No reading this weekend.

Email about final projects soon.

Polynomial Rings: division, GCDs, Eucl. alg.

Stated: let F be a field e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$
but not $\mathbb{Z}$ or $\mathbb{Z}_6$ ...

let $f, g \in F[x]$ $\quad g \neq 0$

then $\exists\, q, r \in F[x]$ with $\deg r < \deg g$ or $r = 0$
and $f = qg + r$.

remainder.

quotient

Example: in $\mathbb{Z}_5[x]$

in $\mathbb{Z}_5$:

$\bar{1} + \bar{4} = \bar{0} \quad \bar{2} + \bar{3} = \bar{0}$

$\bar{2} \cdot \bar{3} = \bar{1} \quad \bar{4} \cdot \bar{4} = \bar{1}$

$$
\begin{array}{r|l}
 & \bar{3}x + \bar{1} \quad q \\
\hline
\bar{2}x^2 + x + \bar{1} & x^3 + \bar{0}x^2 + \bar{0}x + \bar{2} \quad \leftarrow f \\
g & -\ (\bar{1}x^3 + \bar{3}x^2 + \bar{3}x) \quad \leftarrow hg \\
\hline
 & \bar{0}x^3 + \bar{2}x^2 + \bar{2}x + \bar{2} \quad \leftarrow f - hg \\
 & -\ (\bar{2}x^2 + x + \bar{1}) \\
\hline
 & 0x^2 + x + \bar{1} \quad r
\end{array}
$$

$f = qg + r$

$\deg r = 1$

$\deg g = 2$

$1 < 2$ ✓

$\forall f \forall g \neq 0 \;\exists\, q, r$ $\deg r < \deg g$ and $f = qg + r$

Proof of thm: by induction on $\deg f$.

Base case: if $\deg f < \deg g$, just take $q = 0$ and $r = g$

Inductive step: Suppose we know the thm for all polys of $\deg < \deg f$.

Write $f = ax^n$ + lower terms. where $a, b \in F$ not zero

$g = bx^m$ + lower terms and $n \geq m$

consider $h = \frac{a}{b} x^{n-m}$ ← possible bc. we're in a field!

then $f - hg = ax^n + \Box x^{n-1} + \cdots$
$- \frac{a}{b} x^{n-m} (bx^m + \Box x^{m-1} + \cdots)$

$= ax^n + \Box x^{n-1} + \cdots$
$- ax^n + \Diamond x^{n-1} + \cdots$

= something of deg $< n$.

by inductive hypothesis, can write

$f - hg = q'g + r'$ where $\deg r' < \deg g$

then $f = (h + q')g + r'$

take $q = h + q'$ and $r = r'$.

$\boxtimes$

Actually we see that the alg works
as long as the leading coeff of g
is a unit in R.

For $\mathbb{Z}$, what did we do next?

1. given $a, b \in \mathbb{Z}$, consider

$$S = \{ am + bn \mid m, n \in \mathbb{Z} \} \subset \mathbb{Z}$$

then $\exists\, d \in \mathbb{Z}$ called the gcd of a and b
such that $S = \{$all multiples of $d\}$

proof: let d = smallest non-zero elt. of S...

2. Euclidean algorithm to find d
3. primes, unique factorization.

Same story works with $F[x]$ when F is a field.

1. given $f, g \in F[x]$, let

$$S = \{ f \cdot s + g \cdot t \mid s, t \in F[x] \} \subset F[x]$$

then $\exists\, d \in S$ such that $S = \{ d \cdot u \mid u \in F[x] \}$
"GCD of f and g"

proof: let d be an element of S of minimal degree...
details Friday.