12}$$

Question: Solve $x \equiv 1 \pmod{3}$ in \mathbb{Z}_9 ?

$$x = 3k + 1. \text{ Write } k = 3l + r \text{ with } 0 \leq r \leq 2,$$

$$\Rightarrow x = 3 \cdot (3l + r) + 1 = 9l + 3r + 1$$

$$\Rightarrow x \equiv 1, 4, \text{ or } 7 \pmod{9}.$$

Question: Can we solve $x \equiv 1 \pmod{6}$ in \mathbb{Z}_8 ?

Is 7 in \mathbb{Z}_8 (i.e. $[7]_8$) a solution or not?

- $7 \equiv 1 \pmod{6} \Rightarrow$ it should be a solution
- $[7]_8 = [15]_8$ and $15 \not\equiv 1 \pmod{6} \Rightarrow$ maybe not.

So, we cannot solve $x \equiv 1 \pmod{6}$ in \mathbb{Z}_8 .

In general, when does it make sense to solve $x \equiv a \pmod{m}$ in \mathbb{Z}_n ?

- We should have $b \equiv c \pmod{n} \Rightarrow b \equiv c \pmod{m}$,
i.e. $n \mid b - c \Rightarrow m \mid b - c$.

Only when $m \mid n$.

Simultaneous Linear Congruences

Easier case: Which integers x satisfy both
 $x \equiv 1 \pmod{2}$ and $x \equiv 1 \pmod{5}$?

- We can solve $x \equiv 1 \pmod{2}$ in \mathbb{Z}_n for $2 \mid n$.
 - We can solve $x \equiv 1 \pmod{5}$ in \mathbb{Z}_n for $5 \mid n$.
- \Rightarrow We should expect a solution in \mathbb{Z}_{10} .

$$2 \mid x - 1 \text{ and } 5 \mid x - 1 \Leftrightarrow 10 \mid x - 1 \Leftrightarrow x \equiv 1 \pmod{10}$$

What about $x \equiv 2 \pmod{4}$, $x \equiv 2 \pmod{6}$, $x \equiv 2 \pmod{15}$?

$$4 \mid x - 2, 6 \mid x - 2, 15 \mid x - 2 \Leftrightarrow [4, 6, 15] \mid x - 2$$

60

$$\Leftrightarrow x \equiv 2 \pmod{60}.$$

Theorem: $x \equiv a \pmod{m_1}, x \equiv a \pmod{m_2}, \dots, x \equiv a \pmod{m_k}$
is equivalent to $x \equiv a \pmod{m}$ where $m = [m_1, m_2, \dots, m_k]$.
(Special case: $(m_i, m_j) = 1$ for all $i \neq j$ and $m = m_1 m_2 \dots m_k$)

- If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then working with $m_i = p_i^{\alpha_i}$ might be extremely useful.
- e.g., To prove x is divisible by 120 ($x \equiv 0 \pmod{120}$), we can show that x is divisible by all of 8, 3, and 5.

Next, we make our problem a little bit harder.

which integers x satisfy both $x \equiv 1 \pmod{5}$ and $x \equiv 5 \pmod{7}$?

We should expect to find a solution in \mathbb{Z}_{35} .

$$5k+1 \quad k = 7\ell + r$$

$$x \equiv 1 \pmod{5} \Rightarrow x \equiv 1, 6, 11, 16, 21, 26, 31 \pmod{35}$$

$$x \equiv 5 \pmod{7} \Rightarrow x \equiv 5, 12, 19, 26, 33, 40 \pmod{35}$$

$$\Rightarrow x \equiv 26 \pmod{35}$$

What about $x \equiv 1 \pmod{10}$, $x \equiv 5 \pmod{14}$?

$$[10, 14] = 70$$

$$x \equiv 1 \pmod{10} \Rightarrow x \equiv 1, 11, 21, 31, 41, 51, 61 \pmod{70}$$

$$x \equiv 5 \pmod{14} \Rightarrow x \equiv 5, 19, 33, 47, 61 \pmod{70}$$

$$\Rightarrow x \equiv 61 \pmod{70}.$$

What about $x \equiv 1 \pmod{10}$, $x \equiv 4 \pmod{14}$?

$$[10, 14] = 70$$

$$x \equiv 1 \pmod{10} \Rightarrow x \equiv 1, 11, 21, 31, 41, 51, 61 \pmod{70}$$

$$x \equiv 4 \pmod{14} \Rightarrow x \equiv 4, 18, 32, 46, 60 \pmod{70}$$

\Rightarrow No solution.

$$x \equiv 1 \pmod{10} \Rightarrow x \text{ is odd}$$

$$x \equiv 4 \pmod{14} \Rightarrow x \text{ is even.}$$

We should be careful about this kind of compatibility issues in the linear congruences. The congruences above were not compatible in \mathbb{Z}_2 ($2|10$ and $2|14$) and we won't have such a problem if we work with pairwise coprime moduli.

Chinese Remainder Theorem: (pairwise coprime moduli)

$$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_k \pmod{m_k}$$

with $(m_i, m_j) = 1$ for all $i \neq j$ has a unique solution

$$x \equiv a \pmod{m_1 m_2 \dots m_k} \text{ in } \mathbb{Z}_{m_1 m_2 \dots m_k} \text{ for some } a.$$

- Let's see an example with $k=2$: $x \equiv 2 \pmod{15}$ and $x \equiv 3 \pmod{7}$.

$$x \equiv 3 \pmod{7} \Rightarrow x = 7k + 3. \text{ Now, we solve } 7k + 3 \equiv 2 \pmod{15}$$

$$\Rightarrow 7k \equiv -1 \pmod{15} \Rightarrow 7k \equiv 14 \pmod{15} \Rightarrow k \equiv 2 \pmod{15}.$$

$$\begin{aligned} \text{Write } k &= 15l + 2 \text{ and } x = 7k + 3 = 7(15l + 2) + 3 \\ &= 105l + 17 \end{aligned}$$

$$\text{So, } x \equiv 17 \pmod{105}.$$

Proof: We'll prove by induction on k .

$k=1$: trivial

$k=2$: similar to the example given above.

$$x \equiv a_1 \pmod{m_1} \Rightarrow x = c \cdot m_1 + a_1.$$

$$cm_1 + a_1 \equiv a_2 \pmod{m_2} \Rightarrow cm_1 \equiv a_2 - a_1 \pmod{m_2}.$$

Since $(m_1, m_2) = 1$, there is an $m_1^{-1} \pmod{m_2}$.

$$\text{Then } cm_1 \cdot m_1^{-1} \equiv (a_2 - a_1) \cdot m_1^{-1} \pmod{m_2}$$

$$\Rightarrow c \equiv (a_2 - a_1) \cdot m_1^{-1} \pmod{m_2} \Rightarrow c = l \cdot m_2 + (a_2 - a_1) \cdot m_1^{-1}$$

$$\Rightarrow x = (l \cdot m_2 + (a_2 - a_1) \cdot m_1^{-1}) \cdot m_1 + a_1$$

$$= l \cdot m_1 m_2 + \boxed{(a_2 - a_1) \cdot m_1^{-1} \cdot m_1 + a_1} \rightarrow a \pmod{m_1 m_2}.$$

Assume CRT is true for some k and consider it for $k+1$.

Using base case , combine the last two congruences and apply the induction hypothesis for the remaining congruences.

$$(m_1, m_2, \dots, m_{k-1}, m_k, m_{k+1}) \rightarrow (m_1, m_2, \dots, m_{k-1}, m_k \cdot m_{k+1}).$$

What if we don't have $(m_i, m_j) = 1$?

- Split each $(\text{mod } m_i)$ into some $(\text{mod } p^\alpha)$ using prime factorisations

- For each prime, gather all congruences like $(\text{mod } p^\alpha)$. They will be either incompatible or they can be reduced to a single congruence.

\downarrow
highest power of p

- look at $(\text{mod } p^\alpha)$ with largest α . Other congruences might be incompatible with this one or they will be redundant.

- If everything is compatible, then solve the congruences $(\text{mod } p^\alpha)$ using CRT. If at least one of them is incompatible, then there is no solution.

We'll see some examples on wednesday.

Example: Solve the systems of linear congruences

(a) $x \equiv 1 \pmod{30}$; $x \equiv 13 \pmod{36}$; $x \equiv 11 \pmod{40}$

(b) $x \equiv 11 \pmod{36}$; $x \equiv 7 \pmod{40}$; $x \equiv 32 \pmod{75}$

(a) $x \equiv 1 \pmod{2}$ $x \equiv 13 \pmod{4}$ $x \equiv 11 \pmod{8}$
 $x \equiv 1 \pmod{3}$ $x \equiv 13 \pmod{9}$
 $x \equiv 1 \pmod{5}$ $x \equiv 11 \pmod{5}$

$p=5$: $x \equiv 1 \pmod{5}$ and $x \equiv 11 \pmod{5}$

$\Rightarrow x \equiv 1 \pmod{5}$

$p=3$: $x \equiv 1 \pmod{3}$ and $x \equiv 13 \pmod{9}$

$\Rightarrow x \equiv 4 \pmod{9}$

$p=2$: $x \equiv 1 \pmod{2}$ and $x \equiv 13 \pmod{4}$ and $x \equiv 11 \pmod{8}$

$x \equiv 11 \pmod{8} \Rightarrow x \equiv 11 \pmod{4}$ not compatible with
 $x \equiv 13 \pmod{4}$

incompatible

No solution.

$$(b) \quad x \equiv 11 \pmod{4} ; \quad x \equiv 7 \pmod{8}$$

$x \equiv 11 \pmod{9}$ $\xrightarrow{32} \quad x \equiv 32 \pmod{3}$
 $x \equiv 7 \pmod{5}$ $x \equiv 32 \pmod{25}$

$$p=2 : \quad x \equiv 7 \pmod{8} \quad \checkmark$$

$$p=3 : \quad x \equiv 11 \pmod{9} \quad \checkmark$$

$$p=5 : \quad x \equiv 32 \pmod{25} \quad \checkmark$$

We are solving

$$\begin{array}{ll} (1) & x \equiv 7 \pmod{8} \\ (2) & x \equiv 2 \pmod{9} \\ (3) & x \equiv 7 \pmod{25} \end{array}$$

$$(1) \text{ and } (3) : \quad x \equiv 7 \pmod{8} \quad \Rightarrow \quad x \equiv 7 \pmod{200}$$

$$x \equiv 7 \pmod{25}$$

Now we solve

$$x \equiv 7 \pmod{200}$$

$$x \equiv 2 \pmod{9}$$

$$\begin{array}{c} \times \\ \parallel \\ 200k + 7 \equiv 2 \pmod{9} \end{array}$$

$$\Rightarrow 200k \equiv -5 \pmod{9}$$

$$\Rightarrow 2k \equiv 4 \pmod{9}$$

$$\Rightarrow k \equiv 2 \pmod{9}$$

$$x = 200k + 7 = 200(9\ell + 2) + 7 = 1800\ell + 407$$

$$x \equiv 407 \pmod{1800}.$$

Theorem: (CRT) The congruences $x \equiv a_1 \pmod{m_1}$, \dots , $x \equiv a_k \pmod{m_k}$ has 0 or 1 solution in \mathbb{Z}_m , where $m = [m_1, m_2, \dots, m_k]$.

Exercise: read Theorem 3.12 and its proof from the textbook. It says

solution exists $\Leftrightarrow \gcd(m_i, m_j) \mid a_i - a_j$ for all $i \neq j$.

Some non-linear congruences

$$\text{Solve } x^2 \equiv 1 \pmod{16}.$$

$$0^2 \equiv 0 \pmod{16}, 1^2 \equiv 1 \pmod{16} \quad \text{no need to check}$$

$$3^2 \equiv 9 \pmod{16}, 5^2 \equiv 25 \equiv 9 \pmod{16} \quad \text{even numbers}$$

$$7^2 \equiv 1 \pmod{16}, 9^2 \equiv 1 \pmod{16}, 11^2 \equiv 1 \pmod{5}$$

$$13^2 \equiv 9 \pmod{16}, 15^2 \equiv 1 \pmod{16}$$

$$\Rightarrow x \equiv 1, 7, 9, \text{ or } 15 \pmod{16}$$

$$\text{Solve } x^2 \equiv 1 \pmod{17}$$

$$17 | x^2 - 1 \Rightarrow 17 | \overbrace{(x-1) \cdot (x+1)}^{(x-1)(x+1)}$$

$$\Rightarrow 17 | x-1 \text{ or } 17 | x+1$$

$$\Rightarrow x \equiv 1 \text{ or } 16 \pmod{17}$$

$$\text{Solve } x^2 \equiv -1 \pmod{35}$$

$$\begin{matrix} \downarrow & \downarrow \\ 5 & 7 \end{matrix}$$

$$x^2 \equiv -1 \pmod{5} \quad \text{and} \quad x^2 \equiv -1 \pmod{7}$$

$$x \equiv 2, 3 \pmod{5}$$

no solution

\Rightarrow no solution

Theorem: (CRT) If x has n_i possible values modulo m_i , for $i = 1, 2, \dots, k$ and $(m_i, m_j) = 1$ for all $i \neq j$, then x has $n_1 n_2 \dots n_k$ possible values modulo $m_1 m_2 \dots m_k$.

- How many solutions $x^2 \equiv 1 \pmod{p^\alpha}$ has?

Case - I : p is odd.

$$p^\alpha \mid x^2 - 1 \Rightarrow p^\alpha \mid (x-1) \cdot (x+1)$$

\rightarrow p cannot divide both

$$\Rightarrow p^\alpha \mid x-1 \text{ or } p^\alpha \mid x+1$$

$$\Rightarrow x \equiv 1 \text{ or } -1 \pmod{p^\alpha}$$

\Rightarrow Two solutions

Case - II : $p = 2$

both of them even

$$2^\alpha \mid x^2 - 1 \Rightarrow 2^\alpha \mid (x-1) \cdot (x+1)$$

\rightarrow one of them $4k+2$

$$\Rightarrow 2^{\alpha-1} \mid x-1 \text{ and } 2 \mid x+1$$

or

$$2 \mid x-1 \text{ and } 2^{\alpha-1} \mid x+1$$

$$\Rightarrow x \equiv 1 \text{ or } -1 \pmod{2^{\alpha-1}}$$

$$\Rightarrow x \equiv 1, 2^{\alpha-1}-1, 2^{\alpha-1}+1, 2^\alpha-1 \pmod{2^\alpha}$$

\Rightarrow Four solutions

However, $\alpha=1$ and $\alpha=2$ are exceptional cases (why?) For $\alpha=1$: one sol. $\alpha=2$: two sol

Question: How many solutions does the congruence $x^2 \equiv 1 \pmod{n}$ have in \mathbb{Z}_n ?
(Example 3.18)

$$\begin{array}{ccc}
 & & x^2 \equiv 1 \pmod{9} \\
 & \nearrow & \\
 x^2 \equiv 1 \pmod{36} & & \\
 & \searrow & \\
 & & x^2 \equiv 1 \pmod{4}
 \end{array}$$

We should try to understand \mathbb{Z}_{p^α} to understand \mathbb{Z}_n in general. We begin with the case of $\alpha = 1$, \mathbb{Z}_p .

$$\mathbb{Z}_p = \{[0], [1], [2], \dots, [p-1]\}$$

Congruences modulo p

Linear congruences : $ax \equiv b \pmod{p}$

- Case I: $(p, a) = p$, i.e. $p | a$ (or $a \equiv 0 \pmod{p}$)

Solution x exist $\Leftrightarrow b \equiv 0 \pmod{p}$

- Case II: $(p, a) = 1 \Rightarrow$ There is a unique

solution x in $\mathbb{Z}_{\frac{p}{(p,a)}} = \mathbb{Z}_p$.

- In particular, a^{-1} always exist \pmod{p} unless $a \equiv 0 \pmod{p}$

Let's rewrite this congruence as $f(x) \equiv 0 \pmod{p}$
 where $f(x) = ax - b$.

Note that $f(x) = 3x - 5$ and $g(x) = 10x + 2$ are
 essentially the same modulo 7 (always $f(x) \equiv g(x) \pmod{7}$)
 because $3 \equiv 10 \pmod{7}$ and $-5 \equiv 2 \pmod{7}$. So,
 we can always replace the coefficients with any
 representative of the same congruence class.

In \mathbb{R}, \mathbb{C} a non-zero polynomial of degree d
 has at most d roots. Can we say the same
 thing for the roots in \mathbb{Z}_p ?

- $d=0$: trivial
- $d=1$: shown above

Theorem: (Lagrange) $f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$
 is a polynomial with integer coefficients such that
 $a_i \not\equiv 0 \pmod{p}$ for at least one i . Then,
 $f(x) \equiv 0 \pmod{p}$ has at most d solutions in \mathbb{Z}_p .

- Could be less than d roots : $\boxed{px^2 + 2x + 3}$ has
 degree 2 but can be reduced to $2x + 3$ which
 can have at most 1 root in mod p .

$$(px^2 \equiv 0 \pmod{p}) \Rightarrow px^2 + 2x + 3 \equiv 2x + 3 \pmod{p}$$

- Could be less than d roots even if $a_d \not\equiv 0 \pmod{p}$.
For example $x^2 + 1 \pmod{3}$.
- If $d \gg p \Rightarrow$ trivial.

Proof: Induction on d .

Base cases $d=0, d=1$ are already done.

Assume true for $d-1$, prove for d .

- If $f(x) \equiv 0 \pmod{p}$ has no root, then we are done as $0 \leq d$.

- Suppose a is a root, i.e. $f(a) \equiv 0 \pmod{p}$

$$f(x) - f(a) = a_d(x^d - a^d) + a_{d-1}(x^{d-1} - a^{d-1}) + \dots + a_1(x - a)$$

$$\bullet x^i - a^i = (x - a)(x^{i-1} + ax^{i-2} + a^2x^{i-3} + \dots + a^{i-2}x + a^{i-1})$$

Taking out the common factor $x - a$, we can write $f(x) - f(a) = (x - a) \cdot g(x)$ for some polynomial $g(x)$ with integer coefficient (and $\deg g(x) = d-1$)

$$\Rightarrow f(x) = f(a) + (x - a) \cdot g(x)$$

$$f(x) \equiv 0 \pmod{p} \iff f(a) + (x - a)g(x) \equiv 0 \pmod{p}$$

$$\iff (x - a)g(x) \equiv 0 \pmod{p}$$

$$\iff x \equiv a \pmod{p} \text{ or } g(x) \equiv 0 \pmod{p}$$

\Rightarrow At most $1 + (d-1) = d$ solutions.

Remark: $f(a) \equiv 0 \pmod{p} \Rightarrow f(x) \equiv (x-a)g(x) \pmod{p}$

Corollary: If $f(x) \equiv a_d x^d + \dots + a_0 \equiv 0 \pmod{p}$ has more than d roots, then $a_i \equiv 0 \pmod{p}$ for all i .

Examples:

1. $f(x) = x^2 - 10x + 4 \pmod{5}$.

$f(x) \equiv x^2 + 4 \equiv x^2 - 1 \pmod{5}$ roots: 1, 4 in \mathbb{Z}_p .

2. $f(x) = 8x^3 + 4x^2 - 5x \pmod{7}$

$f(x) = x \cdot (8x^2 + 4x - 5)$

$\bullet 8x^2 + 4x - 5 \equiv 0 \pmod{7}$

Try 0, 1, 2, 3, 4, 5, 6 $\Rightarrow x \equiv 1, x \equiv 2 \pmod{7}$

$8x^2 + 4x - 5 \equiv c \cdot (x-1)(x-2) \pmod{7}$

$8x^2 + 4x - 5 \equiv c \cdot x^2 - 3c \cdot x + 2c \pmod{7}$

$c \equiv 1 \pmod{7} \Rightarrow f(x) = x \cdot (x-1)(x-2) \pmod{7}$

3. $f(x) = x^3 + 2x^2 + 3x - 1 \pmod{5}$

$$f(1) = 5 \equiv 0 \pmod{5}$$

$$f(x) \equiv (x-1)(x^2 + 3x + 1)$$

$$g(x) = x^2 + 3x + 1 \Rightarrow g(1) \equiv 0 \pmod{5}$$

$$g(x) = (x-1)(x+4)$$

$$\Rightarrow f(x) \equiv (x-1)^2 \cdot (x+4) \equiv (x-1)^3 \pmod{5}$$

Solving polynomial congruences \pmod{p} , we can reduce the coefficients \pmod{p} and the next theorem will allow us to reduce the degree of the polynomial as well.

Theorem: (Fermat) For $a \not\equiv 0 \pmod{p}$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Observe that the sets $\{1, 2, \dots, p-1\}$ and

$\{a, 2 \cdot a, 3 \cdot a, \dots, (p-1) \cdot a\}$ are the same \pmod{p} .

For each $b \in \{1, 2, \dots, p-1\}$, we have $ax \equiv b \pmod{p}$ for a unique x .

Then, the product of the elements of these sets must also be the same:

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv a \cdot (2a) \cdot (3a) \cdot \dots \cdot ((p-1)a) \pmod{p}$$

$$\Rightarrow (p-1)! \equiv (p-1)! \cdot a^{p-1} \pmod{p} \quad ((p-1)!, p) = 1.$$

$$\Rightarrow 1 \equiv a^{p-1} \pmod{p}.$$

- $f(x) = x^{p-1} - 1$ and $g(x) = (x-1)(x-2) \cdot \dots \cdot (x-(p-1))$.

$\Rightarrow f(x)$ and $g(x)$ have the same coefficients modulo p .

Proof: Define $h(x) = f(x) - g(x)$

$\deg h \leq p-2$ and $1, 2, \dots, p-1$ are roots of h in \mathbb{Z}_p (more than $\deg h$ roots)

$\Rightarrow h$ has all coefficients 0 mod p

$\Rightarrow f$ and g have the same coefficients mod p .

- For all a , we have $a^p \equiv a \pmod{p}$

- $x^p - x$ and $x \cdot (x-1)(x-2) \cdot \dots \cdot (x-(p-1))$ have the same coefficients modulo p .

Some Applications of Fermat's Theorem

① Compute $2^{1003} \pmod{11}$

$$2^{1003} \equiv (2^{10})^{100} \cdot 2^3 \equiv 1^{100} \cdot 2^3 \equiv 8 \pmod{11}$$

(2) Prove that $n^{25} - n$ is divisible by 30 for all n .

• 5 divides $n^{25} - n$:

- If $n \equiv 0 \pmod{5}$, then $n^{25} - n \equiv 0 \pmod{5}$

- If $n \not\equiv 0 \pmod{5}$, then

$$n^{25} - n \equiv (n^4)^6 \cdot n - n \equiv 1^6 \cdot n - n \equiv 0 \pmod{5}$$

• 3 divides $n^{25} - n$:

- If $n \equiv 0 \pmod{3}$, then $n^{25} - n \equiv 0 \pmod{3}$

- If $n \not\equiv 0 \pmod{3}$, then

$$n^{25} - n \equiv (n^2)^{12} \cdot n - n = 1^{12} \cdot n - n \equiv 0 \pmod{3}$$

• 2 divides $n^{25} - n$:

"similar"

$\Rightarrow [2, 3, 5] = 30$ divides $n^{25} - n$.

$$\textcircled{3} \quad \text{Solve } x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \pmod{5}$$

• If $x \equiv 0 \pmod{5}$, then "not a solution"

$$x^{17} + 6x^{14} + 2x^5 + 1 \not\equiv 0 \pmod{5}.$$

• If $x \not\equiv 0 \pmod{5}$

$$x^{17} + 6x^{14} + 2x^5 + 1 \equiv (x^4)^4 \cdot x + (x^4)^3 \cdot x^2 + 2x^4 \cdot x + 1$$

$$\equiv x + x^2 + 2x + 1$$

$$\equiv x^2 + 3x + 1.$$

$$\Rightarrow x^2 + 3x + 1 \equiv 0 \pmod{5}$$

$$\Rightarrow x^2 - 2x + 1 \equiv 0 \pmod{5}$$

$$\Rightarrow (x-1)^2 \equiv 0 \pmod{5}$$

$$\Rightarrow x \equiv 1 \pmod{5}.$$

Recall : (Fermat's Theorem) $a \not\equiv 0 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

- $x^{p-1} - 1$ and $(x-1)(x-2) \cdot \dots \cdot (x-(p-1))$ have the same coefficients in mod p.
- $x^p - x$ for all a.
- $x^p - x$ and $x(x-1)(x-2) \cdot \dots \cdot (x-(p-1))$ have the same coefficients in mod p.

① Compute $2^{1003} \pmod{11}$

② Prove $30 \mid n^{25} - n$

③ Solve $x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \pmod{5}$

We continue with some applications of Fermat's Theorem.

④ Wilson's Theorem: $n \geq 2$ is a prime if

and only if $(n-1)! \equiv -1 \pmod{n}$

If n is not a prime, then $n = ab$ for some $2 \leq a, b \leq n-1$.

$\Rightarrow (n-1)!$ is divisible by $a \Rightarrow (n-1)! \equiv 0 \pmod{a}$

However $(n-1)! \equiv -1 \pmod{n}$ will require $(n-1)! \equiv -1 \pmod{a}$, not possible.

If n is a prime, then by Fermat's Theorem
 we have $x^{n-1} - 1 \equiv (x-1)(x-2) \cdots (x-(n-1)) \pmod{n}$

Plugging $x=0$ in, we get

$$-1 \equiv (-1) \cdot (-2) \cdot \dots \cdot (-n+1) \pmod{n}$$

$$-1 \equiv (-1)^{n-1} \cdot (n-1)! \pmod{n}$$

$$-1 \equiv (n-1)! \pmod{n} \quad \text{because } n-1 \text{ is even or } n=2.$$

(5) Theorem: p odd prime. $x^2 + 1 \equiv 0 \pmod{p}$

has a solution if and only if $p \equiv 1 \pmod{4}$.

If $x^2 + 1 \equiv 0 \pmod{p} \Rightarrow x^2 \equiv -1 \pmod{p}$

$$\Rightarrow (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

$$\Rightarrow x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

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

$$\Rightarrow \frac{p-1}{2} = 2k \text{ is even}$$

$$\Rightarrow p = 4k+1.$$

If $p \equiv 1 \pmod{4}$, then we write $p = 4k + 1$.

Choose $x = (2k)! = 1 \cdot 2 \cdot 3 \cdots 2k$, then

$$\begin{aligned}x^2 &\equiv (1 \cdot 2 \cdot 3 \cdots 2k) \cdot (1 \cdot 2 \cdot 3 \cdots 2k) \\&\equiv (1 \cdot 2 \cdot 3 \cdots 2k) \cdot (-4k \cdots -(4k-1) \cdots -(4k-2) \cdots \cdots -(2k+1)) \\&\equiv (1 \cdot 2 \cdot 3 \cdots 2k) \cdot ((2k+1) \cdots 4k) \cdot (-1)^{2k} \\&\equiv (4k)! \rightarrow (p-1)! \\&\equiv -1 \pmod{p}\end{aligned}$$

To test whether n is a prime or not, Wilson's Theorem can be used

- $(n-1)! \not\equiv -1 \pmod{n} \Rightarrow n$ is not prime.
 ↓ not easy to compute

On the other hand, computing powers mod n is much easier:

(Successive squaring method)

Compute $11^{42} \pmod{53}$

$$11^{42} = 11^{32} \cdot 11^8 \cdot 11^2$$

$$11^1 \equiv 11 \pmod{53}, 11^2 \equiv 15 \pmod{53}, 11^4 \equiv 13 \pmod{53}$$

$$11^8 \equiv 10 \pmod{53}, 11^{16} \equiv -6 \pmod{53}, 11^{32} \equiv 36 \pmod{53}$$

$$\Rightarrow 11^{42} \equiv 36 \cdot 10 \cdot 15 \equiv (-11) \cdot 15 \equiv -6 \pmod{53}$$

Can we use Fermat's Theorem $a^p \equiv a \pmod{p}$
for primality testing?

- If $a^n \not\equiv a \pmod{n} \Rightarrow n$ is not prime.
- Can we say n is not prime $\Rightarrow a^n \not\equiv a \pmod{p}$?
Answer is "No".

Let's say " n passes the base a test" if
 $a^n \equiv a \pmod{n}$.

Smallest value of a to try is $a=2$.

Question: Is there any composite number n
which passes the base 2 test?

Yes and we'll call such numbers pseudoprimes.

- $341 = 11 \cdot 31$ is a pseudoprime;

To prove $2^{341} \equiv 2 \pmod{341}$

$$\bullet 2^{341} \equiv (2^{10})^{34} \cdot 2 \equiv 1^{34} \cdot 2 \equiv 2 \pmod{11}$$

$$\bullet 2^{341} \equiv (2^{30})^{11} \cdot 2^1 \equiv 1^{11} \cdot 2^1 \equiv 2 \pmod{31}$$



$$2^5 \cdot 2^5 \cdot 2 \equiv 2 \pmod{31}$$

Theorem: There are infinitely many pseudoprimes

Proof: n pseudoprime $\Rightarrow 2^n - 1$ is also pseudoprime

(Textbook Theorem 4.7.)

Exercise

$$\textcircled{1} \quad 3x^2 - y! = 2022$$

mod 2 : $3x^2$ can be $\boxed{0}$ or 1

$y!$ will be $\boxed{0}$ when $y \geq 2$

2022 is $\boxed{0} \times$

mod 3

$3x^2$ is

$y!$ is $\boxed{0}$ when $y \geq 3$

202 is $\boxed{0} \times$

mod 4

$3x^2$ can be 0 or 3

$$3 \cdot 0^2 \equiv 0, \quad 3 \cdot 1^2 \equiv 3, \quad 3 \cdot 2^2 \equiv 0, \quad 3 \cdot 3^2 \equiv 3$$

$y!$ is 0 when $y \geq 4$

2022 is 2

$$0 - 0 \not\equiv 2$$

$$3 - 0 \not\equiv 2$$

no solution

Try $y = 1, 2, 3$

$$3x^2 = y! + 2022$$
$$= 2023, 2024, 2028$$

$$x^2 = \frac{2023}{3}, \frac{2024}{3}, \frac{2028}{3}$$
$$\downarrow \quad \downarrow \quad \downarrow$$
$$\notin \mathbb{Z} \quad \notin \mathbb{Z} \quad 676$$

$$x = 26$$

$$(26, 3)$$

Alternatively, mod 9 works
as well.

(2) (a) $ax \equiv c \pmod{m}$ no sol. or

(m, a) sol. in \mathbb{Z}_m

(b) $ax + by \equiv c \pmod{m}$ no sol.

or $m \cdot (m, a, b)$ sol. $0 \leq x, y \leq m-1$.

(a) From the lectures :

- no sol. if $(m, a) \nmid c$ ✓

→ • unique sol. mod $\frac{m}{(m, a)}$ if $(m, a) \mid c$.

If we say $t \pmod{\frac{m}{(m, a)}}$ is the

unique solution.

In \mathbb{Z}_m , this corresponds to

$$t, t + \frac{m}{(m, a)}, t + 2 \cdot \frac{m}{(m, a)}, \dots, t + ((m, a)-1) \cdot \frac{m}{(m, a)}$$

⇒ There are (m, a) sol. in \mathbb{Z}_m .

(b) $ax + by \equiv c \pmod{m}$

Fix a y

- $ax \equiv c - by \pmod{m}$ has no
sol. in \mathbb{Z}_m or $\boxed{(m, a) \text{ sol. in } \mathbb{Z}_m}$.

for how many fixed values
of y , this is the case?

$ax \equiv c - by \pmod{m}$ has sol.

when $(m, a) \mid c - by$, i.e.

$by \equiv c \pmod{(m, a)}$

- This has $((m, a), b)$ solutions y

in $\mathbb{Z}_{(m, a)}$.

- When we lift these solutions

to \mathbb{Z}_m , there will be

$((m, a), b) \cdot \frac{m}{(m, a)}$ solutions y .

$$\Rightarrow \# \text{ sol.} = ((m, a), b) \cdot \frac{m}{(m, a)} \cdot (m, a)$$

$$= ((m, a), b) \cdot m$$

||

$$= (m, a, b) \cdot m$$

$$\textcircled{3} \quad s_i = \frac{i^2 + i}{2}$$

(a) $m = 2^n$, then $\{s_0, s_1, \dots, s_{m-1}\}$ is CSR mod m

Observation: $\{s_0, s_1, \dots, s_{m-1}\}$ is a CSR

mod m if and only they are all distinct mod m .

WTS: $s_i \not\equiv s_j \pmod{m}$ when $i \neq j$

Assume $i \neq j$ and $s_i \equiv s_j \pmod{m}$

$\Rightarrow s_i - s_j \equiv 0 \pmod{m} \Rightarrow m \mid s_i - s_j$.

$$s_i - s_j = \frac{i^2 + i - j^2 - j}{2} \equiv \frac{(i-j)(i+j+1)}{2}$$

$$\Rightarrow 2^n \mid \frac{(i-j)(i+j+1)}{2}$$

$$\Rightarrow 2^{n+1} \mid (i-j)(i+j+1)$$

both of them
cannot be even

$$\Rightarrow 2^{n+1} \mid i-j \quad \text{or} \quad 2^{n+1} \mid i+j+1$$

$$0 \leq i, j \leq 2^n - 1 \quad \begin{matrix} \nearrow \\ 1 \leq i+j+1 \leq 2^{n+1} - 1 \end{matrix}$$

X

$$-(2^n - 1) \leq i-j \leq 2^n - 1$$

||
v

$$i-j = 0 \Rightarrow i = j, \quad \text{---X}$$

$$(b) m = k \cdot 2^n \quad k \geq 3 \quad \text{odd}.$$

At least 2^{n+1} of s_0, s_1, \dots, s_{m-1}
are divisible by k

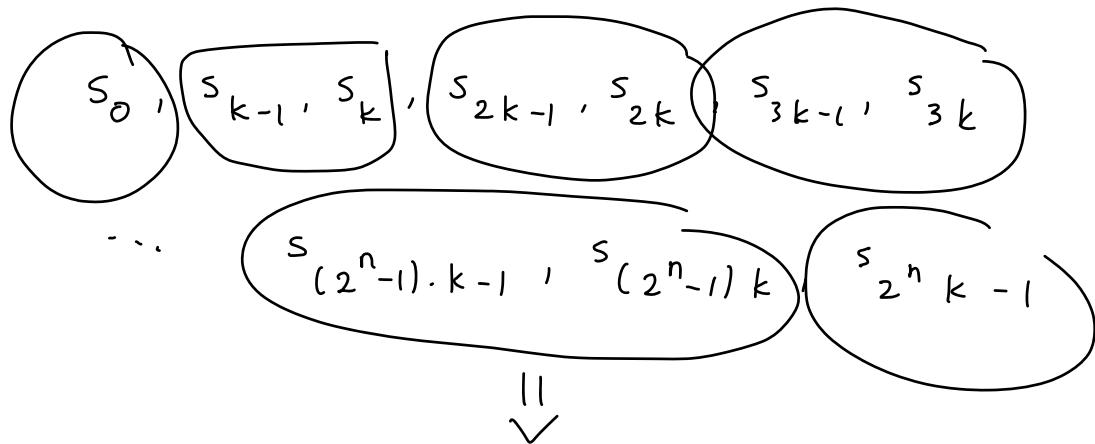
$\{s_0, s_1, \dots, s_{m-1}\}$ is not CSR.

$$k \mid s_i \quad k \mid i^2 + i$$

(with a circle around $i^2 + i$)

$$k \mid i^2 + i = \underbrace{i}_{} \underbrace{(i+1)}_{}$$

$$i \equiv 0, -1 \pmod{k} \Rightarrow k \mid s_i$$



at least 2^{n+1} s_i divisible by k .

In $\pmod{m = 2^n \cdot k}$, which congruence classes are divisible by k

$$k, 2k, 3k, \dots, 2^n \cdot k$$

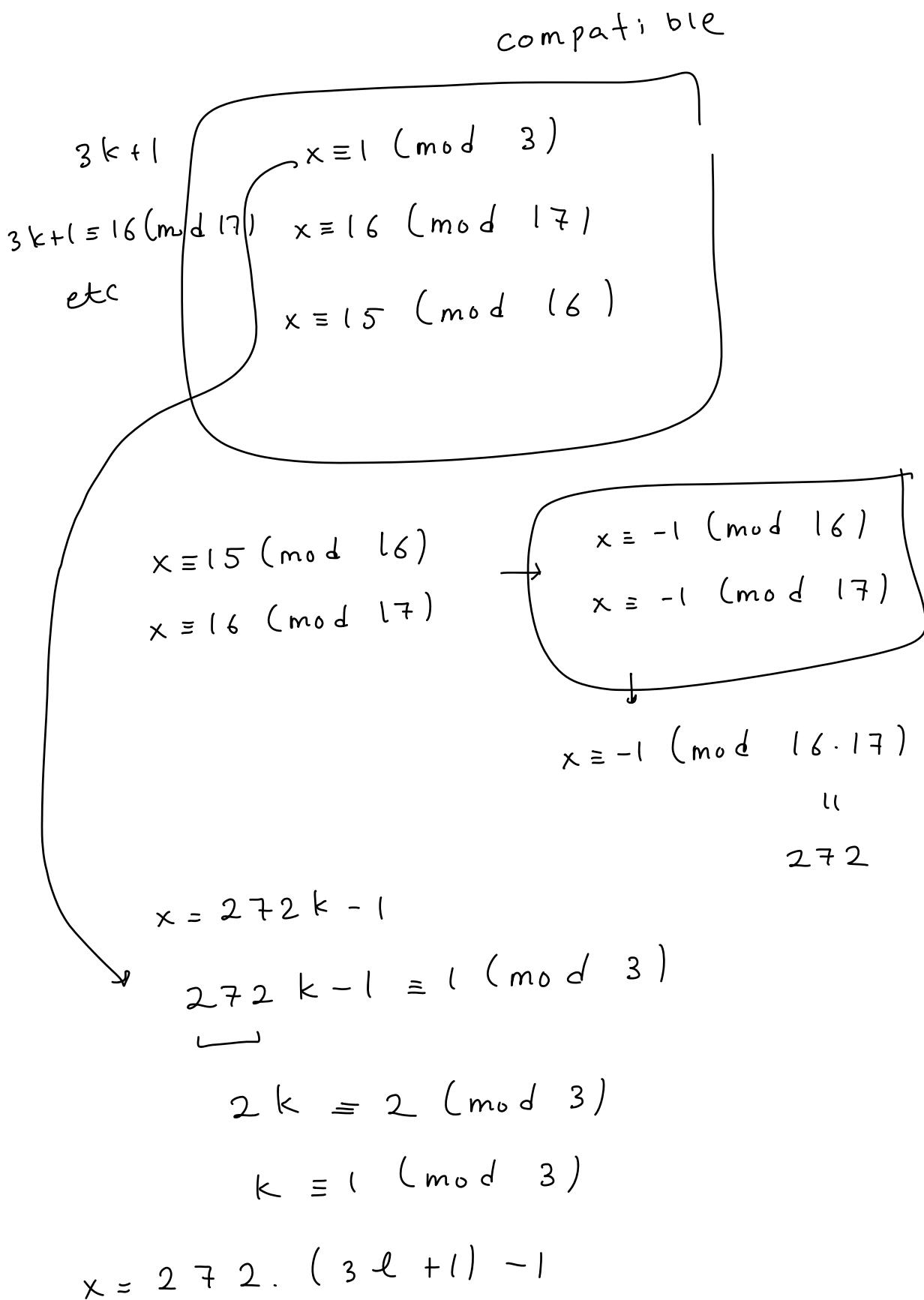
$\underbrace{2^n}_{\text{of them}}$ of them

2^{n+1} si should correspond
 to these 2^n congruence classes
 $\Rightarrow s_i \equiv s_j$ for some i, j .

(4)

$$\begin{aligned}
 & x \equiv 15 \pmod{16} \\
 & x \equiv 16 \pmod{17} \\
 & 3x \equiv 3 \pmod{18} \\
 & x \equiv 1 \pmod{6} \\
 & x \equiv 1 \pmod{2} \\
 & x \equiv 1 \pmod{3}
 \end{aligned}$$

$$\begin{aligned}
 & x \equiv 1 \pmod{3} \\
 & x \equiv 16 \pmod{17} \\
 & x \equiv 15 \pmod{16} \quad x \equiv 1 \pmod{2}
 \end{aligned}$$



$$= \boxed{816 \ell + 271}$$

⑤ $100 \leq n \leq 999$

$$n^2 = \overline{\dots \dots n}$$

$$n^2 \equiv n \pmod{1000}$$

$$n^2 - n \equiv 0 \pmod{1000}$$

$$\rightarrow 2^3 \cdot 5^3$$

$$n \cdot (n-1) \equiv 0 \pmod{1000}$$

$$n \cdot (n-1) \equiv 0 \pmod{8}$$



$$8 \mid n(n-1)$$

$$8 \mid n$$

$$8 \mid n-1$$

$$n(n-1) \equiv 0 \pmod{125}$$



$$125 \mid n(n-1)$$



$$125 \mid n$$



$$125 \mid n-1$$

$$\boxed{n \equiv 0, 1 \pmod{8}}$$

$$\boxed{n \equiv 0, 1 \pmod{125}}$$

$2 \cdot 2 = 4$ solutions in $\mod 1000$.

• $n \equiv 0 \pmod{8}$, $n \equiv 0 \pmod{125}$

||
↓

$$n \equiv 0 \pmod{1000} \quad x$$

• $n \equiv 1 \pmod{8}$, $n \equiv 1 \pmod{125}$

||
∨

$$n \equiv 1 \pmod{1000} \quad x$$

• $n \equiv 0 \pmod{8}$, $n \equiv 1 \pmod{125}$

$$125k + 1 \equiv 0 \pmod{8}$$

$$5k + 1 \equiv 0 \pmod{8} \quad \left. \begin{array}{l} \\ \end{array} \right\} \text{solve}$$
$$k \equiv 3 \pmod{8}$$

$$125k + 1 = 125 \cdot (8\ell + 3) + 1$$

$$= 1000\ell + \boxed{376}$$

$$\bullet n \equiv 1 \pmod{8} \quad n \equiv 0 \pmod{125}$$

$$125k \equiv 1 \pmod{8}$$

$$\begin{aligned} 5k &= 8m + 1 \\ 5k - 8m &= 1 \end{aligned} \quad \left. \begin{aligned} k &\equiv 1 \pmod{8} \\ k &\equiv 5 \pmod{8} \end{aligned} \right\} \text{ solve}$$

$$125k = 125(8l + 5)$$

$$= 1000l + \overline{625}$$

⑥ n powerful if $p|n \Rightarrow p^2|n$

All the exponents are at least two

in the prime factorisation

Inf. many a s.t

$a, a+1, a+2$ not powerful.

$$\boxed{2|n \quad 4+n} \rightarrow 2 \pmod{4}$$

$$3 \mid n \quad 9 \nmid n \rightarrow 3 \text{ or } 6 \pmod{9}$$

$$5 \mid n \quad 25 \nmid n \rightarrow 5, 10, 15, 20 \pmod{25}$$

$\left. \begin{array}{l} a \equiv 2 \pmod{4} \\ a \equiv 2 \pmod{9} \\ a \equiv 3 \pmod{25} \end{array} \right\} \begin{array}{l} a \text{ not powerful} \\ \rightarrow a+1 \text{ not powerful} \\ \rightarrow a+2 \text{ not powerful} \end{array}$

\emptyset

There is a unique solution

$$t \pmod{900}.$$

$$t, t+900, t+2 \cdot 900, t+3 \cdot 900, \dots$$

they all satisfy the condition

back at

$$12 : 23$$

n pseudo prime

$$2^n \equiv 2 \pmod{n}$$

WTS: $2^{2^n - 1} \equiv 2 \pmod{2^n - 1}$

WTS: $2^{2^{2^n - 2}} \equiv 1 \pmod{2^n - 1}$

WTS: $2^{2^{2^n - 2} - 1} \equiv 0 \pmod{2^n - 1}$

WTS: $2^n - 1 \mid 2^{2^n - 2} - 1$.

$2^n - 2 \equiv 0 \pmod{n} \Rightarrow 2^n - 2 = n \cdot k$

WTS: $2^n - 1 \mid 2^{n \cdot k} - 1$



$$(2^n)^k - 1 = (2^n - 1)(\dots)$$

$$2^n \mid 2^{n \cdot k} - 1$$

✓