Journal of Number Theory 202 (2019) 254–277

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Elliptic curves over the rationals with good reduction outside two odd primes

Andrzej Dąbrowski *, Tomasz Jędrzejak

Institute of Mathematics, University of Szczecin, 70-451 Szczecin, Poland

ARTICLE INFO

Article history:
Received 17 July 2018
Received in revised form 22 January 2019
Accepted 23 January 2019
Available online 18 February 2019
Communicated by A. Pal

MSC:
14G25
14H52
14G05

Keywords:
Elliptic curve
Rational point
Diophantine equation
Class number

ABSTRACT

We classify elliptic curves over $\mathbb{Q}$ with a rational point of order 2 or ≥ 4 and good reduction outside two odd primes. We also exhibit some families of elliptic curves with a rational point of order 3, collect some general existence/non-existence results, and present some information concerning upper bounds for the rank.

1. Introduction

It is well known (due to Shafarevich) that the number of isomorphism classes of elliptic curves over a given number field and having good reduction outside a finite set of primes is finite. In particular, given a positive integer N, there are only finitely many

* Corresponding author.
E-mail addresses: dabrowskiandrzej7@gmail.com, andrzej.dabrowski@usz.edu.pl (A. Dąbrowski), tjedrzejak@gmail.com (T. Jędrzejak).

https://doi.org/10.1016/j.jnt.2019.01.007
0022-314X/

isomorphism classes of elliptic curves over $\mathbb{Q}$ of conductor N. Note that modularity of elliptic curves over $\mathbb{Q}$ gives, as a trivial corollary, finiteness of the set of isogeny classes of elliptic curves of a given conductor.

The conductor N_E of an elliptic curve E over $\mathbb{Q}$ is a positive integer that encodes the primes of bad reduction. We always have $N_E|\Delta_E$ (where Δ_E denotes the discriminant of E), and prime divisors of N_E and Δ_E are the same. If $p|N_E$, then $p||N_E$ exactly if E has multiplicative reduction at p. E has additive reduction at p exactly if $p^{2+\delta_p}||N_E$, where $\delta_p = 0$ for $p \geq 5$, and $0 \leq \delta_2 \leq 6$, $0 \leq \delta_3 \leq 3$ can be calculated explicitly using Ogg-Saito formula (see [20], Appendix C16).

The online tables by Cremona [5] exhibit all elliptic curves over $\mathbb{Q}$ of conductors up to 400000, together with much additional information (torsion subgroup, rank, etc.). Let us mention that the paper by Cremona and Lingham [6] gives an explicit algorithm for finding all the elliptic curves over a number field with good reduction outside a given finite set of (nonarchimedean) primes.

Let us give an overview of known results concerning classification of elliptic curves over $\mathbb{Q}$ with good reduction outside at most two primes.

(i) $N = p^k$, with p a prime. Elliptic curves of conductors 2^k (resp. 3^k) were completely classified by Ogg [16] (resp. Hadano [9]). Setzer [19] proved, that there is an elliptic curve over $\mathbb{Q}$ of conductor p with a rational point of order 2 if and only if $p = 17$ or $p = u^2 + 64$ for some integer u. Assuming $p \equiv \pm 1 (\mathrm{mod}\ 8)$, and the class numbers of both $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$ are not divisible by 3, Setzer proved that in these cases each elliptic curve of conductor p defined over $\mathbb{Q}$ has a rational point of order 2. Edixhoven et al. [8] proved that if $p \equiv 5 (\mathrm{mod}\ 12)$, then every elliptic curve over $\mathbb{Q}$ of conductor p^2 is a twist of one of conductor p.

(ii) $N = 2^n p$, with p odd prime. Elliptic curves of conductors $2^k 3$ were completely classified by Ogg [17]. Ivorra [12] has classified elliptic curves over $\mathbb{Q}$ of conductor $2^k p$ with a rational point of order 2. Let us mention the following result by Hadano: assume $p \equiv 1, 7 (\mathrm{mod}\ 8)$, and the class numbers of the following four fields $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{2p})$ and $\mathbb{Q}(\sqrt{-2p})$ are not divisible by 3, then each elliptic curve of conductor $2^k p$ defined over $\mathbb{Q}$ has a rational point of order 2.

(iii) $N = p^m q^n$, with p, q different odd primes. Bennett, Vatsal and Yazdani [3] classified all elliptic curves over $\mathbb{Q}$ with a rational 3-torsion point and good reduction outside the set $\{3, p\}$, for a fixed prime p. It is an open problem to classify elliptic curves over $\mathbb{Q}$ with a rational 3-torsion point and good reduction outside the set $\{p, q\}$, with p and q different primes ≥ 5. In a paper by Howe [10] it is proved that if there is an elliptic curve over $\mathbb{Q}$ of odd conductor pq with a rational point of order 2, then one of the diophantine equation (from an explicit list) has a solution. In that paper, Howe also stated some general existence and non-existence results. In a recent paper by Sadek [18], the author finds all elliptic curves defined over $\mathbb{Q}$ with good reduction outside two distinct primes and a rational point of fixed order $N \geq 4$ (actually, he only finds possible minimal discriminants of such curves). It turns out that some of his claims are incomplete - for instance some curves with a rational point of order 8 are missing (see subsection 5.4).

Our paper is a common extension (and clarification) of the work given by Ogg, Hadano, Neumann, Setzer, Edixhoven-de Groot-Top, Ivorra, Bennett-Vatsal-Yazdani, Howe, Sadek and others. In sections 3 and 5, we give explicit description of elliptic curves over $\mathbb{Q}$ with good reduction outside two odd primes and a rational point of order 2 or ≥ 4, and exhibit some families of elliptic curves with a rational point of order 3. It turns out that an elliptic curve with a rational point of order 2 belongs to one of 77 (conjecturally, infinite) families or to a finite "exceptional set". Elliptic curves with a rational point of order 4 belong to one of 16 (conjecturally, infinite) families or to a finite "exceptional set". In section 6 we collect some general existence/non-existence results. In section 7 we present some information concerning upper bounds for ranks of elliptic curves of odd conductors $p^a q^b$ and with $\mathbb{Q}$-rational point of order 2.

Acknowledgment. We would like to thank the anonymous referee for useful suggestions and comments which allow to improve the final version of the article.

2. Some Diophantine equations

In this section we list some of the diophantine equations we use in the next sections.

Consider a generalized Fermat equation $x^p + y^q = z^r$, with p, q, r positive integers satisfying $1/p+1/q+1/r < 1$, and where x, y, z are coprime integers. If we fix the triple (p, q, r), then the number of solutions to such an equation is finite [7]. It is expected (commonly known as Tijdeman-Zagier conjecture) that the following ten solutions are the only solutions to the above equation:

$$1^p + 2^3 = 3^2,\ 2^5 + 7^2 = 3^4,\ 7^3 + 13^2 = 2^9,\ 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2,\ 17^7 + 76271^3 = 21063928^2,$$
$$1414^3 + 2213459^2 = 65^7,\ 9262^3 + 15312283^2 = 113^7,$$
$$43^8 + 96222^3 = 30042907^2,\ 33^8 + 1549034^2 = 15613^3.$$

Lemma 1. *([18], Lemma 2.2) There are no integer solutions (x, m, y, n) to the equation $16x^m + 1 = y^n$, where $|x|$, n are primes, $m > 1$, and $y = l^t$ with $|l|$ a prime and $t > 0$.*

The diophantine equation (Lebesgue-Nagell equation) $x^2 + C = y^n$ $(x, y \geq 1,\ n \geq 3)$ has a rich history. This equation has no solution for many values of C (see, for instance, [4], where all solutions of this equation are given when $1 \leq C \leq 100$). Barros [2] in his PhD thesis considered the range $-100 \leq C \leq -1$. Here are special cases for $C = \pm 16$ and 64.

Lemma 2. *There are no integer solutions (x, y, n), y odd, $n \geq 3$, to the equations $x^2 \pm 16 = y^n$ and $x^2 + 64 = y^n$.*

3. Elliptic curves over $\mathbb{Q}$ with good reduction outside two odd primes and a rational point of order two

Theorem 1. *Let $p \neq q$ be odd primes. Any elliptic curve E defined over $\mathbb{Q}$, of conductor $N = pq$, and with $E(\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$ is isomorphic (over $\mathbb{Q}$) to one of the following four curves of the form $Y^2 = X^3 + AX^2 + BX$:*

	A	B	Δ_E	$E(\mathbb{Q})_{tors}$		A	B	Δ_E	$E(\mathbb{Q})_{tors}$
a	14	-15	$3^2 \times 5^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	c	-2	-63	$3^4 \times 7^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
b	6	-55	$5^2 \times 11^2$	$(\mathbb{Z}/2\mathbb{Z})^2$	d	-10	-39	$3^2 \times 13^2$	$(\mathbb{Z}/2\mathbb{Z})^2$

or belongs to one of the following two families:

	A	B	*condition*	Δ_E
e	$\pm 2\sqrt{64 + p^\alpha q^\beta}$	$p^\alpha q^\beta$	$p^\alpha - q^\beta = \pm 16$	$p^{2\alpha} q^{2\beta}$
f	$\pm 2\sqrt{64p^{2a} + \varepsilon q^\beta}$	εq^β	$q^\beta - 16p^\alpha = \varepsilon$	$p^{2\alpha} q^{2\beta}$

where $\epsilon = \pm 1$ and the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

Remark. (i) Primes of the type $p = q^\beta \pm 16$ (with q another odd prime and $\beta \geq 1$) give an explicit (conjecturally, infinite) family of elliptic curves of conductor pq with three $\mathbb{Q}$-rational points of order 2. The diophantine equations $p^2 = q^\beta \pm 16$ ($\beta \geq 2$) have solutions only for $\beta = 2$ (use Lemma 2), and produce the elliptic curve $Y^2 = X^3 - 34X^2 + 225X$ of conductor 15. If we believe the (mentioned in Section 2) conjecture of Tijdeman and Zagier then there are no other solutions (and, hence, there are no corresponding elliptic curves).

(ii) Lemma 1 states that the diophantine equation $q^\beta - 16p^\alpha = \pm 1$ has only the obvious solutions $q = 16p^\alpha \pm 1$, and we obtain an explicit (conjecturally, infinite) family of elliptic curves of conductor pq with three $\mathbb{Q}$-rational points of order 2.

Theorem 2. *Let $p \neq q$ be odd primes. Any elliptic curve E defined over $\mathbb{Q}$, of conductor $N = pq$, and with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ is isomorphic (over $\mathbb{Q}$) to one of the following four curves of the form $Y^2 = X^3 + AX^2 + BX$:*

	A	B	Δ_E	$E(\mathbb{Q})_{tors}$		A	B	Δ_E	$E(\mathbb{Q})_{tors}$
a	1	16	$-3^2 \times 7$	$\mathbb{Z}/4\mathbb{Z}$	c	-3	16	-5×11	$\mathbb{Z}/2\mathbb{Z}$
b	5	16	-3×13	$\mathbb{Z}/2\mathbb{Z}$	d	-7	16	-3×5	$\mathbb{Z}/4\mathbb{Z}$

or belongs to one of the following families of elliptic curves (with $\epsilon = \pm 1$).

	A	B	*conditions*	Δ_E
ia	$\pm 2u$	q^β	$u^2 = q^\beta - 64p^{2\alpha}, \quad \pm u \equiv 3 (\mathrm{mod}\ 4)$	$-p^{2\alpha}q^{2\beta}$
ib	$\pm 2u$	$p^\alpha q^\beta$	$u^2 = p^\alpha q^\beta - 64, \quad \pm u \equiv 3 (\mathrm{mod}\ 4)$	$-p^{2\alpha}q^{2\beta}$
iia	$\pm 2u$	1	$u^2 = 64p^{2\alpha}q^{2\beta+1} + 1, \quad \pm u \equiv 3 (\mathrm{mod}\ 4)$	$p^{2\alpha}q^{2\beta+1}$
iib	$\pm 2u$	ϵp^α	$u^2 = 64q^{2\beta+1} + \epsilon p^\alpha, \quad \pm u \equiv 3 (\mathrm{mod}\ 4)$	$p^{2\alpha}q^{2\beta+1}$
iic	$\pm u$	16ϵ	$u^2 = p^{2\alpha}q^{2\beta+1} + 64\epsilon, \quad \pm u \equiv 1 (\mathrm{mod}\ 4)$	$p^{2\alpha}q^{2\beta+1}$
iid	$\pm u$	$16\epsilon p^\alpha$	$u^2 = q^{2\beta+1} + 64\epsilon p^\alpha, \quad \pm u \equiv 1 (\mathrm{mod}\ 4)$	$p^{2\alpha}q^{2\beta+1}$
iiia	$\pm 2u$	p^α	$u^2 = p^\alpha - 64q^{2\beta+1}, \quad \pm u \equiv 3 (\mathrm{mod}\ 4)$	$-p^{2\alpha}q^{2\beta+1}$
iiib	$\pm u$	$16p^\alpha$	$u^2 = 64p^\alpha - q^{2\beta+1}, \quad \pm u \equiv 1 (\mathrm{mod}\ 4)$	$-p^{2\alpha}q^{2\beta+1}$
iva	$\pm 2u$	1	$u^2 = 64p^{2\alpha+1}q^{2\beta+1} + 1, \quad \pm u \equiv 3 (\mathrm{mod}\ 4)$	$p^{2\alpha+1}q^{2\beta+1}$
ivb	$\pm u$	16ϵ	$u^2 = p^{2\alpha+1}q^{2\beta+1} + 64\epsilon, \quad \pm u \equiv 1 (\mathrm{mod}\ 4)$	$p^{2\alpha+1}q^{2\beta+1}$

Remark. It is still a conjecture that there are infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order two and of odd conductor pq (p, q different odd primes). On the other hand, there are infinitely many elliptic curves over $\mathbb{Q}$ with rational point of order two, and of conductor p or pq. It is enough to consider the Neumann-Setzer curves [19], and the (generalized Neumann-Setzer) curves (ii.d) or (v.b) above, and apply the following result of Iwaniec [13]: there are infinitely many integers n such that $n^2 + 64$ is the product of at most two primes.

Theorem 3. *Let $p \neq q$ be odd primes. Any elliptic curve E defined over $\mathbb{Q}$, of conductor $N = p^a q$ ($a \geq 2$), and with $E(\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$ is isomorphic (over $\mathbb{Q}$) to one of the following curves of the form $Y^2 = X^3 + AX^2 + BX$ (all with $E(\mathbb{Q})_{tors} \simeq (\mathbb{Z}/2\mathbb{Z})^2$):*

	A	B	Δ_E		A	B	Δ_E
a	-75	-400	$5^6 \times 17^2$	e	30	-351	$3^8 \times 13^2$
b	45	-144	$3^6 \times 17^2$	f	30	-1375	$5^8 \times 11^2$
c	-51	144	$3^8 \times 5^2$	g	14	-3087	$3^4 \times 7^8$
d	85	400	$3^2 \times 5^8$	h	-363	32912	$11^6 \times 17^2$

or belongs to one of the following families (with $\epsilon = \pm 1$):

	A	B	*conditions*	Δ_E
i	$\pm 2up$	ϵp^{m+2}	$u^2 = 64q^{2n} + \epsilon p^m, \quad \pm up \equiv 3 (\mathrm{mod}\ 4)$	$p^{2m+6}q^{2n}$
ii	$\pm 15p$	$-16p^2$	$p \neq 17, \quad \pm p \equiv 3 (\mathrm{mod}\ 4)$	$17^2 p^6$
iii	$\pm up$	$16\epsilon p^{2m+2}$	$u^2 = q^{2n} + 64\epsilon p^{2m}, \quad \pm up \equiv 1 (\mathrm{mod}\ 4)$	$p^{2m+6}q^{2n}$
iv	$\pm 2up$	$\epsilon p^2 q^n$	$u^2 = 64p^{2m} + \epsilon q^n, \quad \pm up \equiv 3 (\mathrm{mod}\ 4)$	$p^{2m+6}q^{2n}$
v	$\pm 2up$	$p^{m+2}q^n$	$u^2 = 64 + p^m q^n, \quad \pm up \equiv 3 (\mathrm{mod}\ 4)$	$p^{2m+6}q^{2n}$
vi	$\pm up$	$16\epsilon p^2 q^n$	$u^2 = p^{2m-2} + 64\epsilon q^n, \quad \pm up \equiv 1 (\mathrm{mod}\ 4)$	$p^{2m+4}q^{2n}$
vii	$\pm up$	$16p^{m+2}q^n$	$u^2 = 1 + 64p^m q^n, \quad \pm up \equiv 1 (\mathrm{mod}\ 4)$	$p^{2m+6}q^{2n}$

Remark. The conditions in (i), (iv) and (vii) lead to diophantine equations of the type $p^a - 16q^b = \pm 1$ or $q^b - 16p^a = \pm 1$. The condition in (v) leads to diophantine equation of the type $p^a - q^b = \pm 16$. The conditions in (iii) and (vi) lead to both types of diophantine equations.

Theorem 4. *Let $p \neq q$ be odd primes. Any elliptic curve E defined over $\mathbb{Q}$, of conductor $N = p^a q$ ($a \geq 2$), and with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ is isomorphic (over $\mathbb{Q}$) to one of the following curves of the form $Y^2 = X^3 + AX^2 + BX$:*

	A	B	Δ_E	$E(\mathbb{Q})_{tors}$		A	B	Δ_E	$E(\mathbb{Q})_{tors}$
a	-3	144	$-3^8 \times 7$	$\mathbb{Z}/2\mathbb{Z}$	*k*	41	656	-23×41^3	$\mathbb{Z}/2\mathbb{Z}$
b	-7	784	$-3^2 \times 7^7$	$\mathbb{Z}/4\mathbb{Z}$	*l*	-47	752	-17×47^3	$\mathbb{Z}/2\mathbb{Z}$
c	9	48	$-3^3 \times 37$	$\mathbb{Z}/2\mathbb{Z}$	*m*	53	848	-11×53^3	$\mathbb{Z}/2\mathbb{Z}$
d	-3	48	$-3^3 \times 61$	$\mathbb{Z}/2\mathbb{Z}$	*n*	-59	944	-5×59^3	$\mathbb{Z}/2\mathbb{Z}$
e	-15	80	$-5^3 \times 19$	$\mathbb{Z}/2\mathbb{Z}$	*o*	61	976	-3×61^3	$\mathbb{Z}/2\mathbb{Z}$
f	5	80	$-5^3 \times 59$	$\mathbb{Z}/2\mathbb{Z}$	*p*	21	144	$-3^7 \times 5$	$\mathbb{Z}/2\mathbb{Z}$
g	-11	176	$-11^3 \times 53$	$\mathbb{Z}/2\mathbb{Z}$	*q*	-15	144	$-3^7 \times 13$	$\mathbb{Z}/4\mathbb{Z}$
h	17	272	$-17^3 \times 47$	$\mathbb{Z}/2\mathbb{Z}$	*r*	-35	400	-3×5^7	$\mathbb{Z}/2\mathbb{Z}$
i	-23	368	$-23^3 \times 41$	$\mathbb{Z}/2\mathbb{Z}$	*s*	33	1936	-5×11^7	$\mathbb{Z}/4\mathbb{Z}$
j	37	592	$-3^3 \times 37^3$	$\mathbb{Z}/2\mathbb{Z}$	*t*	65	2704	-3×13^7	$\mathbb{Z}/4\mathbb{Z}$

or belongs to one of the following families of elliptic curves (with $\epsilon = \pm 1$)

	A	B	*conditions*	Δ_E
ia	$\pm 2up$	p^{m+2}	$u^2 = p^m - 64q^{2n}, \quad \pm up \equiv 3 \pmod 4$	$-p^{2m+6}q^{2n+6}$
ib	$\pm 2up$	p^2q^n	$u^2 + 64 = q^n, \quad \pm up \equiv 3 \pmod 4$	$-p^6q^{2n}$
ic	$\pm 2up^{m+1}$	p^2q^n	$u^2p^{2m} + 64 = q^n, \quad \pm up^{m+1} \equiv 3 \pmod 4$	$-p^6q^{2n}$
id	$\pm 2up$	p^2q^n	$u^2 + 64p^{2m} = q^n, \quad \pm up \equiv 3 \pmod 4$	$-p^{2m+6}q^{2n}$
ie	$\pm 2up$	$p^{m+2}q^n$	$u^2 + 64 = p^mq^n, \quad \pm up \equiv 3 \pmod 4$	$-p^{2m+6}q^{2n}$
iia	$\pm 66p$	p^2	$p \neq 17, \quad \pm p \equiv 3 \pmod 4$	$17p^6$
iib	$\pm 2up^{m+1}$	p^2	$u^2p^{2m} = 1 + 64q^{2n-1}, \quad \pm up^{m+1} \equiv 3 \pmod 4$	p^6q^{2n-1}
iic	$\pm 2up$	p^2	$u^2 = 1 + 64p^{2m}q^{2n-1}, \quad \pm up \equiv 3 \pmod 4$	$p^{2m+6}q^{2n-1}$
iid	$\pm 2up$	ϵp^{m+2}	$u^2 = 64q^{2n-1} + \epsilon p^m, \quad \pm up \equiv 3 \pmod 4$	$p^{2m+6}q^{2n-1}$
iie	$\pm up$	$16\epsilon p^2$	$u^2 = q^{2n-1} + 64\epsilon, \quad \pm up \equiv 1 \pmod 4$	p^6q^{2n-1}
iif	$\pm up^{m+1}$	$16\epsilon p^2$	$u^2p^{2m} = q^{2n-1} + 64\epsilon, \quad \pm up^{m+1} \equiv 1 \pmod 4$	p^6q^{2n-1}
iig	$\pm up$	$16\epsilon p^2$	$u^2 = p^{2m}q^{2n-1} + 64\epsilon, \quad \pm up \equiv 1 \pmod 4$	$p^{2m+6}q^{2n-1}$
iih	$\pm up$	$16\epsilon p^{m+2}$	$u^2 = q^{2n-1} + 64\epsilon p^m, \quad \pm up \equiv 1 \pmod 4$	$p^{2m+6}q^{2n-1}$
iiia	$\pm 2up$	p^{m+2}	$u^2 = p^m - 64q^{2n-1}, \quad \pm up \equiv 3 \pmod 4$	$-p^{2m+6}q^{2n-1}$
iva	$\pm 2up^k$	$\epsilon p^{2k-2m+1}$	$u^2p^{2m-1} = 64q^{2n} + \epsilon, \quad \pm up^k \equiv 3 \pmod 4$	$p^{6k-6m+3}q^{2n}$
ivb	$\pm 2up$	p^2	$u^2 = 1 + 64p^{2m-1}q^{2n}, \quad \pm up \equiv 3 \pmod 4$	$p^{2m+5}q^{2n}$
ivc	$\pm up^k$	$16\epsilon p^{2k-2m+1}$	$u^2p^{2m-1} = q^{2n} + 64\epsilon, \quad \pm up^k \equiv 1 \pmod 4$	$p^{6k-6m+3}q^{2n}$
ivd	$\pm up$	$16\epsilon p^2$	$u^2 = p^{2m-1}q^{2n} + 64\epsilon, \quad \pm up \equiv 1 \pmod 4$	$p^{2m+5}q^{2n}$
ive	$\pm 2up^k$	$\epsilon p^{2k-2m+1}q^n$	$u^2p^{2m-1} = 64 + \epsilon q^n, \quad \pm up^k \equiv 3 \pmod 4$	$p^{6k-6m+3}q^{2n}$
ivf	$\pm 2up$	ϵp^2q^n	$u^2 = 64p^{2m-1} + \epsilon q^n, \quad \pm up \equiv 3 \pmod 4$	$p^{2m+5}q^{2n}$
ivg	$\pm up^k$	$16p^{2k-2m+1}q^n$	$u^2p^{2m-1} = 1 + 64q^n, \quad \pm up^k \equiv 1 \pmod 4$	$p^{6k-6m+3}q^{2n}$
ivh	$\pm up$	$16\epsilon p^2q^n$	$u^2 = p^{2m-1} + 64\epsilon q^n, \quad \pm up \equiv 1 \pmod 4$	$p^{2m+5}q^{2n}$
va	$\pm 2up^k$	$p^{2k-2m+1}q^n$	$u^2p^{2m-1} = q^n - 64, \quad \pm up^k \equiv 3 \pmod 4$	$-p^{6k-6m+3}q^{2n}$
vb	$\pm 2up$	p^2q^n	$u^2 = q^n - 64p^{2m-1}, \quad \pm up \equiv 3 \pmod 4$	$-p^{2m+5}q^{2n}$
vc	$\pm up^k$	$16p^{2k-2m+1}q^n$	$u^2p^{2m-1} = 64q^n - 1, \quad \pm up^k \equiv 1 \pmod 4$	$-p^{6k-6m+3}q^{2n}$
vd	$\pm up$	$16p^2q^n$	$u^2 = 64q^n - p^{2m-1}, \quad \pm up \equiv 1 \pmod 4$	$-p^{2m+5}q^{2n}$
via	$\pm 2up^k$	$\epsilon p^{2k-2m+1}$	$u^2p^{2m-1} = 64q^{2n-1} + \epsilon, \quad \pm up^k \equiv 3 \pmod 4$	$p^{6k-6m+3}q^{2n-1}$
vib	$\pm 2up$	p^2	$u^2 = 64p^{2m-1}q^{2n-1} + 1, \quad \pm up \equiv 3 \pmod 4$	$p^{2m+5}q^{2n-1}$
vic	$\pm up^k$	$16\epsilon p^{2k-2m+1}$	$u^2p^{2m-1} = q^{2n-1} + 64\epsilon, \quad \pm up^k \equiv 1 \pmod 4$	$p^{6k-6m+3}q^{2n-1}$
vid	$\pm up$	$16\epsilon p^2$	$u^2 = p^{2m-1}q^{2n-1} + 64\epsilon, \quad \pm up \equiv 1 \pmod 4$	$p^{2m+5}q^{2n-1}$

where m, n are positive integers, and $k = m, m+1$.

Remark. There are infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order two and of odd conductor p^aq (p, q different odd primes and $a \geq 2$). Take the family (ii) in Theorem 3 or the family (iia) in Theorem 4.

Theorem 5. *Let $p \neq q$ be odd primes. Any elliptic curve E defined over $\mathbb{Q}$, of conductor $N = p^aq^b$ $(a, b \geq 2)$, and with $E(\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$ is isomorphic (over $\mathbb{Q}$) to one of the following four curves of the form $Y^2 = X^3 + AX^2 + BX$ (all with $E(\mathbb{Q})_{tors} \simeq (\mathbb{Z}/2\mathbb{Z})^2$):*

	A	B	Δ_E		A	B	Δ_E
a	918	44217	$3^6 \times 17^8$	c	-255	3600	$3^8 \times 5^8$
b	-1275	-115600	$5^6 \times 17^8$	d	-6171	9511568	$11^6 \times 17^8$

or belongs to one of the following four families (with $\epsilon = \pm 1$):

	A	B	*conditions*	Δ_E
i	$\pm 2upq$	ϵp^2q^{n+2}	$u^2 = 64p^{2m} + \epsilon q^n, \quad \pm upq \equiv 3 \pmod 4$	$p^{2m+6}q^{2n+6}$
ii	$\pm 2upq$	$\epsilon p^{m+2}q^{n+2}$	$u^2 = 64 + \epsilon p^mq^n, \quad \pm upq \equiv 3 \pmod 4$	$p^{2m+6}q^{2n+6}$
iii	$\pm 306p$	17^3p^2	$p \neq 17, \quad \pm p \equiv 3 \pmod 4$	17^8p^6
iv	$\pm upq$	$16p^{m+2}q^{n+2}$	$u^2 = 64p^mq^n + 1, \quad \pm upq \equiv 1 \pmod 4$	$p^{2m+6}q^{2n+6}$

Remark. The conditions in (i) and (iv) lead to diophantine equations of the type $p^a - 16q^b = \pm 1$ or $q^b - 16p^a = \pm 1$. The condition in (ii) leads to diophantine equations of the type $p^a \pm q^b = 16$.

Theorem 6. *Let $p \neq q$ be odd primes. Any elliptic curve E defined over $\mathbb{Q}$, of conductor $N = p^a q^b$ $(a, b \geq 2)$, and with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ is isomorphic (over $\mathbb{Q}$) to one of the following curves of the form $Y^2 = X^3 + AX^2 + BX$:*

	A	B	Δ_E	$E(\mathbb{Q})_{tors}$		A	B	Δ_E	$E(\mathbb{Q})_{tors}$
a	126	-63	$3^6 \times 7^3$	$\mathbb{Z}/2\mathbb{Z}$	l	-799	217328	$-17^7 \times 47^3$	$\mathbb{Z}/2\mathbb{Z}$
b	21	7056	$-3^8 \times 7^7$	$\mathbb{Z}/2\mathbb{Z}$	m	285	28880	$-5^3 \times 19^7$	$\mathbb{Z}/2\mathbb{Z}$
c	-63	1008	$-3^6 \times 7^3$	$\mathbb{Z}/2\mathbb{Z}$	n	-943	347024	$-23^7 \times 41^3$	$\mathbb{Z}/2\mathbb{Z}$
d	-130	65	$5^3 \times 13^3$	$\mathbb{Z}/2\mathbb{Z}$	o	333	65712	$-3^3 \times 37^7$	$\mathbb{Z}/2\mathbb{Z}$
e	65	1040	$5^3 \times 13^3$	$\mathbb{Z}/2\mathbb{Z}$	p	-943	618608	$-23^3 \times 41^7$	$\mathbb{Z}/2\mathbb{Z}$
f	165	48400	$-5^7 \times 11^7$	$\mathbb{Z}/2\mathbb{Z}$	q	-799	600848	$-17^3 \times 47^7$	$\mathbb{Z}/2\mathbb{Z}$
g	-195	24336	$-3^7 \times 13^7$	$\mathbb{Z}/2\mathbb{Z}$	r	-583	494384	$-11^3 \times 53^7$	$\mathbb{Z}/2\mathbb{Z}$
h	105	3600	$-3^7 \times 5^7$	$\mathbb{Z}/4\mathbb{Z}$	s	-295	278480	$-5^3 \times 59^7$	$\mathbb{Z}/2\mathbb{Z}$
i	-183	8784	$-3^7 \times 61^3$	$\mathbb{Z}/2\mathbb{Z}$	t	-183	178608	$-3^3 \times 61^7$	$\mathbb{Z}/2\mathbb{Z}$
j	-295	23600	$-5^7 \times 59^3$	$\mathbb{Z}/2\mathbb{Z}$	u	-111	5328	$-3^9 \times 37^3$	$\mathbb{Z}/2\mathbb{Z}$
k	-583	102608	$-11^7 \times 53^3$	$\mathbb{Z}/2\mathbb{Z}$					

or belongs to one of the following families of elliptic curves (with $\epsilon = \pm 1$)

	A	B	*conditions*	Δ_E
ia	$\pm 2up^{m+1}q$	p^2q^{n+2}	$u^2p^{2m} + 64 = q^n$, $\pm up^{m+1}q \equiv 3 \pmod 4$	$-p^6q^{2n+6}$
ib	$\pm 2upq$	$p^{m+2}q^2$	$u^2 = p^m - 64q^{2n}$, $\pm upq \equiv 3 \pmod 4$	$-p^{2m+6}q^{2n+6}$
ic	$\pm 2upq$	$p^{m+2}q^{n+2}$	$u^2 = p^mq^n - 64$, $\pm upq \equiv 3 \pmod 4$	$-p^{2m+6}q^{2n+6}$
iia	$\pm 2up^{m+1}q$	p^2q^2	$u^2p^{2m} = 64q^{2n-1} + 1$, $\pm up^{m+1}q \equiv 3 \pmod 4$	p^6q^{2n+5}
iib	$\pm 2upq$	$\epsilon p^{m+2}q^2$	$u^2 = 64q^{2n-1} + \epsilon p^m$, $\pm upq \equiv 3 \pmod 4$	$p^{2m+6}q^{2n+5}$
iic	$\pm 2upq$	p^2q^2	$u^2 = 64p^{2m}q^{2n-1} + 1$, $\pm upq \equiv 3 \pmod 4$	$p^{2m+6}q^{2n+5}$
iid	$\pm 2upq^l$	$\epsilon p^{m+2}q^{2l+1-2n}$	$u^2q^{2n-1} = 64 + \epsilon p^m$, $\pm upq^l \equiv 3 \pmod 4$	$p^{2m+6}q^{6l-6n+3}$
iie	$\pm 2upq^l$	$\epsilon p^2q^{2l+1-2n}$	$u^2q^{2n-1} = 64p^{2m} + \epsilon$, $\pm upq^l \equiv 3 \pmod 4$	$p^{2m+6}q^{6l-6n+3}$
iif	$\pm 42p$	$-7p^2$	$p \neq 7$, $\pm p \equiv 3 \pmod 4$	7^3p^6
iig	$\pm up^{m+1}q$	$16\epsilon p^2q^2$	$u^2p^{2m} = q^{2n-1} + 64\epsilon$, $\pm up^{m+1}q \equiv 1 \pmod 4$	p^6q^{2n+5}
iih	$\pm upq$	$16\epsilon p^{m+2}q^2$	$u^2 = q^{2n-1} + 64\epsilon p^m$, $\pm upq \equiv 1 \pmod 4$	$p^{2m+6}q^{2n+5}$
iii	$\pm upq$	$16\epsilon p^2q^2$	$u^2 = p^{2m}q^{2n-1} + 64\epsilon$, $\pm upq \equiv 1 \pmod 4$	$p^{2m+6}q^{2n+5}$
iij	$\pm upq^l$	$16\epsilon p^2q^{2l+1-2n}$	$u^2q^{2n-1} = p^{2m} + 64\epsilon$, $\pm upq^l \equiv 1 \pmod 4$	$p^{2m+6}q^{6l-6n+3}$
iik	$\pm upq^l$	$16p^{2m+2}q^{2l+1-2n}$	$u^2q^{2n-1} = 64p^{2m} + 1$, $\pm upq^l \equiv 1 \pmod 4$	$p^{4m+6}q^{6l-6n+3}$
$iiia$	$\pm 2upq$	$p^{m+2}q^2$	$u^2 = p^m - 64q^{2n-1}$, $\pm upq \equiv 3 \pmod 4$	$-p^{2m+6}q^{2n+5}$
$iiib$	$\pm 2upq^l$	$p^{m+2}q^{2l+1-2n}$	$u^2q^{2n-1} = p^m - 64$, $\pm upq^l \equiv 3 \pmod 4$	$-p^{2m+6}q^{6l-6n+3}$
$iiic$	$\pm upq$	$16p^{m+2}q^2$	$u^2 = 64p^m - q^{2n-1}$, $\pm upq \equiv 1 \pmod 4$	$-p^{2m+6}q^{2n+5}$
$iiid$	$\pm upq^l$	$16p^{m+2}q^{2l+1-2n}$	$u^2q^{2n-1} = 64p^m - 1$, $\pm upq^l \equiv 1 \pmod 4$	$-p^{2m+6}q^{6l-6n+3}$
$iiie$	$\pm 21p$	$112p^2$	$p \neq 7$, $\pm p \equiv 1 \pmod 4$	-7^3p^6
iva	$\pm 2upq^l$	$\epsilon p^2q^{2l+1-2n}$	$u^2q^{2n-1} = 64p^{2m-1} + \epsilon$, $\pm upq^l \equiv 3 \pmod 4$	$p^{2m+5}q^{6l-6n+3}$
ivb	$\pm 2upq$	p^2q^2	$u^2 = 64p^{2m-1}q^{2n-1} + 1$, $\pm upq \equiv 3 \pmod 4$	$p^{2m+5}q^{2n+5}$
ivc	$\pm upq^l$	$16\epsilon p^2q^{2l+1-2n}$	$u^2q^{2n-1} = p^{2m-1} + 64\epsilon$, $\pm upq^l \equiv 1 \pmod 4$	$p^{2m+5}q^{6l-6n+3}$
ivd	$\pm upq$	$16\epsilon p^2q^2$	$u^2 = p^{2m-1}q^{2n-1} + 64\epsilon$, $\pm upq \equiv 1 \pmod 4$	$p^{2m+5}q^{2n+5}$

where m, n are positive integers, and $l = n, n+1$.

Remark. There are infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order two and of odd conductor $p^a q^b$ (p, q different odd primes and $a, b \geq 2$). Take the family (iii) in Theorem 5 or the families (iif), (iiie) in Theorem 6.

4. Proofs of Theorems 1 - 6

4.1. Proofs of Theorems 1 and 2

Any semistable elliptic curve defined over $\mathbb{Q}$, with $\mathbb{Q}$-rational point of order 2, has a unique Weierstrass model of the type

$$Y^2 = X^3 + AX^2 + BX, \tag{1}$$

where $A, B \in \mathbb{Z}$ and $\gcd(A, B) = 1$ ([14], Lemme 1). This model is minimal outside 2, with the discriminant $\Delta = 2^4 B^2(A^2 - 4B)$ and $c_4 = 2^4(A^2 - 3B)$. The minimal discriminant $\Delta_E = 2^{-8} B^2(A^2 - 4B)$ (note that $c_4/16$ is odd).

Lemma 3. *We can choose A, B such that*

$$A \equiv 6 (\mathrm{mod}\ 8), \quad B \equiv 1 (\mathrm{mod}\ 8) \tag{2}$$

or

$$A \equiv 1 (\mathrm{mod}\ 4), \quad B \equiv 0 (\mathrm{mod}\ 16). \tag{3}$$

Proof. See [19], p. 374 or [14], Remarque on p. 176.

Proof of Theorem 1. Our assumptions lead to $\Delta = 2^{12} p^s q^t$, with $2 \mid s$ and $2 \mid t$ (note that Δ must be a square of a nonzero integer, since the equation $X^2 + AX + B = 0$ has two rational solutions). Hence

$$B^2(A^2 - 4B) = 2^8 p^{2\alpha} q^{2\beta}$$

with the assumption $\gcd(A, B, pq) = 1$ (since E has multiplicative reduction at p and q).

From (2) it follows that $A = 2A_0$, $A_0 \equiv 3 (\mathrm{mod}\ 4)$, hence $B^2(A_0^2 - B) = 2^6 p^{2\alpha} q^{2\beta}$ and $2^6 \mid A_0^2 - B$, $\gcd(B, A_0^2 - B) = 1$. Therefore we have the following possibilities:

$$A_0^2 - B = 64 p^{2\alpha} q^{2\beta}, \quad B = 1, \tag{4}$$

$$A_0^2 - B = 64 p^{2\alpha}, \quad B^2 = q^{2\beta} \quad (A_0^2 - B = 64 q^{2\beta}, \quad B^2 = p^{2\alpha}), \tag{5}$$

$$A_0^2 - B = 64, \quad B^2 = p^{2\alpha} q^{2\beta}. \tag{6}$$

Consider the case (4). Then we have $A_0^2-1=(A_0-1)(A_0+1)=64p^{2\alpha}q^{2\beta}$, $A_0-1\equiv 2(\mathrm{mod}\ 4)$, $32\mid A_0+1$ and $\gcd(A_0-1,A_0+1)=2$. Elementary calculations show that there exist no elliptic curve satisfying these conditions.

Consider the case (5). We have $A_0^2-64p^{2\alpha}=\pm q^\beta$. Since $(A_0-8p^\alpha)+16p^\alpha=(A_0+8p^\alpha)$, hence $\gcd(A_0-8p^\alpha,A_0+8p^\alpha,q)=1$. Moreover, $A_0-8p^\alpha\equiv A_0+8p^\alpha\equiv 3(\mathrm{mod}\ 4)$. Taking into account the above conditions, we are arriving at the following two possibilities:

$$A_0-8p^\alpha=-q^\beta \quad \text{and} \quad A_0+8p^\alpha=-1,$$
$$A_0-8p^\alpha=-1 \quad \text{and} \quad A_0+8p^\alpha=q^\beta.$$

The corresponding families of elliptic curves are given by the following models:

$$Y^2=X^3\pm 2\sqrt{2^6p^{2\alpha}+\epsilon q^\beta}X^2+\epsilon q^\beta X, \quad \text{if } q^\beta-16p^\alpha=\epsilon,$$

where $\epsilon=\pm 1$, and the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

Let us consider the remaining case (6). Here we have $A_0^2-2^6=\pm p^\alpha q^\beta$, $\gcd(A_0-8,A_0+8,pq)=1$ and $A_0-8\equiv A_0+8\equiv 3(\mathrm{mod}\ 4)$. The possibilities

$$A_0-8=-1 \quad \text{and} \quad A_0+8=15=p^\alpha q^\beta, \tag{7}$$
$$A_0-8=-p^\alpha \quad \text{and} \quad A_0+8=q^\beta, \tag{8}$$
$$A_0-8=-q^\beta \quad \text{and} \quad A_0+8=p^\alpha, \tag{9}$$

produce the four elliptic curves (a), (b), (c) and (d). The remaining cases lead to the equations $p^\alpha q^\beta=\pm 17$ (which have no solution) or $p^\alpha-q^\beta=\pm 16$. The last equations produce the family

$$Y^2=X^3\pm 2\sqrt{64+p^\alpha q^\beta}X^2+p^\alpha q^\beta X, \quad \text{if } p^\alpha-q^\beta=\pm 16,$$

where the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

We will show that the case (3) does not produce any new curve. In this case $B=16B_0$, $B_0^2(A^2-64B_0)=p^{2\alpha}q^{2\beta}$, $2\nmid B_0$, and $\gcd(B_0,A^2-64B_0)=1$. Therefore we have the following possibilities:

$$A^2-64B_0=p^{2\alpha}q^{2\beta}, \quad B_0^2=1, \tag{10}$$
$$A^2-64B_0=p^{2\alpha}, \quad B_0^2=q^{2\beta} \quad (A^2-64B_0=q^{2\beta}, \quad B_0^2=p^{2\alpha}), \tag{11}$$
$$A^2-64B_0=1, \quad B_0^2=p^{2\alpha}q^{2\beta}. \tag{12}$$

Note that (10) implies $A^2-p^{2\alpha}q^{2\beta}=\pm 64$. The equation $A^2-p^{2\alpha}q^{2\beta}=-64$ leads to conditions $p^\alpha q^\beta=\pm 17$, hence does not produce any elliptic curve. On the other hand, the equation $A^2-p^{2\alpha}q^{2\beta}=64$ leads to an elliptic curve $Y^2=X^3+17X^2+16X$ (isomorphic to (a)).

The case (11) implies $A^2 - 64q^\beta = \pm p^{2\alpha}$. From $(A - p^\alpha) + 2p^\alpha = A + p^\alpha$ it follows that one of the factors $A - p^\alpha, A + p^\alpha$ is divisible by 2^5, and the other by 2. Moreover, of course $\gcd(A - p^\alpha, A + p^\alpha, q) = 1$. Checking all the possibilities, we obtain the curves (isomorphic to) (b), (c) and (d) if $p^\alpha + q^\beta = 16$, and the following families:

$$Y^2 = X^3 \pm \sqrt{p^{2\alpha} + 64q^\beta}X^2 + 16q^\beta X, \quad \text{if } 16q^\beta - p^\alpha = 1 \quad \text{or } p^\alpha - q^\beta = -16,$$
$$Y^2 = X^3 \pm \sqrt{p^{2\alpha} - 64q^\beta}X^2 - 16q^\beta X, \quad \text{if } 16q^\beta - p^\alpha = -1 \quad \text{or } p^\alpha - q^\beta = 16,$$

where the sign before the quadratic square is chosen so that it is congruent to 1 modulo 4. If $p^\alpha - q^\beta = \pm 1$ (respectively, $16p^\alpha - q^\beta = \pm 1$), then the change of variables $x \mapsto x \pm q^\beta$, $y \mapsto y$ (respectively, $x \mapsto x - 1$, $y \mapsto y$) leads to elliptic curves from the family (e) (respectively (f)).

Let us consider the remaining case (12). The conditions $(A - 1)(A + 1) = 64p^\alpha q^\beta$, $A + 1 \equiv 2 \pmod 4$ imply $2 \mid A + 1$, $32 \mid A - 1$. Here we produce the elliptic curve $Y^2 = X^3 - 31X^2 + 240X$ (isomorphic to (a)), and the family

$$Y^2 = X^3 \pm \sqrt{64p^\alpha q^\beta + 1}X^2 + 16p^\alpha q^\beta X, \quad \text{if } 16p^\alpha - q^\beta = \pm 1 \text{ or } 16q^\beta - p^\alpha = \pm 1,$$

where the sign before the quadratic square is chosen so that it is congruent to 1 modulo 4. The change of variables $x \mapsto x + q^\beta$, $y \mapsto y$, leads to elliptic curves from the family (f).

Proof of Theorem 2. We start in the same way as in the proof of Theorem 1. Note that now Δ is not a square of a nonzero integer. Also notice that still $A_0 = A/2$ in the case (2), and $B_0 = B/16$ in the case (3) (cf. Lemma 3).

$\underline{\Delta < 0, s = 2\alpha, t = 2\beta}$. In this case we have $B^2(A^2 - 4B) = -2^8 p^{2\alpha} q^{2\beta}$, hence $B > 0$. Assume, that A, B satisfy the conditions (2). We have the following cases:

$$A_0^2 - B = -64p^{2\alpha}q^{2\beta}, \quad B = 1, \tag{13}$$
$$A_0^2 - B = -64p^{2\alpha}, \quad B = q^\beta \quad (A_0^2 - B = -64q^{2\beta}, \quad B = p^\alpha), \tag{14}$$
$$A_0^2 - B = -64, \quad B = p^\alpha q^\beta. \tag{15}$$

The case $A_0^2 - B = -1$ does not hold, since otherwise $B = 8p^\alpha q^\beta$, which contradicts the condition for B in (2). Let us consider the case (13). We have $A_0^2 - B = A_0^2 - 1 = (A_0 - 1)(A_0 + 1) = -64p^{2\alpha}q^{2\beta}$, where $A_0 - 1 \equiv 2 \pmod 4$, $A_0 + 1 \equiv 0 \pmod{32}$ and $\gcd(A_0 - 1, A_0 + 1) = 2$. Hence it is easy to see that (13) does not produce any elliptic curve.

Let us consider the case (14). We have $A_0^2 + 64p^{2\alpha} = q^\beta$. Consequently, we obtain the following models of elliptic curves:

$$Y^2 = X^3 \pm 2\sqrt{q^\beta - 64p^{2\alpha}}X^2 + q^\beta X,$$

where the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

Let us consider the case (15). Then we have $A_0^2 - p^\alpha q^\beta = -64$, and we obtain the following models of elliptic curves:

$$Y^2 = X^3 \pm 2\sqrt{p^\alpha q^\beta - 64}X^2 + p^\alpha q^\beta X,$$

where the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

Assume that A, B satisfy the conditions (3). We have the following cases:

$$A^2 - 64B_0 = -p^{2\alpha}q^{2\beta}, \quad B_0 = 1, \tag{16}$$

$$A^2 - 64B_0 = -p^{2\alpha}, \quad B_0 = q^\beta \quad (A^2 - 64B_0 = -q^{2\beta}, \quad B_0 = p^\alpha), \tag{17}$$

$$A^2 - 64B_0 = -1, \quad B_0 = p^\alpha q^\beta. \tag{18}$$

Let us consider the case (16). The corresponding equation $A^2 + p^{2\alpha}q^{2\beta} = 64$ has no solution (reduce modulo 8).

The case (17) (resp. the case (18)) leads to $A^2+p^{2\alpha} = 64q^\beta$ (resp. to $A^2+1 = 64p^\alpha q^\beta$), with no solution.

$\underline{\Delta > 0, s = 2\alpha, t = 2\beta + 1.}$

Assuming (2), we obtain $B^2(A_0^2 - B) = 64p^{2\alpha}q^{2\beta+1}$, and, in consequence:

$$A_0^2 - B = 64p^{2\alpha}q^{2\beta+1}, \quad B = 1, \tag{19}$$

$$A_0^2 - B = 64q^{2\beta+1}, \quad B = p^{2\alpha}. \tag{20}$$

The conditions (19) lead to the following pairs of equations:

$$A_0 - 1 = \pm 2p^{2\alpha} \quad \text{and} \quad A_0 + 1 = \pm 32q^{2\beta+1},$$
$$A_0 - 1 = \pm 2q^{2\beta+1} \quad \text{and} \quad A_0 + 1 = \pm 32p^{2\alpha},$$
$$A_0 - 1 = \pm 2p^{2\alpha}q^{2\beta+1} \quad \text{and} \quad A_0 + 1 = \pm 32.$$

Consequently, if $16q^{2\beta+1} - p^{2\alpha} = \pm 1$ or $16p^{2\alpha} - q^{2\beta+1} = \pm 1$, we obtain the following models of elliptic curves:

$$Y^2 = X^3 \pm 2\sqrt{64p^{2\alpha}q^{2\beta+1} + 1}X^2 + X,$$

where the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

The conditions (20) lead to the following models of elliptic curves:

$$Y^2 = X^3 \pm 2\sqrt{64q^{2\beta+1} \pm p^\alpha}X^2 \pm p^\alpha X,$$

where the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

Assume that A, B satisfy the conditions (3). Then we obtain the following classes of elliptic curves:

$$Y^2 = X^3 \pm \sqrt{p^{2\alpha}q^{2\beta+1} + 64}X^2 + 16X, \quad \text{if } p^{2\alpha} - q^{2\beta+1} = \pm 16,$$
$$Y^2 = X^3 \pm \sqrt{p^{2\alpha}q^{2\beta+1} - 64}X^2 - 16X,$$
$$Y^2 = X^3 \pm \sqrt{q^{2\beta+1} + 64p^{\alpha}}X^2 + 16p^{\alpha}X,$$
$$Y^2 = X^3 \pm \sqrt{q^{2\beta+1} - 64p^{\alpha}}X^2 - 16p^{\alpha}X,$$

where the sign before the quadratic square is chosen so that it is congruent to 1 modulo 4.

$\Delta < 0, s = 2\alpha, t = 2\beta + 1$. If we assume the conditions (2), then $B = 1$ or $B = p^{\alpha}$. The case $B = 1$ does not produce any elliptic curve. On the other hand, the case $B = p^{\alpha}$ (and conditions (2)) lead to:

$$Y^2 = X^3 \pm 2\sqrt{p^{\alpha} - 64q^{2\beta+1}}X^2 + p^{\alpha}X,$$

where the sign before the quadratic square is chosen so that it is congruent to 1 modulo 4.

The conditions (3) lead to the following models of elliptic curves:

$$Y^2 = X^3 - X^2 + 16X,$$
$$Y^2 = X^3 \pm \sqrt{64p^{\alpha} - q^{2\beta+1}}X^2 + 16p^{\alpha}X,$$

where the sign before the quadratic square is chosen so that it is congruent to 1 modulo 4.

$\Delta < 0, s = 2\alpha + 1, t = 2\beta + 1$. In this case $B^2(A^2 - 4B) = -2^8 p^{2\alpha+1}q^{2\beta+1}$. Of course $B > 0$. The conditions (2) lead to

$$A_0^2 - B = -64p^{2\alpha+1}q^{2\beta+1}, \quad B = 1,$$

hence $(A_0 - 1)(A_0 + 1) = -64p^{2\alpha+1}q^{2\beta+1}$, where $A_0 - 1 \equiv 2 (\mathrm{mod}\ 4)$ and $A_0 + 1 \equiv 0 (\mathrm{mod}\ 32)$. This case does not produce any elliptic curve.

Assume that A, B satisfy the conditions (3). Then we obtain

$$A^2 - 64B_0 = -p^{2\alpha+1}q^{2\beta+1}, \quad B_0 = 1,$$

hence $A^2 + p^{2\alpha+1}q^{2\beta+1} = 64$, where $A \equiv 1 (\mathrm{mod}\ 4)$. Consequently, we obtain the following models of elliptic curves:

$$Y^2 = X^3 + 5X^2 + 16X,$$
$$Y^2 = X^3 - 3X^2 + 16X,$$
$$Y^2 = X^3 - 7X^2 + 16X.$$

$\Delta > 0, s = 2\alpha + 1, t = 2\beta + 1$. Assuming (2) we obtain $B^2(A_0^2 - B) = 64p^{2\alpha+1}q^{2\beta+1}$, hence

$$A_0^2 - B = 2^6 p^{2\alpha+1} q^{2\beta+1}, \quad B^2 = 1.$$

$B = -1$ leads to $A_0^2 + 1 = 64p^{2\alpha+1}q^{2\beta+1}$ with no solution.

If $B = 1$, then we have the following possibilities:

$$\begin{aligned}
&A_0 - 1 = \pm 2 \quad \text{and} \quad A_0 + 1 = \pm 32 p^{2\alpha+1} q^{2\beta+1},\\
&A_0 - 1 = \pm 2 p^{2\alpha+1} \quad \text{and} \quad A_0 + 1 = \pm 32 q^{2\beta+1},\\
&A_0 - 1 = \pm 2 q^{2\beta+1} \quad \text{and} \quad A_0 + 1 = \pm 32 p^{2\alpha+1},\\
&A_0 - 1 = \pm 2 p^{2\alpha+1} q^{2\beta+1} \quad \text{and} \quad A_0 + 1 = \pm 32.
\end{aligned}$$

In this case we obtain the family of elliptic curves

$$Y^2 = X^3 \pm 2\sqrt{64p^{2\alpha+1}q^{2\beta+1} + 1}X^2 + X, \quad \text{if } p^{2\alpha+1} - 16q^{2\beta+1} = \pm 1,$$

where the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

Assuming (3) we obtain $B_0^2(A^2 - 64B_0) = p^{2\alpha+1}q^{2\beta+1}$, and hence

$$A^2 - 2^6 B_0 = p^{2\alpha+1} q^{2\beta+1}, \quad B_0^2 = 1.$$

If $B_0 = -1$, then we obtain the family of elliptic curves

$$Y^2 = X^3 \pm \sqrt{p^{2\alpha+1}q^{2\beta+1} - 64}X^2 - 16X,$$

where the sign before the quadratic square is chosen so that it is congruent to 3 modulo 4.

If $B_0 = 1$, then $(A - 8)(A + 8) = p^{2\alpha+1}q^{2\beta+1}$, when $\gcd(A - 8, A + 8, pq) = 1$, $A - 8 \equiv A + 8 \equiv 1 (\mathrm{mod}\ 4)$. In this case we obtain the family of elliptic curves

$$Y^2 = X^3 \pm \sqrt{p^{2\alpha+1}q^{2\beta+1} + 64}X^2 + 16X, \quad \text{if } p^{2\alpha+1} - q^{2\beta+1} = \pm 16,$$

where the sign before the quadratic square is chosen so that it is congruent to 1 modulo 4.

4.2. Proofs of Theorems 3 - 6

Proof of Theorem 3. Now E has additive reduction at p (so $p|\Delta_E$ and $p|c_4$). Hence, in this case, E has a unique Weierstrass model of the type $Y^2 = X^3 + AX^2 + BX$, where $A, B \in \mathbb{Z}$ with $A = ap^k$, $B = bp^l$, $\gcd(p, ab) = 1$, and $\gcd(a, b) = 1$. Our assumptions lead to $\Delta = 2^{12}p^{2\alpha}q^{2\beta}$. Hence

$$b^2(a^2p^{2k} - 4bp^l) = 2^8 p^{2\alpha-2k} q^{2\beta}$$

with the assumptions $\gcd(ab, p) = 1$, and $\gcd(a, b) = 1$. We have four cases to consider: (i) $b^2 = 1$, (ii) $b^2 = 2^8$, (iii) $b^2 = q^{2\beta}$, and (iv) $b^2 = 2^8 q^{2\beta}$.

The case (i) leads to four subcases (with $a_0 = a/2$):
$a_0^2 - 64q^{2\beta} = \pm 1$ (no solution),
$a_0^2 p^{2m} - 64q^{2\beta} = \pm 1$ (no solution),
$a_0^2 - 64p^{2m}q^{2\beta} = \pm 1$ (no solution),
$a_0^2 - 64q^{2\beta} = \epsilon p^m$ (produces the family (i)).

The case (ii) leads to four subcases:
$a^2 \pm 64 = q^{2\beta}$ (produces the family (ii)),
$a^2 p^{2m} \pm 64 = q^{2\beta}$ (produces examples (a), (b)),
$a^2 \pm 64 = p^{2m}q^{2\beta}$ (produces examples (c), (d)),
$a^2 - 64\epsilon p^{2m} = q^{2\beta}$ (produces the family (iii),

The case (iii) leads to four subcases (with $a_0 = a/2$):
$a_0^2 - 64 = \pm q^{\beta}$ (produces the family (ii)),
$a_0^2 p^{2m} - 64 = \pm q^{\beta}$ (produces an example (b),
$a_0^2 - 64p^{2m} = \epsilon q^{\beta}$ (produces the family (iv)),
$a_0^2 - 64 = \pm p^m q^{\beta}$ (produces the family (v) and examples (e), (f), (g)).

The case (iv) leads to four subcases:
$a^2 - 1 = \pm 64q^{\beta}$ (produces the family (ii)),
$a^2 p^{2m} - 1 = \pm 64q^{\beta}$ (produces examples (b), (h)),
$a^2 - p^{2m} = 64\epsilon q^{\beta}$ (produces the family (vi)),
$a^2 - 1 = \pm 64p^m q^{\beta}$ (produces the family (vii)).

The equations in (i) - (vii) have discriminants $2^{12}p^{2\alpha}q^{2\beta}$. These equations are minimal (the conductor is even) or non-minimal at 2 (the conductor is odd). To decide this we apply Tate's algorithm at 2, obtaining the conditions for $\pm up$, $\pm 2up$, etc.

Proof of Theorem 4. Follows the same lines as above.

Proof of Theorem 5. Now E has additive reduction at p and at q (so $pq|\Delta_E$ and $pq|c_4$). Hence, in this case, E has a unique Weierstrass model of the type $Y^2 = X^3 + AX^2 + BX$, where $A, B \in \mathbb{Z}$ with $A = ap^k q^l$, $B = bp^s q^t$, $\gcd(pq, ab) = 1$, and $\gcd(a, b) = 1$. Our assumptions lead to $\Delta = 2^{12}p^{2\alpha}q^{2\beta}$. Hence

$$b^2(a^2 p^{2k} q^{2l} - 4bp^s q^t) = 2^8 p^{2\alpha - 2s} q^{2\beta - 2t}$$

with the assumptions $\gcd(ab, pq) = 1$, and $\gcd(a, b) = 1$. We have two cases to consider: (i) $b^2 = 1$ and (ii) $b^2 = 2^8$. The case (i) produces an example (a), and the families (i), (ii), (iii), and the case (ii) produces examples (a), (b), (c), (d), and the family (iv). To decide the signs of $\pm p$ and $\pm upq$, we use Tate's algorithm at 2.

Proof of Theorem 6. Theorem 5 treats the case $\Delta_E = p^{2\alpha}q^{2\beta}$. Theorem 6 treats the remaining cases, and the proof follows under the same (case by case) method.

5. Elliptic curves over $\mathbb{Q}$ with good reduction outside two odd primes and a rational point of order ≥ 3

5.1. Elliptic curves over $\mathbb{Q}$ with odd conductor p^aq^b and a rational point of order 3

Bennett, Vatsal and Yazdani [3] completely characterized elliptic curves over $\mathbb{Q}$ that possess both a rational 3-torsion point and conductor 3^aq^b for nonnegative integers a and b, and q a prime > 3. They proved that such an elliptic curve E is isogenous over $\mathbb{Q}$ to a curve of the form $Y^2+a_1XY+a_3Y = X^3$, with coefficients given by explicit list of values ([3], Prop. 6.1). To do this, they first develop machinery to solve ternary Diophantine equations of the shape $Ax^n + By^n = Cz^3$ for various choices of coefficients (A, B, C). Next, they solve (among others) Diophantine equations of the type $x^n + 3^\alpha y^n = Cz^3$ for specific choices of C ([3], Theorem 1.5). When $q \not| a_1$, then there exists a nonzero integer x and a nonnegative integer m such that one of the following occurs: (i) $x^3 = q^n \pm 3^m$, (ii) $3^m x^3 = q^n \pm 1$, (iii) $x^3 = 3^m q^n \pm 1$. They use Theorem 1.5 to conclude that the largest prime factor of n is at most 3. Such a reduction is crucial for the proof of Proposition 6.1.

The next task is to characterize elliptic curves over $\mathbb{Q}$ that possess both a rational 3-torsion point and a conductor p^aq^b for any different odd primes $p, q \geq 5$, and $1 \leq a, b \leq 2$. In general, it is a difficult problem. Variants of the equations (i) - (iii) above lead to new cases of Diophantine equations $Ax^n + By^n = Cz^3$, which are very difficult to solve.

Below we exhibit several families of semistable elliptic curves over $\mathbb{Q}$ that possess a rational point of order 3 of conductor pq, where p and q are different primes > 3. First let us observe the following easy result.

Lemma 4. *Assume that an elliptic curve (over $\mathbb{Q}$) $E : Y^2 + a_1XY + a_3Y = X^3$ has conductor $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, with $p_1, \dots, p_k$ different primes ≥ 5. If $v_{p_i}(a_1) = 0$ for all $i = 1, \dots, k$, then E is semistable.*

Proof. We have $c_4 = a_1(a_1^3 - 27a_3)$ and $\Delta = a_3^3(a_1^3 - 27a_3) = \pm p_1^{\beta_1} \dots p_k^{\beta_k}$. It is easy to observe that $v_{p_i}(a_1) = 0$ implies $v_{p_i}(c_4) = 0$, and the assertion follows.

Theorem 7. *The following families give elliptic curves over $\mathbb{Q}$ of conductor pq and a rational point of order 3.*

(i) $Y^2 + (p^k + 3)XY + Y = X^3$, where p and $q = p^{2k} + 9p^k + 27$ are primes ≥ 5,

(ii) $Y^2 + aXY + pY = X^3$, where p and $q = 27p - a^3$ are primes ≥ 5,

Proof. The minimal discriminants are pq in case (i) and $-p^3q$ in case (ii), respectively. In both cases, the point $(0, 0)$ has order 3.

Remark. The families in Theorem 7 have the torsion subgroups isomorphic to $\mathbb{Z}/3\mathbb{Z}$ (use the results of Sadek [18] that there are no elliptic curves over $\mathbb{Q}$ of conductor odd pq and a rational point of order 6 or 9).

5.2. Elliptic curves over $\mathbb{Q}$ with odd conductor p^aq^b and a rational point of order 4

Theorem 8. *Any elliptic curve E over $\mathbb{Q}$ with odd $N_E = pq$ and $E(\mathbb{Q})[4] \neq \{0\}$ is isomorphic (over $\mathbb{Q}$) to one of the following curves of the form $Y^2 = X^3 + AX^2 + BX$:*

A	B	Δ_E	$E(\mathbb{Q})_{tors}$	A	B	Δ_E	$E(\mathbb{Q})_{tors}$
14	-15	$3^2 \times 5^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	54	25	$5^4 \times 11$	$\mathbb{Z}/4\mathbb{Z}$
-2	-63	$3^4 \times 7^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	1	16	$-3^2 \times 7$	$\mathbb{Z}/4\mathbb{Z}$
-34	225	$3^4 \times 5^4$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	6	841	-13×29^4	$\mathbb{Z}/4\mathbb{Z}$
14	625	$-3^2 \times 5^8$	$\mathbb{Z}/8\mathbb{Z}$	62	1	3×5	$\mathbb{Z}/4\mathbb{Z}$
38	169	3×13^4	$\mathbb{Z}/4\mathbb{Z}$	-7	16	-3×5	$\mathbb{Z}/4\mathbb{Z}$
46	81	$3^8 \times 7$	$\mathbb{Z}/8\mathbb{Z}$				

or belongs to one of the following families

A	B	*conditions*	Δ_E
$-2(p^{2m} - 16)$	$(p^{2m} + 16)^2$	$q = p^{2m} + 16$	$-p^{2m}q^4$
$2(16p^{2m} - 1)$	$(16p^{2m} + 1)^2$	$q = 16p^{2m} + 1$	$-p^{2m}q^4$
$2p^m + 64$	p^{2m}	$p^m + 16 = q^{2n-1}, \quad q \equiv 3 (\mathrm{mod}\ 4)$	$p^{4m}q^{2n-1}$
$p^{2m} + 8$	16	$q = p^{2m} + 16$	$p^{2m}q$
$1 + 8p^m$	$16p^{2m}$	$q^{2n-1} = 16p^m + 1$	$p^{4m}q^{2n-1}$
$-2(p^m - 32)$	p^{2m}	$p^m = q^{2n-1} + 16, \quad q \equiv 1 (\mathrm{mod}\ 4)$	$-p^{4m}q^{2n-1}$
$1 - 8p^m$	$16p^{2m}$	$q^{2n-1} = 16p^m - 1$	$-p^{4m}q^{2n-1}$

where m, n are positive integers.

Theorem 9. *Any elliptic curve E over $\mathbb{Q}$ with odd $N_E = p^aq$ $(a \geq 2)$ and $E(\mathbb{Q})[4] \neq \{0\}$ is isomorphic (over $\mathbb{Q}$) to one of the following five curves of the form $Y^2 = X^3 + AX^2 + BX$ with $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/4\mathbb{Z}$:*

A	B	Δ_E	A	B	Δ_E
-7	784	$-3^2 \times 7^7$	65	2704	-3×13^7
-15	144	$-3^7 \times 13$	582	9	$3^7 \times 7^2$
33	1936	-5×11^7			

or belongs to one of the following families of elliptic curves

A	B	*conditions*	Δ_E
$p\,(p-8)$	$16p^2$	$p = 16 + q^{2n}$	p^7q^{2n}
$2p\left(1+16p^{2m-1}\right)$	p^2q^{2n}	$q^n = 16p^{2m-1} - 1, \quad p \equiv 3 \pmod 4$	$p^{2m+5}q^{4n}$
$p\,(1+8q^n)$	$16p^2q^{2n}$	$16q^n = p^{2m-1} - 1, \quad p \equiv 1 \pmod 4$	$p^{2m+5}q^{4n}$
$2p\left(16p^{2m-1}-1\right)$	p^2q^{2n}	$q^n = 16p^{2m-1} + 1, \quad p \equiv 1 \pmod 4$	$-p^{2m+5}q^{4n}$
$p\,(8q^n-1)$	$16p^2q^{2n}$	$16q^n = p^{2m-1} + 1, \quad p \equiv 3 \pmod 4$	$-p^{2m+5}q^{4n}$
$2p\left(32p^{2m-1}+1\right)$	p^2	$q^{2n-1} = 16p^{2m-1} + 1, \quad p \equiv 3 \pmod 4$	$p^{2m+5}q^{2n-1}$
$2p\left(32p^{2m-1}-1\right)$	p^2	$q^{2n-1} = 16p^{2m-1} - 1, \quad p \equiv 1 \pmod 4$	$p^{2m+5}q^{2n-1}$
$p\left(p^{2m-1}-8\right)$	$16p^2$	$p^{2m-1} = q^{2n-1} + 16$	$p^{2m+5}q^{2n-1}$
$p\left(p^{2m-1}+8\right)$	$16p^2$	$p^{2m-1} = q^{2n-1} - 16$	$p^{2m+5}q^{2n-1}$

where m, n are positive integers.

Theorem 10. *If E is an elliptic curve over $\mathbb{Q}$ with odd $N_E = p^aq^b$ $(a, b \geq 2)$ and $E(\mathbb{Q})[4] \neq \{0\}$, then E is isomorphic (over $\mathbb{Q}$) to the curve $Y^2 = X^3 + 105X^2 + 3600X$ of the (minimal) discriminant $\Delta = -3^7 \times 5^7$.*

Proof. For the proofs of Theorems 8, 9 and 10, we consider all elliptic curves listen in Theorems 1 - 6, and check whether exists a point $P \in E(\mathbb{Q})$ such that $2P$ has order two or not. Let $E : Y^2 = X^3 + AX^2 + BX$. Existence of a point $P \in E(\mathbb{Q})$ such that $2P = (0, 0)$ leads to the conditions (and is equivalent to) (i) B is a square of an integer, (ii) at least one of the numbers $A \pm 2\sqrt{B}$ is a square of an integer. If E has three points of order two ($(0, 0)$, P_1, and P_2, say), then we have additionally to consider the equations $2P = P_i$, $i = 1, 2$.

5.3. Elliptic curves over $\mathbb{Q}$ with odd conductor p^aq^b and a rational point of order 5

Theorem 11. *If E is an elliptic curve over $\mathbb{Q}$ with (possibly even) $N_E = p^aq^b$ and $E(\mathbb{Q})[5] \neq \{0\}$, then E is isomorphic to one of the following curves of the form $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2$ with $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z}$:*

	a_1	a_2	a_3	N_E		a_1	a_2	a_3	N_E
a	3	2	4	38	g	8	7	49	203
b	5	4	16	58	h	1	−2	−4	50
c	9	8	64	50	i	6	−7	−49	175
d	4	3	9	75	j	14	13	169	325
e	10	9	81	57	k	38	37	1369	1147
f	6	5	25	155					

or belongs to one of the following two families of elliptic curves with odd conductor pq $(p \neq 5)$

	a_1	a_2	a_3	*conditions*	Δ_E
l	q^v-1	$-q^v$	$-q^{2v}$	$p^{2k+1}=q^{2v}+11q^v-1,\ k,v\geq 0$	$-p^{2k+1}q^{5v}$
m	q^v+1	q^v	q^{2v}	$p^{2k+1}=q^{2v}-11q^v-1,\ k,v\geq 0$	$p^{2k+1}q^{5v}$

We will use the following elementary result.

Lemma 5. *The equation* $1+11q^v-q^{2v}=p^u$ *has exactly seven solutions in positive integers* u,v *and primes* p,q*:*

q	v	p	u	q	v	p	u
2	1	19	1	3	2	19	1
2	2	29	1	5	1	31	1
2	3	5	2	7	1	29	1
3	1	5	2				

Proof. Easy calculations.

Proof of Theorem 11. Less explicit version of this theorem is also given in [18]; below we give independent and short proof of this result.

Any elliptic curve over $\mathbb{Q}$, with a rational 5-torsion point is isomorphic to a curve $E: Y^2+(1-c)XY-cY=X^3-cX^2$, where c is any nonzero rational number [11]. Writing $c=a/b$, $(a,b\in\mathbb{Z}, b>0, \gcd(a,b)=1)$ we obtain $E: Y^2+(b-a)XY-ab^2Y=X^3-abX^2$. We have $\Delta_E=a^5b^5(a^2-11ab-b^2)$.

Assume $\Delta_E=\pm p^\alpha q^\beta$. The case $a^2-11ab-b^2=\pm 1$ does not produce any elliptic curve of conductor p^nq^m. The remaining case we divide into two subcases.

(i) $a=1$, $b=q^v$, $1-11q^v-q^{2v}=\pm p^u$. Of course, $1-11q^v-q^{2v}<0$.

Assuming $p=5$, we deduce $u=2$, $q=2$, $v=1$ or $u=3$, $q=7$, $v=1$, and obtain the elliptic curves (h) and (i).

Assume $p\neq 5$. It turns out that the equation $q^{2v}+11q^v-p^u-1=0$ has no solution in primes $p\neq 5$ and q, if $u=2k$. The case $u=2k+1$ leads to the family (l).

(ii) $a=-1$, $b=q^v$, $1+11q^v-q^{2v}=\pm p^u$. The equation $1+11q^v-q^{2v}=p^u$ has exactly seven solutions with $u,v\geq 1$ and p,q primes (cf. Lemma 5). The corresponding elliptic curves are given by (a),...,(g).

Consider the equation $1+11q^v-q^{2v}=-p^u$. Assuming $p=5$, we deduce $u=2$, $q=13$, $v=1$; the corresponding elliptic curve is (j). Now assume $p\neq 5$. It turns out that the equation $q^{2v}-11q^v-1-p^u=0$ has no solution in primes p,q, $p\neq 5$, if $u=2k+2$. The case $u=2$ leads to the elliptic curve (k): $p=31$, $q=37$, $u=2$, $v=1$. The case $u=2k+1$ leads to the family (m).

We have $c_4=q^{4v}+12q^{3v}+14q^{2v}-12q^v+1=p^{4k+2}-10q^vp^{2k+1}+5q^{2v}$ in case (l), and $c_4=q^{4v}+-2q^{3v}+14q^{2v}+12q^v+1=p^{4k+2}+10q^vp^{2k+1}+5q^{2v}$ in case (m). Therefore, if $p\neq 5$, then the elliptic curves from families (l) and (m) have multiplicative reductions at p and q.

Remark. We expect that the family (l) consists of the curves with $k = 0$ only. Similarly for the family (m). It leads to the following question, which may be of independent interest.

Question. Let p be an odd prime, different from 5. Does the equation $t^2 - 125 = 4p^{2k+1}$ has any solution in positive integers t, k?

5.4. Elliptic curves over $\mathbb{Q}$ with odd conductor p^aq^b and a rational point of order ≥ 6

From the results of Sadek [18] it follows that there are no elliptic curves over $\mathbb{Q}$ of odd conductor p^aq^b and a rational point of order ≥ 6. On the other hand, it is easy to check that, for instance, the curves $A : Y^2 = X^3 + 14X^2 + 625X$ (with $\Delta = -3^2 \times 5^8$) and $B : Y^2 = X^3 + 46X^2 + 81X$ (with $\Delta = 3^8 \times 7$) both have a rational point of order 8. We have checked, using Theorems 8 - 10, that these are the only elliptic curves over $\mathbb{Q}$ of odd conductor p^aq^b and a rational point of order 8.

Proof of Theorem 3.7 in [18] is erroneous, since the Weierstrass equations considered there are, in general, not minimal. For instance, the curve A has non-minimal model $y^2 - 14xy - 120y = x^3 - 20x^2$ (i.e. $s = 1$, $t = 6$), and in this case the proof in [18] doesn't work. The same for the second curve B.

6. Existence and non-existence of elliptic curves over $\mathbb{Q}$ with certain odd conductors p^aq^b

The following results by Howe [10] concern the problem of existence/non-existence of elliptic curves over $\mathbb{Q}$ with certain odd conductors pq, and generalize Theorems 1 and 3 from [19]. Proofs of these results use the methods of Ogg [16] [17] and Setzer [19], applying in particular basic class field theory.

Theorem 12. *([10], Theorem 4.8) Let $N = pq$, with $p \neq q$, and $p, q \equiv \pm 1 \pmod 8$. Assume that the class numbers of the quadratic fields $\mathbb{Q}(\sqrt{\pm p})$, $\mathbb{Q}(\sqrt{\pm q})$, and $\mathbb{Q}(\sqrt{\pm pq})$ are not divisible by 3. Then any elliptic curve over $\mathbb{Q}$ of conductor N has a rational point of order 2.*

Theorem 13. *([10], Theorem 6.1) Assume that p, q are distinct primes satisfying $p \equiv 7 \pmod{16}$, $q \equiv 15 \pmod{16}$. Assume furthermore that the class numbers of the quadratic fields $\mathbb{Q}(\sqrt{\pm p})$, $\mathbb{Q}(\sqrt{\pm q})$, and $\mathbb{Q}(\sqrt{\pm pq})$ are not divisible by 3. Then there are no elliptic curves over $\mathbb{Q}$ of conductor pq.*

Edixhoven, de Groot and Top in [8] considered elliptic curves over $\mathbb{Q}$ with bad reduction at only one prime p and proved *inter alia* that for $p \equiv 5 \pmod{12}$ any such a curve with conductor p^2 is a twist of one with conductor p. Here we prove analogous result for elliptic curves with conductor p^2q^2.

Let p and q be distinct prime numbers greater than 3. Given an elliptic curve over the rationals with additive reduction at p and q, and good reduction at all other primes (i.e. with the conductor p^2q^2), one can twist it over quadratic extension of $\mathbb{Q}$ unramified outside $\{p, q\}$. The discriminant of the resulting elliptic curve is a product of powers of p and q as well. Moreover, we have the following

Lemma 6. *Let $p, q \geq 5$ be distinct primes and K be the quadratic extension of $\mathbb{Q}$ unramified outside $\{p, q\}$. Then up to quadratic twist over K all elliptic curves over $\mathbb{Q}$ with good reduction away from p and q are*

(i) the ones with multiplicative reduction at p and q,

(ii) the ones with multiplicative reduction at p and additive reduction at q or vice versa,

(iii) the ones with discriminant $\pm p^i q^j$, where $i, j \in \{2, 3, 4\}$.

Proof. We proceed similarly as in the proof of Lemma 1 in [8]. We omit the details.

Now we present an auxiliary diophantine result.

Lemma 7. *If p and q are distinct primes congruent to 5 modulo 12 and $\left(\frac{p}{q}\right) = 1$, then the diophantine equation*

$$pqx^3 - y^2 = \pm 1728 p^s q^t, \text{ where } s, t \in \{0, 1, 2\} \tag{21}$$

has no integer solution (x, y) with $y \neq 0$.

Proof. Since $p \equiv 5 \pmod{12}$, by quadratic reciprocity laws we get $-1 = (\frac{2}{3}) = (\frac{p}{3}) = (\frac{3}{p})$, and the same holds for q. Consequently, $\left(\frac{\pm 1728}{p}\right) = \left(\frac{\pm 1728q}{p}\right) = \left(\frac{\pm 1728}{q}\right) = \left(\frac{\pm 1728p}{q}\right) = -1$. If (21) has a solution for $s = 0$, then $-y^2 \equiv \pm 1728 q^t \pmod{p}$, so $\pm 1728 q^t$ must be a square modulo p, but it is not true. If $t = 0$, then we obtain a contradiction by the same way. Assume now that (21) has a solution (x, y) for $s = 2$. Then p divides y, and so p divides x too. Putting $x' = x/p$, $y' = y/p$, we get $p^2 q x'^3 - y'^2 = \pm 1728 q^t$. Hence again $\pm 1728 q^t$ must be a square modulo p which is impossible. The similar argument holds for $t = 2$. Now assume that $pqx^3 - y^2 = \pm 1728pq$ has a solution (x, y). Then $y = pqy'$ for some integer y'. Consequently $pqy'^2 = x^3 \mp 1728$, and we obtain the rational affine point on the quadratic twist of the elliptic curve $Y^2 = X^3 + 1$ by $\mp 3pq$. Nagell [15] showed that if an integer d is not divisible by primes congruent to ± 1 or 7 modulo 12 then the only rational solution of $dy^2 = x^3 + 1$ is the one with $y = 0$. Therefore the assertion follows.

The above two lemmata imply:

Theorem 14. *If p and q are distinct primes congruent to 5 modulo 12 and $\left(\frac{p}{q}\right) = 1$, then every elliptic curve over $\mathbb{Q}$ with conductor p^2q^2 is a twist of one with conductor pq, p^2q or pq^2.*

Proof. Suppose that such elliptic curve do not come from the ones with multiplicative reduction at p or at q. Then by Lemma 6, it has discriminant $\Delta = \pm p^i q^j$, where $i, j \in \{2, 3, 4\}$. Moreover, the invariants c_4 and c_6 satisfy the relation $c_4^3 - c_6^2 = 1728\Delta$, and by assumption p and q divide c_4. Consequently also p and q divide c_6, and we obtain equation (21). But by Lemma 7, this equation has no nontrivial integral solution, and we are done.

7. Upper bounds for the ranks

Here we present some information about upper bounds for ranks of elliptic curves E defined over $\mathbb{Q}$ of odd conductor $N_E = p^a q^b$ $(a, b \geq 1)$ and with a $\mathbb{Q}$-rational point of order 2. If E has three $\mathbb{Q}$-rational points of order 2 and $N_E = pq$, we also compute the coefficients $a_p(E)$ and $a_q(E)$ explicitly (where $a_l(E) := l + 1 - \#E(\mathbb{F}_l)$ for any prime l, and any elliptic curve E over $\mathbb{Q}$), and consequently we (conjecturally) determine the ranks. We start with the following

Lemma 8. *Let E be an elliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order 2. Let m and n denote the number of primes of multiplicative and additive reduction of E respectively. Then rank $(E(\mathbb{Q})) \leq m + 2n - 1$.*

Proof. It follows by descent via 2-isogeny. See also ([1], Prop. 1.1).

We immediately obtain the following corollaries.

Corollary 1. *Any elliptic curve E over $\mathbb{Q}$ of conductor pq and with a $\mathbb{Q}$-rational point of order 2 has rank ≤ 1.*

Corollary 2. *Any elliptic curve E over $\mathbb{Q}$ of conductor $p^a q$ $(a > 1)$ and with a $\mathbb{Q}$-rational point of order 2 has rank ≤ 2.*

Corollary 3. *Any elliptic curve E over $\mathbb{Q}$ of conductor $p^a q^b$ $(a, b > 1)$ and with a $\mathbb{Q}$-rational point of order 2 has rank ≤ 3.*

Now we restrict to the case when $N_E = pq$ and E has three $\mathbb{Q}$-rational points of order 2 (i.e., to the curves from Theorem 1). It is easy to check using Magma (or find in Cremona online tables [5]) that the elliptic curves a)-d) from Theorem 1 all have rank 0. For the elliptic curves given by e) and f) we have the following results which allow us to compute their ranks under the parity conjecture.

Proposition 1. *Let* $E_1 : Y^2 = X^3 \pm 2\sqrt{64 + p^\alpha q^\beta}X^2 + p^\alpha q^\beta X$, *where* $p^\alpha - q^\beta = \pm 16$, *and* $E_2 : Y^2 = X^3 \pm 2\sqrt{64p^{2\alpha} + \epsilon q^\beta}X^2 + \epsilon q^\beta X$, *where* $q^\beta - 16p^\alpha = \epsilon$, *be the curves given by e) and f) in Theorem 1. Then*

$$a_p(E_1) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } \alpha \text{ is even} \\ -1 & \text{if } p \equiv 3 \pmod 4 \text{ and } \alpha \text{ is odd,} \end{cases}$$

$$a_q(E_1) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4 \text{ or } \beta \text{ is odd} \\ -1 & \text{if } q \equiv 3 \pmod 4 \text{ and } \beta \text{ is even,} \end{cases}$$

$$a_p(E_2) = 1,$$

$$a_q(E_2) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4 \\ -1 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. First consider the family $E_1 : Y^2 = X^3 + AX^2 + BX$, where $A = 2\eta\sqrt{64 + p^\alpha q^\beta}$, $B = p^\alpha q^\beta$, $\eta = \pm 1$ and $\eta\sqrt{64 + p^\alpha q^\beta} \equiv 3 \pmod 4$. Without loss of generality $p^\alpha - q^\beta = 16$ (in the case $p^\alpha - q^\beta = -16$ we switch p and q). Note that $A = 2\eta(p^\alpha - 8) = 2\eta(q^\beta + 8)$, in particular $\eta p^\alpha \equiv \eta q^\beta \equiv 3 \pmod 4$. Hence the curve E_1 after reduction modulo p has the form $Y^2 = X^2(X - 16\eta)$. Then

$$\#E_1(\mathbb{F}_p) = 1 + \sum_{x=0}^{p-1}\left(1 + \left(\frac{x^2(x - 16\eta)}{p}\right)\right)$$

$$= 1 + p + \sum_{x=1}^{p-1}\left(\frac{x - 16\eta}{p}\right) = 1 + p - \left(\frac{-\eta}{p}\right),$$

hence $a_p(E_1) = \left(\frac{-\eta}{p}\right)$. Similarly, E_1 modulo q is $Y^2 = X^2(X + 16\eta)$, so $a_q(E_1) = \left(\frac{\eta}{q}\right)$. Since $a_p(E_1) = 1 \Leftrightarrow \eta = -1$ or $\eta = 1$ and $p \equiv 1 \pmod 4$, we obtain the above formula for $a_p(E_1)$. In similar way, we get the formula for $a_q(E_1)$. Now consider the curve E_2 i.e., $A = 2\eta\sqrt{64p^{2\alpha} + \varepsilon q^\beta}$ and $B = \varepsilon q^\beta$, where $q^\beta - 16p^\alpha = \varepsilon = \pm 1$. Then $A = 2\eta(8p^\alpha + \varepsilon) = \eta\left(q^\beta + \varepsilon\right)$, in particular $\eta\varepsilon \equiv 3 \pmod 4$ hence $\varepsilon = -\eta$. Then reducing modulo p we have $Y^2 = X(X - 1)^2$, so $a_p(E_2) = 1$, and modulo q we obtain $Y^2 = X^2(X - 1)$, hence $a_q(E_2) = \left(\frac{-1}{q}\right)$, and the assertion follows.

Corollary 4. *Let* $w(E_i) = \pm 1$ *denote the global root number of* E_i $(i = 1, 2)$. *Then* $w(E_1) = -a_p(E_1)\,a_q(E_1) = -1$ *if and only if* $q \equiv 1 \pmod 4$, *and* $w(E_2) = -a_q(E_2) = -1$ *if and only if* $q \equiv 1 \pmod 4$. *Therefore under the parity conjecture*

$$rank(E_1(\mathbb{Q})) = \begin{cases} 0 & \text{if } q \equiv 3 \pmod 4, \\ 1 & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

$$rank\left(E_2\left(\mathbb{Q}\right)\right) = \begin{cases} 0 & \text{if } q \equiv 3 \pmod 4, \\ 1 & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

In particular, the curve E_2 with $\varepsilon = -1$ has always rank zero.

References

[1] J. Aguirre, Á. Lozano-Robledo, J.C. Peral, Elliptic curves of maximal rank, Rev. Mat. Iberoam. (2010) 1–28, Proceedings of the Conference "Segundas Jornadas de Teoria de Números".
[2] C.F. Barros, On the Lebesgue-Nagell Equation and Related Subjects, PhD Thesis, University of Warwick, 2010.
[3] M.A. Bennett, V. Vatsal, S. Yazdani, Ternary Diophantine equations of signature $(p, p, 3)$, Compos. Math. 140 (2004) 1399–1416.
[4] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations II. The Lebesgue-Nagell equation, Compos. Math. 142 (2006) 235–265.
[5] J. Cremona, Elliptic curve data, http://www.warwick.ac.uk/~masgaj/ftp/data/INDEX.html.
[6] J. Cremona, M. Lingham, Finding all elliptic curves with good reduction outside a given set of primes, Exp. Math. 16 (2007) 303–312.
[7] H. Darmon, A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. Lond. Math. Soc. 27 (1995) 513–543.
[8] B. Edixhoven, A. de Groot, J. Top, Elliptic curves over the rationals with bad reduction at only one prime, Math. Comp. 189 (1990) 413–419.
[9] T. Hadano, On the conductor of an elliptic curve with a rational point of order 2, Nagoya Math. J. 53 (1974) 199–210.
[10] S. Howe, On Elliptic Curves of Conductor $N = PQ$, Bachelor's thesis, University of Arizona, 2010.
[11] D. Husemöller, Elliptic Curves, Graduate Texts in Math., vol. 111, Springer-Verlag, 1987.
[12] W. Ivorra, Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^N p$, Dissertationes Math. 429 (2004) 1–55.
[13] H. Iwaniec, Almost primes represented by quadratic polynomials, Invent. Math. 47 (1978) 171–188.
[14] J.-F. Mestre, J. Oesterlé, Courbes de Weil semi-stables de discriminant une puissance m-ième, J. Reine Angew. Math. 400 (1989) 173–184.
[15] M.T. Nagell, L'analyse indeterminee de degre superieur, Méml. Sci. Math. 39 (1929).
[16] A.P. Ogg, Abelian curves of 2-power conductor, Proc. Camb. Philos. Soc. 62 (1966) 143–148.
[17] A.P. Ogg, Abelian curves of small conductor, J. Reine Angew. Math. 226 (1967) 204–215.
[18] M. Sadek, On elliptic curves whose conductor is a product of two prime powers, Math. Comp. 83 (2014) 447–460.
[19] B. Setzer, Elliptic curves of prime conductor, J. Lond. Math. Soc. 10 (1975) 367–378.
[20] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math., vol. 106, Springer-Verlag, 1986.