Introduction

Soient p un nombre premier impair et N un entier naturel. On s'intéresse dans ce travail au problème suivant :

PROBLÈME 1. *Déterminer toutes les classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$.*

D'après les résultats de I. Papadopoulos ([Pa]) ou bien de P. Lockhart, M. Rosen et J. H. Silverman ([LRS]), il n'existe pas de courbes elliptiques définies sur $\mathbb{Q}$ dont le conducteur soit divisible par 2^9. On supposera donc dans toute la suite que

$$0 \leq N \leq 8.$$

Par ailleurs, d'après le théorème de Shafarevich, il n'existe qu'un nombre fini de telles classes d'isomorphisme ([Si, p. 263]). Dans le cas où N est nul, B. Setzer a obtenu en 1974 le résultat ci-dessous (cf. [Se]) :

THÉORÈME. *Soit p un nombre premier distinct de 17. Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur p et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si $p-64$ est un carré dans $\mathbb{Z}$. Dans ce cas, il existe à $\mathbb{Q}$-isomorphisme près deux telles courbes elliptiques. Des équations de ces courbes sont*

$$y^2 = x^3 + \sqrt{p-64}\,x^2 - 16x, \qquad y^2 = x^2 - 2\sqrt{p-64}\,x^2 + px,$$

où $\sqrt{p-64}$ désigne la racine carrée de $p-64$ congrue à 1 modulo 4.

Des modèles minimaux de ces courbes sont donnés par les équations

$$y^2 + xy = x^3 + \left(\frac{\sqrt{p-64}-1}{4}\right)x^2 - x,$$
$$y^2 + xy = x^3 + \left(\frac{\sqrt{p-64}-1}{4}\right)x^2 + 4x + \sqrt{p-64},$$

pour lesquelles les discriminants sont respectivement p et $-p^2$. Il se trouve aussi dans [Se] la liste des quatre classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ qui sont de conducteur 17.

Dans ce travail, on obtient des résultats analogues au théorème de Setzer pour les entiers $N \leq 8$. Pour cela, on est principalement confronté, comme dans *loc. cit.*, au problème de la détermination des solutions entières de certaines équations diophantiennes ternaires (cf. le paragraphe 2.2). Un problème typique auquel on est conduit est celui de la détermination, pour tous les entiers naturels r et s non nuls, des entiers $x \in \mathbb{Z}$ vérifiant

l'égalité

$$x^2 - 2^r = p^s.$$

Si $r = 1$, en utilisant les résultats de M. Mignotte sur les minorations de formes linéaires en deux logarithmes qui se trouvent dans [Mi], on démontre que

$$s \leq 164969.$$

Cette inégalité nous suffit en pratique pour obtenir les entiers x cherchés. Supposons $r \geq 2$. Si $s \geq 2$, on est amené à utiliser les résultats démontrés dans [Iv], qui sont des conséquences des travaux de A. Wiles sur les représentations modulaires. Si $s = 1$, les travaux de F. Beukers ([Be, cor. 1 et 2]) permettent de borner l'entier r par une fonction qui ne dépend que du logarithme de p (formule (1)). Là encore, la majoration obtenue nous suffit pour les résultats que l'on a en vue.

Signalons que dans le cas où p est congru à 3 ou 5 modulo 8 et distinct de 3, T. Hadano a déterminé en 1974 les entiers x vérifiant l'égalité ci-dessus, à condition de supposer que les conjectures d'Ankeny–Artin–Chowla et leurs analogues soient vraies (cf. [Ha, lemmas p. 200]). Ces conjectures ne sont toujours pas démontrées aujourd'hui.

Afin de simplifier la présentation des résultats, on s'est limité au cas où $p \geq 29$. Ce choix n'est pas restrictif, puisque J. Cremona a explicité toutes les classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ dont le conducteur est plus petit que 20000 (cf. [Cr1], [Cr2]). En particulier, le problème 1 est résolu si $2^N p \leq 20000$.

Les lemmes diophantiens se trouvant dans la partie 2.2 de ce travail permettent aussi de résoudre le problème posé si $p \leq 29$. Dans ce cas, on pourra trouver à l'adresse http://www.math.jussieu.fr/~ivorra les tables donnant les classes de $\mathbb{Q}$-isomorphisme cherchées. Il se trouve aussi à cette adresse un programme fonctionnant sous le logiciel de calculs PARI (cf. [Pari]) permettant, un nombre premier p étant donné, de résoudre le problème 1. À titre indicatif, pour $p = 414977$, les courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ et ayant au moins un point d'ordre 2 sur $\mathbb{Q}$ sont, à $\mathbb{Q}$-isomorphisme près, celles indiquées dans les tableaux ci-dessous. Elles sont données par des équations minimales de la forme

$$y^2 + a_1 xy = x^2 + a_2 x^2 + a_4 x + a_6.$$

a_1	a_2	a_4	a_6	N
1	160	−64	0	1
1	160	256	41024	1
0	−641	−1024	0	4
0	1282	414977	0	4

a_1	a_2	a_4	a_6	N
0	1282	−4096	0	6
0	−2564	1659908	0	6
0	−1282	−4096	0	6
0	2564	1659908	0	6

Par exemple, si $p = 4000237$, il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ ayant un point d'ordre 2 sur $\mathbb{Q}$.

Le problème 1 est un cas particulier du problème suivant, que nous ne savons pas traiter en général :

Problème 2. *Déterminer toutes les classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$.*

Il semble que les premiers résultats démontrés sur ce problème soient dus à A. Ogg en 1966. Il a déterminé les courbes elliptiques définies sur $\mathbb{Q}$ dont le conducteur est de la forme 2^N ou $2^N \cdot 3$ (cf. [Og1] et [Og2]). Celles de conducteur 11 ont été ensuite explicitées par J. Vélu (cf. [Ve1]). En ce qui concerne la recherche des courbes elliptiques de conducteur premier p, J.-F. Mestre et J. Oesterlé ont obtenu des tables de courbes de Weil fortes de conducteur $p < 10000$; A. Brumer et O. McGuinness ont déterminé les courbes elliptiques de conducteur $p < 10^8$. Ces travaux ne sont pas publiés dans la littérature. Par ailleurs, comme nous l'évoquions ci-dessus, le problème 2 est résolu si $2^N p$ est plus petit que 20000. Ce sont, à notre connaissance, les principaux travaux existants concernant ce problème.

Pour certains nombres premiers p, toute courbe elliptique sur $\mathbb{Q}$ ayant un conducteur de la forme $2^N p$ a aussi un point d'ordre 2 rationnel sur $\mathbb{Q}$. Pour un tel nombre premier p, les résultats que l'on obtient permettent ainsi de résoudre le problème 2. Rappelons un critère pour qu'il en soit ainsi (cf. [Se] et [Ha]) :

PROPOSITION. *Soit p un nombre premier.*

1. *Supposons que les nombres de classes des deux corps*

$$\mathbb{Q}(\sqrt{p}) \quad \textit{et} \quad \mathbb{Q}(\sqrt{-p})$$

ne soient pas divisibles par 3 et que p soit congru à 1 ou 7 modulo 8. Alors, toute courbe elliptique sur $\mathbb{Q}$ de conducteur p a au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$.

2. *Supposons que les nombres de classes des quatre corps*

$$\mathbb{Q}(\sqrt{p}), \quad \mathbb{Q}(\sqrt{-p}), \quad \mathbb{Q}(\sqrt{2p}) \quad \textit{et} \quad \mathbb{Q}(\sqrt{-2p})$$

ne soient pas divisibles par 3.

   (i) *Si p est congru à 3 ou 5 modulo 8, il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2p$.*

   (ii) *Si p est congru à 1 ou 7 modulo 8, toute courbe elliptique sur $\mathbb{Q}$ de conducteur $2^N p$, avec $N \geq 1$, a au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$.*

Les nombres premiers $p < 1000$ congrus à 1 ou 7 modulo 8 pour lesquels les nombres de classes des corps $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{2p})$ et $\mathbb{Q}(\sqrt{-2p})$ ne sont pas divisibles par 3 sont les suivants :

$$\{7, 17, 41, 47, 73, 97, 103, 113, 191, 193, 281, 409, 463, 479, 577, 607\},$$
$$\{647, 719, 769, 887, 911, 919, 937, 953, 967\}.$$

Par exemple, si $p = 967$, on peut ainsi démontrer qu'il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ si $N = 0, 2, 3, 5$ ou 7. Si $N = 1, 4, 6$ ou 8, la liste exhaustive des courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ est donnée, comme précédemment, dans les tableaux suivants :

a_1	a_2	a_4	a_6	N
1	21	128	0	1
1	21	−512	−10880	1
0	−85	2048	0	4
0	170	−967	0	4
0	170	8192	0	6
0	−340	−3868	0	6
0	−170	8192	0	6
0	340	−3868	0	6

a_1	a_2	a_4	a_6	N
0	88	2	0	8
0	−176	7736	0	8
0	−88	2	0	8
0	176	7736	0	8
0	88	1934	0	8
0	−176	8	0	8
0	−88	1934	0	8
0	176	8	0	8

Si $N = 1$ les courbes sont, à $\mathbb{Q}$-isomorphisme près, celles notées $1934A1$ et $1934A2$ dans les tables de Cremona (cf. [Cr2]).

Signalons enfin que si $p = 1299709$, l'hypothèse de l'assertion 2 de la proposition est aussi satisfaite, et il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$.

Je remercie A. Kraus pour l'aide qu'il m'a apportée pendant la réalisation de ce travail, ainsi que Y. Bugeaud pour les conversations que nous avons eues concernant certains points de cet article.

1. Énoncé des résultats

Soient p un nombre premier et N un entier vérifiant les inégalités

$$p \geq 29 \quad \text{et} \quad 1 \leq N \leq 8.$$

Nous énonçons dans ce qui suit huit théorèmes qui décrivent, à $\mathbb{Q}$-isomorphisme près, toutes les courbes elliptiques sur $\mathbb{Q}$, de conducteur $2^N p$, ayant au moins un point d'ordre 2 sur $\mathbb{Q}$. Chaque théorème correspond à une valeur de N. Les résultats que l'on a obtenus sont présentés sous forme de tableaux analogues à ceux de [Cr1]. Dans chaque ligne on explicite une courbe elliptique E définie sur $\mathbb{Q}$ réalisant les conditions souhaitées. Les colonnes des tableaux fournissent les données suivantes sur E :

1. Un modèle minimal de E de la forme
$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x + a_6,$$
où les a_i sont dans $\mathbb{Z}$. Si l'on a $N \geq 2$, on peut choisir un tel modèle avec $a_1 = a_6 = 0$. Dans les énoncés des théorèmes 2 à 8, on a donc omis les colonnes qui correspondent à ces coefficients.
2. L'ordre $|T_2|$ du groupe T_2 des points de 2-torsion de E rationnels sur $\mathbb{Q}$.
3. La factorisation du discriminant minimal Δ de E.
4. Les symboles de Kodaira de E en 2 et p.
5. Les courbes elliptiques liées à E par une isogénie sur $\mathbb{Q}$ de degré 2.

Il apparaît par ailleurs dans les tableaux des lettres d'identifications $(A, B, \ldots)$ pour chaque courbe elliptique. Les courbes elliptiques qui sont libellées par une même lettre sont liées par une isogénie sur $\mathbb{Q}$ de degré 2 ou un composé de deux telles isogénies. Elles sont de plus numérotées dans l'ordre où elles ont été déterminées. Dans la colonne

Isogénies, nous avons indiqué par leurs numéros les courbes liées à E par une isogénie de degré 2. Ce degré est rappelé en gras.

NOTATIONS. a) Pour toute courbe elliptique E sur $\mathbb{Q}$, on désignera par E' la courbe elliptique sur $\mathbb{Q}$ déduite de E par torsion par $\sqrt{-1}$.

b) On notera f la fonction réelle définie sur $\mathbb{N}^*$ par

$$f(n) = \begin{cases} 18 + 2\,\dfrac{\log n}{\log 2} & \text{si } n < 2^{96}, \\ 435 + 10\,\dfrac{\log n}{\log 2} & \text{si } n \geq 2^{96}. \end{cases} \tag{1}$$

c) Étant donné un entier n qui soit un carré dans $\mathbb{Z}$, on désignera, *pour toute la suite*, par $\sqrt{n}$ la racine carrée de n vérifiant la condition suivante :

$$\begin{cases} \sqrt{n} \equiv 1 \bmod 4 & \text{si } n \text{ est impair}, \\ \sqrt{n} \geq 0 & \text{si } n \text{ est pair}. \end{cases} \tag{2}$$

THÉORÈME 1. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $2p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles il existe un entier k vérifiant les inégalités*

$$7 \leq k < f(p),$$

tel que l'une des conditions suivantes soit satisfaite :

1) *l'entier $p - 2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques* :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	1	$(\sqrt{p-2^k}-1)/4$	-2^{k-6}	0	2	$2^{2k-12}p$	I_{2k-12}, I_1	**2** : 2
A2	1	$(\sqrt{p-2^k}-1)/4$	2^{k-4}	$2^{k-6}\sqrt{p-2^k}$	2	$-2^{k-6}p^2$	I_{k-6}, I_2	**2** : 1

2) *l'entier $p + 2^k$ est un carré, k est impair et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques* :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	1	$(\sqrt{p+2^k}-1)/4$	2^{k-6}	0	2	$2^{2k-12}p$	I_{2k-12}, I_1	**2** : 2
B2	1	$(\sqrt{p+2^k}-1)/4$	-2^{k-4}	$-2^{k-6}\sqrt{p+2^k}$	2	$2^{k-6}p^2$	I_{k-6}, I_2	**2** : 1

3) *l'entier k est pair, on a $p = 2^{k/2+1} + 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques* :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	1	$(1-p)/4$	$(1-p)/16$	0	4	$2^{k-6}p^2$	I_{k-6}, I_2	**2** : 2, 3, 4
C2	1	$(p-1)/2$	$(p-1)(p+5)/16$	$(p-1)(p+3)/64$	2	$-2^{k/2-3}p^4$	$\mathrm{I}_{k/2-3}$, I_4	**2** : 1
C3	1	$(p-1)/8$	$(p-1)^2/2^8$	0	2	$2^{2k-12}p$	I_{2k-12}, I_1	**2** : 1
C4	1	$1-p$	$(1-p)/2$	$(1-p)/16$	2	$2^{k/2-3}p$	$\mathrm{I}_{k/2-3}$, I_1	**2** : 1

4) *l'entier $2^k - p$ est un carré, k est impair et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques* :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
D1	1	$(\sqrt{2^k-p}-1)/4$	2^{k-6}	0	2	$-2^{2k-12}p$	I_{2k-12}, I_1	$\mathbf{2}:2$
D2	1	$(\sqrt{2^k-p}-1)/4$	-2^{k-4}	$-2^{k-6}\sqrt{2^k-p}$	2	$2^{k-6}p^2$	I_{k-6}, I_2	$\mathbf{2}:1$

5) *l'entier k est pair, on a $p=2^{k/2+1}-1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques* :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
E1	1	$(p+1)/4$	$(p+1)/16$	0	4	$2^{k-6}p^2$	I_{k-6}, I_2	$\mathbf{2}:2,3,4$
E2	1	$-(p+1)/2$	$(p+1)(p-5)/16$	$(p+1)(p-3)/64$	2	$2^{k/2-3}p^4$	$\mathrm{I}_{k/2-3}$, I_4	$\mathbf{2}:1$
E3	1	$-(p+1)/8$	$(p+1)^2/2^8$	0	2	$-2^{2k-12}p$	I_{2k-12}, I_1	$\mathbf{2}:1$
E4	1	$p+1$	$(p+1)/2$	$(p+1)/16$	2	$2^{k/2-3}p$	$\mathrm{I}_{k/2-3}$, I_1	$\mathbf{2}:1$

COROLLAIRE. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $2p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si il existe un entier k vérifiant les inégalités*

$$7 \leq k < f(p),$$

tel que l'un des entiers $p-2^k$, $p+2^k$ et 2^k-p soit un carré. Si tel est le cas, p est congru à 1 ou 7 modulo 8.

THÉORÈME 2. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $4p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles la condition suivante est satisfaite : l'entier $p-4$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$\sqrt{p-4}$	-1	2	2^4p	IV, I_1	$\mathbf{2}:2$
A2	$-2\sqrt{p-4}$	p	2	-2^8p^2	IV^*, I_2	$\mathbf{2}:1$

COROLLAIRE. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $4p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si $p-4$ est un carré. Si tel est le cas, p est congru à 5 modulo 8.*

THÉORÈME 3. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $8p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles l'une des conditions suivantes est satisfaite* :

1) *l'entier $p-16$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$\sqrt{p-16}$	-4	2	2^8p	I_1^*, I_1	$\mathbf{2}:2$
A2	$-2\sqrt{p-16}$	p	2	$-2^{10}p^2$	III^*, I_2	$\mathbf{2}:1$

2) *l'entier $p-32$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	$\sqrt{p-32}$	-8	2	$2^{10}p$	III^*, I_1	$\mathbf{2}:2$
B2	$-2\sqrt{p-32}$	p	2	$-2^{11}p^2$	II^*, I_2	$\mathbf{2}:1$

3) *l'entier* $p+32$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$\sqrt{p+32}$	8	2	$2^{10}p$	III^*, I_1	**2** : 2
C2	$-2\sqrt{p+32}$	p	2	$2^{11}p^2$	II^*, I_2	**2** : 1

4) *on a* $p=31$ *et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
D1	1	8	2	$-2^{10}\cdot 31$	III^*, I_1	**2** : 2
D2	-2	-31	2	$2^{11}\cdot 31^2$	II^*, I_2	**2** : 1

Corollaire. *Supposons* $p>31$. *Il existe une courbe elliptique définie sur* $\mathbb{Q}$, *de conducteur* $8p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$, *si et seulement si l'un des entiers* $p-16$, $p-32$ *et* $p+32$ *est un carré. Si tel est le cas*, p *est congru à* 1 *modulo* 8.

Théorème 4. *Les courbes elliptiques* E *définies sur* $\mathbb{Q}$, *de conducteur* $16p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$, *sont celles pour lesquelles il existe un entier* k *vérifiant les inégalités*

$$4\leq k<f(p),$$

tel que l'une des conditions suivantes soit satisfaite :

1) *l'entier* $p-2^k$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$-\sqrt{p-2^k}$	-2^{k-2}	2	$2^{2k}p$	I^*_{2k-8}, I_1	**2** : 2
A2	$2\sqrt{p-2^k}$	p	2	$-2^{k+6}p^2$	I^*_{k-2}, I_2	**2** : 1

2) *l'entier* $p+2^k$ *est un carré*, k *est impair et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	$-\sqrt{p+2^k}$	2^{k-2}	2	$2^{2k}p$	I^*_{2k-8}, I_1	**2** : 2
B2	$2\sqrt{p+2^k}$	p	2	$2^{k+6}p^2$	I^*_{k-2}, I_2	**2** : 1

3) *l'entier* k *est pair, on a* $p=2^{k/2+1}+1$ *et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$p+1$	p	4	$2^{k+6}p^2$	I^*_{k-2}, I_2	**2** : 2, 3, 4
C2	$-(p+1)/2$	$(p-1)^2/16$	2	$2^{2k}p$	I^*_{2k-8}, I_1	**2** : 1
C3	$2(2p-1)$	1	2	$2^{9+k/2}p$	$\mathrm{I}^*_{k/2+1}$, I_1	**2** : 1
C4	$2(2-p)$	p^2	2	$-2^{9+k/2}p^4$	$\mathrm{I}^*_{k/2+1}$, I_4	**2** : 1

4) *l'entier* $p-4$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
D1	$-\sqrt{p-4}$	-1	2	2^4p	II, I_1	**2** : 2
D2	$2\sqrt{p-4}$	p	2	-2^8p^2	I^*_0, I_2	**2** : 1

5) *l'entier* $2^k - p$ *est un carré,* k *est impair et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
E1	$-\sqrt{2^k-p}$	2^{k-2}	2	$-2^{2k}p$	I^*_{2k-8}, I_1	$\mathbf{2}$: 2
E2	$2\sqrt{2^k-p}$	$-p$	2	$2^{k+6}p^2$	I^*_{k-2}, I_2	$\mathbf{2}$: 1

6) *l'entier* k *est pair, on a* $p = 2^{k/2+1} - 1$ *et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
F1	$1-p$	$-p$	4	$2^{k+6}p^2$	I^*_{k-2}, I_2	$\mathbf{2}$: 2, 3, 4
F2	$(p-1)/2$	$(p+1)^2/16$	2	$-2^{2k}p$	I^*_{2k-8}, I_1	$\mathbf{2}$: 1
F3	$2(p+2)$	p^2	2	$2^{k/2+9}p^4$	$\mathrm{I}^*_{k/2+1}$, I_4	$\mathbf{2}$: 1
F4	$-2(2p+1)$	1	2	$2^{k/2+9}p$	$\mathrm{I}^*_{k/2+1}$, I_1	$\mathbf{2}$: 1

Corollaire. *Il existe une courbe elliptique définie sur* $\mathbb{Q}$*, de conducteur* $16p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, si et seulement si il existe un entier* k *vérifiant les inégalités*

$$4 \leq k < f(p),$$

tel que l'un des entiers $p-4$*,* $p-2^k$*,* $p+2^k$ *et* 2^k-p *soit un carré. Si tel est le cas,* p *est congru à* 1*,* 5 *ou* 7 *modulo* 8*.*

Théorème 5. *Les courbes elliptiques* E *définies sur* $\mathbb{Q}$*, de conducteur* $32p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, sont celles pour lesquelles l'une des conditions suivantes est satisfaite* :

1) *l'entier* $p-1$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$2\sqrt{p-1}$	-1	2	2^6p	III, I_1	$\mathbf{2}$: 2
A2	$-4\sqrt{p-1}$	$4p$	2	$-2^{12}p^2$	I^*_3, I_2	$\mathbf{2}$: 1
A1′	$-2\sqrt{p-1}$	-1	2	2^6p	III, I_1	$\mathbf{2}$: 2
A2′	$4\sqrt{p-1}$	$4p$	2	$-2^{12}p^2$	I^*_3, I_2	$\mathbf{2}$: 1

2) *l'entier* $p-8$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	$\sqrt{p-8}$	-2	2	2^6p	III, I_1	$\mathbf{2}$: 2
B2	$-2\sqrt{p-8}$	p	2	-2^9p^2	I^*_0, I_2	$\mathbf{2}$: 1
B1′	$-\sqrt{p-8}$	-2	2	2^6p	III, I_1	$\mathbf{2}$: 2
B2′	$2\sqrt{p-8}$	p	2	-2^9p^2	I^*_0, I_2	$\mathbf{2}$: 1

3) *l'entier* $p+8$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$\sqrt{p+8}$	2	2	2^6p	III, I_1	$\mathbf{2}$: 2
C2	$-2\sqrt{p+8}$	p	2	2^9p^2	I^*_0, I_2	$\mathbf{2}$: 1
C1′	$-\sqrt{p+8}$	2	2	2^6p	III, I_1	$\mathbf{2}$: 2
C2′	$2\sqrt{p+8}$	p	2	2^9p^2	I^*_0, I_2	$\mathbf{2}$: 1

Corollaire. *Il existe une courbe elliptique définie sur* $\mathbb{Q}$, *de conducteur* $32p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$, *si et seulement si l'un des entiers* $p-1$, $p-8$ *et* $p+8$ *est un carré. Si tel est le cas*, p *est congru à* 1 *modulo* 4.

Théorème 6. *Les courbes elliptiques* E *définies sur* $\mathbb{Q}$, *de conducteur* $64p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$, *sont celles pour lesquelles il existe un entier* k *vérifiant les inégalités*

$$2 \leq k < f(p),$$

tel que l'une des conditions suivantes soit satisfaite :

1) *l'entier* $p-1$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$2\sqrt{p-1}$	p	2	-2^6p^2	II, I_2	**2** : 2
A2	$-4\sqrt{p-1}$	-4	2	$2^{12}p$	I_2^*, I_1	**2** : 1
A1′	$-2\sqrt{p-1}$	p	2	-2^6p^2	II, I_2	**2** : 2
A2′	$4\sqrt{p-1}$	-4	2	$2^{12}p$	I_2^*, I_1	**2** : 1

2) *l'entier* $p-2^k$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	$2\sqrt{p-2^k}$	-2^k	2	$2^{2k+6}p$	I_{2k-4}^*, I_1	**2** : 2
B2	$-4\sqrt{p-2^k}$	$4p$	2	$-2^{k+12}p^2$	I_{k+2}^*, I_2	**2** : 1
B1′	$-2\sqrt{p-2^k}$	-2^k	2	$2^{2k+6}p$	I_{2k-4}^*, I_1	**2** : 2
B2′	$4\sqrt{p-2^k}$	$4p$	2	$-2^{k+12}p^2$	I_{k+2}^*, I_2	**2** : 1

3) *l'entier* $p+2^k$ *est un carré,* k *est impair et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$2\sqrt{p+2^k}$	2^k	2	$2^{2k+6}p$	I_{2k-4}^*, I_1	**2** : 2
C2	$-4\sqrt{p+2^k}$	$4p$	2	$2^{k+12}p^2$	I_{k+2}^*, I_2	**2** : 1
C1′	$-2\sqrt{p+2^k}$	2^k	2	$2^{2k+6}p$	I_{2k-4}^*, I_1	**2** : 2
C2′	$4\sqrt{p+2^k}$	$4p$	2	$2^{k+12}p^2$	I_{k+2}^*, I_2	**2** : 1

4) *l'entier* k *est pair, on a* $p = 2^{k/2+1}+1$ *et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
D1	$2(p+1)$	$4p$	4	$2^{k+12}p^2$	I_{k+2}^*, I_2	**2** : 2, 3, 4
D2	$4(2p-1)$	4	2	$2^{k/2+15}p$	$I_{k/2+5}^*$, I_1	**2** : 1
D3	$4(2-p)$	$4p^2$	2	$-2^{k/2+15}p^4$	$I_{k/2+5}^*$, I_4	**2** : 1
D4	$-(p+1)$	$(p-1)^2/4$	2	$2^{2k+6}p$	I_{2k-4}^*, I_1	**2** : 1
D1′	$-2(p+1)$	$4p$	4	$2^{k+12}p^2$	I_{k+2}^*, I_2	**2** : 2, 3, 4
D2′	$-4(2p-1)$	4	2	$2^{k/2+15}p$	$I_{k/2+5}^*$, I_1	**2** : 1
D3′	$-4(2-p)$	$4p^2$	2	$-2^{k/2+15}p^4$	$I_{k/2+5}^*$, I_4	**2** : 1
D4′	$p+1$	$(p-1)^2/4$	2	$2^{2k+6}p$	I_{2k-4}^*, I_1	**2** : 1

5) *l'entier* $2^k - p$ *est un carré,* k *est impair et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
E1	$2\sqrt{2^k-p}$	2^k	2	$-2^{2k+6}p$	I^*_{2k-4}, I_1	**2** : 2
E2	$-4\sqrt{2^k-p}$	$-4p$	2	$2^{k+12}p^2$	I^*_{k+2}, I_2	**2** : 1
E1′	$-2\sqrt{2^k-p}$	2^k	2	$-2^{2k+6}p$	I^*_{2k-4}, I_1	**2** : 2
E2′	$4\sqrt{2^k-p}$	$-4p$	2	$2^{k+12}p^2$	I^*_{k+2}, I_2	**2** : 1

6) *l'entier* k *est pair, on a* $p = 2^{k/2+1} - 1$ *et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
F1	$-2(p-1)$	$-4p$	4	$2^{k+12}p^2$	I^*_{k+2}, I_2	**2** : 2, 3, 4
F2	$-4(2p+1)$	4	2	$2^{k/2+15}p$	$\mathrm{I}^*_{k/2+5}$, I_1	**2** : 1
F3	$4(p+2)$	$4p^2$	2	$2^{k/2+15}p^4$	$\mathrm{I}^*_{k/2+5}$, I_4	**2** : 1
F4	$p-1$	$(p+1)^2/4$	2	$-2^{2k+6}p$	I^*_{2k-4}, I_1	**2** : 1
F1′	$2(p-1)$	$-4p$	4	$2^{k+12}p^2$	I^*_{k+2}, I_2	**2** : 2, 3, 4
F2′	$4(2p+1)$	4	2	$2^{k/2+15}p$	$\mathrm{I}^*_{k/2+5}$, I_1	**2** : 1
F3′	$-4(p+2)$	$4p^2$	2	$2^{k/2+15}p^4$	$\mathrm{I}^*_{k/2+5}$, I_4	**2** : 1
F4′	$-(p-1)$	$(p+1)^2/4$	2	$-2^{2k+6}p$	I^*_{2k-4}, I_1	**2** : 1

Corollaire. *Il existe une courbe elliptique définie sur* $\mathbb{Q}$*, de conducteur* $64p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, si et seulement si il existe un entier* k *vérifiant les inégalités*

$$2 \leq k < f(p),$$

tel que l'un des entiers $p-1$, $p-2^k$, $p+2^k$ *et* $2^k - p$ *soit un carré.*

Théorème 7. *Les courbes elliptiques* E *définies sur* $\mathbb{Q}$*, de conducteur* $128p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, sont celles pour lesquelles l'une des conditions suivantes est satisfaite* :

1) *il existe* $k \in \{1, 2\}$ *tel que* $2p^k - 1$ *soit un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$2\sqrt{2p^k-1}$	-1	2	2^7p^k	II, I_k	**2** : 2
A2	$-4\sqrt{2p^k-1}$	$8p^k$	2	$-2^{14}p^{2k}$	III*, I_{2k}	**2** : 1
A1′	$-2\sqrt{2p^k-1}$	-1	2	2^7p^k	II, I_k	**2** : 2
A2′	$4\sqrt{2p^k-1}$	$8p^k$	2	$-2^{14}p^{2k}$	III*, I_{2k}	**2** : 1
B1	$2\sqrt{2p^k-1}$	$2p^k$	2	-2^8p^{2k}	III, I_{2k}	**2** : 2
B2	$-4\sqrt{2p^k-1}$	-4	2	$2^{13}p^k$	I^*_2, I_k	**2** : 1
B1′	$-2\sqrt{2p^k-1}$	$2p^k$	2	-2^8p^{2k}	III, I_{2k}	**2** : 2
B2′	$4\sqrt{2p^k-1}$	-4	2	$2^{13}p^k$	I^*_2, I_k	**2** : 1

2) *il existe un entier impair* k *vérifiant les inégalités* $1 \leq k \leq 164969$*, tel que* $p^k + 2$ *soit un carré et* E *soit* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$2\sqrt{p^k+2}$	p^k	2	2^7p^{2k}	II, I_{2k}	$\mathbf{2}:2$
C2	$-4\sqrt{p^k+2}$	8	2	$2^{14}p^k$	III^*, I_k	$\mathbf{2}:1$
C1′	$-2\sqrt{p^k+2}$	p^k	2	2^7p^{2k}	II, I_{2k}	$\mathbf{2}:2$
C2′	$4\sqrt{p^k+2}$	8	2	$2^{14}p^k$	III^*, I_k	$\mathbf{2}:1$
D1	$2\sqrt{p^k+2}$	2	2	2^8p^k	III, I_k	$\mathbf{2}:2$
D2	$-4\sqrt{p^k+2}$	$4p^k$	2	$2^{13}p^{2k}$	I_2^*, I_{2k}	$\mathbf{2}:1$
D1′	$-2\sqrt{p^k+2}$	2	2	2^8p^k	III, I_k	$\mathbf{2}:2$
D2′	$4\sqrt{p^k+2}$	$4p^k$	2	$2^{13}p^{2k}$	I_2^*, I_{2k}	$\mathbf{2}:1$

3) *l'entier* $p-2$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
E1	$2\sqrt{p-2}$	p	2	-2^7p^2	II, I_2	$\mathbf{2}:2$
E2	$-4\sqrt{p-2}$	-8	2	$2^{14}p$	III^*, I_1	$\mathbf{2}:1$
E1′	$-2\sqrt{p-2}$	p	2	-2^7p^2	II, I_2	$\mathbf{2}:2$
E2′	$4\sqrt{p-2}$	-8	2	$2^{14}p$	III^*, I_1	$\mathbf{2}:1$
F1	$2\sqrt{p-2}$	-2	2	2^8p	III, I_1	$\mathbf{2}:2$
F2	$-4\sqrt{p-2}$	$4p$	2	$-2^{13}p^2$	I_2^*, I_2	$\mathbf{2}:1$
F1′	$-2\sqrt{p-2}$	-2	2	2^8p	III, I_1	$\mathbf{2}:2$
F2′	$4\sqrt{p-2}$	$4p$	2	$-2^{13}p^2$	I_2^*, I_2	$\mathbf{2}:1$

Corollaire. *Il existe une courbe elliptique définie sur* $\mathbb{Q}$*, de conducteur* $128p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, si et seulement si il existe un entier impair* k *vérifiant les inégalités*

$$1 \leq k \leq 164969,$$

tel que l'un des entiers p^k+2*,* $2p-1$*,* $2p^2-1$ *et* $p-2$ *soit un carré.*

Théorème 8. *Les courbes elliptiques* E *définies sur* $\mathbb{Q}$*, de conducteur* $256p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, sont celles pour lesquelles l'une des conditions suivantes est satisfaite* :

1) *il existe* $k \in \{1,2\}$ *tel que* $(p^k-1)/2$ *soit un carré et* E *soit* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$4\sqrt{(p^k-1)/2}$	-2	2	2^9p^k	III, I_k	$\mathbf{2}:2$
A2	$-8\sqrt{(p^k-1)/2}$	$8p^k$	2	$-2^{15}p^{2k}$	III^*, I_{2k}	$\mathbf{2}:1$
A1′	$-4\sqrt{(p^k-1)/2}$	-2	2	2^9p^k	III, I_k	$\mathbf{2}:2$
A2′	$8\sqrt{(p^k-1)/2}$	$8p^k$	2	$-2^{15}p^{2k}$	III^*, I_{2k}	$\mathbf{2}:1$
B1	$4\sqrt{(p^k-1)/2}$	$2p^k$	2	-2^9p^{2k}	III, I_{2k}	$\mathbf{2}:2$
B2	$-8\sqrt{(p^k-1)/2}$	-8	2	$2^{15}p^k$	III^*, I_k	$\mathbf{2}:1$
B1′	$-4\sqrt{(p^k-1)/2}$	$2p^k$	2	-2^9p^{2k}	III, I_{2k}	$\mathbf{2}:2$
B2′	$8\sqrt{(p^k-1)/2}$	-8	2	$2^{15}p^k$	III^*, I_k	$\mathbf{2}:1$

2) *il existe* $k \in \{1,2\}$ *tel que l'entier* $(p^k+1)/2$ *soit un carré et* E *soit* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques* :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$4\sqrt{(p^k+1)/2}$	2	2	2^9p^k	III, I_k	$\mathbf{2}:2$
C2	$-8\sqrt{(p^k+1)/2}$	$8p^k$	2	$2^{15}p^{2k}$	III^*, I_{2k}	$\mathbf{2}:1$
C1′	$-4\sqrt{(p^k+1)/2}$	2	2	2^9p^k	III, I_k	$\mathbf{2}:2$
C2′	$8\sqrt{(p^k+1)/2}$	$8p^k$	2	$2^{15}p^{2k}$	III^*, I_{2k}	$\mathbf{2}:1$
D1	$4\sqrt{(p^k+1)/2}$	$2p^k$	2	2^9p^{2k}	III, I_{2k}	$\mathbf{2}:2$
D2	$-8\sqrt{(p^k+1)/2}$	8	2	$2^{15}p^k$	III^*, I_k	$\mathbf{2}:1$
D1′	$-4\sqrt{(p^k+1)/2}$	$2p^k$	2	2^9p^{2k}	III, I_{2k}	$\mathbf{2}:2$
D2′	$8\sqrt{(p^k+1)/2}$	8	2	$2^{15}p^k$	III^*, I_k	$\mathbf{2}:1$

Corollaire. *Il existe une courbe elliptique définie sur* $\mathbb{Q}$*, de conducteur* $256p$ *et ayant au moins un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, si et seulement si l'un des entiers* $(p-1)/2$*,* $(p^2-1)/2$*,* $(p+1)/2$ *et* $(p^2+1)/2$ *est un carré.*

2. Lemmes préliminaires

2.1. Modèles de Weierstrass. Considérons une courbe elliptique E définie sur $\mathbb{Q}$, de conducteur 2^Np avec $N \geq 1$, ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. On utilisera dans toute la suite du texte le résultat suivant :

Lemme 1. *Il existe un modèle de Weierstrass de* E *de la forme*

$$y^2 = x(x^2+ax+b), \tag{3}$$

où a *et* b *sont des entiers sans diviseurs communs impairs. Ce modèle est minimal en dehors de* 2*. Les invariants standard* c_4*,* c_6 *et* Δ *qui lui sont associés sont*

$$c_4 = 2^4(a^2-3b), \quad c_6 = 2^5a(9b-2a^2), \quad \Delta = 2^4b^2(a^2-4b). \tag{4}$$

Dans le cas où $N \geq 2$*, l'équation* (3) *est un modèle minimal de* E*.*

Démonstration. Si $N = 1$ cet énoncé est une version particulière du lemme 1 de [M-O].

Supposons $N \geq 2$, autrement dit, que E ait mauvaise réduction de type additif en 2. Considérons un modèle de Weierstrass minimal de E sur $\mathbb{Z}$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Posons, comme dans [Ta],

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6.$$

En effectuant le changement de variables

$$X = x, \quad Y = y + \frac{a_1x + a_3}{2}, \tag{5}$$

on obtient comme nouveau modèle de E

$$Y^2 = X^3 + \frac{b_2}{4}X^2 + \frac{b_4}{2}X + \frac{b_6}{4}. \tag{6}$$

C'est un modèle entier de E. En effet, il résulte de l'hypothèse faite sur E que l'on a les congruences (cf. [Pa, tableau IV, p. 129])

$$c_4 \equiv 0 \bmod 16, \quad c_6 \equiv 0 \bmod 32.$$

D'après les égalités

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

on a ainsi

$$b_2 \equiv 0 \bmod 4, \quad b_4 \equiv 0 \bmod 2, \quad b_6 \equiv 0 \bmod 4,$$

ce qui prouve notre assertion. Vu le changement de variables (5), le modèle (6) est donc minimal. Soit u l'abscisse d'un point d'ordre 2 de E dans ce modèle ; c'est un entier relatif. Le changement de variables

$$X = x + u, \quad Y = y,$$

conduit alors à un modèle minimal de E de la forme $y^2 = x(x^2 + ax + b)$ où a et b sont des entiers. On vérifie que l'on a les formules (4) (cf. [Ta]). Le fait que E ait réduction semi-stable en dehors de 2 entraîne que a et b n'ont pas de diviseurs communs impairs, d'où le lemme.

2.2. Lemmes diophantiens. Dans ce paragraphe, la lettre p désigne un nombre premier impair. On explicite ici des résultats concernant certaines équations diophantiennes qui interviendront dans la suite.

Les lemmes 2 et 3 ci-dessous se trouvent respectivement dans les alinéas 1 et 2 du lemme p. 200 de [Ha].

LEMME 2. *Soient m et n deux entiers naturels. Soit x un entier ≥ 1 tel que*

$$x^2 - 1 = 2^m p^n.$$

On est dans l'un des cas suivants :

1. $p = 3$ *et* $(x, m, n) \in \{(2, 0, 1), (5, 3, 1), (7, 4, 1), (17, 5, 2)\}$;
2. $p = 5$ *et* $(x, m, n) = (9, 4, 1)$;
3. $p = 2^{m-2} + 1$ *avec* $m \geq 5$ *et* $(x, n) = (2p - 1, 1)$;
4. $p = 2^{m-2} - 1$ *avec* $m \geq 5$ *et* $(x, n) = (2p + 1, 1)$;
5. $(x, m, n) = (3, 3, 0)$.

LEMME 3. *Soient m et n deux entiers naturels. Soit x un entier ≥ 1 tel que*

$$x^2 + 1 = 2^m p^n.$$

On est dans l'un des cas suivants :

1. $p \equiv 3 \bmod 4$ *et* $(x, m, n) = (1, 1, 0)$;
2. $p = 13$ *et* $(x, m, n) \in \{(5, 1, 1), (239, 1, 4)\}$;
3. $p \neq 13$, $p \equiv 1 \bmod 4$ *et* $(m, n) \in \{(0, 1), (1, 1), (1, 2)\}$.

LEMME 4. *Soient m et n deux entiers naturels ≥ 1. Soit x un entier ≥ 2 tel que*

$$x^2 + 2^m = p^n.$$

On est dans l'un des cas suivants :

1. $p = 3$ *et* $(x, m, n) \in \{(5, 1, 3), (7, 5, 4), (1, 3, 2)\}$;
2. $p = 5$ *et* $(x, m, n) \in \{(11, 2, 3), (3, 4, 2)\}$;
3. $p = 2^{m-2} + 1$ *avec* $m \geq 5$ *et* $(x, n) = (p - 2, 2)$;
4. $n = 1$ *et* $m < \log p / \log 2$.

Démonstration. Le cas où $n \geq 3$ est traité dans [Le]. Supposons $n = 2$. On a dans ce cas $(p - x)(x + p) = 2^m$; d'où l'existence de deux entiers naturels u et v tels que $u \geq v$, $p + x = 2^u$, $p - x = 2^v$ et $u + v = m$. On a $2p = 2^u + 2^v$, d'où $p = 2^{u-1} + 2^{v-1}$. Puisque $u \geq v$ et que p est impair, on a $v = 1$. Donc $m \geq 2$, $p = 2^{u-1} + 1$, puis $p = 2^{m-2} + 1$. On en déduit les triplets (x, m, n) intervenant dans l'énoncé du lemme lorsque $n = 2$. Si $n = 1$, $p - 2^m$ est positif, d'où $m < \log p / \log 2$, et le lemme.

Lemme 5. *Soient m et n deux entiers naturels tels que $m \geq 2$ et $n \geq 1$. Soit x un entier naturel non nul tel que*

$$x^2 - 2^m = p^n.$$

On est dans l'un des cas suivants :

1. $p = 17$ *et* $(x, m, n) = (71, 7, 3)$;
2. $p = 2^{m-2} - 1$ *avec* $m \geq 4$ *et* $(x, n) = (p + 2, 2)$;
3. $n = 1$ *et* $m < f(p)$.

Démonstration. Si $n \geq 3$, le corollaire de [Iv] montre que l'assertion 1 est satisfaite.

Supposons $n = 2$. Dans ce cas, $(x + p)(x - p) = 2^m$. Par conséquent, puisque x et p sont des entiers positifs, il existe deux entiers naturels u et v vérifiant $u + v = m$ et $u \geq v$, tels que

$$p + x = 2^u, \quad x - p = 2^v.$$

Cela conduit à $x = p + 2^v$ et à $p = 2^{u-1} - 2^{v-1}$. Comme les entiers u et v vérifient l'inégalité $u \geq v$ et que p est impair, ceci entraîne $v = 1$, puis $u = m - 1$. Par conséquent,

$$p = 2^{m-2} - 1, \quad x = p + 2,$$

ce qui entraîne en particulier $m \geq 4$.

Si $n = 1$, les corollaires 1 et 2 de [Be] conduisent alors à la majoration de m se trouvant dans l'assertion 3.

Lemme 6. *Soient m et n deux entiers naturels ≥ 1. Soit x un entier ≥ 1 tel que*

$$x^2 - 2^m = -p^n.$$

On est dans l'un des cas suivants :

1. $p = 7$ *et* $(x, m, n) = (13, 9, 3)$;
2. $n = 1$ *et* $m < f(p)$.

Démonstration. D'après le théorème p. 3204 de [Bu], l'entier n est impair. Si $n = 1$, la majoration de m résulte des corollaires 1 et 2 de [Be]. Supposons $n \geq 3$; on a $m \geq 2$, et le corollaire de [Iv] entraîne que l'assertion 1 est satisfaite.

LEMME 7. *Soient n et x des entiers naturels ≥ 1.*

1. *Supposons que*
$$2x^2 + 1 = p^n.$$
On est dans l'un des cas suivants :
(i) $p = 3$ *et* $(x, n) = (11, 5)$;
(ii) $n = 1$ *ou* 2.

2. *Supposons que*
$$2x^2 - 1 = p^n.$$
On est dans l'un des cas suivants :
(i) $p = 23$ *et* $(x, n) = (78, 3)$;
(ii) $n = 1$ *ou* 2.

Démonstration. L'assertion 1 est une reformulation de l'alinéa 4 du lemme de [Ha]. L'assertion 2 est une conséquence directe de la proposition 8.1 de [B-S].

LEMME 8. *Supposons $p \geq 29$. Soient n et x des entiers ≥ 2 tels que*
$$x^2 - 2 = p^n.$$
Alors, n est impair et $n \leq 164969$.

Démonstration. Dans toute la suite, pour tout $z \in \mathbb{C}$, on désigne par $|z|$ le module de z. Supposons qu'il existe deux entiers naturels non nuls x et n tels que
$$x^2 - 2 = p^n.$$
Le fait que n soit impair se vérifie directement. Pour démontrer l'inégalité annoncée, nous allons utiliser des minorations de formes linéaires de logarithmes qui se trouvent dans [Mi].

Notons $\sqrt{2}$ la racine carrée positive de 2. Soient A l'anneau d'entiers de $\mathbb{Q}(\sqrt{2})$ et u l'unité fondamentale de A. On a
$$u = \sqrt{2} - 1.$$
Dans A,
$$p^n = (x - \sqrt{2})(x + \sqrt{2}). \tag{7}$$
Puisque p est impair, il en est de même de x. Il en résulte que les entiers $x - \sqrt{2}$ et $x + \sqrt{2}$ sont premiers entre eux. De plus, 2 étant un carré modulo p, l'entier p est décomposé dans $\mathbb{Q}(\sqrt{2})$. Il existe ainsi deux éléments irréductibles conjugués et positifs π_1 et π_2 de A vérifiant les conditions suivantes :

1. $p = \pi_1\pi_2$;
2. il existe deux entiers relatifs t et k vérifiant $0 \leq t < n$ tels que
$$x + \sqrt{2} = u^{t+kn}\pi_1^n, \quad x - \sqrt{2} = u^{-t-kn}\pi_2^n. \tag{8}$$

Pour tout nombre réel x non nul, on note $\log x$ le logarithme de x : si $x > 0$, c'est le logarithme usuel ; si $x < 0$ on le définit par l'égalité
$$\log x = \log |x| \ + \ i\pi.$$

En suivant les notations de [Mi], posons

$$(9)\quad b_1 = t,\quad b_2 = n,\quad \alpha_1 = -\frac{1}{u^2},\quad \alpha_2 = (-1)^k u^{2k}\,\frac{\pi_1}{\pi_2},\quad \Lambda = t\log\alpha_1 - n\log\alpha_2.$$

En utilisant la remarque 4 p. 111 de *loc. cit.* avec la forme linéaire de logarithme Λ, on va démontrer l'inégalité

$$(10)\qquad \log|\Lambda| \geq -634{,}304\left(\mathrm{Max}\left\{0{,}06 + \log\left(\frac{n}{\log p + 3{,}604} + \frac{n}{3,604}\right), \frac{21}{2}\right\}\right)^2 \times \left(\frac{\log p}{2} + 1{,}802\right).$$

Par ailleurs, on va prouver l'inégalité

$$(11)\qquad \log|\Lambda| \leq \log 2\sqrt{2} - \frac{n}{2}\log p + 0{,}103.$$

On déduit alors de (10) et (11) la majoration de n indiquée dans l'énoncé du lemme.

Commençons par démontrer l'inégalité (11). On a

$$\Lambda = \log\left(\frac{\alpha_1^t}{\alpha_2^n}\right).$$

Posons

$$\alpha = \frac{2\sqrt{2}}{u^{t+kn}\pi_1^n}.$$

On a

$$\frac{\alpha_1^t}{\alpha_2^n} = 1 - \alpha.$$

Puisque $x \geq 2$, on a $u^{t+kn}\pi_1^n = x + \sqrt{2} \geq 2 + \sqrt{2} \geq 2\sqrt{2}$, d'où $\alpha \leq 1$. On en déduit que

$$|\Lambda| = -\log(1-\alpha).$$

Il en résulte l'inégalité $|\Lambda| \leq \frac{\alpha}{1-\alpha}$. Par ailleurs,

$$\frac{\alpha}{1-\alpha} = \frac{2\sqrt{2}}{u^{t+kn}\pi_1^n - 2\sqrt{2}}.$$

D'après (7), on a $u^{t+kn}\pi_1^n \geq p^{n/2}$, d'où l'on déduit l'inégalité

$$\log|\Lambda| \leq \log\left(\frac{2\sqrt{2}}{p^{n/2} - 2\sqrt{2}}\right).$$

On obtient ainsi

$$\log|\Lambda| \leq \log 2\sqrt{2} - \frac{n}{2}\log p - \log\left(1 - \frac{2\sqrt{2}}{p^{n/2}}\right).$$

Les inégalités $p \geq 29$ et $n \geq 2$ entraînent alors (11).

Démontrons maintenant l'inégalité (10). Vérifions pour cela les deux conditions suivantes :

3. les nombres réels α_1 et α_2 sont multiplicativement indépendants ;
4. $|\alpha_1| \geq 1$ et $|\alpha_2| \geq 1$.

Supposons qu'il existe deux entiers relatifs n_1 et n_2 tels que

$$\alpha_1^{n_1}\alpha_2^{n_2} = 1.$$

En considérant la valuation en π_1 des deux membres de cette égalité, on constate que $n_2 = 0$. Par suite, $\alpha_1^{n_1} = 1$, d'où $n_1 = 0$ et l'assertion 3. On a $|\alpha_1| \geq 1$. Par ailleurs, l'inégalité

$$|x + \sqrt{2}| \geq |x - \sqrt{2}|\,|u^{2t}|,$$

entraîne

$$\left|\frac{u^{2kn}\pi_1^n}{\pi_2^n}\right| \geq 1,$$

d'où $|\alpha_2| \geq 1$ et l'assertion 4.

Déterminons les constantes qui interviennent dans la remarque 4 de [Mi] dont on reprend les notations sans autre précision. On a $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\sqrt{2})$, d'où

$$D = 2.$$

Il s'agit ensuite de choisir des nombres réels A_i, pour $i \in \{1, 2\}$, tels que

$$\log A_i \geq \mathrm{Max}\left\{h(\alpha_i), \frac{|\log \alpha_i|}{2}, \frac{1}{2}\right\},$$

où $h(\alpha_i)$ est la hauteur logarithmique absolue de α_i.

On vérifie que $h(\alpha_1) = -\log u$, d'où $h(\alpha_1) \approx 0{,}8813$. De plus $|(\log \alpha_1)/2| \approx 1{,}8011$, de sorte que l'on peut prendre

$$\log A_1 = 1{,}802.$$

Calculons $h(\alpha_2)$. La norme sur $\mathbb{Q}$ de α_2 est égale à 1 ; en utilisant l'assertion 4 ci-dessus, on vérifie que

$$h(\alpha_2) = \frac{\log |\alpha_2|}{2}.$$

Démontrons que

$$h(\alpha_2) \leq \frac{\log p}{2} + 0{,}882. \tag{12}$$

On a $|\alpha_2| = |u^{2k}\pi_1/\pi_2|$. On déduit de $p = \pi_1\pi_2$ que

$$|\alpha_2| = p\left|\frac{u^{2k}}{\pi_2^2}\right|.$$

Remarquons que puisque $p \geq 29$, l'entier x est supérieur ou égal à 3, ce qui entraîne $x - \sqrt{2} > 1$. Il résulte alors de (8) que

$$\left|\frac{u^{2k}}{\pi_2^2}\right| \leq |u|^{-2t/n},$$

d'où

$$\log |\alpha_2| \leq \log p + \frac{2t}{n}\log\frac{1}{u},$$

puis

$$\log |\alpha_2| \leq \log p + 1{,}763,$$

ce qui conduit à l'inégalité (12).

Il reste à majorer $|\log \alpha_2|$. D'après (9), on a les égalités

$$\log \alpha_2 = \log(-1)^k + \log|\alpha_2| = i\pi + \log|\alpha_2|.$$

On obtient alors

$$|\log \alpha_2| \le \log p + |1{,}763 + i\pi| \le \log p + 3{,}603,$$

de sorte que

$$\frac{|\log \alpha_2|}{2} \le \frac{\log p}{2} + 1{,}802.$$

Il en résulte que l'on peut prendre

$$\log A_2 = \frac{\log p}{2} + 1{,}802.$$

La remarque 4 de [Mi] conduit alors à l'inégalité

$$\log|\Lambda| \ge -352\left(\operatorname{Max}\left\{0{,}06 + \log\left(\frac{t}{\log p + 3{,}604} + \frac{n}{3{,}604}\right), \frac{21}{2}\right\}\right)^2 \times 1{,}802\left(\frac{\log p}{2} + 1{,}802\right).$$

L'inégalité (10) résulte alors du fait que $t \le n$.

Posons

$$A = \operatorname{Max}\left\{0{,}06 + \log\left(\frac{n}{\log p + 3{,}604} + \frac{n}{3,604}\right), \frac{21}{2}\right\}.$$

Les inégalités (10) et (11) entraînent que

$$\log 2\sqrt{2} - \frac{\log p}{2}\, n + 0{,}103 \ge -634{,}304A^2 \times \left(\frac{\log p}{2} + 1{,}802\right),$$

d'où

$$\log 2\sqrt{2} + 0{,}103 + 634{,}304A^2 \times \left(\frac{\log p}{2} + 1{,}802\right) \ge \frac{\log p}{2}\, n,$$

et

$$2\left(\frac{\log 2\sqrt{2} + 0{,}103}{\log p}\right) + 634{,}304A^2 \times \left(1 + \frac{3{,}604}{\log p}\right) \ge n.$$

Puisque $p \ge 29$, on a

$$2\left(\frac{\log 2\sqrt{2} + 0{,}103}{\log 29}\right) \ge 2\left(\frac{\log 2\sqrt{2} + 0{,}103}{\log p}\right), \quad 1 + \frac{3{,}604}{\log 29} \ge 1 + \frac{3{,}604}{\log p},$$

$$\operatorname{Max}\left\{0{,}06 + \log\left(\frac{n}{\log 29 + 3{,}604} + \frac{n}{3{,}604}\right), \frac{21}{2}\right\} \ge A.$$

On en déduit l'inégalité

$$0{,}679 + 1313{,}197\ \operatorname{Max}\left\{0{,}06 + \log\left(\frac{n}{\log 29 + 3{,}604} + \frac{n}{3{,}604}\right), \frac{21}{2}\right\}^2 \ge n. \tag{13}$$

Supposons $n \ge 81254$. Alors

$$\operatorname{Max}\left\{0{,}06 + \log\left(\frac{n}{\log 29 + 3{,}604} + \frac{n}{3{,}604}\right), \frac{21}{2}\right\} = 0{,}06 + \log\left(\frac{n}{\log 29 + 3{,}604} + \frac{n}{3{,}604}\right).$$

D'après (13), on a ainsi

$$0{,}679 + 1313{,}197\left(0{,}06 + \log\left(\frac{n}{\log 29 + 3{,}604} + \frac{n}{3{,}604}\right)\right)^2 \geq n.$$

Cela entraîne l'inégalité

$$n \leq 164\ 969,$$

d'où le lemme 8.

3. Démonstration des résultats

3.1. Principe de la démonstration. On démontre d'abord que les courbes elliptiques se trouvant dans les énoncés des théorèmes 1 à 8 vérifient bien les propriétés voulues. On utilise pour cela la classification obtenue par I. Papadopoulos (cf. [Pa]) des types de Néron des courbes elliptiques en fonction de leurs invariants minimaux. On explicite ensuite toutes les classes de $\mathbb{Q}$-isomorphisme possibles de courbes elliptiques définies sur $\mathbb{Q}$, de conducteur $2^N p$ (avec $N \geq 1$) et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. Le lemme 1 permet de ramener ce problème à la recherche des entiers a et b sans diviseurs premiers communs impairs, pour lesquels il existe des entiers naturels m et n vérifiant l'égalité

$$b^2(a^2 - 4b) = \pm 2^m p^n.$$

Les lemmes diophantiens permettent la détermination de ces entiers. On en déduit alors que, à $\mathbb{Q}$-isomorphisme près, les courbes elliptiques indiquées dans les théorèmes 1 à 8 sont les seules à avoir les propriétés annoncées.

3.2. Les courbes elliptiques intervenant dans les énoncés des théorèmes. Dans cette partie, nous allons démontrer que les courbes elliptiques figurant dans les énoncés des théorèmes 1 à 8 vérifient bien les propriétés annoncées.

Pour cela, il nous faut vérifier :

(i) que les modèles indiqués dans les tableaux sont entiers ;
(ii) les factorisations indiquées dans la colonne Δ ;
(iii) l'ordre du groupe T_2 ;
(iv) les informations données dans la colonne Isogénies ;
(v) que le conducteur des courbes elliptiques est bien celui annoncé ;
(vi) que les modèles se trouvant dans les tableaux sont minimaux ;
(vii) les symboles de Kodaira indiqués.

1. En ce qui concerne les théorèmes 2 à 8, le point (i) se vérifie directement à partir des conditions précédant chaque tableau. Pour les modèles se trouvant dans l'énoncé du théorème 1, on utilise de plus la condition (2).

2. Pour le point (iii), on vérifie que les courbes elliptiques indiquées dans l'énoncé des résultats ont toutes au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. On a donc $|T_2| = 4$ si le discriminant de l'équation considérée est un carré et $|T_2| = 2$ sinon.

Considérons alors une courbe elliptique E intervenant dans l'un des énoncés des théorèmes 1 à 8 et donnée par l'équation

$$E : y^2 + a_1xy = x^3 + a_2x^2 + a_4x + a_6,$$

où les a_i sont dans $\mathbb{Z}$. Soient b_2, b_4, b_6, b_8, c_4, c_6 et Δ les invariants standard qui lui sont associés par les formules qui se trouvent dans [Ta, p. 36].

3. Les factorisations indiquées dans la colonne Δ des tableaux se déduisent de *loc. cit.* Dans certains cas, on est amené à utiliser la remarque ci-dessous :

Remarque 1. Soit k un entier naturel pair. Alors :

(i) l'entier $p + 2^k$ est un carré si et seulement si $p = 2^{k/2+1} + 1$;
(ii) l'entier $2^k - p$ est un carré si et seulement si $p = 2^{k/2+1} - 1$.

En effet, soit u l'entier positif tel que $p + 2^k = u^2$. On a $(u + 2^{k/2})(u - 2^{k/2}) = p$, de sorte que $u + 2^{k/2} = p$ et $u - 2^{k/2} = 1$, puis $p - 1 = 2^{k/2+1}$. De même, soit v l'entier positif tel que $2^k - p = v^2$. On a $(2^{k/2} + v)(2^{k/2} - v) = p$, d'où $2^{k/2} + v = p$, $2^{k/2} - v = 1$ et $p + 1 = 2^{k/2+1}$. Les implications réciproques sont immédiates.

4. Les informations qui se trouvent dans la colonne Isogénies des tableaux s'obtiennent à partir des résultats de J. Vélu [Ve2]. Plus précisément, si P est un point d'ordre 2 de E, notons $\langle P\rangle$ le sous-groupe de E engendré par P. Il existe une courbe elliptique $E/\langle P\rangle$ sur $\mathbb{Q}$, unique à $\mathbb{Q}$-isomorphisme près, qui est liée à E par une isogénie sur $\mathbb{Q}$ de degré 2 et de noyau $\langle P\rangle$. Nous indiquons dans les tableaux ci-dessous, en utilisant les résultats de *loc. cit.*, une équation de $E/\langle P\rangle$. Les isogénies indiquées dans l'énoncé des résultats se déduisent alors de ces tableaux par spécialisation des paramètres a et b. On utilise les tableaux des alinéas 1 et 2 pour le théorème 1 et les tableaux des alinéas 3 et 4 pour les autres théorèmes.

Lemme 9. 1) *Supposons qu'il existe a et b dans $\mathbb{Z}$ tels que E ait pour modèle de Weierstrass*

$$y^2 + xy = x^3 + ax^2 + bx.$$

Le point (0,0) *est d'ordre* 2 *dans $E(\mathbb{Q})$ et une équation de $E/\langle(0,0)\rangle$ est donnée ci-dessous* :

	a_1	a_2	a_4	a_6	Isogénies
E	1	a	b	0	**2** : 2
$E/\langle(0,0)\rangle$	1	a	$-4b$	$-b(1+4a)$	**2** : 1

2) *Supposons qu'il existe a et b dans $\mathbb{Z}$ tels que E ait pour modèle de Weierstrass*

$$y^2 + xy = x^3 + ax^2 + \frac{a}{4}\,x.$$

Les points (0,0), $(-1/4, 1/8)$ *et* $(-a, a/2)$ *sont d'ordre* 2 *dans $E(\mathbb{Q})$ et l'on a le tableau ci-dessous* :

	a_1	a_2	a_4	a_6	Isogénies
E	1	a	$a/4$	0	**2** : 2, 3, 4
$E/\langle(0,0)\rangle$	1	$-2a$	$(a/2)(2a-3)$	$(a/4)(a-1)$	**2** : 1
$E/\langle(-1/4,1/8)\rangle$	1	$-a/2$	$a^2/16$	0	**2** : 1
$E/\langle(-a,a/2)\rangle$	1	$4a$	$2a$	$a/4$	**2** : 1

3) *Supposons qu'il existe a et b dans $\mathbb{Z}$ tels que E ait pour modèle de Weierstrass*

$$y^2 = x^3 + ax^2 + bx.$$

Le point (0,0) *est d'ordre* 2 *dans* $E(\mathbb{Q})$ *et une équation de* $E/\langle(0,0)\rangle$ *est donnée ci-dessous* :

	a_1	a_2	a_4	a_6	Isogénies
E	0	a	b	0	**2** : 2
$E/\langle(0,0)\rangle$	0	$-2a$	a^2-4b	0	**2** : 1

4) *Supposons qu'il existe a et b dans $\mathbb{Z}$ tels que E ait pour modèle de Weierstrass*

$$y^2 + xy = x^3 - (a+b)x^2 + abx.$$

Les points (0,0), $(a,0)$ *et* $(b,0)$ *sont d'ordre* 2 *dans* $E(\mathbb{Q})$ *et l'on a le tableau ci-dessous* :

a	a_1	a_2	a_4	a_6	Isogénies
E	0	$-(a+b)$	ab	0	**2** : 2, 3, 4
$E/\langle(0,0)\rangle$	0	$(a+b)/2$	$(a-b)^2/16$	0	**2** : 1
$E/\langle(a,0)\rangle$	0	$2(b-2a)$	b^2	0	**2** : 1
$E/\langle(b,0)\rangle$	0	$2(a-2b)$	a^2	0	**2** : 1

Démonstration. 1) L'alinéa 1 s'obtient directement à partir des formules de [Ve2].

2) Vérifions les assertions relatives à l'alinéa 2. On vérifie directement que les points indiqués sont d'ordre 2 dans $E(\mathbb{Q})$. Soit P l'un de ces points. L'équation de $E/\langle P\rangle$ que l'on obtient en utilisant les formules de Vélu est :

$$y^2 + xy = x^3 + ax^2 - ax - (1+4a)\,\frac{a}{4} \qquad \text{si } P = (0,0),$$

$$y^2 + xy = x^3 + ax^2 + \left(\frac{3}{2}\,a - \frac{5}{16}\right)x + a^2 - \frac{7}{16}\,a + \frac{3}{64} \qquad \text{si } P = \left(-\frac{1}{4}, \frac{1}{8}\right),$$

$$y^2 + xy = x^3 + ax^2 - \left(5a^2 - \frac{3}{2}\,a\right)x + 3a^3 - \frac{7}{4}\,a^2 + \frac{1}{4}\,a \qquad \text{si } P = \left(-a, \frac{a}{2}\right).$$

Les changements de variables

$$x = X - a, \qquad y = Y + \frac{a}{2} \qquad \text{si } P = (0,0),$$

$$x = 4X + 1/4 - a, \qquad y = 8Y + 2X + \frac{a}{2} - \frac{1}{8} \qquad \text{si } P = \left(-\frac{1}{4}, \frac{1}{8}\right),$$

$$x = X + a, \qquad y = Y - \frac{a}{2} \qquad \text{si } P = \left(-a, \frac{a}{2}\right),$$

conduisent alors aux équations indiquées dans le tableau.

3) En ce qui concerne l'alinéa 3, une équation de $E/\langle(0,0)\rangle$ est

$$y^2 = x^3 + ax^2 - 4bx - 4ab.$$

Le changement de variables

$$x = X - a, \qquad y = Y,$$

conduit alors au modèle indiqué.

4) Vérifions les assertions relatives à l'alinéa 4. Soit P l'un des points d'ordre 2 indiqués dans l'énoncé. L'équation de $E/\langle P\rangle$ obtenue en utilisant les formules de Vélu est :

$$\begin{aligned} &y^2 = x^3 - (a+b)x^2 - 4abx + 4ab(a+b) && \text{si } P=(0,0),\\ &y^2 = x^3 - (a+b)x^2 + a(6b-5a)x + a(7ab-4b^2-3a^2) && \text{si } P=(a,0),\\ &y^2 = x^3 - (a+b)x^2 + b(6a-5b)x + b(7ab-4a^2-3b^2) && \text{si } P=(b,0). \end{aligned}$$

Les changements de variables

$$\begin{aligned} &x = 4X + a + b, \quad y = 8Y && \text{si } P=(0,0),\\ &x = X + b - a, \quad y = Y && \text{si } P=(a,0),\\ &x = X + a - b, \quad y = Y && \text{si } P=(b,0), \end{aligned}$$

entraînent alors le résultat.

Cela termine la démonstration du lemme 9.

5. Compte tenu de ce qui précède, il nous reste à vérifier les points (v) à (vii). On utilise pour cela les résultats de [Pa]. Après avoir vérifié que le conducteur de E est bien celui annoncé, les symboles de Kodaira et la minimalité du modèle considéré se déduisent des tableaux de *loc. cit.*

La suite de ce paragraphe est donc désormais consacrée à la détermination du conducteur de E. Le calcul des invariants c_4, c_6 et Δ montre que E a bonne réduction en dehors de 2 et p, et que E a réduction multiplicative en p. Par suite, le conducteur de E est de la forme $2^N p$ où N est un entier tel que $0 \leq N \leq 8$. Deux courbes elliptiques sur $\mathbb{Q}$ qui sont $\mathbb{Q}$-isogènes ont le même conducteur. Par suite, il nous suffira de choisir pour E une seule courbe elliptique parmi celles identifiées par la même lettre dans les énoncés des théorèmes.

Dans toute la suite, étant donné un entier relatif n, on désignera par $v(n)$ sa valuation 2-adique.

3.2.1. *Le théorème 1.* On est amené à déterminer les conducteurs des courbes elliptiques notées A1, B1, C1, D1 et E1 dans l'énoncé du théorème 1. Soit k un entier naturel vérifiant les inégalités $7 \leq k < f(p)$. Les invariants standard de ces courbes sont donnés dans le tableau ci-dessous :

	A1	B1	C1	D1	E1
c_4	$p - 2^{k-2}$	$p + 2^{k-2}$	$p + 2^{k+2}$	$2^{k-2} - p$	$2^{k+2} - p$
Δ	$2^{2k-12}p$	$2^{2k-12}p$	$2^{k-6}p^2$	$-2^{2k-12}p$	$2^{k-6}p^2$

On constate alors que les entiers c_4 et Δ sont premiers entre eux. Ces courbes ont donc réduction multiplicative en 2 et p et leur conducteur est $2p$.

3.2.2. *Le théorème 2.* Vérifions que la courbe elliptique A1 est de conducteur $4p$. On a

$$c_4 = 2^4(p-1), \qquad c_6 = -2^5\sqrt{p-4}\,(2p+1), \qquad \Delta = 2^4 p.$$

On en déduit que $v(c_4) = 6$, $v(c_6) = 5$ et $v(\Delta) = 4$. D'après le tableau IV p. 129 de [Pa], on est dans le cas 3 ou 5 de Tate. Utilisons la proposition 1 p. 124 de *loc. cit.* avec

$r = t = 1$. On a $r^2 - 1 = 0$ et $t^2 - \sqrt{p-4}$ est pair. D'après la condition (2), 4 divise $-1 + \sqrt{p-4}$. On est donc dans le cas 5 de Tate, d'où l'assertion.

3.2.3. *Le théorème 3.* 1) Vérifions que la courbe elliptique A1 est de conducteur $8p$. On a

$$a_1 = 0, \quad a_2 = \sqrt{p-16}, \quad a_3 = 0, \quad a_4 = -4, \quad a_6 = 0,$$
$$b_2 = 4\sqrt{p-16}, \quad b_4 = -2^3, \quad b_6 = 0, \quad b_8 = -2^4,$$
$$c_4 = 2^4(p-4), \quad c_6 = -2^6\sqrt{p-16}(p+2), \quad \Delta = 2^8 p.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) = 6, \quad v(\Delta) = 8.$$

D'après le tableau IV p. 129 de [Pa], on est dans le cas de Tate 6, 7 ou 8. Utilisons les propositions 3 et 4 de *loc. cit.* Posons $r = 2$ et $t = 2$. On a la congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \bmod 32.$$

Par ailleurs, en utilisant la condition (2), on vérifie que

$$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv 0 \bmod 16.$$

On est donc dans un cas de Tate ≥ 7. De plus, si s est un entier, alors

$$a_2 + 3r - sa_1 - s^2 \equiv \sqrt{p-16} + 2 - s^2 \equiv 3 - s^2 \bmod 4.$$

Il n'existe donc pas d'entier s tel que $a_2 + 3r - s^2 \equiv 0 \bmod 4$. On est donc dans le cas de Tate 7 et le conducteur de A1 est $8p$.

2) Vérifions que la courbe elliptique B1 est de conducteur $8p$. On a

$$a_1 = 0, \quad a_2 = \sqrt{p-32}, \quad a_3 = 0, \quad a_4 = -8, \quad a_6 = 0,$$
$$b_2 = 4\sqrt{p-32}, \quad b_4 = -2^4, \quad b_6 = 0, \quad b_8 = -2^6,$$
$$c_4 = 2^4(p-8), \quad c_6 = -2^6\sqrt{p-32}\,(p+4), \quad \Delta = 2^{10}p.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) = 6, \quad v(\Delta) = 10.$$

On est dans le cas de Tate 7 ou 9. Utilisons la proposition 4 de [Pa]. L'entier $r = 4$ vérifie la congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \bmod 32.$$

L'entier $s = 1$ vérifie la congruence $a_2 + 3r - sa_1 - s^2 \equiv 0 \bmod 4$. On est donc dans le cas de Tate 9, d'où l'assertion.

3) Vérifions que la courbe elliptique C1 est de conducteur $8p$. On a

$$a_1 = 0, \quad a_2 = \sqrt{p+32}, \quad a_3 = 0, \quad a_4 = 8, \quad a_6 = 0,$$
$$b_2 = 4\sqrt{p+32}, \quad b_4 = 2^4, \quad b_6 = 0, \quad b_8 = -2^6,$$
$$c_4 = 2^4(p+8), \quad c_6 = -2^6\sqrt{p+32}\,(p-4), \quad \Delta = 2^{10}p.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) = 6, \quad v(\Delta) = 10.$$

On est dans le cas de Tate 7 ou 9. Comme ci-dessus, l'entier $r = 4$ vérifie la congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \bmod 32.$$

L'entier $s = 1$ vérifie donc la congruence $a_2 + 3r - sa_1 - s^2 \equiv 0 \bmod 4$. On est dans le cas de Tate 9, d'où le résultat.

4) Supposons que p soit égal à 31. Dans ce cas, on vérifie par exemple à l'aide du logiciel de calculs PARI (cf. [Pari]) que le conducteur de D1 est $8 \times 31 = 248$.

3.2.4. *Le théorème 4.* Soit k un entier naturel vérifiant les inégalités $4 \leq k < f(p)$.

1) Vérifions que la courbe A1 est de conducteur $16p$. On a

$$a_1 = 0, \quad a_2 = -\sqrt{p - 2^k}, \quad a_3 = 0, \quad a_4 = -2^{k-2}, \quad a_6 = 0,$$
$$b_2 = -4\sqrt{p - 2^k}, \quad b_4 = -2^{k-1}, \quad b_6 = 0, \quad b_8 = -2^{2k-4},$$
$$c_4 = 2^4(p - 2^{k-2}), \quad c_6 = 2^6\sqrt{p - 2^k}\,(p + 2^{k-3}), \quad \Delta = 2^{2k}p.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) = 6, \quad v(\Delta) = 2k.$$

On est dans un cas de Tate ≥ 6. On utilise les propositions 3 et 4 de [Pa].

1.1) Supposons $k = 4$. L'entier $r = 2$ vérifie la congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \bmod 32.$$

Avec $t = 2$, on a

$$v(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1) = 3.$$

On est alors dans le cas 6 de Tate et le conducteur de A1 est $16p$.

1.2) Supposons $k \geq 5$. On est dans un cas de Tate ≥ 7. L'entier $r = 4$ vérifie la congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \bmod 32.$$

Par ailleurs, il n'existe pas d'entier s vérifiant la congruence

$$a_2 + 3r - sa_1 - s^2 \equiv 0 \bmod 4.$$

On est donc dans le cas 7 de Tate et le conducteur de A1 est $16p$.

2) Vérifions que la courbe B1 est de conducteur $16p$. La démonstration est la même que celle de l'alinéa 1.2) ci-dessus. On a

$$c_4 = 2^4(p + 2^{k-2}), \quad c_6 = 2^6\sqrt{p + 2^k}\,(p - 2^{k-3}), \quad \Delta = 2^{2k}p,$$

d'où

$$v(c_4) = 4, \quad v(c_6) = 6, \quad v(\Delta) = 2k,$$

et l'on est dans un cas de Tate ≥ 7. La proposition 4 de [Pa], utilisée avec $r = 4$, entraîne alors notre assertion.

3) Vérifions que la courbe elliptique C1 est de conducteur $16p$. On a

$$a_1 = 0, \quad a_2 = p + 1, \quad a_3 = 0, \quad a_4 = p, \quad a_6 = 0,$$
$$b_2 = 4(p + 1), \quad b_4 = 2p, \quad b_6 = 0, \quad b_8 = -p^2,$$
$$c_4 = 2^4(p^2 - p + 1), \quad c_6 = -2^5(p + 1)(2p^2 - 5p + 2), \quad \Delta = 2^{k+6}p^2.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) = 6, \quad v(\Delta) = k + 6.$$

On est dans un cas de Tate ≥ 7. L'entier $r = -1$ vérifie la congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \bmod 32.$$

Par ailleurs, il n'existe pas d'entier s vérifiant la congruence $a_2 + 3r - sa_1 - s^2 \equiv 0 \bmod 4$. D'après la proposition 4 de [Pa], on est dans le cas 7 de Tate, ce qui entraîne notre assertion.

4) Vérifions que la courbe elliptique D1 est de conducteur $16p$. On a

$$a_1 = 0, \quad a_2 = -\sqrt{p-4}, \quad a_3 = 0, \quad a_4 = -1, \quad a_6 = 0,$$
$$c_4 = 2^4(p-1), \quad c_6 = 2^5\sqrt{p-4}\,(2p+1), \quad \Delta = 2^4p.$$

On a donc

$$v(c_4) = 6, \quad v(c_6) = 5, \quad v(\Delta) = 4.$$

On est dans un cas de Tate 3 ou 5. Utilisons la proposition 1 de [Pa] avec $r = t = 1$. Les entiers $a_4 + r^2$ et $t^2 + a_4a_2 - a_6$ sont pairs. De plus, d'après la condition (2), 4 ne divise pas $a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$. On est donc dans le cas 3 de Tate, d'où l'assertion.

5) Vérifions que la courbe elliptique E1 est de conducteur $16p$. La démonstration est la même que celle de l'alinéa 1.2) ci-dessus. On a

$$c_4 = 2^4(2^{k-2} - p), \quad c_6 = -2^6\sqrt{2^k - p}\,(p + 2^{k-3}), \quad \Delta = -2^{2k}p,$$

d'où

$$v(c_4) = 4, \quad v(c_6) = 6, \quad v(\Delta) = 2k,$$

et l'on est dans un cas de Tate ≥ 7. La proposition 4 de [Pa], utilisée avec $r = 4$, entraîne alors notre assertion.

6) Vérifions que la courbe elliptique F1 est de conducteur $16p$. On a

$$a_1 = 0, \quad a_2 = 1 - p, \quad a_3 = 0, \quad a_4 = -p, \quad a_6 = 0,$$
$$b_2 = 4(1-p), \quad b_4 = -2p, \quad b_6 = 0, \quad b_8 = -p^2,$$
$$c_4 = 2^4(p^2 + p + 1), \quad c_6 = 2^5(p-1)(2p^2 + 5p + 2), \quad \Delta = 2^{k+6}p^2.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) = 6, \quad v(\Delta) = k + 6.$$

On est dans un cas de Tate ≥ 7. L'entier $r = -1$ vérifie la congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \bmod 32.$$

Il n'existe pas d'entier s tel que $a_2 + 3r - sa_1 - s^2 \equiv 0 \bmod 4$, donc on est dans le cas 7 de Tate et le conducteur de F1 est $16p$.

3.2.5. *Le théorème 5.* 1) Vérifions que la courbe A1 est de conducteur $32p$. On a

$$a_1 = 0, \quad a_2 = 2\sqrt{p-1}, \quad a_3 = 0, \quad a_4 = -1, \quad a_6 = 0,$$
$$c_4 = 2^4(4p-1), \quad c_6 = -2^6\sqrt{p-1}\,(8p+1), \quad \Delta = 2^6p.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) \geq 6, \quad v(\Delta) = 6.$$

On est dans le cas 3 ou 4 de Tate. Posons $r = 1$ et $t = 0$. Les entiers $a_4 + r^2$ et $t^2 + a_4a_2 - a_6$ sont pairs. De plus, l'entier $a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$ est un multiple de 4. D'après la proposition 1 de [Pa], on est dans le cas 4 de Tate. Le conducteur de A1 est donc $32p$.

2) Vérifions que la courbe A1′ est de conducteur $32p$. On a

$$a_1 = 0, \quad a_2 = -2\sqrt{p-1}, \quad a_3 = 0, \quad a_4 = -1, \quad a_6 = 0,$$
$$c_4 = 2^4(4p-1), \quad c_6 = 2^6\sqrt{p-1}\,(8p+1), \quad \Delta = 2^6p.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) \geq 6, \quad v(\Delta) = 6.$$

On est dans le cas 3 ou 4 de Tate. On démontre alors comme dans l'alinéa 1 ci-dessus que l'on est dans le cas 4 de Tate, d'où l'assertion.

3) Vérifions que les courbes B2, B2′, C2, C2′ sont de conducteur $32p$. Les invariants standard des courbes B2 et C2 sont donnés dans le tableau ci-dessous :

	B2	C2
c_4	$2^4(p-32)$	$2^4(p+32)$
c_6	$-2^6\sqrt{p-8}\,(p+64)$	$-2^6\sqrt{p+8}\,(p-64)$
Δ	-2^9p^2	2^9p^2

On constate que l'on a dans les deux cas $v(c_4) = 4$, $v(c_6) = 6$ et $v(\Delta) = 9$. On utilisera à plusieurs reprises la remarque suivante :

Remarque 2. Soient W et W' deux équations de Weierstrass sur $\mathbb{Q}$ qui sont tordues quadratiques l'une de l'autre par $\sqrt{-1}$. Soient c_4, c_6 et Δ les invariants standard associés à W et c_4', c_6' et Δ' ceux de W'. On a les égalités

$$c_4 = c_4', \quad c_6 = -c_6', \quad \Delta = \Delta'.$$

Les courbes B2′ et C2′ sont les tordues quadratiques respectivement de B2 et C2 par $\sqrt{-1}$. D'après la remarque 2, les valuations des invariants de B2 et C2 sont les mêmes que celles des invariants de B2′ et C2′. Notre assertion se déduit alors directement du tableau IV p. 129 de [Pa].

3.2.6. *Le théorème 6.* Soit k un entier vérifiant les inégalités $2 \leq k < f(p)$.

1) Vérifions que la courbe A1 est de conducteur $64p$. On a

$$a_1 = 0, \quad a_2 = 2\sqrt{p-1}, \quad a_3 = 0, \quad a_4 = p, \quad a_6 = 0,$$
$$c_4 = 2^4(p-4), \quad c_6 = 2^6\sqrt{p-1}\,(p+8), \quad \Delta = -2^6p^2.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) \geq 6, \quad v(\Delta) = 6.$$

On est dans le cas 3 ou 4 de Tate. Posons $r = 1$ et $t = 0$. Les entiers $a_4 + r^2$ et $t^2 + a_4a_2 - a_6$ sont pairs. Puisque $p - 1$ est un carré on a $p \equiv 1 \bmod 4$. On vérifie alors

que l'entier $a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$ n'est pas divisible par 4. On est dans le cas 3 de Tate, d'où l'assertion.

2) Vérifions que la courbe A1′ est de conducteur $64p$. On a

$$a_1 = 0, \quad a_2 = -2\sqrt{p-1}, \quad a_3 = 0, \quad a_4 = p, \quad a_6 = 0,$$
$$c_4 = 2^4(p-4), \quad c_6 = -2^6\sqrt{p-1}\,(p+8) \quad \Delta = -2^6p^2.$$

On a donc

$$v(c_4) = 4, \quad v(c_6) \geq 6, \quad v(\Delta) = 6.$$

On est dans le cas 3 ou 4 de Tate et la même démonstration que celle de l'alinéa 1 ci-dessus montre que l'on est dans le cas 3 de Tate, d'où l'assertion.

3) Vérifions que les courbes B2, B2′, C2, C2′, D1, D1′, E2, E2′, F1 et F1′ sont de conducteur $64p$. Les invariants standard des courbes B2, C2, D1, E2 et F1 sont donnés dans les tableaux ci-dessous :

	B2	C2	D1
c_4	$2^6(p-2^{k+2})$	$2^6(p+2^{k+2})$	$2^6(p^2-p+1)$
c_6	$-2^9\sqrt{p-2^k}\,(p+2^{k+3})$	$-2^9\sqrt{p+2^k}\,(p-2^{k+3})$	$-2^8(p-2)(2p-1)(p+1)$
Δ	$-2^{k+12}p^2$	$2^{k+12}p^2$	$2^{k+12}p^2$

	E2	F1
c_4	$2^6(2^{k+2}-p)$	$2^6(p^2+p+1)$
c_6	$2^9\sqrt{2^k-p}\,(p+2^{k+3})$	$2^8(p-1)(2p+1)(p+2)$
Δ	$2^{k+12}p^2$	$2^{k+12}p^2$

On constate que l'on a dans tous les cas $v(c_4) = 6$, $v(c_6) = 9$ et $v(\Delta) \geq 14$. Compte tenu de la remarque 2, notre assertion se déduit directement du tableau IV p. 129 de [Pa].

3.2.7. *Le théorème 7.* Vérifions que les courbes A1, B1, C1, D1, E1 et F1, ainsi que leurs tordues quadratiques par $\sqrt{-1}$, sont de conducteur $128p$. Leurs invariants standard sont donnés dans les tableaux ci-dessous :

	A1	B1	C1	D1
c_4	$2^4(8p^i-1)$	$2^5(p^i-2)$	$2^4(p^k+8)$	$2^5(2p^k+1)$
c_6	$-2^6\sqrt{2p^i-1}\,(16p^i+1)$	$2^7\sqrt{2p^i-1}\,(p^i+4)$	$2^6\sqrt{p^k+2}\,(p^k-16)$	$-2^7\sqrt{p^k+2}\,(4p^k-1)$
Δ	2^7p^i	-2^8p^{2i}	2^7p^{2k}	2^8p^k

	E1	F1
c_4	$2^4(p-8)$	$2^5(2p-1)$
c_6	$2^6\sqrt{p-2}\,(p+16)$	$-2^7\sqrt{p-2}\,(4p+1)$
Δ	-2^7p^2	2^8p

On constate alors que l'on est dans l'un des cas suivants :

1) $v(c_4) = 4$, $v(c_6) = 6$ et $v(\Delta) = 7$;
2) $v(c_4) = 5$, $v(c_6) = 7$ et $v(\Delta) = 8$.

La remarque 2 et le tableau IV p. 129 de [Pa] entraînent alors notre assertion.

3.2.8. *Le théorème 8.* Vérifions que les courbes A1, B1, C1 et D1, ainsi que leurs tordues quadratiques par $\sqrt{-1}$, sont de conducteur $256p$. Les invariants standard des courbes A1, B1, C1 et D1 sont donnés dans le tableau ci-dessous :

	A1	B1	C1	D1
c_4	$2^5(4p^k-1)$	$2^5(p^k-4)$	$2^5(4p^k+1)$	$2^5(p^k+4)$
$c_6/2^8$	$-\sqrt{(p^k-1)/2}\,(8p^k+1)$	$\sqrt{(p^k-1)/2}\,(p^k+8)$	$-\sqrt{(p^k+1)/2}\,(8p^k-1)$	$\sqrt{(p^k+1)/2}\,(p^k-8)$
Δ	2^9p^k	-2^9p^{2k}	2^9p^k	2^9p^{2k}

On constate alors que l'on a dans tous les cas $v(c_4) = 5$, $v(c_6) \geq 8$ et $v(\Delta) = 9$. La remarque 2 et le tableau IV p. 129 de [Pa] entraînent alors notre assertion.

Cela termine la vérification du fait que les courbes elliptiques qui interviennent dans les énoncés des théorèmes satisfont aux conditions annoncées.

3.3. Liste des classes de $\mathbb{Q}$-isomorphisme. Soit E une courbe elliptique définie sur $\mathbb{Q}$, ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$ et de conducteur de la forme $2^N p$ avec $N \geq 1$. D'après le lemme 1, il existe deux entiers a et b sans diviseurs communs impairs tels que E ait un modèle de Weierstrass, minimal en dehors de 2, de la forme

$$y^2 = x^3 + ax^2 + bx.$$

Rappelons que les invariants standard c_4, c_6 et Δ associés à ce modèle sont

$$c_4 = 2^4(a^2 - 3b), \quad c_6 = 2^5a(9b - 2a^2), \quad \Delta = 2^4b^2(a^2 - 4b).$$

On déduit de l'hypothèse faite sur le conducteur de E l'existence de deux entiers naturels m et n, avec $n \neq 0$, tels que l'on ait l'égalité

$$b^2(a^2 - 4b) = \pm 2^m p^n. \tag{14}$$

On a $b \neq 0$. Dans ce qui suit, on va examiner les quatre cas suivants :

A) $b > 0$ et p ne divise pas b ;
B) $b > 0$ et p divise b ;
C) $b < 0$ et p ne divise pas b ;
D) $b < 0$ et p divise b.

A) *Cas où b est positif et p ne divise pas b.* On a le lemme ci-dessous :

LEMME 10. *Supposons $b > 0$ non divisible par p. Alors, on est dans l'un des cinq cas suivants* :

1. *il existe un entier k vérifiant les inégalités $2 \leq k < f(p)$ tel que l'une des conditions ci-dessous soit vérifiée* :

   (i) *l'entier $p+2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm \sqrt{p+2^k}\,x^2 + 2^{k-2}x, \quad y^2 = x^3 \pm 2\sqrt{p+2^k}\,x^2 + 2^kx,$$

   (ii) *l'entier $2^k - p$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm \sqrt{2^k-p}\,x^2 + 2^{k-2}x, \quad y^2 = x^3 \pm 2\sqrt{2^k-p}\,x^2 + 2^kx\,;$$

2. *il existe un entier $k \geq 5$ tel que l'une des conditions ci-dessous soit vérifiée* :

(i) $p = 2^k + 1$ *et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 = x^3 \pm 2(2p-1)x^2 + x, \quad y^2 = x^3 \pm 4(2p-1)x^2 + 4x,$$

(ii) $p = 2^k - 1$ *et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 = x^3 \pm (p+2)x^2 + (p+1)x, \quad y^2 = x^3 \pm 2(p+2)x^2 + 4(p+1)x,$$
$$y^2 = x^3 \pm 2(2p+1)x^2 + x, \quad y^2 = x^3 \pm 4(2p+1)x^2 + 4x\,;$$

3. *il existe un entier impair k vérifiant $1 \leq k \leq 164969$ tel que $p^k + 2$ soit un carré et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 = x^3 \pm 2\sqrt{p^k+2}\,x^2 + 2x, \quad y^2 = x^3 \pm 4\sqrt{p^k+2}\,x^2 + 8x\,;$$

4. *l'entier $(p^2+1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 = x^3 \pm 4\sqrt{(p^2+1)/2}\,x^2 + 2x, \quad y^2 = x^3 \pm 8\sqrt{(p^2+1)/2}\,x^2 + 8x\,;$$

5. *l'entier $(p+1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 = x^3 \pm 4\sqrt{(p+1)/2}\,x^2 + 2x, \quad y^2 = x^3 \pm 8\sqrt{(p+1)/2}\,x^2 + 8x.$$

Démonstration. Il résulte de (14) que les seuls diviseurs premiers positifs possibles de b sont 2 et p. Il existe donc un entier i tel que

$$0 \leq 2i \leq m, \quad b = 2^i.$$

On obtient ainsi

$$a^2 - 2^{i+2} = \pm 2^{m-2i} p^n. \tag{15}$$

On est donc dans l'un des trois cas 1), 2) et 3) ci-dessous :

1) $i + 2 > m - 2i$. Dans ce cas, $v(a^2) = m - 2i$. On a donc

$$m \equiv 0 \bmod 2.$$

En posant

$$u = \frac{a}{2^{m/2-i}}, \tag{16}$$

on déduit de (15) que

$$u^2 - 2^{3i+2-m} = \pm p^n.$$

1.1) Supposons que

$$u^2 - 2^{3i+2-m} = p^n. \tag{17}$$

1.1.1) Supposons que

$$3i + 2 - m \geq 2. \tag{18}$$

D'après le lemme 5, on est dans l'un des cas ci-dessous :

(i) $p = 2^{3i-m} - 1$ avec $3i - m \geq 5$, $n = 2$ et $u = \pm(p+2)$.
(ii) $n = 1$, $3i + 2 - m < f(p)$.

Supposons que l'on soit dans le cas (i). La courbe E a alors pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{m/2-i}\,(p+2)x^2 + 2^i x.$$

Il existe deux entiers q_1 et r_1 tels que

$$m/2 - i = 2q_1 + r_1 \quad \text{avec } r_1 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_1}}, \quad Y = \frac{y}{2^{3q_1}}, \tag{19}$$

on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm (p+2)X^2 + (p+1)X \quad \text{ou} \quad Y^2 = X^3 \pm 2(p+2)X^2 + 4(p+1)X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On se trouve ainsi dans le cas 2(ii) de l'énoncé du lemme avec $k = 3i - m$.

Supposons que l'on soit dans le cas (ii). D'après (16) et (17), l'entier $p + 2^{3i+2-m}$ est un carré et

$$a = \pm 2^{m/2-i}\sqrt{p + 2^{3i+2-m}}.$$

La courbe E a donc pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{m/2-i}\sqrt{p + 2^{3i+2-m}}\, x^2 + 2^i x.$$

En effectuant le changement de variables (19), on obtient comme modèle de E

$$Y^2 = X^3 \pm \sqrt{p + 2^{3i+2-m}}\, X^2 + 2^{3i-m} X$$

ou bien

$$Y^2 = X^3 \pm 2\sqrt{p + 2^{3i+2-m}}\, X^2 + 2^{3i+2-m} X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On est donc dans le cas 1(i) du lemme avec $k = 3i + 2 - m$. D'après (18) et la condition (ii) envisagée ci-dessus on a $2 \leq k < f(p)$.

1.1.2) Supposons que

$$3i + 2 - m = 1. \tag{20}$$

D'après (17) on a l'égalité

$$u^2 - 2 = p^n.$$

D'après le lemme 8, n est impair et $n \leq 164969$. L'entier $p^n + 2$ est un carré et

$$a = \pm 2^{m/2-i}\sqrt{p^n + 2}.$$

La courbe E a donc pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{m/2-i}\sqrt{p^n + 2}\, x^2 + 2^i x.$$

Il existe deux entiers q_2 et r_2 tels que

$$m/2 - i - 1 = 2q_2 + r_2 \quad \text{avec } r_2 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_2}}, \quad Y = \frac{y}{2^{3q_2}},$$

on obtient, en utilisant la condition (20), comme nouveau modèle de E

$$Y^2 = X^3 \pm 2\sqrt{p^n + 2}\, X^2 + 2X \quad \text{ou} \quad Y^2 = X^3 \pm 4\sqrt{p^n + 2}\, X^2 + 8X.$$

suivant que $r_2 = 0$ ou $r_2 = 1$. On est ainsi dans le cas 3 du lemme avec $k = n$.

1.2) Supposons que

$$u^2 - 2^{3i+2-m} = -p^n.$$

D'après le lemme 6, on a $n = 1$ et $3i + 2 - m < f(p)$. L'entier $2^{3i+2-m} - p$ est un carré et l'on a

$$a = \pm 2^{m/2-i}\sqrt{2^{3i+2-m} - p}.$$

La courbe E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{m/2-i}\sqrt{2^{3i+2-m} - p}\, x^2 + 2^i x.$$

Le changement de variables (19) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm \sqrt{2^{3i+2-m} - p}\, X^2 + 2^{3i-m} X$$

ou bien

$$Y^2 = X^3 \pm 2\sqrt{2^{3i+2-m} - p}\, X^2 + 2^{3i-m+2} X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On est donc dans le cas 1(ii) du lemme avec $k = 3i + 2 - m$. Notons que $2 \leq k < f(p)$.

2) $i + 2 = m - 2i$. D'après (15), on a dans ce cas

$$v(a^2) \geq i + 2.$$

On est alors dans l'un des cas ci-dessous :

2.1) Supposons que l'entier i soit pair. Dans ce cas,

$$v(a) \geq i/2 + 1.$$

Posons

$$u = \frac{a}{2^{i/2+1}}.$$

Il résulte de (15) que

$$u^2 - 1 = p^n.$$

Le lemme 2 entraîne alors une contradiction.

2.2) Supposons que l'entier i soit impair. Dans ce cas,

$$v(a) \geq (i + 1)/2 + 1.$$

Posons

$$u = \frac{a}{2^{(i+1)/2+1}}.$$

Il résulte de (15) que

$$2u^2 - 1 = p^n.$$

D'après l'alinéa 2 du lemme 7, on a $n = 1$ ou $n = 2$.

(i) Supposons $n = 2$. L'entier $(p^2 + 1)/2$ est un carré, on a $u = \pm\sqrt{(p^2 + 1)/2}$ et E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{(i+1)/2+1}\sqrt{(p^2 + 1)/2}\, x^2 + 2^i x.$$

Il existe deux entiers q_3 et r_3 tels que

$$(i - 1)/2 = 2q_3 + r_3 \quad \text{avec } r_3 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_3}}, \quad Y = \frac{y}{2^{3q_3}}, \tag{21}$$

on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm 4\sqrt{(p^2+1)/2}\,X^2 + 2X \quad \text{ou} \quad Y^2 = X^3 \pm 8\sqrt{(p^2+1)/2}\,X^2 + 8X,$$

suivant que $r_3 = 0$ ou $r_3 = 1$. On est donc dans le cas 4 du lemme.

(ii) Supposons $n = 1$. L'entier $(p+1)/2$ est un carré. On a $u = \pm\sqrt{(p+1)/2}$ et E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{(i+1)/2+1}\sqrt{(p+1)/2}\,x^2 + 2^i x.$$

Le changement de variables (21) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 4\sqrt{(p+1)/2}\,X^2 + 2X \quad \text{ou} \quad Y^2 = X^3 \pm 8\sqrt{(p+1)/2}\,X^2 + 8X,$$

suivant que $r_3 = 0$ ou $r_3 = 1$. On est alors dans le cas 5 du lemme.

3) $i + 2 < m - 2i$. D'après (15), on a $v(a^2) = i + 2$, de sorte que i est pair. On a donc $v(a) = i/2 + 1$. Posons

$$u = \frac{a}{2^{i/2+1}}.$$

On déduit de (15) que

$$u^2 - 1 = 2^{m-3i-2}p^n.$$

D'après le lemme 2, on est dans l'un des cas ci-dessous :

(i) $p = 2^{m-3i-4} + 1$ avec $m - 3i - 2 \geq 5$, $n = 1$ et $u = \pm(2p-1)$;
(ii) $p = 2^{m-3i-4} - 1$ avec $m - 3i - 2 \geq 5$, $n = 1$ et $u = \pm(2p+1)$.

Supposons que l'on soit dans le cas (i). La courbe E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{i/2+1}(2p-1)x^2 + 2^i x.$$

Il existe deux entiers q_4 et r_4 tels que

$$i/2 = 2q_4 + r_4 \quad \text{avec } r_4 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_4}}, \quad Y = \frac{y}{2^{3q_4}}, \tag{22}$$

on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm 2(2p-1)X^2 + X \quad \text{ou} \quad Y^2 = X^3 \pm 4(2p-1)X^2 + 4X,$$

suivant que $r_4 = 0$ ou $r_4 = 1$. On constate alors que l'on est dans le cas 2(i) du lemme avec $k = m - 3i - 4$.

Supposons que l'on soit dans le cas (ii). La courbe E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{i/2+1}(2p+1)x^2 + 2^i x.$$

Le changement de variables (22) conduit au nouveau modèle

$$Y^2 = X^3 \pm 2(2p+1)X^2 + X \quad \text{ou} \quad Y^2 = X^3 \pm 4(2p+1)X^2 + 4X,$$

suivant que $r_4 = 0$ ou $r_4 = 1$. On est ainsi dans le cas 2(ii) du lemme avec $k = m - 3i - 4$.

Cela termine la démonstration du lemme.

B) *Cas où b est positif et p divise b.* On a le lemme ci-dessous :

LEMME 11. *Supposons $b > 0$ divisible par p. Alors, on est dans l'un des neuf cas suivants :*

1. *il existe un entier k vérifiant les inégalités $0 \le k < f(p)$ tel que l'une des conditions ci-dessous soit vérifiée :*
   (i) *l'entier $p - 2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 2\sqrt{p-2^k}\,x^2 + px, \quad y^2 = x^3 \pm 4\sqrt{p-2^k}\,x^2 + 4px,$$
   (ii) *l'entier $p + 2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 2\sqrt{p+2^k}\,x^2 + px, \quad y^2 = x^3 \pm 4\sqrt{p+2^k}\,x^2 + 4px\,;$$
2. *il existe un entier $k \ge 5$ tel que l'une des conditions ci-dessous soit vérifiée :*
   (i) *$p = 2^k + 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm (2p-1)x^2 + (p-1)px, \quad y^2 = x^3 \pm 2(2p-1)x^2 + 4(p-1)px,$$
   $$y^2 = x^3 \pm 2(p-2)x^2 + p^2x, \quad y^2 = x^3 \pm 4(p-2)x^2 + 4p^2x,$$
   (ii) *$p = 2^k - 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm (2p+1)x^2 + (p+1)px, \quad y^2 = x^3 \pm 2(2p+1)x^2 + 4(p+1)px,$$
   $$y^2 = x^3 \pm 2(p+2)x^2 + p^2x, \quad y^2 = x^3 \pm 4(p+2)x^2 + 4p^2x\,;$$
3. *l'entier $2p^2 - 1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 2\sqrt{2p^2-1}\,x^2 + 2p^2x, \quad y^2 = x^3 \pm 4\sqrt{2p^2-1}\,x^2 + 8p^2x\,;$$
4. *l'entier $2p - 1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 2\sqrt{2p-1}\,x^2 + 2px, \quad y^2 = x^3 \pm 4\sqrt{2p-1}\,x^2 + 8px\,;$$
5. *l'entier $(p^2-1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 4\sqrt{(p^2-1)/2}\,x^2 + 2p^2x, \quad y^2 = x^3 \pm 8\sqrt{(p^2-1)/2}\,x^2 + 8p^2x\,;$$
6. *l'entier $(p-1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 4\sqrt{(p-1)/2}\,x^2 + 2px, \quad y^2 = x^3 \pm 8\sqrt{(p-1)/2}\,x^2 + 8px\,;$$
7. *l'entier $(p^2+1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 4\sqrt{(p^2+1)/2}\,x^2 + 2p^2x, \quad y^2 = x^3 \pm 8\sqrt{(p^2+1)/2}\,x^2 + 8p^2x\,;$$
8. *l'entier $(p+1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 4\sqrt{(p+1)/2}\,x^2 + 2px, \quad y^2 = x^3 \pm 8\sqrt{(p+1)/2}\,x^2 + 8px\,;$$
9. *il existe un entier impair k vérifiant $1 \le k \le 164969$ tel que $p^k + 2$ soit un carré et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
   $$y^2 = x^3 \pm 2\sqrt{p^k+2}\,x^2 + p^kx, \quad y^2 = x^3 \pm 4\sqrt{p^k+2}\,x^2 + 4p^kx.$$

Démonstration. D'après (14), les seuls diviseurs premiers positifs possibles de b sont 2 et p. Puisque a et b n'ont pas de diviseur commun impair, p ne divise pas a et on a

$$n \equiv 0 \bmod 2.$$

Il existe donc un entier i tel que

$$0 \le 2i \le m, \quad b = 2^i p^{n/2}.$$

En utilisant (14), on obtient ainsi

$$a^2 - 2^{i+2}p^{n/2} = \pm 2^{m-2i}. \tag{23}$$

On est donc dans l'un des trois cas 1), 2) et 3) ci-dessous :

1) $i+2 > m-2i$. Dans ce cas, on a $v(a^2) = m-2i$, donc

$$m \equiv 0 \bmod 2.$$

En posant

$$u = \frac{a}{2^{m/2-i}}, \tag{24}$$

on déduit de (23) que

$$u^2 - 2^{3i+2-m}p^{n/2} = \pm 1.$$

1.1) Supposons que

$$u^2 - 2^{3i+2-m}p^{n/2} = 1.$$

D'après le lemme 2, on est dans l'un des cas suivants :

(i) $p = 2^{3i-m}+1$ avec $3i+2-m \geq 5$, $n/2 = 1$ et $u = \pm(2p-1)$;
(ii) $p = 2^{3i-m}-1$ avec $3i+2-m \geq 5$, $n/2 = 1$ et $u = \pm(2p+1)$.

Supposons que l'on soit dans le cas (i). D'après (24), la courbe E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{m/2-i}(2p-1)x^2 + 2^i px.$$

Il existe deux entiers q_1 et r_1 tels que

$$m/2 - i = 2q_1 + r_1 \quad \text{avec } r_1 = 0 \text{ ou } 1.$$

Posons

$$X = \frac{x}{2^{2q_1}}, \quad Y = \frac{y}{2^{3q_1}}. \tag{25}$$

En effectuant ce changement de variables, on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm (2p-1)X^2 + (p-1)pX \quad \text{ou} \quad Y^2 = X^3 \pm 2(2p-1)X^2 + 4(p-1)pX,$$

selon que $r_1 = 0$ ou $r_1 = 1$. Puisque $p \geq 29$, on a $3i - m \geq 5$; on est ainsi dans le cas 2(i) du lemme avec $k = 3i-m$.

Supposons que l'on soit dans le cas (ii). Il résulte de (24) que la courbe E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{m/2-i}(2p+1)x^2 + 2^i px.$$

En effectuant le changement de variables (25), on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm (2p+1)X^2 + (p+1)pX \quad \text{ou} \quad Y^2 = X^3 \pm 2(2p+1)X^2 + 4(p+1)pX,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On est dans le cas 2(ii) du lemme avec $k = 3i-m$.

1.2) Supposons que

$$u^2 - 2^{3i+2-m}p^{n/2} = -1.$$

D'après le lemme 3, on est dans l'un des cas suivants :

(i) $3i+2-m = 1$ et $n/2 = 2$;
(ii) $3i+2-m = 1$ et $n/2 = 1$.

Supposons que l'on soit dans le cas (i). L'entier $2p^2-1$ est un carré et $u=\pm\sqrt{2p^2-1}$. On déduit de (24) que la courbe E a pour modèle de Weierstrass

$$y^2=x^3\pm 2^{m/2-i}\sqrt{2p^2-1}\,x^2+2^ip^2x.$$

Il existe deux entiers q_2 et r_2 tels que

$$m/2-i-1=2q_2+r_2 \quad \text{avec } r_2=0 \text{ ou } 1.$$

En posant

$$X=\frac{x}{2^{2q_2}}, \quad Y=\frac{y}{2^{3q_2}}, \tag{26}$$

on obtient comme nouveau modèle de E

$$Y^2=X^3\pm 2\sqrt{2p^2-1}\,X^2+2p^2X \quad \text{ou} \quad Y^2=X^3\pm 4\sqrt{2p^2-1}\,X^2+8p^2X,$$

selon que $r_2=0$ ou $r_2=1$. On est dans le cas 3 du lemme.

Supposons que l'on soit dans le cas (ii). Alors, l'entier $2p-1$ est un carré et $u=\pm\sqrt{2p-1}$. On déduit de (24) que la courbe E a pour modèle de Weierstrass

$$y^2=x^3\pm 2^{m/2-i}\sqrt{2p-1}\,x^2+2^ipx.$$

Le changement de variables (26) conduit au nouveau modèle de E

$$Y^2=X^3\pm 2\sqrt{2p-1}X^2+2pX \quad \text{ou} \quad Y^2=X^3\pm 4\sqrt{2p-1}\,X^2+8pX,$$

selon que $r_2=0$ ou $r_2=1$. On est dans le cas 4 du lemme.

2) $i+2=m-2i$. Alors, d'après (23),

$$v(a^2)\geq i+2.$$

On est donc dans l'un des cas ci-dessous :

2.1) Supposons que l'entier i soit pair. On a

$$v(a)\geq i/2+1.$$

Posons

$$u=\frac{a}{2^{i/2+1}}. \tag{27}$$

On déduit de (23) que

$$u^2-p^{n/2}=\pm 1.$$

On est donc dans l'un des cas suivants :

2.1.1) Supposons que

$$u^2-p^{n/2}=-1.$$

D'après le lemme 3, $n/2=1$. L'entier $p-1$ est donc un carré et $u=\pm\sqrt{p-1}$. On déduit de (27) que la courbe E a pour modèle de Weierstrass

$$y^2=x^3\pm 2^{i/2+1}\sqrt{p-1}\,x^2+2^ipx.$$

Il existe deux entiers q_3 et r_3 tels que

$$i/2=2q_3+r_3 \quad \text{avec } r_3=0 \text{ ou } 1.$$

En posant

$$X=\frac{x}{2^{2q_3}}, \quad Y=\frac{y}{2^{3q_3}},$$

on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm 2\sqrt{p-1}\,X^2 + pX \quad \text{ou} \quad Y^2 = X^3 \pm 4\sqrt{p-1}\,X^2 + 4pX,$$

selon que $r_3 = 0$ ou $r_3 = 1$. On est dans le cas 1(i) du lemme avec $k = 0$.

2.1.2) Supposons que

$$u^2 - p^{n/2} = 1.$$

On déduit alors du lemme 2 une contradiction.

2.2) Supposons que l'entier i soit impair. On a alors

$$v(a) \geq (i+1)/2 + 1.$$

Posons

$$u = \frac{a}{2^{(i+1)/2+1}}. \tag{28}$$

On déduit de (23) que

$$2u^2 - p^{n/2} = \pm 1.$$

On est donc dans l'un des cas suivants :

2.2.1) Supposons que

$$2u^2 - p^{n/2} = -1.$$

D'après l'alinéa 1 du lemme 7, on est dans l'un des cas ci-dessous :

(i) $n/2 = 2$;
(ii) $n/2 = 1$.

Supposons que l'on soit dans le cas (i). L'entier $(p^2-1)/2$ est un carré et $u = \pm\sqrt{(p^2-1)/2}$. On déduit de (28) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{(i+1)/2+1}\sqrt{(p^2-1)/2}\,x^2 + 2^i p^2 x.$$

Il existe deux entiers q_4 et r_4 tels que

$$(i-1)/2 = 2q_4 + r_4 \quad \text{avec } r_4 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_4}}, \quad Y = \frac{y}{2^{3q_4}}, \tag{29}$$

on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm 4\sqrt{(p^2-1)/2}\,X^2 + 2p^2X \quad \text{ou} \quad Y^2 = X^3 \pm 8\sqrt{(p^2-1)/2}\,X^2 + 8p^2X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 5 du lemme.

Supposons que l'on soit dans le cas (ii). L'entier $(p-1)/2$ est un carré et $u = \pm\sqrt{(p-1)/2}$. On déduit de (28) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{(i+1)/2+1}\sqrt{(p-1)/2}\,x^2 + 2^i p x.$$

En utilisant le changement de variables (29), on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm 4\sqrt{(p-1)/2}\,X^2 + 2pX \quad \text{ou} \quad Y^2 = X^3 \pm 8\sqrt{(p-1)/2}X^2 + 8pX,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 6 du lemme.

2.2.2) Supposons que

$$2u^2 - p^{n/2} = 1.$$

D'après l'alinéa 2 du lemme 7, on est dans l'un des cas ci-dessous :

(i) $n/2 = 2$;
(ii) $n/2 = 1$.

Supposons que l'on soit dans le cas (i). L'entier $(p^2+1)/2$ est un carré et $u = \pm\sqrt{(p^2+1)/2}$. On déduit de (28) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{(i+1)/2+1}\sqrt{(p^2+1)/2}\,x^2 + 2^i p^2 x.$$

Le changement de variables (29) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 4\sqrt{(p^2+1)/2}\,X^2 + 2p^2X \quad \text{ou} \quad Y^2 = X^3 \pm 8\sqrt{(p^2+1)/2}\,X^2 + 8p^2X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 7 du lemme.

Supposons que l'on soit dans le cas (ii). L'entier $(p+1)/2$ est un carré et $u = \pm\sqrt{(p+1)/2}$. On déduit de (28) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{(i+1)/2+1}\sqrt{(p+1)/2}\,x^2 + 2^i p x.$$

En utilisant le changement de variables (29), on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm 4\sqrt{(p+1)/2}\,X^2 + 2pX \quad \text{ou} \quad Y^2 = X^3 \pm 8\sqrt{(p+1)/2}\,X^2 + 8pX,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 8 du lemme.

3) $i+2 < m-2i$. On déduit de (23) que $v(a^2) = i+2$. Par conséquent, i est pair et $v(a) = i/2+1$. Posons

$$u = \frac{a}{2^{i/2+1}}. \tag{30}$$

Il résulte de (23) que

$$u^2 - p^{n/2} = \pm 2^{m-3i-2}.$$

On est donc dans l'un des cas ci-dessous :

3.1) Supposons que

$$u^2 - p^{n/2} = -2^{m-3i-2}.$$

On déduit du lemme 4 que l'on est dans l'un des cas suivants :

(i) $p = 2^{m-3i-4}+1$ avec $m-3i-2 \geq 5$, $n/2 = 2$ et $u = \pm(p-2)$;
(ii) $n/2 = 1$ et $m-3i-2 < \log p/\log 2$.

Supposons que l'on soit dans le cas (i). Il résulte de (30) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{i/2+1}(p-2)x^2 + 2^i p^2 x.$$

Il existe deux entiers q_5 et r_5 tels que

$$i/2 = 2q_5 + r_5 \quad \text{avec } r_5 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_5}}, \quad Y = \frac{y}{2^{3q_5}}, \tag{31}$$

on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm 2(p-2)X^2 + p^2X \quad \text{ou} \quad Y^2 = X^3 \pm 4(p-2)X^2 + 4p^2X,$$

selon que $r_5 = 0$ ou $r_5 = 1$. On a $m - 3i - 4 \geq 5$ et l'on est dans le cas 2(i) du lemme avec $k = m - 3i - 4$.

Supposons que l'on soit dans le cas (ii). L'entier $p - 2^{m-3i-2}$ est un carré et $u = \pm\sqrt{p - 2^{m-3i-2}}$. Il résulte de (30) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{i/2+1}\sqrt{p - 2^{m-3i-2}}\, x^2 + 2^i p x.$$

Le changement de variables (31) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 2\sqrt{p - 2^{m-3i-2}}\, X^2 + pX \quad \text{ou} \quad Y^2 = X^3 \pm 4\sqrt{p - 2^{m-3i-2}}\, X^2 + 4pX,$$

selon que $r_5 = 0$ ou $r_5 = 1$. On est dans le cas 1(i) du lemme avec $k = m - 3i - 2$.

3.2) Supposons que

$$u^2 - p^{n/2} = 2^{m-3i-2}.$$

Distinguons les cas suivants :

3.2.1) Supposons que $m - 3i - 2 \geq 2$. D'après le lemme 5, on est dans l'un des cas ci-dessous :

(i) $p = 2^{m-3i-4} - 1$ avec $m - 3i - 2 \geq 4$, $n/2 = 2$ et $u = \pm(p + 2)$;
(ii) $n/2 = 1$ et $m - 3i - 2 < f(p)$.

Supposons que l'on soit dans le cas (i). Il résulte de (30) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{i/2+1}(p + 2)x^2 + 2^i p^2 x.$$

Le changement de variables (31) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 2(p + 2)X^2 + p^2 X \quad \text{ou} \quad Y^2 = X^3 \pm 4(p + 2)X^2 + 4p^2 X,$$

selon que $r_5 = 0$ ou $r_5 = 1$. On a $m - 3i - 4 \geq 5$ et l'on est dans le cas 2(ii) du lemme avec $k = m - 3i - 4$.

Supposons que l'on soit dans le cas (ii). L'entier $p + 2^{m-3i-2}$ est un carré et $u = \pm\sqrt{p + 2^{m-3i-2}}$. Il résulte de (30) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{i/2+1}\sqrt{p + 2^{m-3i-2}}\, x^2 + 2^i p x.$$

Le changement de variables (31) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 2\sqrt{p + 2^{m-3i-2}}\, X^2 + pX \quad \text{ou} \quad Y^2 = X^3 \pm 4\sqrt{p + 2^{m-3i-2}}\, X^2 + 4pX.$$

On est dans le cas 1(ii) du lemme avec $k = m - 3i - 2$.

3.2.2) Supposons que $m - 3i - 2 = 1$. On a

$$u^2 - p^{n/2} = 2.$$

D'après le lemme 8, $n/2$ est impair et $n/2 \leq 164969$. L'entier $p^{n/2} + 2$ est un carré, on a $u = \pm\sqrt{p^{n/2} + 2}$ et E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{i/2+1}\sqrt{p^{n/2} + 2}\, x^2 + 2^i p^{n/2} x.$$

Le changement de variables (31) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 2\sqrt{p^{n/2} + 2}\, X^2 + p^{n/2} X \quad \text{ou} \quad Y^2 = X^3 \pm 4\sqrt{p^{n/2} + 2}\, X^2 + 4p^{n/2} X.$$

On est donc dans le cas 9 du lemme avec $k = n/2$.

Cela termine la démonstration du lemme.

C) *Cas où b est négatif et p ne divise pas b.* On a le lemme suivant :

LEMME 12. *Supposons $b < 0$ non divisible par p. Alors on est dans l'un des huit cas ci-dessous* :

1. *il existe un entier k vérifiant les inégalités $2 \le k < f(p)$ tel que l'entier $p - 2^k$ soit un carré et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
$$y^2 = x^3 \pm \sqrt{p-2^k}\, x^2 - 2^{k-2}x, \quad y^2 = x^3 \pm 2\sqrt{p-2^k}\, x^2 - 2^k x\,;$$
2. *il existe un entier $k \ge 5$ tel que $p = 2^k + 1$ et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
$$y^2 = x^3 \pm (p-2)x^2 - (p-1)x, \quad y^2 = x^3 \pm 2(p-2)x^2 - 4(p-1)x\,;$$
3. *l'entier $p-2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
$$y^2 = x^3 \pm 2\sqrt{p-2}\, x^2 - 2x, \quad y^2 = x^3 \pm 4\sqrt{p-2}\, x^2 - 8x\,;$$
4. *l'entier $p-1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
$$y^2 = x^3 \pm 2\sqrt{p-1}\, x^2 - x, \quad y^2 = x^3 \pm 4\sqrt{p-1}\, x^2 - 4x\,;$$
5. *l'entier $(p^2-1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
$$y^2 = x^3 \pm 4\sqrt{(p^2-1)/2}\, x^2 - 2x, \quad y^2 = x^3 \pm 8\sqrt{(p^2-1)/2}\, x^2 - 8x\,;$$
6. *l'entier $(p-1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
$$y^2 = x^3 \pm 4\sqrt{(p-1)/2}\, x^2 - 2x, \quad y^2 = x^3 \pm 8\sqrt{(p-1)/2}\, x^2 - 8x\,;$$
7. *l'entier $2p^2-1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
$$y^2 = x^3 \pm 2\sqrt{2p^2-1}\, x^2 - x, \quad y^2 = x^3 \pm 4\sqrt{2p^2-1}\, x^2 - 4x\,;$$
8. *l'entier $2p-1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*
$$y^2 = x^3 \pm 2\sqrt{2p-1}\, x^2 - x, \quad y^2 = x^3 \pm 4\sqrt{2p-1}\, x^2 - 4x.$$

Démonstration. Il résulte de (14) que le seul diviseur premier positif possible de b est 2. Il existe donc un entier i tel que
$$0 \le 2i \le m, \quad b = -2^i.$$
On déduit de (14) que
$$a^2 + 2^{i+2} = 2^{m-2i}p^n. \tag{32}$$
On est donc dans l'un des trois cas 1), 2) et 3) ci-dessous :

1) $i + 2 > m - 2i$. Dans ce cas, $v(a^2) = m - 2i$. On a donc
$$m \equiv 0 \bmod 2.$$
En posant
$$u = \frac{a}{2^{m/2-i}}, \tag{33}$$
on déduit de (32) que
$$u^2 + 2^{3i+2-m} = p^n.$$
D'après le lemme 4, on est dans l'un des cas suivants :

(i) $p = 2^{3i-m} + 1$, $3i - m + 2 \geq 5$, $n = 2$ et $u = \pm(p-2)$;
(ii) $n = 1$ et $3i + 2 - m < \log p / \log 2$.

Supposons que l'on soit dans le cas (i). On déduit de (33) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{m/2-i}(p-2)x^2 - 2^i x.$$

Il existe deux entiers q_1 et r_1 tels que

$$m/2 - i = 2q_1 + r_1 \quad \text{avec } r_1 = 0 \text{ ou } 1.$$

Posons

$$X = \frac{x}{2^{2q_1}}, \quad Y = \frac{y}{2^{3q_1}}. \tag{34}$$

En effectuant ce changement de variables, on obtient comme nouveau modèle de E

$$Y^2 = X^3 \pm (p-2)X^2 - (p-1)X \quad \text{ou} \quad Y^2 = X^3 \pm 2(p-2)X^2 - 4(p-1)X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On est dans le cas 2(i) du lemme avec $k = 3i - m$.

Supposons que l'on soit dans le cas (ii). Alors l'entier $p - 2^{3i+2-m}$ est un carré et $u = \pm\sqrt{p - 2^{3i+2-m}}$. On déduit de (33) que E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{m/2-i}\sqrt{p - 2^{3i+2-m}}\, x^2 - 2^i x.$$

Supposons $3i + 2 - m \geq 2$. Le changement de variables (34) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm \sqrt{p - 2^{3i+2-m}}\, X^2 - 2^{3i-m} X,$$

ou bien

$$Y^2 = X^3 \pm 2\sqrt{p - 2^{3i+2-m}}\, X^2 - 2^{3i+2-m} X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On est dans le cas 1 du lemme avec $k = 3i + 2 - m$.

Supposons $3i + 2 - m = 1$. Il existe deux entiers q_2 et r_2 tels que

$$m/2 - i - 1 = 2q_2 + r_2 \quad \text{avec } r_2 = 0 \text{ ou } 1.$$

Le changement de variables

$$X = \frac{x}{2^{2q_2}}, \quad Y = \frac{y}{2^{3q_2}},$$

conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 2\sqrt{p-2}\, X^2 - 2X \quad \text{ou} \quad Y^2 = X^3 \pm 4\sqrt{p-2}\, X^2 - 8X,$$

selon que $r_2 = 0$ ou $r_2 = 1$. On est dans le cas 3 du lemme.

2) $i + 2 = m - 2i$. D'après (32), on a $v(a^2) \geq i + 2$. On est dans l'un des cas suivants :

2.1) Supposons que l'entier i soit pair. En posant

$$u = \frac{a}{2^{i/2+1}},$$

d'après (32) on obtient

$$u^2 + 1 = p^n.$$

D'après le lemme 3, on a $n = 1$. L'entier $p - 1$ est un carré, $u = \pm\sqrt{p-1}$ et E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{i/2+1}\sqrt{p-1}\, x^2 - 2^i x.$$

Il existe deux entiers q_3 et r_3 tels que

$$i/2 = 2q_3 + r_3 \quad \text{avec } r_3 = 0 \text{ ou } 1.$$

Le changement de variables

$$X = \frac{x}{2^{2q_3}}, \quad Y = \frac{y}{2^{3q_3}},$$

conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 2\sqrt{p-1}\,X^2 - X \quad \text{ou} \quad Y^2 = X^3 \pm 4\sqrt{p-1}\,X^2 - 4X.$$

selon que $r_3 = 0$ ou $r_3 = 1$. On est dans le cas 4 du lemme.

2.2) Supposons que l'entier i soit impair. Dans ce cas on a

$$v(a) \geq (i+1)/2 + 1.$$

En posant

$$u = \frac{a}{2^{(i+1)/2+1}},$$

on déduit de (32) que

$$2u^2 + 1 = p^n.$$

D'après l'alinéa 1 du lemme 7, on est dans l'un des cas suivants :

(i) $n = 2$;
(ii) on a $n = 1$.

Supposons que l'on soit dans le cas (i). Alors l'entier $(p^2-1)/2$ est un carré. On a $u = \pm\sqrt{(p^2-1)/2}$ et E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{(i+1)/2+1}\sqrt{(p^2-1)/2}\,x^2 - 2^i x.$$

Il existe deux entiers q_4 et r_4 tels que

$$(i-1)/2 = 2q_4 + r_4 \quad \text{avec } r_4 = 0 \text{ ou } 1.$$

Le changement de variables

$$X = \frac{x}{2^{2q_4}}, \quad Y = \frac{y}{2^{3q_4}}, \tag{35}$$

conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 4\sqrt{(p^2-1)/2}\,X^2 - 2X \quad \text{ou} \quad Y^2 = X^3 \pm 8\sqrt{(p^2-1)/2}\,X^2 - 8X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 5 du lemme.

Supposons que l'on soit dans le cas (ii). L'entier $(p-1)/2$ est alors un carré. On a $u = \pm\sqrt{(p-1)/2}$ et E a pour modèle de Weierstrass

$$y^2 = x^3 \pm 2^{(i+1)/2+1}\sqrt{(p-1)/2}\,x^2 - 2^i x.$$

Le changement de variables (35) conduit au nouveau modèle de E

$$Y^2 = X^3 \pm 4\sqrt{(p-1)/2}\,X^2 - 2X \quad \text{ou} \quad Y^2 = X^3 \pm 8\sqrt{(p-1)/2}\,X^2 - 8X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 6 du lemme.

3) $i + 2 < m - 2i$. Il résulte de (32) que $v(a^2) = i + 2$, de sorte que i est pair. On a donc $v(a) = i/2 + 1$. Posons

$$u = \frac{a}{2^{i/2+1}}. \tag{36}$$

On déduit alors de (32) que

$$u^2+1=2^{m-3i-2}p^n.$$

Rappelons que n est non nul. D'après le lemme 3, on est dans l'un des cas suivants :

(i) $m-3i-2=1$ et $n=2$;
(ii) $m-3i-2=1$ et $n=1$.

Supposons que l'on soit dans le cas (i). L'entier $2p^2-1$ est alors un carré et $u=\pm\sqrt{2p^2-1}$. Il résulte de (36) que E a pour modèle de Weierstrass

$$Y^2=X^3\pm 2^{i/2+1}\sqrt{2p^2-1}\,X^2-2^iX.$$

Il existe deux entiers q_5 et r_5 tels que

$$i/2=2q_5+r_5 \quad \text{avec } r_5=0 \text{ ou } 1.$$

Le changement de variables

$$X=\frac{x}{2^{2q_5}},\quad Y=\frac{y}{2^{3q_5}}, \tag{37}$$

conduit au nouveau modèle de E

$$Y^2=X^3\pm 2\sqrt{2p^2-1}\,X^2-X \quad \text{ou} \quad Y^2=X^3\pm 4\sqrt{2p^2-1}\,X^2-4X,$$

selon que $r_5=0$ ou $r_5=1$. On est dans le cas 7 du lemme.

Supposons que l'on soit dans le cas (ii). Dans ce cas, l'entier $2p-1$ est un carré et $u=\pm\sqrt{2p-1}$. On déduit de (36) que E a pour modèle de Weierstrass

$$y^2=x^3\pm\ 2^{i/2+1}\sqrt{2p-1}\,x^2-2^ix.$$

Le changement de variables (37) conduit au nouveau modèle de E

$$Y^2=X^3\pm 2\sqrt{2p-1}\,X^2-X \quad \text{ou} \quad Y^2=X^3\pm 4\sqrt{2p-1}\,X^2-4X,$$

selon que $r_5=0$ ou $r_5=1$. On est dans le cas 8 du lemme.

Cela termine la démonstration du lemme.

D) *Cas où b est négatif et p divise b.* On a le lemme ci-dessous :

Lemme 13. *Supposons $b<0$ divisible par p. Alors il existe un entier k vérifiant les inégalités $2\leq k<f(p)$ tel que l'entier 2^k-p soit un carré et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2=x^3\pm 2\sqrt{2^k-p}\,x^2-px,\quad y^2=x^3\pm 4\sqrt{2^k-p}\,x^2-4p.$$

Démonstration. D'après (14), les seuls diviseurs premiers positifs possibles de b sont 2 et p. Puisque a et b n'ont pas de diviseur commun impair, p ne divise pas a et

$$n\equiv 0 \bmod 2.$$

Il existe donc un entier i tel que

$$0\leq 2i\leq m,\quad b=-2^ip^{n/2}.$$

Il résulte alors de (14) que

$$a^2+2^{i+2}p^{n/2}=2^{m-2i}. \tag{38}$$

On est donc dans l'un des trois cas 1), 2) et 3) ci-dessous :

1) $i+2 > m-2i$. Dans ce cas, on a $v(a^2) = m-2i$. On a donc

$$m \equiv 0 \bmod 2.$$

En posant

$$u = \frac{a}{2^{m/2-i}},$$

on déduit de (38) que

$$u^2 + 2^{3i+2-m} p^{n/2} = 1,$$

d'où une contradiction.

2) $i+2 = m-2i$. On a alors, d'après (38), l'inégalité

$$v(a^2) \geq i+2.$$

On est donc dans l'un des cas ci-dessous :

2.1) Supposons que l'entier i soit pair. Posons

$$u = \frac{a}{2^{i/2+1}}.$$

D'après (38), on a

$$u^2 + p^{n/2} = 1,$$

ce qui est impossible.

2.2) Supposons que l'entier i soit impair. On a alors

$$v(a) \geq (i+1)/2 + 1.$$

Posons

$$u = \frac{a}{2^{(i+1)/2+1}}.$$

On déduit de (38) que

$$2u^2 + p^{n/2} = 1.$$

On obtient de nouveau une contradiction.

3) $i+2 < m-2i$. D'après (38), on a $v(a^2) = i+2$, donc i est pair et $v(a) = i/2+1$. Posons

$$u = \frac{a}{2^{i/2+1}}.$$

Il résulte de (38) que

$$u^2 + p^{n/2} = 2^{m-3i-2}.$$

D'après le lemme 6, on a $n/2 = 1$ et $m-3i-2 < f(p)$. On en déduit que l'entier $2^{m-3i-2}-p$ est un carré et que $u = \pm\sqrt{2^{m-3i-2}-p}$. Ainsi E a pour modèle de Weierstrass

$$y^2 = x^2 \pm 2^{i/2+1}\sqrt{2^{m-3i-2}-p}\, x^2 - 2^i p x.$$

Il existe deux entiers q et r tels que

$$i/2 = 2q + r \quad \text{avec } r = 0 \text{ ou } 1.$$

Le changement de variables

$$X = \frac{x}{2^{2q}}, \quad Y = \frac{y}{2^{3q}},$$

conduit au mouveau modèle de E

$$Y^2 = X^3 \pm 2\sqrt{2^{m-3i-2}-p}\, X^2 - pX \quad \text{ou} \quad Y^2 = X^3 \pm 4\sqrt{2^{m-3i-2}-p}\, X^2 - 4pX,$$

selon que $r = 0$ ou $r = 1$. Posons $k = m - 3i - 2$. On a $2 \leq k < f(p)$ et la conclusion du lemme avec l'entier k.

3.4. Fin de la démonstration. Dans ce paragraphe, nous allons démontrer que les courbes elliptiques indiquées dans les énoncés des théorèmes 1 à 8 sont les seules, à $\mathbb{Q}$-isomorphisme près, vérifiant les propriétés annoncées. Il suffit pour cela de démontrer l'assertion ci-dessous :

(∗) *Soit F une courbe elliptique se trouvant dans les énoncés des lemmes* 10, 11, 12 *ou* 13. *Alors, F est de conducteur p ou est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques intervenant dans les énoncés des théorèmes* 1 *à* 8.

En effet, soient N un entier tel que $1 \leq N \leq 8$ et E une courbe elliptique sur $\mathbb{Q}$, de conducteur $2^N p$, ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. D'après l'étude faite au paragraphe précédent, E est $\mathbb{Q}$-isomorphe à une courbe elliptique F se trouvant dans les énoncés des lemmes 10, 11, 12 ou 13. Elle n'est pas de conducteur p. D'après l'assertion (∗), F est donc $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques se trouvant dans les énoncés des théorèmes 1 à 8. Par suite, tel est aussi le cas pour E. Puisque E est de conducteur $2^N p$, il résulte alors du paragraphe 3.2 que E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques indiquées dans les tableaux du théorème portant le numéro N. Cela termine alors la démonstration des théorèmes.

Vérifions que l'assertion (∗) est une conséquence de l'assertion (∗∗) suivante :

(∗∗) *Soit F une courbe elliptique se trouvant dans les énoncés des lemmes* 10, 11, 12 *ou* 13. *Soit F' la tordue quadratique de F par $\sqrt{-1}$. Alors, l'une des courbes F et F' est de conducteur p ou est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques intervenant dans les énoncés des théorèmes* 1 *à* 8.

Considérons en effet une courbe elliptique F se trouvant dans les énoncés des lemmes 10, 11, 12 ou 13. Rappelons qu'étant donné un entier relatif d non nul sans facteurs carrés, la tordue quadratique par $\sqrt{d}$ d'une courbe elliptique de modèle de Weierstrass de la forme

$$y^2 = x^3 + ax^2 + bx,$$

où a et b sont des entiers relatifs, est donnée par l'équation

$$y^2 = x^3 + adx^2 + bd^2x.$$

D'après (∗∗), on peut supposer que F' est de conducteur p ou est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques intervenant dans les théorèmes 1 à 8.

a) Supposons F' de conducteur p. Puisque F a un point d'ordre 2 sur $\mathbb{Q}$, tel est aussi le cas de F'. On en déduit que F' est $\mathbb{Q}$-isomorphe à l'une des deux courbes de Setzer se trouvant dans l'introduction. On constate alors que F est $\mathbb{Q}$-isomorphe à l'une des courbes A1 et A2 du théorème 4 avec $k = 6$. L'assertion (∗) est donc démontrée dans ce cas.

b) Supposons que F' soit $\mathbb{Q}$-isomorphe à l'une des courbes intervenant dans les théorèmes 1 à 8.

b.1) Si F' est isomorphe à l'une des courbes des théorèmes 5 à 8, on vérifie qu'il en est de même de F.

b.2) Si F' est isomorphe à l'une des courbes des théorèmes 2 et 3, alors F est isomorphe à l'une des courbes du théorème 4.

b.3) Si F' est isomorphe à l'une des courbes du théorème 1, alors F est isomorphe à l'une des courbes du théorème 4 ; on le vérifie en effectuant les changements de variables qui se trouvent dans le tableau ci-dessous.

	Changement de variables		Nouveau modèle
A1	$x = \frac{X}{4}$,	$y = \frac{Y-X}{8}$	$Y^2 = X^3 + \sqrt{p-2^k}\,X^2 - 2^{k-2}X$
A2	$x = \frac{X-\sqrt{p-2^k}}{4}$,	$y = \frac{Y-X+\sqrt{p-2^k}}{8}$	$Y^2 = X^3 - 2\sqrt{p-2^k}\,X^2 + pX$
B1	$x = \frac{X}{4}$,	$y = \frac{Y-X}{8}$	$Y^2 = X^3 + \sqrt{p+2^k}\,X^2 + 2^{k-2}X$
B2	$x = \frac{X-\sqrt{p+2^k}}{4}$,	$y = \frac{Y-X+\sqrt{p+2^k}}{8}$	$Y^2 = X^3 - 2\sqrt{p+2^k}\,X^2 + pX$
C1	$x = \frac{X-1}{4}$,	$y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - (p+1)X^2 + pX$
C2	$x = \frac{X-1}{4}$,	$y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - 2(2-p)X^2 + p^2X$
C3	$x = \frac{X}{4}$,	$y = \frac{Y-X}{8}$	$Y^2 = X^3 + \frac{p+1}{2}\,X^2 + \frac{(p-1)^2}{16}\,X$
C4	$x = \frac{X-1}{4}$,	$y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - 2(2p-1)X^2 + X$
D1	$x = \frac{X}{4}$,	$y = \frac{Y-X}{8}$	$Y^2 = X^3 + \sqrt{2^k-p}\,X^2 + 2^{k-2}X$
D2	$x = \frac{X-\sqrt{2^k-p}}{4}$,	$y = \frac{Y-X+\sqrt{2^k-p}}{8}$	$Y^2 = X^3 - 2\sqrt{2^k-p}\,X^2 - pX$
E1	$x = \frac{X-1}{4}$,	$y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - (1-p)X^2 - pX$
E2	$x = \frac{X-1}{4}$,	$y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - 2(p+2)X^2 + p^2X$
E3	$x = \frac{X}{4}$,	$y = \frac{Y-X}{8}$	$Y^2 = X^3 - \frac{p-1}{2}\,X^2 + \frac{(p+1)^2}{16}\,X$
E4	$x = \frac{X-1}{4}$,	$y = \frac{Y-X+1}{8}$	$Y^2 = X^3 + 2(2p+1)X^2 + X$

b.4) Supposons maintenant que F' soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques se trouvant dans l'énoncé du théorème 4.

Si F' est isomorphe à l'une des courbes A1 et A2 : si $k = 4$ ou $k = 5$, la courbe F est isomorphe à la courbe A1 ou A2 du théorème 3 ; si $k = 6$, le conducteur de F est p ; si $k \geq 7$, la courbe F est isomorphe à la courbe A1 ou A2 du théorème 1, comme on le constate à l'aide du tableau ci-dessus.

Si F' est isomorphe à la courbe B1 ou B2 : si $k = 5$, alors F est isomorphe à la courbe B1 ou B2 du théorème 3 ; si $k \geq 7$, F est isomorphe à l'une des courbes B1 et B2 du théorème 1.

Si F' est isomorphe à l'une des courbes intervenant dans les alinéas 3 et 6 du théorème 4, alors F est isomorphe à l'une des courbes Ei et Ci du théorème 1.

Si F' est isomorphe à la courbe D1 ou D2, alors F est isomorphe à la courbe A1 ou A2 du théorème 2.

Si F' est isomorphe à la courbe E1 ou E2 : si $k = 5$, alors F est isomorphe à la courbe D1 ou D2 du théorème 3 ; si $k \geq 7$, alors F est isomorphe à l'une des courbes D1 et D2 du théorème 1.

Cela prouve que l'assertion $(*)$ est de nouveau vérifiée dans ce cas.

Tout revient ainsi à démontrer l'assertion $(**)$ pour chacun des lemmes 10 à 13.

3.4.1. *Le lemme 10*

I) Considérons un entier k vérifiant les inégalités $2 \leq k < f(p)$.

1. Supposons que $p + 2^k$ soit un carré. Rappelons que si k est pair, compte tenu de la remarque 1 et de la condition (2), on a

$$p = 2^{k/2+1} + 1, \qquad \sqrt{p + 2^k} = (p+1)/2, \qquad k \geq 8 \quad (\text{car } p \geq 29).$$

(i) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 = x^3 - \sqrt{p + 2^k}\, x^2 + 2^{k-2} x.$$

Supposons k pair. Le modèle ci-dessus s'écrit

$$y^2 = x^3 - \frac{p+1}{2}\, x^2 + \frac{(p-1)^2}{16}\, x.$$

On obtient dans ce cas la courbe C2 du théorème 4. Supposons k impair. Si $k = 3$, on retrouve la courbe C1$'$ du théorème 5. Si $k \geq 5$, on retrouve la courbe B1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + 2\sqrt{p + 2^k}\, x^2 + 2^k x.$$

Supposons k pair. L'équation ci-dessus s'écrit

$$y^2 = x^3 + (p+1)x^2 + \frac{(p-1)^2}{4}\, x.$$

On obtient alors la courbe D4$'$ du théorème 6. Si k est impair, on retrouve la courbe C1 du théorème 6.

2. Supposons que $2^k - p$ soit un carré. Dans le cas où k est pair, compte tenu de la remarque 1 et de la condition (2), on a

$$p = 2^{k/2+1} - 1, \qquad \sqrt{2^k - p} = (1-p)/2, \qquad k \geq 8 \quad (\text{car } p \geq 29).$$

(i) Considérons la courbe elliptique d'équation

$$y^2 = x^3 - \sqrt{2^k - p}\, x^2 + 2^{k-2} x.$$

Si k pair, le modèle ci-dessus s'écrit

$$y^2 = x^3 + \frac{p-1}{2}\, x^2 + \frac{(p+1)^2}{16}\, x,$$

et l'on obtient la courbe F2 du théorème 4. Pour k impair, on a $k \geq 5$ et l'on obtient la courbe E1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + 2\sqrt{2^k - p}\,x^2 + 2^k x.$$

Si k est pair, l'équation s'écrit

$$y^2 = x^3 + (1-p)x^2 + \frac{(p+1)^2}{4}\,x,$$

et l'on obtient la courbe F4′ du théorème 6. Si k est impair, on retrouve la courbe E1 du théorème 6.

II) Soit k un entier ≥ 5.

1. Supposons que l'on ait $p = 2^k + 1$. En posant $k = t/2 + 1$, on a $t \geq 8$ et t est pair. Il en résulte que :

(i) la courbe elliptique d'équation

$$y^2 = x^3 + 2(2p-1)x^2 + x$$

est la courbe C3 du théorème 4 ;

(ii) la courbe elliptique d'équation

$$y^2 = x^3 + 4(2p-1)x^2 + 4x$$

est la courbe D2 du théorème 6.

2. Supposons que $p = 2^k - 1$. Comme ci-dessus, si $k = t/2+1$, on a $t \geq 8$ et t est pair.

(i) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 = x^3 - (p+2)x^2 + (p+1)x.$$

Le changement de variables $x = X + 1$ et $y = Y$ conduit à la courbe F1 du théorème 4.

(ii) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 = x^3 + 2(p+2)x^2 + 4(p+1)x.$$

Le changement de variables $x = X - 2$ et $y = Y$ conduit à la courbe F1′ du théorème 6.

(iii) La courbe elliptique d'équation

$$y^2 = x^3 - 2(2p+1)x^2 + x$$

est la courbe F4 du théorème 4.

(iv) La courbe elliptique d'équation

$$y^2 = x^3 + 4(2p+1)x^2 + 4x.$$

est la courbe F2′ du théorème 6.

III) On vérifie que les courbes elliptiques intervenant dans l'alinéa 3 du lemme sont les courbes D1, D1′, C2 et C2′ du théorème 7. Celles des alinéas 4 et 5 sont les courbes C1, C1′, D2 et D2′ du théorème 8.

3.4.2. *Le lemme 11*

I) Soit k un entier vérifiant les inégalités $0 \leq k < f(p)$.

1. Supposons que $p - 2^k$ soit un carré.

(i) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 = x^3 + 2\sqrt{p - 2^k}\, x^2 + px.$$

On retrouve les courbes A1 du théorème 6, E1 du théorème 7, D2 du théorème 4, B2′ du théorème 5 et A2 du théorème 4, selon respectivement que $k = 0, 1, 2, 3$ ou $k \geq 4$.

(ii) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 = x^3 + 4\sqrt{p - 2^k}\, x^2 + 4px.$$

On retrouve les courbes A2′ du théorème 5, F2′ du théorème 7, B2′ du théorème 6, selon respectivement que $k = 0, 1$ ou $k \geq 2$.

2. Supposons que $p + 2^k$ soit un carré. Si k est pair, compte tenu de la remarque 1 et de la condition (2), rappelons que l'on a

$$p = 2^{k/2+1} + 1, \qquad \sqrt{p + 2^k} = (p + 1)/2, \qquad k \geq 8 \quad (\text{car } p \geq 29).$$

(i) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + 2\sqrt{p + 2^k}\, x^2 + px.$$

Si k est impair, on retrouve les courbes elliptiques C1 du théorème 7, C2′ du théorème 5 et B2 du théorème 4, selon respectivement que $k = 1$, 3 ou $k \geq 5$. Si k est pair, l'équation ci-dessus s'écrit

$$y^2 = x^3 + (p + 1)x^2 + px,$$

qui est la courbe C1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + 4\sqrt{p + 2^k}\, x^2 + 4px.$$

Si k est impair, on retrouve les courbes D2′ du théorème 7 et C2′ du théorème 6, selon respectivement que $k = 1$ ou $k \geq 3$. Si k est pair, l'équation ci-dessus s'écrit

$$y^2 = x^3 + 2(p + 1)x^2 + 4px,$$

qui est la courbe D1 du théorème 6.

II) Soit k un entier ≥ 5.

1. Supposons que $p = 2^k + 1$. Si $k = t/2 + 1$, on a $t \geq 8$ et t est pair.

(i) Considérons la courbe elliptique d'équation

$$y^2 = x^3 - (2p - 1)x^2 + (p - 1)px.$$

Le changement de variables $x = X + p$ et $y = Y$ conduit à la courbe C1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + 2(2p - 1)x^2 + 4(p - 1)px.$$

Le changement de variables $x = X - 2p$ et $y = Y$ conduit à la courbe D1′ du théorème 6.

(iii) La courbe elliptique d'équation

$$y^2 = x^3 - 2(p - 2)x^2 + p^2x$$

est la courbe C4 du théorème 4.

(iv) La courbe elliptique d'équation

$$y^2 = x^3 + 4(p-2)x^2 + 4p^2x$$

est la courbe D3′ du théorème 6.

2. Supposons que $p = 2^k - 1$. Comme ci-dessus, en posant $k = t/2 + 1$, on a $t \geq 8$ et t est pair.

(i) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + (2p+1)x^2 + (p+1)px.$$

Le changement de variables $x = X - p$ et $Y = y$ conduit à la courbe F1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + 2(2p+1)x^2 + 4(p+1)px.$$

Le changement de variables $x = X - 2p$ et $Y = y$ conduit à la courbe F1 du théorème 6.

(iii) La courbe elliptique d'équation

$$y^2 = x^3 + 2(p+2)x^2 + p^2x$$

est la courbe F3 du théorème 4.

(iv) La courbe elliptique d'équation

$$y^2 = x^3 + 4(p+2)x^2 + 4p^2x$$

est la courbe F3 du théorème 6.

III) On vérifie que les courbes elliptiques intervenant dans les alinéas 3 et 4 du lemme sont les courbes B1, B1′, A2 et A2′ du théorème 7. Les courbes les alinéas 5, 6, 7 et 8 du lemme sont les courbes B1, B1′, A2, A2′, D1, D1′, C2 et C2′ du théorème 8. Celles de l'alinéa 9 du lemme sont les courbes C1, C1′, D2 et D2′ du théorème 7.

3.4.3. *Le lemme 12*

I) Soit k un entier vérifiant les inégalités $2 \leq k < f(p)$ et tel que $p - 2^k$ soit un carré.

(i) Considérons la courbe elliptique d'équation

$$y^2 = x^3 - \sqrt{p-2^k}\,x^2 - 2^{k-2}x.$$

On retrouve les courbes elliptiques D1 du théorème 4, B1′ du théorème 5 et A1 du théorème 4, selon respectivement que $k = 2, 3$ ou $k \geq 4$.

(ii) La courbe elliptique d'équation

$$y^2 = x^3 + 2\sqrt{p-2^k}\,x^2 - 2^kx$$

est la courbe B1 du théorème 6.

II) Soit k un entier ≥ 5 tel que $p = 2^k + 1$. En posant $k = t/2 + 1$, on a $t \geq 8$ et t est pair.

(i) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + (p-2)x^2 - (p-1)x.$$

Le changement de variables $x = X + 1$ et $Y = y$ conduit à la courbe C1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + 2(p-2)x^2 - 4(p-1)x.$$

Le changement de variables $x = X + 2$ et $Y = y$ conduit à la courbe D1 du théorème 6.

III) On vérifie que les courbes elliptiques intervenant dans l'alinéa 3 du lemme sont les courbes F1, F1′, E2 et E2′ du théorème 7. Les courbes de l'alinéa 4 du lemme sont les courbes A1, A1′ du théorème 5 et A2, A2′ du théorème 6. Les courbes des alinéas 5 et 6 sont les courbes A1, A1′, B2 et B2′ du théorème 8. Celles des alinéas 7 et 8 sont les courbes A1, A1′, B2 et B2′ du théorème 7.

3.4.4. *Le lemme 13.* Soit k un entier vérifiant les inégalités $2 \leq k < f(p)$ tel que $2^k - p$ soit un carré. Si k est impair, on a $k \geq 5$. Si k est pair, compte tenu de la remarque 1 et de la condition (2), on a

$$p = 2^{k/2+1} - 1, \qquad \sqrt{2^k - p} = (1-p)/2, \qquad k \geq 8 \quad (\text{car } p \geq 29).$$

(i) Considérons la courbe elliptique d'équation

$$y^2 = x^3 + 2\sqrt{2^k - p}\, x^2 - px.$$

Si k est impair, on retrouve la courbe E2 du théorème 4. Si k est pair, le modèle s'écrit

$$y^2 = x^3 + (1-p)x^2 - px,$$

et l'on obtient la courbe F1 du théorème 4.

(ii) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 = x^3 + 4\sqrt{2^k - p}\, x^2 - 4px.$$

Si k est impair, on retrouve la courbe E2′ du théorème 6. Si k est pair le modèle s'écrit

$$y^2 = x^3 + 2(1-p)x^2 - 4px,$$

qui est la courbe F1 du théorème 6.

Cela termine la démonstration de l'assertion $(**)$ et des théorèmes.

Compte tenu de la remarque 1, les corollaires résultent directement des théorèmes.

Bibliographie

[B-S] M. A. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. 56 (2004), 23–54.

[Be] F. Beukers, *On the generalized Ramanujan–Nagell equation. I*, Acta Arith. 38 (1981), 389–410.

[Bu] Y. Bugeaud, *On the Diophantine equation* $x^2 - 2^m = \pm y^n$, Proc. Amer. Math. Soc. 125 (1997), 3203–3208.

[Cr1] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, 1997.

[Cr2] —, *Elliptic curves data*, http://www.maths.nott.ac.uk/personal/jec/ftp/data/

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

[Iv] W. Ivorra, *Sur les équations* $x^p + 2^\beta y^p = z^2$ *et* $x^p + 2^\beta y^p = 2z^2$, Acta Arith. 108 (2003), 327–338.

[Le] M. Le, *Diophantine equation* $x^2 + 2^m = y^n$, Chinese Sci. Bull. 42 (1997), 1515–1517.

[LRS] P. Lockhart, M. Rosen and J. H. Silverman, *An upper bound for the conductor of an abelian variety*, J. Algebraic Geom. 2 (1993), 569–601.

[M-O] J. F. Mestre et J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math. 400 (1989), 173–184.

[Mi] M. Mignotte, *A corollary to a theorem of Laurent–Mignotte–Nesterenko*, Acta Arith. 86 (1998), 101–111.

[Og1] A. P. Ogg, *Abelian curves of* 2*-power conductor*, Proc. Cambridge Philos. Soc. 62 (1966), 143–148.

[Og2] —, *Abelian curves of small conductor*, J. Reine Angew. Math. 226 (1967), 205–215.

[Pa] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3, J. Number Theory 44 (1993), 119–152.

[Pari] C. Batut, D. Bernardi, K. Belabas, H. Cohen and M. Olivier, *User's guide to PARI-GP* (*version* 2.0.12), Lab A2X, Univ. de Bordeaux I, 1998.

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

[Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[Ta] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in: Modular Functions of One Variable IV, Lecture Notes in Math. 476, Springer, 1975, 33–52.

[Ve1] J. Vélu, *Courbes elliptiques sur* $\mathbb{Q}$ *ayant bonne réduction en dehors de* 11, C. R. Acad. Sci. Paris Sér. A 273 (1971), 73–75.

[Ve2] —, *Isogénies entre courbes elliptiques*, ibid., 238–241.