Math 152 Notes

Lucas Garron

October 29, 2009

20091029

Count solution points to $ax^2 + by^2 =$ over $\mathbb{Z}_p$ (p odd).
$d = -ab$
$(ax)^2 + aby^2 = a$
$(ax)^2 - dy^2 = a$; make var change: $x \to ax$
$x^2 - dy^2 = a$; assume $a, b \neq 0$ in $\mathbb{Z}_p$, so $d \neq 0$.
Two cases:
If d is a square (i.e. $(\frac{-ab}{p}) = 1$)
There will be $p - 1$ elements.
$d = c^2$, $x^2 - (cy)^2 = a$, $c \neq 0$
$(x - cy)(x + cy) = a$
$u = x - cy$, $v = x + cy$
$x = (u + v)/2$, $y = \frac{1}{2c}(v - u)$
$uv = a$; There are $p - 1$ solutions:
$u \neq 0$ and $v = \frac{a}{u}$, $p - 1$ possibilities.

Let F be any field, $d \in F$ a non-square.
Examples:
$F = \mathbb{R}, d = -1$
$F = \mathbb{Z}_p, d$ any QNR (p prime)
Claim: $\exists$ a bigger field $K \supset F$ where d has a square root.
Let K be all formal linear combinations $\{a + b\sqrt{d} | a, b \in F\}$
$(a + b\sqrt{d})(a' + b'\sqrt{d}) = a'' + b''\sqrt{d}$
This would produce a ring even if d is a square.
Why is this a field?
$Q = a \neq a + b\sqrt{d}$ (so a, b not both 0)
Claim: $\frac{a - b\sqrt{d}}{a^2 - b^2 d}$ is an inverse: denominator is never 0 (else $a^2 - b^2 d = 0 \Rightarrow d = (\frac{a}{b})^2$, contradicting assumption of no square root in F).

There is a map $N : K \to F$ "norm" map, $N(xy) = N(x)N(y)$ multiplicative:
$N(a + b\sqrt{d}) = a^2 - b^2 d$
$N(a + b\sqrt{d}) = (a + d\sqrt{d})(a - b\sqrt{d})$
$(N(x) = x \cdot \overline{x}$, $\overline{a + b\sqrt{d}} = a - b\sqrt{d})$
$\overline{x + y} = \overline{x} + \overline{y}, \overline{xy} = \overline{x} \cdot \overline{y}$ (A "Galois Automorphism")

Essentially: Since $-\sqrt{d}$ is another square root of d, we can substitute it without changing the addition and multiplication.
So $N(xy) = xy\overline{xy} = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$.

Take $F = \mathbb{Z}_p$, d a nonsquare.
$K = F(\sqrt{d})$ - we've constructed a field with p^2 elements.
This is not $\mathbb{Z}/p^2\mathbb{Z}$ (which would not be a field).

Theorem: If K is a any field with q elements ($q < \infty$), then $K^\times$ is cyclic of order $q-1$.
Observe if $f(x)$ is any polynomial of degree d, then f has $\leq d$ roots (true for any field, e.g. K)
Claim: If $d|q-1$ then $x^d - 1$ has exactly d roots in K. It has $\leq d$ roots, and cannot have more...
$x^{q-1} = 0$ has exactly $q-1$ roots.
(Analog of Fermat's Theorem) since $X^\times$ is a group of order $q-1$, so everey element satisfies $x^{q-1} = 1$, i.e. is a root of $x^{q-1} - 1$
If $x^d - 1$ had $< d$ roots, then $\frac{x^{q-1}-1}{x^d-1} = x^{q-d-1} + x^{q-2d-1} + ... + 1$ (would have $> (q-1) - (q-1-d) = d$ roots, a contradiction)

Claim: # of $X \in K^\times$ having order d (where $d|q-1$) is exactly $\phi(d)$
$\psi(d) =$ # of $x \in K^\times$ with order exactly d, $x^d - 1 = 0 \Leftrightarrow$ order r of x ($\psi(r)$ of these) divides d giving equation. ($r =$ smallest r with$x^r = 1$)
So $\displaystyle\sum_{r|d} \psi(r) = d, \sum_{r|d} \phi(r) = d$

If d is the smallest divisor of $q-1$ such that $\psi(d) \neq \phi(d) \Rightarrow \phi(d) = d - \displaystyle\sum_{r|d, r<d} \psi(d) = d - \sum_{r|d, r<d} \phi(d) \underset{\text{(induction hypothesis)}}{=} \phi(d)$
So there are $\phi(q-1)$ elements of order $q-1$, $\Rightarrow K^\times$ cyclic.

Theorem: IF d is notn a square in $\mathbb{Z}_p$ and $d \neq 0$, then $x^2 - dy^2 = a$ has exactly $p+1$ solutions.
(Sanity check: $p^2 - 1$ choices for x, y (not both 0), $p-1$ choices for a and $(p-1)(p+1) = p^2 - 1$)
$K^\times =$ multiplicative group of $K = F(\sqrt{d})$ $F = \mathbb{Z}_p$ is cyclic of order $p^2 - 1$. Let g be a generator.
$F^\times =$ a cyclic subgroup of order $p-1$
Lemma: $g^h \in F^\times \Leftrightarrow p+1|k$ (g^{p+1} generates a cyclic group of order $\frac{p^2-1}{p+1} = p-1$)
A cyclic group of order n has exactly m elements that satisfy $x^m = 1$, where m is any divisor of G. If g is a generator of G, $g^{\frac{n}{m}}$ generates a cyclic subgroup of G of order m and this is the unique such subgroup.
If $G = K^\times, n = p^2 - 1, m = p - 1, \frac{n}{m} = p + 1$ this subgroup is $F^\times$.

Theorem: $x \to \overline{x}$ maps $x \to x^p$, $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$
Proof: Let $f(x) = x^p$
$F(xy) = f(x) + F(y), f(xy) = f(x)f(y)$ (expand binomial cofficients: $f(x+y) = (x+y)^p = x^p + (0 \text{ in } \mathbb{Z}_p) + y^p = x^p + y^p = f(x) + f(y)$)
And $f(x) = x$ if $x \in F$ by Fermat, $x^p = x$ in $\mathbb{Z}_p = F$
Observe $f(\sqrt{d}) = -\sqrt{d}$ since if $f(\sqrt{d}) = \lambda$, $(\sqrt{d})^2 = d$, so $f(\sqrt{d})^2 = f(d) \underset{d \in F}{=} d$
So $f(\sqrt{d})$ is another square root of d.It can't be $\sqrt{d}$ since then f would be the identity map so $x^p = x$ would have p^4 roots.

$f(x) = x^p$ (def.)
$f(x+y) = f(x) + f(y)$
$f(xy) = f(x)f(y)$
$f(x) - x \Leftrightarrow x \in F$
If $f(\sqrt{d}) = \sqrt{d}$, we would have $\sqrt{d} \in F$, contradiction.
So $f(-\sqrt{d}) =$ other square root $f(\sqrt{d}) = -\sqrt{d}$.
$f(a + b\sqrt{d}) = f(a) + f(b)f(\sqrt{d}) = a + b(\sqrt{d}) = a - b\sqrt{d} = \overline{a + b\sqrt{d}}$

$x \in F^\times$
$N(x) = x\overline{x} = x \cdot x^p = x^{p+1}$
This homomorphism maps g (gen. of $K^\times$) to g^{p+1} (gen. of $F^\times$)
Claim: If $a \in F^\times$, $X^2 - dy^2$ has exactly $p+1$ solutions (x, y)
$x - \sqrt{d}y = Z$ equation becomes $N(Z) = a$ or $Z^{p+1} = a$. This has exactly $p+1$ roots in K. This is a fact about cyclic groups, or argue as follows:
$\mu(a) = \#$ of roots of $K^{p+1} = a$ with $Z \in K^\times$
$Z^{p+1} = N(Z) \in F^\times$ for any $Z \in K^\times$
So $\sum_{a \in F^\times} \mu(a) = |K^\times| = p^2 - 1$
$\sum_{a \in F^\times} \mu(a) = p^2 - 1$, so $\mu(a) = p + 1 \wedge a$
$\mu(a) \leq p + 1$ since poly $x^{p+1} - a = 0$ has $\leq p + 1$ roots.

$(\frac{104513}{3446111})$
$104513 \equiv 1 \bmod a, \equiv 1 \bmod 8$
$= (\frac{344611}{104513}) = (\frac{31072}{104513})$
$= (\frac{2^5}{104513})(\frac{971}{104513}) = (\frac{971}{104513})$
$= (104513) = (\frac{616}{971}) = (\frac{2^3}{971})(\frac{77}{971})$ $(971 \equiv 3 \bmod 8, (\frac{2}{971}) = -1)$
$= -(\frac{77}{971}) = -(\frac{971}{77}) = (\frac{47}{77}) = -(\frac{77}{47}) = -(\frac{30}{47}) = -(\frac{15}{47}) = (\frac{47}{15}) = (\frac{2}{15}) = 1$