Mon Nov 11

Today: Modular Arithmetic.

Fix $0 \neq n \in \mathbb{Z}$ and define the relation

$$a \equiv_n b \iff n \mid (a-b)$$
$$(\text{i.e. } \exists k,\ a = b + nk)$$

You showed on Exam 2 that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

Given $a \in \mathbb{Z}$, consider the equivalence class

$$[a]_n = \{ b \in \mathbb{Z} : a \equiv_n b \}$$
$$= \{ a + nk : k \in \mathbb{Z} \}$$
$$= \{ \ldots, a-2n, a-n, a, a+n, a+2n, \ldots \}$$

Each class has a distinguished representative in the range $0, 1, \ldots, n-1$.

Proof: By Division Algorithm $\exists q, r \in \mathbb{Z}$ with

- $a = qn + r$ (i.e. $[a]_n = [r]_n$)
- $0 \leq r < n-1$.

Notation: Let $\mathbb{Z}/n$ stand for the set of equivalence classes

$$\mathbb{Z}/n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

We will "add" and "multiply" classes as follows:

$$[a]_n + [b]_n := [a+b]_n$$

$$[a]_n [b]_n := [ab]_n.$$

You proved on HW 4 that this makes sense.

Now we can think of $(\mathbb{Z}/n, +, \times)$ as a number system.

Example: Here are the + and × tables for $\mathbb{Z}/2$

+	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

×	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

When context is understood we will sometimes write a instead of $[a]_n$.

Example: $+$ and $\times$ tables of $\mathbb{Z}/6$.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

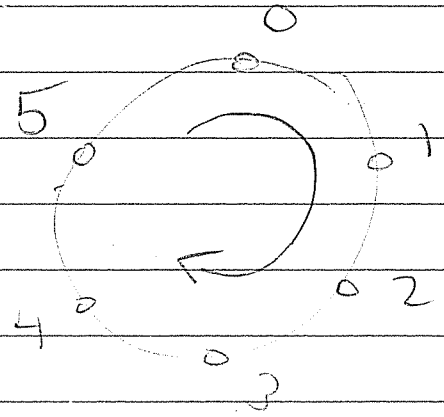
(eg. $4+4 \equiv_6 8 \equiv_6 2$)

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(e.g. $3 \cdot 5 \equiv_6 15 \equiv_6 3$)

Idea: $\mathbb{Z}/n$ is just like $\mathbb{Z}$, but we think "$n = 0$"

$\mathbb{Z}/n$ obeys the same axioms $\mathbb{Z}$ axioms of order. It makes no sense to say that $2 < 3 \bmod 6$ because:

$\mathbb{Z}/6 =$ 

In particular, the Cancellation property can fail.

$$2 \cdot 3 \equiv_6 2 \cdot 0 \quad (\equiv_6 0)$$

But $3 \not\equiv_6 0$

We can't cancel the 2! However, you showed on HW 4 that if $\gcd(c, n) = 1$ then $\forall\, a, b \in \mathbb{Z}$ we have

$$a \cdot c \equiv_n b \cdot c \implies a \equiv_n b$$

Example: Let $n = 41$ and consider $12 \in \mathbb{Z}/41$.

Apply Extended Euclidean Algorithm

1	0	41	①
0	1	12	②
1	-3	5	③ = ① - 3②
-2	7	2	④ = ② - 2③
5	-17	1	⑤ = ③ - 2④

to find that $41(5) + 12(-17) = 1$

This means

$$12 \cdot (-17) \equiv_{41} 1 - \cancel{41(5)}^{0} \equiv_{41} 1$$

$$12 \cdot (-17) \equiv_{41} 1$$

↑ The "multiplicative inverse" of $12 \in \mathbb{Z}/41$.

Notation: We write

$$12^{-1} \equiv_{41} -17 \equiv_{41} 24.$$

Check: $12 \cdot 24 \equiv_{41} 288 \equiv_{41} 1 + \cancel{7 \cdot 41}$

$$\equiv_{41} 1 \quad \checkmark$$

Could we say

$$\frac{1}{12} \equiv_{41} 24 \quad ??$$

Sure, if you want to.

This is great because it allows us to solve equations in $\mathbb{Z}/41$.

Solve for $x \in \mathbb{Z}/41$ in equation

$$12x \equiv_{41} 3$$

Divide both sides by 12 (i.e. multiply both sides by 24) to get

$$\begin{aligned} 24 \cdot 12x &\equiv_{41} 24 \cdot 3 \\ 1x &\equiv_{41} 72 \\ x &\equiv_{41} 41 + 31 \\ x &\equiv_{41} 31. \end{aligned}$$

$12x \equiv_{41} 3 \implies x \equiv_{41} 31$ ☺

If p is prime, then every nonzero element of $\mathbb{Z}/p$ has an inverse.

Example: $\mathbb{Z}/5$.

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	(1)	2	3	4
2	0	2	4	(1)	3
3	0	3	(1)	4	2
4	0	4	3	2	(1)

We get $1 \cdot 1 \equiv_5 1$

$2 \cdot 3 \equiv_5 1$

$3 \cdot 2 \equiv_5 1$

$4 \cdot 4 \equiv_5 1$.

So $1^{-1} \equiv_5 1$, $2^{-1} \equiv_5 3$, $3^{-1} \equiv_5 2$, $4^{-1} \equiv_5 4$.

Now you can solve any equation

$$ax \equiv_5 b.$$

$$x \equiv_5 a^{-1} b.$$

Wed Nov 13.

HW 5 due next Friday Nov 22.

Nov 25 – 29 No CLASS (Thanksgiving).

Exam 3 Mon Dec 9.

NO FINAL EXAM

Now: Tricks with modular arithmetic.

The most famous theorem of modular arithmetic is called

★ Fermat's Little Theorem (1640):

Given $a, p \in \mathbb{Z}$ with p prime and $p \nmid a$ (i.e. $a \not\equiv 0 \bmod p$) we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

If we multiply both sides by a then we get

$$a^p \equiv a \pmod{p}.$$

Now this holds even if $a \equiv 0 \bmod p$.

Example: Consider $p = 5$.

Then we have

$$1^4 = 1 \mod 5$$

$$\begin{aligned} 2^4 &= 2 \cdot 8 \\ &= 2 \cdot 3 \\ &= 6 \\ &= 1 \mod 5 \end{aligned}$$

$$\begin{aligned} 3^4 &= 9 \cdot 9 \\ &= 4 \cdot 4 \\ &= 16 \\ &= 1 \mod 5. \end{aligned}$$

$$\begin{aligned} 4^4 &= 16 \cdot 16 \\ &= 1 \cdot 1 \\ &= 1 \mod 5. \end{aligned}$$

It works!

Of what use is this??

Problem: What is the remainder when 3^{101} is divided by 5?

We know $3^4 = 1 \mod 5$ so we have

$$3^{103} = 3^{4 \cdot 25 + 3}$$
$$= 3^{4 \cdot 25} \cdot 3^3$$
$$= (3^4)^{25} \cdot 3^3$$
$$= (1)^{25} \cdot 3^3$$
$$= 3^3 = 27 = 2 \mod 5$$

Answer: 3

We could also look for the pattern:

$3 = (3) \mod 5$

$3^2 = 9 = (4) \mod 5$

$3^3 = 3 \cdot 3^2 = 3 \cdot 4 = 12 = (2) \mod 5$

$3^4 = 3 \cdot 3^3 = 3 \cdot 2 = 6 = (1) \mod 5$

$3^5 = 3 \cdot 3^4 = 3 \cdot 1 = (3) \mod 5$

$3^6 = 3 \cdot 3^5 = 3 \cdot 3 = 9 = (4) \mod 5$

$3^7 = (2)$

$3^8 = (1)$

⋮

etc.

$3^{103} = (2)$

(ones)

Problem: What is the final digit of 3^{103}?

We are looking for r such that

$$3^{103} = q\,10 + r.$$

$$3^{103} = r \mod 10.$$

However, 10 is not prime.

☆ **Euler-Fermat Theorem (1736):**

Given $a, n \in \mathbb{Z}$ with $\gcd(a,n) = 1$ we have

$$a^{\varphi(n)} = 1 \mod n,$$

where

$$\varphi(n) = \left|\{ d \le n : \gcd(d,n) = 1 \}\right|$$

Example:

$$\varphi(10) = \left|\{ \checkmark 1, \cancel{2}, \checkmark 3, \cancel{4}, \cancel{5}, \cancel{6}, \checkmark 7, \cancel{8}, \checkmark 9, \cancel{10} \}\right|$$

$$= 4$$

Hence for all $\gcd(a, 10) = 1$ we have

$$a^4 = 1 \mod 10.$$ ///

So the final digit of 3^{103} is

$$\begin{aligned} 3^{103} &= 3^{4 \cdot 25 + 3} \\ &= (3^4)^{25} \cdot 3^3 \\ &= (1)^{25} \cdot 3^3 \\ &= 3^3 \\ &= 27 = 7 \mod 10 \end{aligned}$$

The final digit is 7. ///

If p is prime then $\varphi(p) = p-1$,

$$\varphi(p) = |\{1, 2, 3, \ldots, p-1, \cancel{p}\}| = p-1$$

So we get $a^{p-1} = 1 \mod p$.

i.e. Euler-Fermat is a generalization of Fermat's Little Theorem

To prove FLT, we will use induction to show that

$$n^p \equiv n \mod p$$

for all $n \geq 1$. We will need one lemma.

Lemma: For all $a, b \in \mathbb{Z}$ we have

$$(a+b)^p \equiv a^p + b^p \mod p.$$

Proof Postponed. ///

Then we have

$1^p \equiv 1 \mod p$ ✓

$2^p = (1+1)^p = 1^p + 1^p = 1+1 = 2 \mod p$ ✓

$3^p = (2+1)^p$
$\equiv 2^p + 1^p$
$\equiv 2 + 1$
$\equiv 3 \mod p$ ✓

etc.

We just need to prove the lemma:

$$(a+b)^p \equiv a^p + b^p \mod p$$

We will need the Binomial Theorem.

Idea:

$$(a+b)^0 = 1$$
$$(a+b)^1 = a+b$$
$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Look for a pattern....

Fri Nov 15

HW 5 due next Fri Nov 22.
NO CLASS Nov 25 → 29
Exam 3 Mon Dec 9
NO FINAL EXAM.

We want to prove Fermat's little Theorem, which says that $\forall a, p \in \mathbb{Z}$ with p prime we have

$$a^p \equiv a \pmod{p}.$$

First let's look more closely at the sequence of primes:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Does it ever stop? NO.

Can you prove it?

Theorem (Euclid):

There are infinitely many primes

Proof: Assume for contradiction that there are finitely many primes and call them

$$p_1 < p_2 < p_3 < \cdots < p_k.$$

Now consider the number

$$N := p_1 p_2 p_3 \cdots p_k + 1.$$

We know that N has a prime factor $p \mid N$ (by Well-Ordering), but if so this prime p is not in our list because.

$$p_i \equiv 1 \pmod{N}$$

and hence $p_i \nmid N$ for all $i = 1, 2, \ldots, k$.
Contradiction.

"The primes never stop because we can always find another."

On HW 5 you will consider the following:
Reduce the primes mod 4.

p	2	3	5	7	11	13	17	19	23	29	31	...
$p \bmod 4$	2	3	1	3	3	1	1	3	3	1	3	...

Euclid proved the primes go on forever, but does $p \equiv 3 \bmod 4$ happen infinitely often? (ie. do the 3's ever stop?)

You will modify Euclid's proof to show that the 3's go on forever. It's a little tricky.

Idea: Assume for contradiction that there are only finitely many primes $\equiv 3 \bmod 4$ and call them

$$3 < p_1 < p_2 < \cdots < p_k$$

Now consider the number

$$N := 4p_1p_2 \cdots p_k + 3$$

Step 1: I claim that $\exists$ prime $p \mid N$ such that $p \equiv 3 \bmod 4$.

Proof: Suppose not. Then all the prime factors of N must be $\equiv 1 \bmod 4$ because...
This implies that $N \equiv 1 \bmod 4$.
Contradiction.

Step 2: We have prime $p \mid N$ with $p \equiv 3 \bmod 4$, but p is not in the list

$$3 < p_1 < p_2 < \cdots < p_k$$

because...
Contradiction.

Hence $\exists$ ∞ many primes $p \equiv 3 \bmod 4$.

///

If you want a challenge, try to prove that $\exists$ ∞ many primes $p \equiv 1 \bmod 4$.

There is a famous theorem of Dirchlet (1837) that says $\forall\ a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$,

$\exists\ \infty$ many primes $p \equiv a \pmod{b}$

It is very hard to prove.

Now we return to our goal. To prove

$$a^p \equiv a \pmod{p}$$

we will use the Freshman's Dream:

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

Why is this true?

Let's start by investigating $(1+x)^n$

$$(1+x)^0 = 1$$
$$(1+x)^1 = 1 + x$$
$$(1+x)^2 = 1 + 2x + x^2$$
$$(1+x)^3 = 1 + 3x + 3x^2 + x^3$$
$$(1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + x^4$$
$$\vdots$$

To be continued