Interesting Families of Elliptic Curves

Steven Miller*

February 28, 2002

Abstract

We list several interesting one-parameter families over $\mathbf{Q}(t)$, provide a sketch on calculating the number of t such that an integral polynomial is square-free, and go through the steps of applying Tate's Algorithm (as given in Cremona) to calculate the conductors. There is much material in this handout that is not needed; I've cut and pasted from several documents, and this is to ensure that any time I quote a theorem, it will be referenced properly. If you only care for the list of interesting families, just read section one. If you want to know how we prove that it isn't restrictive to sieve to square-free (ie, a positive percent of curves in the family are square-free), read section two. If you want to see the calculations to determine the conductors, read section three. If you don't have Tate's algorithm, I'll make copies.

Part I
Interesting Families

1 Families of Constant Sign

1.1 Complex Multiplication Examples, Rank 0 over $\mathbf{Q}(t)$

We give two families with constant $j(t)$ and constant sign in the functional equation.

$$E_t : y^2 = x^3 + 2^4 \cdot (-3)^3 \cdot (9t+1)^2 \tag{1.1}$$

*E-mail: sjmiller@math.princeton.edu

For $9t+1$ square-free, all curves are even, and the conductors are $N_t = 3^3(9t+1)^2$.

$$E_t : y^2 = x^3 \pm 4(4t+2)x \tag{1.2}$$

For $4t+2$ square-free, the conductors are $N_t = 2^6(4t+2)^2$. For $4t+2$ square-free and a positive sign, the curves are odd; for $4t+2$ square-free and a negative sign, the curves are even.

1.2 Washington's Family, Rank 1 over $\mathbf{Q}(t)$

Consider the family

$$E_t : y^2 = x^3 + tx^2 - (t+3)x + 1, \quad j(t) = 256(t^2+3t+9), \tag{1.3}$$

for every $t \in \mathbf{Z}$, E_t has odd functional equation. This example is due to Washington. Note we do not need to sieve to a polynomial being square-free to observe constancy in sign.

For convenience, we send t to $6t$, and consider the family

$$E_t : y^2 = x^3 + (6t+1)x^2 - (6t+4)x + 1. \tag{1.4}$$

The discriminant is $\Delta(t) = 2^4(144t^2+60t+13)^2$. For $144t^2+60t+13$ square-free, the conductors are $N_t = 2^3(144t^2+60t+13)^2$. (Changing to $6t$ makes it significantly easier to calculate the conductors).

2 Families of Rank 0 over $\mathbf{Q}(t)$

2.1 $y^2 = x^3 + (t+1)x^2 + tx$

$$E_t : y^2 = x^3 + (t+1)x^2 + tx. \tag{2.5}$$

For $t(t-1)$ square-free, the conductors are $N_t = 2^4t(t-1)$.

2.2 $y^2 = x^3 + 5x^2 + 16(30t+1)x$

Consider the family

$$E_t : y^2 = x^3 + 5x^2 + 16(30t+1)x. \tag{2.6}$$

The discriminant is

$$\Delta(t) = 2^{12}\Big(30t+1\Big)^2\Big(25 - 64(30t+1)\Big) = 2^{12}\Delta_1^2(t)\Delta_2(t). \tag{2.7}$$

For $\Delta_1(t)\cdot\Delta_2(t)$ square-free, the conductors are $N_t = \Big(30t+1\Big)\Big(64(30t+1) - 25\Big)$.

Note this family is very similar to one from Fermigier's list: $E_t : y^2 = x^3 + 5x^2 + 16tx$; we sent t to $30t+1$ to ease the determination of the conductors.

3 Families of Rank 1 over $\mathbf{Q}(t)$

3.1 $y^2 = x^3 + x^2 + 12t + 1$

Consider the family

$$E_t : y^2 = x^3 + x^2 + 12t + 1,\ \Delta(t) = -2^4(12t+1)(324t+31). \tag{3.8}$$

For $(12t+1)(324t+31)$ square-free, the conductors are $N_t = 2^3(12t+1)(324t+31)$. This is a modification of the family $y^2 = x^3 + x^2 + t$, where we replaced t with $12t+1$ to simplify some of the calculations for the conductors.

4 $y^2 = x^3 + (6t+1)x^2 + 1$

Consider the family

$$E_t : y^2 = x^3 + (6t+1)x^2 + 1,\ \Delta(t) = -2^4\Big(4(6t+1)^3 + 27\Big). \tag{4.9}$$

For $\Big(4(6t+1)^3 + 27\Big)$ square-free, the conductors are $N_t = 2^2\Big(4(6t+1)^3 + 27\Big)$. This is a modification of the family $y^2 = x^3 + tx^2 + 1$, where we replaced t with $6t+1$ to simplify the calculations for the conductors.

5 Families of Rank 2 over $\mathbf{Q}(t)$

5.1 $y^2 = x^3 - (6t+1)^2 x + (6t+1)^2$

Consider the family

$$E_t : y^2 = x^3 - (6t+1)^2 x + (6t+1)^2. \tag{5.10}$$

The discriminant is

$$\Delta(t) = 2^4 \Big(6t+1\Big)^4 \Big(4(6t+1)^2 - 27\Big) = 2^4 \Delta_1^4(t)\Delta_2(t). \tag{5.11}$$

For $D_1(t)D_2(t)$ square-free, the conductors are $N_t = 2^2\Big(6t+1\Big)^2\Big(4(6t+1)^2 - 27\Big)$. This is a modification of the family $y^2 = x^3 - t^2x + t^2$, where we replaced t with $6t+1$ to simplify the calculations for the conductors.

5.2 $y^2 = x^3 - (6t+1)^2 x + (6t+1)^4$

Consider the family

$$E_t : y^2 = x^3 - (6t+1)^2 x + (6t+1)^4. \tag{5.12}$$

The discriminant is

$$\Delta(t) = -2^4 \Big(6t+1\Big)^6 \Big(27(6t+1)^2 - 4\Big) = -2^4 \Delta_1^6(t)\Delta_2(t). \tag{5.13}$$

For $D_1(t)D_2(t)$ square-free, the conductors are $N_t = 2^2\Big(6t+1\Big)^2\Big(27(6t+1)^2 - 4\Big)$. This is a modification of the family $y^2 = x^3 - t^2x + t^4$, where we replaced t with $6t+1$ to simplify the calculations for the conductors.

Part II

Cardinalities of Sieved Families

We show, for all the families we've considered, a positive percent of $t \in [N, 2N]$ give $D(t)$ square-free, where $D(t)$ is related to $\Delta(t)$.

6 Sieving Linear Polynomials

Consider the families $\mathcal{F}_1 : y^2 = x^3 + 2^4(-3)^3(9t+1)^2$ and $\mathcal{F}_2 : y^2 = x^3 \pm 4(4t+2)x$. We develop enough of the theory for linear polynomials to handle the two cases of interest.

For $\mathcal{F}_1$, $\Delta(t) = -2^{12} \cdot 3^9(9t+1)^4$. If $D(t) = 9t+1$ is square-free, $N_t = 3^3(9t+1)^2$ by Theorem 10.4.

For $\mathcal{F}_2$, $\Delta(t) = \mp 2^{12}(4t+2)^3$. If $D(t) = 4t+2$ is square-free, $N_t = 2^6(4t+2)^2$ by Theorem 11.1.

These families are very similar. In the first case, we need to sieve to $9t+1$ square-free; in the second, to $4t+2$ square-free. We do both simultaneously by sieving $D(t) = \beta t + \gamma$.

6.1 Number of Square-Free Numbers

In the special case $\beta = 1$, $\gamma = 0$, standard inclusion / exclusion arguments yields the number of square-free numbers:

$$\begin{aligned}
N_0 &= \sum_{d=1}^{\sqrt{2N}} \mu(d)\left(\frac{N}{d^2} + O(1)\right) \\
&= N \sum_{d=1}^{\sqrt{2N}} \frac{\mu(d)}{d^2} + O(\sqrt{N}) \\
&= N \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(\sqrt{N}) \\
&= N \prod_p \left(1 - \frac{1}{p^2}\right) + O(\sqrt{N}) \\
&= \frac{N}{\zeta(2)} + O(\sqrt{N}). \qquad (6.14)
\end{aligned}$$

As $\frac{1}{\zeta(2)} \approx .607927 > 0$, we see a positive percent of numbers in $[N, 2N]$ are square-free.

6.2 Special Case of Linear Polynomials

We want $D(t) = \beta t + \gamma$ to be square-free. For our two choices of β and γ, (β, γ) is square-free. Assume $d^2 | D(t)$. Clearly $d^2 \dagger \beta$, because if $d^2 | \beta$ and $d^2 | D(t)$, then $d^2 | D(t) - \beta t = \gamma$, which contradicts (β, γ) is square-free. Hence if $d^2 | \beta t + \gamma$ then $d^2 \dagger \beta\gamma$. We study two cases: $D(t) = 9t + 1$ and $D(t) = 4t + 2$. In the first case, the only restriction is $3 \dagger d$. In the second case, $2 \dagger d$. Let $\mathcal{P}$ represent the set of primes to be excluded, and let $\mathcal{D}$ denote the set of d's to be excluded.

We use inclusion / exclusion. We first consider all $t \in [N, 2N]$. We then subtract off $\frac{N}{d^2}$ where d is a prime not in $\mathcal{P}$. We then add back $\frac{N}{d^2}$ where d is the product of two primes not in $\mathcal{P}$. Continuing yields

$$\begin{aligned} N_{\mathcal{F}} &= \sum_{\substack{d=1 \\ d \notin \mathcal{D}}}^{\sqrt{2N}} \mu(d) \left(\frac{N}{d^2} + O(1) \right) \\ &= N \sum_{\substack{d=1 \\ d \notin \mathcal{D}}}^{\infty} \frac{\mu(d)}{d^2} + O(\sqrt{N}) \\ &= N \prod_{p \notin \mathcal{P}} \left(1 - \frac{1}{p^2}\right) + O(\sqrt{N}) \\ &= \frac{N}{\zeta(2)} \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^2}\right)^{-1} + O(\sqrt{N}). \end{aligned} \tag{6.15}$$

In the first case, $\mathcal{P} = \{3\}$, and $N_{\mathcal{F}} = \frac{9}{8} N_0$. In the second case, $\mathcal{P} = \{2\}$, and $N_{\mathcal{F}} = \frac{4}{3} N_0$.

Theorem 6.1 (Cardinality of $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$) *For the family $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ square-free, $N_{\mathcal{F}} = \frac{9}{8\zeta(2)} N + O(\sqrt{N})$.*

Theorem 6.2 (Cardinality $y^2 = x^3 \pm 4(4t+2)x$) *For the family $y^2 = x^3 \pm 4(4t+2)x$, $4t+2$ square-free, $N_{\mathcal{F}} = \frac{4}{3\zeta(2)} N + O(\sqrt{N})$.*

7 Sieving Quadratics Polynomials

7.1 Preliminaries

We calculate the cardinality of t such that $D(t) = D_1(t) D_2(t)$ is square-free, assuming $D_i(t) = \beta_i t + \gamma_i$, $(\beta_i, \gamma_i) = 1$, and $\forall t$, $\big(D_1(t), D_2(t)\big) = 1$.

For square-free d, let $\nu(d)$ denote the number of incongruent solutions of $D(t) \equiv 0 \bmod d^2$. If $d^2|D(t)$, since $D_1(t)$ and $D_2(t)$ are relatively prime, $\exists d_1$, d_2, $(d_1,d_2)=1$ and $d_1d_2=d$, such that $d_i^2|D_i(t)$.

If $(d_i,\beta_i)=1$, there is one incongruent solution to $D_i(t) \equiv 0 \bmod d_i^2$, as β_i is invertible mod d_i^2. Assume $p|(d_i,\beta_i)$. If $d_i^2|D_i(t)$, then $p|D_i(t)$. As $p|\beta_i$, this forces $p|\gamma_i$, which contradicts our assumption that $(\beta_i,\gamma_i)=1$.

To each relatively prime pair (d_1,d_2) with $d_1d_2=d$, let $\nu(d_1,d)$ be the number of incongruent solutions to $d_i^2|D_i(t)$ (d_1 and d determine d_2).

Lemma 7.1 *With the above assumptions, for square-free d,*

$$\nu(d) = \sum_{d_1|d} \nu(d_1,d). \tag{7.16}$$

We prove the above does not double count a root of $D(t) \equiv 0 \bmod d^2$. Assume two distinct pairs (d_1,d_2) and (d_1',d_2') yield the same root t. We may assume $\exists p|d_1$ such that $p \dagger d_1'$; hence $p|d_2'$ as $d_1d_2 = d_1'd_2'$.

As $p|d_1$, $p|D_1(t)$; as $p|d_2'$, $p|D_2(t)$, which contradicts $D_1(t)$ and $D_2(t)$ are relatively prime. $\Box$.

Corollary 7.2 *With the above assumptions, for square-free d, if $(d,\beta_1\beta_2) = 1$, $\nu(d) = \tau(d)$.*

7.2 Special Case: $p|\beta_1$ iff $p|\beta_2$

Theorem 7.3 (Cardinality for Special Reducible Quadratic) *Let $D(t) = D_1(t)D_2(t)$, $D_i(t) = \beta_i t + \gamma_i$, $(\beta_i,\gamma_i)=1$. Assume $\forall t$, $\Big(D_1(t),D_2(t)\Big)=1$ and β_1 and β_2 are divisible by the same primes. Let β be the product of primes dividing the β_i's. In the limit,*

$$\prod_{p \dagger \beta}\left(1 - \frac{\tau(p)}{p^2}\right) = \prod_{p\dagger\beta}\left(1-\frac{2}{p^2}\right)$$

t give $D(t)$ square-free.

Proof: By inclusion / exclusion, in the limit we have

$$\prod_p \left(1 - \frac{\nu(p)}{p^2}\right). \tag{7.17}$$

If $p|\beta$, then $p|\beta_i$ and $p\dagger\gamma_i$. Thus, $\nu(p)=0$ for $p|\beta$. For $p\dagger\beta$, by Corollary 7.2 $\nu(p)=\tau(p)=2$.

7.3 $y^2 = x^3 + (t+1)x^2 + tx$

$\Delta(t) = 16\Big(t\cdot(t-1)\Big)^2$. For $D(t) = t(t-1)$ square-free, $N_t = 2^4 t(t-1)$ by Theorem 12.1.

At least 10% of $t \in [N, 2N]$ have $t(t-1)$ square-free. This follows immediately from the fact that over 60% of all numbers in this interval (for large N) are square-free, so there must be significant overlap. See Equation 6.14.

For this family, $D_1(t) = t$, $D_2(t) = t-1$. Clearly $D_1(t)$ and $D_2(t)$ are relatively prime, $(\beta_i, \gamma_i) = 1$, and $\beta = \prod_{p|(\beta_1,\beta_2)} p = 1$. Hence Theorem 7.3 is applicable, and we obtain

Theorem 7.4 **($N_{\mathcal{F}}$ for $y^2 = x^3 + (t+1)x^2 + tx$)** *In the limit as $N \to \infty$, the number of t giving $D(t)$ square-free is approximately*

$$N_{\mathcal{F}} = \prod_p \left(1 - \frac{2}{p^2}\right) N. \tag{7.18}$$

7.4 $y^2 = x^3 + x^2 + 12t + 1$

$\Delta(t) = -16(2t+1)(54t+31)$. For $D(t) = (2t+1)(54t+31)$ square-free, $N_t = 2^4(2t+1)(54t+31)$ if t is odd and $2^3(2t+1)(54t+31)$ if t is even. By breaking into two families ($t = 2u$ and $t = 2u+1$), we will be able to perform the necessary sieving by arithmetic progressions, as the conductors for square-free $D(t)$ will be monotonic polynomials.

There are, however, complications if we try to apply Theorem 7.3: $\beta_1 = 2$, $\beta_2 = 2\cdot 3^3$. Thus, β_1 and β_2 do not have the same prime factors.

To simplify the calculations, replace t with $6t$. Now $\Delta(t) = -16(12t+1)(324t+31)$, and all the conditions of Theorem 7.3 are met:

Theorem 7.5 **($N_{\mathcal{F}}$ for $y^2 = x^3 + x^2 + 12t + 1$)** *In the limit as $N \to \infty$, the number of t giving $D(t)$ square-free is approximately*

$$N_{\mathcal{F}} = \prod_{p\neq 2,3} \left(1 - \frac{2}{p^2}\right) N. \tag{7.19}$$

7.5 $y^2 = x^3 + (12t+1)x^2 - (12t+4)x + 1$

$\Delta(t) = 2^4(144t^2 + 60t + 13)$, and for square-free $D(t) = 144t^2 + 60t + 13$, by Theorem 15.1, $N_t = 2^3(144t^2 + 60t + 13)^2$. As our quadratic is not reducible, we need to slightly modify the previous argument.

The discriminant of $D(t)$ is $\delta = -2^4 \cdot 3^5$. $D(t)$ is a primitive integral polynomial. For $p \dagger 6$, we may use Nagell, Theorem 52: the number of incongruent solutions of $D(t) \equiv 0 \bmod p^2$ equals the number of incongruent solutions of $D(t) \equiv 0 \bmod p$.

If δ is a non-zero square mod p, $D(t) \equiv 0 \bmod p$ has two incongruent solutions, if $\delta \equiv 0 \bmod p$ there is one solution, and if δ is not a square mod p there are no solutions.

As $\delta = -3 \cdot 6^4$ and $p \dagger 6$, the number of incongruent solutions to $D(t) \equiv 0 \bmod p$ is $1 + (\frac{-3}{p})$. By Quadratic Reciprocity, $(\frac{-3}{p}) = 1$ if $p \equiv 1 \bmod 3$ and -1 if $p \equiv 2 \bmod 3$.

Let $\nu(p)$ be the number of incongruent roots of $D(t) \equiv 0 \bmod p^2$. Then $\nu(p) = 0$ for $p = 2$, 3, or $p \equiv 2 \bmod 3$, and $\nu(p) = 2$ for $p \equiv 1 \bmod 3$.

As before, by inclusion / exclusion we find

Theorem 7.6 ($N_{\mathcal{F}}$ for $y^2 = x^3 + (12t+1)x^2 - (12t+4)x + 1$) *In the limit as $N \to \infty$, the number of t giving $D(t)$ square-free is approximately*

$$N_{\mathcal{F}} = \prod_{p \equiv 1(3)} \left(1 - \frac{2}{p^2}\right) N. \tag{7.20}$$

8 Sieving Cubic Polynomials

8.1 $y^2 = x^3 + (6t+1)x^2 + 1$

$\Delta(t) = -2^4\Big(4(6t+1)^3+27\Big) = -2^4 D(t)$. For $D(t)$ square-free, the conductor is $N_t = 2^3\Big(4(6t+1)^3 + 27\Big)$ by Theorem 16.1. Thus, the conductor is monotone in t, and given by an integral polynomial.

From Hooley ([Ho], Theorem 3, page 69), a positive percent of $t \in [N, 2N]$ yield $D(t)$ square-free. We may calculate $N_{\mathcal{F}}$ exactly by taking $S(t) = 1$.

$$\begin{aligned} N_{\mathcal{F}} &= \sum_{\substack{t=N \\ \Box \dagger D(t)}}^{2N} 1 \\ &= \sum_{d=1}^{10N^{3/2}} \sum_{\substack{t=N \\ t \in E(d)}}^{2N} \mu(d) \end{aligned}$$

$$= \sum_{d=1}^{10N^{3/2}} \mu(d) \sum_{i=1}^{\nu(d)} \sum_{\substack{t'=0 \\ t_i(d)+t'd^2 \leq 2N}}^{\frac{N}{d^2}} 1. \tag{8.21}$$

As the terms in the d-sum decay like $\frac{d^\epsilon}{d^2}$, we can obtain a good bound on the error, and brute force will show we do have a positive percentage. In fact, we can bound the cardinality of the family from below:

$$N_{\mathcal{F}} \geq N\left(1 - 1\sum_{d\geq 5} \mu^2(6d)\frac{1-\mu(6d)}{2}\frac{\tau^{\frac{\log 3}{\log 2}}(d)}{d^2}\right). \tag{8.22}$$

Let $h(N)$ be the subtracted sum above. Direct computation gives $h(10^4) = .27466$, $h(10^5) = .27481$, $h(10^6) = .274831$, $h(10^7) = .274834$.

Theorem 8.1 *For $y^2 = x^3 + (6t+1)x^2 + 1$, a positive percent of t have $4(6t+1)^3 + 27$ square-free.*

8.2 $y^2 = x^3 - (6t+1)^2 x + (6t+1)^m$, $m = 2$ or 4

We handle these families as we did $y^2 = x^3 + (6t+1)x^2 + 1$. Let $\mathcal{F}_2$ denote the family from $m = 2$ and $\mathcal{F}_4$ the family from $m = 4$.

$$\begin{aligned} \Delta(t) &= 2^4\Big(6t+1\Big)^{2+m}\Big(\alpha_m(6t+1)^2 - \beta_m\Big) \\ D_m(t) &= \Big(6t+1\Big)\Big(\alpha_m(6t+1)^2 - \beta_m\Big) \end{aligned} \tag{8.23}$$

where $(\alpha_2, \beta_2) = (4, 27)$ and $(\alpha_4, \beta_4) = (27, 4)$. Let $D(t) = D_m(t)$. Sieving to $D(t)$ square-free yields, by Theorems 17.1 and 18.1

$$N_t = 2^2\Big(6t+1\Big)^2\Big(a_m(6t+1)^2 - b_m\Big). \tag{8.24}$$

Thus, for square-free $D(t)$, the conductors are monotone increasing, and given by an integral polynomial. As our cubic in t is reducible, we cannot quote Hooley's result ([Ho], Theorem 3, page 69) to immediately obtain $N_{\mathcal{F}} = c_{\mathcal{F}} N$; however, the estimates from the family $y^2 = x^3 + (6t+1)x^2 + 1$ (Equation 8.22) are applicable, and we find there are a positive percent of $t \in [N, 2N]$ yielding square-free $\Delta_m(t)$.

Theorem 8.2 *For $y^2 = x^3 - (6t+1)^2 x + (6t+1)^m$, $m = 2$ or 4, a positive percent of t have $D_m(t)$ square-free.*

Part III

Calculating Conductors for Various One-Parameter Families

9 Introduction

We calculate the conductors N_t for many families of elliptic curves. $N_t = \prod_{p|\Delta} p^{f_p}$. The difficult computations will be for $p = 2, 3$. We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr], pages $49 - 52$.

We let $T(r, s, t, u)$ denote the standard change of variables $x = u^2x' + r$, $y = u^2y + su^2x + t$. Hence

$$\begin{aligned}
ua_1' &= a_1 + 2s \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\
u^3a_3' &= a_3 + ra_1 + 2t \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \\
u^{12}\Delta' &= \Delta
\end{aligned} \tag{9.1}$$

Note that $T(r, s, t, 1)$ does not change Δ, and $T(0, 0, 0, 1)$ is the identity transformation. We record the relation between the a_i's and the b_i's and the c_i's:

$$\begin{aligned}
b_2 &= a_1^2 + 2^2a_2 \\
b_4 &= a_1a_3 + 2a_4 \\
b_6 &= a_3^2 + 2^2a_6 \\
b_8 &= a_1^2a_6 - a_1a_3a_4 + 2^2a_2a_6 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 2^3 \cdot 3b_4 \\
c_6 &= -b_2^3 + 2^2 \cdot 3^2b_2b_4 - 2^3 \cdot 3^3b_6 \\
\Delta &= -b_2^2b_8 - 2^3b_4^3 - 3^3b_6^2 + 3^2b_2b_4b_6.
\end{aligned} \tag{9.2}$$

10 N_t for the Family $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$

We calculate the conductors N_t for the family of elliptic curves $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, where $9t+1$ is square-free. $N_t = \prod_{p|\Delta} p^{f_p}$. If $p \neq 2, 3$ then $f_p = 2$ if $p|9t+1$ and 0 otherwise.

For our curve, $a_1 = a_2 = a_3 = a_4 = 0$, $a_6 = -3^3 \cdot 2^4 \cdot (9y+1)^2$. Hence $b_2 = b_4 = b_8 = 0$, $b_6 = -2^6 \cdot 3^3 \cdot (9y+1)^2$, $c_4 = 0$, $c_6 = -2^9 \cdot 3^6 \cdot (9y+1)^2$, and $\Delta = -2^{12} \cdot 3^9 \cdot (9y+1)^4$. Note: we're changing notation from $9t+1$ to $9y+1$ as t is used in Tate's algorithm.

10.1 $p = 2$

We apply Tate's algorithm.

(2) Calculate $b_2, \ldots, \Delta$.

(3) $n = \text{ord}(2, \Delta)$. $n = 12 + 4 \cdot \text{ord}(2, 9t+1)$, where $\text{ord}(p, m)$ denotes the power of p dividing m.

(4) $n \neq 0$, so continue to line 5.

$(5-18)$ $p = 2$, $2|b_2$, so $r = 0$, $t = 0$, and we apply the change of variables $T(0,0,0,1)$, which leaves everything alone.

$(19-28)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, $2^3|b_6$, so continue to line 29.

$(29-33)$ $p = 2$, so $s = 0$, $t = 0$, change variables by $T(0,0,0,1)$.

$(34-36)$ $b = 0$, $c = 0$, $d = \frac{a_6}{2^3} = -2 \cdot 3^3(9y+1)^2$, $w = 2 \cdot 3^3(9y+1)^2$.

$(37-38)$ $2|w$, $2|x$, so continue to line 65.

$(65-69)$ $r = 0$, apply $T(0,0,0,1)$, $x_3 = 0$, $x_6 = -3^3(9y+1)^2$.

(70) $2|x_3^2 + 2^2 x_6$, so continue to line 74. Write y as $4k+z$, where $z = 0$, 1 or 2; as $9y+1$ is square-free, $y \not\equiv 3 \bmod 4$. Then $a_6 = -2^4 \cdot 3^3(36k+9z+1)^2$, $x_6 = -3^3(36k+9z+1)^2$.

$(74-75)$ $p = 2$ so $t = -2^2(x_6 \bmod 2)$. There are two possibilities: z is even (0, 2) or $z = 1$.

10.2 z is even

If z is even, let $z = 2m$, $m = 0$ or 1. Then $x_6 \equiv 1 \bmod 2$, hence $t = -2^2$.

(76) $T(0,0,-2^2,1)$. This gives $a_3' = -2^3$, $a_6' = -2^4 \cdot 3^3(36k+18m+1) - 2^4$, and Δ is unchanged, $\Delta = -2^{12} \cdot 3^9 \cdot (36y+18m+1)^4$, so $\text{ord}(2, \Delta) = 12$.

(77) $2^4|a_4$, so continue to line 78.

(78) $2^6|a_6$, so continue to line 80.

(80) Apply $T(0,0,0,2)$. $a_3' = -1$, $a_6' = \frac{1}{2^2}\Big[-3^3(36k+18z+1)^2 - 1\Big]$, $2^{12}\Delta' = \Delta$. Hence $\Delta' = -3^9 \cdot (36k+18m+1)^4$. We now restart the algorithm.

(2) Calculate $b_2, \ldots, \Delta$. We have $\Delta = -3^9 \cdot (36k + 18m + 1)^4$.
(3) $n = \text{ord}(2, \Delta) = 0$.
(4) As $n = 0$, $f_2 = 0$.

Therefore there are no factors of 2 in N_t if $t \equiv 0, 2 \bmod 4$ ($f_2 = 0$).

10.3 $z = 1$

We resume the algorithm on line 75 with $y = 4k + z$ and $z = 1$.

(75 − 76) $t = 0$, apply $T(0,0,0,1)$. Note $a_6 = -2^4 \cdot 3^3(36k + 10)^2 = -2^6 \cdot 3^3(18k + 5)^2$, $\Delta = -2^{16} \cdot 3^9 \cdot (18k + 5)^4$.

(77 − 78) $2^4|a_4$, $2^6|a_6$, so continue to line 79.

(79 − 80) Apply $T(0,0,0,2)$, which gives $a_6' = -3^3(18k+5)^2$, $2^{12}\Delta' = \Delta$, so $\Delta' = -2^4 \cdot 3^9(18k + 5)^4$.

(2) Calculate $b_2, \ldots, \Delta$. $a_6' = -3^3(18k + 5)^2$, $a_1, a_2, a_3, a_4, b_2, b_4, b_8, c_4 = 0$, $b_6 = -2^2 3^3(18k + 5)^2$, $c_6 = -2^4 \cdot 3^6(18k + 5)^2$, $\Delta = -2^4 \cdot 3^9(18k + 5)^4$.

(3) $n = \text{ord}(2, \Delta) = 4$.

(4) $n \neq 0$, so continue to line 5.

(5 − 18) $p = 2$, $2|b_2$ so $r = 0$, $t = 1$. Apply $T(0,0,1,1)$; $a_3' = 2$, $a_6' = -3^3(18k + 5)^2 - 1$, $b_6 = -2^2 \cdot 3^3(18k + 5)$, $c_4 = 0$.

(19 − 22) $2|c_4$, so continue to line 23.

(23) $2^2|a_6$, so continue to line 24.

(24) $2^3|b_8$, so continue to line 25.

(25) As $2^3 \dagger b_6$, $f_2 = \text{ord}(2, \Delta) - 2 = 4 - 2 = 2$.

Therefore $f_2 = 2$ if $t \equiv 1 \bmod 4$. We have shown:

Lemma 10.1 *For all square-free $9t+1$, if $E_t : y^2 = x^3 + 2^4 \cdot (-3)^3 \cdot (9t+1)^2$, then $f_2 = 0$ if $t \equiv 0, 2$ mod 4 and $f_2 = 2$ if $t \equiv 1$ mod 4.*

10.4 $p = 3$

We again apply Tate's algorithm.

(2) Calculate $b_2, \ldots, \Delta$. $a_1, a_2, a_3, a_4 = 0$, $a_6 = -3^3 \cdot 2^4(9y + 1)^2$, $b_2, b_4, b_8 = 0$, $b_6 = -3^3 \cdot 2^6(9y + 1)^2$, $c_4 = 04$, $c_6 = 3^6 \cdot 2^9(9y + 1)^2$, $\Delta = -3^9 \cdot 2^{12}(9y + 1)^2$.

(3 − 4) $n = \text{ord}(2, \Delta) = 9$. As $n \neq 0$, continue to line 5.

(5 − 18) $p = 3$, $3|b_2$ so $r = 0$, $t = 0$. Apply $T(0,0,0,1)$; no change.

(19 − 33) $3|c_4$, $3^2|a_6$, $3^3|b_8$, $3^3|b_6$, and $p \neq 2$ so continue to line 34.

(34 − 36) $b = 0$, $c = 0$, $d = -2^4(9y + 1)^2$, $w = -3^3 \cdot 2^4(9y + 1)^2$, $x = 0$.

$(37-38)$ $3|w$, $3|x$, so continue to line 65.

$(65-68)$ $p=3$ so $r = 3\cdot(2^4(9y+1)^2 \bmod 3) = 3$. Apply $T(3,0,0,1)$; $a_1', a_3' = 0$, $a_2' = 3^2$, $a_6' = -3^3\left[2^4(9y+1)^2 - 1\right]$. Hence $a_6' = -3^4(3^3\cdot 2^4 y^2 + 3\cdot 2^5 y + 5)$.

(69) $x_3 = 0$, $x_6 = \frac{a_6}{3^4} = -(3^3\cdot 2^4y^2 + 3\cdot 2^5 y + 5)$.

$(70-72)$ As $3 \dagger x_3^2 + 2^2 x_6 \equiv 5 \bmod 3$, $f_3 = \text{ord}(3,\Delta) - 6 = 9 - 6 = 3$.

We have therefore shown

Lemma 10.2 *For all square-free* $9t+1$, $f_3 = 3$ *for the curve* $y^2 = x^3 + 2^4\cdot(-3)^3(9t+1)^2$.

10.5 Explicit Formula for Conductors of Square-Free $9t+1$

Lemma 10.3 *Let* $E_t : y^2 = x^3 + 2^4\cdot(-3)^3\cdot(9t+1)^2$, $9t+1$ *square-free. Then* $N_t = 2^{f_2(t)}3^3\prod_{p|(9t+1),p\neq 2,3} p^2$, *where* $f_2(t)$ *equals* 0 *if* $t \equiv 0,2$ *mod* 4 *and* $f_2(t)$ *equals* 2 *if* $t\equiv 1$ *mod* 4. *Note* $t \not\equiv 3$ *mod* 4 *as* $9t+1$ *is square-free.*

For $p > 3$, both cases have $f_p = 2$ if $p|9t+1$ and $f_p = 0$ otherwise. For $p=3$, $3 \dagger (9t+1)^2$, and both cases have $f_3 = 3$. Further, if $t \equiv 0,2 \bmod 4$, then $2\dagger(9t+1)^2$, so $N_t = 2^0\cdot 3^3\cdot(9t+1)^2$. If $t\equiv 1 \bmod 4$, then $2^2 \parallel (9t+1)^2$, and $N_t = 2^2\cdot 3^3\prod_{p|(9t+1),p\neq 2,3} p^2 = 3^3\cdot(9t+1)^2$. Hence we have shown

Theorem 10.4 *Let* $E_t : y^2 = x^3 + 2^4\cdot(-3)^3\cdot(9t+1)^2$, $9t+1$ *square-free. Then* $N_t = 3^3(9t+1)^2$.

10.6 Numerically Verifying f_2, f_3 for Square-Free $9t+1$

To numerically check Theorem 10.4, one may use the following PARI program. First define the following shortcuts:

$$\begin{aligned}
\mathbf{mu}(x) &= \mathbf{moebius}(x)\\
f(t) &= 9t+1\\
E(t) &= [0,0,0,0,-16*27*f(t)*f(t)]\\
F(t) &= \mathbf{ellinit}(E(t))\\
\mathbf{root}(Q) &= \mathbf{ellrootno}(Q,1)\\
\mathbf{cond}(Q) &= \mathbf{ellglobalred}(Q)[1]\\
g(t) &= f(t)*f(t).
\end{aligned}\tag{10.3}$$

To find f_2, f_3 for an elliptic curve E_t, first make sure $9t+1$ is square-free by typing $\mathbf{mu}(f(t))$. Then type $G = F(t)$ to initialize an elliptic curve G, then $\mathbf{cond}(G)/g(t)$ to get $2^{f_2}3^{f_3}$. To check the root number, type $\mathbf{root}(Q)$.

11 N_t for the Family $y^2 = x^3 \pm 4(4t+2)x$

We calculate the conductors N_t for the family of elliptic curves $y^2 = x^3 + 4(4t+2)x$, where $4t+2$ is square-free. $N_t = \prod_{p|\Delta} p^{f_p}$. If $p \neq 2, 3$ then $f_p = 2$ if $p|4t+2$ and 0 otherwise. We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr].

We first calculate the a_i's, b_i's, c_i's, and Δ for our curve. $a_1 = a_2 = a_3 = a_6 = 0$, $a_4 = 2^2(2t+1)$, $b_2 = b_6 = 0$, $b_4 = 2^4(2t+1)$, $b_8 = -2^6(2t+1)^2$, $c_4 = -2^7 \cdot 3(2t+1)$, $c_6 = 0$, $\Delta = -2^{15}(2t+1)^3$.

11.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta) = 15$, $n > 0$ so skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = t = 0$. Apply $T(0,0,0,1)$, which has no affect.

$(19-28)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, $2^3|b_6$, so continue to line 29.

$(29-33)$ $p = 2$ so $s = t = 0$. Apply $T(0,0,0,1)$; no change.

$(34-36)$ $b = 0$, $c = 2(2t+1)$, $d = 0$, $w = 2^3(2t+1)$, $x = 2 \cdot 3(2t+1)$.

$(37-38)$ $2|w$, $2|x$, so skip to line 65.

$(65-68)$ $r_p = 0$, $r = 0$. Apply $T(0,0,0,1)$; no change.

$(69-70)$ $x_3 = x_6 = 0$, $2|(x_3^2 + 4x_6)$, so skip to line 74.

$(74-76)$ $p = 2$, so $t = 0$. Apply $T(0,0,0,1)$; no change.

(77) $2^4 \dagger a_4$, therefore $f_2 = n - 7 = 8$.

11.2 $p = 3$

We again apply Tate's algorithm.

(3) $n = \text{ord}(3, \Delta) = \text{ord}(3, (2t+1)^3)$. As $4t+2$ is square-free, $\text{ord}(3, (2t+1)^3)$ is either 0 or 3. If $n = 0$ we are done and $f_3 = 0$. Else assume $3||(2t+1)$ and $n = 3$.

$(5-18)$ $p = 3$, $3|b_2$, $r = t = 0$. Apply $T(0,0,0,1)$; no change.

$(19-23)$ $3|c_4$, $3^2|a_6$, so continue to line 24.

(24) $3^3 \dagger b_8 = -2^6(2t+1)^2$, therefore $f_3 = n - 1 = 2$.

11.3 Explicit Formula for Conductors of Square-Free $4t + 2$

We calculate N_t for the curve $y^2 = x^3 + 4(4t + 2)x$, $4t + 2$ square-free. If $p > 3$, then $f_p = 2$ if $p|4t + 2$ and 0 otherwise. If $p = 3$ then $f_3 = 2$ if $3||(4t+2)$ and 0 otherwise. If $p = 2$ then $f_2 = 8$. Note $2||(4t+2)$. Therefore we have proved

Theorem 11.1 *Let $E_t : y^2 = x^3 + 4(4t + 2)x$, $4t + 2$ square-free. Then $N_t = 2^6(4t + 2)^2$.*

12 N_t for the Family $y^2 = x^3 + (t + 1)x^2 + tx$

We calculate the conductors N_t for the family of elliptic curves $y^2 = x^3 + (t + 1)x^2 + tx$, where $t(t - 1)$ is square-free.

We first calculate the a_i's, b_i's, c_i's, and Δ for our curve. $a_1 = a_3 = a_6 = 0$, $a_2 = (2t + 1)$, $a_4 = t$, $b_2 = 2^2(t + 1)$, $b_4 = 2t$, $b_6 = 0$, $b_8 = -t^2$, $c_4 = 2^4(t^2 - t + 1)$, $c_6 = -2^5(2t^3 - 3t^3 - 3t + 2)$, $\Delta = 2^4t^2(t - 1)^2$.

$N_t = \prod_{p|\Delta} p^{f_p}$, where for primes greater than 3, $f_p = 2$ if $p|c_4(t) = 2^4(t^2 - t + 1)$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4$, as no factors of t divide $t^2 - t + 1$, and no factor of $t - 1$ divides $t^2 - t + 1 = t(t - 1) + 1$. Therefore, for primes greater than 3, $f_p = 1$.

We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr].

12.1 $p = 2$

We apply Tate's algorithm.

$(3 - 4)$ $n = \text{ord}(2, \Delta) = 6$, $n > 0$ so skip to line 5.

$(5 - 18)$ $p = 2$, $2|b_2$ so $r = t \bmod 2$, $t = 0$. Apply $T(r, 0, 0, 1)$, which has no affect if $t \equiv 0(2)$. In this case, (19) $2|c_4$ so continue to (23) $2^2|a_6$ so continue to (24) $2^3 \dagger b_8$, so $f_2 = n - 1 = 5$. Assume now that $t \equiv 1(2)$. Then on line (18) we apply $T(1, 0, 0, 1)$. This gives $a_1 = 0$, $a_2 = t + 4$, $a_3 = 0$, $a_4 = 3t + 5$, $a_6 = 2t + 2$, $b_8 = 2^2(t + 4)(2t + 2) - (3t + 5)^2$. We actually don't need to calculate b_2, b_4, or b_6. Note c_4, c_6 and Δ are unchanged. Also, as $t \equiv 1(2)$ and $t - 1$ is square-free, $t = 4k + 3$.

$(19 - 24)$ $2|c_4$, $2^2|a_6$ (as $t = 4k + 3$), but $2^3 \dagger b_8$. $2^3|2^2(t + 4)(2t + 2)$, but $(3t + 5)^2 = 2^2(6k + 7)^2$, which is not divisible by 2^3. Hence $f_2 = n - 1 = 5$, and we get the same answer again.

12.2 $p = 3$

We again apply Tate's algorithm. If $t \equiv 2(3)$ then $\text{ord}(3, \Delta) = 0$ and $f_3 = 0$. Hence assume $t \equiv 0$ or 1 mod 3.

(3) $n = \text{ord}(3, \Delta) = \text{ord}(3, t^2(t-1)^2)$. As $t(t-1)$ is square-free, $n = 0$ or 2. If $t \equiv 2(3)$ then $\text{ord}(3, \Delta) = 0$ and $f_3 = 0$. Hence assume $t \equiv 0$ or 1 mod 3, and $n = 2$. In particular, $3 \dagger (t+1)$.

$(5-18)$ $p = 3$, $3 \dagger b_2$, $r = t = 0$. Apply $T(0,0,0,1)$; no change.

(19) $3 \dagger c_4 = 2^4(t+1)^2 - 3 \cdot 2^4 t$. Thus $f_3 = 1$.

12.3 Explicit Formula for Conductors of Square-Free $t(t-1)$

Note, for square-free $t(t-1)$, $2||t(t-1)$. As $f_2 = 5$ and f_3 is the power of 3 dividing $t(t-1)$ we've shown:

Theorem 12.1 *Let $E_t : y^2 = x^3 + (t+1)x^2 + tx$, $t(t-1)$ square-free. Then $N_t = 2^4 t(t-1)$.*

13 N_t for the Family $y^2 = x^3 + x^2 + 2t + 1$

We calculate the conductors N_t for the family of elliptic curves $y^2 = x^3 + x^2 + 2t + 1$, where $(2t+1)\ (54t+31)$ is square-free.

We first calculate the a_i's, b_i's, c_i's, and Δ for our curve. $a_1 = a_3 = a_4 = 0$, $a_2 = 1$, $a_6 = 2t+1$, $b_2 = 2^2$, $b_4 = 0$, $b_6 = 2^2(2t+1)$, $b_8 = 2^2(2t+1)$, $c_4 = 2^4$, $c_6 = -2^5(54t+29)$, $\Delta = -2^4(2t+1)(54t+31)$.

$N_t = \prod_{p|\Delta} p^{f_p}$, where for primes greater than 3, $f_p = 2$ if $p|c_4(t) = 2^4$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4$. Therefore, for primes greater than 3, $f_p = 1$.

We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr]. We show $N_t = 2^4(2t+1)(54t+31)$ if t is odd and $2^3(2t+1)(54t+31)$ if t is even.

13.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta) = 4$, $n > 0$ so skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 0$, $t = 1$. Apply $T(0,0,1,1)$. This gives $a_1 = 0$, $a_2 = 1$, $a_3 = 2$, $a_4 = 0$, $a_6 = 2t$, $b_8 = 2^2(2t+1)$. We don't need b_2, b_4, or b_6. Note c_4, c_6 and Δ are unchanged.

$(19-24)$ $2|c_4$. $2^2 \dagger a_6$ if t is odd, in which case we find $f_2 = n = 4$. If t is even, $2^2|a_6$ but $2^3 \dagger b_8$. Therefore $f_2 = n - 1 = 3$.

13.2 $p = 3$

We again apply Tate's algorithm.

(3) $n = \text{ord}(3, \Delta) = \text{ord}(3, 2t+1)$. Thus $n = 0$ or 2. If $t \equiv 0$ or 2 mod (3) then $\text{ord}(3, \Delta) = 0$ and $f_3 = 0$. Hence assume $t \equiv 1$ mod 3, and $n = 1$.

$(5-18)$ $p = 3$, $3 \nmid b_2$, $r = t = 0$. Apply $T(0,0,0,1)$; no change.

(19) $3 \nmid c_4 = 2^4 t$. Thus $f_3 = 1$.

13.3 Explicit Formula for Conductors of Square-Free $(2t+1)(54t+31)$

Theorem 13.1 *Let $E_t : y^2 = x^3 + x^2 + 2t + 1$, $(2t+1)(54t+31)$ square-free. Then $N_t = 2^4(2t+1)(54t+31)$ if t is odd and $2^3(2t+1)(54t+31)$ if t is even.*

14 N_t for the Family $y^2 = x^3 + x^2 + 12t + 1$

We calculate the conductors N_t for the family of elliptic curves $y^2 = x^3 + x^2 + 12t + 1$, where $(12t+1)$ $(324t+31)$ is square-free.

We first calculate the a_i's, b_i's, c_i's, and Δ for our curve. $a_1 = a_3 = a_4 = 0$, $a_2 = 1$, $a_6 = 12t + 1$, $b_2 = 2^2$, $b_4 = 0$, $b_6 = 2^2(12t+1)$, $b_8 = 2^2(12t+1)$, $c_4 = 2^4$, $c_6 = -2^5(324t+29)$, $\Delta = -2^4(12t+1)(324t+31)^2$. Note $12 = 2^2 \cdot 3$ and $324 = 2^2 \cdot 3^4$.

$N_t = \prod_{p|\Delta} p^{f_p}$, where for primes greater than 3, $f_p = 2$ if $p | c_4(t) = 2^4$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4$. Therefore, for primes greater than 3, $f_p = 1$.

We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr]. We show that $N_t = 2^4(12t+1)(324t+31)$.

14.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta) = 4$, $n > 0$ so skip to line 5.

$(5-18)$ $p = 2$, $2 | b_2$ so $r = 0$, $t = 1$. Apply $T(0,0,1,1)$. This gives $a_1 = 0$, $a_2 = 1$, $a_3 = 2$, $a_4 = 0$, $a_6 = 12t$, $b_8 = 2^2(12t+1)$. We don't need b_2, b_4, or b_6. Note c_4, c_6 and Δ are unchanged.

$(19-24)$ $2 | c_4$, $2^2 | a_6$ but $2^3 \nmid b_8$. Therefore $f_2 = n - 1 = 3$.

14.2 $p = 3$

We again apply Tate's algorithm.

(3) $n =$ord$(3, \Delta) = 0$, as $\Delta(t) \equiv 1 \cdot 31 \equiv 1 \bmod 3$. Thus $f_3 = 0$.

14.3 Explicit Formula for Conductors of Square-Free $(12t+1)(324t+31)$

Theorem 14.1 *Let $E_t : y^2 = x^3 + x^2 + 12t + 1$, $(12t+1)(324t+31)$ square-free. Then $N_t = 2^3(12t+1)(324t+31)$.*

15 $y^2 = x^3 + (12t+1)x^2 - (12t+1+3)x + 1$

We calculate the conductors N_t for the family of elliptic curves $y^2 = x^3 + (12t+1)x^2 - (12t+4)x + 1$, where $144t^2 + 60t + 13$ is square-free. We have sent t to $12t$ in Washington's family to simplify the calculations for N_t.

We first calculate the a_i's, b_i's, c_i's, and Δ for our curve. $a_1 = a_3 = 0$, $a_2 = 12t + 1$, $a_4 = -(12t+4)$, $a_6 = 1$, $b_2 = 2^2(12t+1)$, $b_4 = -2^2(6t+2)$, $b_6 = 2^2$, $b_8 = -2^2 \cdot 3(12t^2 + 4t + 1)$, $c_4 = 2^4(144t^2 + 60t + 13)$, $c_6 = 2^5(24t+5)(144t^2 + 60t + 13)$, $\Delta = 2^4(144t^2 + 60t + 13)^2$.

$N_t = \prod_{p|\Delta} p^{f_p}$, where for primes greater than 3, $f_p = 2$ if $p|c_4(t) = 2^4(144t^2 + 60t + 13)$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4(144t^2 + 60t + 13)$. Therefore, for primes greater than 3, $f_p = 2$.

We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr]. We show that $N_t = 2^3(144t^2 + 60t + 13)$.

15.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta) = 4$, $n > 0$ so skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 0$, $t = 1$. Apply $T(0,0,1,1)$. This gives $a_1 = 0$, $a_2 = 12t + 1$, $a_3 = 2$, $a_4 = -2^2(3t+1)$, $a_6 = 0$, $b_8 = -2^2 \cdot 3(12t^2 + 4t + 1)$. We don't need b_2, b_4, or b_6. Note c_4, c_6 and Δ are unchanged.

$(19-24)$ $2|c_4$, $2^2|a_6$, $2^3 \dagger b_8$. Therefore $f_2 = n - 1 = 3$.

15.2 $p = 3$

We again apply Tate's algorithm.

(3) $n =$ord$(3, \Delta) = \text{ord}(3, 36t^2 + 30t + 13) = 0$. Thus $f_3 = 0$.

15.3 Explicit Formula for Conductors of Square-Free $144t^2 + 60t + 13$

Theorem 15.1 *Let* $E_t : y^2 = x^3 + (6t+1)x^2 - (6t+4)x + 1$*, where* $144t^2 + 60t + 13$ *is square-free. Then* $N_t = 2^3(144t^2 + 60t + 13)^2$.

16 N_t for the Family $y^2 = x^3 + (6t+1)x^2 + 1$

Earlier we studied the family $y^2 = x^3 + tx^2 + 1$. For convenience in calculating the conductors, we consider the related family $y^2 = x^3 + (6t+1)x^2 + 1$. The discriminant is

$$\Delta(t) = -2^4\Big(4(6t+1)^3 + 27\Big) = -\Delta_1(t)\Delta_2(t). \qquad (16.1)$$

We will sieve to $\Delta_2(t)$ square-free. Note $(6, \Delta_2(t)) = 1$.

We first calculate the a_i's, b_i's, and c_i's for our curve. $a_1 = a_4 = a_6 = 0$, $a_2 = 6t+1$, $a_3 = 2$, $b_2 = 2^2(6t+1)$, $b_4 = 0$, $b_6 = 2^2$, $b_8 = 2^2(6t+1)$, $c_4 = 2^4(6t+1)^2$.

$N_t = \prod_{p|\Delta} p^{f_p}$, where for primes greater than 3, $f_p = 2$ if $p|c_4(t) = 2^4(6t+1)^2$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4$, as no factors of $6t+1$ divide $\Delta_2(t)$. Therefore, for primes greater than 3, $f_p = 1$.

We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr].

16.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 4$, $n > 0$ so skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 0$ and $t = 1$. Apply $T(0,0,1,1)$. Now $a_1 = a_4 = a_6 = 0$, $a_2 = 6t+1$, $a_3 = 2$, $b_2 = 2^2(6t+1)$, $b_4 = 0$, $b_6 = 2^2$, $b_8 = 2^2(6t+1)$, and the other quantities are unchanged.

$(19-24)$ $2|c_4$, $2^2|a_6$, but $2^3 \dagger b_8$. Hence $f_2 = n - 1 = 3$.

16.2 $p = 3$

As $(3, \Delta(t)) = 1$, $f_3 = 0$. This is one of the reasons we changed variables from t to $6t+1$.

16.3 N_t

Theorem 16.1 *Let $E_t : y^2 = x^3 + (6t+1)x^2 + 1$, $4(6t+1)^3 + 27$ square-free. Then $N_t = 2^2\Big(4(6t+1)^3 + 27\Big)$.*

17 N_t for the Family $y^2 = x^3 - (6t+1)^2x + (6t+1)^2$

Earlier we studied the family $y^2 = x^3 - t^2x + t^2$. For convenience in calculating the conductors, we consider the related family $y^2 = x^3 - (6t+1)^2x + (6t+1)^2$. The discriminant is

$$\Delta(t) = 2^4\Big(6t+1\Big)^4\Big(4(6t+1)^2 - 27\Big) = 2^4\Delta_1^4(t)\Delta_2(t). \tag{17.1}$$

We will sieve to $\Delta_1(t) \cdot \Delta_2(t)$ square-free. Note $(6, \Delta_1(t)\Delta_2(t)) = 1$.

We first calculate the a_i's, b_i's, and c_i's for our curve. $a_1 = a_2 = a_3 = 0$, $a_4 = -(6t+1)^2$, $a_6 = (6t+1)^2$, $b_2 = 0$, $b_4 = -2(6t+1)^2$, $b_6 = 2^2(6t+1)^2$, $b_8 = (6t+1)^4$, $c_4 = 2^4 \cdot 3 \cdot (6t+1)^2$.

$N_t = \prod_{p|\Delta} p^{f_p}$, where for primes greater than 3, $f_p = 2$ if $p|c_4(t) = 2^4 \cdot 3 \cdot (6t+1)^2$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4(6t+1)^2$. Thus, for $p \geq 5$, $f_p = 1$ if $p|\Delta_2(t)$ and $f_p = 2$ if $p|\Delta_1(t)$.

We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr].

17.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 4$, $n > 0$ so skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 1$ and $t = 1$. Apply $T(1,0,1,1)$. Now $a_1 = a_6 = 0$, $a_2 = 3$, $a_3 = 2$, $a_4 = -2(18t^2 + 6t - 1)$, $b_2 = 2^2 \cdot 3$, $b_4 = -2^2(18t^2 + 6t - 1)$, $b_6 = 2^2$, $b_8 = 2^3(162t^4 + 108t^3 - 6t - 1)$, and the other quantities are unchanged.

$(19-25)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, but $2^3 \dagger b_6$. Hence $f_2 = n - 2 = 2$.

17.2 $p = 3$

As $(3, \Delta(t)) = 1$, $f_3 = 0$. This is one of the reasons we changed variables from t to $6t+1$.

17.3 N_t

Theorem 17.1 *Let* $E_t : y^2 = x^3 - (6t+1)^2 x + (6t+1)^2$, $\Big(6t+1\Big)\Big(4(6t+1)^2 - 27\Big)$ *square-free. Then* $N_t = 2^2\Big(6t+1\Big)^2\Big(4(6t+1)^2-27\Big)$.

18 N_t for the Family $y^2 = x^3 - (6t+1)^2 x + (6t+1)^4$

Earlier we studied the family $y^2 = x^3 - t^2x + t^4$. For convenience in calculating the conductors, we consider the related family $y^2 = x^3 - (6t+1)^2 x + (6t+1)^4$. The discriminant is

$$\Delta(t) = -2^4\Big(6t+1\Big)^6\Big(27(6t+1)^2 - 4\Big) = -2^4\Delta_1^6(t)\Delta_2(t). \qquad (18.1)$$

We will sieve to $\Delta_1(t)\cdot\Delta_2(t)$ square-free. Note $(6, \Delta_1(t)\Delta_2(t)) = 1$.

We first calculate the a_i's, b_i's, and c_i's for our curve. $a_1 = a_2 = a_3 = 0$, $a_4 = -(6t+1)$, $a_6 = (6t+1)^4$, $b_2 = 0$, $b_4 = -2(6t+1)^2$, $b_6 = 2^2(6t+1)^4$, $b_8 = (6t+1)^4$, $c_4 = 2^4\cdot 3\cdot(6t+1)^2$.

$N_t = \prod_{p|\Delta} p^{f_p}$, where for primes greater than 3, $f_p = 2$ if $p|c_4(t) = 2^4\cdot 3\cdot(6t+1)^2$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4(6t+1)^2$. Thus, for $p\geq 5$, $f_p = 1$ if $p|\Delta_2(t)$ and $f_p = 2$ if $p|\Delta_1(t)$.

We determine below f_2 and f_3 by using an algorithm of Tate, taken from Cremona [Cr].

18.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 4$, $n > 0$ so skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 1$ and $t = 1$. Apply $T(1,0,1,1)$. Now $a_1 = 0$, $a_2 = 3$, $a_3 = 2$, $a_4 = -2(18t^2+6t-1)$, $a_6 = 2^2\cdot 3t(3t+1)(6t+1)$, $b_2 = 2^2\cdot 3$, $b_4 = -2^2(18t^2+6t-1)$, $b_6 = 2^2(1296t^4+864t^3+180t^2+12t+1)$, $b_8 = 2^3(1782t^4+1188t^3+270t^2+24t+1)$, and the other quantities are unchanged.

$(19-25)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, but $2^3 \dagger b_6$. Hence $f_2 = n-2 = 2$.

18.2 $p = 3$

As $(3, \Delta(t)) = 1$, $f_3 = 0$. This is one of the reasons we changed variables from t to $6t+1$.

18.3 N_t

Theorem 18.1 *Let $E_t : y^2 = x^3 - (6t+1)^2 x + (6t+1)^4$, $\Big(6t+1\Big)\Big(27(6t+1)^2 - 4\Big)$ square-free. Then $N_t = 2^2\Big(6t+1\Big)^2\Big(27(6t+1)^2 - 4\Big)$.*

19 N_t for the Family $y^2 = x^3 + 5x^2 + 16(30t+1)x$

Earlier we studied the family $y^2 = x^3 + 5x^2 + 16tx$. For convenience in calculating the conductors, we consider the related family $y^2 = x^3 + 5x^2 + 16(30t+1)x$. The discriminant is

$$\Delta(t) = 2^{12}\Big(30t+1\Big)^2\Big(25 - 64(30t+1)\Big) = 2^{12}\Delta_1^2(t)\Delta_2(t). \qquad (19.1)$$

We sieve to $\Delta_1(t) \cdot \Delta_2(t)$ square-free. Note $(10, \Delta_1(t)\Delta_2(t)) = 1$.

We first calculate the a_i's, b_i's, and c_i's for our curve. $a_1 = a_3 = a_6 = 0$, $a_2 = 5$, $a_4 = 2^4(30t+1)$, $b_2 = 2^2 \cdot 5$, $b_4 = 2^5(30t+1)$, $b_6 = 0$, $b_8 = 2^8(30t+1)^2$, $c_4 = -2^4(2^5 \cdot 3^2 \cdot 5t + 23) = -2^4\Big(48(30t+1) - 25\Big)$.

$N_t = \prod_{p|\Delta} p^{f_p}$, where for primes greater than 3, $f_p = 2$ if $p|c_4(t) = 2^4 \cdot 3 \cdot (6t+1)^2$, and 0 otherwise. $(\Delta(t), c_4(t)) = 2^{12}$. Clearly there are no common factors of $c_4(t)$ and $\Delta_1(t) = 30t+1$. Assume $(c_4(t), \Delta_2(t)) = d > 1$. Then

$$d|3\Big(64(30t+1) - 25\Big) - 4\Big(48(30t+1) - 25\Big) = 25. \qquad (19.2)$$

Thus, $d|5$ but $5 \nmid \Delta(t)$. Thus, for $p \geq 5$, $f_p = 1$ if $p|\Delta_1(t)\Delta_2(t)$.

19.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 12$, $n > 0$ so skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 0$ and $t = 0$. Apply $T(0,0,0,1)$. which leaves all quantities unchanged.

$(19-28)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, $2^3|b_6$.

$(29-33)$ $p = 2$ so $s = 1$, $t = 0$. Apply $T(0,1,0,1)$, yielding $a_1 = 2$, $a_2 = 2^2$, $a_3 = 0$, $a_4 = 2^4(30t+1)$, $a_6 = 0$, $b_2 = 2^2 \cdot 5$, $b_4 = 2^5(30t+1)$, $b_6 = 0$, $b_8 = 2^8(30t+1)^2$, and the other quantities are unchanged.

$(34-36)$ $b = 2$, $c = 2^2(30t+1)$, $d = 0$, $w = 4(2^2(30t+1) - 1)c^2$, $x = 4(90t+2)$.

(37) $2|w$ so skip to (38).

(38) $2|x$ so skip to (65).

$(65-68)$ $p=2$ so $rp=-2$, $r=0$. Apply $T(0,0,0,1)$, which leaves all quantities unchanged.

(69) $x_3=0$, $x_6=0$.

$(70-72)$ $2|(x_3^2+4x_6)$ so skip to (73).

$(73-76)$ $p=2$ so $t=0$, apply $T(0,0,0,1)$ which leaves all quantities unchanged.

$(77-80)$ $2^4|a_4$ and $2^6|a_6$. Thus, apply $T(0,0,0,2)$ and restart the algorithm. This changes Δ to $\Delta'=2^{-12}\Delta$. Before $n=\text{ord}(2,\Delta)=12$; now $n=\text{ord}(2,\Delta')=0$. Thus by line (4) we find $f_2=0$.

19.2 $p=3$

We apply Tate's algorithm, assuming $\Delta_1(t)\Delta_2(t)$ is square-free.

$(3-4)$ $n=\text{ord}(3,\Delta(t))=1$, $n>0$ so skip to line 5.

$(5-18)$ $p=3$, $3\nmid b_2$ so $r=2$ and $t=0$. Apply $T(2,0,0,1)$. Now $a_1=a_3=0$, $a_2=11$, $a_4=2^4\cdot 3(10t+1)$, $a_6=2^2\cdot 3\cdot 5(16t+1)(6t+1)$, $b_2=2^2\cdot 11$, $b_4=2^5\cdot 3(10t+1)$, $b_6=2^4\cdot 3\cdot 5(16t+1)$, $b_8=-2^4\cdot 3(4800t^2+80t-1)$, and the other quantities are unchanged.

(19) $3\nmid c_4$. Hence $f_3=1$.

19.3 N_t

Theorem 19.1 *Let $E_t : y^2=x^3+5x^2+16(30t+1)x$, $\Big(30t+1\Big)\Big(25-64(30t+1)\Big)$ square-free. Then $N_t=\Big(30t+1\Big)\Big(64(30t+1)-25\Big)$.*

References

[Al] Alfhors, *Complex Analysis*,

[BEW] B. Berndt, R. Evans and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. **21**, Wiley-Interscience Publications, John Wiley & Sons, Inc., New York, 1998.

[Bi] B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43**, 1968, 57 – 60.

[BS] B. Birch and N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5**, 1966, 295 – 299.

[BSD1] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. reine angew. Math. **212**, 1963, 7 – 25.

[BSD2] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. reine angew. Math. **218**, 1965, 79 – 108.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14**, number 4, 2001, 843 – 939.

[Br] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. **109**, 1992, 445 – 472.

[BM] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. AMS **23**, 1991, pages 375 – 382.

[Cr] Cremona, *Algorithms for Modular Elliptic Curves*,

[Da] H. Davenport, *Multiplicative Number Theory,* 2*nd edition*, Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 1980, revised by H. Montgomery.

[Di] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. **144**, 1996, 137 – 166.

[Fe1] S. Fermigier, *Zéros des fonctions L de courbes elliptiques*, Exper. Math. **1**, 1992, 167 – 173.

[Fe2] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathcal{Q}$, Exper. Math. **5**, 1996, 119 – 130.

[Fo] G. Folland, *Real Analysis: Modern Techniques and their Applications*, Wiley-Interscience Publications, John Wiley & Sons, New York, 1984.

[FNT] E. Fouvry, M. Nair and G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France, **120**, 1992, 485 – 506.

[FP] E. Fouvrey and J. Pomykala, *Rang des courbes elliptiques et sommes d'exponentelles*, Monat. Math. **116**, 1993, 111 – 125.

[GM] F. Gouvéa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4**, 1991, 45 – 65.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (PRoc. Conf. in Carbondale, 1979), Lecture Notes in Math. **751**, Springer-Verlag, New York, 1979, 108 – 118.

[GH] Goldfeld and Hoffstein, *On The Number Of Fourier Coefficients That Determine A Modular Form*, Contemporary Mathematics, Vol **143**, 1993.

[HW] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Oxford Science Publications, Clarendon Press, Oxford, 1995.

[Ho] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press, Cambridge, 1976.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics **97**, Springer-Verlag, New York, 1972.

[ILS] H. Iwaniec, W. Luo and P. Sarnak, *Low lying zeros of families of L-functions*,

[Ka] N. Katz, *Twisted L-Functions and Monodromy*, Annals of Mathematical Studies **150**, Princeton University Press, Princeton, 2002.

[KS1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications, 45, AMS, Providence, 1999.

[KS2] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36**, 1999, $1-26$.

[Kn] A. Knapp, *Elliptic Curves*, Mathematical Notes, volume **40**, Princeton University Press, Princeton, 1992.

[La1] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1986.

[La2] S. Lang, *Real and Functional Analysis*, Graduate Texts in Mathematics **142**, Springer-Verlag, New York, 1993.

[Mai] L. Mai, *The analytic rank of a family of elliptic curves*, Canadian Journal of Mathematics **45**, 1993, $847-862$.

[Meh] M. Mehta, *Random Matrices, 2nd edition*, Academic Press Inc., Boston, 1991.

[Mes1] J. Mestre, *Formules explicites et minorations de conducteurs de varits algbriques*, Compositio Mathematica **58**, 1986, $209-232$.

[Mes2] J. Mestre, *Courbes elliptiques de rang $\geq$ 11 sur $\boldsymbol{Q}(t)$*, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, 139 – 142. 209 – 232.

[Mes3] J. Mestre, *Courbes elliptiques de rang $\geq$ 12 sur $\boldsymbol{Q}(t)$*, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, 171 – 174. 209 – 232.

[Mi] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monat. Math. **120**, 1995, 127 – 136.

[Mon] H. Montgomery, *The pair correlation of zeros of the zeta function* in Analytic Number Theory, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, 1973, 181 – 193.

[Mor] Mordell, *Diophantine Equations*, **1968**,

[Na1] K. Nagao, *On the rank of elliptic curve $y^2 = x^3 - kx$*, Kobe J. Math. **11**, 1994, 205 – 210.

[Na2] K. Nagao, *Construction of high-rank elliptic curves*, Kobe J. Math. **11**, 1994, 211 – 219.

[Na3] K. Nagao, *$\mathcal{Q}(t)$-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92**, 1997, 13 – 32.

[Nag] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York, 1981.

[Od1] A. Odlyzko, *On the distribution of spacings between zeros of the zeta function*, Math. Comp. **48**, 1987, no. 177, 273 – 308.

[Od] A. Odlyzko, *The 10^{22}-nd zero of the Riemann zeta function*, Proc. Conference on Dynamical, Spectral and Arithmetic Zeta-Functions, M. van Frankenhuysen and M. L. Lapidus, eds., Amer. Math. Soc., Contemporary Math. series, 2001, http://www.research.att.com/~amo/doc/zeta.html

[Ri] Rizzo, *Average root numbers for a non-constant family of elliptic curves*,

[Ro] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compos. Math. **87**, 1993, 119 – 151.

[RSi] M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133**, 1998, 43 – 67.

[Ru] M. Rubinstein, *Evidence for a spectral interpretation of the zeros of L-functions*, P.H.D. Thesis, Princeton University, 1998, http://www.ma.utexas.edu/users/miker/thesis/thesis.html.

[RS] Z. Rudnick and P. Sarnak, *Zeros of principal L-functions and random matrix theory*, Duke Journal of Math. **81**, 1996, 269 − 322.

[Sh] T. Shioda, *Construction of elliptic curves with high-rank via the invariants of the Weyl groups*, J. Math. Soc. Japan **43**, 1991, 673 − 719.

[Si1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, Berlin - New York, 1986.

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, Berlin - New York, 1994.

[Si3] J. Silverman, *The average rank of an algebraic family of elliptic curves*, J. reine angew. Math. **504**, 1998, 227 − 236.

[St1] N. Stephens, *A corollary to a conjecture of Birch and Swinnerton-Dyer*, J. London Math. Soc. **43**, 1968, 146 − 148.

[St2] N. Stephens, *The diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **231**, 1968, 16 − 162.

[ST] C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, Journal of the American Mathematical Society, vol. **40**, number 4, 1995.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141**, 1995, 553 − 572.

[Wa] L. Washington, *Class numbers of theh simplest cubic fields*, Math. Comp. **48**, number 177, 1987, 371 − 384.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math **141**, 1995, 443 − 551.