

## Math 127, Mon Feb 15

- ▶ 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: 3.4–3.5; reading for Wed: 3.6, 4.1–4.2.
- ▶ PS02 due tonight; PS03 outline due Wed, full version due Mon Feb 22.
- ▶ Next problem session Fri Feb 19, 10:00–noon on Zoom.
- ▶ **Exam 1 now on Wed Feb 24**, in 9 days.

# Struggle

PS01 wasn't meant to be easy, and PS02 even more so.

- ▶ The problem sets are challenging because everyone learns through struggle.
- ▶ If you don't get all of the problems the first time around, or even after trying many times — that's OK! I'm not expecting that you get 100% on the homework, even after revision.
- ▶ Remember: The most productive learning experiences are **problems**, where your method of solution may not be clear, and you may not even know how to get started. That's where you really start to understand the material.
- ▶ Corollary: You need to do the homework **yourself**, without outside “help”. Think: There are two times you can choose to try a class of problems for the very first time, on the problem sets, or on an exam.



## 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:

$$\underbrace{3x^4}_{\deg 4} \cdot \underbrace{(2x^3+1)}_{\deg 3} = 6x^7 + 3x^4 = \underbrace{3x^4}_{\deg 4}$$

*mod 6*

### 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.

*i.e., no this*

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

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

(Even true if  $f$  or  $g$  is the zero poly b/c  $-\infty + \text{anything} = -\infty$ .)

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  $\frac{\deg(f(x))}{2}$ .

Corollary

Special case: The polynomial  $x$  has no inverse in  $R[x]$ .

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  $R$ .

(Any field)

## Flashback: Long division

What is 50153 divided by 327?

$$\begin{array}{r} 153 \\ \hline 327 \overline{) 50153} \\ \underline{- 327} \phantom{00} \\ 1745 \\ \underline{- 1635} \phantom{00} \\ 1103 \end{array}$$

$$50153 = 153(327) + 122$$

We stop because remainder 122 is smaller than divisor 327.

$$0 \leq r < d \rightarrow \begin{array}{r} 1103 \\ \hline - 981 \\ \hline 122 < 327 \end{array}$$

## A more recent flashback: Polynomial long division

What is  $5x^4 + x^2 + 5x + 3$  divided by  $3x^2 + 2x + 7$  in  $\mathbf{R}[x]$ ?

$$\begin{array}{r} \frac{5}{3}x^2 - \frac{10}{9}x - \frac{76}{27} \\ 3x^2 + 2x + 7 \overline{) 5x^4 \phantom{+ 10x^3} + x^2 + 5x + 3} \\ \underline{-(5x^4 + \frac{10}{3}x^3 + \frac{35}{3}x^2)} \phantom{+ 5x + 3} \end{array}$$

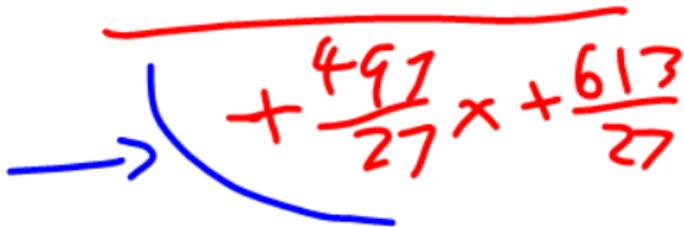
$$\begin{array}{r} -\frac{10}{3}x^3 - \frac{32}{3}x^2 + 5x + 3 \\ \underline{-( -\frac{10}{3}x^3 - \frac{20}{9}x^2 - \frac{70}{9}x )} \phantom{+ 3} \end{array}$$

$$-\frac{76}{9}x^2 + \frac{115}{9}x + 3$$

$$\underline{-( -\frac{76}{9}x^2 - \frac{152}{27}x - \frac{532}{27} )}$$

At each stage,  
we knock out the highest  
power monomial term.

We stopped here  
because remainder  
now has degree 1,  
which is strictly less  
than the degree of the  
divisor  $3x^2+2x+7$ .



A blue arrow points from the text on the left to the handwritten expression on the right. The expression is written in red ink and consists of three terms: a plus sign, a fraction with 497 in the numerator and 27 in the denominator, followed by 'x', another plus sign, and a fraction with 613 in the numerator and 27 in the denominator. A horizontal red line is drawn above the entire expression.

$$+ \frac{497}{27}x + \frac{613}{27}$$

# Something new: Long division in $\mathbf{F}_{11}[x]$

$M = 11$

What is  $5x^4 + x^2 + 5x + 3$  divided by  $3x^2 + 2x + 7$  in  $\mathbf{F}_{11}[x]$ ?

$$\begin{array}{r}
 3x^2 + 2x + 7 \overline{) 5x^4 + x^2 + 5x + 3} \\
 \underline{-(5x^4 + 7x^3 + 8x^2)} \\
 4x^3 + 4x^2 + 5x + 3 \\
 \underline{-(4x^3 + 10x^2 + 2x)} \\
 5x^2 + 3x + 3 \\
 \underline{-(5x^2 + 7x + 8)} \\
 7x + 6
 \end{array}$$

$\uparrow$  deg 2  
 $\frac{5}{3}x^2 \sim \frac{10}{7}x$   
 $\parallel \parallel$   
 $5x^2 + 5x$

$\circlearrowleft 7x + 6$  deg 1

$$3 \cdot 4 = 1$$

$$\frac{1}{3} = 4$$

$$\frac{5}{3} = 4 \cdot 5 = 9$$

$$\frac{4}{3} = 4 \cdot 4 = 5$$

We stop when degree of remainder is < degree of divisor.

So

$$5x^4 + x^2 + 5x + 3 = (9x^2 + 5x + 9)(3x^2 + 2x + 7) + (7x + 6)$$

$$\begin{array}{ccc} \left(-\frac{5}{3}x^2\right) & \left(-\frac{10}{9}x\right) & \left(-\frac{76}{27}\right) \\ \parallel & \parallel & \parallel \\ 9x^2 & + & 5x & + & 9 \end{array}$$

Note:

## A money-making note

Your division problems will be in  $\mathbf{F}_p[x]$  for  $p = 2, 3, 5$ .

- ▶  $p = 2$  is where the money is made.
- ▶ But to make sure you understand the signs involved in division (and later the Euclidean algorithm), you'll have some problems for odd  $p$ .
- ▶ And just so you're aware of the role of fractions and denominators, also a few problems for  $p = 5$ .

# Generalizing the division theorem for integers

## Theorem (The Division Theorem for Polynomials)

Let  $F$  be a field, and let  $a(x)$  and  $d(x)$  be polynomials in  $F[x]$  with  $d(x) \neq 0$ . There exist unique  $q(x), r(x) \in F[x]$  such that

$$a(x) = d(x)q(x) + r(x),$$

with  $\deg(r(x)) < \deg(d(x))$ .

**Why does that work?** Because what we did in  $\mathbf{R}[x]$  and  $\mathbf{F}_{11}[x]$  works in  $F[x]$  for any field  $F$ . Key points:

- ▶ Can always divide by leading coefficient of  $d(x)$  (since the leading coefficient is always  $\neq 0$ ).
- ▶ Can always keep going until  $\deg(r(x)) < \deg(d(x))$ .

*i.e.*, the "size" of a polynomial is its degree.

# Some consequences of polynomial division

## Corollary (Remainder Theorem)

Let  $F$  be a field, let  $f(x) \in F[x]$  be a polynomial, and let  $\alpha$  be an element of  $F$ . When we divide  $f(x)$  by  $(x - \alpha)$ , the remainder is a constant, namely  $r = f(\alpha)$  (the element of  $F$  obtained by substituting  $\alpha$  for  $x$  in  $f(x)$ ).

## Corollary (Factor Theorem)

Let  $F$  be a field,  $f(x) \in F[x]$ , and  $\alpha \in F$ . Then  $(x - \alpha)$  divides  $f(x)$  (i.e., with a remainder of 0) exactly when  $f(\alpha) = 0$ .

## Corollary

Let  $F$  be a field and let  $f(x) \in F[x]$  be a polynomial of degree  $m \geq 1$ . Then  $f(x)$  has at most  $m$  distinct zeros in  $F$ , i.e., there are at most  $m$  distinct elements  $\alpha \in F$  such that  $f(\alpha) = 0$ .

Last Cor is false for  $(\mathbb{Z}/(8))[x]$ :  $x^2=1$  has four solutions.

## An important meta-principle

For a field  $F$ , the ring  $F[x]$  works just like the ring of ordinary integers, except replacing the integer Division Theorem with the Division Theorem for Polynomials.

So, just as we used the ordinary Division Theorem repeatedly to compute  $\gcd(a, b)$ , we can use the polynomial division theorem repeatedly to compute  $\gcd(a(x), b(x))$ .

But first, let's define the problem more precisely.

# Polynomial GCDs

## Definition

Let  $F$  be a field, and let  $f(x), g(x), d(x) \in F[x]$  be polynomials with coefficients in  $F$ . To say that  $d(x)$  **divides**  $f(x)$  in  $F[x]$  means that  $f(x) = q(x)d(x)$  for some  $q(x) \in F[x]$ . Similarly, to say that  $d(x)$  is a **common divisor** of  $f(x)$  and  $g(x)$  means that  $d(x)$  divides both  $f(x)$  and  $g(x)$ .

## Definition

Let  $F$  be a field, and let  $f(x), g(x) \in F[x]$  be polynomials with coefficients in  $F$ , at least one of which is nonzero. To say that  $d(x) \in F[x]$  is a **greatest common divisor** of  $f(x)$  and  $g(x)$  means that  $d(x)$  is a common divisor of  $f(x)$  and  $g(x)$  of highest possible degree.

But there's an ambiguity in  $\gcd(f(x), g(x))$ . For example, in  $\mathbf{R}[x]$ , if  $f(x) = x^2 - x$  and  $g(x) = x^2$ , then

$$\gcd(f(x), g(x)) = x \text{ or } 2x \text{ or } \pi x$$

# The Polynomial Euclidean Algorithm

Let  $r_{-1}(x) = a(x)$ ,  $r_0(x) = b(x)$ . To calculate  $\gcd(a(x), b(x))$ :

$$r_{-1}(x) = q_1(x)r_0(x) + r_1(x) \quad (\deg r_1 < \deg r_0)$$

$$r_0(x) = q_2(x)r_1(x) + r_2(x) \quad (\deg r_2 < \deg r_1)$$

$$r_1(x) = q_3(x)r_2(x) + r_3(x) \quad (\deg r_3 < \deg r_2)$$

$\vdots$

$$r_{N-4}(x) = q_{N-2}(x)r_{N-3}(x) + r_{N-2}(x) \quad (\deg r_{N-2} < \deg r_{N-3})$$

$$r_{N-3}(x) = q_{N-1}(x)r_{N-2}(x) + r_{N-1}(x) \quad (\deg r_{N-1} < \deg r_{N-2})$$

$$r_{N-2}(x) = q_N(x)r_{N-1}(x)$$