$\mathbb{Z}$: set of integers

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

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

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 $a \mid b$ in that case and $a \nmid b$ otherwise

- $a \mid 0$ • $a \mid a$ • $a \mid -a$ • $1 \mid a$ for every a.

Next, we prove some properties

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

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

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

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

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

Exercise.

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

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

- $m \neq 0$. $a \mid b \Leftrightarrow ma \mid mb$

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

$\Rightarrow ma \mid mb$.

($\Leftarrow$): If $ma \mid mb$, then $mb = k \cdot ma$

$\Rightarrow b = k \cdot a \Rightarrow a \mid b$. ($m \neq 0$)

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

$x \mid a \Rightarrow a = k \cdot x$

$x \mid b \Rightarrow b = \ell \cdot x$

$\Rightarrow ma + nb = mkx + n\ell x = x(mk + n\ell)$

$\Rightarrow x \mid ma + nb$

Can generalize: $x|a$, $x|b$, $x|c \Rightarrow x|\ell a+mb+nc$ 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 = set of all non-negative integers of the form $a - kb$ ($a, a\pm b, a\pm 2b, a\pm 3b, \ldots$)

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 $0 \leq r_0, r_1 < b$.

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

$\Rightarrow r_0 - r_1 = (k_1 - k_0) \cdot b \Rightarrow b \mid r_0 - r_1 \qquad -b < r_0 - r_1 < b$

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

$\Rightarrow r_0 = r_1$

Now $k_0 b + r_0 = k_1 b + r_1$ 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

- $2k$ (↑ even), $2k+1$ (↑ odd)
- $3k$, $3k+1$, $3k+2$
- $4k$, $4k+1$, $4k+2$, $4k+3$
- $2k$, $4k+1$, $4k+3$

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

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

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

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

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

... continue

Pattern: $(4k)^2 \to 0$

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

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

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

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 $c \mid a$ and $c \mid b$

d is a common multiple of a and b if $a \mid d$ and $b \mid d$.

We define

- $\gcd(a, b)$ (or simply (a, b)) as the greatest common divisor of a and b (except $a = b = 0$)
- $\operatorname{lcm}(a, b)$ (or simply $[a, b]$) as the smallest (positive) common multiple of 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

- $a = k_0 \cdot b + r_0$, $0 \leq r_0 < |b|$

Lemma: $(a, b) = (b, r_0)$. (will prove later)

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

- $b = k_1 \cdot r_0 + r_1$, $0 \leq r_1 < r_0$ $\rightarrow$ $(b, r_0) = (r_0, r_1)$
- $r_0 = k_2 \cdot r_1 + r_2$, $0 \leq r_2 < r_1 < r_0$ $\rightarrow$ $(r_0, r_1) = (r_1, r_2)$

$\vdots$

- $r_{n-2} = k_n \cdot r_{n-1} + r_n$, $r_n = 0$ because $r_0, r_1, r_2, \ldots$ decreasing.

$$\Rightarrow (a, b) = (b, r_0) = (r_0, r_1) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, \underset{\|}{0}\, r_n)$$
$$= r_{n-1}.$$

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

$r_{n-4} = k_{n-2} \cdot r_{n-3} + r_{n-2} \Rightarrow r_{n-2} = r_{n-4} - k_{n-2} \cdot r_{n-3}$

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

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

Same common divisors mean same gcd.

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

$$600 = 4 \cdot 136 + 56$$
$$136 = 2 \cdot 56 + 24$$
$$56 = 2 \cdot 24 + 8$$
$$24 = 3 \cdot 8 + 0$$

$$\Rightarrow (600, 136) = 8$$

$$8 = 56 - 2 \cdot 24 = 56 - 2 \cdot (136 - 2 \cdot 56)$$
$$= 5 \cdot 56 - 2 \cdot 136$$
$$= 5 \cdot (600 - 4 \cdot 136) - 2 \cdot 136$$
$$= 5 \cdot 600 - 22 \cdot 136 .$$

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

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

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.

$a = 24 \quad b = 30$

$(a, b) = 6$

$c \mid a$ and $c \mid b \iff c \mid (a, b)$ common divisors

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

Common divisors are divisors of greatest common divisor

Proof: ($\Leftarrow$): obvious.

$c \mid (a, b) \mid a$ and $c \mid (a, b) \mid b$

($\Rightarrow$): $c \mid a$ and $c \mid b \Rightarrow c \mid ax + by$

$=$

(a, b)

- a, b not both zero

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

$x \mid a, x \mid b, x \mid c \Rightarrow x \mid (a, b)$ and $x \mid c$

$y \mid (a, b)$ and $y \mid c \Rightarrow y \mid a$ and $y \mid b, y \mid c$

Same common divisors, same gcd.

- $m > 0$

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

$(ma, mb) =$ smallest pos. int. $max + mby$

$=$ smallest pos. int. $m(ax + by)$

$= m \cdot$ smallest pos. int. $ax + by$

$= m \cdot (a, b)$

- $\left(\frac{a}{(a,b)} , \frac{b}{(a,b)} \right) = 1$

- $(a,b) = c \Rightarrow a = c \cdot a_1$ 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 $a \mid bc \Rightarrow a \mid c$.

a, b coprime $\Rightarrow ax + by = 1$ for some x and y.
$\Rightarrow acx + bcy = c$

$a \mid acx$ and $a \mid bc \mid bcy \Rightarrow a \mid acx + bcy \Rightarrow a \mid c$.

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 $b \mid c$.

$b \mid c \Rightarrow c = k \cdot b$ and we have $a \mid k \cdot b \Rightarrow a \mid k$
$\Rightarrow k = \ell \cdot a \Rightarrow c = \ell \cdot ab$
$\Rightarrow$ A (positive) common multiple c is at least $|ab|$

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

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

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

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

$c \cdot [a_1, b_1]$: 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:

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

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

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

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

$$\Rightarrow \quad \frac{b}{(a,b)} \;\Big|\; x - x_0 \quad \Rightarrow \quad x - x_0 = m \cdot \frac{b}{(a,b)}$$

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

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

are all of the solutions.

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

a) $66x + 121y = 100$ b) $14x + 8y = 6$

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

b) $14 = 1 \cdot 8 + 6$

$8 = 1 \cdot 6 + 2$

$6 = 3 \cdot 2 + 0$

$\Rightarrow$ $(14, 8) = 2$ and

$$2 = 8 - 1 \cdot 6$$
$$= 8 - (14 - 1 \cdot 8)$$
$$= 2 \cdot 8 - 14$$

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

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

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

$\{ (4m-3, -7m+6) : m \in \mathbb{Z} \}$: 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 $a \mid n$ 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 $(n, p) \mid p \Rightarrow (n, p) = 1$ or p

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

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

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

1	1	$\longrightarrow$ not possible
1	p	$\longrightarrow p \mid b$
p	1	$\longrightarrow p \mid a$
p	p	$\longrightarrow$ both

Can generalize: $p \mid a_1 a_2 \ldots a_k \Rightarrow p \mid a_1$ or $p \mid a_2$ or $\ldots$ $p \mid a_k$.
(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 $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ 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: $n = 2 \longrightarrow n = 2^1$ ✓

Assume $2, 3, \ldots, k$ 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 $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} = n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_\ell^{\beta_\ell}$.

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

$\Rightarrow p_1 = q_i$ 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.

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

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

(They don't have to have same prime factors, but we can write p^0 if p is missing in one of them.
e.g. $196 = 2^2 \cdot 7^2 \cdot 11^0 \cdot 13^0$, $1001 = 2^0 \cdot 7^1 \cdot 11^1 \cdot 13^1$).

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

Questions: 1. When does a divide b?

Answer: $\alpha_1 \le \beta_1, \alpha_2 \le \beta_2, \ldots, \alpha_k \le \beta_k$

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

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

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

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

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

- $(a, b) \cdot [a, b] = a\, b$

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

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

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

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 $a = 2^x \cdot \ldots$ and $b = 2^y \cdot \ldots$

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

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

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

($p^e \| a$: p^e fully divides)

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

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

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

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.

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ and $b = p_{k+1}^{\alpha_{k+1}} \cdot \dots \cdot p_{k+\ell}^{\alpha_{k+\ell}}$

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

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

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

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

Can generalize: If $a_1, a_2, \dots, a_k$ are mutually coprime and $a_1 a_2 \dots a_k$ 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 $m = p_1 p_2 \cdots p_n + 1$.

- 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 $p_i \mid p_1 p_2 \cdots p_n \Rightarrow p_i \mid m - p_1 p_2 \cdots p_n$

$\Rightarrow p_i \mid 1$, 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 $3 = p_1, 7 = p_2, p_3, \cdots, p_n$ are all the primes of the form $4k+3$.

$m = 4p_1p_2\cdots p_n - 1$.

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

$m = 4(p_1p_2\cdots p_n - 1) + 3$

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

- Say $p_i \mid m$.

$p_i \mid 4p_1p_2\cdots p_n \Rightarrow p_i \mid 1$, 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

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

This is true for every a and b, but you may want to have $b|a$ as well because we didn't precisely define what does $p^e \| x$ mean for a rational number x. For example, $5^2 \| \frac{75}{7}$ while $5^{-3} \| \frac{3}{125}$. 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 $2, 3, 4, \ldots, n-1$.

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 $p|a$ and $a|n \Rightarrow p|n$.

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	~~20~~ 3
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~ 5
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~ 7
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

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)

$\Rightarrow n = a_0 + 10 a_1 + 10^2 \cdot a_2 + 10^3 \cdot a_3 + \dots + 10^k \cdot a_k$. (base 10 expansion)

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

So, $2 \mid n \iff 2 \mid a_0$.

- Divisibility by 4: $n = a_0 + 10a_1 + (10^2 a_2 + 10^3 a_3 + \dots + 10^k a_k)$ (12)

So, $4 \mid n \iff 4 \mid \underbrace{a_0 + 10a_1}_{\| \; a_1 a_0}$

can generalize to divisibility by 2^m

- Divisibility by 3:

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

So, $3 \mid n \iff 3 \mid a_0 + a_1 + \dots + a_k$.

- Divisibility by 11:

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

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

So, $11 \mid n \iff 11 \mid a_0 - a_1 + a_2 - \dots + (-1)^k a_k$.

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

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

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

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

- m cannot be odd, because otherwise $2^m + 1 = (2+1)(\dots\dots)$ cannot be prime.

- m is not divisible by any odd number, except 1.

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

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

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

For $2^m + 1$ to be prime, $2^k + 1 = 2^m + 1$

$\Rightarrow k = m \Rightarrow (2a+1) = 1$.

- 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 $j = i + k$.

$$F_i = 2^{2^i} + 1 \;\Big|\; 2^{2^{i+1}} - 1 \;\Big|\; 2^{2^{i+k}} - 1 = F_j - 2$$

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

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

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

$\downarrow$

F_i is odd

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

Modular Arithmetic

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

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

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

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

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

- 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)

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 $b = 4\ell + r$ $\Rightarrow a - b = 4(k-\ell)$ 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)

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

- $[a]_n = [b]_n \iff n \mid a-b$ (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. $[a]_n = [c]_n$ and $[b]_n = [d]_n \Rightarrow [a+b]_n = [c+d]_n$

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

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

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

1. $n \mid c-a$ and $n \mid d-b \Rightarrow n \mid c-a+d-b$
$\Rightarrow n \mid (c+d)-(a+b) \Rightarrow [a+b]_n = [c+d]_n$.

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

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

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

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

- $a+b \equiv c+d \pmod n$
- $ab \equiv cd \pmod n$ $(k \in N)$
- $a^2 \equiv c^2 \pmod n$, $a^3 \equiv c^3 \pmod n$, ..., $a^k \equiv c^k \pmod n$

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.

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

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

$\Rightarrow p(x) \equiv 1 \pmod{3}$, 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 $d \mid m$, then

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

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

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

- Suppose $c > 0$, then

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

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

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

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

The next property is similar to

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

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

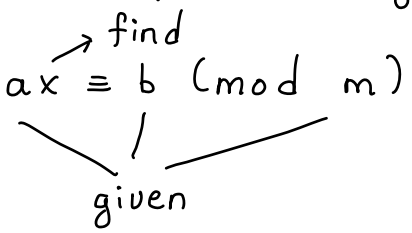
$ax \equiv ay \pmod{m} \Rightarrow m \mid ax - ay \Rightarrow m \mid a \cdot (x-y)$

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

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

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

This property is useful solving linear congruences:



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

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

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

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).

$k \in \mathbb{Z}$

$ax \equiv b \pmod{m}$ means $m \mid ax-b$, i.e. $ax - b = m \cdot k$.

Rewrite it as $ax - mk = b$.

- 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

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

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

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

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

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

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

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

(c) $(121, 66) = 11 \nmid 100 \Rightarrow$ no solution.

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

$\Rightarrow 14x - 45k = 1$

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

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

Recall: The congruence $ax \equiv b \pmod{m}$ has a solution if and only if $(a,m) \mid b$. When $(a,m) \mid b$, 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 $(a,n) \mid 1$, 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 $9x \equiv 6 \pmod{12}$.

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 $\mathbb{Z}_{12}$.

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

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

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

$x = 3k + 1$. Write $k = 3\ell + r$ with $0 \leq r \leq 2$,

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

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

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 $\mathbb{Z}_{10}$.

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

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

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

$[4, 6, 15] = 60$

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

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

- 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 ($x \equiv 0 \pmod{120}$), where $120 = 2^3 \cdot 3^1 \cdot 5^1$,
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 $\mathbb{Z}_{35}$.

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

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

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

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

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.

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

$x \equiv 4 \pmod{14} \Rightarrow x$ 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)

$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, ..., $x \equiv a_k \pmod{m_k}$ with $(m_i, m_j) = 1$ for all $i \neq j$ has a unique solution $x \equiv a \pmod{m_1 m_2 \cdots m_k}$ in $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ for some a.

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

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

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

Write $k = 15\ell + 2$ and $x = 7k + 3 = 7 \cdot (15\ell + 2) + 3$

$= 105\ell + 17$

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 $m_1^{-1} \pmod{m_2}$.

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

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

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

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

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.

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

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.

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

$30 = 2 \cdot 3 \cdot 5$, $36 = 4 \cdot 9$, $40 = 8 \cdot 5$

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

$36 = 4 \cdot 9$, $40 = 8 \cdot 5$, $75 = 3 \cdot 25$

(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) $x \equiv 11 \pmod 4$; $x \equiv 7 \pmod 8$

$x \equiv 11 \pmod 9$

$x \equiv 32 \pmod 3$ (11)

$x \equiv 7 \pmod 5$ (32)

$x \equiv 32 \pmod{25}$

$p = 2$: $x \equiv 7 \pmod 8$ ✓

$p = 3$: $x \equiv 11 \pmod 9$ ✓

$p = 5$: $x \equiv 32 \pmod{25}$ ✓

We are solving

(1) $x \equiv 7 \pmod 8$

(2) $x \equiv 2 \pmod 9$

(3) $x \equiv 7 \pmod{25}$

(1) and (3) : $x \equiv 7 \pmod 8$

$x \equiv 7 \pmod{25}$

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

Now we solve

$x \equiv 7 \pmod{200}$

$x \equiv 2 \pmod 9$

$$\underset{\parallel}{x}$$

$200k + 7 \equiv 2 \pmod 9$

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

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

$\Rightarrow k \equiv 2 \pmod 9$

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

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

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

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

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

Some non-linear congruences

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

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

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

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

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

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

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

$17 \mid x^2 - 1 \Rightarrow 17 \mid (x-1)\cdot(x+1)$

$\Rightarrow 17 \mid x-1$ or $17 \mid x+1$

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

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

$5 \quad 7$

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

$x \equiv 2, 3 \pmod{5}$ no solution

$\Rightarrow$ no solution

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

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

Case - I : p is odd .

$p^\alpha \mid x^2 - 1 \Rightarrow p^\alpha \mid (x-1)\cdot(x+1)$ → p cannot divide both

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

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

$\Rightarrow$ Two solutions

Case - II : $p = 2$

$2^\alpha \mid x^2 - 1 \Rightarrow 2^\alpha \mid (x-1)\cdot(x+1)$ → both of them even; one of them $4k+2$

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

or

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

$\Rightarrow x \equiv 1$ 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)

$$x^2 \equiv 1 \pmod{36} \;\Rightarrow\; \begin{cases} x^2 \equiv 1 \pmod{9} \\ x^2 \equiv 1 \pmod{4} \end{cases}$$

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

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

Congruences modulo p

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

- Case I : $(p, a) = p$, i.e. $p \mid a$ (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 : $px^2 + 2x + 3$ has degree 2 but can be reduced to $2x + 3$ which can have at most 1 root in mod p.

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

- Could be less than d roots even if $a_d \not\equiv 0 \pmod p$. For example $x^2+1 \pmod 3$.
- If $d \geq p \Rightarrow$ 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. $f(a) \equiv 0 \pmod p$

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

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

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 $\deg g(x) = d-1$)

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

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

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

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

$\Rightarrow$ 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. $f(x) = x^2 - 10x + 4$ in mod 5.

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

2. $f(x) = 8x^3 + 4x^2 - 5x$ in mod 7

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

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

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

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

$8x^2 + 4x - 5 \equiv cx^2 - 3cx + 2c \pmod 7$

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

3. $f(x) = x^3 + 2x^2 + 3x - 1$ in mod 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 $\{1, 2, \ldots, p-1\}$ and $\{a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a\}$ are the same mod p.

For each $b \in \{1, 2, \ldots, p-1\}$, 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:

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

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

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

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

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

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

  $\deg h \leq p-2$ and $1, 2, \ldots, p-1$ 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 $x \cdot (x-1)(x-2) \cdot \ldots \cdot (x-(p-1))$ 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 $n^{25}-n$.

③ 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 $(x-1)(x-2)\cdots(x-(p-1))$ have the same coefficients in mod p
- $a^p \equiv a \pmod{p}$ for all a.
- $x^p - x$ and $x(x-1)(x-2)\cdots(x-(p-1))$ 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

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

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

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

because $n-1$ 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 $x = (2k)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2k$, then

$$x^2 \equiv (1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2k) \cdot (1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2k)$$

$$\equiv (1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2k) \cdot \left(-4k \cdot -(4k-1) \cdot -(4k-2) \cdot \ldots \cdot -(2k+1)\right)$$

$$\equiv (1 \cdot 2 \cdot 3 \cdot \ldots 2k) \cdot ((2k+1) \cdot \ldots \cdot 4k) \cdot (-1)^{2k}$$

$$\equiv (4k)! \longrightarrow (p-1)!$$

$$\equiv -1 \pmod p$$

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

- $2^{341} \equiv (2^{10})^{34} \cdot 2 \equiv 1^{34} \cdot 2 \equiv 2 \pmod{11}$
- $2^{341} \equiv (2^{30})^{11} \cdot 2^{11} \equiv 1^{11} \cdot 2^{11} \equiv 2 \pmod{31}$

$\downarrow$

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

Theorem: There are infinitely many pseudoprimes

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

Exercise

(Textbook Theorem 4.7.)

① $3x^2 - y! = 2022$

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

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

2022 is $\boxed{0}$ x

mod 3

$3x^2$ is $\boxed{0}$

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

202 is $\boxed{0}$ x

mod 4

$3x^2$ can be 0 or 3

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

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

2022 is 2

$0 - 0 \not\equiv 2$

$3 - 0 \not\equiv 2$

no solution

Try $y = 1, 2, 3$

$$3x^2 = y! + 2022$$

$$= 2023, 2024, 2028$$

$$x^2 = \frac{2023}{3}, \frac{2024}{3}, \frac{2028}{3}$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$\notin \mathbb{Z} \qquad \notin \mathbb{Z} \qquad 676$$

$$x = 26$$

$$\boxed{(26, 3)}$$

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 $t \bmod \frac{m}{(m,a)}$ is the unique solution.

In $\mathbb{Z}_m$, this corresponds to

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

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

1

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

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

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

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

$$\| \quad (m, a), b)$$

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

③ $s_i = \dfrac{i^2 + i}{2}$

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

Observation: $\{s_0, s_1, \ldots, s_{m-1}\}$ 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 $s_i \equiv s_j \pmod m$

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

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

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

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

both of them cannot be even

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

$0 \le i, j \le 2^n - 1$ $\qquad$ $1 \le i+j+1 \le 2^{n+1}-1$ ×

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

$$\Downarrow$$

$$i-j=0 \Rightarrow i=j \quad , \quad \not\rightarrow$$

(b) $m = k \cdot 2^n \qquad k \ge 3 \quad$ odd.

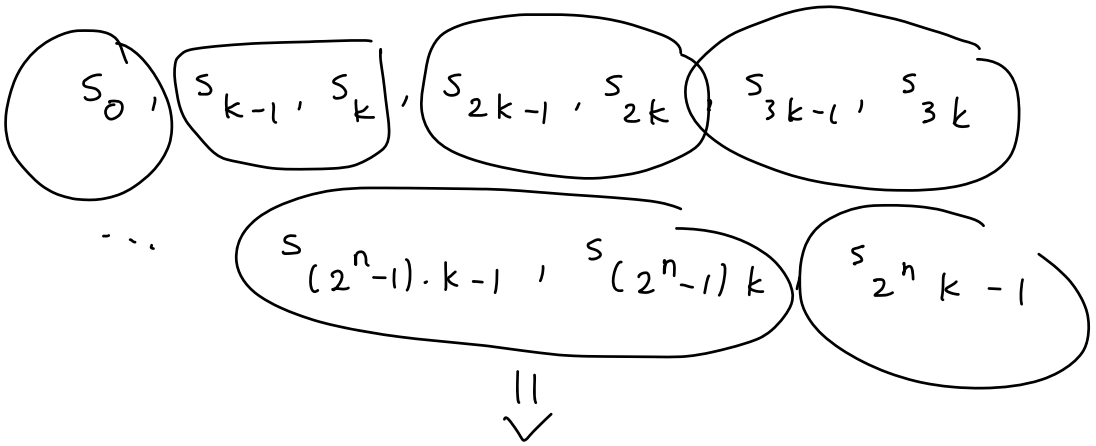
At least 2^{n+1} of $s_0, s_1, \dots, s_{m-1}$ are divisible by k]

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

$k \mid s_i$ $\qquad$ $k \mid \frac{i^2+i}{2}$

$$k \mid i^2 + i = i(i+1)$$

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



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

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

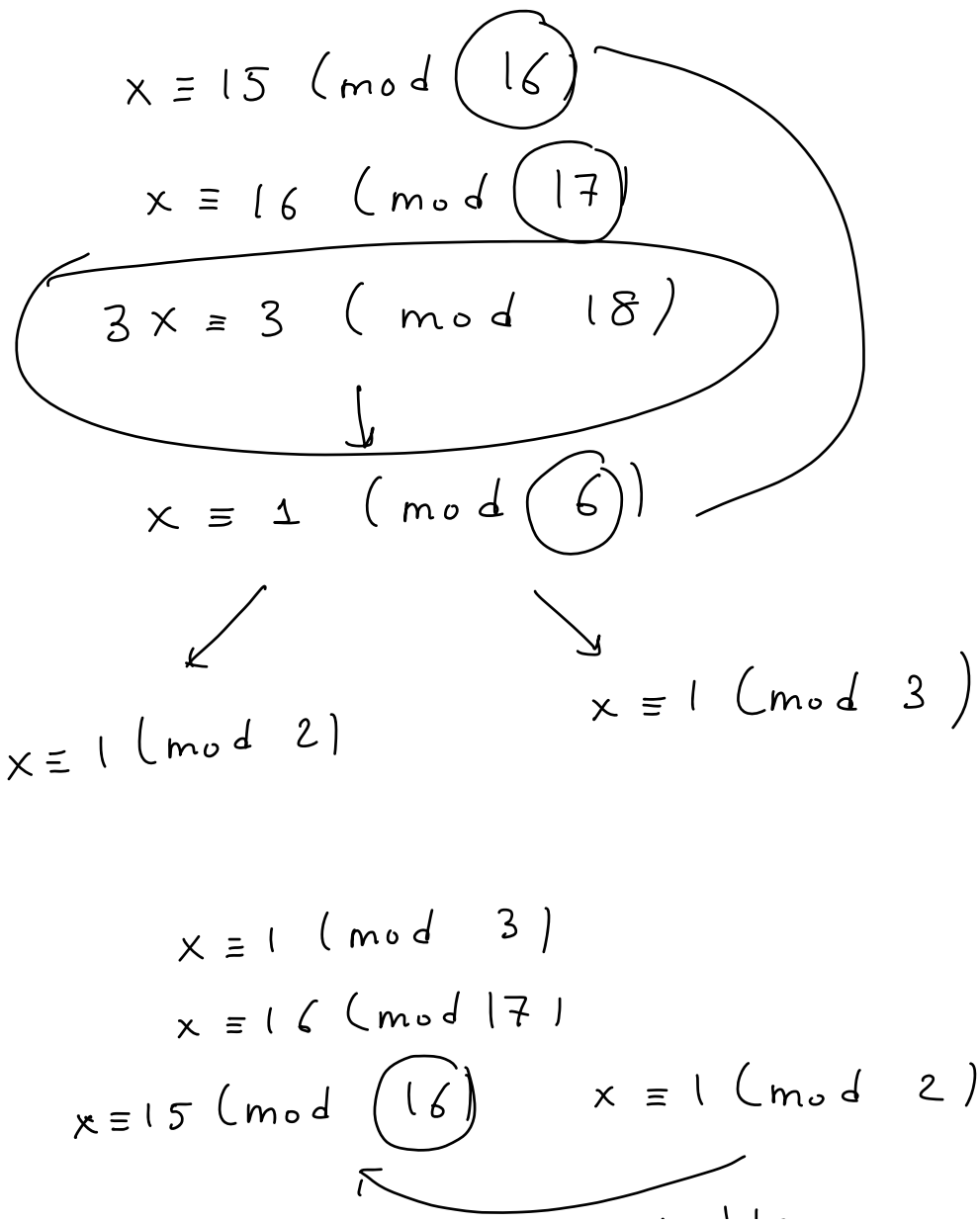
$$\underbrace{k, 2k, 3k, \ldots, 2^n \cdot k}_{2^n \text{ of them}}$$

2^{n+1} s_i should correspond to these 2^n congruence classes

$\Rightarrow$ $s_i \equiv s_j$ for some i, j.

---

(4)



compatible

$3k+1$

$3k+1 \equiv 16 \pmod{17}$

etc

$x \equiv 1 \pmod{3}$

$x \equiv 16 \pmod{17}$

$x \equiv 15 \pmod{16}$

$x \equiv 15 \pmod{16}$

$x \equiv 16 \pmod{17}$

$x \equiv -1 \pmod{16}$

$x \equiv -1 \pmod{17}$

$x \equiv -1 \pmod{16 \cdot 17}$

$=$

272

$x = 272k - 1$

$272k - 1 \equiv 1 \pmod{3}$

$2k \equiv 2 \pmod{3}$

$k \equiv 1 \pmod{3}$

$x = 272 \cdot (3\ell + 1) - 1$

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

(5) $100 \le n \le 999$

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

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

$n^2 - n \equiv 0 \pmod{1000}$ → $2^3 \cdot 5^3$

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

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

$8 \mid n(n-1)$

$8 \mid n$ $\quad$ $8 \mid n-1$

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

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

$125 \mid n(n-1)$

$125 \mid n$ $\quad$ $125 \mid n-1$

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

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

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

$$\Downarrow$$

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

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

$$\Downarrow$$

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

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

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

$$5k + 1 \equiv 0 \pmod 8 \quad \text{solve}$$

$$k \equiv 3 \pmod 8$$

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

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

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

$125k \equiv 1 \pmod 8$

$5k = 8m + 1$ → $5k \equiv 1 \pmod 8$ → solve

$5k - 8m = 1$

$k \equiv 5 \pmod 8$

$125k = 125(8\ell + 5)$

$= 1000\ell + \boxed{625}$

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

All the exponents are at least two in the prime factorisation

Inf. many a s.t

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

$2 \mid n \quad 4 \nmid n \longrightarrow 2 \pmod 4$

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

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

$a \equiv 2 \pmod 4$ $\quad a$ not powerful

$a \equiv 2 \pmod 9 \rightarrow a+1$ not powerful

$a \equiv 3 \pmod{25} \rightarrow a+2$ not powerful

There is a unique solution $t \pmod{900}$.

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

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

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

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: $2^n - 1 \mid 2^{nk} - 1$

↓

$(2^n)^k - 1 = (2^n - 1)(\ldots\ldots)$ ✓

$2^n \mid 2^{nk} - 1$

Recall

- Lagrange
- Fermat: $a^{p-1} \equiv 1 \pmod{p}$ for $(a,p)=1$

  $a^{p} \equiv a \pmod{p}$ for all a

- Wilson
- "n passes base a test" if $a^{n} \equiv a \pmod{n}$
- passing base 2 test: pseudoprime.

e.g. $n = 341$ is a pseudoprime.

$341 = 11 \cdot 31$

341 passes base 2 test. What about base 3 test?

- $3^{341} \equiv (\underbrace{3^{10}}_{1})^{34} \cdot 3 \equiv 3 \pmod{11}$

  $3^{8} \equiv 144 \equiv 20 \equiv -11$

  $3^{4} \equiv 9^{2} \equiv 19 \equiv -12$

- $3^{341} \equiv (\underbrace{3^{30}}_{1})^{11} \cdot 3^{11} \equiv 3^{11} \equiv 3^{1} \cdot 3^{2} \cdot 3^{8} = 3 \cdot 9 \cdot (-11) \equiv 13 \pmod{31}$

$\Rightarrow 3^{341} \not\equiv 3 \pmod{341}$

$\Rightarrow 341$ fails base 3 test.

Question: Is there any composite number which passes base a test, i.e. $a^n \equiv a \pmod{n}$ for all a?

Answer: Yes, and they are called Carmichael numbers.

Example: $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number

- $a^{561} \equiv (a^2)^{280} \cdot a \equiv a \pmod 3$ when $(a,3)=1$, $a^{561} \equiv 0 \equiv a \pmod 3$ if $(a,3) \neq 1$.
- $a^{561} \equiv (a^{10})^{56} \cdot a \equiv a \pmod{11}$ when $(a,11)=1$. $a^{561} \equiv 0 \equiv a \pmod{11}$ if $(a,11) \neq 1$.
- mod 17 is similar: $a^{561} = (a^{16})^{35} \cdot a$.

$\Rightarrow a^{561} \equiv a \pmod{561}$ by CRT.

Exercise: Suppose $n = p_1 p_2 \cdots p_k$ is a product of distinct primes such that $p_i - 1 \mid n-1$ for $i = 1, 2, \ldots, k$, then n is a Carmichael number.

- Same idea with the example. The converse is also true, but we'll not prove now.

Congruences modulo p^k

We now focus on $f(x) \equiv 0 \pmod{p^k}$ (f: polynomial)

We can solve $f(x) \equiv 0 \pmod{p}$, using the solution we'll find we can next solve $f(x) \equiv 0 \pmod{p^2}$, and then $f(x) \equiv 0 \pmod{p^3}$, ... until mod p^k.

Example: $x^3 - x^2 - x + 4 \equiv 0 \pmod{27}$

Step 1: $x^3 - x^2 - x + 4 \equiv 0 \pmod{3}$

$\Rightarrow x \equiv 1, 2 \pmod{3}$

$\Rightarrow x = 3k+1$ or $x = 3k+2$

Step 2.1: $x = 3k+1$

$(3k+1)^3 - (3k+1)^2 - (3k+1) + 4 \equiv 0 \pmod{9}$

$\Rightarrow 27k^3 + 27k^2 + 9k + 1 - 9k^2 - 6k - 1 - 3k - 1 + 4 \equiv 0 \pmod{9}$

$\Rightarrow -9k + 3 \equiv 0 \pmod{9}$

$\Rightarrow 3 \equiv 0 \pmod{9}$, no solution.

Step 2.2: $x = 3k+2$

$(3k+2)^3 - (3k+2)^2 - (3k+2) + 4 \equiv 0 \pmod{9}$

$\Rightarrow 27k^3 + 54k^2 + 36k + 8 - 9k^2 - 12k - 4 - 3k - 2 + 4 \equiv 0 \pmod 9$

$\Rightarrow -15k + 6 \equiv 0 \pmod 9$

$\Rightarrow -5k + 2 \equiv 0 \pmod 3$

$\Rightarrow k + 2 \equiv 0 \pmod 3$

$\Rightarrow k \equiv 1 \pmod 3$

$\Rightarrow x = 3k + 2 = 3 \cdot (3\ell + 1) + 2 = 9\ell + 5$.

Step 3 : $x = 9\ell + 5$

$(9\ell+5)^3 - (9\ell+5)^2 - (9\ell+5) + 4 \equiv 0 \pmod{27}$

$\Rightarrow 9^3\ell^3 + 3 \cdot 9^2 \cdot \ell^2 \cdot 5 + 3 \cdot 9 \cdot \ell \cdot 5^2 + 125 - 81\ell^2 - 90\ell - 25 - 9\ell - 5 + 4 \equiv 0 \pmod{27}$

$\Rightarrow -99\ell + 99 \equiv 0 \pmod{27}$

$\Rightarrow -11\ell + 11 \equiv 0 \pmod 3$

$\Rightarrow \ell + 2 \equiv 0 \pmod 3$

$\Rightarrow \ell \equiv 1 \pmod 3$

$x = 9\ell + 5 = 9 \cdot (3m + 1) + 5 = 27m + 14.$

$x \equiv 14 \pmod{27}$.

Hensel's Lemma: If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $0 \leq t \leq p-1$ such that $f(a + t \cdot p^j) \equiv 0 \pmod{p^{j+1}}$

- what does it mean? If $a \pmod{p}$ is a solution, then a can be lifted uniquely to mod p^2, and to mod p^3, ..., to mod p^k when $f'(a) \not\equiv 0 \pmod{p}$

- $f(x) = x^3 - x^2 - x + 4$ $\quad f(2) \equiv 0 \pmod{3}$
  $f'(x) = 3x^2 - 2x - 1$ $\quad f'(2) \not\equiv 0 \pmod{3}$

$\Rightarrow 2 \pmod{3} \rightarrow 14 \pmod{27}$

However, $f'(1) \equiv 0 \pmod{3}$ and we couldn't lift 1 mod 3 to mod 27.

Before proving Hensel's Lemma,

Binomial Theorem:

$$(x+y)^n = \underbrace{x^n + n \cdot x^{n-1} y}_{\binom{n}{0}=1 \quad \binom{n}{1}} + \binom{n}{2} x^{n-2} y^2 + \ldots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} \cdot y^n$$

e.g. $(x+y)^5 = x^5 + 5x^4 y + 10x^3 y^2 + 10x^2 y^3 + 5xy^4 + y^5$

Proof of Hensel : $f(x) = c_d x^d + c_{d-1} x^{d-1} + \dots + c_1 x + c_0$.

We have $f(a) \equiv 0 \pmod{p^j}$

$$f(a + t \cdot p^j) = c_d \cdot (a + t \cdot p^j)^d + c_{d-1} \cdot (a + t \cdot p^j)^{d-1} + \dots + c_2 \cdot (a + t \cdot p^j)^2 + c_1 \cdot (a + t \cdot p^j) + c_0$$

- With Binomial Theorem

$$(a + t p^j)^d \equiv a^d + d \cdot a^{d-1} \cdot t p^j + \text{something divisible by } p^{j+1}$$

$$\equiv a^d + d \cdot a^{d-1} \cdot t p^j \pmod{p^{j+1}}$$

$$f(a + t p^j) \equiv c_d \cdot (a^d + d a^{d-1} t p^j) + c_{d-1} (a^{d-1} + (d-1) a^{d-2} t p^j) + \dots + c_2 \cdot (a^2 + 2 a t p^j) + c_1 \cdot (a + t p^j) + c_0$$

$$\equiv (c_d a^d + c_{d-1} a^{d-1} + \dots + c_2 a^2 + c_1 a + c_0) + t p^j (c_d \cdot d \cdot a^{d-1} + c_{d-1} (d-1) a^{d-2} + \dots + c_2 \cdot 2 \cdot a + c_1)$$

$$\equiv f(a) + t p^j \cdot f'(a) \pmod{p^{j+1}}$$

$f(a + t \cdot p^j) \equiv 0 \pmod{p^{j+1}}$ means

$f(a) + t \cdot p^j \cdot f'(a) \equiv 0 \pmod{p^{j+1}}$

Write $f(a) = p^j \cdot k$

$p^j \cdot k + t \cdot p^j \cdot f'(a) \equiv 0 \pmod{p^{j+1}}$

$k + t \cdot f'(a) \equiv 0 \pmod{p}$.

We proved $f(a + t \cdot p^j) \equiv 0 \pmod{p^{j+1}}$
if and only if $k + t \cdot f'(a) \equiv 0 \pmod{p}$

If $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique solution t. ∎

Actually, we proved something more.

Hensel's Lemma (continued): Let $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \equiv 0 \pmod{p}$

Case 1: $\frac{f(a)}{p^j} \not\equiv 0 \pmod{p} \Rightarrow a$ cannot be lifted to mod p^{j+1}.

Case 2: $\frac{f(a)}{p^j} \equiv 0 \pmod{p} \Rightarrow f(a + t p^j) \equiv 0 \pmod{p}$ for all $t = 0, 1, \ldots, p-1$, i.e. a can be lifted to p solutions in mod p^{j+1}.

Remark: When $f'(a) \equiv 0 \pmod{p}$, either every lift is a solution or none of them is a solution.

Counting solutions with Hensel

① $x^3 - x^2 + 4x + 1 \equiv 0 \pmod{125}$

In mod 5, $f(1) \equiv f(4) \equiv 0 \pmod{5}$

$f'(x) = 3x^2 - 2x + 4$.

$f'(1) \equiv 0 \pmod{5}$ ↓ no solution

$\frac{f(1)}{5} \not\equiv 0 \pmod{5}$

$f'(4) \not\equiv 0 \pmod{5}$ ↓ unique solution in $\mathbb{Z}_{125}$

$\Rightarrow$ One solution in $\mathbb{Z}_{125}$.

We'll continue with more examples on Wednesday.

Recall

- Lagrange
- Fermat: $a^{p-1} \equiv 1 \pmod{p}$ for $(a,p)=1$

  $a^{p} \equiv a \pmod{p}$ for all a

- Wilson
- "n passes base a test" if $a^{n} \equiv a \pmod{n}$
- passing base 2 test: pseudoprime.

e.g. $n = 341$ is a pseudoprime.

$341 = 11 \cdot 31$

341 passes base 2 test. What about base 3 test?

- $3^{341} \equiv (\underbrace{3^{10}}_{1})^{34} \cdot 3 \equiv 3 \pmod{11}$

  $3^{8} \equiv 144 \equiv 20 \equiv -11$

  $3^{4} \equiv 9^{2} \equiv 19 \equiv -12$

- $3^{341} \equiv (\underbrace{3^{30}}_{1})^{11} \cdot 3^{11} \equiv 3^{11} \equiv 3^{1} \cdot 3^{2} \cdot 3^{8} = 3 \cdot 9 \cdot (-11) \equiv 13 \pmod{31}$

$\Rightarrow 3^{341} \not\equiv 3 \pmod{341}$

$\Rightarrow 341$ fails base 3 test.

Question: Is there any composite number which passes base a test, i.e. $a^n \equiv a \pmod{n}$ for all a?

Answer: Yes, and they are called Carmichael numbers.

Example: $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number

- $a^{561} \equiv (a^2)^{280} \cdot a \equiv a \pmod 3$ when $(a,3)=1$, $a^{561} \equiv 0 \equiv a \pmod 3$ if $(a,3) \neq 1$.
- $a^{561} \equiv (a^{10})^{56} \cdot a \equiv a \pmod{11}$ when $(a,11)=1$. $a^{561} \equiv 0 \equiv a \pmod{11}$ if $(a,11) \neq 1$.
- mod 17 is similar: $a^{561} = (a^{16})^{35} \cdot a$.

$\Rightarrow a^{561} \equiv a \pmod{561}$ by CRT.

Exercise: Suppose $n = p_1 p_2 \cdots p_k$ is a product of distinct primes such that $p_i - 1 \mid n-1$ for $i = 1, 2, \ldots, k$, then n is a Carmichael number.

- Same idea with the example. The converse is also true, but we'll not prove now.

Congruences modulo p^k

We now focus on $f(x) \equiv 0 \pmod{p^k}$ (f: polynomial)

We can solve $f(x) \equiv 0 \pmod{p}$, using the solution we'll find we can next solve $f(x) \equiv 0 \pmod{p^2}$, and then $f(x) \equiv 0 \pmod{p^3}$, ... until mod p^k.

Example: $x^3 - x^2 - x + 4 \equiv 0 \pmod{27}$

Step 1: $x^3 - x^2 - x + 4 \equiv 0 \pmod{3}$

$\Rightarrow x \equiv 1, 2 \pmod{3}$

$\Rightarrow x = 3k+1$ or $x = 3k+2$

Step 2.1: $x = 3k+1$

$(3k+1)^3 - (3k+1)^2 - (3k+1) + 4 \equiv 0 \pmod{9}$

$\Rightarrow 27k^3 + 27k^2 + 9k + 1 - 9k^2 - 6k - 1 - 3k - 1 + 4 \equiv 0 \pmod{9}$

$\Rightarrow -9k + 3 \equiv 0 \pmod{9}$

$\Rightarrow 3 \equiv 0 \pmod{9}$, no solution.

Step 2.2: $x = 3k+2$

$(3k+2)^3 - (3k+2)^2 - (3k+2) + 4 \equiv 0 \pmod{9}$

$\Rightarrow 27k^3 + 54k^2 + 36k + 8 - 9k^2 - 12k - 4 - 3k - 2 + 4 \equiv 0 \pmod 9$

$\Rightarrow -15k + 6 \equiv 0 \pmod 9$

$\Rightarrow -5k + 2 \equiv 0 \pmod 3$

$\Rightarrow k + 2 \equiv 0 \pmod 3$

$\Rightarrow k \equiv 1 \pmod 3$

$\Rightarrow x = 3k + 2 = 3 \cdot (3\ell + 1) + 2 = 9\ell + 5$.

Step 3 : $x = 9\ell + 5$

$(9\ell+5)^3 - (9\ell+5)^2 - (9\ell+5) + 4 \equiv 0 \pmod{27}$

$\Rightarrow 9^3\ell^3 + 3 \cdot 9^2 \cdot \ell^2 \cdot 5 + 3 \cdot 9 \cdot \ell \cdot 5^2 + 125 - 81\ell^2 - 90\ell - 25 - 9\ell - 5 + 4 \equiv 0 \pmod{27}$

$\Rightarrow -99\ell + 99 \equiv 0 \pmod{27}$

$\Rightarrow -11\ell + 11 \equiv 0 \pmod 3$

$\Rightarrow \ell + 2 \equiv 0 \pmod 3$

$\Rightarrow \ell \equiv 1 \pmod 3$

$x = 9\ell + 5 = 9 \cdot (3m + 1) + 5 = 27m + 14.$

$x \equiv 14 \pmod{27}$.

Hensel's Lemma: If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $0 \leq t \leq p-1$ such that $f(a + t \cdot p^j) \equiv 0 \pmod{p^{j+1}}$

- what does it mean? If $a \pmod{p}$ is a solution, then a can be lifted uniquely to mod p^2, and to mod p^3, ..., to mod p^k when $f'(a) \not\equiv 0 \pmod{p}$

- $f(x) = x^3 - x^2 - x + 4$ $\quad f(2) \equiv 0 \pmod{3}$
  $f'(x) = 3x^2 - 2x - 1$ $\quad f'(2) \not\equiv 0 \pmod{3}$

$\Rightarrow 2 \pmod{3} \rightarrow 14 \pmod{27}$

However, $f'(1) \equiv 0 \pmod{3}$ and we couldn't lift 1 mod 3 to mod 27.

Before proving Hensel's Lemma,

Binomial Theorem:

$$(x+y)^n = \underbrace{x^n + n \cdot x^{n-1} y}_{\binom{n}{0}=1 \quad \binom{n}{1}} + \binom{n}{2} x^{n-2} y^2 + \ldots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} \cdot y^n$$

e.g. $(x+y)^5 = x^5 + 5x^4 y + 10x^3 y^2 + 10x^2 y^3 + 5xy^4 + y^5$

Proof of Hensel : $f(x) = c_d x^d + c_{d-1} x^{d-1} + \dots + c_1 x + c_0$.

We have $f(a) \equiv 0 \pmod{p^j}$

$$f(a + t \cdot p^j) = c_d \cdot (a + t \cdot p^j)^d + c_{d-1} \cdot (a + t \cdot p^j)^{d-1} + \dots + c_2 \cdot (a + t \cdot p^j)^2 + c_1 \cdot (a + t \cdot p^j) + c_0$$

- With Binomial Theorem

$$(a + t p^j)^d \equiv a^d + d \cdot a^{d-1} \cdot t p^j + \text{something divisible by } p^{j+1}$$

$$\equiv a^d + d \cdot a^{d-1} \cdot t p^j \pmod{p^{j+1}}$$

$$f(a + t p^j) \equiv c_d \cdot (a^d + d a^{d-1} t p^j) + c_{d-1} (a^{d-1} + (d-1) a^{d-2} t p^j) + \dots + c_2 \cdot (a^2 + 2 a t p^j) + c_1 \cdot (a + t p^j) + c_0$$

$$\equiv (c_d a^d + c_{d-1} a^{d-1} + \dots + c_2 a^2 + c_1 a + c_0) + t p^j (c_d \cdot d \cdot a^{d-1} + c_{d-1} (d-1) a^{d-2} + \dots + c_2 \cdot 2 \cdot a + c_1)$$

$$\equiv f(a) + t p^j \cdot f'(a) \pmod{p^{j+1}}$$

$f(a + t \cdot p^j) \equiv 0 \pmod{p^{j+1}}$ means

$f(a) + t \cdot p^j \cdot f'(a) \equiv 0 \pmod{p^{j+1}}$

Write $f(a) = p^j \cdot k$

$p^j \cdot k + t \cdot p^j \cdot f'(a) \equiv 0 \pmod{p^{j+1}}$

$k + t \cdot f'(a) \equiv 0 \pmod{p}$.

We proved $f(a + t \cdot p^j) \equiv 0 \pmod{p^{j+1}}$
if and only if $k + t \cdot f'(a) \equiv 0 \pmod{p}$

If $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique solution t. ∎

Actually, we proved something more.

Hensel's Lemma (continued): Let $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \equiv 0 \pmod{p}$

Case 1: $\frac{f(a)}{p^j} \not\equiv 0 \pmod{p} \Rightarrow a$ cannot be lifted to mod p^{j+1}.

Case 2: $\frac{f(a)}{p^j} \equiv 0 \pmod{p} \Rightarrow f(a + t p^j) \equiv 0 \pmod{p}$ for all $t = 0, 1, \ldots, p-1$, i.e. a can be lifted to p solutions in mod p^{j+1}.

Remark: When $f'(a) \equiv 0 \pmod{p}$, either every lift is a solution or none of them is a solution.

Counting solutions with Hensel

① $x^3 - x^2 + 4x + 1 \equiv 0 \pmod{125}$

In mod 5, $f(1) \equiv f(4) \equiv 0 \pmod{5}$

$f'(x) = 3x^2 - 2x + 4$.

$f'(1) \equiv 0 \pmod{5}$ ↓ no solution

$\frac{f(1)}{5} \not\equiv 0 \pmod{5}$

$f'(4) \not\equiv 0 \pmod{5}$ ↓ unique solution in $\mathbb{Z}_{125}$

$\Rightarrow$ One solution in $\mathbb{Z}_{125}$.

We'll continue with more examples on Wednesday.

We continue with a few more examples on counting the solutions to polynomial congruences modulo p^k using Hensel's lemma.

② $f(x) = x^2 + x + 7$. $f(x) \equiv 0 \pmod{27}$

$f(0) = 7 \not\equiv 0 \pmod 3$ $f(1) = 9 \equiv 0 \pmod 3$ $f(2) = 13 \not\equiv 0 \pmod 3$

$f'(x) = 2x + 1$ and $f'(1) \equiv 3 \equiv 0 \pmod 3$

In mod 9 either

- 1, 4, 7 are all solutions, or
- none of them is a solution.

$f(1) = 9 \equiv 0 \pmod 9 \Rightarrow$ 1 is a solution mod 9

$\Rightarrow$ 1, 4, 7 are solutions mod 9.

$f(1) = 9 \not\equiv 0 \pmod{27} \Rightarrow$ 1, 10, 19 are not solutions in mod 27.

$f(4) = 27 \equiv 0 \pmod{27} \Rightarrow$ 4, 13, 22 are solutions mod 27.

$f(7) = 63 \not\equiv 0 \pmod{27} \Rightarrow$ 7, 16, 25 are not solutions in mod 27.

$\Rightarrow x \equiv 4, 13, 22 \pmod{27}$

③ $f(x) = x^3 + 4x^2 + 19x + 1 \qquad f(x) \equiv 0 \pmod{25}$

$f(0) \equiv 1$, $f(1) \equiv 0$, $f(2) \equiv 3$, $f(3) \equiv 1$, $f(4) \equiv 0 \pmod 5$

$f'(x) = 3x^2 + 8x + 19 \qquad f'(1) \equiv 0 \pmod 5$, $f'(4) \not\equiv 0 \pmod 5$

- 4 can be lifted uniquely to mod 25.
- $f(1) = 25 \equiv 0 \pmod{25}$

$\Rightarrow$ 1, 6, 11, 16, 21 are solutions mod 25

So, $1 + 5 = 6$ solutions in mod 25.

Recall Fermat's Theorem

$$a^{p-1} \equiv 1 \pmod p \quad \text{when} \quad (a, p) = 1$$

Is it true when p is replaced with a composite number?

Not in general. For example,

$$3^3 \not\equiv 1 \pmod 4$$

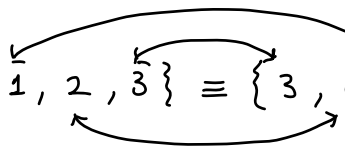
$$5^5 \not\equiv 1 \pmod 6$$

Goal: To modify the proof of Fermat's Theorem to have a result mod n.

Is this true: $(a,n)=1$. $\{1,2,\ldots,n-1\}$ and

$\{a, 2a, \ldots, (n-1)\cdot a\}$ are the same mod n?

- For example $\{1,2,3\} \equiv \{3,6,9\} \pmod 4$.



- This will be true, but let's not prove it.

$$\Rightarrow 1\cdot 2\cdot 3\cdot \ldots \cdot (n-1) \equiv a\cdot 2a\cdot 3a\cdot \ldots (n-1)a \pmod n$$

$$\Rightarrow 1\cdot 2\cdot 3\cdot \ldots \cdot (n-1) \equiv a^{n-1}\cdot 1\cdot 2\cdot 3\cdot \ldots \cdot (n-1) \pmod n$$

However, we cannot do the cancellations here because

$$ux \equiv uy \pmod n \Rightarrow x \equiv y \left(\mod \frac{n}{(n,u)}\right)$$

To have the analog of Fermat's Theorem, we should work with

$$\{u : 1 \leq u \leq n-1 \text{ and } (n,u)=1\}$$

instead of $\{1,2,\ldots,n-1\}$.

Definition: We'll say u is a **unit** modulo n if it has an **inverse** (or equivalently $(u,n)=1$).

↘ $u^{-1} \pmod{n}$: $uu^{-1} \equiv 1 \pmod{n}$

- Definition doesn't depend on the representative u of a congruence class.

e.g. $5 \pmod 6$, $11 \pmod 6$, $17 \pmod 6$

Units of $\mathbb{Z}_8$: $1, 3, 5, 7$

Units of $\mathbb{Z}_9$: $1, 2, 4, 5, 7, 8$

Units of $\mathbb{Z}_{10}$: $1, 3, 7, 9$

Units of $\mathbb{Z}_p$: $1, 2, 3, \dots, p-1$.

Theorem: Let u and v be units in $\mathbb{Z}_n$. Then,

- u^{-1} , v^{-1}
- $-u$, $-v$
- uv

are also units in $\mathbb{Z}_n$.

Proof: • u^{-1} and v^{-1} are units by definition

• $(-u)\cdot(-u^{-1}) \equiv 1 \equiv (-v)\cdot(-v^{-1}) \pmod{n}$

$\Rightarrow -u$ and $-v$ are units

• $(uv)\cdot(u^{-1}v^{-1}) = uu^{-1}\cdot vv^{-1} \equiv 1 \pmod{n}$

$\Rightarrow uv$ is a unit.

Recall : u is a unit mod n when u^{-1} mod n exist, or equivalently when $(u,n)=1$

$u u^{-1} \equiv 1 \pmod{n}$

- $1, -1$ are units
- u is a unit $\Rightarrow u^{-1}$ is also a unit
- u, v are units $\Rightarrow uv$ is a unit

Definition: $\phi(n)$ = number of units in $\mathbb{Z}_n$

(Euler's function)

$= \left| \{ u : 1 \leq u \leq n-1 \text{ and } (u,n)=1 \} \right|$.

$\phi(8) = 4$

$\phi(9) = 6$

$\phi(10) = 4$

$\phi(p) = p-1$.

Back to Fermat's analog in $\mathbb{Z}_n$.

Claim: Suppose $(a,n)=1$, then we have

$$\{u : 1 \le u \le n-1 \text{ and } (u,n)=1\}$$

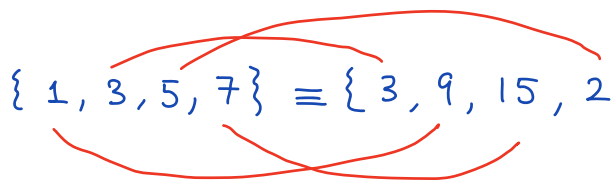
$$\Vert\Vert$$

$$\{au : 1 \le u \le n-1 \text{ and } (u,n)=1\}$$

in $\mathbb{Z}_n$.

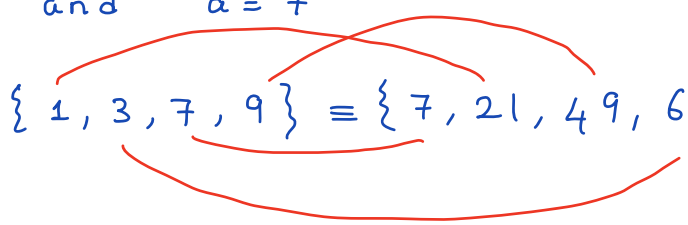
e.g. $n=8$ and $a=3$

$$\{1,3,5,7\} \equiv \{3,9,15,21\} \pmod 8$$



$n=10$ and $a=7$

$$\{1,3,7,9\} \equiv \{7,21,49,63\} \pmod{10}$$



Proof: $\{u : 1 \le u \le n-1 \text{ and } (u,n)=1\}$ has $\phi(n)$ elements, all units.

$(a,n)=1$ and $(u,n)=1 \Rightarrow (au,n)=1 \Rightarrow au$ is unit.

Also $au \equiv av \pmod n \iff u \equiv v \pmod n$

So, $\{au : 1 \le u \le n-1 \text{ and } (u,n)=1\}$ has $\phi(n)$ distinct elements, all units. ■

Similar to Fermat's Theorem, we now have

Euler's Theorem: Suppose $(a, n) = 1$, then we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

- $n = p$ gives Fermat.

How to compute $\phi(n)$?

An example: $n = 12$

$(u, 12) = 1 \iff (u, 4) = 1$ and $(u, 3) = 1$

$\downarrow$ $\qquad$ $\downarrow$

$1 \pmod 4$ $\qquad$ $1 \pmod 3$

$3 \pmod 4$ $\qquad$ $2 \pmod 3$

$\Downarrow$ CRT

$1 \pmod{12}$

$5 \pmod{12}$

$7 \pmod{12}$

$11 \pmod{12}$

$\phi(12) = \phi(4) \cdot \phi(3)$

$= 4$

Theorem: For $(m,n)=1$, we have

$$\phi(mn) = \phi(m)\cdot\phi(n)$$

Proof: $(u, mn) = 1 \iff (u,m)=1$ and $(u,n)=1$

There are $\phi(m)$ values in $\mathbb{Z}_m$ and $\phi(n)$ values in $\mathbb{Z}_n$. By CRT, there are $\phi(m)\,\phi(n)$ units in $\mathbb{Z}_{mn}$.

- $\phi(1) = 1$ by convention.

Corollary: $\phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \ldots \cdot \phi(p_k^{\alpha_k})$

Now, it is remained to compute $\phi(p^k)$.

$(u, p^k) = 1 \iff (u,p) = 1$, i.e. $p \nmid u$.

$\{u : 1 \le u \le p^k - 1 \text{ and } (u, p^k) = 1\}$

$= \{u : 1 \le u \le p^k - 1 \text{ and } p \nmid u\}$

$= \{u : 1 \le u \le p^k - 1\} - \{p, 2p, 3p, \ldots, (p^{k-1}-1)\cdot p\}$

Theorem: p prime, $k \ge 1$. Then,

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}\cdot(p-1) = p^k\cdot\left(1 - \frac{1}{p}\right)$$

Theorem: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Then

$$\phi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1} \right)$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1)$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i} \cdot \left(1 - \frac{1}{p_i} \right)$$

$$= n \cdot \prod_{i=1}^{k} 1 - \frac{1}{p_i} .$$

- Compute $\phi(42)$, $\phi(48)$, $\phi(60)$

$$\phi(42) = \phi(2 \cdot 3 \cdot 7)$$

$$= 42 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7}$$

$$= 12$$

$$\phi(48) = \phi(2^4 \cdot 3)$$

$$= 48 \cdot \frac{1}{2} \cdot \frac{2}{3}$$

$$= 16$$

$$\phi(60) = \phi(2^2 \cdot 3^1 \cdot 5^1)$$

$$= 2^{2-1} \cdot (2-1) \cdot 3^{1-1} \cdot (3-1) \cdot 5^{1-1} \cdot (5-1)$$

$$= 2 \cdot 2 \cdot 4$$

$$= 16$$

- Last two digits of $3^{2001} = ?$

$$3^{2001} \bmod (100) = ?$$

$$\phi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$$\Rightarrow 3^{2001} \equiv (3^{40})^{50} \cdot 3 \equiv 1^{50} \cdot 3 \equiv 3 \pmod{100}$$

$\Rightarrow$ Last two digits 03.

- Prove $a^{12} \equiv 1 \pmod{42}$ for $(a, 42) = 1$.

$$\phi(42) = 12 \Rightarrow a^{12} \equiv 1 \pmod{42}$$

- Similarly,

$$a^{16} \equiv 1 \pmod{48} \quad \text{for} \quad (a, 48) = 1$$

$$a^{16} \equiv 1 \pmod{60} \quad \text{for} \quad (a, 60) = 1.$$

Next goal: to understand the structure of the units of $\mathbb{Z}_n$ better.

Start with $n=p$ prime and the following observation:

- units of $\mathbb{Z}_3$: $\{1, 2\} \equiv \{2, 2^2\} \pmod 3$
- units of $\mathbb{Z}_5$: $\{1, 2, 3, 4\} \equiv \{2, 2^2, 2^3, 2^4\} \pmod 5$
- units of $\mathbb{Z}_7$: $\{1, 2, 3, 4, 5, 6\} \not\equiv \{2, 2^2, 2^3, 2^4, 2^5, 2^6\}$

2^4 → 2 again

However $\{1, 2, 3, 4, 5, 6\} \equiv \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$

$3 \to 2 \to 6 \to 4 \to 5 \to 1$

in $\mathbb{Z}_7$.

We make the following claim:

Theorem: p prime. There exists an integer g such that $\{1, 2, \ldots, p-1\} \equiv \{g, g^2, g^3, \ldots, g^{p-1}\}$ in $\mathbb{Z}_p$.

• g satisfying this condition will be called a primitive root.

We'll prove the theorem later. For now assume it is true if necessary.

Theorem: A unit u is a primitive root (mod p) if and only if the smallest positive integer k satisfying $u^k \equiv 1 \pmod{p}$ is $k = p-1$.

Proof: $\Rightarrow$: Suppose u is a primitive root, then $u, u^2, \ldots, u^{p-2}$ must be different than u^{p-1} which is $1 \pmod{p}$ by Fermat. So, $u^k \not\equiv 1 \pmod{p}$ for $1 \leq k \leq p-2$ and $u^{p-1} \equiv 1 \pmod{p}$ by Fermat.

$\Leftarrow$: Suppose the smallest pos. int. k with $u^k \equiv 1 \pmod{p}$ is $k = p-1$.

$u, u^2, u^3, \ldots, u^{p-1}$ are all distinct mod p since

$$u^i \equiv u^j \pmod{p} \iff u^{i-j} \equiv 1 \pmod{p}$$

shouldn't be $< p-1$

Therefore, $\{u, u^2, \ldots, u^{p-1}\} \equiv \{1, 2, \ldots, p-1\} \pmod{p}$.

Definition: Let u be a unit in $\mathbb{Z}_n$. We call the smallest positive integer k satisfying

$$u^k \equiv 1 \pmod{n}$$

the **order of u modulo n**, denoted by $\mathrm{ord}_n(u)$.

- A primitive root (modulo p) is a unit of order $p-1$.

Theorem: g is a primitive root modulo p and $k \geq 0$ is an integer. Then,

$$g^k \equiv 1 \pmod{p} \iff p-1 \mid k$$

Proof: Write $k = (p-1)\cdot n + r$ with $0 \leq r < p-1$

$$g^k \equiv 1 \pmod{p} \iff g^{(p-1)\cdot n} \cdot g^r \equiv 1 \pmod{p}$$

$$\iff g^r \equiv 1 \pmod{p}$$

because $g^r \equiv 1 \pmod{p}$ and r positive $\Rightarrow r \geq p-1$.

$$\iff r = 0$$

$$\iff k = (p-1)\cdot n$$

$$\iff p-1 \mid k.$$

Next, we compute the orders of the units modulo p. More specifically $\mathrm{ord}_p(g^a)$ for $1 \leq a \leq p-1$.