Cut to the chase

- Where do the finite fields come from? From $Z_p[x]$ itself.
- Fix $f \in Z_p[x]$ and write

$$g \equiv h \bmod f$$

  if f divides $g - h$.
- This is an equivalence relation just like conguences mod n was for integers.
- Notice that every $g \in Z_p[x]$ is equivalent to one with degree $< deg(f)$; in fact, if

$$g = qf + r$$

  then $g \equiv r \bmod f$.
- It follows that there are only finitely many equivalence classes of $Z_p[x]$ mod f.
- In fact, no two polynomials of degree $< deg(f)$ are equivalent and so there are p^n many equivalence classes of polynomials in $Z_p[x]$ mod f where $n = deg(f)$.

The object $Z_p[x]/(f)$

- Write $Z_p[x]/(f)$ for the equivalence classes of $Z_p[x]$ modulo f.
- As with the integers, addition and multiplication of equivalence classes of $Z_p[x]$ mod f is well-defined. That is,

  $$g \equiv g' \bmod f \text{ and } h \equiv h' \bmod f$$

  then

  $$g + h \equiv g' + h' \bmod f \text{ and } gh \equiv g'h' \bmod f.$$

- All basic rules of arithmetic now apply. In particular, the class of 0 is the additive identity and the class of 1 is the multiplicative identity.
- The rest of the properties of $Z_p[x]$ depend on the properties of f.

The object $Z_p[x]/(f)$ cont'd

- If f is reducible over Z_p, say $f = gh$ then $Z_p[x]/(f)$ is not a field since $gh = 0$ mod f but neither g nor h is 0 mod f.
- We want to show that if f is irreducible over Z_p then $Z_p[x]/(f)$ is a field. For this we need to develop the notion of gcd's of polynomials.

Definition

If $f, g \in Z_p[x]$ then $f = \mathrm{gcd}(g, h)$ if f is monic (has lead coefficient 1), divides g and h and if any other f' divides g and h then f' divides f.

- Claim: $\mathrm{gcd}(g, h)$ exists and is unique.

Take away about gcd's

- If $f \in Z_p[x]$ is irreducible, $g \in Z_p[x]$ is not 0 and of degree less than $deg(f)$ then $\gcd(f, g) = 1$.
- In fact, for such f and g, there are $x, y \in Z_p[x]$ such that $1 = xf + gy$.
- Conclusion: If $f \in Z_p[x]$ is irreducible then every non-zero element of $Z_p[x]/(f)$ has a multiplicative inverse i.e. $Z_p[x]$ is a field of size p^n where $n = deg(f)$.
- Examples: $Z_2[x]/(x^2 + x + 1)$ and $Z_2[x]/(x^3 + x + 1)$ are fields of size 4 and 8 respectively.

Main theorem of finite fields

Theorem

- *Every finite field is isomorphic to* $Z_p[x]/(f)$ *for some irreducible polynomial* f.
- *Up to isomorphism, there is exactly one field of size* p^n *for every prime* p *and* $n > 0$.
- *If* F *is a finite field of size* p^n *then there is some* $a \in F$ *such that the order of* a *is* $p^n - 1$ *i.e. the least* m *such that* $a^m = 1$ *is* $p^n - 1$.

Test information

- The second test will Nov. 1 at 1:30 (during class) in the T13, room 123.
- The test will be 50 minutes long.
- The topics covered will be those found in the lecture notes as well as sections 6.1 - 6.4 and 3.11.
- You are allowed to have the standard McMaster calculator, Casio fx-991 (no communication capability). No other aids are allowed. Please bring your ID with you.
- The best gauge of the level of the test is to look at the lecture notes, homework and practice problems.
- There will be a review class on Wednesday, Oct. 31 at 5:30 in HH 109. Please email me suggested review topics.
- I will have an office hour at 2:30 on Wednesday instead of my Thursday office hour.
- I will post practice problems from the text on the website soon.