Ranks of Quadratic Twists of Elliptic Curves over $\mathbb{F}_q(t)$

Enrique Acosta and Martin Leslie
Advisor: Prof. Douglas Ulmer

December 10, 2008

Abstract

Some notes on the analogy between number theory over $\mathbb{Z}$ and $\mathbb{F}_q[t]$ and an attempt to translate a paper of Gouvêa and Mazur on ranks of quadratic twists of elliptic curves over $\mathbb{Q}$ to elliptic curves over $\mathbb{F}_q(t)$.

Contents

1 Introduction

Our RTG paper is based on the 1991 article of Mazur and Gouvêa [GM91] investigating ranks of quadratic twists of elliptic curves over $\mathbb{Q}$. They, assuming the parity conjecture, give asymptotic estimates for a lower bound for the density of quadratic twists with rank ≥ 2 of a fixed elliptic curve E. Our final goal is to obtain analogues of these results for elliptic curves over the function field $\mathbb{F}_q(t)$. Our purpose in this paper, and the subject of our RTG project was to translate the statements and give a rough sketch of what we need to prove, and determine the exact statement that one can prove using the techniques of the original article. We have not yet been fully successful in this goal.

We start by giving an overview of the analogies between the arithmetic of function fields and the arithmetic of the integers. We then go on to give the translation for the statements of the article following the original structure. There are some proofs that we have not yet translated (these are marked as omitted in this paper) and we have not translated the statements of Sections 6 through 8 of the paper except the main result of Section 8.

In this paper we assume basic knowledge of elliptic curves as can for example be found in Silverman's text as well as abstract algebra as taught for example in a first year graduate course. We develop or reference the number theory over $\mathbb{F}_q[t]$ that we require, but of course knowing the parallel theory over $\mathbb{Z}$ would be helpful.

2 Number theory over $\mathbb{F}_q[t]$

2.1 The basic analogy

There are a number of surprising analogies between on the one hand, the integers $\mathbb{Z}$ and the rational numbers $\mathbb{Q}$ and on the other hand, $\mathbb{F}_q[t]$, a one variable polynomial ring over a finite field, and its field of fractions $\mathbb{F}_q(t)$. The analogies are so far reaching, that there is a whole area in number theory (Function Field Arithmetic) which focuses on investigating the analogue of every applicable number theoretic statement about the rationals. This paper is a particular example of this, where we are translating a paper about Elliptic curves over the rationals into its analogue in the arithmetic of function fields. We will go over the basic details of this correspondence.

First of all, both $\mathbb{Z}$ and $\mathbb{F}_q[t]$ are PIDs and so we have unique factorization and the notion of prime or irreducible elements in both. Moreover the notion of positive integer has an analogue in $\mathbb{F}_q[t]$ given by the notion of monic polynomial. This analogy extends to the notion of prime nicely, giving us an analogy between positive primes in $\mathbb{Z}$ and monic irreducible polynomials. Specifically, just like any prime in $\mathbb{Z}$ is associate to a unique positive prime (the numbers which we usually refer to as prime), any irreducible polynomial in $\mathbb{F}_q[t]$ is associate to a unique monic irreducible polynomial.

There is also an analogue of the notion of absolute value: Define $|0| = 0$ and for $f \in \mathbb{F}_q[t] \setminus \{0\}$ define $|f| = q^{\deg f}$. This has all the properties that an absolute value should have (non-negativity, positive definiteness, multiplicativity and subadditivity). Moreover, we have the following fact which is clearly an analogue of $|\mathbb{Z}/nZ| = |n|$.

Proposition 2.1. $|\mathbb{F}_q[t]/(f)| = q^{\deg f}$.

Proof. By the division algorithm for $\mathbb{F}_q[t]$, any class in $\mathbb{F}_q[t]/(f)$ has a unique representative of degree $< \deg f$, and there are $q^{\deg f}$ polynomials in $\mathbb{F}_q[t]$ of degree $< \deg f$. □

The following table summarizes the 'dictionary' we have built up 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
$n \leq x$	$q^{\deg(f)} \leq x$

2.2 Recreating some number theory

In this section we develop some analogues of results of elementary number theory up to quadratic reciprocity following [Ros02].

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

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

Proposition 2.2. *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. For the second part we know that the ideals of $\mathbb{F}_q[t]/(p^e)$ correspond to the ideals of $\mathbb{F}_q[t]$ dividing (p^e) so there is a unique maximal ideal $p\mathbb{F}_q[t]/(p^e)$. Then $\mathbb{F}_q[t]/(p^e)$ is a local ring so its units are everything outside the maximal ideal. That is,

$$|(\mathbb{F}_q[t]/(p^e))^\times| = |(\mathbb{F}_q[t]/(p^e)| - |p\mathbb{F}_q[t]/(p^e)| = |p|^e - |p|^{e-1}$$

as required. □

Then we can define an analogue of the Euler ϕ function by $\Phi(f) = |(\mathbb{F}_q[t]/(f))^\times|$. By the discussion above, if $f = p_1^{e_1} \dots p_t^{e_t}$ then

$$\Phi(f) = \prod \left|(\mathbb{F}_q[t]/(p_i^{e_i}))^\times\right| = \prod |p_i|^{e_i-1}(|p_i|-1) = |f| \prod \left(1 - \frac{1}{|p_i|}\right).$$

We can also think of $\Phi(f)$ as the number of polynomials of degree less than $\deg(f)$ which are relatively prime to f.

Proposition 2.3. *If f is a nonzero polynomial and a is relatively prime to f then*

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

Proof. We can consider $\overline{a} \in (\mathbb{F}_q[t]/(f))^\times$ which is a group of order $\Phi(f)$. Thus $\overline{a}^{\Phi(f)} = \overline{1}$ which implies our desired result. □

This proposition together with the fact that $\Phi(p) = |p| - 1$ implies the following analogue of Fermat's little theorem:

Corollary 2.4. *Let $p \in \mathbb{F}_q[t]$ be irreducible and a a polynomial not divisible by p. Then*

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

Next we prove an analogue of Wilson's theorem.

Proposition 2.5. *Let p be an irreducible polynomial of degree d. Then*

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

Proof. The product is over a set of representatives for $(\mathbb{F}_q[t]/(p))^\times$. Every element of this set is a zero of both the right hand side (by construction) and also the left hand side (by our Fermat's little theorem). Thus the difference of both sides is a polynomial of degree less than $|p| - 1$ which has at least $|p| - 1$ roots so is identically zero. □

Putting $x = 0$ in this proposition we obtain

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

which, noticing that $(-1)^{|p|-1} = 1$, implies that

$$\prod_{0 \le \deg(f) < d} f \equiv -1 \pmod{p}. \tag{2.1}$$

Corollary 2.6. *Let d divide $|p| - 1$. Then the congruence $x^d = \overline{1}$ has exactly d solutions in $(\mathbb{F}_q[t]/(p))^\times$.*

Proof. Since d divides $|p| - 1$ it follows that $x^d - 1$ divides $x^{|p|-1} - 1$. But the latter polynomial splits as a product of linear distinct factors by the proposition so $x^d - 1$ does as well. □

Now we move on to some discussion of d-th power residues. We say that a polynomial a relatively prime to f is a *d-th power residue modulo f* if the equation $x^d \equiv a \pmod{f}$ is solvable in $\mathbb{F}_q[t]$.

Proposition 2.7. *Let p be irreducible and a not divisible by p. Assume d divides $|p|-1$. Then the congruence $x^d \equiv a \pmod{p}$ is solvable if and only if $a^{(|p|-1)/d} \equiv 1 \pmod{p}$.*

Proof. Firstly, if b is a solution to $x^d \equiv a \pmod{a}$ then $a^{(|p|-1)/d} \equiv b^{|p|-1} \equiv 1 \pmod{p}$ by our version of Fermat's little theorem.

Conversely, consider the d-th power map from $(\mathbb{F}_q[t]/(p))^\times$ to itself. Since this group contains all the d-th roots of unity, the kernel of the map has order d. Thus the image, the d–th powers has order $(|p| - 1)/d$. Then each of these d-th powers satisfies the polynomial $x^{(|p|-1)/d} - 1 = 0$ in the field $\mathbb{F}_q[t]/(p)$ and thus the set of d-th powers is exactly the zeros of this polynomial. □

Next notice that for d dividing $q - 1$, $a^{(|p|-1)/d}$ is an element of order dividing d in $\mathbb{F}_q[t]/(p)$. So it is a solution of $x^d = 1$ in $\mathbb{F}_q[t]/(p)$ and $x^d - 1$ divides $x^q - x$ and therefore $a^{(|p|-1)/d}$ is congruent to a unique element of $\mathbb{F}_q^\times$ modulo p.

Definition 2.8. Let d be a number dividing $q - 1$. If p doesn't divide a let $(a/p)_d$ be the unique element of $\mathbb{F}_q^\times$ such that

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

This is the d-th power residue symbol; for $d = 2$ this is the analogue of the Legendre symbol.

Proposition 2.9. *The d-th power residue symbol has the following properties:*

(i) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *if* $a \equiv b \pmod{p}$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) $\left(\frac{a}{p}\right) = 1$ *iff* $x^d \equiv a \pmod{p}$ *has a solution.*

(iv) For any $\zeta \in \mathbb{F}_q^\times$ *of order dividing* d*, there exists* $a \in \mathbb{F}_q[t]$ *such that* $\left(\frac{a}{p}\right) = \zeta$.

Proof. We prove each claim separately.

(i) The definition only depends on $a \mod p$.

(ii) We have
$$\left(\frac{ab}{p}\right) \equiv (ab)^{(|p|-1)/d} \equiv a^{(|p|-1)/d} b^{(|p|-1)/d} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$
and if two constants are congruent modulo p they must be equal.

(iii) This is Proposition 2.7.

(iv) Consider the map $\mathbb{F}_q[t]/(p) \to \mathbb{F}_q$ that sends $a \mapsto (a/P)_d$. From part (iii), the kernel of this map is the d-th powers, and there are $(|p|-1)/d$ of these (consider the dth power map from $(\mathbb{F}_q[t]/(p))^\times$ to itself and use the fact that this set contains d dth roots of unity). Thus by the first isomorphism theorem the image of this map has size d, which implies the desired result because $\mathbb{F}_q^\times$ is cyclic.

□

Theorem 2.10 (d-th Power Reciprocity Law)**.** *Let p, r be monic irreducible polynomials of degree δ and ν respectively. Then*
$$\left(\frac{r}{p}\right)_d = (-1)^{\frac{q-1}{d}\delta\nu}\left(\frac{p}{r}\right)_d.$$

Proof. We prove the result for $d = q-1$ and the result for general d follows upon raising both sides to the power of $(q-1)/d$ because
$$\left(\frac{r}{p}\right)_{q-1}^{(q-1)/d} \equiv (r^{\frac{|p|-1}{q-1}})^{\frac{q-1}{d}} \equiv r^{\frac{|p|-1}{d}} \equiv \left(\frac{r}{p}\right)_d \pmod{p}$$
and constants that are equivalent modulo p are equal.

Let α be a root of p. Then p is the minimal polynomial of α and $\mathbb{F}_q(\alpha)/\mathbb{F}_q$ is a Galois extension so we must have
$$p(t) = (t-\alpha)(t-\alpha^q)\cdots(t-\alpha^{q^{\delta-1}}).$$
Similarly if β is a root of r we must have
$$r(t) = (t-\beta)(t-\beta^q)\cdots(t-\beta^{q^{\nu-1}}).$$
Let $\mathbb{F}'$ be a finite field containing $\mathbb{F}_q, \alpha$ and β and now consider $f(t) \in \mathbb{F}'[t]$. We have $f(t) \equiv f(\alpha) \pmod{t-\alpha}$ and also $f(t)^q = f(t^q)$.

Then

$$\begin{aligned}\left(\frac{r}{p}\right) &\equiv r(t)^{(q^\delta-1)/(q-1)} \pmod{p} \\ &= r(t)^{(1+q+\ldots+q^{\delta-1})} \\ &= r(t)r(t)^q\cdots r(t)^{q^{\delta-1}} \\ &\equiv r(\alpha)r(\alpha)^q\cdots r(\alpha)^{q^{\delta-1}} \pmod{t-\alpha}.\end{aligned}$$

We can repeat this argument to show this result modulo $t-\alpha^{q^i}$ for each i. This implies that it is true modulo p.

Then we can expand each $r(\alpha)$ out to see that

$$\left(\frac{r}{p}\right) \equiv \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}\left(\alpha^{q^i}-\beta^{q^j}\right) \pmod{p}.$$

Once again, both sides are constants so this must be an equality. So

$$\left(\frac{r}{p}\right) = \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}\left(\alpha^{q^i}-\beta^{q^j}\right) = (-1)^{\delta\nu}\prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}\left(\beta^{q^j}-\alpha^{q^i}\right) = (-1)^{\delta\nu}\left(\frac{p}{r}\right).$$

□

2.3 Other useful results

Our next result is a function field version of the well known fact that $d(x) = o(x^\delta)$ for any $\delta > 0$. The template for this proof comes from [HW79].

Proposition 2.11. *Let $d(n)$ be the number of monic divisors of a polynomial $n \in \mathbb{F}_q[t]$. Then $d(n) = o(q^{\delta\deg(n)})$ for any $\delta > 0$.*

Proof. Let $\delta > 0$ and choose $0 < \alpha < \delta$. We will prove that there exists a constant K such that $d(n)/q^{\alpha\deg(n)} \le K$. From this it will follow that $d(n)/q^{\delta\deg(n)} \to 0$ as $\deg(n) \to \infty$.

Note that for only finitely many polynomials $n \in \mathbb{F}_q[t]$ do we have $q^{\alpha\deg(n)} < 2$ since this condition imposes a bound on the degree. Let C be the set of polynomials that satisfy this bound.

Now note that for any $a, M \ge 0$ we have

$$\frac{a}{M^{\alpha a}} \le \frac{1}{\alpha\log(M)}$$

which follows directly from the fact $\log(x) \le x$. We will use this with $M = q^{\alpha\deg(n)}$ giving

$$\frac{a}{q^{\alpha\deg(n)a}} \le \frac{1}{\alpha\log(q^{\deg(n)})} \le \frac{1}{\alpha\log(q)}. \tag{2.2}$$

Also note that if $n \notin C$ then $q^{\alpha\deg(n)} \ge 2$ and so for $a \ge 0$ and an integer we have

$$\frac{1+a}{q^{\alpha\deg(n)a}} \le \frac{1+a}{2^a} \le 1. \tag{2.3}$$

Take now any arbitrary $n \in \mathbb{F}_q[t]$ and factor it into monic irreducibles as $n = \alpha \prod_i p_i^{a_i}$ where some of the p_i may be in C. By the bounds (2.2) and (2.3) we get

$$\frac{d(n)}{q^{\alpha \deg(n)}} = \prod_i \frac{1+a_i}{q^{\alpha \deg(p_i)a_i}} \leq \prod_{p_i \in C} \frac{1+a_i}{q^{\alpha \deg(p_i)a_i}} \leq \prod_{p \in C} (1 + 1/\alpha \log(q)).$$

If we denote this last term by K (note that it is independent of n), then we have $\frac{d(n)}{q^{\alpha \deg(n)}} \leq K$ as desired. □

The next result can be used to prove the analogue of the Prime number theorem but we merely require it for an inequality later.

Proposition 2.12. *Let N_d be the number of monic irreducible polynomials of degree d in $\mathbb{F}_q[t]$. Then*

$$q^n = \sum_{d|n} dN_d.$$

Proof. See [Ros02]. □

The following analogue of Dirichlet's theorem of primes in arithmetic progression was proven by Kornblum before his untimely death in World War I.

Theorem 2.13. *Let $\{a + mx\}$ be an arithmetic sequence for a, m relatively prime polynomials. Then for sufficiently large integer N, there is a monic irreducible p of degree N which lies in this arithmetic progression.*

Proof. See [Ros02]. □

We now state and prove the analogue of Hensel's lemma.

Lemma 2.14 (Hensel's Lemma)**.** *Let $f \in \mathbb{F}_q[t][x]$, $k \geq 2$ an integer and $p \in \mathbb{F}_q[t]$ be monic and irreducible. If r is a solution of $f(r) \equiv 0 \pmod{p^{k-1}}$ and also $f'(r) \not\equiv 0 \pmod{p}$, then there exists a unique monic $s \in \mathbb{F}_q[t]$ with $\deg(s) < \deg(p)$ such that*

$$f(r + sp^{k-1}) \equiv 0 \pmod{p^k}.$$

i.e. a solution modulo p^{k-1} lifts uniquely to a solution modulo p^k.

Proof. First note that we can write $f(r+s) = c_0 + c_1 s + c_2 s^2 + \ldots + c_d s^d$ with $c_i \in \mathbb{F}_q[t]$. Now setting $s = 0$ gives $c_0 = f(r)$ and taking the formal derivative and then setting $s = 0$ gives $c_1 = f'(r)$. So we have

$$\begin{aligned} f(r + sp^{k-1}) &= f(r) + f'(r)sp^{k-1} + c_2(sp^{k-1})^2 + \ldots \\ &\equiv f(r) + f'(r)sp^{k-1} \pmod{p^k} \end{aligned}$$

Now the solutions in the variable s to $f(r) + f'(r)sp^{k-1} \equiv 0 \pmod{p^k}$ are exactly the solutions in s to $sf'(r) \equiv -\frac{f(r)}{p^{k-1}} \pmod{p}$ and with $f'(r) \not\equiv 0 \pmod{p}$ there is a unique solution to this equation. □

3 Translation of the paper to $\mathbb{F}_q(t)$

In this section we attempt to 'translate' the statements of Gouvêa and Mazur's paper [GM91] to elliptic curves over $\mathbb{F}_q(t)$ instead of $\mathbb{Q}$. For simplicity, we assume that the characteristic of $\mathbb{F}_q$ is greater than 3.

3.1 Section 0: Some background

Definition 3.1. Given an elliptic curve $E/\mathbb{F}_q(t)$, for each monic irreducible $p \in \mathbb{F}_q[t]$ define the quantity f_p by

$$f_p = \begin{cases} 0, \text{ if } E \text{ has good reduction at } p, \\ 1, \text{ if } E \text{ has multiplicative reduction at } p, \\ 2, \text{ if } E \text{ has additive reduction at } p. \end{cases}$$

Define the *conductor* of E to be

$$C = \prod_p p^{f_p}$$

where the product is taken over all monic irreducibles.

The *quadratic Dirichlet character* corresponding to the twist by squarefree $D \in \mathbb{F}_q[t]$ is χ_D, defined on monic irreducible $p \in \mathbb{F}_q[t]$ by

$$\chi_D(p) = \begin{cases} 1, \text{ if } \overline{D} \text{ is a square in } (\mathbb{F}_q[t]/(p))^\times, \\ -1, \text{ if } \overline{D} \text{ is not a square in } (\mathbb{F}_q[t]/(p))^\times \\ 0, \text{ if } D \text{ is divisible by } p. \end{cases}$$

and extended multiplicatively to monic polynomials. We have $\chi_D(p) = \left(\frac{D}{p}\right)$, the d-th power residue symbol with $d = 2$, and thus

$$\chi_D\left(\prod p_i^{e_i}\right) = \prod \left(\frac{D}{p_i}\right)^{e_i}.$$

3.2 Section 1: Introduction

Let E be an elliptic curve over $\mathbb{F}_q(t)$ with good reduction at infinity. If E is given by the Weierstrass equation $y^2 = x^3 + ax + b$ then the quadratic twist by a square-free polynomial D is E_D given by $Dy^2 = x^3 + ax + b$.

We have the following version of the parity conjecture from [Ulm08]:

Conjecture 3.2 (Parity Conjecture)**.** *Let $E/\mathbb{F}_q(t)$ be an elliptic curve with good reduction at infinity and conductor C and let D be a square-free polynomial of even degree relatively prime to C. Then the ranks of E and E_D have the same parity if and only if $\chi_D(C) = 1$.*

We aim to prove the following theorem:

Theorem 3.3. *Let $E/\mathbb{F}_q(t)$ be an elliptic curve with good reduction at infinity and a non-square conductor and let*

$$\mathcal{L}_E(x) = \{\textit{square-free } D \textit{ of even degree such that } q^{\deg(D)} \leq x \textit{ and rank}(E_D) \geq 2 \textit{ and even}\}.$$

If the parity conjecture is true, then for any $\epsilon > 0$, $|\mathcal{L}_E(x)| \geq x^{1/2-\epsilon}$ for sufficiently large x.

3.3 Section 2: The square-free counting method

Proposition 3.4. *If $E/\mathbb{F}_q(t)$ is an elliptic curve then there are only a finite number of square-free polynomials D such that E_D has a torsion point of order > 2.*

Proof. Omitted. □

The main difficulty in the proof of Theorem 3.3 is obtaining asymptotic bounds on the density of square-free values of binary forms. Assuming these results we now give a proof of the theorem. The rest of the paper will be devoted to obtaining the required results which can be seen in Section 3.9.

Proof of Theorem 3.3. Given $E/\mathbb{F}_q(t)$ with Weierstrass equation $y^2 = x^3 + ax + b$ and conductor C, define $F(U,V) = V \cdot f(U,V)$ where $f(U,V) = U^3 + aUV^2 + bV^3$.

Now for any pair of polynomials (u,v), if $D = F(u,v)$ is a square-free polynomial then $(X,Y) = (u/v, 1/v^2)$ is an $\mathbb{F}_q(t)$ point on E_D because $DY^2 = F(u,v)/v^4 = (u/v)^3 + a(u/v) + b = X^3 + aX + b$.

Note that (X,Y) is not of order two because $Y \neq 0$. We claim that there are only a finite number of pairs (u,v) such that (X,Y) is torsion. Indeed, by Proposition 3.4 there are only a finite number of D such that E_D has a torsion point of order > 2. Then for each such D there are only a finite number of torsion points on E_D (by the Mordell–Weil theorem over $\mathbb{F}_q(t)$ for example) and for each of these there are only a finite number (at most 2) of pairs (u,v) that give such a point.

Now let Z be a real number and $\mathcal{T}_E(Z)$ be the set of pairs of monic (u,v) with $q^{\deg(u)}, q^{\deg(v)} \leq Z$ such that

(i) $D = F(u,v)$ is a square free polynomial of even degree, relatively prime to M.

(ii) $(X,Y) = (u/v, 1/v^2)$ is not a torsion point on E_D.

(iii) $(u,v) \equiv (a_0, b_0) \mod M$. (In Lemma 3.17 it is seen that this condition, for some a_0, b_0, M to be specified later, implies that E_D has even rank).

Now choose $\lambda = q^{-\frac{1}{4}\max\{1,\deg(a),\deg(b)\}}$ and define a map $\psi\colon \mathcal{T}_E(\lambda \cdot x^{1/4}) \to \mathcal{L}_E(x)$ by $(u,v) \mapsto D = F(u,v)$. Then $q^{\deg(D)} = q^{\deg(F(u,v)} = q^{\deg(vu^3 + av^3u + bv^4)} \leq q^{\max\{1,\deg(a),\deg(b\}}\lambda^4 x = x$. Also we have a non-torsion point (X,Y) on E_D, and rank of E_D is even and therefore ≥ 2 as required.

But this is precisely the set specified in Proposition 3.18 except for a finite number, k, of elements removed (the only extra condition is (ii) above). Thus the cardinality of $\mathcal{T}_E(\lambda \cdot x^{1/4})$ is equal to $\mathcal{N}(\lambda \cdot x^{1/4}) - k \geq c \cdot x^{1/2}$ for some c and for x sufficiently large.

Next we show that fibers of ψ have cardinality bounded above by $o(x^\epsilon)$ for any $\epsilon > 0$. Consider the (u,v) solving $D = vf(u,v)$. Specifying v means there are at most 3 different u's satisfying this equation. But v is a divisor of D so $|\psi^{-1}(D)| \leq 3d(D)$ where $d(D)$ is the number of monic divisors of D. But from Proposition 2.11 we know that $d(D) = o(q^{\deg(D)\epsilon})$ for all $\epsilon > 0$, so for sufficiently large x we have $|\psi^{-1}(D)| \leq c \cdot x^\epsilon$ and therefore

$$|\mathcal{L}_E(x)| \geq \frac{|\mathcal{T}_E(\lambda x^{1/4})|}{|\psi^{-1}(D)|} \geq x^{1/2-\epsilon}.$$

□

3.4 Section 3: The square-free sieve

This section of the original paper explains the strategy of the proof.

3.5 Section 4: Main terms and error terms

Let $F(u,v)$ be a homogeneous polynomial of degree $d \geq 1$ with coefficients in $\mathbb{F}_q[t]$. We can write $F(u,v) = ku^r v^s \prod(u - \alpha_i v)$ with $k \in \mathbb{F}_q[t]$, $r, s \in \mathbb{N} \cup \{0\}$, $\alpha_i \neq 0 \in \overline{\mathbb{F}_q[t]}$. Now if $r \neq 0$ we can make a transformation $u \mapsto u + \alpha v$ and $v \mapsto v$ choosing $\alpha \in \mathbb{F}_q[t]$ such that now $r = 0$. (There are only a finite number of bad choices to avoid and there are infinitely many possible choices). Then we can make a transformation that maps $u \mapsto u$ and $v \mapsto v + \beta u$ with $\beta \in \mathbb{F}_q[t]$ such that $s = 0$. So composing these two transformations we get a linear transformation of determinant 1 defined over $\mathbb{F}_q[t]$.

Thus we may assume that the coefficients of u^d and v^d, call them l and m respectively, are nonzero. So factor $F(u,v) = l \cdot \prod(u - \alpha_i v)$ over $\overline{\mathbb{F}_q(t)}$ and then define $\Delta = ml^{2d-1} \prod(\alpha_i - \alpha_j)$ where the product is over all $i \neq j$. Then Δ is in $\mathbb{F}_q[t]$ because $\prod(\alpha_i - \alpha_j)$ is a symmetric polynomial in the coefficients of F. Also Δ is nonzero if and only if F is squarefree.

Suppose that F is squarefree and also that all irreducible factors of F are of degree ≤ 3. Fix a monic polynomial M and two polynomials a_0, b_0 both relatively prime to M, and define $N(x)$ to be the number of pairs (a,b) satisfying $q^{\deg(a)}, q^{\deg(b)} \leq x$ with $a \equiv a_0$ and $b \equiv b_0 \pmod{M}$ such that $F(a,b)$ is square-free.

Define $N'(x)$ = the number of pairs (a,b) satisfying $q^{\deg(a)}, q^{\deg(b)} \leq x$ with $a \equiv a_0$ and $b \equiv b_0 \pmod{M}$ such that $F(a,b)$ is not divisible by the square of any monic irreducible factor of degree less than or equal to $\xi = 1/3 \log_q(x)$.

The following proposition shows that this choice of ξ gives a bound which we shall use later.

Proposition 3.5. *If l is square-free and all its irreducible factors have degree $\leq \xi$ then* $\deg(l) \leq x^{2/3}$.

Proof. We have $\deg(l) \leq \deg(\prod p)$ where the product is taken over all monic irreducible polynomials of degree $\leq \xi$. This number is equal to $\sum_{d \leq \xi} dN_d$ where N_d is the number of monic irreducible polynomials of degree d. But we know that $dN_d \leq q^d$ (because $\sum_{n|d} nN_n = q^d$, Proposition 2.12) so then if $q \geq 2$ and $[\xi] \geq 1$ we have

$$\begin{aligned}
\sum_{d \leq \xi} dN_d &\leq q^1 + q^2 + \cdots + q^{[\xi]} \\
&= \frac{q^{[\xi]+1} - 1}{q - 1} \\
&\leq q^{[\xi]+1} - 1 \\
&\leq q^{2[\xi]} \\
&\leq x^{2/3}.
\end{aligned}$$

□

Now define the error terms E_i by writing $F(u,v) = \prod_1^r f_i(u,v)$ as a product of irreducible homogeneous forms with coefficients in $\mathbb{F}_q[t]$ and setting

$E_0(x)$ = the number of pairs of monic (a,b) with $q^{\deg(a)}, q^{\deg(b)} \leq x$ such that a, b are both divisible by some irreducible polynomial of degree greater than ξ

and for $i = 1, \ldots, r$,

$E_i(x)$ = the number of pairs of monic (a,b) with $q^{\deg(a)}, q^{\deg(b)} \leq x$ such that $f_i(a,b)$ is divisible by the square of an irreducible polynomial of degree greater than ξ.

Finally, set $E(x) = \sum_0^r E_i(x)$. We have the following proposition.

Proposition 3.6. *For x sufficiently large, we have*

$$N'(x) - E(x) \le N(x) \le N'(x).$$

Proof. The rightmost inequality is true by definition. For the left inequality take x large enough that $\xi > \deg \Delta$. Then if (a, b) is a pair that contributes to $N'(x)$ but not $N(x)$ we must have $q^{\deg(a)}, q^{\deg(b)} \le x$, $(a, b) \equiv (a_0, b_0) \mod M$ and there must exist an irreducible polynomial p of degree $> \xi$ such that p^2 divides $F(a, b)$. Now $\deg(p) > \xi > \deg \Delta$ so p does not divide Δ.

Now if p divides both a and b then the pair contributes to $E_0(x)$. So assume this doesn't happen and then $p^2 \mid F(a, b) = \prod_1^r f_i(a, b)$ implies that either $p^2 \mid f_i(a, b)$ for some i (in which case the pair contributes to $E_i(x)$) or p divides two different factors. But this second case can't happen because this would give repeated roots to the equation $F(u, b) \equiv 0 \mod p$ and this equation has no repeated roots because $\Delta \not\equiv 0 \mod p$.

Thus (a, b) contributes to $E(x)$ and we see that $N'(x) - N(x) \le E(x)$ which is equivalent to the desired inequality. □

3.6 Section 5: Counting points modulo m

For this section we do not need to assume that F has all of its irreducible factors of degree ≤ 3. We will find a bound for the number of solutions of $F(a, b) \equiv 0 \pmod m$ congruent to $(a_0, b_0) \pmod M$ in terms of $m \in \mathbb{F}_q[t]$.

Specifically, define $\rho(m) = 1$ if $m \in \mathbb{F}_q$, and otherwise, define $\rho(m)$ to be the number of noncongruent solutions $\mod m$ in polynomials a, b of the congruence $F(a, b) \equiv 0 \pmod m$ which satisfy the extra condition $(a, b) \equiv (a_0, b_0) \pmod M$.

Note that if $\gcd(m, M) = 1$, the extra congruence condition $(a, b) \equiv (a_0, b_0) \pmod M$ is irrelevant, since for any congruence class $[a] \mod m$ we can find a representative $A \in \mathbb{F}_q[t]$ (i.e., $A \equiv a \pmod m$) with $A \equiv a_0 \pmod M$ by the Chinese Remainder Theorem. However, if $\gcd(m, M) = \delta$ with $\deg(\delta) > 0$, then this extra condition does affect the value of ρ, since there are only $q^{2\deg(m/\delta)}$ tuples of congruence classes mod m which have representatives which are congruent to $(a_0, b_0) \mod M$. One can see this by noting that fixing a class $a_0 \pmod M$ fixes the class $a_0 \pmod \delta$ and so by the isomorphism

$$\mathbb{F}_q[t]/(m) \cong \mathbb{F}_q[t]/(\delta) \times \mathbb{F}_q[t]/(m/\delta) \tag{3.1}$$

there are $q^{\deg(m/\delta)}$ different congruence classes mod m which are congruent to $a_0 \pmod M$.

For this reason we define $r(m) = q^{2\deg(\delta)}\rho(m)$.

Lemma 3.7. *The functions ρ and r are multiplicative.*

Proof. By the Chinese Remainder Theorem. □

Lemma 3.8. *Let $p \in \mathbb{F}_q[t]$ be monic irreducible with $p \nmid \Delta$. Let $n > 0$ and (a, b) be a solution of $F(u, v) \equiv 0 \pmod{p^n}$ in polynomials in $\mathbb{F}_q[t]$. If $\mathrm{ord}_p(a)$ or $\mathrm{ord}_p(b) < n/d$ then $\mathrm{ord}_p(a) = \mathrm{ord}_p(b)$.*

Proof. Assume that a is the one with least order, then we have both $\mathrm{ord}_p(a) < n/d$ and $\mathrm{ord}_p(a) \le \mathrm{ord}_p(b)$. We now assume that $\mathrm{ord}_p(a) < \mathrm{ord}_p(b)$ and derive a contradiction. Note that under this assumption we have $\mathrm{ord}_p(a^d) < \mathrm{ord}_p(a^i b^{d-i})$ for all $i = 1, \ldots, d$.

Now, $F(a,b) \equiv 0 \pmod{p^n}$ implies that

$$la^d \equiv -\sum_{i=1}^{d} c_i a^i b^{d-i} \pmod{p^n}$$

for some c_i. However, since p does not divide Δ, we have that p in particular does not divide l. Therefore, in this last congruence, the order of the left hand side is strictly smaller than the order of the right hand side, giving the contradiction. □

Lemma 3.9. *Let p be a monic irreducible polynomial and let $\rho_1(p)$ be the number of solutions of $F(x,1) \equiv 0 \pmod{p}$. If $p \nmid \Delta$, then for $n \geq 1$,*

$$\rho(p^n) \leq q^{2\deg(p)[n-n/d]} + \rho_1(p) \sum_{\lambda=0}^{\langle n/d \rangle} \phi(q^{\deg(p)(n+d\lambda-2\lambda)}) \tag{3.2}$$

where $[c]$ (resp. $\langle c \rangle$) is the largest integer $\leq c$ (resp. $< c$).

Also, if p does not divide M then we have an equality above.

Proof. We show equality when $p \nmid M\Delta$. The general case follows since if $p \mid M$ then ρ will be smaller than we are expecting it to be by the extra congruence conditions as explained above. We can therefore ignore the congruence conditions mod M in the rest of the proof .

There are two ways a pair (a,b) can be a solution of $F(a,b) \equiv 0 \pmod{p^n}$:

(i) *Solutions of high divisibility*: If a, b are polynomials with $\mathrm{ord}_p(a), \mathrm{ord}_p(b) > n/d$ then (a,b) is automatically a solution because F is homogeneous of degree d.

(ii) *Solutions of a fixed order*: If (a,b) is a solution which is not of high divisibility, then $\mathrm{ord}_p(a) = \mathrm{ord}_p(b)$ by Lemma 3.8. We call this common order the order of the solution.

We now count the number of solutions of each type separately:

Solutions of High Divisibility: We just need to count the number of congruence classes in $\mathbb{F}_q[t]/\langle p^n \rangle$ with order $\geq n/d$ (and then square this result to get the total number of tuples). This is the same as counting the number of polynomials g of degree $< \deg(p^n) = n\deg(p)$ with $\mathrm{ord}_p(g) \geq n/d$. Now any g satisfying this is of the form $p^{\langle n/d \rangle + 1} f$ with $\deg(f) \geq 0$, and so we need to count the possible f. For the upper bound of $\deg(f)$ we have $\deg(p^{\langle n/d \rangle + 1} f) < n\deg(p)$ which gives $\deg(f) < (n - \langle n/d \rangle - 1) = [n - n/d]$. So we see, f needs to satisfy $[n - n/d] > \deg(f) \geq 0$ and there are exactly $q^{\deg(p)[n-n/d]}$ polynomials satisfying this bound.

This gives us exactly $q^{2\deg(p)[n-n/d]}$ solutions of high divisibility.

Solutions of a fixed order: We count the solutions of order λ for a fixed $0 \leq \lambda < n/d$. Consider the following sets:

$A = \{(a,b) \bmod p^n \mid (a,b) \text{ is a solution of order } \lambda\}$,

$B = \{x \in (\mathbb{F}_q[t]/(p^{n-\lambda}))^\times \mid F(x,1) \equiv 0 \pmod{p^{n-d\lambda}}\}$,

$C = \{x \in (\mathbb{F}_q[t]/(p))^\times \mid F(x,1) \equiv 0 \pmod{p}\}$.

Note that if $(a,b) \in A$, then $(a,b) = (p^\lambda \alpha, p^\lambda \beta)$ where $\alpha, \beta \in (\mathbb{F}_q[t]/(p^{n-\lambda}))^\times$, and so the congruence $F(a,b) \equiv 0 \pmod{p^n}$ gives $F(\alpha/\beta, 1) \equiv 0 \pmod{p^{n-d\lambda}}$. This gives a map $A \to B$. We also have a map

$B \to C$ and by definition $\rho_1(p) = |C|$. We now count the size of the fibers of each of these maps to compute the size of A.

For the map $A \to B$, note that the set of elements that go to x is given by $\{(p^\lambda ux, p^\lambda ux) \mid u \in (\mathbb{F}_q[t]/(p^{n-\lambda}))^\times\}$ and so each fiber has size $|(\mathbb{F}_q[t]/(p^{n-\lambda}))^\times| = \phi(q^{(n-\lambda)\deg(p)})$.

For the map $B \to C$, we have that p does not divide Δ which means that $F(x,1)$ is squarefree mod p and thus for $r \in C$ we have both $F(r,1) \equiv 0 \pmod p$ and $F'(r,1) \not\equiv 0 \pmod p$. But this is exactly the condition for Hensel's lemma to apply and thus by Lemma 2.14 applied repeatedly, each solution mod p lifts uniquely to a solution mod $p^{n-d\lambda}$. Now we need to count how many lifts each of these congruence classes has to elements of $(\mathbb{F}_q[t]/(p^{n-\lambda}))^\times$. This is simple: the kernel of the map $\mathbb{F}_q[t]/(p^{n-\lambda}) \to \mathbb{F}_q[t]/(p^{n-d\lambda})$ is $(p^{n-d\lambda})$ which has size equal to the number of polynomials of degree $< (n-\lambda) - (n-d\lambda)$ which is $q^{\deg(p)((n-\lambda)-(n-d\lambda))} = q^{\deg(p)\lambda(d-1)}$.

Multiplying the size of the fibers we get $\phi(q^{\deg(p)(n-\lambda)}) \cdot q^{\deg(p)\lambda(d-1)} = \phi(q^{\deg(p)(n+d\lambda-2\lambda)})$. □

Lemma 3.10. *The generating function*

$$R(T) = \sum_{n=0}^{\infty} \rho(p^n) \cdot T^n$$

is a rational function with at worst simple poles at $T = q^{-\deg(p)}$ and at $T = \zeta \cdot q^{-(2-2/d)\deg(p)}$ where ζ runs through all dth roots of unity. The power series above converges in the open disk about $T = 0$ of radius $q^{-(2-2/d)\deg(p)}$.

Proof. Omitted. Rational case uses techniques of Igusa. □

Lemma 3.11. *We have the following asymptotics:*

(i) If p^n ranges over all powers of irreducible polynomials then $\rho(p^n) = O(q^{n(2-2/d)\deg(p)})$ and $r(p^n) = O(q^{n(2-2/d)\deg(p)})$ as $\deg(p^n) \to \infty$.

(ii) If m ranges over square-free polynomials then $\rho(m^2) = O(q^{2\deg(m)} d_{d+1}(m))$ where $d_k(m)$ is the number of ways in which m can be written as a product of k factors.

Proof. (i) If $p \nmid \Delta$ then noticing that $\rho_1(p) \le d$ because F has degree d we have

$$\begin{aligned}
\rho(p^n) - q^{2\deg(p)[n-n/d]} &\le \rho_1(p) \sum_{\lambda=0}^{\langle n/d\rangle} \phi(q^{\deg(p)(n+d\lambda-2\lambda)}) \\
&\le d \sum_{\lambda=0}^{\langle n/d\rangle} \phi(q^{\deg(p)(n+(d-2)\lambda)}) \\
&= d \sum_{\lambda=0}^{\langle n/d\rangle} \frac{q-1}{q} q^{\deg(p)(n+(d-2)\lambda)} \\
&\le d q^{n\deg(p)} \sum_{\lambda=0}^{\langle n/d\rangle} q^{\deg(p)(d-2)\lambda} \\
&= d q^{n\deg(p)} \frac{q^{\deg(p)(d-2)(\langle n/d\rangle+1)} - 1}{q^{\deg(p)(d-2)} - 1} \\
&= O(q^{n\deg(p)} q^{\deg(p)(d-2)(n/d)}) \\
&= O(q^{\deg(p)n(2-2/d)}).
\end{aligned}$$

But $q^{2\deg(p)[n-n/d]}$ is bounded by the same function so we have $\rho(p^n) = O(q^{\deg(p)n(2-2/d)})$ as $\deg(p^n) \to \infty$ for $p \nmid \Delta$.

Taking the finitely many $p \mid \Delta$ one at a time, the convergence condition in Lemma 3.10 gives us that $\rho(p^n) = O(1/(q^{-(2-2/d)\deg(p)})^n) = O(q^{\deg(p)n(2-2/d)})$ as $n \to \infty$. Putting this together with the bound above we get the desired result.

For the other bound we have $r(p^n) = q^{2\deg(\delta)}\rho(p^n) \leq q^{2\deg(M)}\rho(p^n)$ so $r(p^n)$ is bounded by a constant multiple of $\rho(p^n)$ and the same asymptotics apply.

(ii) We have

$$\rho(p^2) \leq q^{2\deg(p)[2-2/d]} + \rho_1(p) \sum_{\lambda=0}^{\langle 2/d \rangle} \phi(q^{\deg(p)(2+d\lambda-2\lambda)}).$$

Then we have 2 cases: If $d = 1$ then we have

$$\begin{aligned}\rho(p^2) &\leq q^{2\deg(p)[0]} + \sum_{\lambda=0}^{\langle 2 \rangle} \phi(q^{\deg(p)(2-\lambda)}) \\ &= 1 + \phi(q^{2\deg(p)}) + \phi(q^{\deg(p)}) \\ &= q^{2\deg(p)} - q^{2\deg(p)-1} + q^{\deg(p)} - q^{\deg(p)-1} + 1 \\ &\leq q^{2\deg(p)} \leq (d+1)q^{2\deg(p)}.\end{aligned}$$

For $d \geq 2$ we have

$$\begin{aligned}\rho(p^2) &\leq q^{2\deg(p)} + d\sum_{\lambda=0}^{0} \phi(q^{\deg(p)(2+d\lambda-2\lambda)}) \\ &= q^{2\deg(p)} + d\phi(q^{2\deg(p)}) \\ &= (d+1)q^{2\deg(p)} - dq^{2\deg(p)-1} \\ &\leq (d+1)q^{2\deg(p)}.\end{aligned}$$

Thus if m has r factors we see that

$$\rho(m^2) = \rho(c\prod_1^r p_i^2) = \prod_1^r \rho(p_i^2) \leq (d+1)^r \prod_1^r q^{2\deg(p_i)} = d_{d+1}(m)q^{2\deg(m)}$$

where the last equality is obtained by noticing that the number of ways that r distinct factors can be grouped into k factors is k^r.

□

3.7 Sections 6, 7, 8: Square-free values of binary forms

In these sections the paper uses results of Hooley from [Hoo76] to bound the error terms and the main term. The final result translates to the following statement.

Theorem 3.12. *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 (nonconstant) monic irreducible p.

We need a version of this result with $F(a, b)$ of even degree.

Corollary 3.13. *With the same setup as in the theorem above let $N_e(x)$ be the number of pairs with the above conditions but also with $F(a, b)$ of even degree.*

Then for x sufficiently large, we have

$$N_e(x) \geq \frac{A}{q^6} \cdot x^2.$$

Proof. Assume A is nonzero (otherwise the statement is vacuous). From the theorem above we know that there exists a C and an N such that for $n > N$,

$$|N(q^n) - Aq^{2n}| \leq Cq^{2n}/\log^{1/2}(q^n) = E(q^n). \tag{3.3}$$

Now take $N' > N$ and large enough so that for $n > N'$

$$C\left(\frac{q^2}{\sqrt{2n+2}} + \frac{1}{\sqrt{2n}}\right) < A(q^2 - 2).$$

Also take $x > q^{N'+2}$, and take $n+1$ to be the largest even number less than or equal to than $\log_q(x)$. Then n will be an odd number with $n > N$.

We use the equation (3.3) to show that there are enough polynomials of even degree. Indeed

$$\begin{aligned}
N(q^{n+1}) - N(q^n) &\geq Aq^{2(n+1)} - E(q^{n+1}) - Aq^{2n} - E(q^n) \\
&= A(q^2 - 1)q^{2n} - (E(q^{n+1}) + E(q^n)) \\
&= A(q^2 - 1)q^{2n} - Cq^{2n}\left(\frac{q^2}{\sqrt{2n+2}} + \frac{1}{\sqrt{2n}}\right) \\
&= q^{2n}\left(A(q^2 - 1) - C\left(\frac{q^2}{\sqrt{2n+2}} + \frac{1}{\sqrt{2n}}\right)\right) \\
&\geq Aq^{2n}
\end{aligned}$$

So, there are at least Aq^{2n} pairs of polynomials (a, b) of degree $n+1$, which is even. For these pairs $F(a, b)$ is squarefree and even. So then $N_e(x) \geq Aq^{2n}$ but $n + 1 > \log x - 2$ so $N_e(x) \geq Aq^{2(\log x - 3)} = Ax^2q^{-6}$ as desired.

□

3.8 Section 9: Nonvanishing criteria for the constant A

Set $A_p = 1 - r(p^2)/q^{4\deg(p)}$. Then

$$A = (1/q^{2\deg(M)}) \prod_p A_p.$$

Proposition 3.14. *The constant A is zero if and only if $A_p = 0$ for some monic irreducible p.*

Proof. Clearly $A_p = 0$ implies that $A = 0$. For the other implication we use the fact that $r(p^2) = O(q^{2\deg(p)})$. This implies that A_p converges to 1 as $\deg(p) \to \infty$ so the only way A can be zero is if some $A_p = 0$. □

Proposition 3.15. *We have the following conditions for A_p vanishing:*

(i) If p^2 divides all the coefficients of $F(u, v)$ then $A_p = 0$.

(ii) If p^2 does not divide all the coefficients of $F(u, v)$ we have two subcases:

(a) If $p^2 \mid M$ then $A_p = 0$ if and only if (a_0, b_0) is a solution of $F(u, v) \equiv 0 \pmod{p^2}$.

(b) If $p \mid M$ but $p^2 \nmid M$ then $A_p = 0$ if and only if (a_0, b_0) is a singular point on $F(u, v) \equiv 0 \pmod{p}$.

(iii) If p does not divide all the coefficients of $F(u, v)$ and $p \nmid M$ then $A_p = 0$ implies that $q^{\deg(p)} \leq \deg(F)$.

Proof. We prove each claim separately:

(i) Notice first that $A_p = 0$ if and only if $r(p^2) = q^{4\deg(p)}$. But if p^2 divides all the coefficients of $F(u, v)$ then every possible solution is one and this condition is satisfied.

(ii) Now assume that p^2 does not divide all the coefficients of $F(u, v)$.

(a) With $p^2 \mid M$ we have $\delta = p^2$ and thus $r(p^2) = q^{4\deg(p)}$ if and only if $\rho(p^2) = 1$. But this is saying that there is exactly one solution of $F(u, v) \equiv 0 \pmod{p^2}$ also satisfying the auxiliary conditions which is equivalent to saying that (a_0, b_0) is a solution.

(b) We have $\delta = p$ so $r(p^2) = q^{4\deg(p)}$ if and only if $\rho(p^2) = q^{2\deg(p)}$. By the Jacobi criterion, (a_0, b_0) is a singular point if and only if

$$(\partial F/\partial u)(a_0, b_0) \equiv (\partial F/\partial v)(a_0, b_0) \equiv 0 \pmod{p}$$

which, by considering the Taylor series expansion, happens if and only if

$$F(a_0 + p\lambda, b_0 + p\mu) \equiv 0 \pmod{p^2}$$

for all λ and μ, which yields the desired result.

(iii) We have $\delta = 1$ so for $A_p = 0$ we must have $\rho(p^2) = r(p^2) = q^{4\deg(p)}$ which means that every pair of polynomials (a, b) is a solution of $F(u, v) \equiv 0 \mod p^2$. This implies that there are $q^{\deg(p)}$ solutions of $F(u, 1) \equiv 0 \mod p$. But then this is a non-zero one-variable polynomial over a field so has at most $\deg(F(u, 1)) \leq \deg(F)$ solutions and we must have $q^{\deg(p)} \leq \deg(F)$.

□

Corollary 3.16. *If $F(u, v) = v \cdot f(u, v)$ where f is a homogenous form of degree 3, where p doesn't divide all the coefficients of $F(u, v)$, and $p \nmid M$, then $A_p \neq 0$ for all p.*

Proof. We have $\deg(F) = 4$ so since we know that $\deg(p) \geq 1$ and $q \geq 5$ we have $q^{\deg(p)} \geq 5$ and thus $A_p \neq 0$ from part (iii) of Proposition 3.15. □

3.9 Section 10: Application to elliptic curves

Let $E/\mathbb{F}_q(t)$ be an elliptic curve with non-square conductor C. Choose a model for E to be $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q[t]$ both divisible by C. Then let $F(u,v) = v \cdot f(u,v)$ where $f(u,v) = u^3 + auv^2 + bv^3$. Then $F(u,v) \equiv vu^3 \mod C$.

Define the *sign* of a pair of congruence classes (a_0, b_0) both relatively prime to C by choosing a square-free $D \equiv F(a_0, b_0) \equiv b_0 a_0^3 \mod C$ and letting the sign be $\chi_D(C)$. We can always choose a squarefree D by the function field version of Dirichlet's theorem on primes in arithmetic progression since $b_0 a_0^3$ is relatively prime to C. To see that this is well defined note that $\chi_D(C) = (D/C)$ is determined by $D \mod C$.

Lemma 3.17. *Assuming the parity conjecture, we can choose (a_0, b_0) both relatively prime to C so that any pair $(u,v) \equiv (a_0, b_0) \mod C$ which gives rise to a square-free even-degree $D = F(u,v)$ relatively prime to C will have rank of E_D even.*

Proof. Recall that the conductor is $C = \prod p_i^{f_i}$ with $f_i = 0, 1$ or 2 and by our assumption that C is not a square we have at least one $f_i = 1$. Then $\chi_D(C) = (D/C) = \prod (D/p_i)$ where the product is only over the p_i's with $f_i = 1$. By Proposition 2.9 we know that for each such p_i there exists $D \in \mathbb{F}_q[t]$ such that $(D/p_i) = \pm 1$ and we can choose $D \mod p_i$. So choose a D modulo C such that $\chi_D(C) = 1$ if the rank of E is even and $\chi_D(C) = -1$ if the rank of E is odd. Then choose $a_0 = 1$ and $b_0 = D$. The condition that a_0, b_0 are relatively prime to C is satisfied because D is relatively prime to C.

Now $vu^3 \equiv b_0 a_0^3 \mod C$ so $\chi_{F(u,v)}(C) = \chi_{F(a_0,b_0)}(C) = \pm 1$ as chosen above. By Conjecture 3.2 this forces the rank of E_D to be even as desired. □

So choose (a_0, b_0) as in the lemma and the following is the required result to complete the proof of Theorem 3.3.

Proposition 3.18. *With notation as above let $\mathcal{N}(x)$ denote the number of pairs of monic polynomials (u,v) satisfying $q^{\deg(u)}, q^{\deg(v)} \leq x$ with $(u,v) \equiv (a_0, b_0) \pmod{C}$ for which $F(u,v)$ is square-free and of even degree. Then*

$$\mathcal{N}(x) \geq B \cdot x^2$$

where B is a positive constant.

Proof. We have this estimate from Corollary 3.13 with $B = A/q^6$ but need to show that A can't vanish. We check that each A_p can't vanish using Proposition 3.15.

We have $F(u,v) = u^3 v + auv^3 + bv^4$ so we don't have p or p^2 dividing all coefficients. If $p \nmid C$ then by Corollary 3.16 we have $A_p \neq 0$.

If $p \mid C$ then we need to check that (a_0, b_0) don't satisfy the conditions (a) or (b) of (ii). But $F(a_0, b_0) \equiv b_0 a_0^3 \pmod{C}$ where a_0, b_0 are relatively prime to C and thus to p so $F(a_0, b_0) \not\equiv 0 \pmod{p}$. Thus (a_0, b_0) is neither a (singular) point of $F(u,v) \equiv 0 \pmod{p}$ nor a solution to $F(u,v) \equiv 0 \pmod{p^2}$. □

References

[GM91] F. Gouvêa and B. Mazur. The square-free sieve and the rank of elliptic curves. *Journal of the American Mathematical Society*, 4(1):1–23, 1991.

[Hoo76] C. Hooley. *Applications of sieve methods to the theory of numbers*. Cambridge University Press New York, 1976.

[HW79] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers*. Oxford University Press, 1979.

[Ros02] Michael Rosen. *Number Theory in Function Fields*. Springer, 1st edition, 2002.

[Ulm08] Douglas Ulmer. Personal communication, 2008.