Math 127, Wed Feb 09

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, you may 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.
- **IN-PERSON CLASSES START MON FEB 14!!!!**
- Reading for today: 3.2–3.3.
- Reading for ~~Wed~~: 3.4–3.5. Mon
- ~~PS~~02 outline due tonight, full version due Mon Feb 14.
- Next problem session Fri Feb 11, 10:00–noon on Zoom.
- **Exam 1** in two weeks. or Thu

Wed Feb 23

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

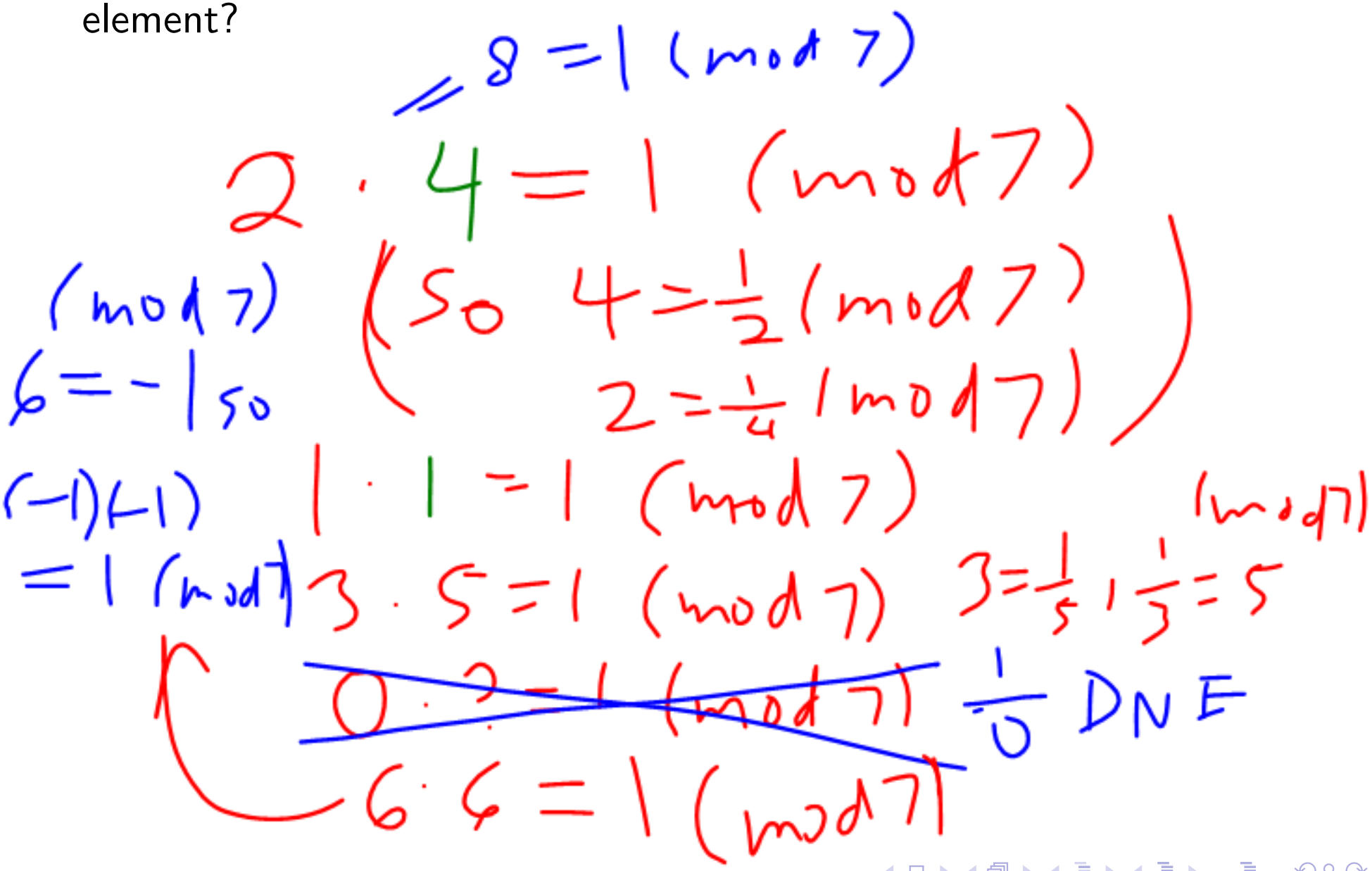
Let m be a positive integer. We define the ring $\mathbf{Z}/(m)$, or the **integers (mod m)**, as follows.

- 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?



Why is $-1 = 6 \pmod 7$?

m = 0 Principle: If we are working in the ring Z/(m), then we can apply/use any identity, equation, etc., that we can deduce from the fact that m=0.

So mod 7 (m=7):

$-1 = -1 + 7 = 6 \pmod 7$

New prob

$-38 = -38 + 35 = -3 \pmod 7$
$-3 + 7 = 4 \pmod 7$

So $-38 = 4 \pmod 7$.

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 ~~2~~ a.

- Is 2 primitive in $\mathbf{Z}/(5)$? 2 is primitive mod 5. Alt: 2 is prim in Z/(5).

$2^1=2, 2^2=4, 2^3=8=3, 2^4=2(3)=6=1$

(0) 1, 2, 3, 4 ✓ Yes

- Is 2 primitive in $\mathbf{Z}/(7)$? 2 is not primitive mod 7.

$2^1=2, 2^2=4, 2^3=8=1, 2^4=2(1)=3$

2, 4, 1, 2, 4, 1 ... No missing 3, 5, 6

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

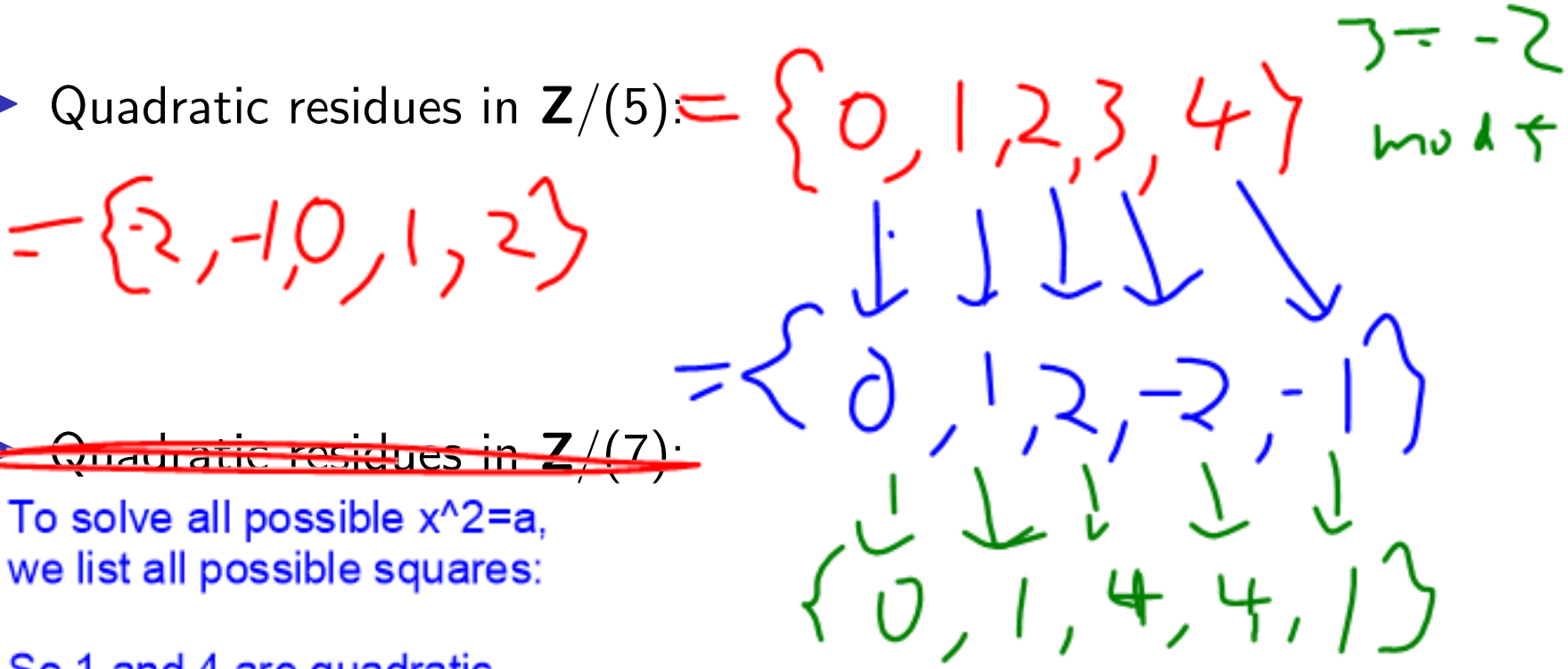
$2^0=1, 2^1=2(2^0)=2, \ldots$

Experiment: Quadratic residues

Defn: To say that $a \in \mathbf{Z}/(m)$ is a **quadratic residue** means that $a \neq 0$ and a is a square in $\mathbf{Z}/(m)$, i.e., $x^2 = a$ has a solution in $\mathbf{Z}/(m)$.

Here we use a weird method for solving $x^2 = a$: Because there are only finitely many values of $x \in \mathbf{Z}/(m)$, we can just try all possible x.

- Quadratic residues in $\mathbf{Z}/(5)$:



- ~~Quadratic residues in $\mathbf{Z}/(7)$:~~

To solve all possible x^2=a, we list all possible squares:

So 1 and 4 are quadratic residues mod 5, and 2 and 3 are not.

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 (mod m) has a solution x in Z/(m)

<=> ax = b + my has a solution x,y in Z

<=> ax - my = b has a solution x,y in Z.

We can solve equations like ax - my = b in Z by:

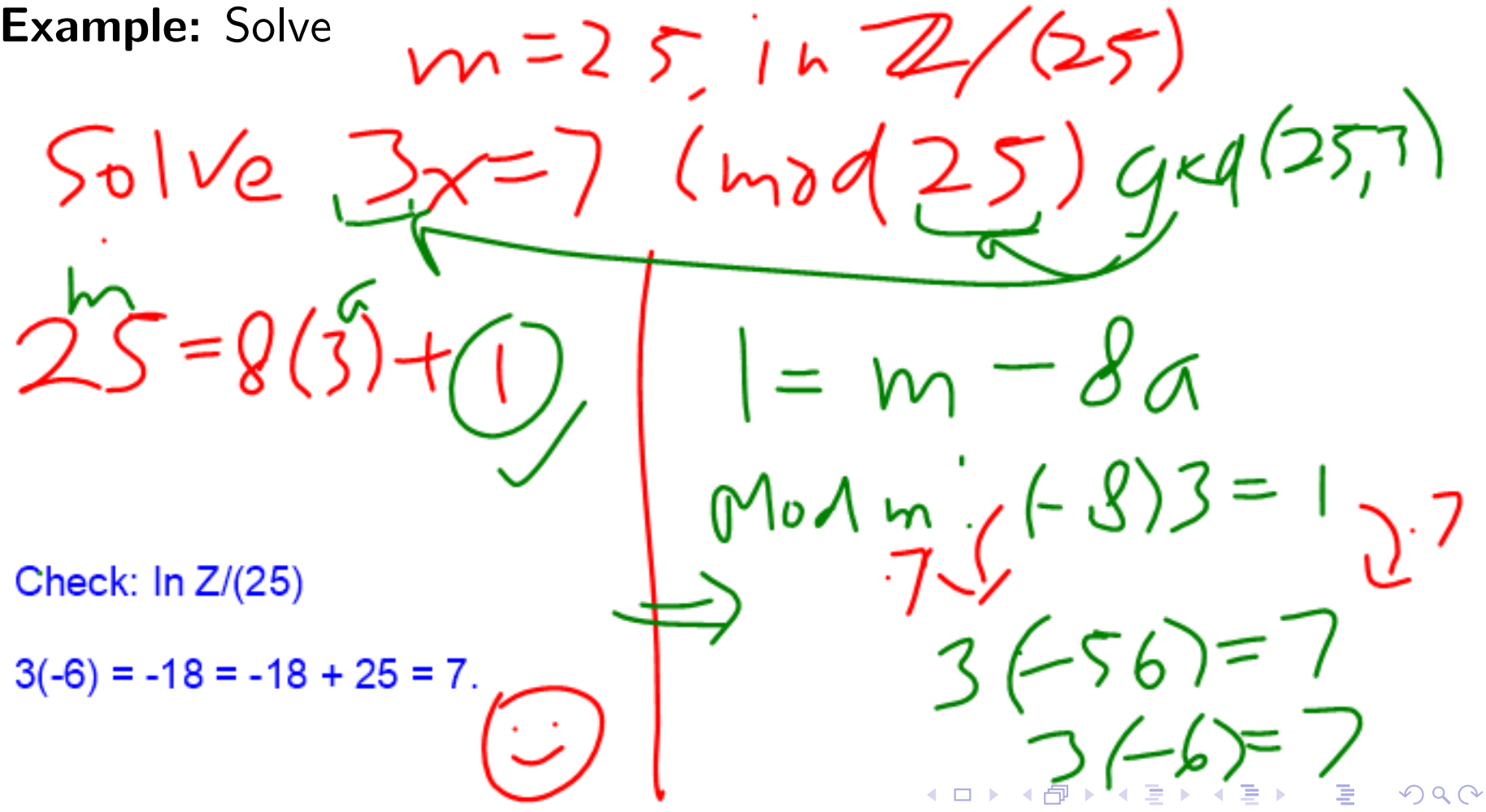
EUCLIDEAN ALG/REWRITING
(i.e. gcd(a, m))

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



Ex. In $\mathbb{Z}/(42)$, solve

$$17x = 1 \pmod{42}$$

Ans: gcd(42, 17)

$42 = 2(17) + 8$ (m, q)

$17 = 2(8) + 1$ (q)

gcd = 1, divides b = 1, so soln.

$8 = m - 2q$

$1 = q - 2(m - 2q)$

$= q - 2(m - 2q)$

$= 5q - 2m$

$5(17) - 2(42) = 1$

$m = 0$

$8 = -2q$

$1 = 5q$

$x = 5$

Check.

$5 \cdot 17 = 85$

$= 1$

Check: In Z/(42), 42 = 0.

5 * 17 = 85. What do you get when you reduce 85 (mod 42)?

85 - 42 = 43 Still not small enough

43 - 42 = 1. Done.

So 5 * 17 = 85 = 1 (mod 42).

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 (mod p)), then $ax = 1$ for some $x \in \mathbf{Z}/(p)$.

I.e.: Every nonzero element of Z/(p) has a multiplicative inverse in Z/(p).

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 $\mathbf{Z}$.

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.*

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.

Set: All expressions of the form

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

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: $\mathbf{F}_7[x]$

Addition:

Multiplication:

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

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

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

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

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

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.