Lecture 5: Number Theory II

Reading: 4.5.0, 4.6-4.6.3, 4.7

Announcement: No recitation on Friday (student holiday)

Modular Arithmetic: relationships between properties of numbers

e.g. Even + Odd = Odd
Even × Even = Even, etc } "arithmetic modulo 2"

Applications we will cover today: Error detection/correction

The key definition:

def: $a \equiv b \pmod{n}$ iff $n \mid (a-b)$

read: "a is congruent to b modulo n"

Alternatively, if a & b differ by a multiple of n

e.g. $\{\ldots, -6, -4, -2, 0, 2, 4, 6 \ldots\} \equiv$ Evens

are all congruent modulo 2, similarly

$\{\ldots -5, -3, -1, 1, 3, 5 \ldots\} \equiv$ Odds

also congruent modulo 2.

More interesting example:

$$\{\ldots -15, -8, -1, 6, 13, \ldots\}$$

are all congruent modulo 7.

Question: How do we add and multiply modulo n?

Answer: You just kind of do it

$$\begin{array}{rl} & 10 \equiv 3 \pmod 7 \\ + & 12 \equiv 5 \pmod 7 \\ \hline & 22 \equiv 8 \pmod 7 \end{array}$$

} modular addition

which is true, because $7 \mid \underbrace{(22-8)}_{14}$

$$\begin{array}{rl} & 10 \equiv 3 \pmod 7 \\ \times & 12 \equiv 5 \pmod 7 \\ \hline & 120 \equiv 15 \pmod 7 \end{array}$$

which is true, because $7 \mid (120-15)$

See handout for basic facts, there are some things (mostly division) that don't always work

Let's develop some other ways to think about modular arithmetic

Lemma 1: $a \equiv b \pmod{n}$ iff $\text{rem}(a,n) = \text{rem}(b,n)$

Proof: Using the Division algorithm

$$a = qn + r \qquad 0 \le r < n$$
$$b = q'n + r' \qquad 0 \le r' < n$$

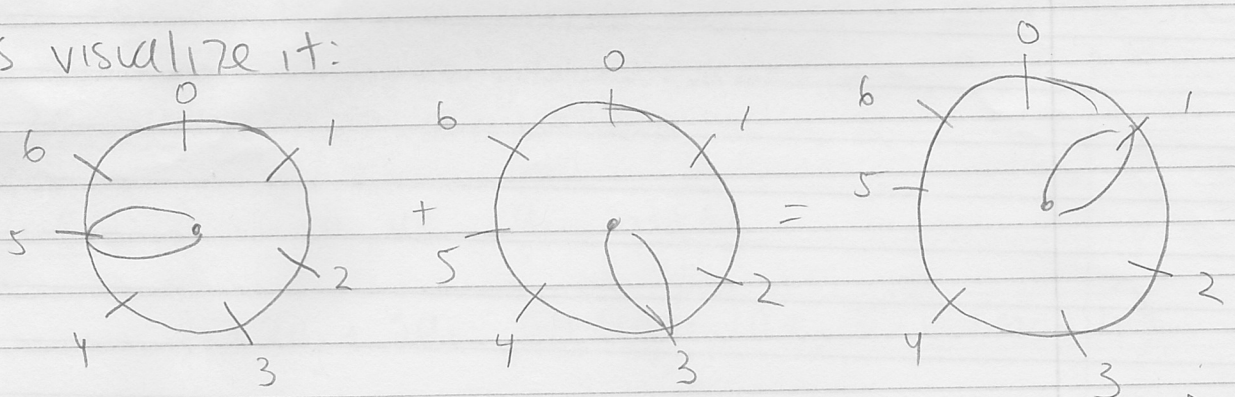
Then $a - b = (q - q')n + (r - r')$

$-n < r - r' < n \Rightarrow$ n cannot divide it

Hence $n \mid a - b$ iff $r - r' = 0$ ∎

original definition of congruence

Let's visualize it:



$12 \equiv 5 \pmod{7}$ $10 \equiv 3 \pmod{7}$ $22 \equiv 1 \pmod{7}$

This is called clock arithmetic

Let's study some cool applications, to make this less abstract

(Ask for volunteer)

Lemma 2: $10^k \equiv 1 \pmod 9$ for all $k \in \mathbb{N}$

Proof: $10^k = 1 + \underbrace{999\ldots9}_{k \text{ nines}} = 1 + 9(\underbrace{111\ldots1}_{k \text{ ones}})$

Now take the expression mod 9

$$10^k = 1 + 9(111\ldots1) \pmod 9 \quad \square$$

Hence any integer, say 359127 satisfies

$$3 \times 10^5 + 5 \times 10^4 + 9 \times 10^3 + 1 \times 10^2 + 2 \times 10 + 7 \cdot 10^0$$

($10^5 + 10^5 + 10^5$ etc)

$$\equiv 3 + 5 + 9 + 1 + 2 + 7 \pmod 9$$

So we can check computations using modular arithmetic!

Other examples:

ISBN: digits $a_1, a_2 \ldots a_{10}$ satisfy

$$a_1 + 2a_2 + 3a_3 \ldots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$$

allows to correct single digit error, or swap of two digits

RAID: Similar, recover from disk failures

$$\underbrace{a_1 + a_2 + a_3}_{\text{bits you want to store}} + \underbrace{a_4}_{\text{extra bit to recover from errors}} \equiv 0 \pmod 2$$

In modular arithmetic, division is subtle

$$2 \cdot 3 \equiv 4 \cdot 3 \pmod 6$$

But we can't just cancel the 3s ($2 \not\equiv 4 \pmod 6$)

Question: When can we divide? Which numbers have a multiplicative inverse?

Answer #1: If n is prime, can always divide mod n

Lemma 3: If n is prime and $k \not\equiv 0 \pmod n$, then there is an integer k^{-1} so that

$$k^{-1} k \equiv 1 \pmod n$$

e.g. ask students $3 \cdot 5 \equiv 1 \pmod 7$ what is 3's multiplicative inverse?

Proof: Since n is prime and $k \not\equiv 0 \pmod n$ (k is not a multiple of n)

$$\gcd(k, n) = 1 = \underbrace{sk + tn}_{\text{from Pulverizer}}$$

Now $\underbrace{s}_{k^{-1}} k = 1 - tn \pmod n$ ☒

So the problem with (mod 6) is that 6 is not prime!

This isn't quite a complete answer, e.g.

$$5 \cdot 5 \equiv 1 \pmod 6$$

why does 5 have a multiplicative inverse modulo 6, but 2 does not? ($\gcd(5,6)=1$, but $\gcd(2,6)\neq 1$)

Lemma 4: For any integers n, k where $\gcd(k,n)=1$, there is an integer k^{-1} so that

$$k^{-1}k \equiv 1 \pmod{n}$$

Ultimately, we will hide messages using modular arithmetic and Lemma 4 tells us how to get it back

(same proof)

Application: Choosing who goes first

player 0	player 1	player 2	player 3	
2	+ 1	+ 3	+ 0	$\equiv 2 \pmod 4$

what goes wrong if we multiply? If someone plays 2, can never multiply to 1.

Our last topic, another very useful way to compute an inverse:

Fermat's Little Theorem: If n is prime and $k \not\equiv 0 \pmod n$ then

$$k^{p-1} \equiv 1 \pmod n$$

(equiv. $k^p \equiv k \pmod n$)

i.e $k^{p-1} = k^{-1}$

Visualization: $k=2$, $p=3$

$$3 \mid (2^3 - 2)/3$$

2^3: # of strings; 2: # monochromatic strings

$(2^3 - 2)/3$: # non monochromatic necklaces

Hence $3 \mid (2^3 - 2)$, i.e. $2^3 \equiv 2 \pmod 3$

Is there a variant of Fermat's Little theorem that works over composites?

$$5^{(3-1)(2-1)} \equiv 1 \pmod 6$$