Math 152 Notes

Lucas Garron

October 20, 2009

20091020

When are two polynomials equivalent (or congruent)?
$x^p - x \equiv 0 \bmod p \forall x \in \mathbb{Z}$
$x^p - x \equiv 0 \forall x \in \mathbb{Z}_p$
$x^p - x$ in ring $\mathbb{Z}_p[x]$ is NOT zero.
$x^p - x \equiv 0 \bmod p$ is not a congruence of polys.
$x^p - x = 0$ for all $x \in \mathbb{Z}_p$
$\mathbb{Z}_p \subset$ larger fields with p^r elements for any r
$\mathbb{Z}_p[x]$ polynomial ring is a unique factorization domain. So you can define ideals, factor into irreducibles, etc. You would lose this algebra if you declare $x^p - x = 0$.

p an odd prime.
If $GCD(a,p) = 1$ we call a a quadratic residue if $x^2 \equiv a \bmod p$ has a solution $x = b$. Then $x = -b$ is also a solution, so the equation has exactly two solutions.
If $c^2 \equiv a \bmod p$, $c^2 \equiv b^2 \Rightarrow (c-b)(c+b) = c^2 - b^2 \equiv 0 \Rightarrow c = \pm b$ (c, b are the only roots).
$Ax^2 + Bx + C \equiv 0$ will have roots
$\Rightarrow D = B^2 - 4AC \equiv 0 \bmod p$ or D is a QR.
Work in $\mathbb{Z}_p$; $Ax^2 + Bx + C \equiv 0$ $(\frac{B^2-AC}{4A}) + A(x - \frac{B}{2A})^2 = Ax^2 + Bx - \frac{B^2}{4A} - (\frac{B^2-AC}{4A}) = Ax^2 + Bx + C$.
This is zero $\Rightarrow (x - \frac{B}{2A})^2 = \frac{D}{4A^2}$.
So D must be a square mod$p$, i.e. a QR.

Euler's criterion: Let $GCD(a,p) = 1$.
Then a is a QR $\Rightarrow a^{\frac{p-1}{2}} = 1 \bmod p$.
Observe: In any case $a^{\frac{p-1}{2}} \equiv \pm 1$ because if $a^{\frac{p-1}{2}} = \lambda$, $\lambda^2 = a^{p-1} \equiv 1 \bmod p \Rightarrow x \equiv \pm 1 \bmod p$.

Proof of Euler's criterion:
Suppose a is a QR $\Rightarrow a = b^2 \bmod p$
$a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} = 1 \bmod p$
$\Leftarrow$ Let g be a primitive root $a \equiv g^k \bmod p$ for some k
$a^{\frac{p-1}{2}} = g^{\frac{k}{2}(p-1)}$ so k must be even.
Let $c = g^{\frac{k}{2}}$. $c^2 \equiv g^k \equiv a \bmod p \Rightarrow a$ is a QR.

Paraphrase: If G is a cyclic group or order $2n$ (e.g. $2n = p-1$), $x \in G \Leftrightarrow x^N = 1$ in G (proof same).
More generally, if G is a cyclic group of order $MN \Rightarrow a \in G$ is a solution of $x^M = a \Leftrightarrow a^M = 1$

(Taking $M = 2$ gives previous statement.)
Proof: If g is a generator, $a = g^k$ for some k
$a^N = 1 \Leftrightarrow g^{Nk} = 1 \Leftrightarrow NM|Nk$ since $NM =$ order of $g \Leftrightarrow M|k$.
If this is true, $a = g^k = b^n$, where $b = g^{\frac{k}{M}}$
"Euler's criterion is just a reflection of the fact that the group is cyclic."

Euler: a is a QR $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$.
Special case: -1 is a QR $\Leftrightarrow p \equiv 1 \bmod 4$.
Because $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1$ (Since $p \neq 2$ both $(-1)^{\frac{p-1}{2}}, 1$ are ± 1).
Surprising: This depends only on $p \bmod 4$.
Even more surprising: hether z is a QR depends only on $p \bmod 8$. We'll prove later 2 is a QR $\Leftrightarrow p \equiv \pm 1 \bmod 8$
If $p \equiv q \bmod 8$ (odd primes), 2 is a QR mod$p \Leftrightarrow$ 2 is a QR mod$q$

Legendre Symbol: I $(a, p) = 1$,
$(\frac{a}{p}) = 1$ if a is a QR mod$p$
$(\frac{a}{p}) = -1$ if a is a QNR mod$p$

Clear: If $a \equiv b \bmod p \Rightarrow (\frac{a}{b}) = (\frac{b}{p})$
Less clear: Given a $\exists M = M(a)$ s.t. if $p \equiv q \bmod M \Rightarrow (\frac{a}{p}) = (\frac{a}{q})$
$a = -1 \Rightarrow M = 4$,
$A = 2, M = 8$
Fact: $(\frac{ab}{p}) = (\frac{a}{p})(\frac{a}{p})$
Proof: $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\frac{b}{p})$
Both sides are ± 1, so they are equal.

Def (pg. 404 in book): Let M be some modulus. A Dirichlet character mod$M$ is a function χ on the res. classes mod$M$ prime to M such that $\chi(ab) = \chi(a)\chi(b)$.
Note: We extend χ to all res. classes by $\chi(a) = 0$ if $GCD(a, M) \neq 1$ and $\chi(ab) = \chi(a)\chi(b)$ remains true.

So $\chi(a) = (\frac{a}{p})$ gives a Dirichlet character mod$p$.
Much deeper: Given a, there is a Dirichlet character χ' mod $M(a)$ s.t. if p is an odd prime $(\frac{a}{p}) = \chi'(p)$

Gauss' Lemma: Consider the least residues of $a, 2a, ..., \frac{p-1}{2}a \bmod p$ ($k \equiv r \bmod p$, $0 \leq r \leq p$; r is called the least residue of $k \bmod p$ (remainder on dividing k by p)).
Let $n =$ the number of these least residues that are $> p/2$. Then $(\frac{a}{p}) = (-1)^n$.

Let $a = 2, p = 11, \frac{p-1}{2} = 5$
$2, 4, 6, 8, 10$ have least res.
$2, 4, 6, 8, 10$.
Of these $6, 8, 10 > \frac{11}{2}$, so $(\frac{2}{11}) = (-1)^3 = -1 \bmod 11$
(Using Gauss' Lemma you can prove $(\frac{2}{p})$ if $\substack{p \equiv \pm 1 \bmod 8 \\ p \equiv \pm 3 \bmod 8}$).

$a = 3, p = 11$

$3, 6, 9, 12, 15$ are
$3, 6, 9, 1, 4$.
Two (6,9) are $> \frac{11}{2}$; $(\frac{3}{11})$.
(And indeed, $5^2 \equiv 3 \bmod 11$ QR).

Proof of Gauss' Lemma:
Let $r_1, r_2, ..., r_n$ be the least residues of the numbers among $a, 2a, 3a, \frac{p-1}{2}a$ that satisfy $r_i > \frac{p}{2}$. Let $s_1, s_2, ..., s_m$ be the least res. $< \frac{p}{2}$.
We have $a(2a)(3a)...(\frac{p-1}{2}a) = a^{\frac{p-1}{2}}(\frac{p-1}{2})! \equiv (\frac{p-1}{2})!(\frac{a}{p})$
$\equiv r_1...r_n \cdot r_1...r_m$ (are $1, 2, ..., \frac{p-1}{2}$ rearranged?)
Claim: $s_1, ..., s_m, p - r_1, .., p - r_m$ are all in $1 \leq x \leq \frac{p-1}{2}$
If $n = \#$ of least res. of $a, 2a, ... \frac{p-1}{2}a$ that are $> \frac{p}{2} \Rightarrow (\frac{a}{p}) = (-1)^n$.
Enough to show no repetitions among s_i.
If $s_i \equiv s_j \Rightarrow s_i = ta$ ($t \in \{1, 2, ..., \frac{p-1}{2}\}$), $s_j \equiv ua$.
$\Rightarrow t \equiv u$ impossible unless $t = u$. Similarly no rep. among r_j, hence none among $p - r_j$. Have to exclude $s_i = p - r_j$.
$s_i \equiv ta, r_j \equiv ua$ if $s_i = p - r_j \Rightarrow ta = p - ua \Rightarrow t + u \equiv 0 \bmod p$. Also impossible with $t, u \in \{1, 2, ..., \frac{p-1}{2}\} \Rightarrow$ claim proved.
$(\frac{p-1}{2})! = s_1...s_m \cdot (p - r_1)...(p - r_n) \equiv s_1...s_m \cdot r_1...r_m(-1)^n \equiv (\frac{p-1}{2})!(\frac{a}{p})(-1)^n$ (from before).
Cancel $(\frac{a}{p})(-1)^n \equiv 1 \Rightarrow (\frac{a}{p}) = (-1)^n$