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

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

quotient remainder

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

$$2x^2 + x + 1 \div x^3 + x^2 + x + 2 = f$$

$$- (x^3 + 3x^2 + 3x) \quad \in \text{ hg}$$

$$6x^3 + 2x^2 + 2x + 2 \quad \in \text{ f - hg}$$

$$\frac{f}{g} = f \div g$$

$\deg r = 1$

$\deg g = 2$

$1 < 2$ \checkmark
Proof of this: 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 theorem for all polynomials of degree $< \deg f$.

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

$g = bx^m + \text{lower terms}$ and $n < m$.

Consider $h = \frac{a}{b} x^{n-m} \leq \text{possible (even we're in a field!)}$.

Then $f - hg = ax^n + \sum x^{n-1} + \cdots$

$\quad - \frac{a}{b} x^{n-m}(bx^m + \sum x^{m-1} + \cdots)$

$\quad = ax^n + \sum x^{n-1} + \cdots$

$\quad = a x^n + \sum x^{n-1} + \cdots$

$\quad = \text{something of degree } < n$.

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 $r = r'$.\[\Box\]
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 $d \in \mathbb{Z}$ called the gcd of $a$ and $b$ such that $S = \{ \text{all multiples of } d \}$

Proof: let $d = \text{smallest non-zero elt. of } S$...

2. Euclidean Algorithm to find $d$

3. Primes, Unique Factorization.

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

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

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

Then $d \in S$ such that $S = \{ d.u \mid u \in F[x] \}$

"GCD of $f$ and $g"$

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