Math 152 Notes

Lucas Garron

October 15, 2009

20091015

Midterm 1, Problem 5:
Show that if $GCD(m, n) = 1$, and
(1) ($x^2 \equiv 1 \bmod m$ has a solution) and ($y^2 \equiv 1 \bmod n$ has a solution) $\Rightarrow$ ($z^2 \equiv 1 \bmod mn$ has a solution).
a is a solution to $x^2 \equiv -1 \bmod m$
b is a solution to $x^2 \equiv -1 \bmod n$
CRT $\Rightarrow \exists r$ with $r \equiv a \bmod m$ and $r \equiv b \bmod n$
$r^2 \equiv a^2 \equiv -1 \bmod m$ and $r^2 \equiv b^2 \equiv -1 \bmod n$
$\Rightarrow r^2 \equiv -1 \bmod mn$

A group G of order n is <u>cyclic</u> (with generator x) if $G = 1, x, x^2, ..., x^(n-1)$
If this is true, $x^n = 1$, and in fact $x^k = 1 \Leftrightarrow n|k$.
Theorem: p prime $\Rightarrow \mathbb{Z}_p$ cyclic of order $p - 1$.
If m is composite, $\mathbb{Z}_m^x$ = group of res. classes prime to m has order $\phi(m)$ may or may not be cyclic.
If $\mathbb{Z}_m^x$ is cyclic, a generator is called a <u>primitive root</u>.

Saw Thursday, <u>Theorem</u>: if F is a field (e.g. $F = \mathbb{Z}_p$), any monic (leading coefficient 1) polynomial $x^k + a_{k-1}x^{k-1} + ... + a_0$, $a_i \in F$, has at most k roots, i.e. $\{r \in F | f(r) = 0\}$ has $\leq k = deg(f)$.
We know $x^{p-1} = 0$ has exactly $p - 1$ roots in $F = \mathbb{Z}_p$ (namely, the non-zero res. classes.)
<u>Lemma</u>: If $d|p-1$, then $x^d - 1 = 0$ has exactly d roots.
Proof: It has $\leq d$ roots, by theorem.
$\frac{x^{p-1}-1}{x^d-1} = x^{p-d-1} + x^{p-2d-1} + ... + x^d$ $(d|p-1)$
$x^{p-1} = (x^d - 1)(x^{p-d-1} + x^{p-2d-1} + ... + x^d) = (x^d - 1)g(x)$
Since $x^{p-1} = 0$ has $p-1$ roots, if $x^d - 1$ had $< d$ roots then $g(x)$ would have $> p-d-1$ roots, namely the roots of $x^{p-1}-1$ that are not roots of $x^d - 1 = 0$. This is a contradiction, since $p-d-1 = deg(g)$.

If $d|p-1$ define $\psi(d)$ = the number of $a \in F^\times = \mathbb{Z}_p^x$ with order d ("belonging to d"). a^d and $a^k = 1 \Leftrightarrow d|k$ order of a is cardinality of $\{1, a, a^2, ..., a^k\}$.
$\psi(1) = 1, \psi(2) = 2, \psi(2) = 1, \psi(6) = 2$ (We'll prove $\psi(d) = \phi(d)$).
<u>Lemma</u> If $m|p-1 \Rightarrow m = \sum_{d|m} \psi(d)$
Because: $a \in F$ is a root of $x^m - 1 \Leftrightarrow$ order of a divides m. There are $\psi(d)$ of these for each possible order d of a $inF^\times$.

Counting, $m = \#$ of roots of $x^m - 1 = \sum_{d|m} \#$ of elts of order d $= \sum_{d|m} \psi(d)$.
If $m|p-1$, $\sum_{d|m} \psi(d) = m = \sum_{d|m} \phi(d)$.
Claim: If $m|p-1 \Rightarrow \psi(m) = \phi(m)$.
If not, let m be a minimal counterexample, so $\psi(d) = \phi(d)$. If $d|p-1$ and $d < m$.
$\psi(m) = m - \sum_{d|m, d<m} \psi(d) \underset{induction}{=} = m - \sum_{d|m, d<m} \phi(d) = \phi(m)$. Completes the proof of proposition.

You can prove (using Hensel's Lemma) if p is an odd prime, there are primitive roots modp^k for all k
if $p = 2$, false. $\mathbb{Z}_{2^k}^\times$ (a group of order $2^{k-1} = C_2$ (cyclic group of order 2) $\times C_{2^{k-2}}$ (cyclic group of order 2^{k-1}))

"Chinese Remainder Theorem": The arithmetics in $\mathbb{Z}_m$ and $\mathbb{Z}_n$ ($GCD(m, n) = 1$) are independent.
For example: If $f(x) = x^k + a_{k-1}x^{k-1} + ... + a_0$ ($a_i \in \mathbb{Z}$) is a monic polynomial, it may or may not have solutions in $\mathbb{Z}_m$, same $\mathbb{Z}_n$.
It a solution in $\mathbb{Z}_{mn} \Leftrightarrow$ has a solution in $\mathbb{Z}_n$ and one in $\mathbb{Z}_m$.

We'll prove:
Suppose p, q are distinct, odd primes, $p \not| a$, $q \not| a$, and $x^2 \equiv a \bmod p$ has a solution:
$x^2 \equiv a \bmod p$ has a solution $\Leftrightarrow$ has exactly two solutions.
Say a is a "quadratic residue" mod$p$ if this is true.
Proposition: Exactly $\frac{1}{2}(p-1)$ of the $p-1$ res. classes prime to p are quadratic residues.
($p = 7$: 1, 2, 4 are quadratic residues; 3, 5, 6 quadratic nonresidues (not quadratic residues))

Quadratic Reciprocity: p is a QR mod$q \Leftrightarrow q$ is a QR mod$p$ UNLESS $p \equiv q \equiv 3 \bmod 4$, in which case p is a QR mod$q \Leftrightarrow q$ is a QNR mod$p$

First proof: (not using $\mathbb{Z}_p^\times$ is cyclic). p odd prime, $p \not| a$.
Lemma: If $x^2 \equiv a \bmod p$ has a solution, it has exactly 2 solutions.
Let u be one solution, $-u$ is another ($(-u)^2 \equiv u^2 \equiv a \bmod p$).
Claim: If $v^2 \equiv a \Rightarrow v \pm u$ because $p|v^2 - a = v^2 - u^2 = (v-u)(v+u) \Rightarrow p|(v-u)$ or $p|(v+u) \Rightarrow v = \pm u \bmod p$ ($x^2 - a$ cannot have > 2 roots)
$p-1$ pigeons, p-1 boxes, 2 pigeons in each box. $\Rightarrow \frac{1}{2}(p-1)$ boxes with pigeons.
More formally, map $\gamma : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$, $\gamma(x) = x^2$.
This map is 2-1 (lemma), so the image has $\frac{1}{2}(p-1)$ elements.
Second Proof: Consider a cyclic group with m elements with (e.g. $m = p-1$) $d|m$ (e.g. $d = 2$).
Define $\gamma : G \to G$, $\gamma(x) = x^d$.
Claim: image of γ has order $\frac{m}{d}$.
Because: G has a generator g, $G = \{1, g, g^2, ..., g^{m-1}\}$.
Consider the subgroup of G generated by g^d. Call it H. $H = \{1, g^d, g^{2d}, ..., g^{d(\frac{m}{d}-1)}\}$; H has order $\frac{m}{d}$.
But H is just the image of γ.
γ(typical element) $= \gamma(g^k) = g^{dk}$, so image of γ has exactly $\frac{m}{d}$ elements all lying in a subgroup (subset of G closed under multiplication).
Applying this in the case $G = \mathbb{Z}_p^\times$, $m = p-1$, $d = 2 \underset{secondproof}{\Rightarrow} H =$ image of $\gamma =$ quad. res.