Math 127, Wed Feb 10

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 3.2–3.3.
- Reading for Wed: 3.4–3.5.
- PS02 outline due tonight, full version due Mon Feb 15.
- Next problem session Fri Feb 12, 10:00–noon on Zoom.
- **Exam 1** in 12 days.

Recap: $\mathbf{Z}/(m)$, the integers mod m

Let m be a positive integer. We define the ring $\mathbf{Z}/(m)$, or the **integers (mod m)**, as follows.

- The underlying set of $\mathbf{Z}/(m)$ is $\{0, \ldots, m-1\}$.
- For $a, b \in \mathbf{Z}/(m)$, we define $a + b$ to be the ordinary integer sum of a and b, reduced mod m.
- Similarly, for $a, b \in \mathbf{Z}/(m)$, we define the product ab to be the ordinary integer product of a and b, reduced mod m.

When we work in $\mathbf{Z}/(m)$, we refer to m as the **modulus** of our ring.

Example: Fractions in $\mathbf{Z}/(7)$

In $\mathbf{Z}/(7) = \{0, 1, 2, 3, 4, 5, 6\}$, what is the reciprocal of each element?

$1 \cdot 1 = 1$, so $1^{-1} = 1$

$2 \cdot 4 = 8 = 1$ in $\mathbb{Z}/(7)$

So $2^{-1} = 4$, $4^{-1} = 2$.

$3 \cdot 5 = 15 = \underbrace{14}_{=0} + 1 = 1$

So $3^{-1} = 5$, $5^{-1} = 3$.

$6 \cdot 6 = 36 = \overbrace{35}^{=0} + 1 = 1$

trial & error

So $6^{-1} = 6$.

(Alt: $\underbrace{6 = -1}_{\text{diff}=7}$, $(-1)(-1) = 1$

So $(-1)^{-1} = -1$

So always true in $\mathbb{Z}/(m)$ that

$(m-1)^{-1} = (-1)^{-1} = -1 = m-1$)

$1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $6^{-1} = 6$

$4^{-1} = 2$ $5^{-1} = 3$

0 has no inverse.

Experiment: Primitive elements

Defn: To say that $a \in \mathbf{Z}/(m)$ is **primitive** means that every nonzero element of $\mathbf{Z}/(m)$ is a power of a.

$m=5$

- Is 2 primitive in $\mathbf{Z}/(5)$?

$2^0=1,\ 2^1=2,\ 2^2=4,\ 2^3=8=3$

$1, 2, 3, 4$ ✓ So 2 is primitive in Z/(5).

- Is 2 primitive in $\mathbf{Z}/(7)$?

$2^0=1,\ 2^1=2,\ 2^2=4,\ 2^3=8=1,\ 2^4=2^3\cdot 2$
$=1\cdot 2$

$1, 2, 4, 1, 2, 4, \ldots$ 2 is not primitive in Z/(7).

- Is 2 primitive in $\mathbf{Z}/(11)$?

$n=11$

$2^0=1,\ 2^1=2,\ 2^2=4,\ 2^3=8,\ 2^4=16=5$

$2^5=2^4\cdot 2=5\cdot 2=10$

k	2^k in $\mathbb{Z}/(11)$
0	1
1	2
2	4
3	8
4	5
5	10
6	9
7	7
8	3
9	6
10	1

$\times 2 \pmod{11}$

~~1~~ ~~2~~ ~~3~~ ~~4~~ ~~5~~ ~~6~~ ~~7~~ ~~8~~ ~~9~~ ~~10~~

So 2 is primitive in Z/(11).

Open question (i.e., no person on earth knows the answer to this question):
Are there infinitely many primes p such that 2 is primitive in Z/(p)?
(Experts believe yes.)

The point of the last few problems in PS02: Experiment!

Try a bunch of examples and see if you find any patterns!

(And yes, the other point is for you to get better at computation in $\mathbf{Z}/(m)$ through practice — but you might as well do something interesting in the process.)

Solving $ax = b$ in $\mathbf{Z}/(m)$

Question

For which $a, b \in \mathbf{Z}/(m)$ can we solve the equation $ax = b$ in $\mathbf{Z}/(m)$ (i.e., for some $x \in \mathbf{Z}/(m)$)?

Turns out this is an old problem in disguise!

$ax = b$ in $\mathbb{Z}/(m)$

$\iff \underbrace{ax = qm + b}_{\text{divide ax by m, get remainder of b (when 0 <= b <= m-1)}}$ for some $x, q \in \mathbb{Z}$.

$\iff ax - mq = b$ for some $x, q \in \mathbb{Z}$

$\iff ax + my = b$ for some $x, y \in \mathbb{Z}$

Bezout + Euclidean Reduction!

Bezout's identity and $ax = b$

Corollary

For $a, b \in \mathbf{Z}/(m)$, $ax = b$ has a solution $x \in \mathbf{Z}/(m)$ exactly when $\gcd(a, m)$ divides b (in $\mathbf{Z}$). Furthermore, Euclidean Rewriting gives an explicit algorithm for solving $ax = b$.

Example: Solve $\underset{a}{42}x = \underset{b}{36}$ in $\mathbb{Z}/(\underset{m}{76})$

$\iff$ Solve $42x + 76y = 36$ in $\mathbb{Z}$.

$\overset{m}{76} = 1(\overset{a}{42}) + 34$

$\overset{a}{42} = 1(\overset{m-a}{34}) + 8$

$34 = 4(8) + 2$ gcd

$8 = 4(2)$

2 divs 36, so there is sol'n.

$34 = m - a$

Signs never cancel, always reinforce; signs of m, a alternate

$8 = a - (m-a) = 2a - m$

$=36$

$2 = 34 - 4(8)$

$= (m-a) - 4(2a-m)$

$\boxed{2 = 5m - 9a}$

$5(76) - 9(42) = 380 - 378 = 2$ ✓

$\boxed{\text{Mod } m=76}$ $(-9)(42) = 2$

$42(-9)(18) = 2(18) = 36$

$-162 \equiv 66 \pmod{76}$

$+3(76)$

$42 \cdot 66 \equiv 36 \pmod{76}$

$\boxed{x \equiv 66}$

0 in $\mathbb{Z}/(76)$

$\parallel$

Alt: $\left.\begin{aligned} 34 &= m - n \\ 2 &= 5m - 9n \end{aligned}\right\} + \quad 36 = \cancel{6m} - 10n$

So $42(-10) = 36$ in $\mathbb{Z}/(76)$

$\boxed{-10 = 66}$ in $\mathbb{Z}/(76)$

Solving $ax = b$ in $\mathbf{Z}/(p)$

To repeat:

Corollary

For $a, b \in \mathbf{Z}/(m)$, $ax = b$ has a solution $x \in \mathbf{Z}/(m)$ exactly when $\gcd(a, m)$ *divides b (in $\mathbf{Z}$).*

So when the modulus is a prime p:

Corollary

If p is prime, and $a \neq 0$ in $\mathbf{Z}/(p)$ (i.e., a is not congruent to $0 \pmod p$), then $ax = 1$ for some $x \in \mathbf{Z}/(p)$.

So every nonzero element of Z/(p) has a multiplicative inverse!

Units and fields

Definition

Let R be a ring. For $a \in R$, the **multiplicative inverse of** a is $b \in R$ such that $ab = 1$. We use a^{-1} to denote the inverse of a. To say that a is a **unit** in R means that a has a multiplicative inverse in R.

Note: 2 is a unit in $\mathbf{R}$ but is not a unit in $\mathbf{Z}$. $\left(\frac{1}{2} \notin \mathbb{Z}\right)$

Definition

A **field** is a ring R in which every nonzero element is a unit (and $1 \neq 0$).

Fields you know include $\mathbf{R}$, $\mathbf{Q}$, and now:

Corollary

The ring $\mathbf{Z}/(p)$ is a field. (p prime) $\mathbb{Z}/(p)$

Because this makes $\mathbf{Z}/(p)$ special, we often refer to it as $\mathbf{F}_p$, the **field of order** p.

Polynomials with coefficients in a ring R

Let R be a ring. (Think: R is one of $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}/(m)$.) We define the ring $R[x]$, the **ring of polynomials with coefficients in** R, as follows.

all in ring R

Set: All expressions of the form

$$\sum_{i=1}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0, \qquad (1)$$

where each a_i is an element of the ring R.

Addition and multiplication: in $R[x]$ are each defined to work like addition and multiplication of polynomials with real coefficients, except that all coefficient arithmetic is performed in the ring R.

Example: $\mathbf{F}_7[x]$ $= R$

$\mathbb{F}_7 = \mathbb{Z}/(7)$, so coeffs mod 7.

Addition:

$$
\begin{array}{r}
3x^2 + 4x + 6 \\
+ \quad 5x^2 + x + 5 \\
\hline
x^2 + 5x + 4
\end{array}
\quad \text{in } \mathbb{F}_7[x].
$$

Multiplication:

$$
\begin{array}{r}
5x^2 + 2x + 4 \\
\cdot \quad 5x^2 + 3x + 1 \\
\hline
5x^2 + 2x + 4 \\
x^3 + 6x^2 + 5x \quad \\
4x^4 + 3x^3 + 6x^2 \qquad \\
\hline
4x^4 + 4x^3 + 3x^2 \qquad + 4
\end{array}
$$

$12 = 5$

$15 = 1$

$\mathbb{F}_7[x]$

An important and subtle point

Polynomials are not (just) functions — they are abstract objects that are elements of a ring. In fact, we will most often use polynomials as if they were numbers in some very strange system of numbers.

The degree of a polynomial

If $\neq 0$ $\deg f$

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \neq 0$.
The **degree** of $f(x)$, or $\deg f(x)$, is defined to be the largest k such that $a_k \neq 0$.
If $\deg f(x) = n$, then a_n is called the **leading coefficient** of $f(x)$, and $a_n x^n$ is called the **leading term** of $f(x)$. To say that a polynomial $f(x)$ is **monic** means that the leading coefficient of $f(x)$ is 1.
We also define $\deg 0 = -\infty$.

A weird and unpleasant example

You may remember from high school algebra/precalc that

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)). \tag{2}$$

However, in $(\mathbf{Z}/(6))[x]$, we have:

Definition

To say that a ring R has the **zero factor property** (ZFP) means that if $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$. Equivalently, having ZFP means that the product of two nonzero elements of R is still nonzero.

ZFP defines the problem away

Suppose R is a ring with ZFP (e.g., $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{F}_p$).

Theorem

For $f(x), g(x) \in R[x]$,

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)). \tag{3}$$

Corollary

If $f(x), g(x), h(x)$ are polynomials in $R[x]$ such that $f(x) = g(x)h(x)$, then one of $g(x)$ and $h(x)$ must have degree at most $\dfrac{\deg(f(x))}{2}$.

Corollary

If $u(x)$ is a unit in $R[x]$, then $u(x)$ must be a nonzero constant polynomial $u = u(x)$; in fact, u must actually be a unit in R.