Last time: Poly's $\leftrightarrow$ integers

- if $f(x), g(x) \in F[x]$

$\exists!$ $q, r \in F[x]$

s.t. q = quotient, r = remainder

(1) $f = gq + r$

(2) $\deg r < \deg g$.

eg

$$f(x) = 6x^3 - 2x^2 + x + 3$$

$$g(x) = x^2 - x + 1$$

$$\begin{array}{r} 6x+4 \\ x^2-x+1 \;\overline{)\; 6x^3-2x^2+x+3} \\ \underline{-(6x^3-6x^2+6x)} \end{array}$$

$$r_1 = 4x^2 - 5x + 3$$

$$4x^2 - 4x + 4$$

$$-x - 1$$

$$6x^3 - 2x^2 + x + 3 = (x^2 - x + 1)(6x + 4) - (x + 1).$$

Def: A poly $f(x) \in \mathbb{F}[x]$ is <u>prime</u> (irreducible) if it cannot be decomposed as $f = a \cdot b$ with $\deg a, \deg b \geq 1$

Examples

(1) Any poly f of $\deg f = 1$

is prime $(f(x) = \alpha x + \beta)$

(2) $F = F_3$. $f(x) = x^2 + 1$

is prime. If it wasn't

$f(x) = (x-a)(x-b)$ for

some $a, b \in F$

but f has no roots

over F_3.

(3) $F = F_5$. $f(x) = x^2 + 1$

then f is not prime:

$3^2 + 1 = 0 \mod 5$

$2^2 + 1 = 0 \mod 5$

$x^2 + 1 = (x-2)(x-3)$.

We restrict attention to

monic poly's, ie where

the coefficient of the

leading monomial is 1.

Prop: Let $f(x) \in F[x]$ be

a monic poly. Then there is

$k \geq 1$ and monic prime poly's

$a_1, \ldots, a_k$ s.th

$$f = a_1 \cdot \ldots \cdot a_k$$

and $a_1, \ldots, a_k$ are unique

up to re-ordering.

Proof: Existence is clear.

For uniqueness, suppose that f is of minimal degree s.th

$$b_1 \cdot \ldots \cdot b_\ell = f = a_1 \cdot \ldots \cdot a_k$$

Where a_i, b_i's are monic primes. Now a_1 cannot appear on the LHS since o/w we could cancle it and contradict the minimality of f. Similarly, b_1 cannot appear on RHS.

Wlog, $\deg b_1 \leq \deg a_1$.

Then $\exists\, q, r$ s.th

$$\rightarrow \boxed{a_1 = b_1 \cdot q + r}$$

w/ $\boxed{\deg r < \deg b_1.}$ $\leftarrow$

r has monic prime factorisation:

$$r = \alpha \cdot r_1 \cdot \ldots \cdot r_m \quad (\alpha \in \mathbb{F}^\times)$$

and $b_1 \mid r_i \quad \forall\ 1 \le i \le m$

bcs of degree reasons.

Now

$$(*)\quad \underbrace{(q b_1 + \alpha r_1 \cdot \ldots \cdot r_m)}_{a_1} \cdot a_2 \cdot \ldots \cdot a_k = b_1 \cdot \ldots \cdot b_\ell .$$

Set $f' = r_1 \cdot \ldots \cdot r_m \cdot a_2 \cdot \ldots \cdot a_k .$

Then $(*)$ implies

$$(**)\quad f' = \alpha^{-1} b_1 (b_2 \cdot \ldots \cdot b_\ell - q a_2 \cdot \ldots \cdot a_k)$$

$$= r_1 \cdot \ldots \cdot r_m \cdot a_2 \cdot \ldots \cdot a_k$$

So we get two factorisations

of f where b_1 appers in one fact. but not in the other. and

$$\deg f' < \deg f$$

contradiction to minimality of $\deg f$. //

Def: Let $f, g \in F[x]$.

A greatest common divisor

$\gcd(f,g)$ is a poly that divides both f and g and is of maximal degree.

Rem if f, g are monic

$\gcd(f,g)$ is unique

$p_1 \cdots p_k \quad q_1 \cdots q_\ell$

if f or g are not monic

$\gcd(f,g)$ is unique up to multiplication by invertible element of $\alpha \in \mathbb{F}$.

Recall

Lem: For positive integers $a, b \in \mathbb{Z}$

$\exists\ u, v \in \mathbb{Z}$ s.th

$$au + bv = \gcd(u,v).$$

Pf: Consider the set

$$k = \{ au + bv \mid u, v \in \mathbb{Z} \}$$

and let k be the smallest element in k.

positive element

Since $k \in K$, $\exists\, u, v \in \mathbb{Z}$

s.th $k = au + bv$.

We can write

$$a = k \cdot q + r \quad \text{w/} \quad 0 \leq r < k$$

hence:

$$r = a - qk = a - q(au + bv)$$

$$= a(1 - qu) + b(-qv) \in K$$

$$\Rightarrow \quad r = 0$$

Thus $a = qk$ so $k \mid a$.

Similarly $k \mid b$ so

$$k \leq \gcd(a, b)$$

Since $\gcd(a,b) \mid a$ and

Since $\gcd(a,b) \mid a$

$\gcd(a,b) \mid b$

and $k = \underline{\underline{a}}u + \underline{\underline{b}}v$,

$\gcd(a,b) \mid k$

so $\underline{\gcd(a,b) \leq k}$

$au+bv = k = \gcd(a,b)$. //.

Lemma: Let $\mathbb{F}$ be a field and $a, b \in \mathbb{F}[x]$ monic. Then

$\exists\, u, v \in \mathbb{F}[x]$ s.th

$au + bv = \gcd(a,b)$

Pf: Consider

$$k = \{ au + bv \mid u, v \in \mathbb{F}[x] \}$$

Let $\underline{\underline{k}} \in k$ be an element

of smallest degree $\neq 0$.

$$k = au + bv.$$

We can write

$$a = k \cdot q + r \quad , \quad 0 \leq \deg r < \deg k.$$

$$r = a - qk = a - (au + bv)q$$

$$= a(1 - qu) + b(-qv) \in k$$

$$\Rightarrow \quad r = 0$$

$$\Rightarrow \quad a = k \cdot q$$

$\Rightarrow$ $k \mid a$ and similarly $k \mid b$ so

k is a common divisor of a and b, so

$$\deg k \leq \deg \gcd(a, b)$$

but $\gcd(a,b) \mid a$

and $\gcd(a,b) \mid b$

so $\gcd(a,b) \mid au + bv = k$

ie $\deg \gcd(a,b) \leq \deg k$

$\Rightarrow \deg \gcd(a,b) = \deg k$

Since we assume a, b are monic then

$$\gcd(a,b) = k = au + bv \; . \; //$$

Modulo arithmetic of poly's.

Let $\phi(x) \in \mathbb{F}[x]$ be of $\deg \phi = n$. We define

$$\mathbb{F}_{\phi} := \left\{ r(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \;\middle|\; a_i \in \mathbb{F} \;\forall i \right\}$$

$\mathbb{F}_{\phi(x)}$ [illegible]

the set of all possible remainders of long division

$f \,\%.\, \phi$ for $f \in \mathbb{F}[x]$

on $\mathbb{F}_{\phi(x)}$ we have

mod-ϕ arithmetic:

$r, s \in \mathbb{F}_{\phi(x)}$ ←

- $r+s \mod \phi := r+s$
- $r \cdot s \mod \phi := rs \,\%.\, \phi$

(these op'n are associative)

if $\begin{cases} r = f \mod \phi \\ s = g \mod \phi \end{cases}$

$$f = q \cdot \phi + r$$

$$g = t \cdot \phi + s.$$

$$f+g = (q+t)\phi + (r+s)$$

$$\Rightarrow \quad f+g \bmod \phi = r+s.$$

similarly

$$f \cdot g = r \cdot s \bmod \phi.$$

Thus $\underline{\underline{F_{\phi(x)}}}$ is almost a field

$-r$ is the additive inverse, 0 is neutral to addition, 1 is neutral to mult.

Thm: $F_{\phi(x)}$ is a field

$\mathbb{F}_{\phi(x)}$

iff $\phi \in \mathbb{F}[x]$ is prime.

Proof: If ϕ is not prime,

write $\phi = f \cdot g$ w

$1 \leq \deg f, \deg g < \deg \phi$.

then $f, g \in \mathbb{F}_{\phi(x)}$

and $f \cdot g = 0 \mod \phi$

so $\mathbb{F}_{\phi(x)}$ has zero divisors

and cannot be a field.

Conversly, suppose ϕ is prime,

and let $0 \neq r \in \mathbb{F}_{\phi(x)}$ (say monic)

Then $\gcd(r, \phi) = 1$

$\exists u, v \in \mathbb{F}[x]$ s.t.

hence $\exists\, u, v \in F[x]$ s.t.

$$ru + \phi v = 1$$

ie $ru = 1 \mod \phi$,

so u is a multiplicative inverse to r.

$\Rightarrow$ $\mathbb{F}_{\phi(x)}$ is a field. //

Cor: If $\mathbb{F} = \mathbb{F}_p$ and

$\phi \in \mathbb{F}_p[x]$ a prime poly

$\mathbb{F}_{\phi(x)}$ is a field

with p^n elements

where $n = \deg \phi$.

Example: Let us construct

a field w/ 4 elements.

Let $\mathbb{F} = \mathbb{F}_2$ and

$$\phi(x) = x^2 + x + 1.$$

ϕ has no roots over $\mathbb{F}_2$

hence ϕ is prime.

$$\boxed{\mathbb{F}_{\phi(x)}} = \{ 0, 1, x, x+1 \}$$

+	0	1	x	x + 1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

x	0	1	x	x + 1

	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

$x^2+x+1 = 0 \mod \emptyset$

$$x^2 = -(x+1) \mod (x^2+x+1)$$
$$= x+1 \mod \emptyset.$$

Note: There are prime poly's of arbitrarily large degree over $\mathbb{F}_p$: o/w there would be finitely many prime poly's over $\mathbb{F}_p$, say $a_1, \ldots, a_k$.

But then

$$a = a_1 \cdot \ldots \cdot a_k + 1$$

is also prime bcs

$$\forall i \quad a_i \nmid a$$

– contradiction