URA REPORT - CONDUCTORS OF ELLIPTIC CURVES OVER $\mathbb{Q}$

SEAN HOWE (ADVISED BY KIRTI JOSHI)

Abstract. We discuss the occurrence of numbers of the form pq for p, q prime as the conductors of elliptic curves.

Contents

1. Introduction

In this report we discuss some of the basics of the conductors of elliptic curves with an eye towards the study of which numbers of the form pq for p and q prime occur as the conductors of elliptic curves. In Section 2 we give a quick overview of some of the basic terminology of elliptic curves. In Section 3 we discuss the important reduction mod p map, paying special attention to the phenomenon of bad reduction and the role of the conductor in measuring this. In this section we also discuss the modularity theorem and mention the importance of the conductor in the relation given by the Hasse-Weil conjecture between elliptic curves and modular forms. In Section 4 we discuss some of the past work on elliptic curves of conductor p and pq for p, q prime. In Section 5 we present a naive approach to looking for patterns in the congruency classes of conductors of the form pq based on John Cremona's table of known elliptic curves of conductor <130000. We use this table to make and support a formal conjecture that no such simple pattern exists (the source code for the SAGE script used in this section appears in Section 7). In Section 6 we discuss the next steps to be taken in this project.

A special thanks to Kirti Joshi for advising this project and to the NSFG VIGRE program for funding it.

Date: 12/20/2009.

2. Elliptic Curves

An *elliptic curve* is a smooth, projective algebraic curve of genus one together with a distinguished point lying on the curve that we use to define a group law. Any elliptic curve E can be given as the zero set of a cubic equation and if it's possible to find such an equation with coefficients in the field K then we say that E is an elliptic curve defined over K and write E/K. If K is a field of characteristic not equal to 2 or 3 then, up to projective transformation, any elliptic curve over K can be given by an equation of the form

$$E: y^2 = x^3 + ax + b \tag{2.1}$$

with $a, b \in K$. This is called the Weierstrass form [S, ch. 3].

If E/K is an elliptic curve then the points on E with coordinates contained in an extension L/K form a group under the group law and we will denote this subgroup by $E(L)$ [S, ch. 3]. A question of fundamental importance in elliptic curves is, for an elliptic curve defined over a number field K, what is the group structure of $E(K)$? A seminal result, the Mordell-Weil theorem, states that this group is finitely generated [S, ch. 8]. For elliptic curves over $\mathbb{Q}$, work by Lutz, Nagell, and more recently Mazur, has firmly established the possible structure of the torsion subgroup of $E(\mathbb{Q})$ and provided methods for calculating this subgroup on specific curves [ST, ch. 2]. The question of the rank of $E(\mathbb{Q})$, however, remains relatively wide open, and more generally the question of the rank of $E(K)$ for any number field K. The latter is the subject of the Birch and Swinnerton Dyer conjecture, a Millenium Prize problem and one of the most important unsolved problems in number theory, which relates the rank of an elliptic curve to the order of the zero of its associated L-function at $s = 1$ [W].

Elliptic curves also find significant use in applied mathematics. They are used heavily in cryptography due to the presumed difficulty of the discrete log problem on an elliptic curve over a finite field, and in a related vein they are also used in factoring algorithms and primality tests [ST, ch. 4].

Here, we discuss the conductors of elliptic curves over $\mathbb{Q}$ with specific attention to conductors of the form $N = pq$ for p and q prime.

3. Conductors of Elliptic Curves

A common technique in the study of elliptic curves over $\mathbb{Q}$ is to consider them as curves over the p-adic numbers - if $E/\mathbb{Q}$ is an elliptic curve then we can consider the group $E(\mathbb{Q}_p)$. A natural map that arises in this context is the reduction mod p map: after a change of coordinates we can write an equation for E in Weierstrass form as in (2.1) with a, b integers, and after taking a "minimal" such equation, we can reduce the coefficients mod p to obtain a curve $\tilde{E}/\mathbb{F}_p$ (indeed, by considering a more general form of the elliptic curve equation we can find an equation that is minimal at all primes). Note that any point on $E(\mathbb{Q}_p)$ can be written uniquely as $[x : y : z]$ with each of x, y, and z contained in $\mathbb{Z}_p$ and at least one in the units group $\mathbb{Z}_p^\times$, and so reduction of the coordinates mod p makes sense and in fact provides a homomorphism from $E(\mathbb{Q}_p)$ to $\tilde{E}(\mathbb{F}_p)$. This restricts to a very useful homomorphism $E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p)$ - for instance, we can use it to determine the structure of the torsion subgroup as it can be shown that if we restrict to the m-torsion in $E(\mathbb{Q})$ then this reduction mod p map becomes an injection (note that this is contingent upon $\tilde{E}$ being nonsingular) [S, ch. 7].

An interesting question to ask is what happens when $\tilde{E}$ is a singular curve? This phenomenon is called *bad reduction*, and can occur in two ways: if $\tilde{E}$ has a cuspidal singularity then we call it additive reduction and if it has a nodal singularity we call it multiplicative reduction. An elliptic curve can only have bad reduction at finitely many primes, namely those that divide its discriminant (though it is not necessarily true that an elliptic curve given by a Weierstrass equation has bad reduction at every prime dividing its discriminant - it may be possible to make a rational change of variables to obtain a new Weierstrass equation whose discriminant is not divisible by that prime) [S, ch. 7]. To understand the group structure of $E(\mathbb{Q})$ it is important to understand at which primes it has bad reduction - for instance, the terms used in defining the curve's L-function, which as mentioned earlier is connected to the rank of $E(\mathbb{Q})$, differ between primes where bad reduction occurs and primes where it does not [W].

The information about the reduction of an elliptic curve is encoded in an invariant called the conductor. If an elliptic curve has good reduction at p then p does not divide N and if it has multiplicative reduction at p then p divides N exactly once. For $p \geq 5$ if the curve has additive reduction at p then p divides N exactly twice [EGT]. For $p = 2, 3$ if the curve has additive reduction at p then $\mathrm{ord}_p N \geq 2$.

The famous Taniyama-Shimura-Weil conjecture, now the Modularity Theorem, and the closely related Hasse-Weil conjecture connect elliptic curves with modular forms and the conductor plays an important role in this connection. More specifically, to any elliptic curve over $\mathbb{Q}$ of conductor N there is an associated cusp form of weight two and level N obtained by using the coefficients of its L-series in a fourier series. Before this conjecture was proved one reason that the conductors of elliptic curves were studied was to provide evidence for this conjecture: if you could produce a list of elliptic curves of certain conductors then it could be matched against a list of elliptic curves parameterized by modular functions. To this end and following the work of Ogg [O], Setzer provides some theorems on the existence and non-existence of elliptic curves of prime conductor [Se] and Hadano provides similar theorems for elliptic curves of conductor $2^a p^b$ [H]. We discuss their work in the following section.

4. Literature Review

A theorem typical of the papers by Ogg, Setzer, and Hadano is the following:

Theorem 4.1 ([H, Thm. 1])**.** *If none of the class numbers of the four quadratic fields $\mathbb{Q}(\sqrt{\pm p})$, $\mathbb{Q}(\sqrt{\pm 2p})$ for a prime $p \equiv 3$ or 5 mod 8 is divisible by 3 then there are no elliptic curves of conductor $N = 2p$.*

The method of proof is generally as follows:

(1) Suppose we have such a curve and consider its 2-division field K (the smallest extension of $\mathbb{Q}$ over which all 2-torsion points are defined). If the curve is given by the equation $y^2 = f(x)$ then K is just the splitting field of f. By studying the ramification of primes in K and its subfields, we find that there must be a 2-torsion point defined over $\mathbb{Q}$.
(2) Use the existence of a rational 2-torsion point to produce an integer solution to a Diophantine equation.
(3) Show that this Diophantine equation can have no such solution.

Of course, there are many ways in which this can vary. For instance, Setzer proves the following:

Theorem 4.2 ([Se, Thm. 2]). *Let p be a prime, $p \neq 2, 3, 17$. There is an elliptic curve of conductor p over $\mathbb{Q}$ if and only if $p = u^2 + 64$ for some rational integer u. If p is of the form $u^2 + 64$, there are, up to isomorphism, just two such curves.*

To prove this theorem Setzer uses some of the methods above but then uses the solution of a Diophantine equation to produce an elliptic curve with the desired property.

There is an even more direct way to connect integer solutions of Diophantine equations to the conductors of elliptic curves. Indeed, as mentioned earlier the discriminant of a curve is tightly connected to the conductor and whether there is an elliptic curve over $\mathbb{Q}$ with a given discriminant is determined by whether there is a rational point on another elliptic curve whose equation is simply the formula for the discriminant in terms of the coefficients. Because we can make a rational change of coordinates to reduce the power of a prime dividing the discriminant by multiples of 12, there are only finitely many discriminants we need to examine to exhaust all possible discriminants for a given conductor. This is the approach taken by Edixhoven, *et al.* in [EGT].

5. A Naive Approach

John Cremona has put together a table of known elliptic curves of conductors $N < 130000$. One might hope that there would be a simple congruence pattern in this data for either the conductors for which there are elliptic curves or for the conductors for which there are no elliptic curves. In particularly, we have written a SAGE script to search for a pattern in conductors of the form pq for p and q distinct primes. Based on an examination of the tables using a computer program, we conjecture that there is no such pattern in either case. We make formal statements in Conjectures 5.1 and 5.2 and provide evidence for them produced by this script. The source code of the script is available in Section 7.

Conjecture 5.1. *Let p be a prime. Then for any n coprime to p and any a coprime to n there exists a prime q such that $pq \equiv a \bmod n$ and such that there are no elliptic curves of conductor pq*

Evidence below is based on Cremona's table of elliptic curves of conductor $N < 130000$. For each prime $1 < p < 50$ we find the first n such this conjecture fails within Cremona's data, i.e. the first n coprime to p such that there is some congruence class mod n with no representative in the list of possible conductors less than 130000 not correspoding to known elliptic curves.

p	Number of $N = pq < 130000$ with no known elliptic curve of conductor N	First failure (fails mod n)
2	3392	491
3	2629	457
5	1703	257
7	1373	239
11	802	127

p	Number of $N = pq < 130000$ with no known elliptic curve of conductor N	First failure (fails mod n)
13	831	149
17	616	139
19	551	101
23	527	109
29	400	107
31	424	101
37	265	67
41	311	73
43	266	71
47	279	97

Conjecture 5.2. *Let p be a prime. Then for any n coprime to p and any a coprime to n there exists a prime q such that $pq \equiv a \bmod n$ and such that there is an elliptic curves of conductor pq.*

p	Number of $N = pq < 130000$ with a known elliptic curve of conductor N	First failure (fails mod n)
2	3101	463
3	1893	299
5	1157	163
7	752	109
11	614	109
13	398	83
17	354	83
19	330	89
23	216	61
29	208	53
31	150	37
37	225	59
41	138	43
43	167	49
47	123	29

6. Future Work

There are several avenues down which I would like to continue. The techniques of Ogg, Setzer, and Hadano, should work for more specific primes of the form pq, for instance, $3q$. Hadano [H] covers $2q$ and suggests several other cases that would yield easily to the same methods. I plan to try to work these out on my own as well as check through the literature to see if I can find anything more building on these techniques. Because of advances in computing power since this paper was written, these same techniques may be usable to prove theorems that, along side calculated data, will yield more existence and non-existence results for larger p and q (in particular, class number calculations will be more reasonable to do in bulk). The techniques of [EGT] also merit further investigation, though they seem at first

glance much less generally applicable. A more thorough search in more recent literature is also warranted.

The analysis of Cremona's tables for a pattern should be redone, this time also considering class number as in the theorems of Ogg, Setzer, and Hadano.

Finally, I plan to learn more about modular forms in order to understand how the Hasse-Weil conjecture can be used in this problem, specifically in regard to raising level as in [R].

7. Source Code

Below we present the source code for searching for patterns in the gaps in Cremona's table as discussed in Section 5. As the code for searching for patterns in the conductors that appear is very similar, we do not include it here.

```
C=CremonaDatabase()
maxconductor=C.conductor_range()[1];
conductors=[];
for p in prime_range(1,maxconductor):
    for q in prime_range(p,maxconductor/p):
        n=p*q;
        if (len(C.list((n,n)))==0):
            conductors.append((n,p,q));
def withpfactor(p,L):
    M=[];
    for a in L:
        if a[1]==p:
            M.append(a);
        elif a[2]==p:
            M.append((a[0],a[2],a[1]));
    return M;
def checkcongclasses(n, L):
    foundclasses=[];
    for a in L:
        if mod(a[0],n) not in foundclasses:
            foundclasses.append(mod(a[0],n));
    return foundclasses;
for n in range(1,250):
    if gcd (n,p)==1:
        CC=checkcongclasses(n,S);
        num_cc_coprime=0;
        for a in CC:
            if gcd(a,n)==1:
                num_cc_coprime=num_cc_coprime+1;
        if num_cc_coprime!=euler_phi(n):
            print "!", n, num_cc_coprime, euler_phi(n);
```

References

[EGT] Bas Edixhoven, Arnold de Groot, and Jaap Top. Elliptic curves over the rationals with bad reduction at only one prime. *Mathematics of Computation*, vol. 54, no. 189, January 1990.

[H] Toshihiro Hadano. On the conductor of an elliptic curve with a rational point of order 2. *Nagoya Math. J.* Vol. 53 (1974), 199-210.

[O] A. P. Ogg. Abelian curves of small conductors. *J. reine. agnew. Math.*, 226 (1967), 206-215.

[R] Kenneth A. Ribet. Raising the levels of modular representations. Séminaire de Théorie des Nombres, Paris 1987-88, 259-271, *Progr. Math.*, 81, Birkhäuser Boston, Boston, MA, 1990.

[Se] Bennett Setzer. Elliptic curves of prime conductor. *J. London Math Soc.* (2), 10 (1975), 367-378.

[S] Joseph H. Silverman. *The arithmetic of elliptic curves.* Graduate Texts in Math., vol. 106, Springer-Verlag, 1986.

[ST] Joseph H. Silverman and John Tate. *Rational points on elliptic curves.* Springer-Verlag, 1992.

[W] Birch and Swinnerton Dyer Conjecture. *Wikipedia.* Accesed 9/11/2009, available at http://en.wikipedia.org/wiki/Birch_and_Swinnerton-Dyer_conjecture.