Math 152 Notes

Lucas Garron

October 27, 2009

20091027

Question: If m is compoosite, how many solutions to $x^2 \equiv\ a \bmod m$ are there?
Assume m odd (for simplicity).
By CRT if $m = m_1 m_2$, m_1, m_2 coprime, then # of sols to $x^2 \equiv a \bmod m$ = product of the # of sols for m_1 and m_2.
Reduced to the case $m = p^k$ (assume p odd).
Claim: If x_1 is a solution to $x^2 \equiv a \bmod p^j$ $(j \geq 1)$
There is a unique $x_{j+1} \bmod p^{j+1}$ solving $x^2 \equiv a \bmod p^{j+1}$
Proof of claim: $x_j^2 \equiv a \bmod p^j$ so let $x_j^2 \equiv a + \lambda p^j \bmod p^{j+1}$ such that $x^{j+1} \equiv x_j \bmod p^j$
Let us ask for a condition of μ $(0 \leq \mu < p)$ such that $(x_j + \mu p^j)^2$ is a solution to $x^2 \equiv a \bmod p^{j+1}$
$x_j^2 + 2\mu p^j + \mu^2 p^2 j \equiv a + \lambda p^j + 2\mu p^j \bmod p^{j+1}$
Need $(\lambda + 2\mu)p^j \equiv \bmod p^{j+1}$ or $\lambda + 2\mu \equiv 0 \bmod p$
There is a unique $\mu \bmod p$. Therefore, there is a unique $x_j + 1 \bmod p^{j+1}$

Hensel's Lemma: If $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ has a root $f(x_1) \equiv 0 \bmod p^j$ AND $f'(x_2) \not\equiv 0 \bmod p \Rightarrow \exists x_{j+1} \bmod p^{j+1}$ such that $x_{j+1} \equiv x_j \bmod p^j$ and $f(x_{j+1}) \equiv 0 \bmod p^{j+1}$

Proposition: $(\frac{2}{p}) = 1$ if $p \equiv \pm 1 \bmod 8$, -1 if $p \equiv \pm 3 \bmod 8$
Proof:
$(\frac{2}{p}) = (-1)^n$, $n = \#of 2, 4, ..., 2(\frac{p-1}{2})$ (i.e. $2, 4, ..., p-1$) whose least res. $\bmod p$ is $> \frac{p}{2}$
$= \#$ of i in $1, 2, ..., \frac{p-1}{2}$ such that $2i > \frac{p}{2}$, $\frac{p}{4} < i \leq \frac{p-1}{2}$, i.e. $\frac{p}{4} < i < \frac{p}{2}$. So $n = [\frac{p}{2}] - [\frac{p}{4}]$
Observe that the parity of $[\frac{p}{2}] - [\frac{p}{4}]$ only depends on $k \bmod 8$.
$k \equiv 1 \bmod 8 \rightarrow [\frac{1}{2}] - [\frac{1}{4}] = 0$ $k \equiv 3 \bmod 8 \rightarrow [\frac{3}{2}] - [\frac{3}{4}] = 1$ $k \equiv 5 \bmod 8 \rightarrow [\frac{5}{2}] - [\frac{5}{4}] = 1$ $k \equiv 7 \bmod 8 \rightarrow [\frac{7}{2}] - [\frac{7}{4}] = 2$
Conclusion: n is odd if $p \equiv 3$ or $5 \bmod 8$, even if $p \equiv 1$ or $7 \bmod 8$
Call this $\chi(k)$. It's a Dirichlet character: $\chi(ab) = \chi(a)\chi(b)$
Given any a $\exists$ a Dirichlet character χ_a such that $(\frac{a}{p}) = \chi_a(p)$ for odd primes p.
$m = 8$ if $a = 2$
$\chi(c + m) = \chi(c)$
$\chi(cb) = \chi(c)\chi(b)$
$\chi(c) = 0$if $(m, c) = 1$

Consider the primes 37747 and 17729.
$(\frac{17729}{37747}) = (\frac{37747}{17729})$ (because $17729 \equiv 1 \bmod 4$) $(\frac{2289}{17729})$ $(37747 \equiv 2289 \bmod 17729)$
$= (\frac{3}{17729})(\frac{7}{17729})(\frac{109}{17729})$

$= (\frac{17729}{3})(\frac{17729}{7})(\frac{17729}{109})$ (due to $\equiv 1$ above again)
$= (\frac{2}{3})(\frac{5}{7})(\frac{71}{109})$
$= (-1)(-1)(1)$
$= 1$
$((\frac{2}{3}) = -1$, $(\frac{5}{7}) = (\frac{7}{5}) = (\frac{2}{5}) = -1)$
$((\frac{71}{109}) = (\frac{109}{71}) = (\frac{38}{71}) = (\frac{2}{71})(\frac{19}{71}) = (\frac{19}{71}) = -(\frac{71}{19}) = -(\frac{2}{19})(\frac{7}{19}) = -(-1)() = (\frac{7}{19}) = -(\frac{19}{7}) = -(\frac{5}{7}) =$
$-(\frac{7}{5}) = -(\frac{2}{5}) = 1)$
Thus, $\exists x$ s.t. $x^2 \equiv 17729 \bmod 37747$

Jacobi Symbol: defined for $(\frac{p}{q})$, p, q odd, coprime (else $(p,q) > 1 \Rightarrow (\frac{p}{q}) = 1$)
If q is prime, it is the Legendre symbol.
It has some of these properties:
$(\frac{p_1 p_2}{q}) = (\frac{p_1}{q})(\frac{p_2}{q})$, $(\frac{p}{q_1 q_2}) = (\frac{p}{q_1})(\frac{p}{q_2})$
$p_1 \equiv p_2 \bmod q \Rightarrow (\frac{p_1}{q})(\frac{p_2}{q})$
$(\frac{p}{q}) = \pm(\frac{q}{p})$ where the sign is $+$ if $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$, $-$ if $p \equiv q \equiv 3 \bmod 4$
$(\frac{2}{q})$ as before.

Big difference: If q is not prime, $(\frac{p}{q})$ does not detect whether p is a Q.R. mod$p$
$(\frac{2}{3 \cdot 5}) = (\frac{2}{3})(\frac{2}{5}) = (-1)^2 = 1$
But 2 is not a Q.R. mod15 (nor 3, 5).
Definition: If we factor Q into odd primes, $Q = q_1 ... q_r$
$(\frac{p}{Q}) = \prod (\frac{p}{q_i})$ (Legendre symbols)
Proposition: $(\frac{-1}{Q}) = (-1)^{\frac{Q-1}{2}}$ (1 if $Q \equiv 1 \bmod 4$, -1 if $Q \equiv 3 \bmod 4$)
$(\frac{2}{q}) = (-1)^{\frac{Q-1}{2}}$ ($= 1$ if $Q \equiv \pm 1 \bmod 8$, -1 if $Q \equiv \pm 3 \bmod 8$)
Proof: Define $\chi_4(a) = 1$ if $a \equiv \pm 1 \bmod 4$, -1 if $a \equiv \pm 3 \bmod 4$,
$\chi_8(a) = 1$ if $a \equiv \pm 1 \bmod 8$, -1 if $a \equiv \pm 3 \bmod 8$
$\chi_4(a) = \chi_8(a) = 0$ if a is even.
Both are multiplicative.
...
$(\frac{-1}{Q}) = \prod (\frac{-1}{q_i}) = \prod \chi_4(q_i) = \chi_4(\prod q_i) = \chi_4(Q)$
$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \chi_4(p)^{\frac{q-1}{2}} = \chi_4(q)^{\frac{p-1}{2}}$
Def $M(a,b) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ ($M(a,b) = 0$ if either argument is even)
M is bilinear. In this context, this means $M(a_1 a_2, b) = M(a_1, b)M(a_2, b)$ (same over second arg)
Can check cases $b = 1$ ($M(a_1 a_2) = 1M(a_1, b)M(a_2, b)$), $b = 3$ (use χ_4)

Theorem: If p and q are odd, coprime, $(\frac{p}{q})(\frac{q}{p}) = M(P, Q)$
$(P,Q)(\frac{Q}{P}) = \prod_{i,j} (\frac{p_i}{q_j})(\frac{q_j}{p_i}) = \prod_{i,j} M(p_i, q_j) = \prod_i M(p_i, \prod_j q_j) = M(\prod_i p_i, \prod_j q_j) = M(P,Q)$