M 328K

Katherine Ho

Contents

Lecture 1

August 27, 2024

1.1 Open Problems

- Twin Primes Conjecture: Do there exist infinitely many pairs of primes that are 2 apart?
- Collatz Conjecture, 3n+1 Problem - Does this process eventually stop for all n?
- Fermat's Last Theorem: The equation $x^n + y^n = z^n$ has no (non-trivial) integer solution when $n \geq 3$. Note: When $n = 2$, there are infinite solutions (Pythagorean triples)

1.2 Notation

- Natural numbers: $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$
- Integers: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- Rational Numbers: $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$

1.3 Divisibility

Definition 1.3.1. *Let $n, m \in \mathbb{Z}$. We say that n divides m and write $n|m$ if there exists an integer k such that $m = nk$.*

Ex: $2|4, 5|-5, 3|0, 0|0$

If n does not divide m: $n \nmid m$

Ex: $2 \nmid 3, 0 \nmid 5$

Theorem 1.3.0.1. *For $a, b, c \in \mathbb{Z}$, the following hold:*

1. $a|0$, $1|a$, $a|a$
2. $a|1$ *iff* $a = \pm b$
3. *If $a|b$ and $c|d$ then $ac|bd$*
4. *If $a|b$ and $b|c$ then $a|c$*
5. $a|b$ *and* $b|a$ *iff* $a = \pm b$
6. *If $a|b$ and $b \neq 0$, then $|a| \leq |b|$*
7. *If $a|b$ and $a|c$, then $a|(bx + cy)$ for $x, y \in \mathbb{Z}$*
   Ex. If b, c are even, then (any multiple of b) + (any multiple of c) is even.

Proof (2). First, assume $a|1$. By definition, there exists an integer k such that $1 = ak$.
Note: $k \neq 0$ and $a \neq 0$, so

$$|ak| = |a||k| \geq |a| \text{ since } |k| \geq 1$$

Thus, $1 = |ak| \geq |a|$.
Also, $|a| \geq 1$ since $a \neq 0$ and $a \in \mathbb{Z}$. Thus, $|a| = 1$ which is equivalent to $a = \pm 1$.

Next, assume $a = \pm 1$.

- If $a = 1$: $a|1$ since $1 = a \cdot 1$
- If $a = -1$: $1 = a \cdot -1$

In both cases, $a|1$ as desired. □

Proof (4). Assume $a|b$ and $b|c$.
By definition, there exist integers i and j such that $b = a \cdot i$ and $c = b \cdot j$.
Then, $c = (a \cdot i) \cdot j = a(ij)$.
So, $a|c$ by definition. □

1.4 The Division Algorithm

Theorem 1.4.0.1. *Given integers a and b with $b \neq 0$, there exist unique integers q and r such that*

$$a = bq + r, \; 0 \leq r \leq |b|$$

Lecture 2

August 29,2024

2.1 Proof by Contradiction

To prove a statement p, assume p is false and derive a contradiction.

Theorem 2.1.0.1. *$\sqrt{2}$ is irrational.*

Proof. Assume $\sqrt{2}$ is rational. So there exist integers a,b s.t.

$$\sqrt{2} = \frac{a}{b}, \text{ where a and b have no common factors.}$$

Thus $2b^2 = a^2$. ie. $2|a^2$. Hence also $2|a$. By definition, we can write $a = 2k$ for some $k \in \mathbb{Z}$. Then,

$$2b^2 = (2k)^2 = 4k^2$$
$$b^2 = 2k^2$$

So $2|b^2$, hence $2|b$. Thus, 2 is a common factor of a and b, a contradiction.
Therefore, $\sqrt{2}$ is irrational. □

2.2 Proof by Induction

Use to prove an infinite number of statements. Ex: Prove that the sum of the first n odd integers is n^2.
Strategy:

- Prove base case(s) n=0,1
- Prove that if the statement is true for n, then it is true for n+1

Proof by Induction. Base case: For n=1, the sum of the first n positive odd integers is 1, which is n^2.
Induction step: Assume that the sum of the first n odd integers is n^2. Consider the sum of the first n+1 odd integers.

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

By the induction hypothesis, we have

$$\begin{aligned}\sum_{k=1}^{n+1} 2k-1 &= n^2+2(n+1)-1\\ &= n^2+2n+2-1\\ &= n^2+2n+1\\ &= (n+1)^2, \text{ as desired}\end{aligned}$$

□

Theorem 2.2.0.1. *For $n \geq 1$, $\frac{d}{dx}x^n = nx^{n-1}$.*

Proof by Induction. Base case: n=1. $\frac{d}{dx}x^1 = 1 = 1 \cdot x^0$.
Induction step: Assume $\frac{d}{dx}x^n = nx^{n-1}$ is true for some $n > 1$. Using the power rule, we have

$$\begin{aligned}\frac{d}{dx}x^{n+1} &= x(nx^{n-1}) + x^n\\ &= n \cdot x^{1+(n-1)} + x^n\\ &= x^n(n+1)\\ &= (n+1)x^n, \text{ as desired.}\end{aligned}$$

□

2.3 Well Ordering Principle (WOP)

Every nonempty subset of $\mathbb{N}$ has a smallest element.

Theorem 2.3.0.1 (Division Algorithm)**.** *For any $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique integers q,s s.t. $a = bq + r, 0 \leq r < |b|$.*

Proof. Consider the set

$$S = \{a - bx | x \in \mathbb{Z}, a - bx \geq 0\}$$

For simplicity, assume $b > 0$. Note that S is nonempty since for $x = -|a|$, we have

$$\begin{aligned}a - bx = a - b - (-|a|) &= a + b|a|\\ &\geq a + |a|\\ &\geq 0\end{aligned}$$

So, $a - bx \in S$.

By WOP, S has a smallest element r. Call the corresponding value of x by q.
So $r = a - bq \Leftrightarrow a = bq + r$.

Now, we want to show that $0 \leq r \leq |b|$ $(= b)$ since $b > 0$.
By way of contradiction, assume $r \geq b$. Consider

$$\begin{aligned}a - b(q+1) &= a - bq - b\\ &= r - b\\ &\geq 0\end{aligned}$$

Thus, $a - b(q+1)$ is an element of S that is smaller than r, a contradiction.

Suppose there exist $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that

$$a = bq_1 + r_1 = bq_2 + r_2$$

where $0 \leq r_1, r_2 < b$ (still assuming $b > 0$). We want to show $q_1 = q_2, r_1 = r_2$. We have

$$\begin{aligned} bq_1 - bq_2 &= r_1 - r_2 \\ b(q_1 - q_2) &= r_1 - r_2 \\ b|q_1 - q_2| &= |r_1 - r_2| < b \end{aligned}$$

But $b|q_1 - q_2| < b$ implies (since $b > 0$) that

$$0 \leq |q_1 - q_2| < 1$$

So, $q_1 - q_2$ since $q_1, q_2 \in \mathbb{Z}$ Thus also $r_1 = r_2$. □

Note: The division algorithm lets us make statements like "Every integer can be expressed uniquely in the form $4k, 4k+1, 4k+2, or 4k+3$"

Theorem 2.3.0.2. *The square of every odd integer is of the form $8k+1$.*

Proof. By the division algorithm, any odd integer n is of the form $n = 4k+1$ or $4k+3$.
In the 1st case,

$$\begin{aligned} n^2 &= (4k+1)^2 \\ &= 16k^2 + 8k + 1 \\ &= 8(2k^2 + 3k + 1) \end{aligned}$$

In the 2nd case,

$$\begin{aligned} n^2 &= (4k+3)^2 \\ &= 16k^2 + 24k + 9 \\ &= 8(2k^2 + 3k + 1) + 1 \end{aligned}$$

□

Definition 2.3.1. *For $a, b, c \in \mathbb{Z}$, if $c|a$ and $c|b$, we say that c is a common divisor and has the property that for any other common c of a and b that $d \geq c$, we call d the greatest common divisor of a and b, and write $d = \gcd(a, b)$.*

Lecture 3

September 3, 2024

3.1 Problem - Diophantine Equations

If a rooster is worth 5 coins, a hen 3 coins, and 3 chicks together 1 coin, how many roosters, hens, and chicks, totaling 100, can be bought for 100 coins?

$$\begin{aligned} x &= \#roosters \\ y &= \#hens \\ z &= \#chicks \end{aligned}$$

$$\begin{aligned} x + y + z &= 100 \\ 5x + 3y + \frac{1}{3}z &= 100 \end{aligned}$$

<u>Diophantine Equations</u>

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

3.2 Bezout's Theorem

Let $a, b \in \mathbb{Z}$ (not both zero). The gcd of a and b is the smallest positive integer d that can be written as $ax + by = d, x, y \in \mathbb{Z}$.

Proof. Let $S = \{ax + by > 0 | x, y \in \mathbb{Z}\}$. Note that S is nonempty since for $x = a$, $y = b$ we have $ax + by = a^2 + b^2 > 0$. By WOP, S has a smallest element, call it d. WTS:

1. $d|a$, $d|b$
2. if $c|a$, $c|b$, then $c \leq d$

To show $d|a$, apply the division algo to obtain $a = d \cdot q + r, 0 \leq r < d$.
Writing $d = ax_0 + by_0$ for $x_0, y_0 \in \mathbb{Z}$, we have

$$\begin{aligned} r &= a - d \cdot y \\ r &= a(ax_0 + by_0) \cdot q \\ r &= a(1 - x_0 q) + b(-y_0 q) \end{aligned}$$

Hence, if $r > 0$ then $r \in S$ which is smaller than d, contradicting d being the smallest element. Then, $r = 0$ and $d|a$. (Same argument for $d|b$).
Now suppose that $c \in \mathbb{Z}$ such that $c|a$ and $c|b$. Recall that if x and y are integers, then $c|(cx + by)$. Hence, $c|(ax_0 + by_0) <=> c|d$. Then $c \leq |d| = d$. Therefore, $d = \gcd(a, b)$. □

Corollary 3.2.1. *Every common divisor of a and b divides* $\gcd(a, b)$.

Corollary 3.2.2. *The linear Diophantine equation $ax + by = c$ has a solution iff $d|c$.*

Proof. First assume that $ax+by = c$ has a solution: $c = ax_0+by_0$. Since $d|a$, and $d|b$, we have $d|(ax_0+by_0)$.
One the other hand, suppose $d|c$. By definition, $c = d|k$ for some k.
By Bezout's theorem, we can write

$$d = ax + by \text{ for some } x, y \in \mathbb{Z}$$

Then,

$$\begin{aligned} d \cdot k &= a(x \cdot k) + b(y \cdot k) \\ c &= a(x \cdot k) + b(y \cdot k) \end{aligned}$$

So c is an integer linear combo $a < b$ as desired. □

Definition 3.2.1. *We say that integers a and b (not both zero) are relatively prime or coprime if*

$$\gcd(a, b) = 1$$

Corollary 3.2.3. *Integers a and b are relatively prime iff there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

Corollary 3.2.4. *If a, b are coprime, then $ax + by = c$ has a solution for any $c \in \mathbb{Z}$.*

3.3 Euclidean Algorithm

1. Start with (a,b) (assume $|a| \geq |b|$)
2. Apply DA: $a = bq + r, 0 \leq r < |b|$
3. If $r = 0$, then $b|a$ and $\gcd(a, b) = |b|$.
4. Otherwise, replace (a, b) with (b, r).
5. Repeat.
6. The final nonzero r is gcd.

Example 3.3.0.1. $\gcd(12378, 3054)$

$$\begin{aligned} 12378 &= 3054 \cdot 4 + 162 \\ 3054 &= 162 \cdot 18 + 138 \\ 162 &= 138 \cdot 1 + 24 \\ 138 &= 24 \cdot 5 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

$$\gcd = 6$$

Note: if you allow for negative remainders, that can be more efficient.

$$\begin{aligned} 3054 &= 162 \cdot 19 - 24 \\ 162 &= (-24)(-7) - 6 \\ -24 &= (-6)(4) + 0 \end{aligned}$$

Example 3.3.0.2. *Solve* $1237x + 3054y = 6$ *via "Extended Euclidean Algorithm".*

$$\begin{aligned} 6 &= 24 - 18 \cdot 1 \\ &= 24 - (138 - 24 * 5) \\ &= 24 \cdot 6 - 138 \\ &= (162 - 138) \cdot 6 - 138 \\ &= 162 \cdot 6 - 138 \cdot 7 \\ &= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\ &= (12378 - 3054 \cdot 4) \cdot 6 - (3054 - (12378 - 3054)) \cdot 7 \end{aligned}$$

Example 3.3.0.3. *Solve*

$$\begin{aligned} x + y + z &= 100 \\ 5x + 3y + \frac{1}{3}z &= 100 \end{aligned}$$

Using $z = 100 - x - y$, *we have* $7x + 4y = 100$.
Note: $7(-1) + 4(2) = 1$.
So $7(-100) + 4(200) = 100$

$$\begin{aligned} 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 1 &= 4 - 3 \\ 1 &= 4 - (7 - 4) \\ 1 &= -7 + 4(2) \end{aligned}$$

Theorem 3.3.0.1. *If* $ax + by = c$ *has a solution* $x_0, y_0 \in \mathbb{Z}$. *Then any other solution* $x, y \in \mathbb{Z}$ *is given by*

$$x = x_0 + \frac{b}{d}k, y = y_0 - \frac{a}{d}k$$

where $k \in \mathbb{Z}$ *and* $d = \gcd(a, b)$.
If $x, y, z > 0$, *then* k *must satisfy*

$$\frac{200}{7} > k > 25$$

So

$$k = 26, 27, 28, \text{ so the only solutions are}$$

$$\begin{aligned} x &= 4, y = 18, z = 78 \\ x &= 8, y = 11, z = 81 \\ x &= 12, y = -1, z = 89 \end{aligned}$$

Lecture 4

September 5, 2024

4.1 Bezout, Euclid's Lemma

1. If $a|c$ and $b|c$, must $ab|c$?
   False: $a = b = c = 2$, $2|2$, $2|2$ but $4 \nmid 2$
2. If $a|bc$ and $a \nmid b$, must $a|c$?
   False: $a = 4, b = c = 2$

But... Proposition: Let $a, b, c \in \mathbb{Z}$

1. If $a|c, b|c$ and $\gcd(a, b) = 1$, then $ab|c$.

   Proof. By Bezout, there exist integers x, y s.t. $ax + by = 1$. Then, $acx + bcy = c$.
   By definition, there exist $r, s \in \mathbb{Z}$ s.t. $c = ar = bs$. Thus,

   $$\begin{aligned} a(bs)x + b(ar)y &= c \\ ab(sx + ry) &= c \end{aligned}$$

   So, $ab|c$. □

2. If $a|bc$, and $\gcd(a, b) = 1$, then $a|c$. (Euclid's Lemma)

   Proof. Again, there exist $x, y \in \mathbb{Z}$ s.t. $ax + by = 1$. Then $acx + bcy = c$.
   Since $a|bc$, we have $bc = ar$ for some $r \in \mathbb{Z}$. Hence

   $$\begin{aligned} acx + ary &= c \\ a(cx + ry) &= c \end{aligned}$$

   So, $a|c$ as desired. □

4.2 Prime Numbers

Definition 4.2.1. *A prime p is an integer greater than 1 that is only divisible by 1 and p.*

Theorem 4.2.0.1 (Euclid's Lemma)**.** *If p is prime and $p|ab$ $(a, b \in \mathbb{Z})$, then $p|a$ or $p|b$ (or both).*

Proof. Suppose $p \nmid a$. Since p is prime, this implies that $\gcd(p, a) = 1$.
Then by Euclid's Lemma, we have $p|b$. □

Corollary 4.2.1. *If p is prime and $p|(a_1 a_2 \dots a_n)$ then $p|a_k$ for some $k, 1 \le k \le n$.*

Proof by Induction. Base case ($n = 1$). Tautology *(If A then A)
Inductive step: Assume that for some $n \geq 1$, if p divides the product of any collection of n integers $a_1 \dots a_n$, then $p|c_k$ for some k.
Suppose $p|a_1 a_2 \dots a_n a_{n+1}$. By Euclid's Lemma, $p|a_1 a_2 \dots a_n$ OR $p|a_n + 1$.
In the latter case, we are done.
Hence assume now that $p|a_1 a_2 \dots a_n$. By IH, $p|a_k$ for some $k, 1 \leq k \leq n$ as desired. □

Corollary 4.2.2. *If p, q_1, q_2, q_n are primes, and $p|q_1 q_2 \dots q_n$, then $p = q_k$ for some k.*

Proof. By the previous result, $p|q_k$ for some k. Since q_k is prime and $p > 1$, we have $p = q_k$. □

Theorem 4.2.0.2 (Fundamental Theorem of Arithmetic, FTA)**.** *Every integer $n > 1$ can be expressed as a product of primes. Moreover, this expression is unique up to reordering the factors.*

Proof by Induction on n. Base case ($n = 2$).
Induction step: Assume that any integer (> 1) less than or equal to n satisfies FTA.
Now consider $n + 1$.
If $n+1$ is prime, we are done. Otherwise, assume $n+1 = ab$ for some $1 < a, b < n+1$. By IH, a and b can be expressed as a product of primes, hence so can $n + 1$. This proves the existence statement.

For uniqueness, take the same IH. Suppose that we can express $n + 1$ as

$$n + 1 = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

where p_r, q_s are prime. Without loss of generality, assume

$$p_1 \leq p_2 \leq \dots \leq p_r, \text{ and } q_1 \leq q_2 \leq \dots \leq q_s$$

Note $p_1|q_1 q_2 \dots q_s$, so $p_1 = q_i$ for some i. By the same argument, $q_1 = p_j$ for some j.
Since $p_1 \leq p_j$ and $q_1 \leq q_2$, this implies $p_1 = q_1$. By cancelling, we have $p_2 \dots p_r = q_2 \dots q_s$.
Since $p_2 \dots p_r = q_1 \dots q_s \leq n$, we can apply IH to conclude that $r = s$ and $p_i = q_i$ for all i. □

Theorem 4.2.0.3. *There exist infinitely many primes.*

Proof (Euclid). Assume that $p_1 \dots p_n$ is a list of n primes.
Consider the integer $N = p_1 \dots p_n + 1$. Note that no p_i can divide N, otherwise

$$p_i|(N - p_1 \dots p_n)$$
$$p_i|1$$
$$nooooo$$

But N is divisible by some prime p with $p \neq p_1, \dots, p_n$. Thus, there are infinitely many primes. □

Lecture 5

September 10, 2024

5.1 Modular Congruences

Recall: We often use arguments like "n is of the form $4k, 4k+1, 4k+2, \text{or } 4k+3\ldots$"

Definition 5.1.1 (Precise)**.** *Let $a, b, n \in \mathbb{Z}$ and $n > 0$. We say that a is congruent to b mod n if $n|(a-b)$. We write*

$$a \equiv b \pmod{n}$$

Definition 5.1.2 (Informal)**.** *$a \equiv b$ mod n if a and b give the same remainder after division by n. Examples:*

- $7 \equiv 2 \pmod 5$
- $-31 \equiv 11 \pmod 7$
- $10^{2024} + 1 \equiv 1 \pmod 1)0$
- $a \equiv b \pmod 2$ *iff a and b are both even or both odd*
- *a can be written in the form*

$$a = nk + r$$

iff $a \equiv r \pmod{n}$

Proposition 5.1.1. *Every integer is congruent modulo n to exactly one of* $0, 1, 2, \ldots, n-1$

Proof. Let $a \in \mathbb{Z}$. By the division algorithm, we can write

$$a = nq + r,\ 0 \leq r < n$$

Then $a - r = nq$, so $n|a-r$, ie.

$$a \equiv r \pmod{n}$$

Uniqueness follows from uniqueness of division algorithm remainder. □

Theorem 5.1.0.1. *Let $a, b, c \in \mathbb{Z}, n > 0$. Then*

1. $a \equiv a \pmod{n}$
2. *if* $a \equiv b \pmod{n}$ *then* $b \equiv a \pmod{n}$
3. *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$*, then* $a \equiv c \pmod{n}$

Proof (3). By definition, $n|a-b$ and $n|b-c$. Recall that if $n|r, n|s$, then $n|(rx+sy)$ for any $x, y \in \mathbb{Z}$. In particular,

$$n|((a-b)+(b-c)) \Leftrightarrow n|(a-c)$$

So $a \equiv c \pmod{n}$. □

Theorem 5.1.0.2. *Let $a, b, c, d \in \mathbb{Z}$ and assume $a \equiv b \pmod{n}$.*

1. *if $c \equiv d \pmod{n}$, then $a+c \equiv b+d \pmod{n}$.*
2. *if $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.*
3. *$a^k \equiv b^k \pmod{n}$ $\forall k \in \mathbb{Z}$.*

Proof (1). Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By definition, $n|a-b$ and $n|c-d$.
But, $(a+c)-(b+d) = (a-b)+(c-d)$ which is divisible by n, so $a+c \equiv b+d \pmod{n}$. □

Proof (3) by Induction. Base case: $k = 1$. Tautology
Inductive step: Assume for some $k > 1$ that $a^k \equiv b^k \pmod{n}$ (WTS: $a^{k+1} \equiv b^{k+1}$)
Note by (2) we have

$$\begin{aligned} a^k &\equiv b^k \pmod{n} && [IH] \\ a^k \cdot a &\equiv b^k \cdot b \pmod{n} && [2] \\ a^{k+1} &\equiv b^{k+1} \pmod{n} \end{aligned}$$

□

WARNING: In general, if $ac \equiv bc \pmod{n}$, it is not true that $a \equiv b \pmod{n}$. Ex: $2 \cdot 3 \equiv 2 \cdot 0 \pmod{6}$

Example 5.1.0.1. *Show* $41|(2^{20}-1) \Leftrightarrow$ *Show* $2^{20} \equiv 1 \pmod{41}$.
First,

$$\begin{aligned} 2^5 &\equiv 32 \pmod{41} \\ (2^5)^2 &\equiv (-9)^2 \\ 2^{10} &\equiv 81 \pmod{41} \\ 2^{10} &\equiv -1 \pmod{41} \\ 2^{20} &\equiv (-1) \equiv 1 \pmod{41} \end{aligned}$$

Proposition 5.1.2. *A decimal integer is divisible by 3 iff the sum of its digits is divisible by 3.*

Proof. Let n be an integer whose decimal representation is

$$(a_n a_{n-1} \dots a_1 a_0)_{10}$$

Then

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 100 + \dots + a_n \cdot 10^n$$

Then

$$a = a_0 + a_1 \cdot 10 + \dots + a_n \cdot 10^n \pmod{n}$$

Since $10 \mod 3 \equiv 1$, we have

$$a \equiv a_0 + a_1 + \dots + a_n \pmod{3}$$

□

5.2 Congruences with Unknowns

Example 5.2.0.1. *Solve*

$$\begin{aligned} x + 12 &\equiv 5 \pmod 8 \\ x &\equiv -7 \pmod 8 \end{aligned}$$

We also have

- $x \equiv 1 \pmod 8$ *is also a solution*
- $x \equiv 9$
- $x \equiv 17$

But we consider these to be the "same" since they are congruent.

Example 5.2.0.2. *Solve*

$$\begin{aligned} 4x &\equiv 3 \pmod{19} \\ 20x &\equiv 15 \pmod{19} \\ x &\equiv 15 \pmod{19} \\ \textit{Since } 20 &\equiv 1 \pmod{19} \end{aligned}$$

Example 5.2.0.3. *Solve*

$$6x \equiv 15 \pmod{514}$$

This has no solutions.
Why?! $6x - 15$ *is always odd.*
In particular, $514 \nmid (6x - 15)$.
In general, we want to understand when $ax \equiv b$ *has solutions and how to find them.*

Example 5.2.0.4. $18x \equiv 8 \pmod{22}$ *has incongruent solutions*
$x \equiv 20 \pmod{22}$ *and* $x \equiv a \pmod{22}$

Lecture 6

September 12, 2024

6.1 From Last Time

Solve $ax \equiv b \pmod{n}$.
It's possible for there to be no solutions OR a single solution OR multiple incongruent solutions.

Theorem 6.1.0.1. *1. $a \equiv a \pmod{n}$*

2. if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$

3. if $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

Example 6.1.0.1. $20 \equiv 1 \pmod{19}$

$$\begin{aligned}
20 &\equiv 1 \pmod{19} && \\
20x &\equiv x \pmod{19} && \\
20x &\equiv 15 \pmod{19} && \textit{We also have this} \\
x &\equiv 20x \pmod{19} && \textit{By (2)} \\
x &\equiv 15 \pmod{19} && \textit{By (3)}
\end{aligned}$$

6.2 Solving stuff

WARNING: If $ac \equiv bc \pmod{n}$, we can't conclude $a \equiv b \pmod{n}$.

Theorem 6.2.0.1. *If $\gcd(c, n) = 1$, then $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$.*

Proof. By definition, we have

$$n \mid (a - b)c$$

By Euclid's Lemma, since $\gcd(n, c) = 1$, we have $n \mid (a - b)$, hence $a \equiv b \pmod{n}$. $\square$

Proposition 6.2.1. *Let $d = \gcd(a, b)$ for some $a, b \in \mathbb{Z}$. Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proof. By Bezout, there exist integers x and y such that $ax + by = d$. Then,

$$(\frac{a}{d}x + \frac{b}{d}y) = 1$$

So $\frac{a}{d}, \frac{b}{d}$ are relatively prime. $\square$

Theorem 6.2.0.2. *Consider $ac \equiv bc \pmod{n}$ and let $d = \gcd(c, n)$. Then $a \equiv b \pmod{\frac{n}{d}}$.*
Note: If $d = 1$, this is the same statement as before.

Proof. $n \mid (a-b)c$ as before. So there exists $k \in \mathbb{Z}$ such that $(a-b)c = nk$. Then,

$$(a-b)\frac{c}{d} = \frac{n}{d}k$$

So,

$$\frac{n}{d} \mid (a-b)\frac{c}{d}$$

By Proposition 2.1, $\gcd(\frac{n}{d}, \frac{c}{d}) = 1$, so Euclid's Lemma says

$$\frac{n}{d} \mid (a-b), \text{ ie. } a \equiv b \pmod{\frac{n}{d}}$$

□

Example 6.2.0.1.

$$2 \cdot 3 \equiv 2 \cdot 0 \pmod 6 \qquad \gcd(2,6) = 2$$
$$3 \equiv 0 \pmod 3$$

Theorem 6.2.0.3 (Build-a-theorem)**.** *Let $a, b, n \in \mathbb{Z}$ with $n > 1$, let $d = \gcd(a, n)$. Then the linear congruence $ax \equiv b \pmod n$.*

- *has no solution if $d \nmid b$*
- *has exactly d incongruent solutions $\pmod n$ if $d \mid b$*

In particular, if x_0 is a solution, then

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$$

is a complete set of solutions $\pmod n$, ie. if x is a solution, then x is congruent modulo n to exactly one of

$$x_0 + t(\frac{n}{d}) \text{ for } 0 \leq t \leq d-1$$

Study $ax \equiv b \pmod n$. If this has a solution x, then $n \mid (ax-b)$. Then there exists $y \in \mathbb{Z}$ such that

$$ax - b = ny$$

So,

$$ax - ny = b$$

This linear diophantine equation has a solution exactly when $\gcd(a,n) = d \mid b$.

<u>Recall</u>: $6x \equiv 15 \pmod{512}$. $\gcd(6, 512) = (1, 2, 3, or\ 6)$. Note $3 \nmid 512$ since $3 + (5+1+2)$.
But $2 \nmid 15$, so there are no solutions.

Example 6.2.0.2. *Solve*

$$9x \equiv 21 \pmod{30}$$

$d = \gcd(9, 30) = 3 \mid 21$ *Either write down*

$$9x - 30y = 21$$

dividing,

$$3x - 10y = 7$$

OR apply Theorem 2.2 to yield

$$3x \equiv 7 \pmod{10}$$

leading to

$$3x - 10y = 7$$

Extended Euclidean algorithm

$$10 = 3 \cdot 3 + 1$$
$$10 - 3 \cdot 3 = 1$$
$$10 \cdot 7 - 3 \cdot 21 = 7$$
$$-10(-7) + 3(-21) = 7$$

$$\boxed{x\text{=-21,}y\text{=-7}}$$

But $x \equiv (-21) + 30 \pmod{30}$. $x \equiv 9 \pmod{30}$. *So we have found one solution (up to congruence).*
Note: $x = 9$ *is a solution to* $3x \equiv 7 \pmod{10}$. *So,* $x = 19$ *and* $x = 29$ *are also soolutions to* $3x \equiv 7 \pmod{10}$ *that are distrinct* $\pmod{30}$.

Example 6.2.0.3. *Solve*

$$18x \equiv 8 \pmod{22}$$

$d = \gcd(18, 22) = 2$. *First find a solution to*

$$9x \equiv 4 \pmod{11}$$

Solve

$$9x - 11y = 4$$

this has a solution $x = -2$, $y = -22$.
Choose $x = -2 + 11 = 9$ *is one solution.*
The other distinct solution $\pmod{22}$ *is*

$$x = 9 + 11 = 20$$

$x = 9, 20$ *is a complete set of solutions up to congruence* $\pmod{22}$.

Lecture 7

September 17, 2024

7.1 Last Time

1. $ax \equiv b \pmod{n}$ If $d = \gcd(a,n)$, then
   (a) If $d \nmid b$, then no solutions
   (b) If $d \mid b$, then there are exactly d incongruent solutions mod n
   (c) If $\gcd(a,n) = 1$, there is a unique solution mod n.
2. $9x \equiv 21 \pmod{30}$
   $d = \gcd(9,30) = 3$
   First divide by d to solve congruence
   $$3x \equiv 7 \pmod{10}$$
   This applies to point 1(c) and has a unique solution mod 10.
   Euclidean Algorithm: $x = -21$ is a solution. There are infinitely many solutions adding multiples of 10 to the solution.
   $$-21 + 10k \quad \text{is also a solution}$$
   They are all congruent to each other mod 10. Infinitely many integer solutions to $3x \equiv 7 \pmod{10}$ are
   $$\ldots, -21, -11, -1, 9, 19, 29, 39, \ldots$$
   This list also includes all solutions to original congruence, but not all the same mod 30.

7.2 Multiplicative Inverse

Consider $ax \equiv 1 \pmod{n}$. This has a (unique) solution iff $\gcd(a,n) = 1$.
A solution is called a multiplicative inverse of a modulo n. We will write it as $x \equiv a^{-1} \pmod{n}$ so $aa^{-1} \equiv 1 \pmod{n}$. Note that $a^{-1} \neq \frac{1}{a}$.
Recall. $4x \equiv 3 \pmod{19}$.
Note.

$$4^{-1} \equiv 3 \pmod{19} \quad \text{Since}$$
$$4 \cdot 5 \equiv 20 \equiv 1 \pmod{19}$$

Multiply $4x \equiv 3 \pmod{19}$ by $4^{-1} \pmod{19}$ to get

$$5 \cdot 4x \equiv 5 \cdot 3 \pmod{19}$$
$$x \equiv 15 \pmod{19}$$

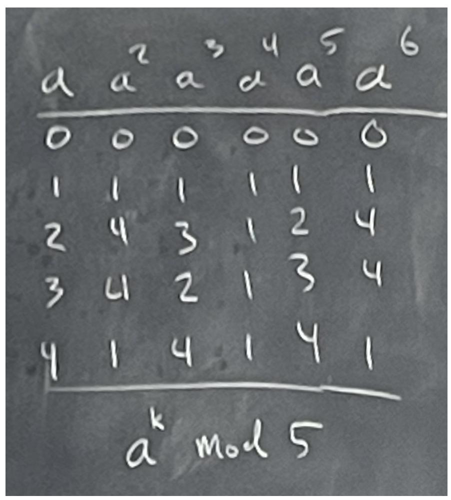
Example 7.2.0.1. *Find* $7^{-1} \pmod{17}$*. Solve* $7x \equiv 1 \pmod{17} \Leftrightarrow 7x - 17y = 1$.
EA:

$$\begin{aligned} 17 &= 7 \cdot 2 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 1 &= 7 - 3 \cdot 2 \\ 1 &= 7 - (17 - 7 \cdot 2)2 \\ &= 17(-2) + 7 \cdot 5 \end{aligned}$$

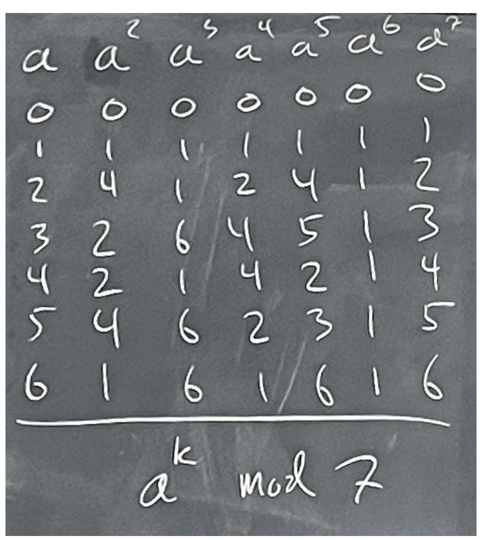
$$\boxed{x = 5}$$

7.3 Stuff

$a^k \pmod 5$



$a^k \pmod 7$



7.3.1 Fermat's Little Theorem

Theorem 7.3.1.1. *Let p be prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then*

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

ie.

$$p \mid (a^{p-1} - 1)$$

Proof (Idea). $p = 5$

$$\begin{aligned} 0,1,2,3,4,5 &\pmod 5 \\ 0,2,4,1,3 &\pmod 5 \\ &0,3,1,4,2 \end{aligned}$$

□

Claim: The integers $0, a, 2a, \ldots, (p-1)a \pmod p$ are the same as the integers $0, 1, 2, \ldots, (p-1)$ but maybe in a different order.

Proof of Claim. If claim is false, then $ia \equiv ja \pmod p$ for some i, j. Then $p \mid a(i-j)$. □

Now Consider

$$\begin{aligned} &a(2a)(3a)\ldots((p-1)(a)) \\ &= a^{p-1}(1)(2)(3)\ldots(p-1) \\ &= a^{p-1}(p-1)! \end{aligned}$$

On the other hand, by the claim,

$$\begin{aligned} a(2a)(3a)\ldots((p-1)a) \equiv (1)(2)(3)\ldots(p-1) \pmod p \\ a^{p-1}(p-1)! \equiv (p-1)! \pmod p \end{aligned}$$

By HW,

$$\gcd((p-1)!, p) = 1$$

So we can cancel:

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

7.3.2 Example

$p = 23$. $6^{22} = 1 \pmod{23}$.
ie.

$$23 | (6^{22} - 1)$$

7.3.3 Primality Test

$n = 10^{100} + 37$
Compute

$$\begin{aligned} 2^{n-1} = 2^{10^{100}+36} &\not\equiv 1 \pmod n \\ &\equiv 367\ldots396 \pmod n \end{aligned}$$

So n is not prime.
Note: This will never show n is prime. It can be true that $a^{n-1} \equiv 1 \pmod{n}$ even if n is composite.
Test 117 with $a = 2$.

$$\begin{aligned} 2^{116} &= 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^{4} \\ &\equiv 16 \cdot 22 \cdot 16 \cdot 16 \\ &\equiv 22 \\ &\not\equiv 1 \pmod{117} \end{aligned}$$

So 117 is composite.

Lecture 8

September 19, 2024

8.1 Last Time

8.1.1 Fermat's Little Theorem

Let p be prime, $a \in \mathbb{Z}$, $p \nmid a$, then

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

$$ax \equiv 1 \pmod{n} \quad \text{has a solution whenever} \quad \gcd(a, n) = 1$$

$$\begin{aligned} 4x &\equiv 3 \pmod{19} \\ 4^{17}(4x) &\equiv 4^{17} \cdot 3 \pmod{19} \\ 4^{18}x &\equiv 5 \cdot 3 \pmod{19} \\ x &\equiv 15 \pmod{19} \end{aligned}$$

Note: Definitely need p to be prime.

Example 8.1.1.1.

$$3^9 \equiv 3 \pmod{10}$$

8.2 Generalization to composite modulus

8.2.1 Euler Totient Function (Euler's Phi Function)

Definition 8.2.1. *The Euler totient function ϕ is the function ϕ $\mathbb{N} \to \mathbb{N}$ defined by*

$$\phi(n) = \#\{a \mid 1 \leq a \leq n-1, \gcd(a, n) = 1\}$$

Example 8.2.1.1.

$$\begin{aligned} \phi(1) &= 1 \\ \phi(2) &= 1 \\ \phi(3) &= 2 \\ \phi(4) &= 2 \\ \phi(20) &= 8 \end{aligned}$$

Proposition 8.2.1. *If p is prime, then*

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

Proposition 8.2.2. *If p is prime and $k > 1$, then*

$$\phi(p^k) = p^k - p^{k-1}$$

Exclude all multiples of p between 1 and p^k:

$$p, 2p, 3p, \ldots, (p^{k-1})p, p^{k-1}p$$

Note: $\phi(n) = n - 1$ iff n is prime. Intuition: ϕ is how close n is to being prime.

8.2.2 Euler's Theorem

Theorem 8.2.2.1 (Euler's Theorem)**.** *Let* $\gcd(a, n) = 1$*. Then*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Note: If $n = p$ is prime, then $\phi(n) = p - 1$, so we get

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

Proof of Euler's Theorem. Let $0 < b_1 < b_2 < \cdots < b_{\phi(n)}$ be the integers between 1 and n that are coprime to n. The claim: The integers $ab_1, ab_2, \ldots, ab_{\phi(n)}$ are the same as $b_1, b_2, \ldots, b_{\phi(n)} \pmod{n}$ but maybe in a different order.

Example 8.2.2.1. *$n = 10$; $a - 3$*

$$\begin{array}{cccccc} b_1 & b_2 & b_3 & b_4 & & \\ 1 & 3 & 7 & 9 & & \\ ab_1 & ab_2 & ab_3 & ab_4 & & \pmod{10} \\ 3 & 9 & 1 & 7 & & \end{array}$$

Proof is same from HW.
So

$$\begin{aligned} (ab_1)(ab_2) &\equiv b_1 b_2 \ldots b_{\phi(n)} \pmod{n} \\ a^{\phi(n)}(b_1 b_2 \ldots b_{\phi(n)}) &\equiv b_1 b_2 \ldots b_{\phi(n)} \end{aligned}$$

Since each b_i is coprime to n, we can cancel to get

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

□

8.2.3 More on ϕ

$$\begin{aligned} \phi(p) &= p - 1 \quad \text{for } p \text{ prime} \\ \phi(p^k) &= p^k - p^{k-1} \end{aligned}$$

Theorem 8.2.3.1. *Let a, b be coprime positive integers. Then,*

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

"ϕ is multiplicative."

WARNING*: We need* $\gcd(a, b) = 1$*. Ex. $\phi(4) = 2$, $\phi(2)\phi(2) = 1$*

Corollary 8.2.1. *If $n = p_1^{r_1} \dots p_k^{r_k}$, then*

$$\phi(n) = \phi(p_1^{r_1}) \dots \phi(p_k^{r_k}) = (p^{r_1} - p^{r_{k-1}}) \dots (p^{r_k} - p^{r_{k-1}})$$

To prove this, we first need to understand how to solve this problem from 4th century China:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

We will solve this using the Chinese Remainder Theorem.

8.2.4 Chinese Remainder Theorem

Theorem 8.2.4.1 (Chinese Remainder Theorem)**.** *Suppose* $\gcd(n_1, n_2) = 1$ *for pos integers n_1 and n_2. Then for any $a_1, a_2 \in \mathbb{Z}$, the system*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}$$

has a unique solution $0 \le x < n_1 n_2$.

Proof (Existence). By Bezout, there exist $m_1, m_2 \in \mathbb{Z}$ such that

$$n_1 m_1 + n_2 m_2 = 1$$

Now let $x = a_2 n_1 m_1 + a_1 n_2 m_2$. Then reducing $\pmod{n_1}$, we have

$$\begin{aligned} x = a_2 n_1 m_1 + a_1 n_2 m_2 &\equiv a_1 n_2 m_2 \pmod{n_1} \\ &\equiv a_1(1 - n_1 m_1) \pmod{n-1} \\ &\equiv a_1 - a_1 n_1 m_1 \pmod{n-1} \\ &\equiv a_1 \pmod{n_1} \end{aligned}$$

By the same argument,

$$x \equiv a_2 \pmod{n_2}$$

Take $x \pmod{n_1 n_2}$ to be a solution between 0 and $n_1 n_2$. □

Example 8.2.4.1. *Going back to this problem,*

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

First use Bezout:

$$\begin{aligned} 3 \cdot 2 + 5(-1) &= 1 \\ x = 3(6) + 2(-5) \pmod{15} &= 8 \end{aligned}$$

$$\begin{aligned} x \equiv 8 &\pmod{15} \\ x \equiv 2 &\pmod 7 \\ 15 \cdot 1 + 7(-2) &= 1 \\ x = 2(15) + 8(-14) &\pmod{105} \\ -82 &\pmod{105} = 23 \end{aligned}$$

Relationship with ϕ: To show

$$\phi(ab) = \phi(a)\phi(b)$$

when $\gcd(a, b) = 1$, we need to count two things:

$$\{x \mid 0 \leq x < ab, \gcd(x, ab) = 1\}$$

Size: $\phi(ab)$

$$\{(y_1, y_2) \mid 0 \leq y_1 < a, \gcd(y_1, a) = 1, 0 \leq y_2 < b, \gcd(y_2, b) = 1\}$$

Size: $\phi(a)\phi(b)$

Lecture 9

September 24, 2024

9.1 Last Time

Chinese Remainder Theorem

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}$$

has a unique solution mod $n_1 n_2$.

$$x \equiv \quad \text{a unique integer in} \quad 0, 1, 2, \ldots, n_1 n_2 - 1$$

Lecture 10

September 26, 2024

10.1 Some more properties of primes

<u>Freshmen's Dream</u>

$$(x+y)^n = x^n + y^n \quad \text{False!}$$

$$(x+y)^n = \sum_{k=0}^{n} x^k y^{n-k}$$

$$\text{where} \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

If $n = p$ is prime, then

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{n-k}$$

From HW: for $0 << k < p$, we have $p \mid \binom{p}{k}$.

So, $(x+y)^p = x^p + y^p + p \cdot$ some poly w/ $\mathbb{Z}$ coeffs.

Reducing $\pmod p$, we have

$$(x+y)^p \equiv x^p + y^p \pmod p$$

On the topic of polynomials...

Solving $F(x) \equiv 0 \pmod n$ can be weird.

Example 10.1.0.1. *Find all solutions (up to congruence) to*

$$x^2 \equiv 0 \pmod 9$$

$x = 0, x = 3, x = 6 \leftarrow 3$ *roots to a polynomial* $F(x) = x^2$ *of degree 2.*
This happens because 9 is not prime.

Theorem 10.1.0.1. *Let* $F(x)$ *be a polynomial of degree* r*. Then* $F(x)$ *has at most* r *roots mod any prime* p *(as long as* $p \nmid$ *(leading coeff)).*

Example 10.1.0.2. *From HW you showed that the only square roots of* $1 \pmod p$ *were 1 and -1.*

10.2 Wilson's Theorem

Theorem 10.2.0.1 (Wilson's Theorem)**.** *Let p be a prime. Then*

$$(p-1)! \equiv -1 \pmod p$$

Example 10.2.0.1. $p = 11$*:*

$$(1)(2)\ldots(9)(10)$$

- *1 and 10 pair to themselves.*
- *2 pairs with 6.* $(2 \cdot 6) - 1$
- *3 pairs with 4.*
- *5 pairs with 9.*
- *7 pairs with 8.*

$$\begin{aligned} 10! &= (1)(2\cdot 6)(3\cdot 4)(5\cdot 9)(7\cdot 8)\cdot 10 \\ &\equiv (1)(1)(1)(1)(1)(-1) - 1 \pmod{11} \end{aligned}$$

Proof. Let p be prime and consider the integers $2, 3, \ldots, p-2$. Each one of these integers has some inverse $\pmod p$. ie. If $a \in \{2, 3, \ldots, p-2\}$, then $ax \equiv 1 \pmod p$ has a solution.

Claim: For each $a \in \{2, 3, \ldots, p-2\}$,

$$a \not\equiv a^{-1} \pmod p$$

Why? If $a \equiv a^{-1} \pmod p$, then

$$a^2 \equiv 1 \pmod p$$

From HW, the solutions are exactly

$$a \equiv 1 \quad \text{or} \quad a \equiv -1$$

Then we can pair each $a \in \{2, 3, \ldots, p-2\}$ with its inverse $\pmod p$ to get

$$(p-1)! = 1((2)(3)\ldots(p-2))(p-1) \equiv -1 \pmod p$$

Note: $(2)(3)\ldots(p-2) \equiv 1 \pmod p$, $(p-1) \equiv -1 \pmod p$. $\square$

Note: We really need p to be prime.

Example 10.2.0.2. *Look at* $x^2 \equiv 1 \pmod 8$.

$$x \equiv 1, x \equiv -1 (\equiv 7), x \equiv 3, x \equiv 5, x \equiv 7$$

Remark: $F(x) = x^2 - 1$ *has 4 roots* $\pmod 8$.

10.3 Review

Example 10.3.0.1. *Compute* $3^{104} \pmod{101}$

$$\begin{aligned} 3^{100} &\equiv 1 \pmod{101} \\ 3^4 \cdot 3^{100} &\equiv 3^4 \pmod{101} \\ 3^{104} &\equiv 81 \pmod{101} \end{aligned}$$

Example 10.3.0.2. *For $n > 3$, $\phi(n)$ is even.*
ϕ is multiplicative. $\to$ compute ϕ from prime factorization.
Write $n = p_1^{k_1} \ldots p_r^{k_r}$ then

$$\phi(n) = \phi(p_1^{k_1} \ldots \phi(p_r^{k_r})) = (p_1^{k_1} - p_1^{k_1-1}) \ldots (p_r^{k_r} - p_r^{k_r-1})$$

Lecture 11

October 3, 2024

11.1

Lecture 12

October 8, 2024

12.1 Miscellaneous

12.1.1 Least Common Multiple

Definition 12.1.1. *Let a, b be positive integers. The least common multiple of a and b denoted by $lcm(a,b)$ is the smallest positive integer divisible by a and b.*
Examples

- $lcm(2,3) = 6$
- $lcm(4,6) = 12$
- $lcm(1,n) = n$
- $lcm(n,n) = n$

$$4 \cdot 6 = 24, \gcd(4,6) = 2, lcm(4,6) = 12$$

$$3 \cdot 9 = 27, \gcd(3,9) = 3, lcm(3,9) = 9$$

Theorem 12.1.1.1. *For positive integers a, b we have*

$$ab = \gcd(a,b) \cdot lcm(a,b)$$

12.1.2 More about ϕ (and number-theoretic functions)

Definition 12.1.2. *A number theoretic function (or arithmetic function) is a function*

$$f : \mathbb{N} \leftrightarrow \mathbb{N} \quad (or\ \mathbb{Z} \leftrightarrow \mathbb{Z})$$

that has "number theory properties"
Ex:

- ϕ
- $\tau(n) = \#$ *of divisors of* n

$$\begin{aligned} 10: &\quad 1, 2, 5, 10 \\ \tau(10) &= 4 \\ 12: &\quad 1, 2, 3, 4, 6, 12 \\ \tau(12) &= 6 \end{aligned}$$

- $\sigma(n) =$ *sum of divisors of* n

$$\begin{aligned}\sigma(10) &= 1 + 2 + 5 + 10 = 18\\ \sigma(12) &= 1 + 2 + 3 + 4 + 6 + 12 = 28\end{aligned}$$

Facts: ϕ, τ, σ *are all multiplicative.*

$$\begin{aligned}\phi(ab) &= \phi(a)\phi(b)\\ \sigma(ab) &= \sigma(a)\sigma(b) \quad \textit{if } \gcd(a, b) = 1\\ \tau(ab) &= \tau(a)\tau(b)\end{aligned}$$

Notice: $\sigma(n) = \sum_{d|n} d, \quad \tau(n) = \sum_{d|n} 1$
($d \mid n$ *is sum over positive divisors of* n*)*

Example 12.1.2.1. *Define* $F(n) = \sum_{d|n} \phi(d)$

$$\begin{aligned}F(12) &= \sum_{d|12} \phi(d)\\ &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6)\phi(12)\\ &= 1 + 1 + 2 + 2 + 2 + 4\\ F(12) &= 12\end{aligned}$$

$$\begin{aligned}F(15) &= \phi(1) + \phi(3) + \phi(5)\phi(15)\\ &= 1 + 2 + 4 + 8\\ F(15) &= 15\end{aligned}$$

Theorem 12.1.2.1. *For all pos integers* n*,*

$$n = \sum_{d|n} \phi(d)$$

Proof. (Step 1) Lemma: If $f : \mathbb{N} \leftrightarrow \mathbb{N}$ is multiplicative, then the function

$$F(n) = \sum_{d|n} f(d)$$

is multiplicative. (Proof: HW)

(Step 2) We know that $F(n) = \sum_{d|n} \phi(d)$ is multiplicative, since ϕ is multiplicative.
Lets show $F(n) = n$ for primes and prime powers.
If p is prime, then $F(p) = \sum_{d|p} \phi(d) = \phi(1) + \phi(p) = 1 + (p - 1) = p$
Now calculate for $k \geq 1$

$$\begin{aligned}F(p^k) &= \sum_{d|p^k} \phi(d)\\ &= \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^k)\\ &= 1 + (p - 1) + (p^2 - p) + \cdots + (p^j - p^{j-1}) + (p^k - p^{k-1})\\ F(p^k) &= p^k\end{aligned}$$

Now let $n = p_1^{k_1} \dots p_r^{k_r}$

$$\begin{aligned} F(n) &= F(p_1^{k_1}) \dots F(p_r^{k_r}) \\ &= p_1^{k_1} \dots p_r^{k_r} \\ &= n \end{aligned}$$

□

12.1.3 Lagrange's Theorem

Recall $x^2 \equiv 1 \pmod 8$ has $x \equiv 1, 3, 5, 7$ (4 solutions). But…

Theorem 12.1.3.1 (Lagrange's Theorem)**.** *Let $f(x)$ be a polynomial of degree d with integer coefficient and p be prime. Suppose $p \nmid$(leading coefficient).*
Then $f(x) \equiv 0 \pmod p$ has at most d incongruent solutions.

Proof. By induction on the degree d.
Base case: $d = 1$, $f(x) = a_1 x + a_o$ and $p \nmid a_1$. Then

$$\begin{aligned} f(x) &\equiv 0 \pmod p \\ a_1 x + a_0 &\equiv 0 \pmod p \\ a_1 x &\equiv a_0 \pmod p \end{aligned}$$

has a unique solution since $\gcd(a_1, p) = 1 \leq d$.

Induction step: Let's assume the statement is true for all polynomials of degree $\leq k$.
Now let $f(x) \equiv a_{k+1} x^{k+1} + \dots + a_1 x + a_0$ where $p \nmid a_{k+1}$. If $f(x) \equiv 0 \pmod p$ has no solutions, then we are done since $0 < k + 1$. Hence suppose $x = a$ is a solution.
By the division algorithm applied to $f(x)$ and $x - a$, we have

$$\begin{aligned} f(x) &= (x - a) \cdot q(x) + r, \quad r \in \mathbb{Z} \\ f(a) &\equiv 0 \pmod p \\ r &\equiv 0 \pmod p \end{aligned}$$

Thus, $f(x) \equiv (x - a) \cdot q(x) \pmod p$. By IH, $q(x) \equiv 0 \pmod p$ has at most k solutions. Thus $f(x) \equiv 0 \pmod p$ has at most $k + 1$ solutions.

□

12.2 Order

12.2.1

Definition 12.2.1. *Let $\gcd(a, n) = 1$. Then the smallest positive integer k such that $a^k \equiv 1 \pmod n$ is called the order of a modulo n and is denoted by $ord_n(a)$ or just $ord(a)$ is it's unambiguous.*

Example 12.2.1.1. $a^k \pmod 7$

Theorem 12.2.1.1. *Suppose $\gcd(a, n) = 1$ and $a^k \equiv 1 \pmod n$. Then $ord(a) \mid k$.*

Proof. By division algorithm, write

$$k = \operatorname{ord}(a) \cdot q + r, \quad 0 \leq r < \operatorname{ord}(a)$$

Then

$$\begin{aligned} a^k &\equiv 1 \pmod n \\ a^{\mathrm{ord}(a)\cdot q} \cdot a^r &\equiv 1 \pmod n \\ a^{\mathrm{ord}(a)^q} \cdot a^r &\equiv 1 \pmod n \\ a^r &\equiv 1 \pmod n \end{aligned}$$

Then $r = 0$, otherwise r is a smaller exponent for $a^r \equiv 1 \pmod n$ contradicting $\mathrm{ord}(a)$ being the smallest. Thus $k = \mathrm{ord}(a) \cdot q$ so $\mathrm{ord}(a) \mid k$. $\square$

Lecture 13

October 10, 2024

13.1

Lecture 14

October 15, 2024

14.1 Recap

If $\gcd(a, n) = 1$, the order of a is the smallest positive exponent k such that $a^k \equiv 1 \pmod{n}$

- If $a^m \equiv 1 \pmod{n}$, then $\operatorname{ord} a \mid m$
- $a, a^n, \ldots, a^{\operatorname{ord} n}$ are all incongruent $\pmod{n}$
- If $\operatorname{ord} a = \phi(n)$, then a is called a primitive root and $a, \ldots, a^{\phi(n)} \pmod{n}$ are congruent to all the integers between 1 and n, coprime to n

14.2 All primes have a primitive root

Theorem 14.2.0.1. *Let p be prime and $d \mid p-1$. Then there are exactly $\phi(d)$ integers (that are mutually incongruent $\pmod{p}$) that have order $d \pmod{p}$. In particular there are $\phi(p-1)$ primitive roots.*

Lemma 1. *If $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d incongruent solutions pmodp.*

Proof. $x^{p-1} - 1 \equiv x^{dk} - 1 = (x^d - 1)(x^{d(k-1)} + \cdots + x^d + x)$ □

Proof of Thm. Define $\psi(d) = \#$ of integers $1 \leq x \leq p-1$ having order $d \pmod{p}$.

WTS: $\psi(d) = \phi(d)$ for $d \mid p-1$
Instead, let's prove $\psi(d) \leq \phi(d)$ when $d \mid p-1$. If there are no integers with order d, then

$$\psi(d) = 0 \leq \phi(d)$$

Hence assume there exists at least one integer a with $\operatorname{ord}_p a = d$.

Claim: If b has order d, then $b \equiv a^h \pmod{p}$ for some h. Why? If b has order d, then b satisfies:

$$x^d \equiv 1 \pmod{p} \quad *$$

which has exactly d incongruent solutions. On the other hand, the integers $a, a^2, a^3, \ldots, a^d$ are all incongruent $\pmod{p}$ and they all satisfy $*$, since

$$(a^i)^d \equiv (a^d)^i \equiv 1^i \equiv 1 \pmod{p}$$

Since $*$ has exactly d solutions $\pmod{p}$, we must have $b \equiv a^h \pmod{p}$ for some h, $1 \leq h \leq d$.

Now, we need to determine which a^k has $\operatorname{ord} a^k = d$. But $\operatorname{ord} a^k = \frac{d}{\gcd(h,d)=d}$ precisely when $\gcd(h, d) = 1$. Hence there are exactly $\phi(d)$ exponents h such that a^h has order d. Thus, we find $\psi(d) = \phi(d)$. We have shown for $d \mid p-1$, $\psi(d)$ is either 0 or $\phi(d)$. But we know $\psi(d) \leq \phi(d)$.

Consider the sum

$$\sum_{d \mid p-1} \psi(d).$$

Note every integer a between $1 \leq a \leq p-1$ has some $\operatorname{ord} a$ that divides $p-1$. Since each integer between 1 and $p-1$ is counted exactly once, we have

$$\sum_{d \mid p-1} \psi(d) = p - 1$$

Example 14.2.0.1. *$p = 7$*

$$\begin{aligned} \operatorname{ord} 1 &= 2 \\ \operatorname{ord} 2 &= 3 \\ \operatorname{ord} 3 &= 6 \\ \operatorname{ord} 4 &= 3 \\ \operatorname{ord} 5 &= 6 \\ \operatorname{ord} 6 &= 2 \end{aligned}$$

$$\begin{aligned} \sum_{d \mid p-1} \psi(d) &= \sum_{d \mid 6} \psi(d) \\ &= \psi(1) + \psi(2) + \psi(3) + \psi(6) \\ &= 1 + 1 + 2 + 2 \\ &= 6 \\ &= p - 1 \end{aligned}$$

Recall

$$\sum_{d \mid p-1} \phi(d) = p - 1$$

Hence

$$\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d), \quad \psi(d) \leq \phi(d)$$

Thus $\psi(d) = \phi(d) \quad \forall \quad d \mid p-1$. □

Note: Once you have a primitive root g, then all the other primitive roots are congruent to g^h where $\gcd(h, p-1) = 1$.

14.3 Index

Definition 14.3.1. *Let g be a primitive root of p (or n if n has a primitive root). If $1 \leq a \leq p-1$, the smallest positive exponent k with $a \equiv g^k \pmod p$ is called the index of $a \pmod p$ relative to g, denoted* $\operatorname{ind}(a)$.

Theorem 14.3.0.1. *The following hold:*

a) $\operatorname{ind}(ab) \equiv \operatorname{ind}(a) + \operatorname{ind}(b) \pmod p$

b) $\mathrm{ind}(a^k) \equiv k\,\mathrm{ind}(a) \pmod{p-1}$ *for* $k \geq 1$.

c) $\mathrm{ind}(1) \equiv 0 \pmod{p-1}$

Proof (a). Let g be a primitive root. By definition of index,

$$\begin{aligned} g^{\mathrm{ind}(a)} &\equiv a \pmod{p} \\ g^{\mathrm{ind}(b)} &\equiv b \pmod{p} \end{aligned}$$

Then,

$$\begin{aligned} g^{\mathrm{ind}(a)} g^{\mathrm{ind}(b)} &\equiv ab \pmod{p} \\ g^{\mathrm{ind}(a)+\mathrm{ind}(b)} &\equiv ab \pmod{p} \\ g^{\mathrm{ind}(a)+\mathrm{ind}(b)} &\equiv g^{\mathrm{ind}(ab)} \pmod{p} \end{aligned}$$

Recall: If $a^i \equiv a^j \pmod{n}$, then $i \equiv j \pmod{}$.
Hence $\mathrm{ind}(a) + \mathrm{ind}(b) \equiv \mathrm{ind}(ab) \pmod{p-1}$. □

The most important property: ”taking indices of both sides” If $a \equiv b \pmod{p}$, then

$$\begin{aligned} g^{\mathrm{ind}(a)} &\equiv g^{\mathrm{ind}(b)} \pmod{p} \\ \mathrm{ind}(a) &\equiv \mathrm{ind}(b) \pmod{p-1} \end{aligned}$$

Example 14.3.0.1. *Solve* $4x^9 \equiv 7 \pmod{13}$.

Take indices of both sides (relative to prim root g)

$$\begin{aligned} \mathrm{ind}(4x^9) &\equiv \mathrm{ind}(7) \pmod{12} \\ \mathrm{ind}(4) + 9\,\mathrm{ind}(x) &\equiv 7 \pmod{12} \\ 2 + 9\,\mathrm{ind}(x) &\equiv 11 \\ 9\,\mathrm{ind}(x) &\equiv 9 \pmod{12} \end{aligned}$$

linear in the unknown $\mathrm{ind}(x) \to 3$ *solutions*
Solutions $\mathrm{ind}(x) \equiv 1, 5, 9$

So $x \equiv 2^1, 2^5, 2^9 \equiv 1, 6, 5 \pmod{13}$.

Lecture 15

October 17, 2024

15.1 Recall

15.1.1 Indices $\pmod p$ relative to a primitive root g

$$g, g^2, \ldots, g^{p-1} \equiv 1, 2, 3, \ldots, p-1 \pmod p$$

Example 15.1.1.1. *Does $x^k \equiv a \pmod p$ have a solution? Take indices of both sides*

$$\begin{aligned} \operatorname{ind}(x^k) &\equiv \operatorname{ind}(a) \pmod{p-1} \\ k \operatorname{ind}(x) &\equiv \operatorname{ind}(a) \pmod{p-1} \\ ky &\equiv \operatorname{ind}(a) \pmod{p-1} \end{aligned}$$

15.1.2

$ax \equiv b \pmod n$ has a solution iff $\gcd(a, n) \mid b$. Let $d = \gcd(k, p-1)$. Then $x^k \equiv a \pmod p$ has a solution iff

$$d \mid \operatorname{ind}(a)$$

Theorem 15.1.2.1. *Let p be prime and $p \nmid a$. Then $x^k \equiv a \pmod p$ has a solution iff*

$$a^{\frac{p-1}{d}} \equiv 1 \pmod p$$

where $d = \gcd(k, p-1)$. If so it has exactly d incongruent solutions.

Proof. Taking indices, the congruence

$$a^{\frac{p-1}{d}} \equiv 1 \pmod p$$

is equivalent to

$$\begin{aligned} \frac{p-1}{d} \operatorname{ind}(a) &\equiv \operatorname{ind}(1) \pmod{p-1} \\ \frac{p-1}{d} \operatorname{ind}(a) &\equiv 0 \pmod{p-1} \end{aligned}$$

is equivalent to

$$\frac{p-1}{d} \operatorname{ind}(a) \equiv (p-1)m \quad \text{for some } m \in \mathbb{Z}$$

$\leftrightarrow \operatorname{ind}(a) = dm$ is equivalent to $d \mid \operatorname{ind}(a)$ iff $x^k \equiv a \pmod p$ has a solution. $\square$

15.2 Quadratic Residue

15.2.1 Quadratic Residue

Definition 15.2.1. *Let p be prime and $p \nmid a$. We say that a is a quadratic residue of p (or $\pmod p$) and write "a is QR" if the congruence $x^2 \equiv a \pmod p$ has a solution.*

Otherwise we say that a is a quadratic nonresidue or "a is NR".

Example 15.2.1.1. *Compute quadratic residues of $p = 13$*

$$\begin{aligned} 1^2 &\equiv 1 \equiv 12^2 \\ 2^2 &\equiv 4 \equiv 11^2 \\ 3^2 &\equiv 9 \equiv 1-^2 \pmod{13} \\ 4^2 &\equiv 3 \equiv 9^2 \\ 5^2 &\equiv 12 \equiv 8^2 \\ 6^2 &\equiv 1- \equiv 7^2 \end{aligned}$$

QR: $1, 3, 4, 9, 10, 12$.
NR: $2, 5, 6, 7, 8, 11$

Q: Given a, how do you determine if a is QR or NR? $\leftrightarrow$ When does $x^2 \equiv a \pmod p$?
Using indices $\rightarrow$ Theorem (Euler's Criterion):
$x^2 \equiv a \pmod p$, p odd has a solution iff

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Example 15.2.1.2. $3^{\frac{13-1}{2}} \equiv 3^6 \equiv (3^2)^3 \equiv (9^3) \equiv (-4)^3 \equiv 1 \pmod{13}$

$$2^{\frac{13-1}{2}} \equiv 2^6 \equiv 2^4 \cdot 2^2 \equiv 4^2 \cdot 4 \equiv -1 \pmod{13}$$

15.2.2 Euler's Criterion

Theorem 15.2.2.1 (Euler's Criterion)**.** *Let p be odd prime and $p \nmid a$. Then a is QR iff*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

and a is NR iff

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Proof. Let p be an odd prime and $p \nmid a$. Assume a is NR. Then we will show $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.
Let $c \in \{1, \ldots, p-1\}$. Consider $cx \equiv a \pmod p$.
Since $\gcd(c, p) = 1$, this has a unique solution $c' \in \{1, \ldots, p-1\}$.
Note $c \neq c'$, otherwise $cc' \equiv a \pmod p$, $c^2 \equiv a \pmod p$ contradicts a is NR. So every $c \in \{1, \ldots, p-1\}$ has a distinct c' such that $cc' \equiv a \pmod p$. Hence we get $\frac{p-1}{2}$ pairs $(c_1, c_1'), \ldots, (c_{\frac{p-1}{2}}, c'_{\frac{p-1}{2}})$ Such that

$$c_2 c_2' \equiv a \pmod p$$

We have

$$\begin{aligned} c_1 c_1' &\equiv a \pmod p \\ c_{\frac{p-1}{2}} c'_{\frac{p-1}{2}} &\equiv a \pmod p \end{aligned}$$

Multiplying these together,

$$(c_1c_1')(c_2c_2')\dots(c_{\frac{p-1}{2}}c'_{\frac{p-1}{2}}) \equiv a^{\frac{p-1}{2}} \pmod p$$

But $c_1, c_1', c_2, c_2', \dots, c_{\frac{p-1}{2}}c'_{\frac{p-1}{2}}$ is just a permutation of $1, 2, \dots, p-1$.
So,

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv c_1c_1'c_2c_2\dots c_{\frac{p-1}{2}}c'_{\frac{p-1}{2}} \\ a^{\frac{p-1}{2}} &\equiv (p-1)! \\ a^{\frac{p-1}{2}} &\equiv -1 \pmod p \qquad \text{(Wilson)} \end{aligned}$$

□

15.3 Legendre

Definition 15.3.1. *Let p be an odd prime and $p \nmid a$. The Legendre symbol of a with respect to p is defined*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is } QR \\ -1 \text{ if } a \text{ is } NR \end{cases}$$

Theorem 15.3.0.1. *The Legendre sumbol has the following properties*

1. $a \equiv b \pmod p \to \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{a}{p^2}\right) = 1$
3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
5. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$
6. $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Proof (4). By Euler's Criterion:

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

But $\left(\frac{x}{p}\right)$ only takes values ± 1, so

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Corollary 15.3.1. *For an odd prime p,*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv 3 \pmod 4 \end{cases}$$

Proof.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ if } \frac{p-1}{2} \text{ is even} \\ -1 \text{ if } \frac{p-1}{2} \text{ is odd} \end{cases} = \begin{cases} 1 \text{ if } \frac{p-1}{2} \equiv 0 \pmod 2 \\ -1 \text{ if } p \equiv 3 \pmod 4 \end{cases}$$

□