M3200

Recitation Notes 9/20

Today: Euclidean algorithm and prime numbers and modular arithmetic

Warm up: 1) if $a|b$, what is $\gcd(a,b)$? a

2) when is $a \equiv b \bmod 2$? mod 1? mod 0?
same parity | always | iff $a=b$

HW1 Review (pre-images)

Let $f: A \to B$ be a fn and $P \subseteq B$. Then $f^{-1}(P) = \{a \in A \mid f(a) \in P\}$

Rmks. (1) f^{-1} is not a function (f^{-1} is fn $\iff$ f is bijective)

(2) Arbitrary elmt of $f^{-1}(P)$ is not of the form $f^{-1}(x)$, since

$$f^{-1}(x) = f^{-1}(\{x\}) = \{a \in A \mid f(a) = x\} \text{ is a subset of } A.$$

Better: Let $y \in f^{-1}(P)$. Then by defn $f(y) = x \in P$. Then...

Exs from HW1

3(4) Let $f: A \to B$ and $P, Q \subseteq B$. Show $f^{-1}(P \setminus Q) = f^{-1}(P) \setminus f^{-1}(Q)$.

Pf (just $\supseteq$)/ Let $x \in f^{-1}(P) \setminus f^{-1}(Q)$, so $x \in f^{-1}(P)$ and $x \notin f^{-1}(Q)$. By defn of pre-image, $f(x) = y \in P$ and $f(x) = y \notin Q$. Thus $y \in P \setminus Q$, so by defn of pre-image $x \in f^{-1}(P \setminus Q)$. Therefore $f^{-1}(P) \setminus f^{-1}(Q) \subseteq f^{-1}(P \setminus Q)$.

4(1) Let $f: A \to B$ and Suppose $P \subseteq A$ and $Q \subseteq B$. Show $P \supseteq f^{-1}(f(P))$ if f is injective.

Pf/ Let $x \in f^{-1}(f(P))$. By defn, this means $f(x) \in f(P)$. Say $f(x) = y$, so $y \in f(P)$. By defn of image, there exists $x' \in P$ s.t. $f(x') = y$. Since $f(x) = f(x')$, injectivity of f implies $x = x'$. So $x \in P$. Hence $f^{-1}(f(P)) \subseteq P$.

Lecture review:
- Divisibility
  - ↳ prime factorization
  - ↳ gcd + Euclid's algorithm
- Modular arithmetic
  - ↳ invertibility

Recall: $a|b$ if $\exists m \in \mathbb{Z}$ s.t. $b = am$. More generally, can always write $b = qa + r$ for some unique $q, r \in \mathbb{Z}$ s.t. $0 \le r < a$.

Ex. (transitivity) For all $a,b,c \in \mathbb{Z}$, if $a|b$ and $b|c$ then $a|c$.

Pf/ Since $a|b$, $b = ma$ for some $m \in \mathbb{Z}$, and since $b|c$, $c = m'b$ for some $m' \in \mathbb{Z}$. Then

$$c = m'b = m'(ma) = (m'm)a$$

so $a|c$ as well. □

Some open problems
- Twin prime conjecture: $\exists$ infinitely many pairs of primes $(p, p+2)$
- There is always a prime btwn 2 consecutive squares
- Goldbach's conjecture: $\forall 2n \in \mathbb{Z}_{>2}$ can be written as a sum of 2 primes ... (Rmk: $\exists$ counterpt for odd integers, proved in 1930's)

Recall:
- $p \in \mathbb{Z}$ is prime if $a|p \Rightarrow a = 1$ or p. Otherwise, composite (except 0, 1).
- Every $n \in \mathbb{Z}$ has a unique (up to ordering) prime factorization

Thm $\sqrt{2}$ is irrational

Pf/ Suppose for contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$. Squaring + rearranging, we get $2b^2 = a^2$. This implies $2b^2$ and a^2 have the same prime factorization. But now consider the prime factorization of a, b: $a = 2^m p_1^{e_1} \cdots p_k^{e_k}$, $b = 2^n q_1^{f_1} \cdots q_j^{f_j}$.

This implies the exponent of 2 in the prime factorizations of a^2 and $2b^2$ are $2m$ and $2n+1$, respectively. This is a contradiction, since $2m$ is even but $2n+1$ is odd. □

Q. How do we decide if a given number is prime? How do we find the prime factorization of a number?

(One) A. Euclid's Algorithm! Computes gcd

Recall: $\gcd(a,b) = d \in \mathbb{Z}$ s.t. (i) $d|a$ and $d|b$; (ii) if d' satisfies (i) then $d'|d$.

e.g. $\gcd(2,6) = 2$, $\gcd(4,6) = 2$, $\gcd(5,6) = 1$

- $a, b \in \mathbb{Z}$ are relatively prime if $\gcd(a,b) = 1$.

Note Can also define the least common multiple $\text{lcm}(a,b) = n$ s.t. (i) $a|n$ and $b|n$; (ii) if n' satisfies (i) then $n|n'$.

e.g. $\text{lcm}(2,6) = 6$, $\text{lcm}(4,6) = 12$, $\text{lcm}(5,6) = 30$.

Exs

1. Use Euclid's algorithm to compute $\gcd(45, 16)$:

1. $45 = 16 \cdot 2 + 13$
2. $16 = 13 \cdot 1 + 3$
3. $13 = 3 \cdot 4 + 1$
4. $3 = 1 \cdot 3 + 0$

$\Rightarrow \gcd(45,16) = 1.$

Note: $45 = 3^2 5$
$16 = 2^4$

Reverse E.A. to write $1 = 45 \cdot x + 16 \cdot y$: $x, y \in \mathbb{Z}$

$1 \overset{(3)}{=} 13 - 3 \cdot 4$
$\overset{(2)}{=} 13 - (16 - 13 \cdot 1) \cdot 4$
$= 13 - 16 \cdot 4 + 13 \cdot 4$
$= 13 \cdot 5 - 16 \cdot 4$
$\overset{(1)}{=} (45 - 16 \cdot 2) \cdot 5 - 16 \cdot 4$
$= 45 \cdot 5 - 16 \cdot 10 - 16 \cdot 4$
$= 45 \cdot 5 + 16 \cdot (-14)$

So $x = 5$ and $y = -14$.

2. $\gcd(300, 18)$ ⇝ Write $6 = x \cdot 300 + y \cdot 18$

$300 = 18 \cdot 16 + 12$
$18 = 12 \cdot 1 + 6$
$12 = 6 \cdot 2 + 0 \Rightarrow 6$ is gcd

$6 = 18 - 12 \cdot 1$
$= 18 - (300 - 18 \cdot 16) \cdot 1$
$= 18 - 300 + 18 \cdot 16$
$= (-1) \cdot 300 + (17) \cdot 18$

So $x = -1$ and $y = 17$.

~ break ~

Modular arithmetic

Recall: • $a \equiv b \pmod n$ if $n \mid (a-b)$ $\iff$ a and b have the same remainder when divided by n.

• Quotient $\mathbb{Z}/n$ has operations + and • which are "nice"

Ex. Compute $2^{2022} \pmod 5$:

$505 \cdot 4 = 2020$

Note $2^4 = 16 \equiv 1 \pmod 5$. Since $2022 = 4 \cdot 505 + 2$,

$2^{2022} = 2^{4 \cdot 505 + 2} = (2^4)^{505} 2^2$
$\equiv (1)^{505} 2^2 \pmod 5$
$= 2^2 = 4$

So $2^{2022} \equiv 4 \pmod 5$.

Invertibility (aka division is difficult)

Recall: • An inverse of $[a] \in \mathbb{Z}/n$ is $[b] \in \mathbb{Z}/n$ s.t. $[a][b] = [1]$.

• $[a]^{-1}$ exists $\iff \gcd(a,n) = 1$; & if it exists, it's unique.

Non/ex: $\mathbb{Z}/4$

- 2 is not invertible
- 3 is $[3]^{-1} = [3]$.

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

This is ok for small n.
For large n, use EA:

$$\gcd(a,n) = a\cdot x + n\cdot y \equiv a\cdot x \pmod{n}$$
$$\| \quad \Rightarrow [x]=[a]^{-1} \text{ in } \mathbb{Z}/n$$
$$1$$

Ex. Solve $[7]x+[3]=[0]$ in $\mathbb{Z}/47$.

Soln. Rewrite this as $7x+3 \equiv 0 \pmod{47}$, and rearrange (using the well-defn'd operations in $\mathbb{Z}/47$):

$$7x \equiv -3 \pmod{47}$$
$$\hookrightarrow \text{or } 44$$

To find $[7]^{-1}$, use the EA to find $\gcd(7,47)$:

$$47 = 7\cdot 6 + 5$$
$$7 = 5\cdot 1 + 2$$
$$5 = 2\cdot 2 + 1$$

which means $\gcd(7,47)=1$, hence $[7]^{-1}$ exists. Moreover, we can compute

$$\begin{aligned} 1 &= 5 - 2\cdot 2 \\ &= 5 - 2\cdot(7-5) \\ &= 3\cdot 5 - 2\cdot 7 \\ &= 3\cdot(47 - 7\cdot 6) - 2\cdot 7 \\ &= 3\cdot 47 - 18\cdot 7 - 2\cdot 7 \\ &= 3\cdot 47 - 20\cdot 7 \end{aligned}$$

So $7\cdot(-20) \equiv 1 \pmod{47}$. Hence $[-20]=[27]=[7]^{-1}$. Finally,

$$\begin{aligned} x &\equiv (-3)\cdot(-20) \pmod{47} \\ &= 60 \\ &\equiv 13 \pmod{47}. \end{aligned}$$

Thus $x=[13]$.

Practice

Part 1.

1) Find $\gcd(-9, 15)$ by enumerating the divisors.

2) Compute $\gcd(270, 192)$ & write as sum $270x + 192y$.

Part 2 (harder)

1) Prove if $n \in \mathbb{Z}$ is square-free, $\sqrt{n} \notin \mathbb{Q}$.

2) Show $\forall a,b \in \mathbb{Z}$, $\gcd(a,b)\,\mathrm{lcm}(a,b) = ab$

3) Prove $\exists$ infinitely many primes:

(i) Show $\forall n \in \mathbb{Z}$, n and $n!+1$ are relatively prime
(ii) Use (i) to prove $\exists$ too many primes (Hint: contradiction)

4) How is the EA computation of $\gcd(45, 16)$ related to

$$\frac{45}{16} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{3}}} \; ?$$

Can you generalize this to show EA for $\gcd(a,b)$ produces continued fraction for $\frac{a}{b}$?

Part 3

1) Make sense of "What is Thursday + Friday?" and answer it. What is Thursday^2?

2) What's the largest m s.t. $12345 \equiv 54321 \pmod{m}$?

3) Find a $k \in \mathbb{Z}/12$ s.t. $k \neq [0]$ but $k^2 = [0]$.

4) Solve $[3]x = [2]$ in $\mathbb{Z}/7$.

5) What are the last 2 digits of $99^{1000^{10}} + 2022$?

Minute sheet

- What was most helpful today?
- What's something you're confused / curious about?

1) sketch

- work mod 7, use "+" in $\mathbb{Z}/7\mathbb{Z}$
- bijection {days of the week} $\to \mathbb{Z}/7\mathbb{Z} = \{0, \ldots, 6\}$

  Sun $\mapsto$ 0
  M $\mapsto$ 1
  Tu $\mapsto$ 2
  ⋮ etc

- Th + F $\mapsto$ 4+5 = 9 $\equiv 2 \pmod 7$
  Tu $\leftarrow$ 2
- Th^2 = Th · Th $\mapsto$ 4·4 = 16 $\equiv 2 \pmod 7$

Tu ← 2

2) Sketch

- $12345 \equiv 54321 \pmod{m} \iff m \mid 54321 - 12345 = 41{,}976$
- the largest m that divides $41{,}976$ is $m = 41{,}976$.