Math 152 Notes

Lucas Garron

October 6, 2009

20091006

Sections relevant to midterm are $\leq 2.3, 2.10, 2.11$

Corection: $q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum \tau(n)q^n = q - 24q^2 + 25q^3...$

What proved and of immediate importance (midterm!):
ϕ is the number of residue classes mod m prime to m. (Makes sense because GCD(a,m) depends only on the res. class of a mod m).
ϕ multiplicative: $GCD(m,n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$
$\phi(p^k) = p^k - p^{k-1}$ (and $\phi(p) = p - 1$)

$\phi(24) = \phi(3 \cdot 8) = \phi(3) \cdot \phi(8) = 2 \cdot 4 = 8$
$|\{1, 5, 7, 11, 13, 17, 19, 23\}| = 8$

Also from last time: $\sum_{d|n} \phi(d) = n$

Euler's Generalization of Fermat's Little Theorem:
$GCD(a,m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \bmod m$
($m =$ prime: Fermat, $a^{p-1} = 1 \bmod p$)
Prove this using ideas from group theory.

Let $b_1, b_2, ..., b_k$ where $k = \phi(m)$ be representatives of the res. classes mod$m$ prime to m.
(e.g. $m = 24, k = 8$: $\{1, 5, 7, 11, 13, 17, 19, 23\}$).
Check: $ab_1, ab_2, ..., ab_k$ are the same res. classes rearranged. $ab_i \equiv b_j$ for some unique j. Almost obvious:
$GCD(ab_i) = 1$ since $GCD(a,m) = GCD(b_i, m) = 1$;
So $ab_i \equiv b_j \exists j$. If $b_i \not\equiv b_{i'}$, then $ab_i \not\equiv ab_{i'} \bmod m$ since if not $m|ab_i - ab_{i'} = a(b_i - b_{i'})$ but $GCD(a,m) = 1$, so $m|b_i = b_{i'}$, contradiction. This proves that $b_i \mapsto ab_i$ is a permutation of these res. classes.
Multiply: $a^k\prod_{i=1}^{k}(b_i) \equiv \prod_{i=1}^{k}(ab_i) \equiv \prod_{i=1}^{k}(b_i) \bmod m$. $\prod b_i$ is prime to m so cancel and $a^k \equiv 1 \bmod m$.
QED.
Suppose $m = p$ odd prime. Then $\prod b_i = (p-1)!$

Wilson's Theorem: $(p-1)! \equiv -1 \bmod p$

Proof: Consider in Z_p = ring of residue classes mod$p$ prime to p each k which is a non-zero res. class (with rep. $a \leq k \leq p-1$) has an inverse in z_p, i.e. k' with $kk' \equiv 1 \bmod p$.

If $k \not\equiv \pm 1 \bmod p$, claim k, k' are distinct.

$k = 7 : k = k'$ only for $k = 1$ or 6.

$k^2 \equiv 1 \bmod p$ $(k-1)(k+1) \equiv 0 \bmod p$. So $p|k-1$ or $k+1$.

$k \equiv \pm 1 \bmod p \Rightarrow$ claim proved.

$$(p-1)! = 1 \cdot 2 \cdot ... \cdot (p-1) = 1 \cdot (p-1) \cdot \prod_{pairs(k,k')kk' \equiv 1, k \not\equiv k'} kk' \equiv 1(-1) \cdot 1 \cdot 1 \equiv -1 \bmod p.$$

A group G is a set with a composition law. This may be written additively or multiplicatively. Start multiplicative.

$m : G \times G \to G$ is then denoted by the usual signs for multiplication. $m(x,y) = x \times y = x \cdot y = xy$. (If additive: $m(x,y) = x + y$).

Axioms (multiplicative version):

$a(bc) = (ab)c$

$\exists 1 \in G$ with $1 \cdot a = a \cdot 1 = a$

$\forall a \exists o^{-1}$ with $aa^{-1} = a^{-1}a = 1$

Not assumed $ab = ba$. If true $\forall a, b$, the group is commutative, or Abelian. (Caution: Additive notation is not used for nonabelian G.)

If R is a ring, there are two groups:

$(R, +)$ (R is an Abelian group with respect to +).

Def.: $R^\times$ = set of units in $R = \{x \in R | xy = yx = 1$ for some $y\}$ (y denoted x^{-1}) is a group with respect to x.

If $R = Z_m \Rightarrow (R, +)$ has order m, $(R^\times, x)$ has order $\phi(m)$

$m = G$, $R^\times = \{\bar{1}, \bar{6}\} = \{\bar{1}, \overline{-1}\}$.

To clarify, if $GCD(a, m) = 1$, and $\bar{a}$ = res. class of a mod m, then $\bar{a}$ is a unit. $ka + lm = 1$ some $k, l \Rightarrow \bar{k} = \bar{a}^{-1}$.

Theorem: If G is a finite group of order N (i.e. G has N elements) and $a \in G \Rightarrow a^N = 1$ in G.

Proof require notion of cosets $\in$ Math 120. Special case G Abelian has easy proof:

The map $f : G \to G$

$f(x) = ax$ is a bijection since it has an inverse $g(x) = a^{-1}x$ f g(x) = x = g f(x), so since G is Abelian $\prod_{x \in G} x$ is well-defined () Abelian).

Since f is a bijection $G \to G$, $\prod_{x \in G} f(x) = \prod_{x \in G} (ax) =_{(G Abelian)} a^N \prod_{x \in G} x$ cancel $\prod x$ from both sides $a^N = 1$.

Section 2.7 (hopefully)

Congruences of the form $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \equiv 0 \bmod p$

($a_n \neq 0 \bmod p$ can't hurt to assume).

More generally, $f(x) \equiv 0 \bmod m$ where m is any modulus.

Theorem: If p is prime, $f(x) \equiv 0 \bmod p$ has at most n roots mod$p$.

False for $n = 8$ composite: $x^2 - 1 = 0 \bmod 8$ has sols $1, 3, 5, 7$

Ex. $x^3 + x^2 + x + 1 \bmod 2 \equiv (x+1)(x^2+1) = (x+1)(x+1)^2 = (x+1)^3$ has root $1 \equiv -1 \bmod 2$

with multiplicity 3.
Reformulate this in the field $F = Z_p$.
(Field is a commutative ring with $R^\times = R - \{0\}$ all nonzero elements are units).

Theorem: In a field, any polynomial of degree n has at most n roots.
$f(x) = a_n(x^n + \frac{a_{n-1}}{a_n} + ... + \frac{a_0}{a_n}) = a_n f_1(x)$
Roots of f, f_1 are the same, so WLOG $a_n = 1$.
If q is a root, may divide f by $x - q$.

Theorem: In any field (e.g. $C, Z_p, R, Q, ...$), any poly. of degree n has $\leq n$ roots.
If f, g polynomials, $deg(g) = d$, can write $f(x) = g \cdot q(x) + r(x)$, q, r are polynomials, $deg(r) < deg(d)$. If α is a root, divide: $f = (x - \alpha)q + r$.
r is a polynomial of degree $< 1 < deg(x - \alpha) \Rightarrow r$ is a constant.
Evaluate by substituting $x = \alpha$. $0 = f(\alpha) = (\alpha - \alpha)q + r$. So r is the constant 0, i.e. $x - \alpha$ divides f.
$f(X) = (x - \alpha)q(x)$. Degree of q (which is n-1) ¡ degree of f, so by induction q has $\leq n - 1$ roots.
So f has roots α, plus the roots of q, $\leq n$ altogether.
$\Rightarrow Z_p^\times$ is a cyclic group.