MATHEMATICS OF COMPUTATION
VOLUME 54, NUMBER 189
JANUARY 1990, PAGES 413–419

ELLIPTIC CURVES OVER THE RATIONALS WITH BAD REDUCTION AT ONLY ONE PRIME

BAS EDIXHOVEN, ARNOLD DE GROOT, AND JAAP TOP

ABSTRACT. A list is given of elliptic curves over $\mathbf{Q}$ having additive reduction at exactly one prime. It is also proved that for primes congruent to 5 modulo 12, no such curves having potentially good reduction exist. This enables one to find in a number of cases a complete list of all elliptic curves with bad reduction at only one prime.

1. INTRODUCTION

This paper grew out of an attempt to find some examples of elliptic curves over $\mathbf{Q}$ with conductor p^2, for various small primes p. The conductor N of an elliptic curve over $\mathbf{Q}$ is an invariant which contains information about the reductions of the curve modulo primes. If the curve has good reduction modulo p, then p does not divide N; if the curve has multiplicative reduction at p, then p divides N exactly once. In case $p \geq 5$ and the curve has additive reduction at p, then p divides N exactly twice. Our main result is that in certain cases the only curves with conductor p^2 are twists of elliptic curves of conductor p. In combination with work of Setzer [9] and Brumer and Kramer [2], this allows one to write down for a number of primes p a complete list of the elliptic curves over $\mathbf{Q}$ with good reduction outside p. In other cases, an extensive computer search provided us with many examples for primes $p < 5000$. These are given in the second half of this paper. There is no guarantee that this list is complete.

2. DIOPHANTINE RESULTS

Suppose p is a prime number. Our problem is to find all elliptic curves over $\mathbf{Q}$ having additive reduction at p and good reduction at all other primes. Since all elliptic curves with good reduction away from 2 and 3 are known (see e.g. [1, pp. 123–134]), one may assume $p \geq 5$. Given an elliptic curve as desired, one can twist it over the quadratic extension of $\mathbf{Q}$ with discriminant p (compare [10, Chapter X, §§2 and 5]). The resulting curve has conductor a power of p as well. Moreover, one has:

Lemma 1. *Let $p \geq 5$ be a prime number and K the quadratic extension of $\mathbf{Q}$ unramified outside p. Up to K-twists, all elliptic curves over $\mathbf{Q}$ with good*

Received September 12, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G05; Secondary 11D25.
The third author was supported by N.W.O.

reduction away from p *are*

1. *the ones with multiplicative reduction at* p;
2. *those given by a Weierstrass model with discriminant* $\pm p^2$, $\pm p^3$, *or* $\pm p^4$.

Proof. Given p and K as in the lemma and any elliptic curve E over $\mathbf{Q}$, let Δ_1 and Δ_2 be the discriminants of Weierstrass models of E and the K-twist of E, respectively. Then the difference of the valuations at p of Δ_1 and Δ_2 is congruent to 6 modulo 12. Since any elliptic curve E over $\mathbf{Q}$ has a global Weierstrass minimal model ([10, p. 226]) and no such curve has everywhere good reduction (e.g. [10, Exercise 8.15]), the lemma follows using the table on p. 46 of [1]. □

Our main interest is in curves which do not come from the ones with multiplicative reduction at p. Curves of conductor p are easily constructed by a method of Mestre [6]. In view of the lemma, this means that we can restrict ourselves to the following case.

Assume one has a Weierstrass model with discriminant Δ, for some $\Delta \in \{\pm p^2, \pm p^3, \pm p^4\}$. The c_4 and c_6 invariants of this model satisfy the relation $c_4^3 - c_6^2 = 1728\Delta$ ([1, p. 36]). Furthermore, since we are only interested in curves with additive reduction, we assume that $c_6 \equiv 0 \bmod p$. Then the relation implies that also c_4 is divisible by p. Hence these invariants yield an integral solution of the equation

$$pX^3 - Y^2 = 1728p^{-2}\Delta.$$

Analyzing this, one obtains:

Proposition 1. *If* p *is a prime number congruent to* 5 *modulo* 12, *then the only integral solutions to*

$$pX^3 - Y^2 \in \left\{\pm 1728, \pm 1728p, \pm 1728p^2\right\}$$

are the ones with $Y = 0$.

Proof. If $pm^3 - n^2 = \pm 1728$ for some integers m and n, then it follows that one of $+1728$ and -1728 must be a square modulo p. If $p \equiv 5 \bmod 12$, neither is, hence the equation has no integral solution in this case.

A similar argument works for $pX^3 - Y^2 = \pm 1728p^2$: given a solution $X = m$ and $Y = n$, one checks that both m and n are divisible by p. The integers m/p and n/p satisfy $p^2(m/p)^3 - (n/p)^2 = \pm 1728$. Again one of ± 1728 must be a square modulo p, which is not the case.

If integers m, n satisfy $pm^3 - n^2 = \pm 1728p$, then it follows that

$$\mp 3p\left(\frac{n}{8 \times 3^2 p}\right)^2 = \left(\frac{m}{\mp 3 \times 4}\right)^3 + 1.$$

Hence we obtain a solution $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ of $dy^2 = x^3 + 1$, for $d = \mp 3p$. By an elementary descent argument, Nagell [7, pp. 48–53]) showed already in 1925 that the only rational solution to this is the one with $y = 0$. This proves the proposition. □

Remark. In fact, more is true: the descent argument referred to is actually performed for $dy^2 = x^3 + 1$, where d is any integer not divisible by primes congruent to ± 1 or 7 modulo 12. (See also Nagell's beautiful review paper on the arithmetic of curves [8, p. 15].) Using the method of descent via two-isogeny, one can easily check this result of Nagell, since one does not come across nontrivial elements in a Shafarevich group (see e.g. [10, pp. 302–304]).

The proposition immediately implies, using the discussion at the beginning of this section:

Theorem 1. *If p is a prime number congruent to 5 modulo 12, then every elliptic curve over $\mathbf{Q}$ with conductor p^2 is a twist of one with conductor p.*

Corollary 1. *For the following primes $p < 1000$ no elliptic curve over $\mathbf{Q}$ with good reduction at all places except p exists:*

$$5, 29, 41, 137, 173, 257, 281, 293, 317, 401, 449, 461, 509, 521, 569,$$
$$617, 641, 761, 809, 821, 857, 881, 929, 953, 977.$$

Proof. This follows from pp. 732–733 of [2] and our theorem. □

Corollary 2. *Suppose p is a prime number of the form $u^2 + 64$ such that $3 \nmid u$. If both the class numbers of $\mathbf{Q}(\sqrt{-p})$ and $\mathbf{Q}(\sqrt{p})$ are not divisible by 3, then there exists exactly one isogeny class of elliptic curves over $\mathbf{Q}$ with conductor p^2. This is, e.g., the case for the following five primes:*

$$113, 353, 3089, 4289, 9473.$$

Proof. Combine our theorem with work of Setzer [9, p. 367]. □

3. Numerical results

As explained in the previous section, we are interested in finding Weierstrass models over $\mathbf{Q}$ whose c_4 and c_6 invariants are related by $c_4^3 - c_6^2 = \pm 1728 p^N$, for $2 \leq N \leq 4$. Given integers c_4, c_6 related like this, there is only one elliptic curve over $\mathbf{Q}$ with these invariants, namely the one given by $y^2 = x^3 - 27c_4x - 54c_6$. This model has discriminant $\pm 2^{12}3^{12}p^N$, hence it defines an elliptic curve with conductor p^2 if and only if it is not minimal at both 2 and 3. Minimality at 3 is easily checked:

Lemma 2. *Suppose c_4 and c_6 are integers satisfying $c_4^3 - c_6^2 = 1728d$ with $3 \nmid d$. Take a such that $a \equiv 2c_6 \bmod 3$ and $w = (a^3 - 2c_6)/3 - ac_4$. The curve given by $y^2 = x^3 - 27c_4x - 54c_6$ is not minimal at 3 if and only if $a^2 - c_4$ is divisible by 3 and w is divisible by 9.*

This follows, e.g., from Tate's algorithm (see [1, pp. 47–52]). Minimality at 2 is also checked using Tate's algorithm, but requires a little bit more work.

The strategy is now as follows. Given p, search for integers c_6 for which $c_6^2 \pm 1728p^N$ is a cube $(2 \leq N \leq 4)$. (By solving this modulo powers of p, one knows in advance the possibilities modulo p^2 of a solution c_6, and even modulo p^4 in case $N = 4$.) Having such a c_6, compute the corresponding c_4 and check whether the equation $y^2 = x^3 - 27c_4x \pm 54c_6$ is minimal at 2 and 3.

If not, compute a global Weierstrass minimal model corresponding to this. This was done for all (relevant) primes p such that $7 \leq p < 5000$ and all values $|c_6| \leq 250000000$. The program found 65 elliptic curves with conductor p^2, given in the following list:

Δ	a_1	a_2	a_3	a_4	a_6	c_4	c_6
7^3	1	−1	0	−37	−78	1785	75411
-7^3	1	−1	0	−2	−1	105	1323
-11^2	1	1	1	−30	−76	1441	54703
-11^3	0	−1	1	−7	10	352	−6776
-11^4	1	1	0	−2	−7	121	5203
-19^3	0	0	1	−38	90	1824	−77976
-37^2	1	−1	1	2	−2	−111	999
-37^2	1	−1	1	−1663	−25680	79809	22546431
37^3	0	1	1	−12	−17	592	10952
37^3	0	1	1	−2602	50229	124912	−44147512
-43^3	0	0	1	−860	9707	41280	−8387064
43^4	1	0	1	−39	−27	1849	20339
-47^2	1	1	1	1	−2	−47	1927
-67^3	0	0	1	−7370	243528	353760	−210408408
79^3	1	−1	0	−64	−179	3081	168507
-157^3	1	1	0	−42	125	2041	−123245
-163^3	0	0	1	−2174420	1234136692	104372160	−1066294102104
-179^2	1	−1	0	−11	−14	537	14499
-191^2	1	0	1	−92	−345	4393	291275
277^2	1	0	0	−75	−256	3601	215783
307^2	1	−1	0	−19	−24	921	24867
-359^2	1	0	1	7	−15	−359	13283
397^2	1	−1	1	−174	924	8337	−761049
-397^3	1	0	0	91	190	−4367	−157609
-431^4	1	0	0	−3870	92773	185761	−80434513
433^4	1	0	0	−3906	−93853	187489	80807759
-443^2	1	0	1	−102	−403	4873	340667
-503^2	1	0	1	10	21	−503	−17605
-673^2	1	0	0	−14	37	673	−32977
739^2	1	−1	0	−46	127	2217	−99765
-863^2	1	−1	0	−701	7322	33657	−6174765
877^3	0	−1	1	−2046	−34926	98224	30765160
-887^2	1	1	0	19	−22	−887	2572
-1069^2	1	1	1	−824	−9602	39553	7999327
-1103^2	1	0	0	23	−30	−1103	27575
-1213^2	1	0	1	−329	2265	15769	−1980829
-1259^2	1	−1	1	−79	−256	3777	237951
-1297^2	1	1	1	−27	−94	1297	71335
-1367^2	1	1	0	29	42	−1367	−25973
-1439^2	1	1	1	30	−16	−1439	24463
-1559^2	1	0	1	32	−21	−1559	20267
-1607^2	1	0	1	33	23	−1607	−17677
1753^2	1	1	0	−36	−5	1753	−8765
-1753^2	1	0	1	−37	−123	1753	103427
1777^2	1	1	1	−37	−30	1777	12439
-1879^3	1	−1	1	−9043	333258	434049	−285981921

Δ	a_1	a_2	a_3	a_4	a_6	c_4	c_6
-1907^2	1	1	1	−257882	50298256	12378337	−43550530865
-1993^2	1	0	1	−42	137	1993	−121573
1999^2	1	1	0	−291	1792	13993	−1653173
2017^2	1	1	1	−42	22	2017	−34289
2089^2	1	1	0	−43	−64	2089	39691
2251^2	1	−1	1	−141	668	6753	−546993
2689^2	1	1	1	−56	−120	2689	83359
2953^2	1	0	1	−62	−125	2953	103355
-3203^2	1	−1	0	−200	−1051	9609	951291
-3229^2	1	1	0	−10561	413370	506953	−360953765
-3313^2	1	0	0	−69	−278	3313	235223
3331^2	1	−1	0	−208	−1093	9993	989307
-3469^2	1	0	1	−940	11007	45097	−9577909
4129^2	1	0	0	−86	227	4129	−202321
-4139^2	1	1	0	−29921	1979690	1436233	−1721223845
-4201^2	1	1	0	−87	338	4201	−323477
4423^2	1	0	0	−645	6248	30961	−5444713
-4513^2	1	1	1	−94	−452	4513	356527
4597^3	1	1	1	−5842	−173646	280417	147926863

It should again be emphasized that there is no reason why this list should be complete. One way to find more examples would be to search for isogenies from the curves in the list to new ones. It turns out that there are no isogenies defined over $\mathbf{Q}$ from curves in our list to new ones, except in the cases where the curve has complex multiplication. In this case, the isogeny is from the curve in our list to its quadratic twist over $\mathbf{Q}(\sqrt{-p})$, so we do not list this isogenous curve. The search for isogenies can be done as follows. Any rational isogeny is built up from rational isogenies of prime degree. Such an isogeny of degree p corresponds to a rational point on the modular curve $X_0(p)$. If the genus of this modular curve is zero (which means $p \in \{2, 3, 5, 7, 13\}$), a good model of it can be found on pp. 238–240 of [6]. In fact we only have to look at integral points on these models, since the curves in our list and those isogenous to them have potentially good reduction, hence integral j-invariants (compare [10, Chapter VII, Proposition 5.5 and the proof of Corollary 7.2]). In this way we find three isogenies:

1. The two curves with conductor 7^2 in the list are 2-isogenous; this corresponds to the point $(-1, -2^{12})$ on the model $xy = 2^{12}$ of $X_0(2)$.
2. There is a 7-isogeny between the curves with discriminant -37^2; it corresponds to $(-1, -49)$ on the model $xy = 49$ of $X_0(7)$.
3. Our curves with discriminant 37^3 are 5-isogenous. This corresponds to the point $(1, 5^3)$ on the model of $X_0(5)$ given by $xy = 5^3$.

In case the genus of $X_0(p)$ exceeds zero, all rational points are known by work of Mazur [5, pp. 129–130]. It turns out that such points only exist for $p \in \{11, 17, 19, 37, 43, 67, 163\}$. We list the results; they do not give any new examples.

1. For $p = 11$, the isogenies can be found on p. 97 of [1]. The new curves this provides are twists of curves in our table.
2. The curves which admit a rational 17-isogeny are given on p. 80 of [1]. They have multiplicative reduction at 2.
3. The case $p = 37$ is also given on p. 80 of [1]. No twist of these curves has bad reduction at only one prime.
4. The remaining cases correspond to elliptic curves having complex multiplication. As remarked above, they are isogenous to a twist. (Compare [10, p. 265].)

Using the methods developed in his thesis [3], B. Edixhoven computed for prime numbers $p < 3500$ the number of so-called 'Weil curves' of conductor p^2 which have potentially supersingular reduction at p. He found exactly the same number of such curves as can be found in our list. However, we do not know whether these curves in our list are actually Weil curves.

4. Complex multiplication cases

An excellent reference for the theory of elliptic curves with complex multiplication is [4]. The following result may be classical (compare loc. cit., p. 35, Theorem 12.2.1):

Fact 1. *For any imaginary quadratic field K with class number one, there exists an elliptic curve over $\mathbf{Q}$ whose endomorphism ring equals the ring of integers of K, and moreover it has good reduction outside the discriminant of K.*

Of course this can be checked by merely writing down a model as desired for each of the eight well-known j-invariants involved. A much more general argument can be found in [4].

The table above contains all the complex multiplication curves (corresponding to imaginary quadratic fields with discriminant $p \geq 5$). For convenience they are listed here again (compare p. 84 of [4]).

Δ	a_1	a_2	a_3	a_4	a_6	c_4	c_6
7^3	1	−1	0	−37	−78	1785	75411
-7^3	1	−1	0	−2	−1	105	1323
-11^3	0	−1	1	−7	10	352	−6776
-19^3	0	0	1	−38	90	1824	−77976
-43^3	0	0	1	−860	9707	41280	−8387064
-67^3	0	0	1	−7370	243528	353760	−210408408
-163^3	0	0	1	−2174420	1234136692	104372160	−1066294102104

Acknowledgment

It is a pleasure to thank F. Oort for his interest in this work and for encouraging us to publish the results.

Bibliography

1. B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable.* IV, Lecture Notes in Math., vol. 476, Springer-Verlag, 1975.
2. A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–743.

3. S. J. Edixhoven, *Stable models of modular curves and applications*, Ph.D. Thesis, Math. Inst., Univ. of Utrecht, 1989.
4. B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Math., vol. 776, Springer-Verlag, 1980.
5. B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
6. J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proc. Internat. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields (Nagoya Univ., Nagoya, 1986), Katata, Japan, 1986, pp. 217–242.
7. T. Nagel, *Über die rationalen Punkte auf einigen kubischen Kurven*, Tôhoku Math. J. **24** (1925), 48–53.
8. M. T. Nagell, *L'analyse indéterminée de degré supérieur*, Mémorial des Sciences Mathématiques **39** (1929).
9. B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. **10** (1975), 367–378.
10. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, 1986.

MATHEMATICAL INSTITUTE, UNIVERSITY OF UTRECHT, BUDAPESTLAAN 6, 3508 TA UTRECHT, THE NETHERLANDS. *E-mail*: bas@math.berkeley.edu
topj@qucdn