Lecture 7 Outline.

1. Modular Arithmetic.
   Clock Math!!
2. Inverses for Modular Arithmetic: Greatest Common Divisor (GCD).
3. Euclid’s GCD Algorithm

Years and years...
80 years from now? February 6, 2104
20 leap years. 366*20 days
60 regular years. 365*60 days
It is day 2 + 366 - 20 + 365 + 60. Equivalent to?

Hm.

What is remainder of 366 when dividing by ? 2.
What is remainder of 365 when dividing by ? 1

Today is day 2.
Get Day: 2 + 20*2 + 60*1 - 102
Remainder when dividing by ? 4.
Or February 6, 2104 is Thursday!

Further Simplify Calculation:
20 has remainder 6 when divided by 7.
60 has remainder 4 when divided by 7.
Get Day: 2 + 6*2 + 4*1 = 18.
Or Day 4. February 6, 2104 is Thursday.

“Reduce” at any time in calculation!

Clock Math

If it is 4:00 now.
What time is it in 5 hours? 9:00!
What time is it in 15 hours? 19:00!
Actually 7:00.
19 is the “same as 7” with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.
What time is it in 100 hours? 104:00!

8 is the same as 104 for a 12 hour clock system.

Modular Arithmetic: Basics.

x is congruent to y modulo m or “x ≡ y (mod m)”
if and only if (x − y) is divisible by m.
...or x = y + km for some integer k.
...or x and y have the same remainder w.r.t. m.

Mod 7 equivalence classes:
{... −7, 0, 7, 14,...} {... −6, 1, 8, 15,...} ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.
or “ a ≡ c (mod m) and b ≡ d (mod m)
⇒ a + b ≡ c + d (mod m) and a · b ≡ c · d (mod m)”

Proof: If a ≡ c (mod m), then a = c + km for some integer k.
If b ≡ d (mod m), then b = d + jm for some integer j.
Therefore, a + b = c + d + (k + j)m and since k + j is integer.
⇒ a + b ≡ c + d (mod m).

Can calculate with representative in {0,...,m−1}.

Day of the week.

Today is Tuesday.
What day is it a year from now? on February 6, 2025?
Number days.
0 for Sunday, 1 for Monday, ... , 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!
two days are equivalent up to addition/subtraction of multiple of 7.
10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.
Day 2+366 or day 368.
Smallest representation:
subtract 7 until smaller than 7.
divide and get remainder.
368/7 leaves quotient of 52 and remainder 4.
or February 6, 2025 is Day 4, a Thursday.

Notation

x (mod m) or mod (x,m)- remainder of x divided by m in (0,...,m−1).

mod (x, m) = x − ⌊x/m⌋ · m
[| |] is quotient.
mod (29, 12) = 29 − (29/12) · 12 = 29 − (2) · 12 = 5

Recap:

a ≡ b (mod m).
Says two integers a and b are equivalent modulo m.

Modulus is m
### Inverses and Factors.

- **Division:** multiply by multiplicative inverse.
  
  \[ 2x - 3 \implies (1/2) \quad 2x = (1/2)3 \implies x = 3/2. \]

- **Multiplicative inverse of \(x\) is \(y\) where \(xy = 1\); 1 is multiplicative identity element.

  In modular arithmetic, 1 is the multiplicative identity element.

- **Multiplicative inverse of \(x \mod m\) is \(y\) with \(xy \equiv 1 \mod m\).**

  For 4 modulo 7 inverse is 2: \[ 2 \cdot 4 = 8 \equiv 1 \mod 7. \]

  Can solve \(4x = 5 \mod 7\).
  
  \[ 4 \cdot 3 \equiv 1 \mod 7 \]

  For 4 modulo 12: no multiplicative inverse!

  \[ x = 3 \mod 7 \]

  Solution for \(4\) \[ \text{gcd}(4,7) = 1 \]

- **Greatest common divisor of 4 and 7, gcd(4,7), is 1, then 4 has a multiplicative inverse modulo 7.**

  \[ \text{gcd}(4,7) = 1 \]

  \[ \implies \text{Prime factorization of 4 and 7 do not contain common primes.} \]

  \[ \implies (a-b)x \equiv 0 \mod m \]

  \[ \implies x \equiv 0 \mod m \]

  \[ (a-b) \text{ has to be multiple of } m \]

  \[ \implies (a-b) \geq m. \]

  \[ \text{But } a, b \in \{0, \ldots, m-1\}. \text{ Contradiction.} \]

### Finding inverses.

How to find the inverse?

How to find if \(x\) has an inverse modulo \(m\)?

Find gcd \((x, m)\).

- Greater than 1? No multiplicative inverse.
- Equal to 1? Multiplicative inverse.

**Algorithm:** Try all numbers up to \(x\) to see if it divides both \(x\) and \(m\).

Very slow.

Next: A Faster algorithm.

### Greatest Common Divisor and Inverses.

**Thm:**

If greatest common divisor of \(x\) and \(m\), \(\text{gcd}(x, m)\), is 1, then \(x\) has a multiplicative inverse modulo \(m\).

**Proof**

\[ \equiv : \text{The set } S = \{0x, 1x, \ldots, (m-1)x\} \text{ contains year } 1 \mod m \text{ if all distinct modulo } m. \]

**Pigeonhole principle:** Each of \(m\) numbers in \(S\) correspond to different one of \(m\) equivalence classes modulo \(m\).

\[ \implies \text{One must correspond to 1 modulo } m. \]

If not distinct, then \(a, b \in \{0, \ldots, m-1\}\), where \(ax \equiv bx \mod m\).

\[ \implies (a-b)x \equiv 0 \mod m \]

Or \((a-b)x = km\) for some integer \(k\).

\[ \text{gcd}(x, m) = 1 \]

\[ \implies \text{Prime factorization of } m \text{ and } x \text{ do not contain common primes.} \]

\[ \implies (a-b) \text{ factorization contains all primes in } m\text{’s factorization.} \]

\[ \text{So } (a-b) \text{ has to be multiple of } m. \]

\[ \implies (a-b) \geq m. \] But \(a, b \in \{0, \ldots, m-1\}\). Contradiction.

### Proof review. Consequence.

**Thm:** If \(\text{gcd}(x, m) = 1\), then \(x\) has a multiplicative inverse modulo \(m\).

**Proof Sketch:** The set \(S = \{0x, 1x, \ldots, (m-1)x\}\) contains \(y = 1 \mod m\) if all distinct modulo \(m\).

For \(x = 4\) and \(m = 6\). All products of 4...

\[ S = \{0, 0, 1, 4, 1, 4, 2, 4, 3, 4, 4, 4, 5, (4)\} = \{0, 4, 8, 12, 16, 20\} \]

reducing \((\mod 6)\)

\[ S = \{0, 4, 2, 0, 4, 2\} \]

Not distinct. Common factor 2.

For \(x = 5\) and \(m = 6\).

\[ S = \{0, 0, 1, 5, 2, 5, 3, 5, 4, 5, 5, 5\} = \{0, 5, 4, 3, 2, 1\} \]

All distinct, contains 1! 5 is multiplicative inverse of 5 \((\mod 6)\).

\[ 5x = 3 \mod 6 \]

What is \(x\)? Multiply both sides by 5.

\[ x = 15 - 3 \mod 6 \]

\[ 4x = 3 \mod 6 \]

No solutions. Can’t get an odd.

\[ 4x = 2 \mod 6 \]

Two solutions! \(x = 2, 5 \mod 6\)

Very different for elements with inverses.