Recitation Notes 9/20

Today: Euclidian algorithm and prime numbers and modular arithmetic

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

2) when is \( a \equiv b \mod 2 \) ? \( \mod 1 \) ? \( \mod 0 \)?

Same parity "always" if \( a = b \)

HW1 Review (pre-images)

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

Remarks: (1) \( f^{-1} \) is not a function (\( f \) is fn \( \iff \) \( f \) is bijective) \n
(2) Arbitrary element of \( f^{-1}(P) \) is not of the form \( f^{-1}(x) \), since

\[ f^{-1}(x) = f^{-1}(f(x)) = \{ a \in A \mid f(a) = x \} \]

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

Exe from HW1

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

Pf (just \( \subseteq \)) 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 \( f^{-1}(P \setminus Q) \subseteq f^{-1}(P) \setminus f^{-1}(Q) \).

4(1) Let \( f : A \rightarrow B \) and suppose \( P \subseteq A \) and \( Q \subseteq B \). Show \( P = f^{-1}(f(P)) \) 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 \( 3m \in \mathbb{Z} \) s.t. \( b = am \). More generally, can always write \( b = qa + r \) for some \( q, r \in \mathbb{Z} \) s.t. \( 0 \leq r < a \).

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

Pf/ Sin \( a | b \), \( b = ma \) 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. \( \square \)

Recall: \( p \in \mathbb{Z} \) is prime if \( \exists p \Rightarrow a = 1 \) or \( p \).
- Otherwise, composite (except 0,1).

Some open problems
- Twin prime conjecture: Infinitely many pairs of primes \( (p, p+2) \)
- There is always a prime between \( 2n \) consecutive squares
- Goldbach's conjecture: Every \( n \in \mathbb{Z} \) can be written as a sum of 2 primes ...
  (ルーク・ジャンンダート for odd integers, Proved in 1930?)

Thm \( \sqrt{2} \) is irrational

Pf/ Suppose for contradiction that \( \sqrt{2} = \frac{a}{b} \in \mathbb{Q} \). Squaring and rearranging, we get
\[
2b^2 = a^2.
\]
This implies \( 2n^2 \) and \( a^2 \) have the same prime factorization. But now consider the prime factorization of \( a, b \):
\[
a = 2^m p_1^{e_1} \ldots p_k^{e_k}, \quad b = 2^n q_1^{f_1} \ldots q_l^{f_l}.
\]
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. \( \square \)

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

Reca:\( \text{gcd}(a, b) = d \in \mathbb{Z} \) s.t. (i) \( d | a \) and \( d | b \)
- \( \text{gcd}(2, 4) = 2 \), \( \text{gcd}(4, 6) = 2 \), \( \text{gcd}(5, 6) = 1 \)
- \( a, b \in \mathbb{Z} \) are relatively prime if \( \text{gcd}(a, b) = 1 \).

Note: Can also define the least common multiple \( \text{lcm}(a, b) = n \) s.t. (i) \( a | n \) and \( b | n \)
- \( \text{lcm}(2, 4) = 4 \), \( \text{lcm}(4, 6) = 12 \), \( \text{lcm}(5, 4) = 20 \)
- (ii) if \( n \) satisfies (i) then \( n | mn \).

Exs:
1. Use Euclid's algorithm to compute \( \text{gcd}(45, 12) \):

\[
\text{gcd}(45, 12) = \text{gcd}(12, 9) = \text{gcd}(9, 3) = 3.
\]
1. \(45 = 16 \cdot 2 + 13\)
2. \(16 = (3 \cdot 1 + 3)\)
3. \(13 = 3 \cdot 4 + 1\)
4. \(3 = 1 \cdot 3 + 0\)

\(\Rightarrow \text{gcd}(45, 16) = 1.\)

Note: \(45 = 3^2 \cdot 5\)
\(16 = 2^4\)

Reverse E.A. to write \(1 = 45 \cdot x + 16 \cdot y:\)
\(\begin{align*}
(1) & \quad 13 = 3 \cdot 4 \\
(2) & \quad 13 = (16 - 13 \cdot 1) \cdot 4 \\
& \quad = 13 - 16 \cdot 4 + 13 \cdot 4 \\
& \quad = 13 \cdot 5 - 16 \cdot 4 \\
& \quad = (45 - 16 \cdot 2) \cdot 5 - 16 \cdot 4 \\
& \quad = 45 \cdot 5 - 16 \cdot 10 - 16 \cdot 4 \\
& \quad = 45 \cdot 5 + 16 \cdot (-14)
\end{align*}\)

So \(x = 5\) and \(y = -14.\)

2. \(\text{gcd}(300, 18)\)

Write \(G = x \cdot 300 + y \cdot 18\)
\(\begin{align*}
300 &= (18 \cdot 16 + 12) \\
18 &= (18 \cdot 1 + 6) \\
12 &= 6 \cdot 2 + 0 \Rightarrow G \text{ is gcd}
\end{align*}\)

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

So \(x = -1\) and \(y = 17.\)

~break~

**Modular arithmetic**

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

- Quotient \(\mathbb{Z}/n\) has operations + and \(\cdot\) which are "nice."

**Ex.** Compute \(2^{2022} \pmod{5}:\)

Note \(2^4 = 16 \equiv 1 \pmod{5}.\) Since \(2022 = 4 \cdot 505 + 2,\)
\(2^{2022} = 2^{4 \cdot 505 + 2} = (2^4)^{505} \cdot 2^2\)
\(\equiv (1)^{505} \cdot 2^2 \pmod{5}\)
\(= 2^2 = 4\)

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

**Invertibility (aka Division is difficult)**

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

- \([a]^{-1} \text{ exists } \iff \text{gcd}(a, n) = 1; \text{ if it exists, it's unique.}\)
Non/ex: \( \mathbb{Z}/4 \)

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

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

\[
\gcd(a,n) = a \cdot x + n \cdot y = a \cdot x \pmod{n}
\]

\[
1 \Rightarrow [x]=[a]^{-1} \text{ in } \mathbb{Z}/n
\]

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-defined operations in \( \mathbb{Z}/47 \)):

\[
7x \equiv -3 \pmod{47}
\]

To find \([9]^{-1}\), use the EA to find \(\gcd(9,47)\):

\[
47 = 9 \cdot 4 + 5
\]
\[
4 = 9 \cdot 1 + 5
\]
\[
5 = 9 \cdot 0 + 2
\]
\[
2 = 9 \cdot 2 + 1
\]

Which means \(\gcd(9,47) = 1\), hence \([9]^{-1}\) exists. Moreover, we can compute

\[
1 = 5 - 2 \cdot 2
\]
\[
= 5 - 2 \cdot (9 \cdot -5)
\]
\[
= 35 - 2 \cdot 7
\]
\[
= 3 \cdot (47 - 9 \cdot 6) - 2 \cdot 7
\]
\[
= 3 \cdot 47 - 18 \cdot 7 - 2 \cdot 7
\]
\[
= 3 \cdot 47 - 20 \cdot 7
\]

So \( 9 \cdot (-20) \equiv 1 \pmod{47} \). Hence \([20]^{-1} = [9]^{-1}\). Finally,

\[
x \equiv (-3) \cdot (-20) \pmod{47}
\]

\[
= 60 \equiv 13 \pmod{47}.
\]

Thus \( x = [13]. \)
Practice

Part 1.

1) Find \( \text{gcd}(9,15) \) by enumerating the divisors.

2) Compute \( \text{gcd}(270, 192) \) and write as sum \( 290x + 192y \).

Part 2 (harder)

1) Prove if \( n \in \mathbb{Z} \) is square-free, \( \mathbb{Z} \not\subseteq \mathbb{Q} \).

2) Show that \( \mathbb{Z} \), \( \text{gcd}(a,b) \cdot \text{lcm}(a,b) = ab \)

3) Prove infinitely many primes:
   
   (i) Show that \( \mathbb{Z} \), \( n \) and \( mn \) are relatively prime.
   (ii) Use (i) to prove \( \infty \) many primes (Hint: Contradiction)

4) How is the EA computation of \( \text{gcd}(45,112) \) related to
   
   \[
   \frac{45}{112} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{4 + \frac{1}{3}}} \ldots}
   \]

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

Part 3

1) Make sense of "What is Thursday + Friday?" and answer it. What is Thursday? 8

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 \( \left[ 3 \right] x = \left[ 2 \right] \) in \( \mathbb{Z/7} \).

5) What are the last 2 digits of \( 97^{1000} + 2022 \)?

1) Work mod 7: use "+" in \( \mathbb{Z/7} \)

- bijection \{days of the week\} \( \rightarrow \mathbb{Z/7} = \{0, \ldots, 6\} \)
  
  \[
  \begin{align*}
  \text{Sun} & \rightarrow 0 \\
  \text{Mon} & \rightarrow 1 \\
  \text{Tue} & \rightarrow 2 \\
  \text{Thu} & \rightarrow 4 \left( \equiv 9 \pmod{11} \right) \\
  \text{Thu} \times \text{Thu} & \rightarrow 4 \cdot 4 \equiv 16 \equiv 2 \pmod{7}
  \end{align*}
  \]
Tu \leftrightarrow 2

2) \quad 12345 \equiv 54321 \pmod{m} \iff m \mid 54321 - 12345 = 41,976

- The largest m that divides 41,976 is m = 41,976.