Local Torsion on Elliptic Curves

Colin Grabowski

A Thesis

in

The Department

of

Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science (Pure Mathematics) at
Concordia University
Montreal, Quebec, Canada

March 2010

Your file Votre référence
ISBN: 978-0-494-67110-8
Our file Notre référence
ISBN: 978-0-494-67110-8

ABSTRACT

Local Torsion on Elliptic Curves

Colin Grabowski

Let E be an elliptic curve over $\mathbb{Q}$. Let p be a prime of good reduction for E. We say that p is a local torsion prime if E has p-torsion over $\mathbb{Q}_p$, and more generally, we say that p is a local torsion prime of degree d if E has p-torsion over an extension of degree d of $\mathbb{Q}_p$.

We study in this thesis local torsion primes by presenting numerical evidence, and by computing estimates for the number of local torsion primes on average over all elliptic curves over $\mathbb{Q}$.

Contents

Chapter 1

Introduction

Let E be an elliptic curve over $\mathbb{Q}$. In [4], the authors present the following conjecture.

Conjecture 1 *Assume that E does not have complex multiplication. Fix $d \geq 1$. Then there are finitely many primes p such that there exists an extension $K/\mathbb{Q}_p$ of degree at most d with $E(K)[p] \neq 0$.*

In [4] the authors showed that Conjecture 1 holds on average. They also gathered numerical data that was supportive of the conjecture in the case where $d = 1$, with E having conductor of at most 1000. A key result to do this was a criterion for distinguishing when an elliptic curve has p-torsion over an extension $K/\mathbb{Q}_p$. The criterion involves the p-rank of elliptic curves over the ring of Witt vectors for which K is the field of fractions. By counting the number of lifts to this ring of Witt vectors, of an elliptic curve over an extension of degree d over $\mathbb{F}_p$ with p-torsion, David and Weston were able to

show that Conjecture 1 holds on average.

In this thesis, we extend the work of [4] by looking at computational and theoretical aspects of the questions raised in their paper. We first extend their numerical evidence by gathering numerical data for $d = 2$ where E has conductor up to 5000. This is performed with the MAGMA Computational Algebra System.

We also investigate the properties of the primes p such that E has p-torsion over an extension of degree d of $\mathbb{Q}_p$, where d is at most $p-1$. In this case, the size of d is allowed to grow with p, unlike the case of Conjecture 1 where d is uniformly bounded. We remark that it is trivial that E has a p-torsion point of degree at most p^2 for each prime p of good reduction by adjoining a root of the division polynomial φ_p. Then letting $E_{a,b} : y^2 = x^3 + ax + b$ such that $a, b \in \mathbb{Z}$ we show that

Theorem 2 *Let $A, B \geq x^{2+\epsilon}$ for some $\epsilon \geq 0$. Then*

$$\frac{1}{4AB} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \pi'_{E_{a,b}}(x) \quad = \quad \log\log x + O(1).$$

In view of Theorem 2, it is not clear what to expect for the asymptotic behaviour of $\pi'_E(x)$ for a fixed elliptic curve E over $\mathbb{Q}$, and this raises interesting avenues for future research.

The structure of this thesis is as follows: in Chapters 2 and 3, we develop the background material needed to state the criterion of [4] which allows to recognize when E has torsion over some extension $K/\mathbb{Q}_p$. In Chapter 4, we use this criterion (Lemma 56 of Chapter 4) to gather numerical data for the cases $d = 1$ and $d = 2$. In Chapter 5, we investigate $\pi'_E(x)$ on average over all $E/\mathbb{Q}$ and present the proof of Theorem 2.

Chapter 2

Backgound

2.1 p-adic Fields

As we will later be looking at elliptic curves over p-adic fields we first need to look at the theory of p-adic fields. To do this we first look at valuations.

Definition 3 *Fix a prime $p \in \mathbb{Z}$. The p-adic valuation on $\mathbb{Z}$ is defined by the function*

$$\nu_p : \mathbb{Z} - \{0\} \to \mathbb{R}$$

which for each $x \in \mathbb{Z} - \{0\}$ is defined as follows, let $\nu_p(x)$ be the unique non-negative integer satisfying

$$x = p^{\nu_p(x)} x' \text{ with } p \nmid x'.$$

One extends ν_p to $\mathbb{Q}$ in the following way. If $x = a/b \in \mathbb{Q}^\times$, with $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$, then $\nu_p(x) = \nu_p(a) - \nu_p(b)$. It is also convention to set $\nu_p(0) = \infty$. This valuation has the following property.

Lemma 4 *For all* $x, y \in \mathbb{Q}$

i) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$

ii) $\nu_p(x+y) \geq \ min\{\nu_p(x), \nu_p(y)\}$

Proof. i) Denote $x = a/b, y = c/d$ where $p \nmid b, p \nmid d$. Then $a = p^e \prod_i p_i^{e_i}, b = \prod_i p_i^{f_i}, c = p^g \prod_i p_i^{g_i}, d = \prod_i p_i^{h_i}$ where p_i are primes not equal to p, and $e, e_i, f_i, g, g_i, h_i \in \mathbb{Z}$. Then

$$\begin{aligned} \nu_p(xy) &= \nu_p(\frac{ac}{bd}) \\ &= \nu_p(ac) - \nu_p(bd) \end{aligned}$$

but as $p \nmid b$, and $p \nmid d$, $\nu_p(bd) = 0$. So consider $\nu_p(ac)$.

$$\begin{aligned} ac &= p^{\nu(ac)} \prod_i p_i^{e_i+g_i} \\ &= p^{e+g} \prod_i p_i^{e_i+g_i} \\ &= p^e p^g \prod_i p_i^{e_i+g_i} \\ &= p^{\nu(a)} p^{\nu(c)} \prod_i p_i^{e_i+g_i} \\ &= p^{\nu(a)+\nu(b)} \prod_i p_i^{e_i+g_i} \end{aligned}$$

So $\nu(xy) = \nu(x) + \nu(y)$.

ii)Let $x = p^e \frac{a}{b}$, and $y = p^f \frac{c}{d}$ such that $p \nmid a, b, c, d$ with $a, b, c, d, e, f \in \mathbb{Z}$. Now if $e = f$ then

$$\begin{aligned} x + y &= p^e(\frac{a}{b} + \frac{c}{d}) \\ &= p^e \frac{(ad + bc)}{bd} \end{aligned}$$

so $\nu_p(x + y) \geq e$ as $p \nmid bd$. Now let $e \neq f$ and let $f > e$. Then

$$\begin{aligned} x + y &= p^e(\frac{a}{b} + p^{f-e}\frac{c}{d}) \\ &= p^e \frac{(ad + p^{f-e}bc)}{bd}. \end{aligned}$$

Then as $f - e > 0$ and $p \nmid ad$, one has that $\nu_p(x+y) = e = \min\{\nu_p(x), \nu_p(y)\}$. Note that by the convention for $\nu_p(0)$ the case where are least one of x or y is zero is trivial.

■

Definition 5 *An absolute value on a field K is a function*

$$|\ |: K \to \mathbb{R}$$

that satisfies the following properties:

i) $|x| = 0$ *if and only if* $x = 0$

ii) $|xy| = |x||y|$ *for all* $x, y \in K$

iii) $|x + y| \leq |x| + |y|$ *for all* $x, y \in K$

If an absolute value on K *satisfies the following additional condition then we say that it in non-archimedean:*

iv) $|x + y| \leq max\{|x|, |y|\}$ *for all* $x, y \in K$

otherwise we say that the absolute value is archimedean.

Note that the trivial absolute value is defined as $|x| = 1$ for all $x \neq 0$. We now use the above valuation to define the p-adic absolute value.

Definition 6 *For any* $x \in \mathbb{Q}$, *define the p-adic absolute value of* x *by*

$$|x|_p = p^{-\nu_p(x)}$$

if $x \neq 0$, *and set* $|0|_p = 0$.

Definition 7 *A metric on a set* X *is a function* $d : X \times X \to \mathbb{R}$. *For all* $x, y, z \in X$ *this function must satisfy the following conditions,*

i) $d(x, y) = 0$ *if and only if* $x = y$, $d(x, y) \geq 0$

ii) $d(x, y) = d(y, x)$

iii) $d(x, z) \leq d(x, y) + d(y, z)$.

In addition a metric is called non-archimedean if it satisfies

iv) $d(x, z) \leq max(d(x, y), d(y, z))$.

One notes that by the Lemma above the function $|\ |_p$ is a non-archimedean absolute value on $\mathbb{Q}$

Definition 8 *Let K be a field and $|\ |$ and absolute value on K. We then define the distance between two elements $x, y \in K$ by $d(x,y) = |x-y|$.*

This distance function $d(x,y)$ is called the metric induced by the absolute value. Then as all metrics define a topology, we now have a topology on K. But first we note that if $|\ |$ is a non-archimedean absolute value, then for any $x, y, z \in K$, $d(x,y) \leq \max\{d(x,z), d(z,y)\}$.

Definition 9 *Let K be a field with absolute value $|\ |$. Let $a \in K$, $r \in \mathbb{R}^+$. Then define the open ball of radius r and center a to be the set*

$$B(a,r) = \{x \in K \mid d(x,a) < r\}.$$

Define the closed ball of radius r and center a to be the set

$$\overline{B}(a,r) = \{x \in K \mid d(x,a) \leq r\}.$$

These sets define a topology on the field K. The topology defined has the following property.

Proposition 10 *If $|\ |$ is a non-archimedean absolute value then the set $B(a,r)$ is both open and closed.*

Proof. All that needs to be shown here is that $B(a,r)$ is closed as it has been defined to be an open set. So let x be in the boundary of $B(a,r)$. Choose a number s such that $0 < s < r$, and consider $B(x,s)$. As x is in the boundary $B(a,r) \bigcup B(x,s) \neq \emptyset$. So let $y \in B(a,r) \bigcup B(x,s)$. This implies that $|y-a| < r$ and $|y-x| < s \leq r$. But then as we are using a non-archimedean absolute value, we get that

$$\begin{aligned} |x-a| &\leq \max\{|x-y|, |y-a|\} \\ &< \max\{s, r\} \\ &\leq r. \end{aligned}$$

So $x \in B(a,r)$, and all boundary points of $B(a,r)$ are elements of $B(a,r)$. ■

Note that similarly if $r \neq 0$ then the set $\overline{B}(a,r)$ is also both open and closed.

Definition 11 *Two absolute values* $|\ |_1$ *and* $|\ |_2$ *on a field* k *are said to be equivalent if they define the same topology on* k.

Definition 12 *Define the absolute value* $|\ |_\infty$ *on* $\mathbb{Q}$ *by* $|x| = x$ *if* $x \geq 0$ *or* $|x| = -x$ *if* $x < 0$.

Theorem 13 *(Ostrowski) Every non-trivial absolute value on* $\mathbb{Q}$ *is equivalent to one of the absolute values* $|\ |_p$*, where* p *is either a prime or* $p = \infty$.

Proof. See [5] Gouvea 3.1.3 ■

In order to define the p-adic numbers we will first need to define and look at the properties of Cauchy Sequences.

Definition 14 *A sequence (x_n) in a field with $|\ |$, is as Cauchy Sequence if for every positive real number ϵ, there is a positive integer N, such that for any $m, n > N$*

$$|x_m - x_n| < \epsilon.$$

Lemma 15 *A sequence (x_n) of rational numbers is a Cauchy sequence with respect to a non-arcimedean absolute value $|\ |$ if and only if* $\lim_{n\to\infty} |x_{n-1} - x_n| = 0$.

Proof. Let $m = n + r$, for $r > 0$. Then

$$\begin{aligned} |x_m - x_n| &= |x_m - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + ... + x_{n+1} - x_n| \\ &\leq \max\{|x_m - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, ..., |x_{n+1} - x_n|\}. \end{aligned}$$

So the result follows. ■

Let $|\ |$ be a non-archimedean absolute value on $\mathbb{Q}$. Then we define CS to be the set of all Cauchy sequences of $\mathbb{Q}$ with respect to $|\ |$, and NS to be the

set of all sequences (x_n) in $\mathbb{Q}$ such that $\lim_{n\to\infty}|x_n| = 0$. Then we can note that $NS \subseteq CS$. Also we can add and multiply elements of CS as follows,

$$\begin{aligned}(x_n) + (y_n) &= (x_n + y_n)\\ (x_n) \times (y_n) &= (x_n y_n).\end{aligned}$$

Proposition 16 *With addition and multiplication defined as above CS is a commutative ring.*

Proof. It is easy to see CS has zero element $0_{CS} = (0)$, and identity element $1_{CS} = (1)$. Now consider $(x_n y_n)$. We have that

$$\begin{aligned}|x_{n+1}y_{n+1} - x_n y_n| &= |x_{n+1}y_{n+1} - x_{n+1}y_n + x_{n+1}y_n - x_n y_n|\\ &\leq \max\{|x_{n+1}y_{n+1} - x_{n+1}y_n|, |x_{n+1}y_n - x_n y_n|\}\\ &= \max\{|x_{n+1}||y_{n+1} - y_n|, |y_n||x_{n+1} - x_n|\}.\end{aligned}$$

As well we have that

$$\begin{aligned}|(x_{n+1} + y_{n+1}) - (x_n + y_n)| &= |(x_{n+1} - x_n) + (y_{n+1} - y_n)|\\ &\leq \max\{|x_{n+1} - x_n)|, |(y_{n+1} - y_n)|\}.\end{aligned}$$

So the sequences $(x_n + y_n)$ and $(x_n y_n)$ are elements of CS. The rest of the commutative ring properties follow. ■

Lemma 17 *NS is a maximal ideal of CS.*

Proof. First we will show that NS is a ideal of CS. To see this let $(x_n) \in NS$ and $(y_n) \in CS$, and consider $(x_n y_n)$. As (y_n) is a Cauchy sequence its terms are bounded, hence as $(x_n) \to 0$, then also $(x_n y_n) \to 0$. So $(x_n y_n) \in NS$, and in the same way one sees that $(y_n x_n) \in NS$, and thus NS is an ideal.

Now we need to show that NS is maximal. Let $(x_n) \in CS$ be a sequence such that $\lim |x_n| = a \neq 0$. Then there exist $b > 0$ and an integer N such that $|x_n| \geq b > 0$ for $n > N$. Now define a sequence (y_n) by letting $y_n = 0$ if $n < N$, and $y_n = \frac{1}{x_n}$ for $n \geq N$. As
$|y_{n+1} - y_n| = |\frac{1}{x_{n+1}} - \frac{1}{x_n}| \leq \frac{x_{n+1} - x_n}{b^2} \to 0$. Now consider $(x_n y_n)$, it is zero for $n < N$, and 1 for $n \geq N$. So $(1) - (x_n y_n)$ tends to zero, and is thus in NS. So (1) can be seen as a multiple of (x_n) plus an element of NS, and is thus an element of the ideal generated by (x_n) and NS. So NS is a maximal ideal. ■

Now that we have considered Cauchy sequences and their properties we are ready to define the p-adic numbers and to consider their properties.

Definition 18 *We define the field of p-adic numbers to be the quotient of the ring CS by the ideal NS,* $\mathbb{Q}_p = CS/NS$.

We notice that two different constant sequences never differ by an element of NS. Thus we have an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, by sending $x \in \mathbb{Q}$ to the equivalence class of (x).

Lemma 19 *Let $(x_n) \in CS$, $(x_n) \notin NS$. Then the sequence $|x_n|$ is eventually stationary.*

Proof. As $(x_n) \notin NS$ then there exists $a > 0$ and N_1 such that for $n \geq N_1$, $|x_n| \geq a$. But as (x_n) is a Cauchy sequence we know that there exists an interger N_2 for which if $n, m \geq N_2$ then $|x_n - x_m| < a$. Then replacing N_1, and N_2 with $\max\{N_1, N_2\}$, we have that for $n, m \geq N$, $|x_n - x_m| < \max\{|x_n|, |x_m|\}$. But this implies that $|x_m| = |x_n + x_m - x_n| = |x_n|$ as our absolute value is non-archimedean. ∎

Definition 20 *If $a \in \mathbb{Q}_p$, and (x_n) is a Cauchy sequence representing a, then define $|a| = lim_{n\to\infty}|x_n|$.*

Note that this is well-defined as if there are 2 Cauchy sequences, (x_n) and (y_n), representing a, then they differ by an element of NS, so $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n$, which implies

$$\lim_{n\to\infty}|x_n| = \lim_{n\to\infty}|y_n|$$

We will now look at extensions of the p-adic numbers, as later we will be looking at elliptic curves over these extensions.

Claim 21 *For each $n \geq 1$ there exists an extension of $\mathbb{Q}_p$ which has degree n and is generated by the n roots of the irreducible polynomial which generate the unique extension of degree n of $\mathbb{F}_p$*

Proof. The claim follows directly from the three claims and corollary that follows.

■

Claim 22 *Suppose $f(x) \in \mathbb{Z}_p[x]$ factors in $\mathbb{Q}_p$, in a non-trivial way, such that $f(x) = g(x)h(x)$ with $g(x)$, $h(x) \in \mathbb{Q}_p[x]$ and non-constant. Then there exists non-constant $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ such that $f(x) = g_0(x)h_0(x)$.*

Proof. If $k(x) = a_n x^n + ... + a_1 + a_0 \in \mathbb{Q}_p[x]$ is any polynomial define $\omega(k(x)) = \min_{0 \geq i \geq n} \nu_p(a_i)$. Then for $a \in \mathbb{Q}_p$ one has that $\omega(ak(x)) = \nu_p(a) + \omega(k(x))$. As well $k(x) \in \mathbb{Z}_p[x]$ iff $\omega(k(x)) \geq 0$. ■

Claim 23 *If Claim 22 is true for $\omega(f(x)) = 0$ then it is true for $\omega(f(x)) \geq 0$.*

Proof. By the definition of ω there exists $a \in \mathbb{Q}_p$ such that $\omega(f(x)) = -\nu_p(a)$ by letting a be the inverse of the coefficient with the smallest valuation. Then as $f(x) \in \mathbb{Z}_p[x]$, $a^{-1} \in \mathbb{Z}_p$, and from above $\omega(a(f(x))) = 0$. Set $\widehat{f}(x) = af(x)$, $\widehat{g}(x) = ag(x)$. Then $\widehat{f}(x) = \widehat{g}(x)h(x)$ with $\omega(\widetilde{f}(x)) = 0$. Then by the assumption of the Claim $\widehat{f}(x) = G_0(x)H_0(x)$ where $G_0(x), H_0(x) \in \mathbb{Z}_p[x]$. This implies that $f(x) = a^{-1}\widehat{f}(x) = a^{-1}G_0(x)H_0(x)$. As $a^{-1} \in \mathbb{Z}_p$, $g_0(x) = a^{-1}G_0(x)$ is in $\mathbb{Z}_p[x]$ and $f(x)$ factors into $f(x) = g_0(x)H_0(x)$ as desired. ■

Claim 24 *Claim 22 is true for $\omega(f(x)) = 0$.*

Proof. Assume $\omega(f(x)) = 0$. Then as above there exists $b, c \in \mathbb{Q}_p$ such that $\omega(bg(x)) = 0$ and $\omega(ch(x)) = 0$. Let $\widehat{g}(x) = bg(x)$, $\widehat{h}(x) = ch(x)$ and $\widehat{f}(x) =$

$bcf(x) = \widehat{g}(x)\widehat{h}(x)$. Let $\overline{g}(x), \overline{h}(x)$ and $\overline{f}(x)$ be the reduction of $g(x), h(x)$ and $f(x)$ modulo p respectively. Then $\overline{g}(x), \overline{h}(x) \in \mathbb{F}_p[x]$ are non-zero and hence $\overline{f}(x)$ is non-zero. Thus $\omega(f(x)) = 0$ the above implies $\nu_p(bc) = 0$, giving the fact that bc is a p-adic unit.And so let $f(x) = (bc)^{-1}\widehat{f}(x) = (bc)^{-1}\widehat{g}(x)\widehat{h}(x)$. Letting $G(x) = (bc)^{-1}\widehat{g}(x)$ gives the desired result. ■

Corollary 25 *If $f(x) \in \mathbb{Z}_p[x]$ is a monic polynomial whose reduction modulo p is irreducible in $\mathbb{F}_p[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}_p$*

Proof. If $f(x)$ factors over $\mathbb{Q}_p$ then it factors over $\mathbb{Z}_p$. Then reducing the factorization modulo p gives a factorization over $\mathbb{F}_p$.

■

2.2 Witt Vectors

As well as looking at elliptic curves over p-adic fields we will also be concerned with elliptic curves over Witt vectors. Thus we will now define and consider the properties of Witt vectors.

Let p be a prime and $(X_0, X_1, ...X_n, ...)$ a sequence of indeterminates, and define the following to be Witt polynomials,

$$
\begin{aligned}
W_0(X) &= X_0 \\
W_1(X) &= X_0^p + pX_1 \\
W_2(X) &= X_0^{p^2} + pX_1^p + p^2X_2
\end{aligned}
$$

$$
W_n(X) = \sum_i p^i X_i^{p^{n-i}}.
$$

Now consider the ring $\mathbb{Z}[p^{-1}]$, then the X_i can be expressed as polynomials in the W_i where the coefficients are elements of $\mathbb{Z}[p^{-1}]$. For example, $X_0 = W_0$, $X_1 = p^{-1}W_1 - p^{-1}W_0^p$. Now let $(Y_0, ..., Y_n, ...)$ be another sequence of indeterminates.

Theorem 26 *For every $\Phi \in \mathbb{Z}[X, Y]$, there exists a unique sequence $(\varphi_0, ..., \varphi_n, ...)$ of elements of $\mathbb{Z}[X_0, ..., X_n, ...; Y_0, ..., Y_n, ...]$ such that;*

$$W_n(\varphi_0, ..., \varphi_n, ...) = \Phi(W_n(X_0, ...), W_n(Y_0, ...)),$$

for $n = 0, 1, ...$

Proof. See [9] Serre ■

We now use the above theorem to define "addition polynomials" $S_0, ...S_n, ...$ which are the polynomials $\varphi_0, ..., \varphi_n, ...$ associated with the polynomial $\Phi(X, Y) = X + Y$ We can also define a product by $P_0, ...P_n, ...$ which are the polynomials $\varphi_0, ..., \varphi_n, ...$ associated with the polynomial $\Phi(X, Y) = X \times Y$

Now let A be a commutative ring, and let $a = (a_0, ..., a_n, ...)$, $b = (b_0, ..., b_n, ...)$ be elements of $A^{\mathbb{N}}$. Set

$$a + b = (S_0(a, b), ..., S_n(a, b), ...),$$
$$a \times b = (P_0(a, b), ..., P_n(a, b), ...)$$

Theorem 27 *The laws of composition above make $A^{\mathbb{N}}$ into a commutative unitary ring (called the ring of Witt vectors with coefficients in A and denoted $W(A)$).*

Proof. Define a map

$$W_* : W(A) \to A^{\mathbb{N}}$$

by assigning to a Witt vector $a = (a_0, ..., a_n, ...)$ the element of the product ring $A^{\mathbb{N}}$ having $W_n(a)$ as the n^{th} coordinate. Then from the definitions of the polynomials S and P we see that W_* is a homomorphism. W_* is an isomorphism if p is invertible in A, and hence in this case $W(A)$ is a commutative ring with unit $1 = (1, 0, ..., 0, ...)$. Then if the theorem is proved for a ring A, it is also true for every subring and quotient ring. As it is true for every polynomial ring $\mathbb{Z}[p^{-1}][T_\alpha]$, where T_α is a family of indeterminates , it is true for $\mathbb{Z}[T_\alpha]$ and thus for all rings. ■

Example 28 *So first 3 addition polynomials are as follows.*

$S_0(a, b) = a_0 + b_0$

$S_1(a, b) = a_1 + b_1 + (\frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p})$

$$S_2(a,b) = (a_2 + b_2 + \frac{(pa_1^p + pb_1^p + a_0^{p^2} + b_0^{p^2} - a_0 + b_0)^{p^2} + p(a_1 + b_1 + (\frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p}))^p}{p^2})$$

Now let $W_n(A)$ be the set of vectors $(a_0, ..., a_{n-1})$ with n elements. As the polynomials φ only deal with variables of index $\leq i$ we see that $W_n(A)$ forms a ring, which is a quotient of $W(A)$, and is called the ring of Witt vectors of length n. Then $W(A)$ is the projective limit of the rings $W_n(A)$ as n tends towards infinity.

Definition 29 *Let A be a commutative ring with identity equipped with a topology defined by a decreasing sequence*

$$...a_3 \supset a_2 \supset a_1.$$

of ideals such that $a_n a_m = a_{n+m}$. Then we say that A is a p-ring if the following conditions hold

i) The residue ring $k = A/a_1$ is a perfect ring of characteristic p

ii) The ring A is Hausdorff and complete with respect to its topology

If in addition the topology on A is defined by the p-adic filtration $a_n = p^n A$ and p is not a zero divisor of A we say that A is a strict p-ring.

Theorem 30 *If k is a perfect ring of characteristic p, $W(k)$ is a strict p-ring with residue ring k.*

Proof. See [9] Serre ■

Note that $\mathbb{Z}_p$ is a strict p-ring with residue ring $\mathbb{F}_p$, so as a direct corollary of the above theorem we have that $W(\mathbb{F}_p) = \mathbb{Z}_p$ and that $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$.

Chapter 3

Elliptic Curves

In order to get the results we desire, we will need to consider elliptic curves over various fields and rings. In order to do this we will now look at the theory of elliptic curves in various situations.

3.1 Elliptic Curves

We begin our exploration of elliptic curves by defining and considering the basic properties of elliptic curves.

Definition 31 *An elliptic curve is an abelian variety of dimension 1. Any*

such curve E, defined over a field K, has a plane cubic model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.1}$$

where x and y are coordinates in the affine plane and the coefficients a_i are in the ground field K.

Note that we call the above equation a Weierstrass equation as in characteristic $\neq 2, 3$ then we can replace x, and y by

$$\rho = x + \tfrac{a_1^2+4a_2}{12},\ \rho' = 2y + a_1x + a_3,$$

and so (3.1) becomes a curve of the form

$$(\rho')^2 = 4\rho^3 - g_2\rho - g_3.$$

The curve (3.1) has a unique point at infinity in the projective plane, that we call $0 = (0 : 1 : 0)$. Given a curve defined by an equation in the form (3.1) we make the following definitions

$b_2 = a_1^2 + 4a_2$

$b_4 = a_1a_3 + 2a_4$

$b_6 = a_3^2 + 4a_6$

$b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$

$c_4 = b_2^2 - 24b_4 (= 12g_2)$

$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 (= g_2^3 - 27g_3^2)$

$j = \frac{c_4^3}{\Delta}$

Definition 32 *The quantity Δ from above is called the discriminant of the Weierstrass equation, j is called the j-invariant of the elliptic curve E.*

Definition 33 *We say that an elliptic is singular if $\Delta = 0$, it has a node if $\Delta = 0$ and $c_4 \neq 0$, it has a cusp if $\Delta = c_4 = 0$.*

One might wonder if the Weierstass equation is unique given an elliptic curve. If we assume that the line at infinity intersects E at only $(0 : 1 : 0)$, then the only change of variables that fixes infinity and keeps the Weierstrass form of the equation is

$$x = u^2x' + r,$$
$$y = u^3y' + u^2sx' + t,$$

with $u, r, s, t, \in \overline{K}$, $u \neq 0$. If the elliptic curve is in the form $(\rho')^2 = 4\rho^3 - g_2\rho - g_3$ then the only change of variables is even simpler, it is

$$x = u^2x',$$
$$y = u^3y',$$

for some $u \in \overline{K}^*$.

Definition 34 *(Group Law) Let E be an elliptic curve given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

i) Let $P_0 = (x_0, y_0) \in E$. *Then* $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.

Now let $P_1 + P_2 = P_3$ *with* $P_i = (x_i, y_i) \in E$.

ii) If $x_1 = x_2$ *and* $y_1 + y_2 + a_1x_2 + a_3 = 0$, *then* $P_1 + P_2 = 0$.

Otherwise let

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \text{ if } x_1 \neq x_2;$$
$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},\ \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \text{ if } x_1 = x_2.$$

iii) $P_3 = P_1 + P_2$ *is given by*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Definition 35 *Let* E_1, E_2 *be elliptic curves over a field* K. *A morphism from* E_1 *to* E_2 *is a rational map which is regular at every point of* E_1.

Theorem 36 *Let* E/K *be an elliptic curve. Then the above equations giving the group law on* E *define morphisms.*

$$+ : E \times E \to E, \quad \text{and} \quad - : E \to E$$
$$(P_1, P_2) \to P_1 + P_2 \qquad P \to -P$$

Proof. Let us first consider the subtraction map,

$$(x, y) \to (x, -y - a_1x - a_3).$$

We see that it as a rational map, and as E is smooth, it follows that it is a morphism.

Now we fix a $Q \neq 0$ and look at the "translation by Q" map,

$$\tau : E \to E$$
$$\tau(P) = P + Q.$$

From the group law above we see again that it is a rational map, and thus as E is smooth, it is a morphism. We also see that as it has an inverse, $P \to P - Q$, it is an isomorphism.

Finally we deal with the general addition map $+ : E \times E \to E$. By inspection we see that it is a morphism, except possibly for points of the form $(P, P), (P, -P), (P, 0), (0, P)$, since it is for these points that the rational funtions

$$\lambda = \tfrac{y_2 - y_1}{x_2 - x_1},\ \nu = \tfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \text{ if } x_1 \neq x_2;$$

are not well-defined. To see that we still have a morphism we let τ_1 and τ_2 by translation maps defined above for the points Q_1 and Q_2 respectively. Consider the composition of maps

$$\phi : E \times E \xrightarrow{\tau_1 \times \tau_2} E \times E \xrightarrow{+} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_1^{-1}} E.$$

As the group law on E is both associative and commutative, the effect of these maps is as follows:

$$(P_1, P_2) \longrightarrow (P_1 + Q_1, P_2 + Q_2) \longrightarrow P_1 + Q_1 + P_2 + Q_2$$

$$\longrightarrow P_1 + P_2 + Q_2 \longrightarrow P_1 + P_2.$$

Now as the $\tau_i's$ are isomorphisms, we see that ϕ is a morphism except possibly at points of the form $(P - Q_1, P - Q_2)$, $(P - Q_1, -P - Q_2)$, $(P - Q_1, -Q_2)$, $(-Q_1, P - Q_2)$. But as Q_1, and Q_2 were chosen arbitrarily, by varying Q_1 and Q_2 we get a set of rational maps

$$\phi_1, \phi_2, ..., \phi_n : E \times E \to E$$

such that

(a) ϕ_1 is the addition map defined above.

(b) For each $(P_1, P_2) \in E \times E$, some ϕ_i is defined at (P_1, P_2). (c) If ϕ_i and ϕ_j are both defined at (P_1, P_2) then $\phi_i(P_1, P_2) = \phi_j(P_1, P_2)$.

It follows that addition is defined on all of $E \times E$, and so is a morphism. ■

We now consider the relationship between two elliptic curves.

Definition 37 *Let E_1 and E_2 be elliptic curves. An isogeny between E_1 and E_2 is a morphism*

$$\phi : E_1 \to E_2$$

such that $\phi(0) = 0$. Then E_1 and E_2 are isogenous if there exists an isogeny between them with $\phi(E_1) \neq \{0\}$.

Now as elliptic curves are groups the maps between them form groups. Hence we can let

$$\text{Hom}(E_1, E_2) = \{ \text{ isogenies } \phi : E_1 \to E_2 \}$$

Then the above addition law implies that $\text{Hom}(E_1, E_2)$ is a group under the addition law,

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

Then if $E_1 = E_2$ we can compose isogenies. So for an elliptic curve E we let

$$\text{End}(E) = \text{Hom}(E, E)$$

be the ring with multiplication defined by composition

$$(\phi\psi)(P) = \phi(\psi(P))$$

Then for $m \in \mathbb{Z}$ we can define the multiplication by m isogeny,

$$[m] : E \to E,$$

in the obvious way. For $m > 0$ then

$$[m](P) = P + P + ... + P \text{ (m terms)}.$$

If $m < 0$ then we let $[m](P) = [-m](-P)$, and for $m = 0$ we have $[0](P) = 0$.

Definition 38 *Let $E(K)$ be an elliptic curve over a field K and $m \in \mathbb{Z}$, $m \neq 0$. The m-torsion subgroup of $E(K)$, denoted by $E[m]$, is the set of points of order m in $E(K)$.*

$$E[m] = \{P \in E(K) : [m]P = 0\}$$

The torsion subgroup of $E(K)$, is the set of points in $E(K)$ which have finite order, and is denoted E_{tors}.

Definition 39 *Suppose that char$(K) = 0$, then if End(E) is strictly larger then $\mathbb{Z}$ we say that E has complex multiplication.*

3.2 Elliptic Curves over Local Fields

We now start to look at elliptic curves in more specific situations that we will need later. We start with looking at elliptic curves over local fields. To start we must first consider local fields.

Definition 40 *A local field is a field that is complete with respect to a discrete valuation, and which has a finite residue class field.*

Examples of local fields include finite extensions of the fields $\mathbb{Q}_p$. When working a local field K which is complete with respect to the valuation ν one uses the following notation.

i) R the ring of integers of K, $R = \{x \in K | \nu(x) \geq 0\}$

ii) R^* the unit group of R, $R^* = \{x \in K | \nu(x) = 0\}$

iii) M the maximal ideal of R, $M = \{x \in K | \nu(x) > 0\}$

iv) π a uniformizer for R $(M = \pi R)$

v) k the residue field of R, $k = R/M$

Note: this notation will be used throughout this section.

In the case where $K = \mathbb{Q}_p$, the ring of integers is $\mathbb{Z}_p = \{x \in \mathbb{Q}_p | \nu(x) \geq 0\}$, the unit group is $\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p | \nu(x) = 0\}$, the maximal ideal is $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p | \nu(x) > 0\}$, the uniformizer is $\pi = p$, and the residue field of $\mathbb{Z}_p$ is $k = \mathbb{Z}/p\mathbb{Z}$.

Now that we have defined local fields and considered their properties we may start to look at elliptic curves over them.
Let E/K be an elliptic curve with a Weierstrass equation

$$y^2 + a_1xy + a_3y \quad = \quad x^3 + a_2x^2 + a_4x + a_6$$

By replacing (x, y) by (u^{-2x}, u^{-3y}) , each a_i becomes $u^i a_i$, so by choosing a u that is divisible by a large power of π, we can find a Weierstrass equation with all $a_i \in R$. Then as the discriminant Δ has $\nu(\Delta) \geq 0$, and as ν is discrete, we can find a equation with $\nu(\Delta)$ minimized.

Definition 41 *Let E/K be an elliptic curve. A Weierstrass equation is called a minimal Weierstrass equation for E at ν if $\nu(\Delta)$ is minimized, with all $a_i \in R$. Then the value $\nu(\Delta)$ is called the valuation of the minimal discriminant of E at ν.*

If we have a Weierstrass equation we can find out if it is a minimal equation as we know the $a_i's$ have to be elements of R, thus $\Delta \in R$. So if our

equation is not minimal then there is a change of coordinates which gives a new equation with discriminant $\Delta' = u^{-12}\Delta \in R$. So $\nu(\Delta)$ can only be changed by multiples of 12. Thus an Weierstrass equation is minimal if all $a_i \in R$ and $\nu(\Delta) < 12$.

As was said above ν is discrete so one can always find a Weierstrass equation with all $a_i \in R$, such that $\nu(\Delta) < 12$. So every elliptic curve over K has a minimal Weierstrass equation.

We will now consider the relationship between an elliptic curve over a local field, and it's residue field.

Now let us consider reduction modulo π, which we will denote by a tilde. Given a minimal Weierstrass equation for the elliptic curve E/K, we can reduce the coefficients modulo π. By doing this we get a curve over k, $\widetilde{E} : y^2 + \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6}$. $\widetilde{E}$ is called the reduction of E modulo π. Then if $P \in E(K)$ we can find homogeneous coordinates $P = (x_0 : y_0 : z_0)$, where $x_0, y_0, z_0 \in R$ and at least one of the coordinates is in R^*. Then the reduction of P, $\widetilde{P} = (\widetilde{x_0} : \widetilde{y_0} : \widetilde{z_0})$ is in $\widetilde{E}(k)$. So we have a reduction map

$$\begin{aligned} E(K) &\rightarrow \widetilde{E}(k) \\ P &\rightarrow \widetilde{P}. \end{aligned}$$

Definition 42 *Let E be a curve given by a Weierstrass equation. A point $P = (x_0, y_0)$ satisfying the Weierstrass equation $f(x, y)$ is a singular point on E if $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$. The non-singular part of E, denoted E_{ns}, is the set of non-singular points of E.*

Proposition 43 *Let E be a curve given by a Weierstrass equation with discriminant $\Delta = 0$ (E has a singular point). Then the group law on elliptic curves makes E_{ns} into an abelian group.*

Proof. see [10] Silverman section III prop 2.5 ■

Thus for all elliptic curves E_{ns} is a group, as if E is given by a Weierstrass equation with discriminant $\Delta \neq 0$, the E_{ns} contains all points of E. So for the curve $\widetilde{E}/k$,we see that $\widetilde{E}_{ns}(k)$, is a group, and we make the following definition.

Definition 44 *We define the set of points of non-singular reduction, $E_0(K) = \{P \in E(K) | \widetilde{P} \in \widetilde{E}_{ns}(k)\}$. We also define the kernel of reduction, $E_1(K) = \{P \in E(K) | \widetilde{P} = \widetilde{0}\}$.*

These sets of points are related in a quite nice way, as below shows.

Proposition 45 *There is an exact sequence of abelian groups*

$$0 \to E_1(K) \to E_0(K) \to \widetilde{E}_{ns}(k) \to 0,$$

where the right-hand map is reduction modulo π.

Proof. First we will let us look at $E(K)$ and $\widetilde{E}_{ns}(k)$, the group laws for these groups are defined by taking the intersection of the curve with line in $\mathbb{P}^2$ (where $\mathbb{P}^2$ is projective 2-space). As the reduction map $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$ takes lines to lines, hence it follows that $E_0(K)$ is a group, and that the map $E_0(K) \to \widetilde{E}_{ns}(k)$ is a homomorphism. Then from the definition of $E_1(K)$ we have exactness at the left and center.

Let E have a minimal Weierstrass equation

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

with $\widetilde{f}(x,y)$ the corresponding polynomial with coefficients reduced modulo π, and $\widetilde{P} = (\alpha, \beta) \in \widetilde{E}_{ns}(k)$ any point. As $\widetilde{P}$ is non-singular, it follows that either $\frac{\partial \widetilde{f}}{\partial \widetilde{x}}(\widetilde{P}) \neq 0$ or $\frac{\partial \widetilde{f}}{\partial \widetilde{y}}(\widetilde{P}) \neq 0$. Wlog we will assume $\frac{\partial \widetilde{f}}{\partial \widetilde{x}}(\widetilde{P}) \neq 0$. Then let $y_0 \in R$ such that $\widetilde{y_0} = \beta$, and consider the equation $f(x, y_0) = 0$. When it is reduced modulo π is has α as a simple root, as $\frac{\partial \widetilde{f}}{\partial x}(\alpha, \widetilde{y_0}) \neq 0$.. Thus by Hensel's lemma, the root α can be lifted to an $x_0 \in R$ such that $\widetilde{x_0} = \alpha$ and $f(x_0, y_0) = 0$ Thus the point $P = (x_0, y_0) \in E_0(K)$ reduces to $\widetilde{P}$, and we have exactness of our sequence. ■

3.3 Elliptic Curve Over Finite Fields

We will now consider what happens when we have an elliptic curve over a finite field. We want to know the number of points that the elliptic curve

could have over a finite field, to do this we must first look at isogenies between elliptic curves.

Definition 46 *Let E_1, E_2 be elliptic curve defined over a field K, let $K(E)$ be the function field of E/K, and let $\phi : E_1 \to E_2$ be a map of curves. A non-constant ϕ induces an injection of function fields fixing K,*

$$\phi^* : K(E_2) \to K(E_1).$$

If ϕ in not constant, then ϕ is said to be finite, and we define its degree by

$$deg\phi = [K(E_1) : \phi^* K(E_2)]$$

We say that ϕ is separable if the extension $K(E_1)/\phi^* K(E_2)$ is separable, and denote the separable degree of the extension $deg_s\phi$

Lemma 47 *Let E_1, E_2 be elliptic curves, and let $\phi : E_1 \to E_2$ be a non-constant isogeny. Then for every $Q \in E_2$, $\#\phi^{-1} = deg_s\phi$. As well assuming ϕ is separable, then $\#ker\phi = deg\phi$.*

Proof. Let $Q, Q' \in E_2$. Then let us choose a $S \in E_1$ such that $\phi(S) = Q' - Q$. Now as ϕ is a homomorphism, there is a one-to-one correspondence

$$\phi^{-1}(Q) \to \phi^{-1}(Q')$$
$$P \to P + S$$

Thus $\#\phi^{-1}(Q) = \deg_s \phi$.

Now consider if ϕ is seperable, as we just saw $\#\phi^{-1}(Q) = \deg_s \phi$, so by setting $Q = 0$ we have $\#\ker\phi = \deg\phi$ ■

For the following let $q = p^n$ for a prime p, K be a finite field with q elements and let E/K be an elliptic curve.

Proposition 48 *Let E be defined over $\mathbb{F}_q$, let $\phi : E \to E$ be the q^{th}-power Frobenious endomorphism, and let $m, n \in \mathbb{Z}$. Then the map*

$$m + n\phi : E \to E$$

is separable if and only if $p \nmid m$. In particular the map $1 - \phi$ is separable.

Proof. Let ω be an invariant differential on E. A map $\psi : E \to E$ is inseparable if and only if $\psi^*\omega = 0$. Then we compute that $(m + n\phi)^*\omega = m\omega + n\phi^*\omega$, and as $\phi^* dx = d(x^q) = 0$ we have that $\phi^*\omega = 0$. So

$$(m + n\phi)^*\omega = m\omega.$$

As $m\omega = 0$ if and only if $p|m$, which gives the result. ■

Definition 49 *Let p be a prime. Let $a_p(E)$ be the integer such that $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$.*

We now have enough background to estimate the number of points an elliptic curve can have over a finite field.

Theorem 50 *Let E/K be an elliptic curve defined over the field with q elements. Then*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

Proof. Fix a Weierstrass equation for E with coeffiencients in K, and consider the q^{th}-power Frobenius morphism, defined by

$$\phi : E \to E$$
$$(x, y) \to (x^q, y^q).$$

Now the Galois group $G_{\overline{K}/K}$ is topologically generated by the q^{th}-power map on $\overline{K}$, so we see that for a point $P \in E(\overline{K})$, $P \in E(K)$ if and only if $\phi(P) = P$. Thus

$$E(K) = \ker(1 - \phi),$$

which implies that $\#E(K) = \#\ker(1-\phi) = \deg(1-\phi)$ as $1 - \phi$ is separable. The degree map on $\mathrm{End}(E)$ is a positive definite form, and $\deg\phi = q$. So consider the following version of the Cauchy-Schwarz inequality.

Lemma 51 *Let A be an abelian group and $d : A \to \mathbb{Z}$ a positive definite quadratic form. Then for all $\alpha, \beta \in A$,*

$$|d(\alpha - \beta) - d(\alpha) - d(\beta)| \leq 2\sqrt{d(\alpha)d(\beta)}.$$

By applying this inequality to $\deg(1-\phi)$ we get the desired result. ■

Now if we let E_1, E_2 be elliptic curves, let $\phi : E_1 \to E_2$ be an isogeny with dual $\widehat{\phi}$ and let $m = \deg\phi$. Then by the definition of the dual isogeny $\widehat{\phi} \circ \phi = [m]$ on E_1.

Proposition 52 *Let E/K be and elliptic curve. Then either*

$$E[p^e] \cong \{0\} \text{ for all } e = 1, 2, 3, ...; \text{ or}$$
$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \text{ for all } e = 1, 2, 3, ...$$

Proof. Let ϕ the the p^{th}-power Frobenious morphism. Then

$$\begin{aligned} \#E[p^e] &= \deg_s[p^e] \\ &= (\deg_s(\widehat{\phi} \circ \phi))^e \\ &= (\deg_s\widehat{\phi})^e \end{aligned}$$

where the last equality coming from the fact that ϕ is purely inseparable. Then as $\deg\widehat{\phi} = \deg\phi = p$, there are two cases.. If $\widehat{\phi}$ is inseparable, then $\deg_s\widehat{\phi} = 1$, thus $\#E[p^e] = 1$ for all e. The other case is if $\widehat{\phi}$ is separable, then $\deg_s\widehat{\phi} = p$, thus $\#E[p^e] = p^e$ for all e. Which implies that $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$. ■

3.4 Elliptic Curves over Rings

Not only will we need to consider elliptic curves over fields, but we will also need to look at elliptic curves over rings. We will follow Lenstra's paper [6]

for our definitions in this case. As rings have less structure then fields, there are more requirements for defining elliptic curves over rings.

Let $n > 0$ be a positive integer. Consider the set of all triples $(\bar{x}, y, z) \in (\mathbb{Z}/n\mathbb{Z})^3$ for which x, y, z generate the unit ideal of $\mathbb{Z}/n\mathbb{Z}$. Then the group of units $(\mathbb{Z}/n\mathbb{Z})^*$ acts on this set by $u(x, y, z) = (ux, uy, uz)$. Denote by $(x : y : z)$ the orbit of (x, y, z). and denote by $\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$ the set of all orbits.

For $a, b \in \mathbb{Z}/n\mathbb{Z}$ consider the curve $E = E_{a,b}$ defined over $\mathbb{Z}/n\mathbb{Z}$ by the equation $y^2 = x^3 + ax + b$. The set of points $E(\mathbb{Z}/n\mathbb{Z})$ of a curve over $\mathbb{Z}/n\mathbb{Z}$ is defined by

$$E(\mathbb{Z}/n\mathbb{Z}) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) : y^2z = x^3 + axz^2 + bz^3\}.$$

If $6(4a^3 + 27b^2) \in (\mathbb{Z}/n\mathbb{Z})^*$ then E is called an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$. Note that if $2|n$ or $3|n$ then $6(4a^3 + 27b^2) \notin (\mathbb{Z}/n\mathbb{Z})^*$, and thus the following does not apply in these cases. Note that this was not the case when we were dealing with fields.

Now before we define an addition algorithm we need to define the "point at infinity". Denote by 0 the point $(0 : 1 : 0) \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$. Then let the subset V_n of $\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$ be the set of "finite" points together with 0.

$$V_n = \{(x : y : 1) : x, y \in (\mathbb{Z}/n\mathbb{Z})\} \bigcup \{0\}$$

For $P \in V_n$ and a prime p such that $p|n$ denote by P_p the point of $\mathbb{P}^2(\mathbb{F}_p)$ obtained by reducing the coordinates of P modulo p. Note that $P_p = 0_p$ if and only if $P = 0$.

We now define an algorithm which we will use to add points on our curves. Given $n > 0$, an integer, $a \in \mathbb{Z}/n\mathbb{Z}$ and $P, Q \in V_n$, the following algorithm will either calculate a non-trivial divisor d of n, or determines a point $R \in V_n$ with the following property, if p is any prime dividing n for which there exists $b \in \mathbb{F}_p$ such that

$$6(4\overline{a}^3 + 27b^2) \neq 0 \quad \text{for } \overline{a} = (a \bmod p),$$
$$P_p \in E_{\overline{a},b}(\mathbb{F}_p), \qquad Q_p \in E_{\overline{a},b}(\mathbb{F}_p),$$

Then $R_p = P_p + Q_p$ in the group $E_{\overline{a},b}(\mathbb{F}_p)$.

The algorithm is as follows, if $P = 0$ put $R = Q$ and stop. If $P \neq 0$, $Q = 0$ put $R = P$ and stop. Lastly if $P = (x_1, y_1, 1) \neq 0$, $Q = (x_2, y_2, 1) \neq 0$, then we use the Euclidean algorithm to calculate $\gcd(x_1 - x_2, n)$. If the $\gcd(x_1 - x_2, n) = d$ and d is neither 1 or n then stop. If $\gcd(x_1 - x_2, n) = 1$ then the Euclidean algorithm also gives $(x_1 - x_2)^{-1}$. Then we set

$$\lambda = (y_1 - y_2)(x_1 - x_2)^{-1},$$
$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$
$$R = (x_3 : y_3 : 1),$$

and stop. If the $\gcd(x_1 - x_2, n) = n$, we then calculate $\gcd(y_1 + y_2, n)$. If this equals a d not equal to 1 or n then stop. If $d = n$ then we have that $x_1 = x_2$, and $y_1 = y_2$ and so we put $R = 0$ and stop. Finally if $\gcd(y_1 + y_2, n) = 1$ then we set

$$\lambda = (3x_1^2 + a)(y_1 + y_2)^{-1},$$
$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$
$$R = (x_3 : y_3 : 1),$$

and stop. If the algorithm computes a point R, then we say that the operation defined on V_n in this way is called addition and denote it $P + Q$. If there exists $b \in \mathbb{Z}/n\mathbb{Z}$ such that

$$6(4a^3 + 27b^2) \in (\mathbb{Z}/n\mathbb{Z})^*,\ P \in E_{a,b}(\mathbb{Z}/n\mathbb{Z}),\ Q \in E_{a,b}(\mathbb{Z}/n\mathbb{Z}),$$

then $P + Q$ is defined. So we have addition and as the only multiplication we do is kP for $k \in \mathbb{Z}$ and a point P, addition is all we need.

Chapter 4

Local torsion primes of a fixed degree d (including numerical data)

We now start using the background that we have developed to gather some numerical data with regards to Conjecture 1.

4.1 Local torsion primes of a fixed degree

Conjecture 53 *Assume that E does not have complex multiplication. Fix $d \geq 1$. Then there are finitely many primes p such that there exists an extension $K/\mathbb{Q}_p$ of degree at most d with $E(K)[p] \neq 0$.*

We remark that the conjecture is false for d large enough when E has complex multiplication as showed in [4].

Definition 54 *We will call a prime p a local torsion prime for E if E possesses a point of order p over $\mathbb{Q}_p$. We will say that p is a local torsion prime of degree d if there is a finite extension of degree d, $K/\mathbb{Q}_p$ with $E(K)[p] \neq 0$.*

Thus a local torsion prime is a local torsion prime of degree 1. So in looking at the conjecture one is looking local torsion primes of finite degree, which leaves the problem of finding these primes.

Lemma 55 *Let E be an elliptic curve over $\mathbb{Q}$. Then E has a point of order p over $\mathbb{Q}_p$ if and only if E has a point of order p over $\mathbb{Z}/p^n\mathbb{Z}$ for all $n \in \mathbb{N}$*

Proof. $\Rightarrow$]
In order to reduce a point $P \in E(\mathbb{Q}_p)[p]$ mod $p^n\mathbb{Z}$ we find homogeneous coordinates $P = (x_0 : y_0 : z_0)$, with at least one of $x_0, y_0, z_0 \in \mathbb{Z}_p^*$. Then the reduced point $\widetilde{P} = (\widetilde{x}_0 : \widetilde{y}_0 : \widetilde{z}_0)$ is in $E(\mathbb{Z}/p^n\mathbb{Z})$. As at least one of $x_0, y_0, z_0 \in \mathbb{Z}_p^*$, $\widetilde{P} \neq 0$. Now as $x_0, y_0, z_0 \in \mathbb{Z}_p$ they can be written $x_0 = \sum_{m=0}^{\infty} b_m p^m$, $y_0 = \sum_{m=0}^{\infty} c_m p^m$, $z_0 = \sum_{m=0}^{\infty} d_m p^m$, for $b_m . c_m, d_m \in \mathbb{Z}/p\mathbb{Z}$. So $\widetilde{x}_0 = \sum_{m=0}^{n} b_m p^m$, $\widetilde{y}_0 = \sum_{m=0}^{n} b_m p^m$, $\widetilde{z}_0 = \sum_{m=0}^{n} b_{\overline{m}} p^m$. So $p(\widetilde{x}_0 : \widetilde{y}_0 : \widetilde{z}_0) = 0$ in $E(\mathbb{Z}/p^n\mathbb{Z})$ because of how addition is defined. Note that the point at infinity reduces to itself.

$\Leftarrow$]

Conversely if for every $n \in \mathbb{N}$, E has a point of order p in in $E(\mathbb{Z}/p^n\mathbb{Z})$ then it can be written in the form $(x_n : y_n : z_n)$ where $x_n = \sum_{m=0}^{n} b_m p^m$, $y_n = \sum_{m=0}^{n} b_m p^m$, $z_n = \sum_{m=0}^{n} b_m p^m$. Then as there exists a set of these points so that they are consistent with respect to reduction. That is if $P_n = (x_n : y_n : z_n)$ is a point of order p in $E(\mathbb{Z}/p^n\mathbb{Z})$ then $P_n \mod p^{n-1} = P_{n-1}$, where P_{n-1} is a point of order p in $E(\mathbb{Z}/p^{n-1}\mathbb{Z})$ in our set. So there exists $x_\infty, y_\infty, z_\infty \in \mathbb{Z}_p$ such that $x_\infty = \sum_{m=0}^{\infty} b_m p^m$, $y_\infty = \sum_{m=0}^{\infty} b_m p^m$, $z_\infty = \sum_{m=0}^{\infty} b_m p^m$, where $P_\infty = (x_\infty : y_\infty : z_\infty)$ such that $pP_\infty = 0$ in $E(\mathbb{Q}_p)$ and P_∞ is consistent with respect to reduction. ■

More generally let $[K : \mathbb{Q}_p] = d$, with residue field k. We now state a criterion to detect local torsion prime of degree d by looking at $W_2(k)$. This is Lemma 3.1 of [4].

Lemma 56 *Let k be a finite extension of $\mathbb{F}_p$ of degree d. Let W be the ring of Witt vectors over k, and K be the field of fractions of W. Then if E is an elliptic curve over W then $rank_p E(W_2) = d$ if $E(K)[p] = 0$ else $rank_p E(W_2) = d + 1$ if $E(K)[p] \neq 0$. Also the following diagram commutes.*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 0 & \longrightarrow & E(K)[p] & \longrightarrow & E(k)[p] & \longrightarrow & (\mathbb{Z}/p)^d \\
\downarrow & & \downarrow & & \downarrow & & \| & & \| \\
0 & \longrightarrow & (\mathbb{Z}/p)^d & \longrightarrow & E(W_2)[p] & \longrightarrow & E(k)[p] & \longrightarrow & (\mathbb{Z}/p)^d
\end{array}$$

Proof. See [4] David and Weston, Lemma 3.1 ■

From this lemma we have a condition on the p-rank of $E(W_2)$ which corresponds to the elliptic curve having a local torsion prime at p. So we will use the above diagram to find when this condition is satisfied.

In the case $d = 1$, the following exact row is obtained from the above diagram:

$$0 \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \longrightarrow E(\mathbb{Z}/p^2\mathbb{Z})[p^\infty] \longrightarrow E(\mathbb{F}_p)[p^\infty] \longrightarrow 0$$

Exactness in the third arrow is a consequence of the following two lemmas.

Lemma 57 *Let $p \neq 2, 3$ and let E be an elliptic curve over $\mathbb{Q}$. If $Q = (x_0, y_0) \in E(\mathbb{F}_p)$ then there are exactly p lifts $\tilde{Q} = (x_0 + px_1, y_0 + py_1) \in E(\mathbb{Z}/p^2\mathbb{Z})$.*

Proof. Let $Q = (x_0, y_0) \in E(\mathbb{F}_p)$, and $x_0 + px_1$, be a lift of the x-coodinate, then we will see what are the possible lifts $y_0 + py_1$ for y_o. We must have

$$\begin{aligned} y^2 &\equiv x^3 + ax + b \bmod p^2 \\ (y_0 + py_1)^2 &\equiv (x_0 + px_1)^3 + a(x_0 + px_1) + b \bmod p^2 \\ y_0^2 + 2py_0y_1 &\equiv x_0^3 + 3px_0^2x_1 + ax_0 + apx_1 + b \bmod p^2 \end{aligned}$$

Now as $y_0^2 \equiv x_0^3 + ax_0 + b \bmod p$, p divides $y_0^2 - x_0^3 - ax_0 - b$, and so we have,

$$\frac{y_0^2 - x_0^3 - ax_0 - b}{p} \equiv -2y_0y_1 + 3x_0^2x_1 + ax_1 \bmod p$$

Then by our restrictions on p there is only one choice for y_1 provided $y_0 \neq 0$. So let us now consider the case when $y_0 = 0$. Suppose py_1 is a lift of the y-coordinate, then we shall see what the possible lifts $x_0 + px_1$ for x_0. We must have

$$\begin{aligned} y^2 &\equiv x^3 + ax + b \bmod p^2 \\ (py_1)^2 &\equiv (x_0 + px_1)^3 + a(x_0 + px_1) + b \bmod p^2 \\ 0 &\equiv x_0^3 + 3px_0^2x_1 + ax_0 + apx_1 + b \bmod p^2 \end{aligned}$$

Then as $0 \equiv x_0^3 + ax_0 + b \bmod p$, p divides $-x_0^3 - ax_0 - b$, and so we have,

$$\begin{aligned} \frac{-x_0^3 - ax_0 - b}{p} &\equiv 3x_0^2x_1 + ax_1 \bmod p \\ &\equiv x_1(3x_0^2 + a) \bmod p \end{aligned}$$

So there is only one choice for x_1 ■

Lemma 58 *Let $p \neq 2, 3$ and let E be an elliptic curve over $\mathbb{Q}$. If $Q = (0 : 1 : 0) \in E(\mathbb{F}_p)$ then there are exactly p lifts $\tilde{Q} = (px_1 : 1 : 0) \in E(\mathbb{Z}/p^2\mathbb{Z})$.*

Proof. As we are looking at the point at infinity it must satisfy the equation $y^2z = x^3 + axz + bz^3$. So suppose that $\tilde{Q} = (px_1 : 1 + py_1 : pz_1)$ is a lift of Q. Then we have

$$\begin{aligned} y^2z &\equiv x^3 + axz + bz^3 \bmod p^2 \\ (1+py_1)^2pz_1 &\equiv p^3x_1^3 + a(px_1)(pz_1) + bp^3z_1^3 \bmod p^2 \\ pz_1 + 2py_1 &\equiv 0 \bmod p^2 \end{aligned}$$

Thus $z_1 = 0$ and $y_1 = 0$, and there are p possible values for x_1. Thus there are p possible lifts $\tilde{Q} = (px_1 : 1 : 0)$ of $Q = (0 : 1 : 0)$.

■

Exactness in the 4th place comes because we are looking p^∞ torsion.

The algorithm for the case $d = 1$ is as follows. Let E be an elliptic curve over $\mathbb{Q}$. If $p = 2, 3$ then we use the division polynomials as shown below. Let p be a prime ≥ 5. A necessary condition for E to have p-torsion over $\mathbb{Q}_p$ is that E has p torsion over $\mathbb{F}_p$ which is equivalent to $p|\#E(\mathbb{F}_p) = p + 1 - a_p(E)$

which is equivalent to $a_p(E) \equiv 1 \bmod p$. By the Hasse bound, this means $a_p(E) = 1$. Then we have that $E(\mathbb{F}_p) = E(\mathbb{F}_p)[p] = E(\mathbb{F}_p)[p^\infty]$ and we have the exact sequence

$$0 \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \longrightarrow E(\mathbb{Z}/p^2\mathbb{Z})[p^\infty] \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

This gives two possible cases

-$E(\mathbb{Z}/p^2\mathbb{Z})[p^\infty] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

In this case $\text{rank}_p E(\mathbb{Z}/p^2\mathbb{Z}) = 2$ by definition of rank, and thus p is a local torsion prime for E

-$E(\mathbb{Z}/p^2\mathbb{Z})[p^\infty] \cong \mathbb{Z}/p^2\mathbb{Z}$

In this case $\text{rank}_p E(\mathbb{Z}/p^2\mathbb{Z}) = 1$ and thus p is a not local torsion prime for E

So then after checking the condition on a_p we must find a point of order p in $E(\mathbb{F}_p)$, say Q, which is not the point at infinity. As all points in $E(\mathbb{F}_p)$ have order p this comes down to finding a point that is not infinity. Now that we have our point Q we must lift it to $\widetilde{Q} \in E(\mathbb{Z}/p^2\mathbb{Z})$. We will use Hensel's lemma to do the lifting in the case $d = 1$. To do this we let either x, or y stay the same and lift the other. To decide which of the variables to lift we denote our elliptic curve by $f(x, y)$ and consider the partial derivatives. If $\frac{\partial f}{\partial x}$ evaluated at the point $Q = (x_0, y_0)$ is not divisible by p then $|f(x_0, y_0)| \leq |\frac{\partial f}{\partial x}(x_0, y_0)^2|$. So we lift x, with the lift of x_0, $x' = x_0 - \frac{f(x_0,y_0)}{\frac{\partial f}{\partial x}(x,y)}$. Else we lift y, with the lift of y_0, $y' = y_0 - \frac{f(x_0,y_0)}{\frac{\partial f}{\partial y}(x_0,y_0)}$. Then all that is left to see

is if our new point $\widetilde{Q}$ has order p, which is done by checking if $(p-1)\widetilde{Q} = -\widetilde{Q}$. If $\widetilde{Q}$ has order p then p is a local torsion prime and if $\widetilde{Q}$ has order not equal to p then p is not a local torsion prime.

This works in the cases where $p \geq 5$, but in the other cases as the addition formulas don't work as we are dealing with elliptic curves over rings. For these cases we need to know about division polynomials. Division polynomials $\psi_m \in \mathbb{Z}[x, y, A, B]$ are inductively defined as follows with x,y, A, and B free variables

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{for m} \geq 2 \\
\psi_{2m} &= \frac{\psi_m}{2y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{for m} \geq 3
\end{aligned}$$

These division polynomials ψ_m vanish precisely on the m-torsion points. Thus by finding the roots of these polynomials one can see if $E(\mathbb{Z}/p^2\mathbb{Z})$ has m torsion simply by seeing if any of the roots lie on $E(\mathbb{Z}/p^2\mathbb{Z})$.

Definition 66 *Let ϑ be an order, and let K be the field of fractions of ϑ. Then a fractional ideal of K is a finitely generated ϑ-submodule $a \neq 0$ of K. Then let $I(\vartheta)$ denote the group of proper fractional ϑ-ideals.*

Definition 67 *The fractional principal ideals $(a) = a\vartheta$, $a \in K^*$, form a subgroup of the group of ideals $I(\vartheta)$, which we will denote $P(\vartheta)$. The quotient group $Cl(\vartheta) = J(\vartheta)/P(\vartheta)$ is called the ideal class group of order ϑ.*

When $\vartheta = \vartheta_K$ the maximal order, then $I(\vartheta_K)$ and $P(\vartheta_K)$ will be denoted I_K and P_K respectively.

Definition 68 *Let ϑ_K be the maximal order, then $h(\vartheta_K) = (I_K : P_K)$ is the class number of ϑ_K*

Theorem 69 *Let d_K be the discriminant of the maximal order ϑ_K. Let ϑ be the order of conductor f in an imaginary quadratic field K. Then*

$$h(\vartheta) = \frac{h(\vartheta_K)f}{[\vartheta_K^* : \vartheta^*]} \prod_{p|f} (1 - (\frac{d_K}{p})\frac{1}{p}). \tag{5.1}$$

where $(\frac{d_K}{p})$ is the Legrendre symbol for primes not equal to two, and the Kronecker symbol for $p = 2$. Also $h(\vartheta)$ is always a integer multiple of $h(\vartheta_K)$

Proof. See [1] Cox Thm 7.24 ■

Definition 70 *Now by letting ϑ be an order in an imaginary quadratic field*

K, the Hurwitz class number is the weighted sum of class numbers

$$H(\vartheta) = \sum_{\vartheta \subset \vartheta' \subset \vartheta_K} \frac{2}{|\vartheta'^*|} h(\vartheta'). \tag{5.2}$$

We also write $H(\vartheta)$ as $H(\Delta)$, where Δ is the discriminant of ϑ.

Lemma 71 *With the definitions above $|H(a^2 - 4p)| \leq \sqrt{p}\log^2(p)$.*

Proof. See [2] Davenport ■

Theorem 72 *(Deuring's Theorem) Let $p > 3$ be prime, and let $N = p+1-r$ be an integer, where $-2\sqrt{p} \leq r \leq 2\sqrt{p}$. Then the number of elliptic curves E over $\mathbb{F}_p$ which have $|E(\mathbb{F}_p)| = N = p + 1 - r$ is*

$$\frac{p-1}{2} H(r^2 - 4p),$$

where H is the weighted Hurwitz class number.

Proof. See [1] Cox, Thm 14.18 ■

In [3], the authors showed that the Lang-Trotter conjecture was true on average by using the fact that the value of $a_p(E)$ depends only on E over $\mathbb{F}_p$ and using Deuring's Theorem. We saw in Chapter 4 that local torsion primes of degree d can be detected by looking at E over $W_2(k)$, where k is an extension of degree d of $\mathbb{F}_p$ (Lemma 56). We now want to count the number

of E over $\mathbb{Z}/p^2\mathbb{Z}$ such that E has a local torsion prime of degree d. This is achieved by the next proposition from [4].

Proposition 73 *Let $E_{a,b}$ be an ordinary elliptic curve over $\mathbb{F}_p$ such that $j(E_{a,b}) \neq 0, 1728$. Let k be an extension of $\mathbb{F}_p$ of degree d such that $E(k)[p] \neq 0$; set $W_2 = W/p^2$ with W the ring of Witt vectors of k. Then there are exactly p distinct pairs $(A_i, B_i) \in \mathbb{Z}/p^2 \times \mathbb{Z}/p^2$ such that $(A_i, B_i) \equiv (a, b)$ mod p and $rank_p E_{A_i,B_i}(W_2) = d + 1$*

We first show how to use Proposition 73 to show that on average, there are only finitely many local torsion primes.

Definition 74 *Let $\pi_{E_{a,b}}(x) = \#\{p \leq x : p$ is a local torsion prime of $E_{a,b}\}$.*

Definition 75 *Let $\nu_p(d)$ be the number of pairs $(a, b) \in \mathbb{Z}/p^2 \times \mathbb{Z}/p^2$ such that $E_{a,b}$ is an elliptic curve with $rank_p E_{a,b}(W_2) = d + 1$. Let $\nu'_p(d)$ (resp. $\nu_d^0(p)$, resp. $\nu_d^{1728}(p)$ be the number of pairs $(a, b) \in \mathbb{Z}/p^2 \times \mathbb{Z}/p^2$ such that $rank_p E_{a,b}(W_2) = d+1$ and $E_{a,b}$ does not have j-invariant 0 or 1728 (resp. has j-invariant 0, resp. has j-invariant 1728).*

Definition 76 *Let $S_{A,B}$ be the set of elliptic curves $E_{a,b}$ with $a, b \in \mathbb{Z}$ and $|a| \leq A$, $|b| \leq B$.*

Note that $\#S_{A,B} = 4AB(1 + o(1))$ as $A, B \to \infty$.

We now can look at what happens as an average for local torsion primes in the case $d = 1$. This is a special case of the results of [4].

Theorem 77 *Let $A, B \geq x^{7/4+\epsilon}$ for some $\epsilon \geq 0$. Then*

$$\frac{1}{4AB} \sum_{\substack{|a|\leq A \\ |b|\leq B}} \pi_{E_{a,b}}(x) < \infty.$$

Proof. We will begin by considering the sum

$$\sum_{\substack{|a|\leq A \\ |b|\leq B}} \pi_{E_{a,b}}(x),$$

$$\sum_{\substack{|a|\leq A \\ |b|\leq B}} \pi_{E_{a,b}}(x) = \sum_{p\leq x} \#\{|a| \leq A, |b| \leq B : p \text{ is a local torsion prime of } E_{a,b}\}$$

then by Lemma 56 (considering the $O(1)$'s as $A, B \to \infty$)

$$\begin{aligned}
&= \sum_{p\leq x} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1)) \#\{E/\mathbb{Z}/p^2\mathbb{Z} : \text{rank}_p E_{a,b}(\mathbb{Z}/p^2\mathbb{Z}) = 2\} \\
&= \sum_{p\leq x} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1)) \#\{E/\mathbb{Z}/p^2\mathbb{Z} : \text{rank}_p E_{a,b}(\mathbb{Z}/p^2\mathbb{Z}) = 2 \ , \\
&\quad j(E_{a,b}) \neq 0, 1728\} \\
&+ \sum_{p\leq x} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1)) \#\{E/\mathbb{Z}/p^2\mathbb{Z} : \text{rank}_p E_{a,b}(\mathbb{Z}/p^2\mathbb{Z}) = 2 \ , \\
&\quad j(E_{a,b}) = 0, 1728\}
\end{aligned}$$

Let us now separate our sum, and work from there. Let

$$S_1 = \sum_{p \leq x} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1)) \#\{E/\mathbb{Z}/p^2\mathbb{Z} : \text{rank}_p E_{a,b}(\mathbb{Z}/p^2\mathbb{Z}) = 2 \ , \\ j(E_{a,b}) \neq 0, 1728\}$$

and let

$$S_2 = \sum_{p \leq x} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1)) \#\{E/\mathbb{Z}/p^2\mathbb{Z} : \text{rank}_p E_{a,b}(\mathbb{Z}/p^2\mathbb{Z}) = 2 \ , \\ j(E_{a,b}) = 0, 1728\}.$$

Now let us consider S_1, from Proposition 73, we get

$$S_1 = \sum_{p \leq x} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1)) p \#\{E/\mathbb{F}_p : E_{a,b}(\mathbb{F}_p)[p] \neq 0, \\ j(E_{a,b}) \neq 0, 1728\}$$

$$= \sum_{p \leq x} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1)) p \#\{E/\mathbb{F}_p : j(E_{a,b}) \neq 0, 1728 \bmod p, \\ a_p = 1\}$$

then by Deuring's Theorem we have that,

$$\begin{aligned} &\ll 4AB\sum_{p\leq x}\frac{1}{p^4}H(1-4p)\frac{(p-1)}{2}p+O\left(2A\sum_{p\leq x}\frac{1}{p^2}H(1-4p)\frac{(p-1)}{2}p\right.\\ &+ \left. 2B\sum_{p\leq x}\frac{1}{p^2}H(1-4p)\frac{(p-1)}{2}p+\sum_{p\leq x}H(1-4p)\frac{(p-1)}{2}p\right). \end{aligned}$$

Note that we get $H(1-4p)$ from the condition that $a_p = 1$. Then by Lemma 71

$$\begin{aligned} &\ll 4AB\sum_{p\leq x}\frac{\sqrt{p}\log^2 p}{p^2}+O\left(2A\sum_{p\leq x}\sqrt{p}\log^2 p+2B\sum_{p\leq x}\sqrt{p}\log^2 p\right.\\ &+ \left.\sum_{p\leq x}p^{5/2}\log^2 p\right). \end{aligned}$$

So now looking at averages we get that

$$\begin{aligned} \frac{S_1}{4AB} &\ll \frac{1}{4AB}\left(4AB\sum_{p\leq x}\frac{\sqrt{p}\log^2 p}{p^2}+O\left(2A\sum_{p\leq x}\sqrt{p}\log^2 p\right.\right.\\ &\quad + \left.\left. 2B\sum_{p\leq x}\sqrt{p}\log^2 p+\sum_{p\leq x}p^{5/2}\log^2 p\right)\right)\\ &\ll \sum_{p\leq x}\frac{\sqrt{p}\log^2 p}{p^2}+O\left(\frac{x^{3/2}\log^2 x}{2B}\right.\\ &\quad + \left.\frac{x^{3/2}\log^2 x}{2A}+\frac{x^{7/2}\log^2 x}{4AB}\right). \end{aligned}$$

The last three terms of the above equation converge because of our condition on A and B. We can see this as $A \geq x^{7/4+\epsilon} > x^{3/2}$, $B \geq x^{7/4+\epsilon} > x^{3/2}$, and $AB \geq x^{7/2+\epsilon} > x^{7/2}$. Thus S_1 converges on average, so all we need to consider now is S_2. In their paper [4] David and Weston showed that $\sum_{p \leq x} \nu_d^0(p) \ll dx^{7/2}$, $\sum_{p \leq x} \nu_d^{1728}(p) \ll dx^{7/2}$ where $\nu_d^0(p)$ (resp. ν_d^{1728}) is the number of pairs $(a, b) \in \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ such that $E(W_2)$ has p-rank $d+1$ and $E_{a,b}$ has j-invariant 0 (resp. 1728). So in our case with $d = 1$, as S_2 is bounded by $A, B,$ and x, where as the sums that David and Weston were looking at were only bounded by x we can see that S_2 must also converge. So $\frac{1}{4AB} \sum_{|a| \leq A, |b| \leq B} \pi_{E_{a,b}}(x)$ converges and leads to the conjecture in the $d = 1$ case.

■

The proof for the general d case is exactly the same, which led David and Weston to their conjecture. We will now look at a slightly different question, what happens when we do not fix d.

Lemma 78 *A necessary condition for an elliptic curve E over $\mathbb{Q}$ to have an point of p-torsion over $\mathbb{F}_{p^d}$ is that $a_p(E)^d \equiv 1 \bmod p$.*

Proof. For E to have an point of p-torsion over $\mathbb{F}_{p^d}$ it is necessary for p to divide $\#E(\mathbb{F}_{p^d})$. This is because of the properties of abelian groups and by Lagrange's Theorem. Now from the Weil conjectures one has that

$\#E(F_{p^d}) = p^d + 1 - (\alpha_p^d + \overline{\alpha}_p^d)$, where α_p and $\overline{\alpha_p}$ come from the zeta function

$$Z(E;T) = \frac{(1-\alpha_p T)(1-\overline{\alpha_p}T)}{(1-T)(1-pT)}.$$

The numerator of this zeta function is $(1-\alpha_p T)(1-\overline{\alpha_p}T) = 1 - a_p T + pT^2$ where $a_p(E) = \alpha_p + \overline{\alpha}_p$ is the trace of the Frobenius. Then by the binomial theorem we have

$$\begin{aligned}(\alpha_p + \overline{\alpha}_p)^d &= \sum_{k=0}^{d} \binom{d}{k} \alpha_p^{d-k} \overline{\alpha_p}^k \\ &= \alpha_p^d + \overline{\alpha}_p^d + \sum_{k=1}^{d-1} \binom{d}{k} \alpha_p^{d-k} \overline{\alpha_p}^k.\end{aligned}$$

Note that as $\alpha_p \times \overline{\alpha_p} = p$, $\sum_{k=1}^{d-1} \binom{d}{k} \alpha_p^{d-k} \overline{\alpha_p}^k$ is divisible by p, so set it equal to pL. Also note that we know that L is an integer, as by the symmetry of the binomial theorem $\sum_{k=1}^{d-1} \binom{d}{k} \alpha_p^{d-k} \overline{\alpha_p}^k$ can be written so that each term is either, mp^s, or $np^t(\alpha_p^u + \overline{\alpha}_p^u)$, for integers m, n, s, t, u with s, t, and u positive. Then as $(\alpha_p^u + \overline{\alpha}_p^u) \in \mathbb{Z}$ for $u \in \mathbb{Z}^+$, we have that L must be an integer. So by putting pL in our equation for the numbers of points on the elliptic curve we get that $\#E(F_{p^d}) = p^d - pL + 1 - a_p^d$. As p must divide this, $a_p^d \equiv 1 \bmod p$.

■

We now investigate the number of primes p such that E has p-torsion over an extension of $\mathbb{Q}_p$ of degree d at most $p-1$ on average over all elliptic curves over $\mathbb{Q}$. Again, this average result is based on the fact that the condition

that E has a local torsion prime of degree d depends on the reduction of E over $\mathbb{Z}/p^2\mathbb{Z}$.

Definition 79 *Let* $\pi'_{E_{a,b}}(x) = \#\{p \leq x : p$ *is a local torsion prime of* $E_{a,b}$ *of degree* d*, for some* $d \leq p-1\}$.

Theorem 80 *Let* $A, B \geq x^{2+\epsilon}$ *for some* $\epsilon \geq 0$. *Then*

$$\frac{1}{4AB} \sum_{\substack{|a|\leq A \\ |b|\leq B}} \pi'_{E_{a,b}}(x) = \log\log x + O(1).$$

Proof. Let us first look at

$$\begin{aligned}
\sum_{\substack{|a|\leq A \\ |b|\leq B}} \pi'_{E_{a,b}}(x) &= \sum_{p\leq x} \#\{|a| \leq A, |b| \leq B : E_{a,b} \text{ has a local torsion prime} \\
&\quad \text{of degree } d, d \leq p-1\} \\
&= \sum_{p\leq x} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1)) \#\{E/\mathbb{Z}/p^2\mathbb{Z} : \\
&\quad \text{rank}_p E(W_2) = d+1, d \leq p-1\},
\end{aligned}$$

by Lemma 56. Once again let us separate our sum into two terms S_1 and S_2, let

$$\begin{aligned} S_1 &= \sum_{p\leq x}(\frac{2A}{p^2}+O(1))(\frac{2B}{p^2}+O(1))\#\{E/\mathbb{Z}/p^2\mathbb{Z}: \\ &\quad \text{rank}_p E_{a,b}(\mathbb{Z}/p^2\mathbb{Z}) = d+1, d\leq p-1\ ,\ j(E_{a,b})\neq 0,1728\} \end{aligned}$$

and let

$$\begin{aligned} S_2 &= \sum_{p\leq x}(\frac{2A}{p^2}+O(1))(\frac{2B}{p^2}+O(1))\#\{E/\mathbb{Z}/p^2\mathbb{Z}: \\ &\quad \text{rank}_p E_{a,b}(\mathbb{Z}/p^2\mathbb{Z}) = d+1, d\leq p-1\ ,\ j(E_{a,b})= 0,1728\}. \end{aligned}$$

By Proposition 73 we have that

$$\begin{aligned} S_1 &= \sum_{p\leq x}(\frac{2A}{p^2}+O(1))(\frac{2B}{p^2}+O(1))\#p\{E_{a,b}/\mathbb{F}_p: \\ &\quad E(k)[p]\neq 0 \text{ for some } k, j\neq 0,1728\} \end{aligned}$$

where k is an extension of $\mathbb{F}_p$ of degree less then $p-1$. Then as $E(k)[p]\neq 0$ if and only if $a_p(E)^d\equiv 1 \bmod p$, by Deuring's Theorem we have that

$$S_1 = \sum_{\substack{p \leq x \\ r^d \equiv 1(p) \\ d \leq p-1}} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1))pH(r^2 - 4p)\frac{(p-1)}{2} + ET$$

Note that Deuring's theorem does not mention elliptic curves with j-invariant 0 or 1728, so the error term, above comes from subtracting the curves with these j-invariants so that they do not get counted twice. Let us look at the above sum without the error term.

$$S_1' = \sum_{\substack{p \leq x \\ r^d \equiv 1(p) \\ d \leq p-1}} (\frac{2A}{p^2} + O(1))(\frac{2B}{p^2} + O(1))pH(r^2 - 4p)\frac{(p-1)}{2}$$

$$
\begin{aligned}
&= 4AB \sum_{\substack{p\le x \\ |r|\le 2\sqrt{p}}} \frac{1}{p^3} H(r^2-4p)\frac{(p-1)}{2} + O\left(2A \sum_{\substack{p\le x \\ |r|\le 2\sqrt{p}}} \frac{1}{p} H(r^2-4p)\frac{(p-1)}{2} \right. \\
&+ \left. 2B \sum_{\substack{p\le x \\ |r|\le 2\sqrt{p}}} \frac{1}{p} H(r^2-4p)\frac{(p-1)}{2} + \sum_{\substack{p\le x \\ |r|\le 2\sqrt{p}}} pH(r^2-4p)\frac{(p-1)}{2} \right) \\
&= 4AB \sum_{p\le x} \frac{1}{p^3} \sum_{|r|\le 2\sqrt{p}} H(r^2-4p)\frac{(p-1)}{2} \\
&+ O\left(2A \sum_{p\le x} \frac{1}{p} \sum_{|r|\le 2\sqrt{p}} H(r^2-4p)\frac{(p-1)}{2} \right. \\
&+ \left. 2B \sum_{p\le x} \frac{1}{p} \sum_{|r|\le 2\sqrt{p}} H(r^2-4p)\frac{(p-1)}{2} + \sum_{p\le x} p \sum_{|r|\le 2\sqrt{p}} H(r^2-4p)\frac{(p-1)}{2} \right)
\end{aligned}
$$

Now the inner sum in each of the above terms is the number of elliptic curves over $\mathbb{F}_p$ because of the condition on r. Since the number of elliptic curves over $\mathbb{F}_p$ is p^2-p (see for example [6]), applying this to the above sum gives

$$
= 4AB \sum_{p\le x} \frac{p^2-p}{p^3} + O\left(2(A+B) \sum_{p\le x} \frac{p^2-p}{p} + \sum_{p\le x} p(p^2-p) \right).
$$

Let us now consider averages. We have that

$$\frac{1}{4AB}\sum_{\substack{p\leq x\\ r^d\equiv 1(p)\\ d\leq p-1}}(\frac{2A}{p^2}+O(1))(\frac{2B}{p^2}+O(1))pH(r^2-4p)\frac{(p-1)}{2}$$

$$=\sum_{p\leq x}\frac{p^2-p}{p^3}+O\left(\frac{A+B}{2AB}\sum_{p\leq x}\frac{p^2-p}{p}+\frac{1}{4AB}\sum_{p\leq x}p(p^2-p)\right).$$

By our condition on A and B the last two terms converge. To see this let us look at each term individually, starting with the second term. We have that $\frac{A+B}{2AB}\sum_{p\leq x}\frac{p^2-p}{p}\ll\frac{x^2}{A}+\frac{x^2}{B}$ and $A,B\geq x^{2+\epsilon}$, so the second term converges. As for the third term we have that $\frac{1}{4AB}\sum_{p\leq x}p(p^2-p)\ll\frac{x^4}{AB}$, and as $AB\geq x^{4+\epsilon}$, so the third term converges. So let us consider the first term.

$$\begin{aligned}\sum_{p\leq x}\frac{p^2-p}{p^3} &= (\sum_{p\leq x}\frac{1}{p}+O(1))\\ &= \log\log x+O(1)\end{aligned}$$

We now look back at the error term of 5.3. We have that

$$ET=-\sum_{p\leq x}\frac{\#\{E/\mathbb{F}_p:j=0,1728\}}{p^4}p\ll-\sum_{p\leq x}\frac{p^2}{p^4},$$

which converges. Similarly looking at S_2, we can see that it will also converge. Thus $\frac{1}{4AB}\sum_{\substack{|a|\leq A\\ |b|\leq B}}\pi'_{E_{a,b}}(x)=\log\log x+O(1)$ which proves the theorem.

■

Bibliography

[1] D. Cox, *Primes of the Form $x^2 + ny^2$*, Fermat, Class field Theory and Complex Multiplication. Wiley-Interscience, New York, 1997.

[2] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, New York, 3rd Edition, 1967.

[3] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, International Mathematics Research Notices. **4** (1999), 165-183.

[4] C. David and T. Weston, *Local Torsion on Elliptic Curves and the Deformation Theory of Galois Representations*. Math. Res. Lett. **15** (2008), 599-611.

[5] F. Gouvea *p-adic Numbers*, An Introduction. Springer-Verlag, New York, 2nd Edition, 2000.

[6] H.W. Lenstra Jr. *Elliptic Curves and Number-Theoretic Algorithms*. 1985.

[7] H.W. Lenstra Jr. *Factoring Integers with Elliptic Curves.* Annals of Math. **126** (1987), 649-673.

[8] J. Neukirch *Algebraic Number Theory.* Springer-Verlag, New York, 1991.

[9] J.P. Serre, *Local Fields* Springer-Verlag, New York, 1979.

[10] J. Silverman, *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.