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: $\mathbb{N} = \{1, 2, 3, 4, \dots\}$
- Integers: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- 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?

$$x = \#roosters$$
$$y = \#hens$$
$$z = \#chicks$$

$$x + y + z = 100$$
$$5x + 3y + \frac{1}{3}z = 100$$

Diophantine Equations

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

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

$$r = a - d \cdot y$$
$$r = a(ax_0 + by_0) \cdot q$$
$$r = a(1 - x_0q) + b(-y_0q)$$

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 $p|(a_1 a_2 \ldots a_n)$ 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

$$\begin{aligned} &p_i|(N - p_1 \dots p_n) \\ &p_i|1 \\ &\quad nooooo \end{aligned}$$

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:

- $7 \equiv 2 \pmod 5$
- $-31 \equiv 11 \pmod 7$
- $10^{2024} + 1 \equiv 1 \pmod 10$
- $a \equiv b \pmod 2$ *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

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

Then

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

Then

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

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

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

□

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 $a \equiv b \pmod{n}$. □

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. □

Theorem 6.2.0.2. *Consider* $ac \equiv bc \pmod{n}$ *and let* $d = \gcd(c, n)$*. Then* $a \equiv b \pmod{\frac{n}{d}}$.
<u>Note</u>: 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

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

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 $\gcd(a,n) = d \mid b$.

Recall: $6x \equiv 15 \pmod{512}$. $\gcd(6,512) = (1,2,3, or\ 6)$. 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

$$\begin{aligned} 10 &= 3 \cdot 3 + 1 \\ 10 - 3 \cdot 3 &= 1 \\ 10 \cdot 7 - 3 \cdot 21 &= 7 \\ -10(-7) + 3(-21) &= 7 \end{aligned}$$

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

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.

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

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

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

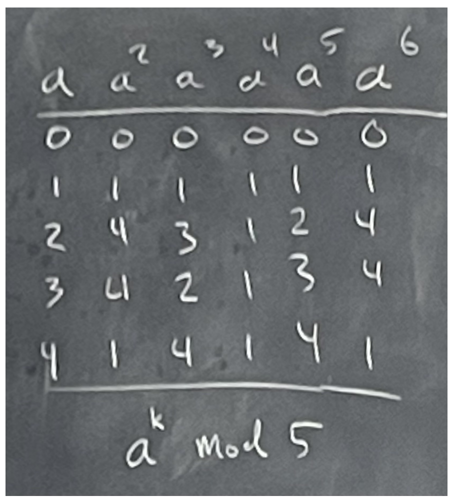
Example 7.2.0.1. *Find* $7^{-1} \pmod{17}$*. Solve* $7x \equiv 1 \pmod{17} \Leftrightarrow 7x - 17y = 1$.
EA:

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

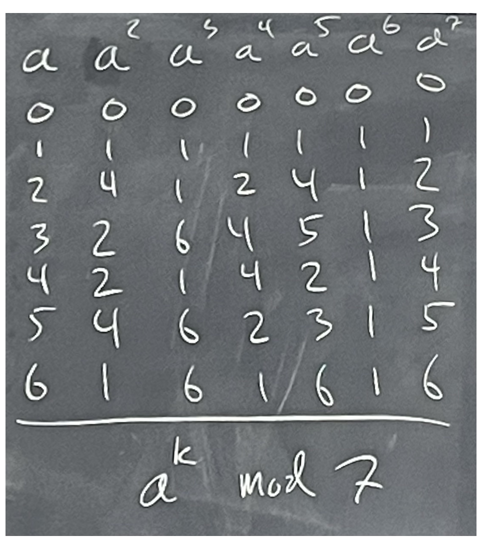
$$\boxed{x = 5}$$

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). $p = 5$

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

□

<u>Claim</u>: 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 <u>not prime</u>.
Note: This will <u>never</u> 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 $\phi\ \mathbb{N} \to \mathbb{N}$ 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. *$n = 10$; $a - 3$*

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

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 $n_1 n_2$. $\square$

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:

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

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

<u>Relationship with ϕ</u>: 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

Freshmen's Dream

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

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

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

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

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. *$p = 11$:*

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

- *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 $2, 3, \dots, p-2$. Each one of these integers has some inverse $\pmod{p}$. ie. If $a \in \{2, 3, \dots, p-2\}$, then $ax \equiv 1 \pmod{p}$ has a solution.

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

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

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 $a \in \{2, 3, \dots, p-2\}$ with its inverse $\pmod{p}$ to get

$$(p-1)! = 1((2)(3)\dots(p-2))(p-1) \equiv -1 \pmod{p}$$

Note: $(2)(3)\dots(p-2) \equiv 1 \pmod{p}$, $(p-1) \equiv -1 \pmod{p}$. ☐

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. $\rightarrow$ compute ϕ from prime factorization.
Write $n = p_1^{k_1} \dots p_r^{k_r}$ then

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

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: $d = 1$, $f(x) = a_1x + a_o$ and $p \nmid a_1$. Then

$$\begin{aligned} f(x) &\equiv 0 \pmod p \\ a_1x + a_0 &\equiv 0 \pmod p \\ a_1x &\equiv a_0 \pmod p \end{aligned}$$

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 $f(x) \equiv a_{k+1}x^{k+1} + \cdots + a_1x + a_0$ 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

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

Then

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

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

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 <u>primitive root</u> 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 $1 \le x \le p-1$ having order $d \pmod{p}$.

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

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

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

<u>Claim</u>: 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, $1 \le h \le d$.

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 $\psi(d) \le \phi(d)$.

Consider the sum

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

Note every integer a between $1 \le a \le p-1$ 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

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

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

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

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

$$g^{\operatorname{ind}(a)} \equiv a \pmod{p}$$
$$g^{\operatorname{ind}(b)} \equiv b \pmod{p}$$

Then,

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

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

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

$$g^{\operatorname{ind}(a)} \equiv g^{\operatorname{ind}(b)} \pmod{p}$$
$$\operatorname{ind}(a) \equiv \operatorname{ind}(b) \pmod{p-1}$$

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

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

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

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

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 $c \in \{1, \dots, p-1\}$. Consider $cx \equiv a \pmod p$.
Since $\gcd(c, p) = 1$, this has a unique solution $c' \in \{1, \dots, p-1\}$.
Note $c \neq c'$, otherwise $cc' \equiv a \pmod p$, $c^2 \equiv a \pmod p$ contradicts a is NR. So every $c \in \{1, \dots, p-1\}$ has a distinct c' such that $cc' \equiv a \pmod p$. Hence we get $\frac{p-1}{2}$ pairs $(c_1, c_1'), \dots, (c_{\frac{p-1}{2}}, c'_{\frac{p-1}{2}})$ 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*

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

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:

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

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,*

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

Proof.

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

□

Lecture 16

October 22, 2024

16.1 Last Time

Legendre Symbol, p odd prime, $p \nmid a$

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

16.2 Legendre 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 (6).

$$\begin{aligned} \left(\frac{-1}{p}\right) &\equiv (-1)^{\frac{p-1}{2}} \pmod p \\ &= \begin{cases} 1 \text{ if } \frac{p-1}{2} \text{ is even} \\ -1 \text{ if } \frac{p-1}{2} \text{ is odd} \end{cases} \\ &= \begin{cases} 1 \text{ if } p-1 \equiv 0 \pmod 4 \\ -1 \text{ if } p-1 \not\equiv 0 \pmod 4 \end{cases} \\ p \equiv 3 &\pmod 4 \text{ since } p \text{ is odd.} \end{aligned}$$

□

16.3 Infinite Primes

Theorem 16.3.0.1. *There exist infinitely many primes of the form* $4k+1$.

Proof. Let $p_1, \ldots, p_r$ be a finite set of primes s.t. $p_i \equiv 1 \pmod 4 \quad \forall i$.
Consider $N = (2p_1p_2 \ldots p_r)^2 + 1$. Let p be an odd prime dividing N. Note $p \neq p_i$ for any i, otherwise $p \mid (N - (2p_1 \ldots p_r)^2) = 1$. But since $p \mid ((2p_1p_2 \ldots p_r)^2 + 1)$, we have

$$(2p_1p_2 \ldots p_r)^2 \equiv -1 \pmod p$$

ie. $\left(\frac{-1}{p}\right) = 1$, so $p \equiv 1 \pmod 4$. So we have constructed another prime $\equiv 1 \pmod 4$ not in the original list. All integers of the form $4k+1$ for an arithmetic progression $1, 5, 9, 13, \ldots$

□

Theorem 16.3.0.2 (Dirichlet)**.** *Any arithmetic progression* $a, a+k, a+2k, \ldots$ *contains infinitely many primes* $(\gcd(a,k) = 1)$

16.4 Gauss' Lemma

Theorem 16.4.0.1 (Gauss' Lemma)**.** *Let* p *be an odd prime and* $\gcd(a,p) = 1$. *Let*

$$\begin{aligned} \gamma(a,p) = \gamma(a) = \\ & \#\ \textit{of integers in the } a, 2a, 3a, \ldots \frac{p-1}{2}a \\ & \textit{that become negative when reduced} \pmod p \textit{ into the interval} \\ & \{-\frac{p-1}{2}, \frac{p-1}{2}\} \end{aligned}$$

Then $\left(\frac{a}{p}\right) = (-1)^{\gamma(a,p)}$.

Proof. After reducing $\pmod p$ to lie in the interval $\{-\frac{p-1}{2}, \frac{p-1}{2}\}$, let $r_1, \ldots, r_m$ be the negative integers $t_1, \ldots, t_n$ be the positive integers. Since $r_1, \ldots, r_m, t_1, \ldots, t_n$ are congruent to $a, 2a, 3a, \ldots, \frac{p-1}{2}a$, we have

$$\begin{aligned} r_1r_2 \ldots r_m t_1 t_2 \ldots t_n &\equiv a \cdot 2a \ldots \frac{p-1}{2}a \pmod p \\ (-1)^m(-r_1) \ldots (-r_m)t_1 \ldots t_n &\equiv a^{\frac{p-1}{2}}(\frac{p-1}{2})! \pmod p \\ (-1)^m(\frac{p-1}{2})! &\equiv a^{\frac{p-1}{2}}(\frac{p-1}{2})! \pmod p \\ (-1)^m &\equiv a^{\frac{p-1}{2}} \pmod p \\ (-1)^m &\equiv \left(\frac{a}{p}\right) \pmod p \end{aligned}$$

But by definition, $m = \gamma(a,p)$. So

$$(-1)^{\gamma(a,p)} = \left(\frac{a}{p}\right)$$

□

Theorem 16.4.0.2. *Let* p *be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \textit{ if } p \equiv 1 \textit{ or } 7 \pmod 8 \\ 1 \textit{ if } p \equiv 3 \textit{ or } 5 \pmod 8 \end{cases}$$

Proof. Apply Gauss' Lemma to the list $2, 4, \ldots, 2 \cdot \frac{p-1}{2}$. Then $\gamma(a)$ is the # of integers $k, 1 \leq k \leq \frac{p-1}{2}$ such that $2k > \frac{p-1}{2}$.

$$\frac{p-1}{2} < 2k \Longleftrightarrow \frac{p-1}{4} < k \leq \frac{p-1}{2}$$

being odd or even depends only on $p \pmod 8$. $\square$

16.5 Quadratic Reciprocity

Theorem 16.5.0.1 (Quadratic Reciprocity)**.** *Let p and q be odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Theorem 16.5.0.2 (Computational version)**.** *p, q are odd primes.*

1.

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

2.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod 8 \\ -1 & p \equiv 3, 5 \pmod 8 \end{cases}$$

3. $\left(\frac{p}{1}\right) = \left(\frac{q}{p}\right)$ *except whenever both p and q are $\equiv 3 \pmod 4$, in which case* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Q: Is 14137 a square $\pmod{30013}$?

$$\left(\frac{14137}{30013}\right) = \left(\frac{67 \cdot 211}{30013}\right) = \left(\frac{67}{30013}\right) \cdot \left(\frac{211}{30013}\right)$$

$$\left(\frac{67}{30013}\right) = \left(\frac{30013}{67}\right) = \left(\frac{64}{67}\right) = \left(\frac{2^6}{67}\right) = \left(\frac{2^{3^2}}{67}\right) = 1$$

$$\left(\frac{211}{30013}\right) = \left(\frac{30013}{211}\right) = \left(\frac{51}{211}\right) = \left(\frac{3}{211}\right) \cdot \left(\frac{17}{211}\right)$$

$$\left(\frac{3}{211}\right) = -\left(\frac{211}{3}\right) \equiv -\left(\frac{1}{3}\right) = -1$$

$$\left(\frac{17}{211}\right) = \left(\frac{211}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1$$

Lecture 17

October 24, 2024

17.1 Last Time: Quadratic Reciprocity

Theorem 17.1.0.1. *p, q are odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Theorem 17.1.0.2. *p, q are odd primes, then*

- $$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \textit{if } p \equiv 1 \pmod 4 \textit{ OR } q \equiv 1 \pmod 4 \\ \left(\frac{-q}{p}\right) & \textit{if } p \equiv 3 \pmod 4 \textit{ AND } q \equiv 3 \pmod 4 \end{cases}$$

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

- $$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod 8 \\ -1 & p \equiv 3, 5 \pmod 8 \end{cases}$$

17.2 More on quadratic reciprocity

17.2.1 Factors of $n^2 - 5$

$f(x) = x^2 - 5 \qquad f(44) = 1931$

n	$f(n)$
1	-2^2
2	-1
3	2^2
4	11
5	$2^2 \cdot 5$
6	$3 \cdot 1$
7	$2^2 \cdot 11$
8	59
9	$2^2 \cdot 19$
10	$5 \cdot 19$

No digit $\equiv 3, 7$ ever appears. What is going on?

If an odd prime p divides $n^2 - 5$

$$\begin{aligned} &\iff n^2 \equiv 5 \pmod p \\ &\iff \left(\frac{5}{p}\right) = 1 \end{aligned}$$

Since $5 \equiv 1 \pmod 4$, we have

$$1 = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & p \equiv 1, 4 \pmod 5 \\ -1 & p \equiv 2, 3 \pmod 5 \end{cases}$$

if $p \equiv 2 \pmod 5$, then $p \not\equiv 2 \pmod{10}$ (p is odd) or $p \equiv 7 \pmod{10}$.
if $p \equiv 3 \pmod 5$, then $p \not\equiv 3 \pmod{10}$ or $p \not\equiv \gamma \pmod{10}$.

$$\left(\frac{14137}{30013}\right) = \left(\frac{67}{30013}\right)\left(\frac{211}{30013}\right)$$

Can we do this without factoring? YES.

17.2.2 Jacobi Symbol

Definition 17.2.1. *Let n be an odd integer with $n = p_1^{e_1} \dots p_r^{e_r}$ and let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Define the Jacobi symbol by*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_r}\right)^{e_r}$$

where $\left(\frac{a}{p_i}\right)$ is a Legendre symbol.

Notes:

- If n is an odd prime, then the Jacobi symbol is the same as Legendre.
- The "denominator" in $\left(\frac{a}{n}\right)$ must always be odd.
- If it is ever even in a computation, something has gone wrong.
- If $\left(\frac{a}{n}\right) = 1$, that does not imply that a is QR of n. But if $\left(\frac{a}{n}\right) = -1$, then a is NR of n.

Example 17.2.2.1. *$a = 2, n = 9$. Note 2 is not a square $\pmod 9$.*
But $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = 1$.
In fact $\left(\frac{a}{9}\right) = \left(\frac{a}{3}\right)^2 = 1$ for all a coprime.

17.2.3 General Quadratic Reciprocity

Theorem 17.2.3.1 (General Quadratic Reciprocity)**.** *Let a and b be odd positive integers. then,*

- $$\left(\frac{-1}{b}\right) = \begin{cases} 1 & b \equiv 1 \pmod 4 \\ -1 & b \equiv 3 \pmod 4 \end{cases}$$
- $$\left(\frac{2}{b}\right) = \begin{cases} 1 & b \equiv 1, 7 \pmod 8 \\ -1 & b \equiv 3, 5 \pmod 8 \end{cases}$$
- $$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}, \left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & a \equiv 1 \pmod 4 \text{ OR } b \equiv 1 \pmod 4 \\ -\left(\frac{b}{a}\right) & a \equiv 3 \pmod 4 \text{ AND } b \equiv 3 \pmod 4 \end{cases}$$

Back to:

$$\left(\frac{14137}{30013}\right) = \left(\frac{67}{30013}\right)\left(\frac{211}{30013}\right)$$

$$\left(\frac{14137}{30013}\right) = \left(\frac{30013}{14137}\right) = \left(\frac{1739}{14137}\right)$$

$$\left(\frac{14137}{1739}\right) = \left(\frac{225}{1739}\right) = \left(\frac{1739}{225}\right) = \left(\frac{164}{225}\right)$$

WARNING: You must factor out powers of 2.

$$= \left(\frac{2^2 \cdot 41}{225}\right) = \left(\frac{41}{225}\right) = \left(\frac{225}{41}\right)$$

$$= \left(\frac{20}{41}\right) = \left(\frac{2^2 \cdot 5}{41}\right) = \left(\frac{5}{41}\right)$$

$$= \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1$$

Example 17.2.3.1.

$$\left(\frac{22}{33}\right) = \left(\frac{2 \cdot 11}{33}\right)$$

$$= \left(\frac{2}{33}\right)\left(\frac{11}{33}\right)$$

then use above property for $\left(\frac{2}{b}\right)$

17.2.4 Solovay-Strassen Primality Test

Let $a \in \{1, \ldots, n-1\}$ coprime to n.

$$\text{If } a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n} \quad \text{then n is composite.}$$

WARNING: If $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$, you <u>cannot</u> conclude n is prime.

17.2.5 Another primality test?

Theorem 17.2.5.1. *If $n > 1$ is composite, then at least half of the integers $\{1, \ldots, n-1\}$ satisfy*

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$$

Example 17.2.5.1. *Let's prove $n = 9$ is composite. Choose $a = 2$*

$$2^{\frac{n-1}{2}} = 2^4 = 16 \equiv 17 \pmod{9}$$

We are done since $\left(\frac{2}{9}\right) = \pm 1$. So 9 is composite.

17.2.6 Polynomials

Q: Let $f(x) = ax^2 + bx + c, a, b, c \in \mathbb{Z}$. When does $f(x) = ax^2 + bx + c \equiv 0 \pmod{p}$ where $\gcd(a, p) = 1$ have a solution? Complete the square.
Note since p is an odd prime and $\gcd(a, p) = 1$, we have $\gcd(4a, p) = 1$. So then $ax^2 + bx + c \equiv 0 \pmod{p}$ is equivalent to $4a(ax^2 + bx + c) \equiv 0 \pmod{p}$.
Now complete the square:

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$$

$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$ is equivalent to

$$\begin{aligned}(2ax + b)^2 - (b^2 - 4ac) &\equiv 0 \pmod{p} \\ (2ax + b)^2 &\equiv b^2 - 4ac \pmod{p}\end{aligned}$$

Let $y = 2ax + b$

$$y^2 \equiv b^2 - 4ac \pmod{p}$$

17.2.7 Application: Primitive Roots

Theorem 17.2.7.1. *Suppose p and $q = 2p + 1$ are odd primes. then*

$$g = (-1)^{\frac{p-1}{2}} 2 \quad \textit{is a primitive root of } q.$$

Proof. $\mathrm{ord}_q(g) \mid q - 1 = 2p \implies \mathrm{ord}_q(g) = 1, 2, p,$ or $2p$ □

Show that $\mathrm{ord}_q(g)$ is not p by considering $g^p \pmod{q}$.
Cases: $p \equiv 1 \pmod{4}$, then $g = 2$. So we look at does $g^p = 2^p \equiv 1 \pmod{q}$?
Rewrite as

$$2^p = 2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) \pmod{q}$$

Claim: If $p \equiv 1 \pmod{4}$, then $\left(\frac{2}{2p+1}\right) = -1$.
If $p \equiv 3 \pmod{4}$, $g^p = (-2)^{\frac{q-1}{2}} \equiv \left(\frac{-2}{2p+11}\right) \equiv \left(\frac{-1}{2p+1}\right)\left(\frac{2}{2p+1}\right) \pmod{q}$

Lecture 18

October 29, 2024

18.1 (Incomplete)

But recall, since $p \equiv 3 \pmod 4$, we have

$$q = 2(3 + 4k) + 1 = 8k + 7 \equiv 7 \pmod 8$$

Hence $\left(\frac{2}{q}\right) = 1$.

On the other hand $q = 8k + 7 \equiv 7 \equiv 3 \pmod 4$. So, $\left(\frac{-1}{q}\right) = -1$. Thus, $(-2)^p \equiv \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) \equiv (-1)(1) \equiv 1 \pmod q$. Hence, $\text{ord}_q(-2) \neq p \implies \text{ord}_q(-2) = 2p$.

Example 18.1.0.1. *Choose $p = 11 \to q = 22 + 1 = 23$ has primitive root $g = -2$. Choose $p = 7 \to q = 15$ not prime.*
Procedure:

1. *Choose some large odd prime p.*
2. *$q = 2p + 1$*
3. *Test if q is prime*
4. *Profit: bc ± 2 is a prim root of q.*

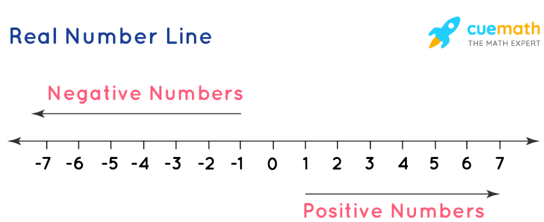
18.2 Number Theory of Complex Numbers

Definition 18.2.1. *A complex number is a number of the form $z = x + iy$ where $x, y \in \mathbb{R}$. Addition is defined by $(a + bi) + (c + di) = (a + c) + (b + d)i$. Multiplication is defined so that "FOIL" works and so that $i^2 = -1$. Then $(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$.*

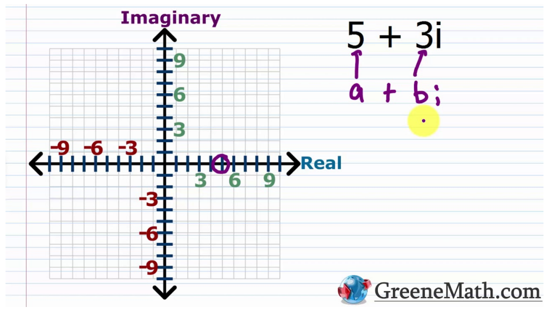
Theorem 18.2.0.1 (Fundamental Theorem of Algebra)**.** *Every polynomial has a complex root.*

18.2.1 Complex Numbers

For $\mathbb{R} \to$ "number-line".

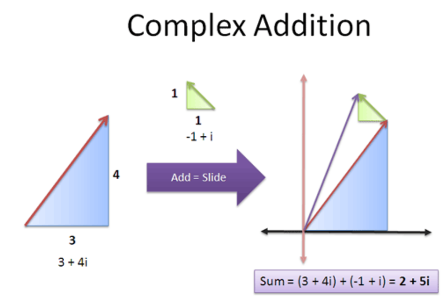


For $\mathbb{C} \to$ "number-plane"



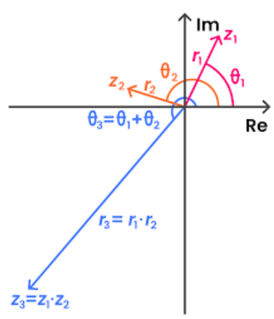
18.2.2 Algebraic Geometric

Addition: vector addition



$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Multiplication:



Use polar form:

$$a + bi = r_1(\cos(\theta_1) + i\sin(\theta_1))$$
$$c + di = r_2(\cos(\theta_2) + i\sin(\theta_2))$$

Euler's Identity:

$$\cos(\theta) + i\sin(\theta) = e^{i\theta}$$

For $\theta = \pi$ $\quad \cos\pi + i\sin\pi = e^{i\pi}, e^{i\pi} = 1$

$$a + bi = r_1 e^{i\theta_1}$$
$$c + di = r_2 e^{i\theta_2}$$

18.2.3 Number Theory

Want to study complex numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$. Called "Gaussian Integers".
Note: Addition/multiplication of 2 Gaussian integers results in a Gaussian integer.
Something weird happens:

$$(1 + i)(1 - i) = (1 + i - i - 1i^2) = 2$$

So 2 is not "prime" in Gaussian integers. On the other hand, 3 is "prime" in Gaussian integers. But $5 = (1 + 2i)(1 - 2i)$ is not prime.

Q: Which prime can be factored in the Gaussian integers?
(Related): Which primes can be expressed as a sum of squares?

$$(a + bi(a - bi) = a^2 + b^2)$$

Lecture 19

October 31, 2024

19.1 Exam Review

19.1.1 HW7 Q4

Show that $\left(\frac{5}{p}\right) = 1$ iff $p \equiv 1, 9, 11, 19 \pmod{20}$.
Since $5 \equiv 1 \pmod 4$

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1 \quad \text{where P is QR of 5}$$

$$\begin{aligned} 1^2 &= 1 \\ 2^2 &= 4 \\ 3^2 &= 9 \equiv 4 \\ 4^2 &= 16 \equiv 1 \end{aligned}$$

So,

$$\left(\frac{5}{1}\right) = 1 \text{ iff } p \equiv 1, 4 \pmod 5$$

19.1.2 Determine congruence conditions for $\left(\frac{-5}{p}\right) = 1$

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \begin{cases} 1 \text{ whenever } \left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1 \text{ or } \left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1 \end{cases}$$

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

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \begin{cases} 1 \text{ when } p \equiv 1, 4 \pmod 5 \\ -1 \text{ when } p \equiv 2, 3 \pmod 5 \end{cases}$$

Hence we have $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1$ iff

$$(p \equiv 1 \pmod 4) \text{ AND } (p \equiv 1 \pmod 5 \text{ or } p \equiv 4 \pmod 5)$$

Equivalently,

$$p \equiv 1 \pmod 4, p \equiv 1 \pmod 5 \quad \text{OR} \quad p \equiv 1 \pmod 4, p \equiv 4 \pmod 5$$

Using Chinese Remainder Theorem,

$$p \equiv 1 \pmod{20} \quad \text{OR} \quad p \equiv 9 \pmod{20}$$

On the other hand, we have $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1$ iff

$$\begin{array}{rcl} p \equiv 3 \pmod 4 & \text{OR} & p \equiv 3 \pmod 4 \\ p \equiv 2 \pmod 5 & & p \equiv 3 \pmod 5 \\ \iff & & \iff \\ p \equiv 7 \pmod{20} & & p \equiv 3 \pmod{20} \end{array}$$

So,

$$\left(\frac{-5}{p}\right) = 1 \text{ iff } p \equiv 1, 3, 7, 9 \pmod{20}$$

19.2 Last Time: Complex Numbers

19.2.1 Gaussian Integers

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

We saw that 2 is not "prime" in $\mathbb{Z}[i]$ since $2 = (1+i)(1-i)$. But what does it mean to be prime in $\mathbb{Z}[i]$?

$3 = (3i)(-i)$, so is 3 "composite" in $\mathbb{Z}[i]$?
Idea: This isn't a "real" factorization, just like $3 = (-3)(-1)$.

Why/how do we exclude $\pm i$? Are there other elements of $\mathbb{Z}[i]$ we should exclude from factorization?

Answer: Only need to exclude $1, -1, i, -i$.

For each $a \in \{1, -1, i, -i\}, \exists b \in \mathbb{Z}[i]$ such that $ab = 1$. Ex: $(-1)(-1) = 1, (i)(-i) = 1$

19.3 Units

Definition 19.3.1. *A Gaussian integer z is called a unit if there exists some $w \in \mathbb{Z}[i]$ such that*

$$zw = 1$$

Theorem 19.3.0.1. *The only units in $\mathbb{Z}[i]$ are $1, -1, i, -i$.*

Use geometry of $\mathbb{C}$ to answer.

Recall: Multiplication has a geometric meaning in polar coordinates

$$z = a + bi \to (a, b) \leftrightarrow (r, \theta)$$

$$zw \leftrightarrow (r_1, \theta_1)(r_2, \theta_2) = (r_1 r_2, \theta_1 + \theta_2)$$

$z = a + bi$ has polar coords (r, θ). Then $r\sqrt{a^2 + b^2}$. We can interpret r as an absolute value of $\mathbb{C}$. The fact that multiplication works geometrically like this means $|zw| = |z||w|$ where $|a + bi| = \sqrt{a^2 + b^2}$.

Definition 19.3.2. *For $z \in \mathbb{Z}[i]$, define the norm of z.*

$$N(z) = |z|^2 = a^2 + b^2 \quad \text{if } z = a + bi$$

Note: $N(zw) = |zw|^2 = |z|^2|w|^2 = N(z)N(w)$

Let $z = a + bi, w = c + di$. then

$$\begin{aligned} zw &= (a+bi)(c+di) \\ &= (ac-bd) + (ad+bc)i \end{aligned}$$

Hence $N(zw) = (ac-bd)^2 + (ad+bc)^2$. On the other hand, $N(z)N(w) = (a^2+b^2)(c^2+d^2)$. We obtain the identity:

Theorem 19.3.0.2. *For any $a, b, c, d \in \mathbb{R}$, we have*

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

19.3.1 Back to units

Suppose u is a unit. Then there exists a unit v such that

$$uv = 1$$

Then

$$N(u)N(v) = N(1) = 1$$

Hence $N(u)$ and $N(v) = 1$. If $u = a + bi$ is a unit, then $a^2 + b^2 = 1$.
Solutions are $(a, b) = (1, 0), (-1, 0), (0, 1), (0, -1)$.
Each correspond to

$$\begin{aligned} (1,0) &\to 1 + 0i = 1 \\ (-1,0) &\to -1 + 0i = -1 \\ (0,1) &\to 0 + i = i \\ (0,-1) &\to o - i = -i \end{aligned}$$

So these are all the units. Unit circle.

19.4 Sum of 2 Squares

To answer which primes in $\mathbb{Z}$ are still prime in $\mathbb{Z}[i]$, we need to first answer the following:

Q: Which primes can be written as a sum of two squares?

$$\begin{aligned} p &= 3 \\ &= 5 = 1^2 + 2^2 \\ &= 7 \\ &= 11 \\ &= 13 = 2^2 + 3^2 \\ &= 17 = 1^2 + 4^2 \\ &= 19 \\ &= 23 \end{aligned}$$

Theorem 19.4.0.1. *If p is an odd prime and the sum of 2 squares, then $p \equiv 1 \pmod 4$.*

Proof. Suppose $p = a^2 + b^2$. then

$$\begin{aligned} a^2 + b^2 &\equiv 0 \pmod p \\ a^2 &\equiv -b^2 \pmod p \end{aligned}$$

Thus

$$\left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right)$$
$$1 = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot 1$$

Thus, $\left(\frac{-1}{p}\right) = 1$ so $p \equiv 1 \pmod 4$. □

In fact:

Theorem 19.4.0.2. *An odd prime p is the sum of two swuares iff $p \equiv 1 \pmod 4$.*

Proof (Fermat). Let $p \equiv 1 \pmod 4$. then

$$\left(\frac{-1}{p}\right) = 1$$

So there exists $a \in \mathbb{Z}$ such that $a^{\equiv} - 1 \pmod p$. Hence $a^2 + 1 = Mp$ for some $M \in \mathbb{Z}$. □

Lemma 2 (Fermat)**.** *If $Mp, M \geq 2$ can be written as a sum of two squares, then there exists $1 \leq m < M$ such that mp can be written as a sum of two squares.*

Example 19.4.0.1. $p = 881$

$$387^2 + 1^2 = 170 \cdot 881 \qquad (M = 170)$$

Reduce $\pmod M$ *to lie in* $\{\frac{-M}{2}, \frac{M}{2}\}$

$$387 \equiv 47 \pmod{170}$$
$$1 \equiv 1 \pmod{170}$$

Then

$$387^2 + 1^2 \equiv 0 \pmod{170}$$
$$47^2 + 1^2 \equiv 0 \pmod{170}$$

Note: $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$.
Multiply $387^2 + 1^2$ *and* $47^2 + 1^2$ *to get*

$$(387^2 + 1^2)(47^2 + 1^2) = (47 \cdot 387 + 1 \cdot 1)^2 + (1 \cdot 387 - 47 \cdot 1)^2 = (18190)^2 + (340)^2$$

But also

$$387^2 + 1^2 = 170 \cdot 881$$
$$47^2 + 1^2 = 170 \cdot 13$$

So

$$170^2 \cdot 13 \cdot 881 = 18190^2 + 340^2$$
$$13 \cdot 881 = 107^2 + 2^2$$

Keep doing this process and eventually you can write 881 as a sum of 2 squares.

Lecture 20

November 7, 2024

20.1 Last Time

Which primes can be written as the sum of 2 squares? Ans: $p = 2, p \equiv 1 \pmod 4$
If p is odd prime and $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$, then $a^2 \equiv -b^2 \pmod p$

$$\left(\frac{a^2}{p}\right) = \left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right)$$
$$1 = \left(\frac{-1}{p}\right) \longrightarrow p \equiv 1 \pmod 4$$

20.2 Sum of 2 Squares

Now suppose $p \equiv 1 \pmod 4$ want to write p as a sum of 2 squares. Use

$$(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA + uB)^2$$

20.2.1 Fermat's Method of Infinite Descent

Since $p \equiv 1 \pmod 4$, we have $\left(\frac{-1}{p}\right) = 1$
ie. $x^2 \equiv -1 \pmod p$ has a solution. ie. $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$
. $x^2 + 1^2 = kp$ is a sum of squares

Suppose now that $A^2 + B^2 = Mp$. We will conduct a smaller multiple of p that is a sum of squares.

Find integers u, v susch that

$$u \equiv A \pmod M$$
$$v \equiv B \pmod M$$

so that

$$-\frac{1}{2}M \leq u, v \leq \frac{1}{2}M$$

Thus $A^2 + B^2 \equiv u^2 + v^2 \equiv 0 \pmod M$
Thus

$$A^2 + B^2 = Mp$$
$$u^2 + v^2 = Mp$$

Then

$$
\begin{aligned}
(A^2+B^2)(u^2+v^2) &= M^2rp \\
(uA+vB)^2+(rA-uB)^2 &= M^2rp \\
uA+vB \equiv AA+BB \equiv A^2rB^2 &\equiv 0 \pmod{M} \\
vA-uB \equiv BA-AB &\equiv 0 \pmod{M} \\
(\frac{uA+vB}{M})^2+(\frac{vA-uB}{M})^2 &= rp
\end{aligned}
$$

20.2.2 Example

Choose $p = 13$.

$$\left(\frac{-1}{13}\right) = 1 \to x^2+1 = k \cdot 13 \to x = 5, k = 2$$

$$
\begin{aligned}
5^2+1^2 &= 2 \cdot 13 \\
5 &\equiv 1 \pmod{2} \\
1 &\equiv 1 \pmod{2} \\
1^2+1^2 &= 2 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
(5^2+1^2)(1^2+1^2) &= 2^2 \cdot 1 \cdot 13 \\
(5+1)^2+(5-1)^2 &= 2^2 \cdot 13 \\
\frac{5+1}{2}^2+\frac{5-1}{2}^2 &= 13 \\
3^2+2^2 &= 13
\end{aligned}
$$

20.3 Gaussian Integers

$$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$$

Primes sometimes factor in $\mathbb{Z}[i]$.
eg. $5 = (1+2i)(1-2i)$ but 3 is "prime" in $\mathbb{Z}[i]$

Suppose $p \equiv 1 \pmod{4}$. Then p can be written as $p = a^2+b^2$ for some $a, b \in \mathbb{Z}$ But then

$$p = a^2+b^2 = (a+bi)(a-bi)$$

Claim: Neither $a+bi$ nor $a-bi$ is a unit in $\mathbb{Z}[i](1,-1,i,-i)$. Hence p is composite in $\mathbb{Z}[i]$.

20.3.1 When is $a+bi \in \mathbb{Z}[i]$?

Prime is a Gaussian integer?

Ex: $\alpha = 1+2i$ is prime.
Suppose $\alpha = 1+2i = (a+bi)(c+di)$
Could write out (ac-bd)+(bc+ad)i

Another way? Use $N(a+bi) = a^2+b^2$. Then

$$
\begin{aligned}
N(1+2i) &= N(c+bi)N(c+di) \\
N &= (a^2+b^2)(c^2+d^2)
\end{aligned}
$$

WLOG

$$a^2+b^2=1 \rightarrow (a,b)=\begin{cases}(1,0),(ai)\\(-1,0),(a-i)\end{cases} \iff a+bi=\begin{cases}1,-1,\\i,-i\end{cases}$$

Corollary 20.3.1. *If $N(a+bi)=a^2+b^2$ is prime, then $a+bi$ is prime in $\mathbb{Z}[i]$*

Theorem 20.3.1.1 (Gaussian Primes)**.** *Let $\alpha=a+bi$.*

1. *If $\alpha\in\mathbb{Z}(b=0)$, then α is prime in $\mathbb{Z}[i]$ iff $\alpha=p$ is an odd prime with $p\equiv 3 \pmod 4$.*
2. *If $\alpha\in i\mathbb{Z}$ then α is $\ldots\alpha=ip\ldots p\equiv 3 \pmod 4$*
3. *If both a and b are nonzero, then α is prime in $\mathbb{Z}[i]$ iff $N(\alpha)$ is a prime in $\mathbb{Z}$.*

Ex. of 3: Suppose $N(\alpha)$ is even so $2\mid N(2)$. Claim: $(1+i)\mid\alpha$

Proof. WTS

$$\frac{a+bi}{1+i}\in\mathbb{Z}[i]$$

$$\frac{a+bi}{1+i}\frac{1-i}{1-i}=\frac{(a+b)+(b-a)i}{2}$$

Since a^2+b^2 is even, a,b are both even or both odd. So $a+b$ and $b-a$ are both even.

So

$$\frac{a+bi}{a+i}=\frac{a+b}{2}+\frac{b-a}{2}i\in\mathbb{Z}[i]$$

So, $(1+i\mid(a+bi))$. ∎

Lecture 21

November 12, 2024

21.1 Midterm 2

21.1.1 Question 1

1. g prim root of p, $d \nmid p-1 \longrightarrow g^d$ prim root $\gcd(d, p-1) = 1$. FALSE
2. if $\exists a, 1 \leq a \leq n-1$ s.t.
$$a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$$
then n is composite. TRUE
3. If $\gcd(a, n) = 1$, then $x^2 \equiv a \pmod{n}$ has e, then 0 or 2 incongruent solutions. FALSE
Example: $x^2 \equiv 1 \pmod{8}, x \equiv 1, 3, 5, 7$
4. If $\left(\frac{a}{n}\right) = -1$, then a is a NR of n. TRUE

21.1.2 Congruence solutions for $\left(\frac{3}{p}\right)$

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

1. if $p \equiv 1 \pmod{4}$, then
$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod{3} \\ -1 \text{ if } p \equiv 2 \pmod{3} \end{cases}$$
2. if $p \equiv 3 \pmod{4}$, then
$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} 1 \text{ if } p \equiv 2 \pmod{3} \\ -1 \text{ if } p \equiv 1 \pmod{3} \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 \\ -1 \end{cases}$$

21.1.3 $p, q = 2p + 1$ odd primes

WTS: -4 is a prime root of q.

$$\text{ord}(-4) \mid (q-1) = 2p \longrightarrow \text{ord}(-4) = 1, 2, p, \text{ or } 2p$$

Rule out $\mathrm{ord}(-4) = p$. Compute $(-4)^p = -4^{\frac{q-1}{2}} \equiv \left(\frac{-4}{q}\right) \pmod q$.

$$\left(\frac{-4}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{4}{q}\right) = \left(\frac{-1}{q}\right)$$

So if $\mathrm{ord}(-4) = p$, then $\left(\frac{-1}{q}\right) = 1$, so $q \equiv 1 \pmod 4$. But $q \equiv 3 \pmod 4$ since $q = 2p+1$, Sophie Germain

21.1.4

Let p be an odd prime, $(p-1) \nmid n$. Show $1^n + 2^n + \cdots + (p-1)^4 \equiv 0 \pmod p$. g = prim root.

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

in some order.

$$\longrightarrow 1^n + \cdots + (p-1)^n \equiv g^n + g^{2n} + \cdots + g^{(p-1)n} \pmod p$$

$$\begin{aligned}(g^n - 1)(g^{n(p-1)} + \cdots + g^n + 1) &= g^{np-1} \\ g^{n(p-1)} + \cdots + g^n &= \frac{g^{np}-1}{g^n-1} - 1 \\ &\equiv 0\end{aligned}$$

21.2 Cryptography Stuff

21.2.1 Remote Coin Flipping

Instead of H/T, we will use roots of $x^2 \equiv a \pmod n$ where $n = pq$.

Procedure:

1. Alice chooses 2 odd primes $p, q (p \equiv q \equiv 3 \pmod 4)$ and computes $n = pq$ and tells Bob n.
2. Bob choose randomly some $1 \le x \le n-1$, compute $a = x^2 \pmod n$ and tell Alice a.
3. Alice computes the square roots of $a \pmod n$, $\pm x_1$, $\pm x_2$ Choose either $\pm x_1$ or $\pm x_2$ (Heads or Tails), tell Bob $\pm x_1$ or $\pm x_2$.
4. If Bob's x is different from Alice's then, Bob can factor n.

$$\begin{gathered} x^2 \equiv 324 \pmod{391}, 391 = 17.23 \\ x^2 \equiv 324 \equiv 1 \pmod{17}, \quad x^2 \equiv 324 \equiv 2 \pmod{23} \\ x \equiv \pm 1 \pmod{17}, \quad x^2 \equiv 2 \pmod{23} \end{gathered}$$

If $p \equiv 3 \pmod 4$ and a is QR of p, then $x = a^{\frac{p+1}{4}}$ is a solution to $x \equiv a \pmod p$

Proof. $x^2 = (a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}} \equiv a \cdot 1 \equiv a \pmod p$
$x = 2^{\frac{23+1}{4}} = 2^6 = 64 \equiv -5$

Solutions are $x \equiv \pm 5 \pmod{23}$. $\to$ 4 systems.

$$\begin{aligned}
x \equiv 1 \pmod{17}, \quad x \equiv 5 \pmod{23} &\to x_1 \pmod{391} \\
x \equiv 1 \pmod{17}, \quad x \equiv -5 \pmod{23} &\to x_2 \pmod{391} \\
x \equiv -1 \pmod{17}, \quad x \equiv 5 \pmod{23} &\to -x_2 \pmod{391} \\
x \equiv -1 \pmod{17}, \quad x \equiv -5 \pmod{23} &\to x_1 \pmod{391}
\end{aligned}$$

$\square$

Back to (4), How does Bob factor n when he has knowledge of all 4 roots $\pm x_1, \pm x_2$ of a? Idea:

$$\begin{aligned}
x_1^2 \equiv a \equiv x_2^2 \pmod{pq} \\
\to pq \mid x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2) \\
p \mid (x_1 - x_2)(WLOG)
\end{aligned}$$

Then $q \nmid (x_1 - x_2)$, $pq = n \mid (x_1 - x_2)$ so $x_1 \equiv x_2 \pmod{n}$.

$\to$ Bob computes $\gcd(x_1 - x_2, n) = p$ or q.

Lecture 22

November 14, 2024

22.1 Recall: Arithmetic Functions

$$f : \mathbb{N} \to \mathbb{R}(\mathbb{C})$$

that have some "number theory" property.

Ex. $\phi =$ totient, $\sigma =$ divisor sum, $\tau =$ divisor count

Definition 22.1.1. *f is multiplicative if $f(ab) = f(a)f(b)$ whenever $\gcd(a, b) = 1$.*

We can express

$$\tau(n) = \sum_{d|n} 1$$

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

Ex. $n = 12$, $\sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6)f(12)$

Conversely, given arithmetic function f we can define $F(n) = \sum_{d|n} f(d)$

Recall

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

Theorem 22.1.0.1. *Let $n = p_1^{e_1} \dots p_r^{e_r}$, then*

1. $\tau(n) = (e_1 + 1)(e_2 + 1) \dots (e_r + 1)$
2. $\sigma(n) = \frac{p_1^{e_1+1}-1}{p_1-1} + \cdots + \frac{p_r^{e_r+1}-1}{p_r-1}$
3. $\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \dots (p_r^{e_r} - p_r^{e_r-1})$

$$\begin{aligned} \sigma(p^e) &= (1 + p + p^2 + \cdots + p^{e-1} + p^e) \\ &= \frac{p^{e+1} - 1}{p - 1} \end{aligned}$$

If $d \mid n = p_1^{e_1} - p_r^{e_r}$, then $d = p_1^{k_1} \dots p_r^{k_r}$ where $0 \leq k_i \leq e_i$

Theorem 22.1.0.2. *If f is multiplicative, then*

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

is multiplicative.

Corollary 22.1.1. *$\tau(n)$, $\sigma(n)$ are multiplicative.*

Theorem 22.1.0.3. *If F is multiplicative, then f is multiplicative.*

22.2 Mobius Function

Let n be a positive integer.

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n = \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 \dots p_r \text{ distinct primes} \end{cases}$$

Ex. $\mu(2) = -1, \quad \mu(p) = -1, \quad \mu(12) = 0, \quad \mu(6) = 1$

Theorem 22.2.0.1. *μ is multiplicative.*

Proof. Let $\gcd(a, b) = 1$. If for some prime p we have $p^2 \mid a$ or $p^2 \mid b$, then $p^2 \mid ab$, so $\mu(a)\mu(b) = 0 = \mu(ab)$.

Now suppose $a = p_1 \dots p_r, \quad b = q_1 \dots q_k$ are square-free. then

$$\begin{aligned} \mu(ab) &= \mu(p_1 \dots p_r q_1 \dots q_k) \\ &= (-1)^{r+k} \\ &= (-1)^r(-1)^k \\ &= \mu(a)\mu(b) \end{aligned}$$

$n = \sum_{d|n} f(d)$, what is $f(d)$? $f(d) = \phi(d)$.

$$F(n) = \sum_{d|n} f(d) = \begin{cases} 1 & n = 1 \\ 0 & \text{otherwise} \end{cases}$$

What is $F(n) = \sum_{d|n} \mu(d)$?

Ex. $F(10) = \sum_{d|10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10) = 1 - 1 - 1 + 1 = 0$.

Ex. $F(12) = \sum_{d|12} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) = 1 - 1 - 1 + 0 + 1 + 0 = 0$.

□

Theorem 22.2.0.2. *Let $F(n) = \sum_{d|n} \mu(d)$. Then*

$$F(n) = \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{if } n > 1 \end{cases}$$

Proof. We have that F is multiplicative. Since μ is multiplicative, let us compute

$$F(p^k) = \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^k) = 1 - 1 + 0 + \dots + 0 = 0$$

If $n = p_1^{e_1} \dots p_r^{e_r}$, then $F(n) = F(p_1^{e_1}) \dots F(p_r^{e_r}) = 0$ □

22.2.1 Mobius Inversion Formula

Theorem 22.2.1.1 (Mobius Inversion Formula)**.** *Let* $F(n) = \sum_{d|n} f(d)$*. Then*

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

(Idea). Use $n = 10$.

$$\begin{aligned}
\sum_{d|10} \mu(d) F(\frac{10}{d}) &= \sum_{d|10} (\mu(d) \sum_{c|\frac{10}{d}} f(c)) \\
&= \mu(1)(f(1) + f(2) + f(5) + f(10)) \\
&\quad + \mu(2)(f(1) + f(5)) \\
&\quad + \mu(5)(f(1) + f(2)) \\
&\quad + \mu(10)(f(1)) \\
&= f(1)(\mu(1) + \mu(2) + \mu(5) + \mu(10)) \\
&\quad + f(2)(\mu(1) + \mu(5)) \\
&\quad + f(5)(\mu(1) + \mu(2)) \\
&\quad + f(10)(\mu(1)) \\
&= \sum_{d|10} f(d)(\sum_{c|\frac{10}{d}} \mu(c))
\end{aligned}$$

$$\begin{aligned}
\sum_{d|n} \mu(d) F(\frac{n}{d}) &= \sum_{d|n} (\mu(d) \sum_{c|\frac{n}{d}} f(c)) \\
&= \sum_{d|n} (f(d) \sum_{c|\frac{n}{d}} \mu(c)) = \begin{cases} 0 & \text{if } \frac{n}{d} > 1 \\ 1 & \text{if } n = d \end{cases} \\
&= \sum_{d=n} f(d) \sum_{d|1} \mu(c) \\
&= f(n)
\end{aligned}$$

To be more precise:

$$\begin{aligned}
&\sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c) \\
&\qquad = \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c) \\
&\qquad = \sum_{d|n, c|\frac{n}{d}} \mu(d) f(c) \\
&\qquad = \sum_{c|n, d|\frac{n}{c}} \mu(d) f(c)
\end{aligned}$$

$\square$

Ex:

$$\begin{aligned}
\tau(n) &= \sum_{d|n} 1 \\
\rightarrow 1 &= \sum_{d|n} \mu(\frac{n}{d})\tau(d) \\
\sigma(n) &= \sum_{d|n} d \\
n = \sum_{d|n} \mu(\frac{n}{d})\sigma(d)(&= \sum_{d|n} \phi(d))
\end{aligned}$$

Lecture 23

November 19, 2024

23.1 Diophantine Equations

Ex:

- Linear $ax + by = c$
- $x^2 + y^2 = p$ (solvable when $p \equiv 1 \pmod 4$) "Easy" for any particular p by brute force bc finitely many possibilities
- $x^2 - y^2 = 1$ infinitely many possibilities $(x+y)(x-y) = 1 \longrightarrow (x+y) \mid 2$ and $(x-y) \mid 2 = (1,0), (-1,0)$
- $x^2 - 2y^2 = 1$ has soln $(x, y) = (3, 2)$

In general, $x^2 - Dy^2 = 1$ is called Pell's Equation. How to find integer solutions?

23.2 Diophantine Approximation

How to approximate irrational numbers by rational numbers in the "best" way

Ex: $\pi \approx \frac{22}{7}$ is the best approximation among all rational numbers with denominator ≤ 7 (much bigger actually)

23.3 Continued Fractions

Definition 23.3.1. *A (simple) finite continued fraction is a rational number expressed as*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

where $a_i \in \mathbb{Z}, a_i > 0$ for $i \geq 1$.

Ex.

$$\begin{aligned}\frac{43}{19} &= 2+\frac{5}{19}\\ &= 2+\frac{1}{\frac{19}{5}}\\ &= 2+\frac{1}{3+\frac{4}{5}}\\ &= 2+\frac{1}{3+\frac{1}{\frac{5}{4}}}\\ &= 2+\frac{1}{3+\frac{1}{1+\frac{1}{4}}}\end{aligned}$$

Notice: Euclidean Algorithm uses a_i values from continued fraction

$$\begin{aligned}43 &= 19(2)+5\\ 19 &= 5(3)+4\\ 5 &= 4(1)+1\\ 4 &= 1(4)\end{aligned}$$

<u>Notation</u>:

$$= [2;3,1,4]$$

Theorem 23.3.0.1. *Every rational number has a continued fraction representation.*

Proof. Eucliean Algorith applied to $\frac{a}{b}$ gives

$$\begin{aligned}a &= a_0b+r_1\\ b &= a_1r_1+r_2\\ r_1 &= a_2r_2+r_3\\ &\dots\\ r_{n-1} &= a_nr_n\\ \frac{a}{b} &= a_0+\frac{r_1}{b} = a_0+\frac{1}{\frac{b}{r_1}}\\ \frac{b}{r_1} &= a_1+\frac{r_2}{r_1}\\ &\to \frac{a}{b} = a_0+\frac{1}{a_1+\frac{r_2}{r_1}}\dots\end{aligned}$$

By continuity, we obtain continued fraction. $\square$

Definition 23.3.2. *An <u>infinite</u> continued fraction is an expression of the form*

$$[a_o;a_1,a_2,\dots] = a_0+\frac{1}{a_1+\frac{1}{a_2+\frac{1}{a_3+\dots}}}$$

$a_i \in \mathbb{Z}, a_i > 0$ *for* $i \geq 1$.

<u>Ex</u>: π

$$\pi = 3+\frac{1}{\frac{1}{0.14159}} = 3+\frac{1}{7+\frac{1}{15+\frac{1}{1+\frac{1}{\dots}}}}$$

No obvious pattern...

Ex: e

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \frac{1}{\cdots}}}}}}}}}} = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \dots]$$

Ex: $[1; 1, 1, 1, 1, \dots] = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$

Let $x = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$

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

$$x^2 - x - 1 = 0 \quad \to \quad x = \frac{1 + \sqrt{5}}{2} = \phi$$

(Golden rule)

Theorem 23.3.0.2. ...

1. *A continued fraction is infinite iff it represents an irrational number*
2. *The continued fraction represenation of an irrational number is unique*
3. *A rational number has exactly two continued fraction representations:*

$$[a_o; a_1, \dots, a_n] = [a_0; a_1, \dots, a_{n-1}, 1] \quad \textit{where} \quad a_n \neq 1$$

Definition 23.3.3. *The* $\underline{k^{th}\ \textit{convergent}}$ *of* $[a_0; a_1, a_2, \dots]$ *is*

$$C_k = [a_0; a_1, a_2, \dots, a_k]$$

Ex: For $\pi = [3; 7, 15, 1, \dots]$

$$C_0 = 3$$
$$C_1 = 3 + \frac{1}{7} = \frac{22}{7}$$
$$C_2 = 3 + \frac{1}{7 + \frac{1}{15}} = \dots$$

Ex: $\frac{19}{51} = [0; 2, 1, 2, 6]$

$$= 0 + \cfrac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}}}$$

$$C_0 = 0$$
$$C_1 = 0 + \frac{1}{2} = \frac{1}{2}$$
$$C_2 = 0 + \frac{1}{2 + \frac{1}{1}} = \frac{1}{3}$$
$$C_3 = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}} = \frac{3}{8}$$
$$C_4 = \frac{19}{51}$$

$$\begin{array}{llll} & & a_i & \\ C_0 & 0 & 0 & \\ C_1 & \frac{1}{2} & 2 & \\ C_2 & \frac{1}{3} & 1 & 51 = 8 * 6 + 3 \\ C_3 & \frac{3}{8} & 2 & \\ C_4 & \frac{19}{51} & 6 & \end{array}$$

Define:

$$p_0 = a_0, q_0 = 1$$
$$p_1 = a_1 a_0 + 1, q_1 = a_1$$
$$p_k = a_k p_{k_1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2}$$

Theorem 23.3.0.3. $C_k = \frac{p_k}{q_k}$

Proof by Induction. Base case for $k = 0$:

$$C_0 = a_0 = \frac{a_0}{1} = \frac{p_0}{q_0}$$

Base case for $k = 1$:

$$C_1 = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1} = \frac{p_1}{q_1}$$

Inductive step: Assume $C_k = \frac{p_k}{q_k}$ for some $k \geq 2$. WTS: $C_{k+1} = \frac{p_{k+1}}{q_{k+1}}$.

$$C_{k+1} = [a_0; a_1, \ldots, a_k, a_{k+1}] = [a_0; a_1, \ldots, a_k, \frac{1}{a_{k+1}}]$$

is a continued function of length k.

$$\begin{aligned} C_{k+1} &= \frac{(a_k + \frac{1}{a_k+1})p_{k+1} + p_{k+2}}{(a_k + \frac{1}{a_k+1})q_{k+1} + q_{k+2}} \\ &= \frac{(a_k + \frac{1}{a_k+1})p_{k+1} + p_{k+2}}{(a_k + \frac{1}{a_k+1})q_{k+1} + q_{k+2}} \\ &= \frac{p_k + 1}{q_k + 1} \end{aligned}$$

□

Lecture 24

November 21, 2024

24.1 Recall: Continued Fractions

pi example:

$$\begin{aligned}
\pi &= [3; 7, 15, 1, 292, \dots] \\
C_0 &= 3, C1 = \frac{22}{7}, \\
C_2 &= \frac{333}{106}, C_3 = \frac{355}{113}, \\
C_4 &= \frac{103993}{33102}
\end{aligned}$$

Continued Fractions

$$[a_0; a_1, a_2, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

nth convergent:

$$C_n = [a_0; a_1, a_2, \dots, a_n]$$

Theorem 24.1.0.1.

$$\begin{aligned}
&p_0 = a_0, q_0 = 1, \\
&p_1 = a_1 a_0 + 1, q_1 = a_1, \\
&p_n = a_n p_{n_1} + p_{n-2}, q_n = a_n q_{n-1} + q_{n-2}
\end{aligned}$$

Then,

$$C_n = \frac{p_n}{q_n}$$

<u>Ex</u>: $\quad e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \dots]$

$$\begin{aligned}
C_0 &= \frac{p_0}{q_0} = \frac{a_0}{1} = 2 \\
C_1 &= \frac{p_1}{q_1} = \frac{a_1 a_0 + 1}{a_1} = \frac{2 \cdot 2 + 1}{1} = \frac{3}{1} \\
C_2 &= \frac{2 \cdot p_1 + p_0}{2 \cdot q_1 + q_0} = \frac{2 \cdot 3 + 2}{2 \cdot 1 + 1} = \frac{8}{3} \\
C_3 &= \frac{1 \cdot 8 + 3}{1 \cdot 3 + 1} = \frac{11}{4}
\end{aligned}$$

Theorem 24.1.0.2.

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1} \quad (p_{k+1} q_k - q_{k+1} p_k = (-1)^k)$$

Proof. Base case: $k = 1$

$$p_1 q_0 = q_1 p_0 = (a_1 a_0 + 1)(1) - (a_1)(a_0) = 1 = (-1)^0$$

Now assume for induction that

$$p_m q_{m-1} - q_m p_{m-1} = (-1)^{m-1}$$

Now consider

$$\begin{aligned} p_{m+1} q_m - q_{m+1} p_m &= (a_{m+1} p_m + p_{m-1}) q_m - (a_{m+1} q_m + q_{m-1}) p_m \\ &= a_m + p_m q_m + p_{m+1} q_m - a_{m+1} q_m p_m - q_{m-1} p_m \\ &= -(p_m q_{m-1} - q_m p_{m-1}) \\ &= -(-1)^{m-1} = (-1)^m \end{aligned}$$

□

<u>Note</u>: This says that

$$p_k x + q_k y = \pm 1$$

has an integer solution.

So Bezout $\to \gcd(p_k, q_k = 1)$

Corollary 24.1.1. $C_k = \frac{p_k}{q_k}$ *is in lowest terms.*

Corollary 24.1.2. $C_{k+1} - C_k = \frac{(-1)^k}{q_k q_{k+1}}$

Proof.

$$\begin{aligned} C_{k+1} - C_k &= \frac{p_{k+1}}{q_{k+1}} \\ &= \frac{p_{k+1} q_k - q_{k+1} p_k}{q_{k+1} q_k} \\ &= \frac{(-1)^k}{q_{k+1} q_k} \end{aligned}$$

□

Note: The relation $q_k = a_k q_{k-1} + q_{k-2}$ implies that $0 < q_o \leq q_1 < q_2 < q_3 < \ldots$

Corollary 24.1.3. *All infinite (simple) continued fractions converge.*

Theorem 24.1.0.3. ...

- $C_0 < C_2 < C_4 < \ldots$
- $C_1 > C_3 > C_5 > \ldots$

Proof.

$$\begin{aligned} C_{k+2} - C_k &= (C_{k+2} - C_{k+1}) + (C_{k+1} - C_k) \\ &= \frac{(-1)^{k+1}}{q_{k+2} q_{k+1}} + \frac{(-1)^k}{q_{k+1} q_k} \\ &= \frac{(-1)^k (q_{k_2} - q_k)}{q_{k+2} q_{k+1} q_k} \end{aligned}$$

□

Theorem 24.1.0.4 (Dirichlet's Approximation). *Let x be irrational. Then there exist infinitely many $\frac{a}{b} \in \mathbb{Q}$ $\quad(\gcd(a,b)=1)$ such that*

$$|x - \frac{a}{b}| < \frac{1}{b^2}$$

Proof. Let $x = [a_0; a_1, \dots]$

We want to bound $|x - C_k|$.

$$\begin{aligned} |x - C_k| &\leq |C_{k+1} - C_k| \\ &= |\frac{(-1)^k}{q_{k+1}q_k}| \\ &= \frac{1}{q_{k+1}q_k} \\ &< \frac{1}{q_k^2} \end{aligned}$$

bc $q_{k+1} > q_k$. ☐

<u>Remark</u>: (Thue-Siegel-Roth Theorem)

If $\alpha > 2$ then there exist at most finitely many $\frac{a}{b} \in \mathbb{C}$ $\quad(\gcd(\frac{a}{b}) = 1)$ such that

$$|x - \frac{a}{b}| < \frac{1}{b^\alpha}$$

Theorem 24.1.0.5. *$C_k = \frac{p_k}{q_k}$ approximates x "the best" in the sense that if $1 \leq b \leq q_k$, then*

$$|x - \frac{p_k}{q_k}| \leq |x - \frac{a}{b}|$$

for any $a \in \mathbb{Z}$.

Lemma 3. *If $\frac{a}{b} \in \mathbb{Q}$ with $1 \leq b \leq q_k$, then*

$$|q_k x - p_k| \leq |bx - a|$$

Proof. Consider the system of equations

$$\begin{aligned} p_k\alpha + p_{k+1}\beta &= a \\ q_k\alpha + q_{k+1}\beta &= b \end{aligned}$$

has a solution iff

$$det \begin{bmatrix} p_k & p_{k+1} \\ q_k & q_{k+1} \end{bmatrix} \neq 0$$

has an integer solution iff

$$det \begin{bmatrix} p_k & p_{k+1} \\ q_k & q_{k+1} \end{bmatrix} = \pm 1$$

☐

Hence 7 integer solutions α, β

Details:

- $\alpha \neq 0$
- $\beta = 0$ then Thm is true.

Now assume both $\alpha, \beta \neq 0$. We want to show that α and β have opposite signs.

Why?

If $\beta < 0$, then $q_k\alpha = b - q_{k+1}\beta$

If $\beta > 0$, then same equations shows $\alpha < 0$.

Thus,

$$\begin{aligned}|bx - a| &= |(q_k\alpha + q_{k+1}\beta)x - (p_k\alpha + p_{k+1}\beta)\\ &= |\alpha(q_kx - p_k) + \beta(q_{k+1}x - p_{k+1})|\end{aligned}$$

If $q_kx - p_k > 0$, then $x - \frac{p_k}{q_k} > 0 \to x - \frac{p_{k+1}}{q_{k+1}} < 0$, then $\alpha(q_kx - p_k)$ and $\beta(q_{k+1}x - p_{k+1})$ have the same sign, so

$$\begin{aligned}&= |\alpha(q_kx - p_k)| + |\beta(q_{k+1}x - p_{k+1})|\\ &\geq |\alpha||q_kx - p_k|\\ &\geq |q_kx - p_k|\end{aligned}$$

Proof Thm. If $1 \leq b \leq q_k$, then $\frac{a}{b}$ satisfies $|x - \frac{p_k}{q_k}| < |x - \frac{a}{b}|$

Suppose $|x - \frac{p_k}{q_k}| > |x - \frac{a}{b}|$. Then

$$|q_kx - p_k > q_k||x - \frac{a}{b}|$$

But by the technical result,

$$|bx - a| > q_k|x - \frac{a}{b}| \geq b|x - \frac{a}{b}|$$

□

Lecture 25

December 3, 2024

25.1 Continue continued fractions

If α is irrational, there exist unique infinite continued fraction expansion

$$\alpha = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \dots}}}} = [a_0; a_1, a_2, \dots] \quad \text{where } a_j \in \mathbb{Z}, a_i > 0, i \geq 1$$

Convergent $C_k = [a_0; a_1, \dots, a_k]$

Theorem 25.1.0.1. *Define*

$$\begin{aligned} &p_0 = a_0, \quad q_0 = 1 \\ &p_1 = a_0 a_1 + 1, \quad q_1 = a_1 \\ &p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2} \end{aligned}$$

Then $C_n = \frac{p_n}{q_n}$ for all n.

Prop:

$$|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = |\frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}}| = \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

since $q_0 < q_1 < q_2 < \dots$

$$\to |\alpha - \frac{p_n}{q_n}| < \frac{1}{q_{n+1} q_n} < \frac{1}{q_n^2}$$

Theorem 25.1.0.2. *If $1 \leq b < q_n$, then*

$$|\alpha - \frac{p_n}{q_n}| < |\alpha - \frac{a}{b}|$$

(follows from the "struggle lemma")

Lemma 4. *If $1 \leq b < q_{n+1}$, then*

$$|q_n \alpha - p_n| < |b\alpha - a|$$

Lecture 26

December 5, 2024

26.1 Square-triangular numbers

$$1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, \ldots$$

Each number is $1 + 2 + 3 + \ldots$

$$T_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

$$T_49 = 1225 = 35^2$$

1225 is a square-triangular number

Q: Are there infinitely many square-triangular numbers? YES!

A **square-triangular number** must satisfy

$$n^2 = \frac{m(m+1)}{2} \quad \text{for some pos integers } m, n$$

$$\begin{aligned} 2n^2 &= m^2 + m \\ 8n^2 &= (2m+1)^2 - 1 \\ (2m+1)^2 - 8n^2 &= 1 \end{aligned}$$

Let $x = 2m + 1$, $y = 2n$.

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

(Pell's Equation)

Find the fundamental solution by computing the components of $\sqrt{2}$.

$$\sqrt{2} = [1; \overline{2}]$$

Convergents: $\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \ldots$

$$\begin{aligned} (x = 1, y = 1) &\quad 1^2 - 2 \cdot 1^2 = -1 \\ (x = 3, y = 2) &\quad 3^2 - 2 \cdot 2^2 = 1 \end{aligned}$$

So $x = 3, y = 2$ is the fundamental solution.

$\leftrightarrow m = 1, n = 1$ corresponds to the square-triangular number $T_1 = 2^2 = 1$

Recall: Every other positive solution is of the form x_n, y_n,

$$x_n = y_n\sqrt{2} = (3 + 2\sqrt{2})^n$$

Ex:

$$
\begin{aligned}
(3+2\sqrt{2})^2 &= 9+8+12\sqrt{2} \\
&= 17+12\sqrt{2} \\
\to m = \frac{17-1}{8}, n = \frac{12}{2} = 6 & \\
\leftrightarrow T_8 = 6^2 = 36 &
\end{aligned}
$$

Ex:

$$
\begin{aligned}
(3+2\sqrt{2})^3 &= (3+2\sqrt{2})(17+12\sqrt{2}) \\
&= 99+70\sqrt{2} \\
\to m = 49, n = 35 & \\
T_{49} = 35^2 = 1225 &
\end{aligned}
$$

26.2 Square-pyramid numbers

"Stacking cannonballs"

$$9+4+1$$

(Sum of consecutive squares)

When is

$$1^2+2^2+\cdots+m^2 = n^2?$$

$$1^2+2^2+\cdots+24^2 \quad \text{is a square}$$

26.3 Wiener's attack on RSA

26.3.1 RSA Recap

Pick two primes p, q, compute $n = pq$.

$$\phi(n) = (p-1)(q-1) = n-p-q+1$$

Choose E, D such that

$$ED = 1 \pmod{\phi(n)}$$

→ Public key (n, E) → Encode $Z \to Z^E \pmod{n}$
→ Private key (n, D) → Decode $W \to W^D \pmod{n}$

26.3.2 Attack Theorem

Theorem 26.3.2.1. *If $D < 3n^{\frac{1}{4}}$, then it is possible to efficiently recover D (and factor n) only given the public key (n, E).*

Ex: If n has 1024 binary digits, then you must have D at least around 256 binary digits long

Proof. Since $DE = 1 \pmod{\phi(n)}$, we have

$$DE = 1 + k\phi(n) \quad \text{for some } k$$

$$|DE - k\phi(n)| = 1$$
$$|\frac{E}{\phi(n) - \frac{k}{D}} = \frac{1}{D\phi(n)}$$
$$\to \frac{k}{D} \text{ approximates } \frac{E}{\phi(n)}$$

□

Idea: $\phi(n)$ is "close" to n.

Now $\phi(n) = n - p - q + 1$.

$$|n - \phi(n)| = p + q - 1 < 3\sqrt{n}$$

Bound

$$\begin{aligned}
|\frac{E}{n} - \frac{k}{D}| &= |\frac{ED - kn}{nD}| \\
&= |\frac{ED = k\phi(n) - kn + k\phi(n)}{nD}| \\
&= |\frac{1 - k(n - \phi(n))}{nD}| \\
&= \frac{1}{nD} + \frac{k(n - phi(n))}{nD} \leq \frac{k(n - \phi(n))}{nD}
\end{aligned}$$

$$\begin{aligned}
|\frac{E}{n} - \frac{k}{D}| &< \frac{k(n - \phi(n))}{nD} \\
&< \frac{3}{k}\sqrt{n}D < \frac{3D}{\sqrt{n}D}
\end{aligned}$$

Claim: $k < D$

Proof of Claim.

$$k\phi(n) = DE - 1 < DE$$

On the other hand, $E < \phi(n)$. □

Assume $D < \frac{1}{3}n^{\frac{1}{4}}$. Now use

$$D < \frac{1}{3}n^{\frac{1}{4}}$$
$$D^2 < \frac{1}{9}\sqrt{n}$$
$$\frac{1}{D^2} > \frac{9}{\sqrt{n}}$$

Hence

$$|\frac{E}{n} - \frac{k}{D}| < \frac{3}{\sqrt{n}} < \frac{3}{9D^2} = \frac{1}{3D^2} < \frac{1}{2D^2}$$

By thm from last time, $\frac{k}{D}$ must be a convergent of $\frac{E}{n}$. In fact, $\gcd(k, D) = 1$ and convergents are always in lowest terms.

Ex: $n = 101.107 = 10807$.

$\phi(n) = 10600, D = 3, E = 7067$.

Public key: $(10807, 7067)$

$\frac{E}{n} = \frac{7067}{10807} = [0; 1, 1, 1, 8, 17, 1, 2, 2]$

Convergents: $\frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{17}{26}$

$3 \cdot 7067 = 2; 10600 + 1$

$$(x-p)(x-q) = x^2 - (p+q)x + n$$

26.4 Final

Exam is cumulative

Half is from this unit (material from homeworks; same topics)

1 sheet of paper cheat sheet

Need a calculator