Ranks of quadratic twists of elliptic curves over $\mathbb{F}_q(t)$

Part I: Number theory in function fields

Enrique Acosta and Martin Leslie
Advisor: Doug Ulmer

Department of Mathematics
University of Arizona

December 11, 2008

Analogies between $\mathbb{Z}$ and $\mathbb{F}_q[t]$

Both $\mathbb{Z}$ and $\mathbb{F}_q[t]$ are Euclidean domains and thus are PIDs and UFDs. So we can set up a correspondence between integers and polynomials over finite fields and a surprising amount of number theory can be recast in this language. Our correspondence:

- Integers are polynomials.
- Positive integers are monic polynomials.
- Positive prime numbers are monic irreducible polynomials.
- What about the size of a polynomial?

The norm on $\mathbb{F}_q(t)$

- Recall that $|\mathbb{Z}/n\mathbb{Z}| = |n|$.
- By the division algorithm

$$|\mathbb{F}_q[t]/(f)| = q^{\deg(f)}.$$

- So define $|0| = 0$ and $|f| = q^{\deg(f)}$ for nonzero polynomial f. Then this extends to an absolute value on the field $\mathbb{F}_q(t)$ and $|\mathbb{F}_q[t]/(f)| = |f|$.
- Then if we want to translate a statement like $n \leq x$ we can use $q^{\deg(n)} \leq x$.

The dictionary so far

Elementary Number Theory	Function Field Arithmetic
$\mathbb{Z}$	$\mathbb{F}_q[t]$
$\mathbb{Q}$	$\mathbb{F}_q(t)$
positive	monic
prime number	monic irreducible
$n \leq x$	$q^{\deg(f)} \leq x$

A translation

Theorem (Prime Number Theorem)

Let $\pi(x)$ be the number of prime numbers less than or equal to x. Then

$$\pi(x) \sim x/\log x.$$

Theorem (Prime Number Theorem for function fields)

Let N_n be the number of monic irreducible polynomials of degree n. Then

$$N_n \sim q^n/n.$$

Starting to rebuild number theory

If $f = p_1^{e_1} \dots p_t^{e_t}$ is the factorization of f into powers of distinct irreducibles then by the Chinese Remainder Theorem

$$(\mathbb{F}_q[t]/(f))^\times \cong (\mathbb{F}_q[t]/(p_1^{e_1}))^\times \times \cdots \times (\mathbb{F}_q[t]/(p_t^{e_t}))^\times.$$

Theorem

Let p be an irreducible polynomial. Then $(\mathbb{F}_q[t]/(p))^\times$ is cyclic of order $|p| - 1$. Also $(\mathbb{F}_q[t]/(p^e))^\times$ has order $|p|^{e-1}(|p| - 1)$.

Proof.

Since p is irreducible, $\mathbb{F}_q[t]/(p)$ is a field so the first result follows from the fact that a finite subgroup of the multiplicative group of a field is cyclic. Second part is (slightly) more complicated. $\square$

An Euler Phi function

- Recall that $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.
- Define $\Phi(f) = |(\mathbb{F}_q[t]/(f))^\times|$. If $f = p_1^{e_1} \dots p_t^{e_t}$ then

$$\Phi(f) = \prod |p_i|^{e_i - 1}(|p_i| - 1) = |f| \prod \left(1 - \frac{1}{|p_i|}\right).$$

- Then if a is relatively prime to nonzero f we have

$$a^{\Phi(f)} \equiv 1 \pmod{f}.$$

- Then since $\Phi(p) = |p| - 1$ we have Fermat's little theorem!

$$a^{|p|-1} \equiv 1 \pmod{p}.$$

Wilson's theorem

In $\mathbb{Z}$

If p is a prime number then

$$(p-1)! \equiv -1 \pmod{p}.$$

In $\mathbb{F}_q[t]$

If $p \in \mathbb{F}_q[t]$ is a monic irreducible then

$$\prod_{0 \le \deg(f) < \deg(p)} f \equiv -1 \pmod{p}.$$

Proof.

Set $x = 0$ in $x^{|p|-1} - 1 \equiv \prod_{0 \le \deg(f) < \deg(p)} (x - f) \pmod{p}$. □

Quadratic residues

Assume characteristic of $\mathbb{F}_q$ is odd.

Theorem

Let p be irreducible and a a polynomial not divisible by p. Then the congruence $x^2 \equiv a \pmod{p}$ is solvable if and only if $a^{(|p|-1)/2} \equiv 1 \pmod{p}$.

Proof.

If b is a solution to $x^2 \equiv a \pmod{a}$ then $a^{(|p|-1)/2} \equiv b^{|p|-1} \equiv 1 \pmod{p}$ by our version of Fermat's little theorem.
Now consider the squaring map from $(\mathbb{F}_q[t]/(p))^\times$ to itself. The kernel of this map has order 2. Thus the image, the set of squares, has order $(|p|-1)/2$. Then each of these squares satisfies the polynomial $x^{(|p|-1)/2} - 1 = 0$ in the field $\mathbb{F}_q[t]/(p)$ and thus the set of squares is exactly the zeros of this polynomial. $\square$

A Legendre symbol

For a relatively prime to p define $\left(\frac{a}{p}\right)$ to be 1 if a is a square $\bmod p$ and -1 otherwise. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{|p|-1}{2}} \pmod{p}.$$

Some properties:

1. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod{p}$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Quadratic Reciprocity

In $\mathbb{Z}$

If p, r are distinct odd prime numbers then

$$\left(\frac{r}{p}\right) = (-1)^{\frac{p-1}{2}\frac{r-1}{2}} \left(\frac{p}{r}\right).$$

In $\mathbb{F}_q[t]$

If p, r are monic and irreducible of degree δ and ν respectively then

$$\left(\frac{r}{p}\right) = (-1)^{\frac{q-1}{2}\delta\nu} \left(\frac{p}{r}\right).$$

What's the point?

- Double the results! Publish more papers.
- More general results. Extend number theory to *global fields* - finite extensions of $\mathbb{Q}$ (number fields) or of $\mathbb{F}_q(t)$ (function fields).
- Results in the function field case are often easier to prove and this gives evidence/ideas to the number field case that number theorists really care about. The Riemann hypothesis is a theorem for function fields!

What we need to translate

Theorem (Gouvea/Mazur, 1991)

Let $F(u, v)$ be a homogeneous square-free polynomial with coefficients in $\mathbb{Z}$ such that all of its irreducible factors are of degree ≤ 3. Let $M, a_0, b_0 \in \mathbb{Z}$ with a_0, b_0 both relatively prime to M. Let $N(x)$ denote the number of pairs of integers (a, b) satisfying $0 < a, b \leq x$ with $(a, b) \equiv (a_0, b_0) \pmod{M}$ for which $F(a, b)$ is square-free.

Then as $x \to \infty$, we have

$$N(x) = A \cdot x^2 + O(x^2/\log^{1/2}(x))$$

where A is given by

$$A = (1/M^2) \prod_p (1 - r(p^2)/p^4)$$

with the product taken over all primes p.

The translation?

Theorem (Acosta/Leslie, 2009?)

Let $F(u,v)$ be a homogeneous square-free polynomial with coefficients in $\mathbb{F}_q[t]$ such that all of its irreducible factors are of degree ≤ 3. Let $M, a_0, b_0 \in \mathbb{F}_q[t]$ with a_0, b_0 both relatively prime to M. Let $N(x)$ denote the number of pairs of monic polynomials (a,b) satisfying $q^{\deg(a)}, q^{\deg(b)} \leq x$ with $(a,b) \equiv (a_0, b_0) \pmod{M}$ for which $F(a,b)$ is square-free.
Then as $x \to \infty$, we have

$$N(x) = A \cdot x^2 + O(x^2/\log^{1/2}(x))$$

where A is given by

$$A = (1/q^{2\deg(M)}) \prod_p (1 - r(p^2)/q^{4\deg(p)})$$

with the product taken over all monic irreducible p.