MATH 453

NUMBER THEORY

W/ prof Alexandru Zaharescu

Meets @ Altgeld 245 12:30-13:50

Tuesday, January 21st 2025

Thursday, January 23rd 2025

HW 1 due Thursday, January 30th 2025
HW 2 due Thursday, February 6th 2025
HW 3 due Thursday, February 13th 2025
MIDTERM 1 Thursday, February 20th 2025

REMINDERS!

Notations:

- $\mathbb{N} = \{0, 1, 2, \dots\}$
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, $(\mathbb{Z}, +, \cdot)$ form a ring
- $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$ $(\mathbb{Q}, +, \cdot)$ form a field
- $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ where $i^2 = -1$, $(\mathbb{C}, +, \cdot)$ form a field

Prove that "$\sqrt{7}$ irrational":

Assume that $\sqrt{7} = \frac{a}{b}$ and a, b not both mult. of 7

$7 = \frac{a^2}{b^2} \Leftrightarrow a^2 = 7b^2$

$7b^2$: multiple of 7 $\Rightarrow$ a^2 is multiple of 7

So a is a multiple of 7

$a = 7k \rightarrow 7b^2 = a^2 = 49k^2$

$b^2 = 7k^2$

multiple of seven $\Rightarrow$ b^2 multiple of 7

Contradiction!

Squares

Ex: write 29 as sum of 2 squares: $5^2 + 2^2 = 29$

Not all numbers can be written as sum of 2 squares

- $x^2 + y^2 = (x + iy)(x - iy)$

Ex: 2929 as sum of 2 squares

$2929 = 29(101) = (5^2 + 2^2)(10^2 + 1^2)$

$= (5 + 2i)(5 - 2i)(10 + i)(10 - i)$

$2929 = (48 + 25i)(48 - 25i) = 48^2 + 25^2$

sum of 2 squares!

CHAPTER 1

DEFINITION: Let $a, b \in \mathbb{Z}$. Then a divides b, denoted $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$. If $a \mid b$, a is said to be a divisor of b. (Notation $a \nmid b$: a doesn't divide b)

↳ Ex: $12 \mid 60$, $5 \mid 15$, $7 \nmid 20$, etc.

PROPOSITION: Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$

↳ Ex: $7 \mid 21$, $21 \mid 42$, $7 \mid 42$

PROPOSITION: Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid ma + nb$ where $m, n \in \mathbb{Z}$

↳ Ex: $7 \mid 21$, $7 \mid 14$ } $10 \cdot (14) + 3(21)$ is also divisible by $7 \rightarrow 7 \mid 203$

DEFINITION: Let $x \in \mathbb{R}$. Then $[x]$ is the greatest integer less-than or equal to x

↳ Ex: $[2.3] = 2$, $[-2.3] = -3$

THEOREM: (DIVISION ALGORITHM)

Let $a, b \in \mathbb{Z}$, $b > 0$. Then there are unique $q, r \in \mathbb{Z}$ s.t. $a = q \cdot b + r$, $0 \leq r < b$

↳ Ex: $a = 100$, $b = 7$, then $q = 14$ and $r = 2$. $100 = 7(14) + 2$

Proof: take $q = \left[\frac{a}{b}\right]$, $r = a - bq$

$$q = \left[\frac{a}{b}\right] \leq \frac{a}{b} < \left[\frac{a}{b}\right] + 1$$

$$qb \leq a < b(q+1)$$

$$0 \leq \underbrace{a - qb}_{r} < b$$

$$\boxed{0 \leq r < b} \quad \square$$

Tuesday, January 28th 2025

PRIME NUMBERS

DEFINITION: Let $p \in \mathbb{Z}$ with $p > 1$. Then p is prime if the only positive divisors of p are 1 and p.
If $n \in \mathbb{Z}$ with $n > 1$ and n not prime, then n is said to be a composite number

PROPOSITION: Let n be a composite number. Then n has a prime divisor p with $p \leq \sqrt{n}$

THEOREM (EUCLID): There are infinitely many prime numbers

↳ Proof: Assume there are only finitely many primes:

$p_1, p_2, \ldots, p_k$

Let $n = p_1 p_2 p_3 \ldots p_k + 1$. Obvious $n > p_k$

If n is a prime, then n is a prime number larger than p_k, contradicting the assumption □

If n is not a prime, let p be a prime divisor of n. So p belongs to the list of primes.

$p = p_j$ where $1 \leq j \leq k$

Then $p_j \mid 1 + p_1 p_2 \ldots p_k$ and $p_j \mid p_1 p_2 \ldots p_k$. Difference 1, but 1 is not a multiple of p_j. Contra □

PROPOSITION: For any positive integer, there are at least n consecutive composite numbers.

"How many zeros in the right end in a factorial?"

In $n!$, how many factor of 5?

Ex: $100!$

CONJECTURE: (TWIN PRIME) Let p and q be primes. If $|p - q| = 2$, then p, q twin primes. There are infinitely many.

DEFINITION: Let $x \in \mathbb{R}$, $x > 0$

$\pi(x) = \#\{p : p \text{ prime}, 2 \leq p \leq x\}$ (Prime counting function)

THEOREM (PRIME NUMBER): $\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$, $\pi(x) \sim \frac{x}{\ln x}$

CONJECTURE: (GOLDBACH) Every even integer greater than 2 can be represented as the sum of 2 prime numbers

DEFINITION: Any prime number of the form $2^p - 1$ with p prime is called a Mersenne prime

↳ CONJECTURE: There are infinitely many Mersenne primes

DEFINITION: Any prime number of the form $2^{2^n} + 1$ with $n \in \mathbb{Z}$, $n \geq 0$ is called a Fermat prime

Thursday, January 30th 2025.

Greatest Common Divisors

DEFINITION: Let $a, b \in \mathbb{Z}$, not both zero, then greatest common divisor of a and b, denoted by $\gcd(a,b)$ is the largest positive integer d s.t. $d|a$ and $d|b$. If $\gcd(a,b)$ is 1, then a and b is said to be relatively prime / coprime

Ex: $a = 30$, $b = 9$

$a = 30 = 3 \cdot 10 = 3 \cdot 2 \cdot 5$

$b = 9 = 3 \cdot 3$

Then $\gcd(a,b) = 3$

Ex: $a = 77$, $b = 96$

$a = 77 = 7 \cdot 11$

$b = 96 = 3 \cdot 32$

$\gcd(a,b) = 1$, therefore a, b relatively prime

PROPOSITION: Let $a, b \in \mathbb{Z}$ with $\gcd(a,b) = d$, then $\frac{a}{d}$ and $\frac{b}{d}$ is relatively prime

PROPOSITION: Let $a, b \in \mathbb{Z}$ not both zero. Then $\gcd(a,b) = \min\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$

Ex: $\gcd(60, 75) = 15$

$\gcd(60, 75) = \min\{60m + 75n : m, n \in \mathbb{Z}, 60m + 75n > 0\}$

$\{60m + 75n : m, n \in \mathbb{Z}, 60m + 75n > 0\} = \{15, 30, 45, \dots\}$

DEFINITION: Let $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}$. Then $\gcd(a_1, a_2 \dots a_n)$ by definition is the greatest integer d s.t. $d|a_1, d|a_2, \dots, d|a_n$. If $\gcd(a_1, a_2 \dots a_n) = 1$, then they're relatively prime

If $\gcd(a_i, a_j)$ for all pairs i, j with $i \neq j \Rightarrow$ pairwise prime

LEMMA: If $a, b \in \mathbb{Z}$, $a \geq b \geq 1$ and $a = bq + r$ where $q, r \in \mathbb{Z}$, then

$$\gcd(a, b) = \gcd(b, r)$$

proof: Let $\gcd(a,b) = d$ and $\gcd(b,r) = D$. We know that $d \mid a$ and $d \mid b$. Then, $d \mid a - bq$. It implies that $d \mid r$. So d are common divisor of b and r, D is the largest common divisor of b and r. So, $D \geq d$. $D \mid b$ and $D \mid r$, therefore $D \mid bq + r$ implies that $D \mid a$. So, $D \mid b$ and $D \mid a$. We have that $D \leq d$. It's only true if $D = d$ □

THEOREM: Let $a, b \in \mathbb{Z}$ with $a \geq b \geq 1$. By the division algorithm, there exists $q_1, r_1 \in \mathbb{Z}$ s.t. $a = bq_1 + r_1$ and $0 \leq r_1 < b$. If $r_1 > 0$, then there exists $q_2, r_2 \in \mathbb{Z}$ s.t. $b = r_1 q_2 + r_2$ and $0 \leq r_2 < r_1$. If $r_2 > 0$, there exists $q_3, r_3 \in \mathbb{Z}$ s.t. $r_1 = r_2 q_3 + r_3$ and $0 \leq r_3 < r_2$. Continue the process, then $r_n = 0$ for some n. Then, $\gcd(a,b) = r_{n-1}$. If $n = 1$, then $\gcd(a,b) = b$.

proof: By the above lemma, $\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \dots = \gcd(r_{n-1}, r_n)$. But by the assumption, $r_n = 0$. Thus, $\gcd(a,b) = \gcd(r_{n-1}, 0) = r_{n-1}$ □

Ex: Find $\gcd(750, 72)$

$$\begin{array}{r|l} 72 & 750 \\ & 72 \\ \hline & 30 \end{array} \quad 10$$

$$750 = 72(10) + \widetilde{30}^{\,r_1}$$

$$72 = 30(2) + \widetilde{12}^{\,r_2}$$

$$30 = 12(2) + \widetilde{6}^{\,r_3}$$

$$12 = 6(2) + \widetilde{0}^{\,r_4}$$

Tuesday, February 4th 2025

Fundamental Theorem of Arithmetic

LEMMA: Let $a, b, p \in \mathbb{Z}$ with p prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

proof: Assume that p prime and $p \mid ab$ but $p \nmid a$. Then, $\gcd(p, a) = 1$.
By proposition, $\exists m, n \in \mathbb{Z}$ s.t. $ma + np = 1$. Follows that $mab + npb = b$.
Then $\frac{b}{p} = \frac{mab}{p} + nb$. By assumption, $p \mid ab$. Therefore, $p \mid b$. □

Corollary: If $a_1, a_2, \dots, a_n \in \mathbb{Z}$, p prime, $p \mid \prod_{i=1}^{n} a_i$, then
$p \mid a_i$ for some i.

THEOREM: Every integer greater than 1 can be expressed in the form $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ with $p_1, p_2, \dots, p_k$ distinct primes and $a_1, a_2, \dots a_k \in \mathbb{N}$. Prime factorization is unique except for the rearrangement of the $p_i^{a_i}$.

Uniqueness proof: Assume $n = p_1^{a_1} \dots p_k^{a_k} = q_1^{b_1} \dots q_\ell^{b_\ell}$. Then $p_1 \mid p_1^{a_1} \dots p_k^{a_k}$, so $p_1 \mid q_1^{b_1} \dots q_\ell^{b_\ell}$.
By corollary, $p_1 \mid q_i$ for some i. But, q_i is a prime. Thus, $p_1 = q_i$. Repeating then we have $p_2^{a_2} \dots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \dots q_i^{b_i - a_i} \dots q_k$. Repeating one have
$1 = \underbrace{q_1 \dots q_u}_{\text{cannot be prime}}$ Thus factorization is unique □

Thursday, February 6th 2025.

DEFINITION: Let $a, b \in \mathbb{Z}$, $a, b > 0$. Then, $\text{lcm}(a,b)$ is the least positive integer m s.t. $a \mid m$ and $b \mid m$

Proposition: Let $a, b \in \mathbb{Z}$, $a, b > 1$ with

$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$
$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$

with $p_1, p_2, \ldots, p_n$ distinct primes
$a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \geq 0$

Then $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$ and $\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$

THEOREM: Let $a, b \in \mathbb{Z}$ with $ab > 0$. Then $\gcd(a,b) \cdot \text{lcm}(a,b) = ab$

THEOREM (DIRICHLET'S): Let $a, b \in \mathbb{Z}$, $a, b \geq 1$ and $\gcd(a,b) = 1$. Then the arithmetic progression:

$a, a+b, a+2b, \ldots, a+nb, \ldots$

contains infinitely many prime numbers

Tuesday, February 11th 2025.

EXAM NEXT WEEK THURSDAY
- Euclidean Algorithm
- Sums of two squares
- gcd, lcm
- prime fact
- Chinese Remainder Theorem

} 75 minutes

CONGRUENCES

DEF: Let $a, b, m \in \mathbb{Z}$ with $m \geq 1$. Then $a \equiv b \bmod m$ if $m \mid a-b$. (a congruent b mod m)

Proposition: Congruence modulo m is an equivalence relation on $\mathbb{Z}$

- Reflexive: $a \equiv a \bmod m$
- Symmetric: $a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$
- Transitive: $a \equiv b \bmod m \wedge b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$

Consequence: $\mathbb{Z}$ is partitioned into equivalence classes under congruence modulo m

Ex: $m = 10$

$[1] = \{\dots, -9, 1, 11, 21, 31, \dots\}$ $\quad [1] = [31]$

$[1]$: class of 1 — All integers that are congruent to $1 \bmod m$

There are m residue classes modulo m

DEF: A complete residue system modulo m is a set of integers such that every integer is congruent to exactly one integer of the set

Ex: $m = 10$

$\{31, 22, 3, 54, 55, 56, 17, 28, 39, 100\}$

$\in [1] \quad \in [2] \quad \in [3] \quad \dots \quad \in [7] \quad \in [8] \quad \in [9]$

$\in [4] \quad \in [5] \quad \in [6] \quad \in [10]$

$\{0, 1, 2, \dots, m-1\} \overset{\text{def}}{=}$ Set of least non-negative residues mod m

Proposition: If $\begin{cases} a \equiv b \bmod m \\ c \equiv d \bmod m \end{cases}$ then $\begin{matrix} a+c \equiv b+d \bmod m \\ ac \equiv bd \bmod m \end{matrix}$

Proof:

- $a \equiv b \bmod m \Rightarrow m \mid a-b$
  $c \equiv d \bmod m \Rightarrow m \mid c-d$
  $\Rightarrow m \mid (a+c)-(b+d)$
  $\Downarrow a+c \equiv b+d \bmod m$ □

- $a \equiv b \bmod m \Rightarrow m \mid a-b \Rightarrow m \mid c(a-b)$ (multiple of m)
  $c \equiv d \bmod m \Rightarrow m \mid c-d \Rightarrow m \mid b(c-d)$
  $\Rightarrow m \mid ac - bc + bc - bd$
  $m \mid ac - bd \Rightarrow ac \equiv bd \bmod m$ □

Ex: $10 \equiv 25 \mod 3$, $8 \equiv 2 \mod 3$ $\Rightarrow$ $18 \equiv 27 \mod 3$, $80 \equiv 50 \mod 3$

Addition and multiplication of residue classes is well-defined

Def: $[a] + [b] = [a+b]$, $[a] \cdot [b] = [ab]$

Ex: $m = 3$

$[10] + [8] = [18]$ by definition (equal / identical)

$[25] + [2] = [27]$ by definition (equal / identical)

$[10] \cdot [8] = [80]$

$[25] \cdot [2] = [50]$

Proposition: Let $a, b, c, m \in \mathbb{Z}$, $m \geq 1$. Then $ca \equiv cb \mod m$ if and only if $a \equiv b \mod \frac{m}{\gcd(c,m)}$

Ex: $10 \equiv 25 \mod 3$. Let $c = 5$, $a = 2$, $b = 5$, $m = 3$

Then $ca \equiv cb \mod m \longrightarrow 5 \cdot 2 \equiv 5 \cdot 5 \mod 3$

$\gcd(c,m) = \gcd(5,3) = 1$

$10 \equiv 25 \mod 3 \Longrightarrow 2 \equiv 5 \mod 3$

If $ca \equiv cb \mod m$ and $\gcd(c,m) = 1$, then $a \equiv b \mod m$

Thursday, February 13th 2025.

Linear Congruences in One Variable

Theorem: Let $ax \equiv b \mod m$ be a linear congruence and let $d = \gcd(a,m)$. If $d \nmid b$, then the congruence has no solutions in $\mathbb{Z}$. If $d \mid b$, then the congruence has exactly d incongruent solutions modulo m in $\mathbb{Z}$

Ex: $4x \equiv 7 \mod 10$

$d \nmid b$ as $d = 2$ and $b = 7$

Thus x doesn't have any sol. in $\mathbb{Z}$.

Ex: $4x \equiv 6 \mod 10$

We should have 2 incongruent solutions

NOT CONGRUENT TO EACH OTHER MOD 10

All solutions: $\{\ldots, 4, 9, 14, 19, \ldots\}$

$[4]$ and $[9]$ $\rightarrow$ $[4] \cup [9]$

Corollary: If $\gcd(a,m)=1$, then the congruence $ax \equiv 1 \bmod m$ has exactly one solution modulo m

x is said to be the multiplicative inverse of $a \bmod m$.

Ex: Find inverse of $7 \bmod 10$

$7x \equiv 1 \bmod 10$

We have $x=3$ satisfies, so $x = \{\dots, -7, 3, 13, \dots\}$

Set of x values: $[3]$

Ex: Solve $4x \equiv 1 \bmod 7$

$x = \{\dots 2, 9, 16, \dots\}$

REMARK: Assume a, m gen. $\neq \gcd(a,m)=1$. To find inverse of $a \bmod m$, solve equation $ax+my=1$. To solve equation $ax+my=1$, use Euclidean algorithm to find $\gcd(a,m)$

Ex: Find inverse of 69 mod 100 (a, m)

find $x \in \mathbb{Z}$ s.t. $69x \equiv 1 \bmod 100$

Solve $69x + 100y = 1$ using Euclidean alg to find $\gcd(69,100)$

$100 = 69 \cdot 1 + 31$

$69 = 31 \cdot 2 + 7$

$31 = 7 \cdot 4 + 3$

$7 = 3 \cdot 2 + 1$

$3 = 1 \cdot 3 + 0$

$\Rightarrow \gcd(69,100) = 1$

$1 = 7 - 2(3)$

$1 = 7 - 31(2) + 8(7)$

$1 = 9(7) - 31(2)$

$1 = 9(69 - 2(31)) - 2(100 - 69)$

$1 = 9(69) - 18(31) - 2(100) + 2(69)$

$1 = 11(69) - 2(100) - 18(100) + 18(69)$

$1 = 29(69) - 20(100)$

$\Rightarrow X = 29$, $Y = -20$

$\Rightarrow 29 \cdot 69 \equiv 1 \bmod 100$

Answer: 29

Ex: Inverse 100 mod 69

$29 \cdot 69 - 20 \cdot 100 = 1$

Then $-20 \cdot 100 \equiv 1 \bmod 69$

$\{\dots, -20, 49, 118, \dots\} = [49]$

Theorem (Chinese Remainder Theorem): Let $m_1, m_2, \dots, m_k$ be pairwise relatively prime positive integers and $b_1, b_2, \dots, b_k \in \mathbb{Z}$.

Then the system of congruences:

$$\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \\ \vdots \\ x \equiv b_k \bmod m_k \end{cases}$$

has a unique solution modulo $m_1 m_2 \dots m_k$

Ex: $\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 12 \end{cases}$ Solve for x

By CRT, there's unique solution modulo 60.

$\begin{cases} x \equiv 2 \bmod 5 \Rightarrow x \in \{\dots -3, 2, 7, 12, 17, 22, (27), \dots\} \\ x \equiv 3 \bmod 12 \Rightarrow x \in \{\dots -9, 3, 15, (27), \dots\} \end{cases}$

$x = 27$ is a solution!

Next solution: 87.

Set of solutions: $\{\dots 27, 87, \dots\}$

$x \equiv 2 \bmod 5 \Leftrightarrow x = 2 + 5n$ for some $n \in \mathbb{Z}$

$x \equiv 3 \bmod 12 \Leftrightarrow x = 3 + 12m$ for some $m \in \mathbb{Z}$

$2 + 5n = 3 + 12m$

$5n - 12m = 1$

Use Euclidean algo!

$n = 5, m = 2$

is a solution

$\boxed{x = 27}$

Tuesday, February 19th 2025

THEOREM (WILSON): For any prime number p, we have $(p-1)! \equiv -1 \bmod p$

Ex: $p = 5$ $\quad$ $p = 7$

$(p-1)! = 4! = 24$ $\quad$ $(p-1)! = 6! = 720$

$24 \equiv -1 \bmod 5$ $\quad$ $720 \equiv -1 \bmod 7$

Proof: idea: combine $a \in \{1, 2, \dots, p-1\}$ with its inverse mod p

write the corresponding congruences

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

$1 \cdot 1 = 1 \bmod p$

Ex: $p = 13$

$1 \cdot 1 \equiv 1 \bmod 13$

$2 \cdot 7 \equiv 1 \bmod 13$

$3 \cdot 9 \equiv 1 \bmod 13$

$4 \cdot 10 \equiv 1 \bmod 13$

$5 \cdot 8 \equiv 1 \bmod 13$

$6 \cdot 11 \equiv 1 \bmod 13$

$12 \equiv -1 \bmod 13$

$12! \equiv -1 \bmod 13$

THEOREM (F. Little): For any prime p and any integer a such that $p \nmid a$:

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

Proof: idea: $\{1, 2, \dots, p-1\}$ times by $a \rightarrow$

$a(1) \equiv r_1 \bmod p$

$a(2) \equiv r_2 \bmod p$

$\vdots$

$a(p-1) \equiv r_{p-1} \bmod p$

$r_1, r_2, \dots, r_{p-1}$ are incongruent mod p

$a^{p-1}(p-1)! \equiv (p-1)! \bmod p$ $\quad$ $\times$

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

EX: $p = 13$, $a = 6$

Check $6^{12} \equiv 1 \bmod 13$

$6 \cdot 1 \equiv 6 \bmod 13$

$6 \cdot 2 \equiv 12 \bmod 13$

$6 \cdot 3 \equiv 5 \bmod 13$

$6 \cdot 4 \equiv 11 \bmod 13$

$6 \cdot 5 \equiv 4 \bmod 13$

$6 \cdot 6 \equiv 10 \bmod 13$

$6 \cdot 7 \equiv 3 \bmod 13$

$6 \cdot 8 \equiv 9 \bmod 13$

$6 \cdot 9 \equiv 2 \bmod 13$

$6 \cdot 10 \equiv 8 \bmod 13$

$6 \cdot 11 \equiv 1 \bmod 13$

$6 \cdot 12 \equiv 7 \bmod 13$

Tuesday, February 25th 2025

THEOREM (FLT): For any $n \geq 3$, $x^n + y^n = z^n$ doesn't have any solutions $x, y, z \in \mathbb{Z}$, $x, y, z \geq 1$

EULER'S FUNCTION: $\varphi(n) = \#\{m \in \mathbb{Z} : 1 \leq m \leq n, \gcd(m, n) = 1\}$

↳ Ex: $\varphi(10) = \#\{m \in \mathbb{Z} : 1 \leq m \leq 10, \gcd(m, 10) = 1\} = \#\{1, 3, 7, 9\} = 4$

Ex: p prime, then $\varphi(p) = p - 1$

THEOREM (EULER): Let n be a positive integer and let a be an integer such that $\gcd(a, n) = 1$.
Then $a^{\varphi(n)} \equiv 1 \bmod n$

Proof: Let n be a positive integer, and let a be an integer s.t. $\gcd(a, n) = 1$.
Let $1 \leq b_1 < b_2 < \ldots < b_{\varphi(n)} \leq n$ where $\gcd(b_1, n) = \gcd(b_2, n) = \ldots = \gcd(b_{\varphi(n)}, n) = 1$
Consider congruences:

$$\begin{cases} ab_1 \equiv r_1 \bmod n \\ ab_2 \equiv r_2 \bmod n \\ \vdots \\ ab_{\varphi(n)} \equiv r_{\varphi(n)} \bmod n \end{cases}$$

$a^{\varphi(n)-1} b_1 b_2 \cdots b_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \bmod n$

$a^{\varphi(n)-1} \equiv 1 \bmod n$ □

Proof of $\gcd(r_j, n) = 1$:
Assume $\gcd(r_j, n) > 1$ where $j \in \{1, 2, \ldots, \varphi(n)\}$. Let p be prime divisor of (r_j, n).
$p \mid r_j$ and $p \mid n$. Recall $ab_j \equiv r_j \bmod n \Rightarrow ab_j - r_j = kn$ where $k \in \mathbb{Z}$.
By assumption, $p \mid r_j$ and $p \mid a$, thus implies $p \mid a \vee p \mid b_j$. $p \mid a$ is false, and $p \mid b_j$ is also false as $\gcd(a, n) = \gcd(b_j, n) = 1$. Thus by contradiction, $\gcd(r_j, n) = 1$.
So, $r_j \in \{b_1, b_2, \ldots, b_{\varphi(n)}\}$.

Assume $r_i = r_j$ and $i, j \in \{1, 2, \ldots \varphi(n)\}$. Then $r_i \equiv ab_i \bmod n$
By contradiction, $b_i \neq b_j$ for $i, j \in \{1, 2, \ldots \varphi(n)\}$. $r_j = ab_j \bmod n$

only possible if $i = j$
$b_i = b_j$
so $ab_i \equiv ab_j \bmod n \rightarrow b_i \equiv b_j \bmod n$

$$\{b_1, b_2, \ldots b_{\varphi(n)}\} = \{r_1, r_2, \ldots r_{\varphi(n)}\}$$

Ex: $n = 10$, $a = 7$

$\varphi(10) = 4$

By Euler's theorem, as $\gcd(7,10)$, then $7^4 \equiv 1 \bmod 10$

For each positive integer n,

$$\varphi(n) = n \prod_{\substack{p \text{ prime} \\ p \text{ div. } n}} \left(1 - \frac{1}{p}\right)$$

Problem: Find last 2 decimal digits of 77^{961}.

$77^{961} \equiv X \bmod 100$

$\gcd(77, 100) = 1$, then Euler's

Thursday, February 27th 2025

Ex: $2023^{2002} \equiv X \bmod 1000$

$2023^{2002} \equiv 23^{2002} \bmod 1000$

By Euler's Theorem, $23^{\varphi(1000)} \equiv 1 \bmod 1000$

$$\varphi(1000) = 1000 \prod_{\substack{p \text{ prime} \\ p \text{ div. } 1000}} \left(1 - \frac{1}{p}\right) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$

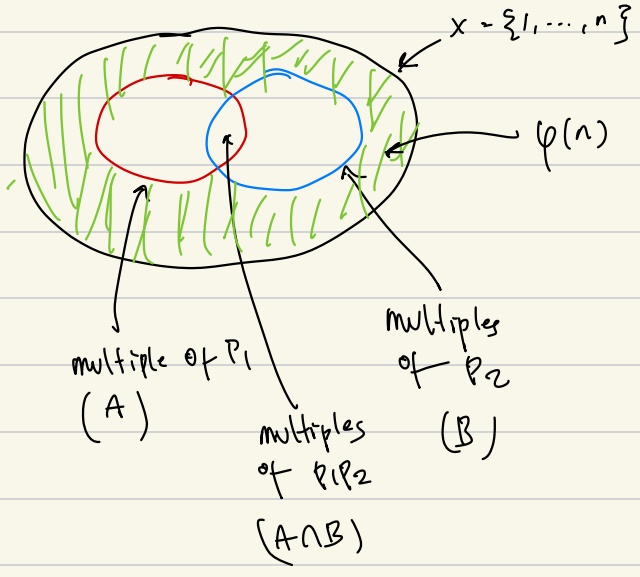
$$= 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$$

Thus, $23^{400} \equiv 1 \bmod 1000$

$23^{2002} \bmod 1000 \equiv (1)^5 \cdot 23^2 \bmod 1000 \equiv 23^2 \bmod 1000 \equiv \boxed{529} \bmod 1000$

INCLUSION-EXCLUSION PRINCIPLE

Let $n = p_1^{a_1} p_2^{a_2}$ where p_1, p_2 prime.



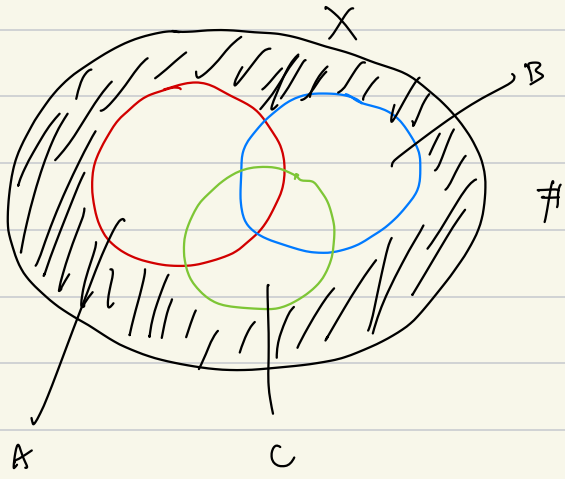
By definition, $\varphi(n) = \#\left(X \setminus (A \cup B)\right)$

$$\varphi(n) = \#(X) - \#(A) - \#(B) + \#(A \cap B)$$

$$= n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2}$$

$$= n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} + \frac{1}{p_1 p_2}\right)$$

$$\boxed{\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)}$$



For $n = p_1^{a_1} p_2^{a_2} p_3^{a_3}$

$$\#(X \setminus (A \cup B \cup C)) = \#(X) - \#(A) - \#(B) - \#(C) + \#(A \cap B) + \#(A \cap C) + \#(B \cap C) - \#(A \cap B \cap C)$$

$$= n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \frac{n}{p_2 p_3} - \frac{n}{p_1 p_2 p_3}$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)$$

ARITHMETIC FUNCTIONS

DEF: An arithmetic function is a function whose domain is the set of positive integers ($\mathbb{N}$)

DEF: An arithmetic function f is multiplicative if $f(nm) = f(n)f(m)$ whenever $\gcd(n,m) = 1$. Function f is completely multiplicative if $f(nm) = f(n)f(m)$ $\forall n, m \in \mathbb{N}$

THEOREM: Euler phi-function is multiplicative

THEOREM: For any $n \in \mathbb{N}$, $\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$

↳ Proof: inclusion-exclusion principle

Proof that $\varphi(n)$ is multiplicative: Let $n, m \in \mathbb{N}$ s.t. $\gcd(n,m) = 1$. Say, $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and as $\gcd(m,n) = 1$, let $m = q_1^{b_1} q_2^{b_2} \dots q_r^{b_r}$ where $p_1, p_2, \dots, p_k, q_1, q_2, \dots q_r$ distinct primes.

Then, $nm = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} q_1^{b_1} q_2^{b_2} \dots q_r^{b_r}$. By the theorem after that,

$$\varphi(nm) = nm\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \dots \left(1 - \frac{1}{q_r}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) m\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \dots \left(1 - \frac{1}{q_r}\right)$$

$$= \varphi(n)\,\varphi(m)$$

Thus, we conclude that $\varphi(nm) = \varphi(n)\varphi(m)$ when $\gcd(n,m) = 1$ □

Claim: $\varphi(n)$ is completely multiplicative

Recall $\varphi(10)=4$, $\varphi(100)=40$, $\varphi(1000)=400$

Let $n=10$, $m=100$. Then $\varphi(1000)=400 \neq \varphi(10)\varphi(100)$] DISPROVEN BY COUNTEREXAMPLE

THEOREM (GAUSS): For any positive integers n, we have $\sum_{d|n} \varphi(d) = n$

Ex: $n=20$

By Gauss' theorem, $\sum_{d|20} \varphi(d) = 20$

$d \in \{1,2,4,5,10,20\} \longrightarrow 20 = \varphi(1)+\varphi(2)+\varphi(4)+\varphi(5)+\varphi(10)+\varphi(20)$

$= 1+1+2+4+4+8 = 20$

Def: Let $n \in \mathbb{Z}$, $n \geq 1$. The number of positive divisors function, denoted $\nu(n)$, is the function defined by $\nu(n) = \#\{d \in \mathbb{Z} : d \geq 1, d|n\}$ or $\nu(n) = |\{d \in \mathbb{Z} : d \geq 1, d|n\}|$

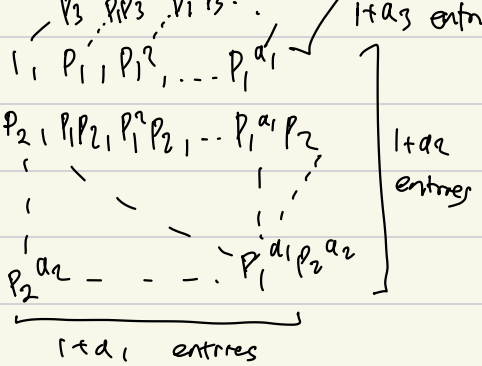
THEOREM: $\nu(n)$ is multiplicative

THEOREM: Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where p_i prime for $1 \leq i \leq k$. Then, $\nu(n) = \prod_{i=1}^{k} (1+a_i)$

↳ Ex: $n = 100 = 2^2 \cdot 5^2$ $\nu(n) = 3 \cdot 3 = 9$

Ex: $n = 1000 = 2^3 \cdot 5^3$ $\nu(n) = 4 \cdot 4 = 16$

IDEA: 2 prime factors $p_1^{a_1} p_2^{a_2}$ and 3 prime factors $p_1^{a_1} p_2^{a_2} p_3^{a_3}$



Imagine higher dimension cuboid with vertices $d_i = 1+a_i$. Then $V = \prod_{i=1}^{k} d_i$

$V_2 = (1+a_1)(1+a_2)$

$V_3 = (1+a_1)(1+a_2)(1+a_3)$

Tuesday, March 4th 2025

$(p-1)! \equiv -1 \bmod p$ $a \in \mathbb{Z}$, p prime (Wilson's theorem)

$a^{p-1} \equiv 1 \bmod p$ $a \in \mathbb{Z}$, p prime, $\gcd(a,p)=1$ (Fermat's little theorem)

$a^{\varphi(m)} \equiv 1 \bmod m$ $a,m \in \mathbb{Z}$, $\gcd(a,m)=1$ (Euler's theorem)

THEOREM: The arithmetic functions $\varphi(n)$, $\nu(n)$, $\sigma(n)$, $\mu(n)$ are multiplicative, none completely

THEOREM: The sum of divisors denoted by $\sigma(n)$ for $n = p_1^{a_1} \cdots p_k^{a_k}$ where p_i prime for $1 \le i \le k$, is defined by $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1}-1}{p_i - 1} = \prod_{i=1}^{k} \sum_{j=0}^{k} p_i^j$

$$\begin{pmatrix} 1 & p_1 & \cdots & p_1^{a_1} \\ p_2 & \ddots & & 1 \\ \vdots & & \ddots & \vdots \\ p_2^{a_2} & \cdots & \cdots & p_1^{a_1} p_2^{a_2} \end{pmatrix} = \sum_{i=0}^{a_1} p_1^i + p_2 \sum_{i=0}^{a_1} p_1^i + p_2^2 \sum_{i=0}^{a_1} p_1^i + \cdots$$

$$= \left(\sum_{i=0}^{a_2} p_2^i \right)\left(\sum_{i=0}^{a_1} p_1^i \right) = \frac{1-p_2^{a_2+1}}{1-p_2} \cdot \frac{1-p_1^{a_1+1}}{1-p_1}$$

Ex: $n=100$, $\sigma(100) = \frac{2^3-1}{1} \cdot \frac{5^3-1}{4} = 7 \cdot \frac{124}{4} = 7 \cdot 31 = 217$

Ex: Find $1 \le n \le 100$ where $\nu(n)$ is maximum

$$\nu(n) = \prod_{i=1}^{k} (1+a_i)$$

Ex: $2^{3000} \cdot 5^{3000}$ or $2^{80} \cdot 5^{80} \cdot 3^{180}$ $\nu(n)$?

$(3001)(3001)$ or $(91)(91)(181)$ 1000^{1000} larger

near $9{,}000{,}000$ near 8100 1466100

Ex: Find $1 \le n \le 100$ where $\sigma(n)$ is maximum

96: $\sigma(96) = (2^6-1) \cdot \frac{3^2-1}{2} = 4(63) = 252$

90: $\sigma(90) = 3(13)(6) = 3(78) = 234$

Thursday, March 6th 2025

DEF: For $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, the Möbius function $\mu(n)$ is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if at least one of } a_1, \ldots a_k \geq 2 \\ (-1)^k & \text{if } a_1 = a_2 = \cdots = a_k = 1 \end{cases}$$

THEOREM: Let $n \in \mathbb{N}$. Then $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \geq 2 \end{cases}$

Ex: $\sum_{d \mid 20} \mu(d) = \mu(1) + \mu(2) + \mu(4) + \mu(5) + \mu(10) + \mu(20)$

$= 1 + -1 + 0 + -1 + 1 + 0 = 0$

Ex: Find smallest $n \geq 47$ such that $\mu(n) = 1$

$7(9)$, $5(11)$, $23(2)$ $3(17)$

63 55 46 51

Ex: $\sigma(400)$

$400 = 2^2 \cdot 100 = 2^2 \cdot (2 \cdot 5)^2 = 2^4 \cdot 5^2$

$\sigma(400) = (2^5 - 1)\left(\frac{5^3 - 1}{4}\right) = 31 \cdot 31 = 930 + 31 = 961$

Tuesday, March 11th 2025

PERFECT NUMBERS

DEF: A perfect number $n \in \mathbb{N}$ is the sum of $d \in \mathbb{N}$ where $d \mid n$ and $d < n$, or $\sigma(n) = 2n$

THEOREM: If p prime for which $2^p - 1$ is also prime, then the number

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

is a perfect number.

Proof: Let p prime such that $2^p - 1$ prime. Denote $2^p - 1$ by q. Then, $n = 2^{p-1}(2^p - 1)$ is equal to $2^{p-1}(q)$. Divisors of n are $1, 2, 2^2, \dots 2^{p-1}, q, 2q, 2^2q, \dots, 2^{p-2}q$.
Then, sum $= 1 + 2 + \dots + 2^{p-1} + q(1 + 2 + \dots + 2^{p-2}) = 2^p - 1 + q \cdot 2^{p-1} - q = 2^{p-1} \cdot q = n$ ∎

OPEN PROBLEM: ARE THERE ANY ODD PERFECT NUMBERS?
UNSOLVED PROB.: ARE THERE INFINITELY MANY EVEN PERFECT NUMBERS?

THEOREM (EULER): Let n be an even perfect number. Then there is a prime p such that $2^p - 1$ prime and $n = 2^{p-1}(2^p - 1)$

Proof: Let n be an even perfect number. Then, $n = 2^a p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. By our assumption, $a \geq 1$.
As n perfect number, it follows that $\sigma(n) = 2n$. By the formula of $\sigma(n)$:
$\sigma(n) = (2^{a+1} - 1)(1 + p_1 + p_1^2 + \dots + p_1^{a_1}) \dots (1 + p_k + \dots + p_k^{a_k}) = 2^{a+1} p_1^{a_1} \dots p_k^{a_k}$
Let p be a prime factor of $2^{a+1} - 1$. Then $p \mid$ LHS, so $p \mid$ RHS, thus $p \mid 2^{a+1} p_1^{a_1} \dots p_k^{a_k}$.
$p \neq 2$ so p is equal to p_j for some $j \in \{1, 2, \dots, k\}$.

Thursday, March 13th 2025

SUMS OF 2 SQUARES

THEOREM: Let p be an odd prime. Then, p can be written as the sums of two squares of integers if and only if $p \equiv 1 \bmod 4$.

Ex: $5, 13, 17, 29, \ldots$
$\quad\;\; \| \quad\;\; \|$
$\quad 2^2+1^2 \quad 2^2+3^2 \quad \cdots$

Proof: Let p be prime such that $p \equiv 3 \bmod 4$. Assume that there are 2 integers a and b such that $a^2+b^2 = p$. a could be congruent to either $0, 1, 2, 3 \bmod 4$. Then, a^2 is congruent to 0 or $1 \bmod 4$. b^2 for the same reason is also congruent to either 0 or $1 \bmod 4$. Adding congruence, a^2+b^2 never congruent to $3 \bmod 4$. So, $a^2+b^2 \neq p$ if $p \equiv 3 \bmod 4$.

Proof: Let p be a prime number s.t. $p \equiv 1 \bmod 4$. By Wilson's theorem, $(p-1)! \equiv -1 \bmod p$. Then, it follows:

$$p-1 \equiv -1 \bmod p$$
$$p-2 \equiv -2 \bmod p$$
$$\vdots$$
$$p-\tfrac{p-1}{2} \equiv -\tfrac{p-1}{2} \bmod p$$

$$\tfrac{p-1}{2} \equiv \tfrac{p-1}{2} \bmod p$$
$$\vdots$$
$$2 \equiv 2 \bmod p$$
$$1 \equiv 1 \bmod p$$

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \tfrac{p-1}{2} \cdot \left(-1 \cdot -2 \cdot -3 \cdot \ldots = \left(\tfrac{p-1}{2}\right)\right)$$
$$\equiv (-1)^{p-1/2} \cdot \left(1 \cdot 2 \cdot \ldots \left(\tfrac{p-1}{2}\right)\right)^2 \bmod p$$

Let $m = \left(\tfrac{p-1}{2}\right)!$, then $(p-1)! \equiv (-1)^{\frac{p-1}{2}} m^2 \bmod p$

Here, $p \equiv 1 \bmod 4$, so $(-1)^{p-1/2} = 1$

Hence, $m^2 \equiv (p-1)! \equiv -1 \bmod p$

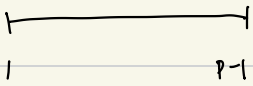
In conclusion, $M^2+1 \equiv 0 \bmod p$

Claim: There are integers u, v such that $1 \le u \le \sqrt{p}$, $-\sqrt{p} < v < \sqrt{p}$, $um \equiv v \bmod p$.

Idea: Take numbers $1, 2, \dots [\sqrt{p}]$. Multiply each by m, reduce mod p

$$m = pq_1 + r_1$$
$$2m = pq_2 + r_2$$
$$3m = pq_3 + r_3$$
$$\vdots$$
$$\underbrace{[\sqrt{p}]}_{k} m = pq_{[\sqrt{p}]} + \underbrace{r_{[\sqrt{p}]}}_{k}$$
$$km = pq_k + r_k$$

$r_1, r_2, \dots, r_k \in \{1, 2, \dots, p-1\}$



$|r_i - r_j| < \sqrt{p}$ $\quad 1 \le u \le \sqrt{p}$ and $|v| = |r_j - r_i| = |r_i - r_j| < \sqrt{p}$

Assume $i < j$, let $u = j - i$ and $v = r_j - r_i$

$$um = (j-i)m = jm - im = p(q_j - q_i) + (r_j - r_i) \Rightarrow \boxed{um \equiv v \bmod p}$$

What we have: $m = \left(\frac{p-1}{2}\right)!$, $m^2 + 1 \equiv 0 \bmod p$

Consider the number $u^2 + v^2$. On one hand, we have $0 < u^2 + v^2 < p + p$

$$0 < u^2 + v^2 < 2p$$

On the other hand, we have $um \equiv v \bmod p \Rightarrow u^2 m^2 \equiv v^2 \bmod p$

$$m^2 + 1 \equiv 0 \bmod p$$
$$u^2 m^2 + u^2 \equiv 0 \bmod p$$
$$u^2 + v^2 \equiv 0 \bmod p \Rightarrow$$ we have sum of 2 squares multiple of p

It follows $u^2 + v^2 = p$

$u^2 + v^2 = kp$ where $0 < u^2 + v^2 < 2p$

Thus k only 1.

Ex: $p = 13$

$13 = u^2 + v^2$

Let $m = \left(\frac{p-1}{2}\right)! = \left(\frac{12}{2}\right)! = 6! = 720$

Claim, $m^2 + 1 \equiv 0 \bmod p$. $m \equiv 5 \bmod 13$, $m^2 \equiv -1 \bmod 13$, $m^2 + 1 \equiv 0 \bmod 13$.

$m = 5$ now, $5^2 + 1 = 26$

Take numbers $1 \le u < \sqrt{p}$ and $|v| < \sqrt{p}$. $k = [\sqrt{13}] = 3$. Then, $u = 1$ or 2 or 3.

$u = j - i = 3 - 1 = 2$

$v = r_j - r_i = -3$

$um \equiv v \bmod p$

$10 \equiv -3 \bmod 13$

$13 \equiv 0 \bmod 13$ ✓

$\Longrightarrow$

$0 < u^2 + v^2 < 26$

$u^2 + v^2 \equiv 0 \bmod 13$

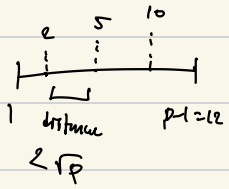
$u^2 + v^2 = p$

$\boxed{2^2 + 3^2 = 13}$

$1 \cdot 5 \equiv 5 \bmod 13$

$2 \cdot 5 \equiv 10 \bmod 13$

$3 \cdot 5 \equiv 2 \bmod 13$



THEOREM: Let $n > 1$. Then n is not a sum of two squares if and only if there is prime $p \equiv 3 \bmod 4$ with an odd exponent in the prime factorization of n

Ex: $n = 7^3 5^2$ is not a sum of two squares as exponent of 7 is 3 (odd)

Ex: $n = 7^2 \cdot 5^3 \cdot 11^2$ is a sum of two squares with the same argument

$n = 5(7 \cdot 5 \cdot 11)^2 = (2 \cdot 7 \cdot 5 \cdot 11)^2 + (7 \cdot 5 \cdot 11)^2$

Ex: $n = 7^2 5^3 11^2 13^{21}$ is a sum of two squares with the same reasoning

$n = 7^2 5^2 11^2 13^{20} \cdot (5 \cdot 13) = 7^2 \cdot 5^2 \cdot 11^2 \cdot 13^{20}(8^2 + 1^2)$

$= (8 \cdot 7 \cdot 5 \cdot 11 \cdot 13^{10})^2 + (7 \cdot 5 \cdot 11 \cdot 13^{10})^2$

Check profs video on quadratic residues

Tuesday, March 25th 2025

QUADRATIC RESIDUES & LEGENDRE SYMBOL

$x^2 \equiv a \mod p$ (quadratic congruence)

Always exist a solution?

Look at base 7:

Palindrome!

$0^2 \equiv 0 \mod 7$
$1^2 \equiv 1 \mod 7$
$2^2 \equiv 4 \mod 7$
$3^2 \equiv 2 \mod 7$
$4^2 \equiv 2 \mod 7$
$5^2 \equiv 4 \mod 7$
$6^2 \equiv 1 \mod 7$
$7^2 \equiv 0 \mod 7$

THEOREM: For any prime p, exists $\frac{p-1}{2}$ possible quadratic residues and $\frac{p-1}{2}$ quadratic non residues on $x^2 \equiv a \mod p$.

Ex: Quadratic residues of 19

$0^2 \equiv 0 \mod 19$
$1^2 \equiv 1 \mod 19$
$2^2 \equiv 4 \mod 19$
$3^2 \equiv 9 \mod 19$
$4^2 \equiv 16 \mod 19$
$5^2 \equiv 6 \mod 19$
$6^2 \equiv 17 \mod 19$
$7^2 \equiv 11 \mod 19$
$8^2 \equiv 7 \mod 19$
$9^2 \equiv 5 \mod 19$

DEF (LEGENDRE SYM): $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if Q.R.} \\ -1 & \text{if Q.N.R} \end{cases}$

THEOREM (EULER'S CRITERION): $\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$

Ex: $p=11$, test $\left(\frac{5}{11}\right) \Rightarrow 5^5 \mod 11 \equiv 3125 \mod 11 \equiv 1 \mod 11$ Quadratic Residue!

$p=11$, test $\left(\frac{2}{11}\right) \Rightarrow 2^5 \mod 11 \equiv 32 \mod 11 \equiv -1 \mod 11$ NON Quadratic Residue!

Thursday, April 3rd 2025

THEOREM: Odd prime p sum of two squares iff $p \equiv 1 \bmod 4$

THEOREM: A positive integer n sum of two squares iff every prime $p \equiv 3 \bmod 4$ appears in the prime factorization of n with an even exponent

Ex: $n = 13 \cdot 17^2 \cdot 19^7 \cdot 23^4$

$13 \equiv 1 \bmod 4 \to 1$

$17 \equiv 1 \bmod 4 \to 2$

$19 \equiv 3 \bmod 4 \to 7$ NOT EVEN! NOT SOTS!

$23 \equiv 3 \bmod 4 \to 4$

Ex: $n = 13 \cdot 17^7 \cdot 19^2 \cdot 23^4$

IS SUM OF 2 SQUARES

BECAUSE BOTH $19 \equiv 3 \bmod 4$ & $23 \equiv \bmod 4$

HAS EVEN EXPONENTS

$n = (13 \cdot 17)(17^6 \cdot 19^2 \cdot 23^4)$

$= \underbrace{(2^2+3^2)(4^2+1^2)(17^6 \cdot 19^2 \cdot 23^4)}_{\text{SOTS!}}$

DEF (BINOMIAL COEFF.): $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

QUADRATIC CONGRUENCES

$Ax^2 + Bx + C \equiv 0 \bmod p$ where A, B, C, p given integers $(A \not\equiv 0 \bmod p)$

Quadratic equation: $Ax^2 + Bx + C = 0 \quad (A \neq 0)$

↳ $x_{1,2} = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$

Ex: $x^2 - 1 \equiv 0 \bmod 15$

Has > 2 congruent solutions

Tuesday, April 8th 2025

Quadratic congruences mod prime p: Given $A, B, C, p \in \mathbb{Z}$, p prime, is there $x \in \mathbb{Z}$ s.t. $Ax^2 + Bx + C \equiv 0 \bmod p$ where $p \nmid A$?

Ex: Non prime modulo ($105 = 3 \cdot 5 \cdot 7$)

$x^2 - 1 \equiv 0 \bmod 105$

$\downarrow$

$x^2 - 1 \equiv 0 \bmod 3 \quad \Rightarrow \quad x \equiv \pm 1 \bmod 3$

$x^2 - 1 \equiv 0 \bmod 5 \quad \Rightarrow \quad x \equiv \pm 1 \bmod 5$

$x^2 - 1 \equiv 0 \bmod 7 \quad \Rightarrow \quad x \equiv \pm 1 \bmod 7$

Prod.

Ex: Solve $3x^2 + 7x + 3 \equiv 0 \bmod 13$

Inverse of 6 mod 13 is 11

$$x_{1/2} \equiv \frac{-7 \pm \sqrt{49 - 36}}{6} \bmod 13$$

$$\equiv 11(-7 \pm 6) \bmod 13$$

$$\equiv -77 \bmod 13 \equiv 1 \bmod 13$$

METHOD: CONGRUENCE ANALOG $Ax^2 + Bx + C \equiv 0 \bmod p$ s.t. $p \nmid A$, p prime

$4A^2x^2 + 4ABx + 4AC \equiv 0 \bmod p$

$4A^2x^2 + 4ABx + B^2 - B^2 + 4AC \equiv 0 \bmod p$

$(2Ax + B)^2 \equiv B^2 - 4AC \bmod p$

If $\exists m \in \mathbb{Z}$ s.t. $B^2 - 4AC \equiv m^2 \bmod p$, then

$(2Ax + B)^2 \equiv B^2 - 4AC \bmod p \equiv m^2 \bmod p$

$(2Ax + B + m)(2Ax + B - m) \equiv 0 \bmod p$

$\Rightarrow p \mid 2Ax + B + m$ or $p \mid 2Ax + B - m$

$p \mid 2Ax + B + m \iff 2Ax \equiv -B - m \bmod p$

OR

$p \mid 2Ax + B - m \iff 2Ax \equiv -B + m \bmod p$

$\Rightarrow 2Ax \equiv -B \pm m \bmod p$

Denote V the inverse of $2A \bmod p$

$\Rightarrow \boxed{x \equiv V(-B \pm m) \bmod p}$

THEOREM: Let p be an odd prime and $A, B, C \in \mathbb{Z}$ s.t. $p \nmid A$. Then the congruence $Ax^2 + Bx + C \equiv 0 \bmod p$ has solutions $x \in \mathbb{Z}$ iff $B^2 - 4AC$ is congruent to a square mod p.

DEF: Let p be an odd prime and let $a \in \mathbb{Z}$ s.t. $p \nmid a$. If $\exists x \in \mathbb{Z}$ s.t. $x^2 \equiv a \bmod p$, a is said to be a quadratic residue mod p. If $\nexists x \in \mathbb{Z}$ s.t. $x^2 \equiv a \bmod p$, a is said to be a quadratic non residue mod p.

DEF: Legendre symbol defined for p odd prime, $a \in \mathbb{Z}$, $p \nmid a$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is quadratic residue mod } p \\ -1 & \text{if } a \text{ is quadratic non residue mod } p \end{cases}$$

Ex: $\left(\frac{18}{13}\right) = \left(\frac{5}{13}\right) = -1$

Thursday, April 10th 2025

Is $10!$ a sum of 2 squares?

Is 777 a sum of 2 squares?

Properties of Legendre symbol: Condition: p prime s.t. $p > 2$, $a \not\equiv 0 \bmod n$, $b \not\equiv 0 \bmod n$

- $\left(\frac{a^2}{p}\right) = 1$
- If $a \equiv b \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\forall a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

THEOREM: Let p, q be distinct odd primes. Then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if at least one of } p, q \text{ is congruent } 1 \bmod 4 \\ -\left(\frac{q}{p}\right) & \text{if both } p, q \text{ is congruent } 3 \bmod 4 \end{cases}$$

Thursday, April 17th 2025

THEOREM: Let p be an odd prime and let $a, b \in \mathbb{Z}$ s.t. $p \nmid a$ and $p \nmid a$.
Then, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof:

Conditions:
- If a is QR and b is QR, then ab is QR (i)
- If exactly one of a or b is QN, then ab is QN (ii)
- If a is QN and b is QN, then ab is QR (iii)

(i.) $\exists m, n \in \mathbb{Z}$ s.t. $a \equiv m^2 \bmod p$ and $b \equiv n^2 \bmod p$. Then $ab \equiv (mn)^2 \bmod p$.
$mn \in \mathbb{Z}$, therefore ab QR if a and b QR

Ex: Find all the Pythagorean triples x, y, z s.t. $z = 65$ $65 = 5 \cdot 13$
$65 = a^2 + b^2 = 8^2 + 1^2$
$x = 64 - 1 = 63$
$y = 2 \cdot 8 \cdot 1 = 16$
$(16, 63, 65)$ and $(39, 52, 65)$ and $(25, 60, 65)$

THEOREM: Let p be an odd prime. There are exactly $\frac{p-1}{2}$ QR and $\frac{p-1}{2}$ QN mod p in the set $\{1, 2, \ldots, p-1\}$

Proof. The numbers $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are incongruent mod p. Any square is congruent to one in the above list mod p.

Assume $c, d \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ s.t. $c \neq d$ and $c^2 \equiv d^2 \bmod p$. Then $c^2 - d^2 \equiv 0 \bmod p$ which implies $p \mid c^2 - d^2$ which also implies $p \mid (c-d)(c+d)$. It follows that $p \mid c-d$ or $p \mid c+d$. But, $c-d$ and $c+d$ can't be a multiple of p as $\max(c+d) = p-1$. Thus proven the numbers $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ is incongruent mod p.

Consider any square m^2 where $m \in \mathbb{Z}$ and $m \not\equiv 0 \bmod p$. Then $m \equiv \ell \bmod p$ for some $\ell \in \left\{1, 2, \ldots, \frac{p-1}{2}, \ldots, p-1\right\}$.
- If $\ell \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, done.
- If $\ell \in \left\{\frac{p+1}{2}, \ldots, p-1\right\}$, then denote $r = p - \ell$. So, $r \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$.
$r^2 = (p-\ell)^2 = p^2 - 2p\ell + \ell^2 \Longrightarrow r^2 \equiv \ell^2 \equiv m^2 \bmod p$.

Tuesday, April 22nd 2025

Ex: Find two consecutive positive integers larger than 1000 such that one of them is a square and the other 2 times a square.

$x^2 - 2y^2 = 1$

Fundamental solution: $x = 3, y = 2 \Rightarrow 3^2 - 2 \cdot 2^2 = 1$

Recall: $(A-B)(A+B) = A^2 - B^2$

$3^2 - 2 \cdot 2^2 = (3+2\sqrt{2})(3-2\sqrt{2}) = 1 \Rightarrow (3+2\sqrt{2})^2 (3-2\sqrt{2})^2 = 1$

$\Rightarrow (17+12\sqrt{2})(17-12\sqrt{2}) = 1 = 17^2 - 2 \cdot 12^2$

$(17+12\sqrt{2})^2 (17-12\sqrt{2})^2 = 1 \Rightarrow (289 + 408\sqrt{2} + 288)(289 - 408\sqrt{2} + 288) = 1$

$\Rightarrow (577 + 408\sqrt{2})(577 - 408\sqrt{2}) = 1$

$577^2 - 2 \cdot 408^2 = 1$

A B

Solution: (332928, 332929)

Ex: $x^2 - 11y^2 = 1$ $\quad (10 - \sqrt{11} \cdot 3)^2 (10 + \sqrt{11}\, 3)^2 = 1$

$100 - 99 = 1$ $\quad (100 + 99 - 60\sqrt{11})(100 + 99 + 60\sqrt{11}) = 1$

$10^2 - 11 \cdot 3^2 = 1$ $\quad (199 - 60\sqrt{11})(199 + 60\sqrt{11}) = 199^2 - 11 \cdot 60^2 = 1$

39601 39600

Solution: (39600, 39601)

THEOREM: All primitive pythagorean triples are given by $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$ where $a, b \in \mathbb{N}$ s.t. $a > b \geq 1$, $\gcd(a,b) = 1$, and exactly one of a and b are even

Ex: Find all right triangles with integer sides such that the largest side has length 55

$z = 55 = d(a^2 + b^2) = 5 \cdot 11 \Rightarrow a^2 + b^2 = 5 \Rightarrow a = 2, b = 1$

55 not 5075, thus we have $d = 11$.

$x = 33, y = 44, z = 55$

Ex: Is the congruence $x^2 \equiv 11 \bmod 97$ solvable?

$\left(\frac{11}{97}\right) = \left(\frac{97}{11}\right) = -\left(\frac{2}{11}\right) = -1 \cdot -1 = 1 \Rightarrow$ As 11 is QR of 97, then $x^2 \equiv 11 \bmod 97$ solvab.

$97 \equiv 1 \bmod 4$ $\quad 97 \equiv -2 \bmod 11$ $\quad \left(\frac{2}{11}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{120}{8}} = (-1)^{15} = -1$

Tuesday, April 29th 2025

THEOREM: All pythagorean triples are of the form (dx, dy, dz) where $d \geq 1$ and

$x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$ where $a, b \in \mathbb{N}$ s.t. $a > b \geq 1$, $\gcd(a, b) = 1$,

and $a + b \equiv 1 \bmod 2$.

Proof. Let (A, B, C) be a pythagorean triple. If two of A, B, C are multiples of a prime p_1, then it follows that the third one is also a multiple of p_1. Denote $A_1 = \frac{A}{p_1}$, $B_1 = \frac{B}{p_1}$, $C_1 = \frac{C}{p_1}$. Then $A_1^2 + B_1^2 = C_1^2$. Continue the reasoning, denote $A_2 = \frac{A_1}{p_2}$, $B_2 = \frac{B_1}{p_2}$, $C_2 = \frac{C_1}{p_2}$ where p_2 prime. Continue until we get A_n, B_n, C_n such that $\gcd(A_n, B_n) = 1$, $\gcd(A_n, C_n) = 1$, $\gcd(B_n, C_n) = 1$, and $A_n^2 + B_n^2 = C_n^2$. Re-denote the variables as $A_n = x$, $B_n = y$, $C_n = z$, thus we get $x^2 + y^2 = z^2$ where x, y, z pairwise relatively prime. Also denote $d = \frac{A}{x} = \frac{B}{y} = \frac{C}{z}$. Thus the triple $(A, B, C) = (dx, dy, dz)$ where $d \geq 1$. First part done.

Claim: If $x, y, z \geq 1$, x, y, z pairwise relatively prime, $x^2 + y^2 = z^2$, then z is odd and exactly one of x, y is even

Proof* Assume z is even. Then $z^2 \equiv 0 \bmod 4$. It follows that $x^2 + y^2 \equiv 0 \bmod 4$. For any $n \in \mathbb{Z}$, we require $n^2 \equiv 0$ or $1 \bmod 4$. For $z^2 \equiv x^2 + y^2 \bmod 4 \equiv 0 \bmod 4$, we require $x^2 \equiv 0 \bmod 4$ and $y^2 \equiv 0 \bmod 4$. This implies x is even and y is even. This contradicts the condition $\gcd(x, y) = 1$. By contradiction, the claim true. □

To make a choice, let y be the even one (valid by symmetry).

$x^2 + y^2 = z^2$

$y^2 = z^2 - x^2$

$\left(\frac{y}{2}\right)^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right)$ $\quad (2 \mid y \Rightarrow 4 \mid y^2) \wedge (2 \mid (z-x) \wedge 2 \mid (z+x))$ (odd − odd, odd + odd)

$\in \mathbb{Z}$ $\in \mathbb{Z}$

Claim: $\gcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$

Proof* Assume that $\gcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right) > 1$. Let p be a prime factor of $\gcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right)$. Then $p \mid \frac{z-x}{2}$ and $p \mid \frac{z+x}{2}$. It follows that $p \mid z$ and $p \mid x$ from the sum and difference. This is a contradiction as $p \mid x$, $p \mid z \Rightarrow \gcd(x, z) = p > 1$. Thus by contradiction, our claim is true. □

If $\gcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$ and $\left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right)$ is a square, then $\frac{z-x}{2}$ and $\frac{z+x}{2}$ square.

Denote $\frac{z-x}{2} = a^2$ and $\frac{z+x}{2} = b^2$. $\frac{z+x}{2} + \frac{z-x}{2} = a^2 + b^2 = z$, $\frac{z+x}{2} - \frac{z-x}{2} = a^2 - b^2 = x$, and

$\left(\frac{y}{2}\right)^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right) = a^2 b^2 \Rightarrow y = 2ab$

If z odd, then $a^2 + b^2$ odd, thus exactly one of a, b is odd

PROVEN

CONTINUED FRACTIONS

Let $\alpha \in \mathbb{R}$ be given. Then write α as $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$ where $a_0 = [\alpha]$, $a_1, a_2, \dots \geq 1$

Take $\alpha = \sqrt{29}$. We know that $\alpha \notin \mathbb{Q}$ therefore the continued fraction goes indefinitely. $\alpha = \sqrt{29}$, close to 25, $\alpha = 5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{10 + \dots}}}}}}}}}}$ $\Rightarrow$ has pattern "2-1-1-2-10"

Claim: The continued fraction above to $\sqrt{29}$.

Proof Let $\beta = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \dots}}}$. Then $\alpha = 5 + \beta$. Notice that $\beta = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{10 + \beta}}}}$. Solve to get β.

Get $\beta = \dfrac{5\beta + 52}{13\beta + 135}$. Follows, $13\beta^2 + 135\beta = 5\beta + 52$

$$\Downarrow$$

$$13\beta^2 + 130\beta - 52 = 0$$

$$\beta^2 + 10\beta - 4 = 0$$

$$\beta_{1,2} = \frac{-10 \pm \sqrt{100 + 16}}{2} \overset{\text{pos}}{=} -5 + \sqrt{\frac{116}{4}} = \boxed{-5 + \sqrt{29}} \quad \square$$

true!

Thursday, May 1st 2025

Consider the rational number $\frac{117}{31}$.

$117 = 3 \cdot 31 + 24 \Rightarrow \frac{117}{31} = 3 + \frac{24}{31} = 3 + \frac{1}{31/24}$

$31 = 1 \cdot 24 + 7 \Rightarrow 31/24 = 1 + \frac{7}{24} \Rightarrow 117/31 = 3 + \cfrac{1}{1 + \cfrac{1}{24/7}}$

$24 = 3 \cdot 7 + 3 \Rightarrow 24/7 = 3 + \frac{3}{7} \Rightarrow \frac{117}{31} = 3 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{7/3}}} = 3 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{3}}}}$

Thus $117/31 = 3 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{3}}}}$

Any $x \in \mathbb{Q}$ can be represented as finite cont. fractions

EUCLIDEAN ALGO !

Claim: e is irrational

THEOREM: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$

Proof. Suppose $\left(\frac{a}{p}\right) = 1$. Then there exists a solution for $x^2 \equiv a \mod p$. Let x_0 be a solution. Then $p \nmid x_0$ since $p \mid a$. Hence, by FLT:

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \mod p$$

Thus, Euler Criterion is true in this first case.

Next, suppose $\left(\frac{a}{p}\right) = -1$. For each $i = 1, 2, \ldots, p-1$ there exists a unique $j \in \mathbb{Z}$ with $1 \le j \le p-1$ such that $ij \equiv a \mod p$. As $x^2 \equiv a \mod p$ has no solutions, $i \neq j$. We can group the integers $1, 2, \ldots, p-1$ to $\frac{p-1}{2}$ pairs, each of which have product congruent to $a \mod p$. Thus $(p-1)! \equiv -1 \mod p \equiv a^{(p-1)/2} \mod p$. Hence Euler's Criterion applies in both cases. □

Proposition: Legendre symbol is completely multiplicative

Proof. For $a, b, p \in \mathbb{Z}$ s.t. $p \mid a$, $p \nmid b$, p prime, Euler's Criterion implies

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

Tuesday, May 6th 2025

PRIMITIVE ROOTS MOD P

DEF: Integer b is primitive root mod p if every integer a with $p \nmid a$, is congruent mod p to a number of the form b^n where $n \in \mathbb{N}_0$.

THEOREM: For any prime p, there are exactly $\varphi(p-1)$ primitive roots incongruent mod p

THEOREM: Let p prime and let b be a primitive root mod p. Then all the primitive roots mod p are given by b^m with $m \in \{1, 2, \dots, p-1\}$ and $\gcd(m, p-1) = 1$.

Ex: $p=7$, $b=3$, then $m \in \{1,5\}$ implies $x = \begin{cases} 3 \equiv 3 \mod 7 \\ 3^5 \equiv 243 \mod 7 \equiv 5 \mod 7 \end{cases}$

$p=7$, $b=5$, then $m \in \{1,5\}$ implies $x = \begin{cases} 5 \equiv 5 \mod 7 \\ 5^5 \equiv 3 \mod 7 \end{cases}$

Generating primitive roots: Every abelian group that belong to finite field is cyclic
Have finite abelian group is always product of cyclic groups

Group G has 35 elements
$a^5 = 1_G$ identity $\Rightarrow \langle a \rangle = \{1_G, a, a^2, a^3, a^4\}$
$b^7 = 1_G$ identity $\Rightarrow \langle b \rangle = \{1_G, b, b^2, b^3, b^4, b^5, b^6\}$

Let $c = ab$. Then $c^7 = a^7 b^7 = a^7 = a^2$...
$c^{35} = a^{35} b^{35} = 1_G$

FINALS REVIEW

just check the midterms grog 😭

- $\gcd(a,b) \cdot \text{lcm}(a,b) = ab$
- Find smallest integer such that $2n$ square, blablabla
- 8 pirates are killed blablabla
- Largest $m \equiv n!$ mod b less than 100 or smth
- Last 3 digits big number
- Arithmetic functions
- Quadratic residues
- Congruence solvable