SERMON 2008:
Torsion Points on CM Elliptic Curves

James Stankewicz

University of Georgia

April 20, 2008

Introduction

Last fall, the UGA Number Theory VIGRE group (led by Drs. Pete Clark and Patrick Corn, including myself, Steve Lane, Alex Rice, Nathan Walters, Steve Winburn and Ben Wyser, with Brian Cook joining in the spring) met to study torsion in elliptic curves over $\mathbb{Q}$.

What we hoped to construct was a program which, given a positive integer d, would output all possible torsion subgroups of CM elliptic curves over a number field of degree d. At the end of the day though, it would be good enough to extend the known results about what groups can occur as torsion subgroups for CM elliptic curves.

Past Results

First, we know this will be a finite list due to the work of Loic Merel, who proved in 1996 that given a particular d, only finitely many groups can appear as torsion subgroups of elliptic curves over a number field of degree d.

As is, we know these finite lists for all elliptic curves over $\mathbb{Q}$(Mazur,1977) and quadratic extensions (Kamienny/Kenku/Momose,1990), and for the CM case we know the more specific answer for $\mathbb{Q}$(Olson,1974) and degree 2 and 3 extensions(Zimmer et. al 1989).

Notation

We let K, F, M denote number fields.

We let E denote an elliptic curve and $E(K)$ the group of K-rational points.

$E(K)[\mathrm{tors}]$ will denote the torsion subgroup of $E(K)$ and $E[N]$ the group of N-torsion points.

D_K will denote the discriminant of the maximal order of K, while D will denote the discriminant of any order.

We let $\mathcal{O}_K$ denote the maximal order of K while $\mathcal{O}(D)$ will denote the imaginary quadratic order of discriminant D. We further let $h(D)$ denote the class number of $\mathcal{O}(D)$.

The theory of Complex Multiplication gives us a bijection between the endomorphism ring of an elliptic curve E and the j-invariant of E. Thus we say that if E has endomorphism ring $\mathcal{O}(D)$, we call the j invariant of E j_D.

Why CM?

We restrict our attention to CM curves for computational reasons. Namely, although there are usually infinitely many elliptic curves with CM over a given number field, they partition into finitely many families parametrized by their j-invariant. We know there are finitely many CM j-invariants over a number field of degree d because we know $[\mathbb{Q}(j_D) : \mathbb{Q}] = h(D)$ and as Heilbronn proved in 1934,

$$\text{As } D \to -\infty, h(D) \to \infty.$$

For instance, the only CM j-invariants defined over $\mathbb{Q}$ are

$$0, 54000, -12288000, 1728, 287496, -3375,$$

$$16581375, 8000, -32768, -884736, -884736000,$$

$$-147197952000 \text{ and } -262537412640768000.$$

Kubert Normal Form

Consider an elliptic curve E with an N-torsion point for $N \geq 4$. Whether or not E has CM, there is a change of coordinates by which the elliptic curve can be put into *Kubert Normal Form*(or is it Tate Normal Form?):

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

with the N-torsion point moved to $(0,0)$.
Then the x and y coordinates of $[m](0,0)$ are rational functions in b and c for any integer m. For example,

$$[3](0,0) = (c, b-c)$$

$$[4](0,0) = (\frac{b^2 - bc}{c^2}, \frac{-b^3 + b^2c^2 + b^2c}{c^3})$$

How our algorithm works

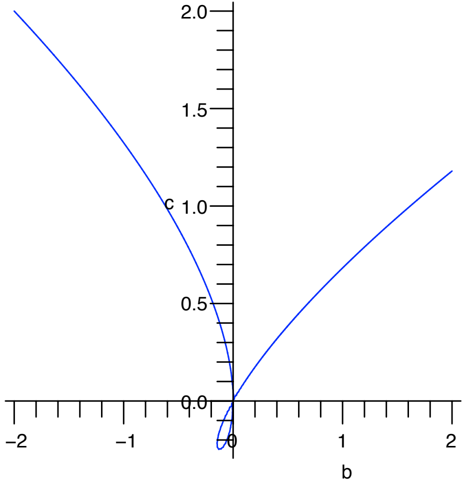
From here on, we restrict our attention to N prime, > 3 for simplicity. We know $(0,0)$ is an N-torsion point if and only if the x values of $\left[\frac{N+1}{2}\right](0,0)$ and $-\left[\frac{N-1}{2}\right](0,0)$ are equal. Then because these are all rational functions in b and c, we can turn this into a polynomial equation

$$f_N(b,c) = 0.$$

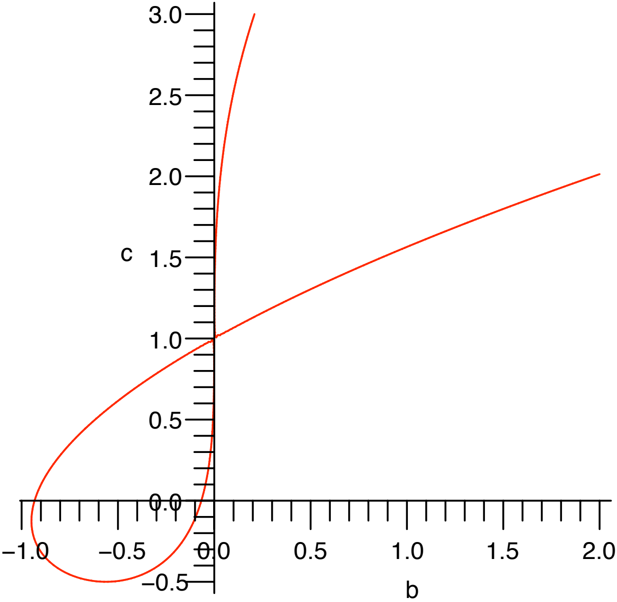
Moreover, the j-invariant of E is also a rational function in b and c, so setting the j-invariant equal to a constant of our choice is equivalent to setting a particular polynomial equation equal to zero.

An Example

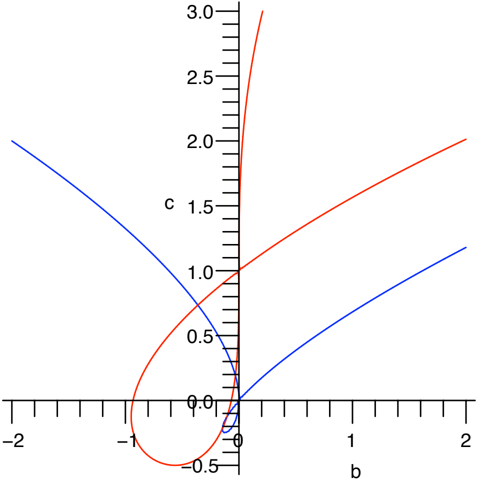
If we for instance take $N = 7$, we get $f_7(b, c) = b^2 - bc - c^3$



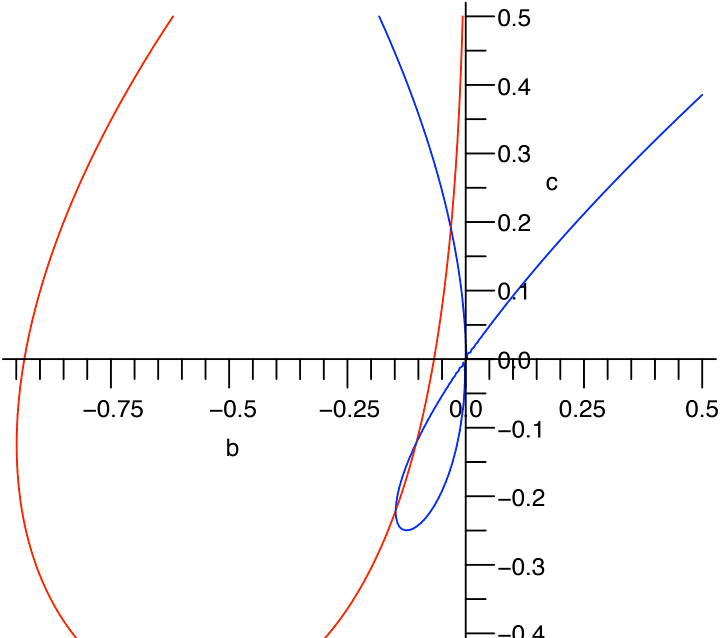
Now if consider $j = 0$, we get the picture:



So our elliptic curves with N-torsion points and prescribed j-invariants are exactly the points (b, c) which are common solutions to the N-polynomial and the j-polynomial.



An Even Closer Look



The b values of these points are then the solutions to the resultant of these two polynomials. The degree of the smallest irreducible factor of the resultant is then the least degree of an extension of $\mathbb{Q}(j)$ over which a CM Elliptic Curve is defined which has an N-torsion point.

To quickly determine how high a degree extension we need to take to find N torsion on an elliptic curve with j invariant j_D, we factor the resultant mod $\mathfrak{p}$ for all primes $\mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(j_D)}$ of small enough norm(it's quicker for a computer to factor in a finite field than otherwise).

We know how many N we need to consider by the *Silverberg-Prasad-Yogananda* bounds, which state that $\phi(e) \leq w(\mathcal{O})d$ where e is the exponent of $E(K)[\mathrm{tors}]$. Then when we suspect that we have a least degree extension we can factor the resultant over $\mathbb{Q}(j_D)$.

All this was coded in MAGMA, and we share some results:

Computational Results

N	$[K:\mathbb{Q}]$	D	N	$[K:\mathbb{Q}]$	D
5	2	-4	43	14	-3
7	2	-3	47	46	several
11	5	-11	53	26	-4
13	4	-3	59	58	several
17	8	-4	61	20	-3
19	6	-3	67	22	-3
23	22	several	71	70	several
29	14	-4	73	24	-3
31	10	-3	79	26	-3
37	12	-3			
41	20	-4			

Notes on the calculation

These calculations took about 10 days in MAGMA, including 30 hours on the $N = 79$ case alone. Notice that typically D is either -4 (corresponding to $\mathbb{Z}[i]$) or -3 (corresponding to $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$).

This is notable because those are the only 2 possible endomorphism rings where the unit group is anything more than ± 1. It's also notable that -4 pops up when $4|(N-1)$(least degree $(N-1)/2$) and -3 pops up when $3|(N-1)$(least degree $(N-1)/3$).

Using this computation as inspiration, we announce the following:

Theorem

Let N be an odd prime, E an elliptic curve defined over a number field F with CM endomorphism ring $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D})$.

1. *If* $\left(\frac{D_K}{N}\right) \neq -1$, $\frac{h(K)}{w(K)}(N-1) | [K:\mathbb{Q}]$.
2. *If* $\left(\frac{D_K}{N}\right) = -1$, $\frac{h(K)}{w(K)}(N^2-1) | [K:\mathbb{Q}]$.

Remark: If N does not divide the conductor of $\mathcal{O} \subset \mathcal{O}_K$, we can get an isogeny between E with $\mathcal{O}$-CM and E' with $\mathcal{O}_K$-CM and so we get the same result.

Compare this to the result we used:

Theorem (Silverberg,Prasad,Yogananda)

If E is an elliptic curve over a number field F with $\mathcal{O}$-CM and e the exponent of $E(F)[tors]$ then

$$\phi(e) \leq w(\mathcal{O})[F:\mathbb{Q}]$$

Moreover if $K = \mathbb{Q}(\sqrt{D})$ is the CM field of $\mathcal{O}(D)$ then

1. $K \subset F$ *implies* $\phi(e) \leq w(\mathcal{O})[F:\mathbb{Q}]/2$,
2. $K \not\subset F$ *implies* $\phi(\#E(f)[\mathrm{tors}]) \leq w(\mathcal{O})[F:\mathbb{Q}]$.

Notice that our bound recovers the first SPY bound in the case of odd prime torsion, and also implies that given our computational range we actually only have to check over the 13 rational j-invariants for the lowest degree because the least prime for which $\left(\frac{D}{N}\right) = -1$ for all 9 applicable discriminants is 3167.

It appears that we can even do a little better than the explicit class field theory result under special cases:

Theorem

If N is large enough with respect to D_K then

1. *If $\left(\frac{D_K}{N}\right) = 1$, the least degree extension over which there is a curve with an N-torsion point is $2\frac{h(\mathcal{O})}{w(\mathcal{O})}(N-1)$.*
2. *If $\left(\frac{D_K}{N}\right) = -1$, the least degree extension over which there is a curve with an N-torsion point is $\frac{h(\mathcal{O})}{w(\mathcal{O})}(N^2-1)$.*

The downside to this theorem(which comes from Serre's Open Image Theorem) is that we have no idea how large N has to be compared to D_0, although it is sharp in every applicable example we have.

Current Happenings

As of now, we are finishing up different areas of the work. I adapted some earlier code to compute some examples of torsion subgroups and the lists for degree ≤ 13(remember the lists are currently known for degree ≤ 3). For an example of high-order torsion, consider the elliptic curve in Kubert Normal Form with b defined by

$$x^8 - 6x^7 + 993x^6 + 3504x^5 + 4193x^4 + 1814x^3 + 347x^2 + 30x + 1$$

and c a certain 7th degree polynomial over b(omitted because the coefficients are huge) This has 34 torsion.