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 $u, v \in Z_p[x]$ such that $1 = uf + vy$.
- 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 $p^n - 1$.*
- *In fact, for a field F of size p^n there is are $\phi(p^n - 1)$ many $a \in F$ of order $p^n - 1$.*