FINDING SUITABLE CURVES FOR THE ELLIPTIC CURVE METHOD OF FACTORIZATION

A. O. L. Atkin *
F. Morain †‡§

December 16, 1992

Abstract

Using the parametrizations of Kubert, we show how to produce infinite families of elliptic curves which have prescribed nontrivial torsion over $\mathbf{Q}$ and rank at least one. These curves can be used to speed up the ECM factorization algorithm of Lenstra. We also briefly discuss curves with complex multiplication in this context.

1 Introduction

1.1

The ECM method of Lenstra [5] for finding a prime factor p of a number N uses a "random" elliptic curve

$$E : y^2 = f(x) = x^3 + ax + b.$$

If the number k of points on E modulo p is smooth, the method succeeds. Suyama [9] and Montgomery [7] developed infinite classes of curves E for which k has some prescribed small factors; on reasonable probabilistic assumptions (borne out in practice) this should lead to a slight improvement in the method. Specifically, Montgomery and Suyama each force a factor of 12 in k, and Montgomery forces a factor of 16 but only on the assumption that p is congruent to 1 modulo 4.

In this paper, we show how to force a factor of 16 without restriction on p, for an infinite class of curves E. More precisely, we exhibit an infinite family of curves defined over $\mathbf{Q}$, for each of which the group of rational points contains a subgroup isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$, and a computable rational point of infinite order. We also discuss the limited use of curves with complex multiplication in the special contexts of the Cunningham project [2] and primality proving [1].

1.2

In order to construct curves with prescribed factors of k, we can look at curves defined over $\mathbf{Q}$ which have large torsion groups. By a theorem of Mazur [6], we know that the only possible torsion groups over $\mathbf{Q}$ are

$$E_{\mathrm{tor}}(\mathbf{Q}) = \begin{cases} \mathbf{Z}/m\mathbf{Z}; & m = 1, 2, \ldots, 10 \text{ or } 12, \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z}; & m = 1, 2, 3, 4. \end{cases} \qquad (1)$$

*University of Illinois at Chicago, Box 4348, Chicago IL 60680 USA
†Institut National de Recherche en Informatique et en Automatique (INRIA), Domaine de Voluceau, B. P. 105 78153 LE CHESNAY CEDEX (France).
‡On leave from the French Department of Defense, Délégation Générale pour l'Armement.
§*AMS Classification:* 11Y05, 11G20, 14H52.

Kubert [4] gave parametrizations for all these groups. In order to make ECM effective with these curves, we need a further condition beyond Kubert's parametrization, namely that we can exhibit a point on E modulo N. This requires that our parametrization must include a rational point of infinite order on E defined over $\mathbf{Q}$.

We shall use Kubert's curves to exhibit families of elliptic curves of rank at least 1 defined over $\mathbf{Q}$ whose torsion group is among $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/5\mathbf{Z}$, $\mathbf{Z}/7\mathbf{Z}$, $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/10\mathbf{Z}$. The remaining groups in the list (1) can also be exhibited by the methods of our paper, but are not included here since they are already subsumed by the Montgomery-Suyama parametrizations. For completeness, we include a brief description of Kubert's theory and of the classical reduction of quartic curves to cubic curves.

2 Preliminaries

2.1 Kubert's curves

Throughout the paper, we follow Kubert's notation. Let b and c be two rational numbers. Kubert used a special form of elliptic curve for his purpose. A *Kubert curve* is given by

$$\mathcal{E}(b,c) : Y^2 + (1-c)XY - bY = X^3 - bX^2$$

for which $P = (0,0)$ is a point of maximal finite order and the tangent to E at P is the straight line $X = 0$. The discriminant of $\mathcal{E}$ is given by

$$\Delta = \gamma^4 b^3 - 8\gamma^2 b^4 - \gamma^3 b^3 + 36\gamma b^4 + 16b^5 - 27b^4$$

(with $\gamma = 1 - c$) and it will be assumed throughout the paper that $\Delta \neq 0$. Some small powers of P on E are tabulated by Reichert [8]. Among these, we have

$$\begin{aligned}
&2P = (b, bc),\\
&3P = (c, b-c),\\
&4P = (r(r-1), r^2(c-r+1)), \text{ with } r = b/c.
\end{aligned}$$

(Note that the expression for $4P$ has a misprint in Reichert's paper.) For our purpose, it is desirable to have the equation of E in the form $y^2 = f(x)$ and so we put $y = Y + ((1-c)X - b)/2$ and $x = X$ to get

$$E(b,c) : y^2 = x^3 + \frac{((c-1)^2 - 4b)}{4}x^2 + \frac{b(c-1)}{2}x + \frac{b^2}{4}. \tag{2}$$

2.2 From quartics to cubics

We recall some well known facts about quartics (see e.g. [3, Chapter 5]). Let $\mathcal{C}$ be the quartic curve whose equation is

$$y^2 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = f(x)$$

with a rational point (x_0, y_0). Then, with

$$x = x_0 + y_0\left(X - \frac{f'(x_0)}{4y_0}\right)^{-1}$$

$$y = \frac{Y}{y_0}(x - x_0)^2$$

$\mathcal{C}$ is birationally equivalent to

$$\mathcal{C}' : Y^2 = X^4 - 6A_2X^2 + 4A_1X + A_0 = F(X).$$

In turn, this latter curve is birationally equivalent to

$$\mathcal{C}'' : T^2 = S^3 - \frac{3A_2^2 + A_0}{4} S + \frac{A_1^2 - A_2(A_2^2 - A_0)}{4} \tag{3}$$

via the formulas

$$X = \frac{T - A_1/2}{S - A_2}, Y = -X^2 + 2S + A_2.$$

3 The construction of the curves

3.1 The Case $E_{\mathrm{tor}} = \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$

In this case, b and c are found successively from

$$d = 2\alpha(4\alpha + 1)/(8\alpha^2 - 1), c = (2d - 1)(d - 1)/d, b = cd. \tag{4}$$

We will write $E(\alpha)$ for $E(b, c)$. We will prove the following.

Proposition 3.1 *Suppose that (s, t) is a rational point on*

$$\mathcal{C}'' : T^2 = S^3 - 8S - 32.$$

Then with

$$\alpha = \left(\frac{t + 25}{s - 9} + 1\right)^{-1}$$

the curve $E(\alpha)$ has a rational point whose abscissa is $-(2d - 1)/4$.

Proof: Let us first look at the curve as parametrized by d and find the coefficient of y. If we require that $(x_0 = -(2d - 1)/4, y_0)$ is a point on $E(\alpha)$, we get

$$y_0^2 = -\left(\frac{c}{8}\right)^2 (4d^2 - 2d - 1).$$

Rewriting in terms of α, we find that

$$z = -\frac{64\alpha^4 + 96\alpha^3 + 48\alpha^2 + 4\alpha - 1}{(8\alpha^2 - 1)^2} \tag{5}$$

must be a square. Substituting $\alpha = 1/(a + 1)$, this leads to

$$z = \frac{a^4 - 54a^2 - 200a - 211}{(a^2 + 2a - 7)^2}. \tag{6}$$

Next consider the curve

$$\mathcal{C} : Y^2 = X^4 - 54X^2 - 200X - 211.$$

By inspection, we find that $(-5, 8)$ is a point on $\mathcal{C}$ and thus we can apply the results of the preceding section. The curve $\mathcal{C}$ is birationally equivalent to

$$\mathcal{C}'' : T^2 = S^3 - 8S - 32$$

with

$$X = \frac{T + 25}{S - 9}, Y = -X^2 + 2S + 9.$$

This completes the proof of Proposition 3.1.

In order to make Proposition 3.1 effective, we observe that $P = (12, 40)$ is a point of infinite order on $\mathcal{C}''$. Each multiple of P gives a different curve $E(\alpha)$ and it is easy to verify that none of the sixteen points of finite order on $E(\alpha)$ have $x_0 = -(2d - 1)/4$, and thus the rational point on $E(\alpha)$ prescribed by Proposition 3.1 will have infinite order as desired.

We describe the remaining cases more briefly.

3.2 The Case $E_{\text{tor}} = \mathbf{Z}/5\mathbf{Z}$

In this case, one has $b = c$ and the reduced form is

$$E(c, c) : 4y^2 = (c(x + 1))^2 - 2cx(3x + 1) + x^2(4x + 1). \tag{7}$$

Let us decide to cancel the last two terms of (7). This yields

$$c = \frac{x(4x + 1)}{6x + 2}. \tag{8}$$

In that case, the point $(x, x(x + 1)(4x + 1)/(4 + 12x))$ is on $E(c, c)$ and by inspection, it has infinite order, provided that $x \neq 0, -1/2, -1/3, -1/4$.

3.3 The Case $E_{\text{tor}} = \mathbf{Z}/7\mathbf{Z}$

We have $c = d^2 - d$ and $b = cd$. We decide to look for a point with $x = (w - 1)d$ on the curve. We find that

$$w^2 d^4 - 2(3w^2 - 4w + 2)d^3 + (3w^2 - 6w + 4)d^2 + 2(2w^3 - 5w^2 + 5w - 2)d + (w - 1)^2 \tag{9}$$

must be a square. Specializing to $w = -1$, we obtain the quartic

$$Y^2 = X^4 - 18X^3 + 13X^2 - 28X + 4 \tag{10}$$

on which $(-1, 8)$ is a point. The cubic form equivalent to it is

$$T^2 = S^3 + \frac{1295}{48}S - \frac{1079}{864} \tag{11}$$

on which $(2185/12, -2458)$ is a point of infinite order. In this case, we have

$$X = \frac{T + 1}{S - 1/12}, Y = -X^2 + 2S + \frac{1}{12}.$$

3.4 The Case $E_{\text{tor}} = \mathbf{Z}/9\mathbf{Z}$

We have $d = f(f - 1) + 1$, $c = f(d - 1)$ and $b = cd$. We now suppose that $x = (2f - 1)f^2$ is the abscissa of a rational point on E. We find that

$$z = 4f^4 - 24f^3 + 48f^2 - 32f + 9$$

must be a square. We remark that $(2, 3)$ is a rational point on the curve

$$\mathcal{C} : y^2 = 4x^4 - 24x^3 + 48x^2 - 32x + 9$$

and so it is birationally equivalent to

$$\mathcal{C}'' : T^2 = S^3 - 9S + 9$$

with

$$x = 2 + \frac{3}{X}, y = \frac{Y}{3}(x - 2)^2$$

and

$$X = \frac{T - 3}{S}, Y = -X^2 + 2S.$$

We then find that $(1, 1)$ is a point on infinite order on $\mathcal{C}''$.

3.5 The Case $E_{\mathrm{tor}} = \mathbf{Z}/10\mathbf{Z}$

We have $d = f^2/(f-(f-1)^2)$, $c = f(d-1)$ and $b = cd$. We now suppose that $x = -fd$ is the abscissa of a point on $E(b,c)$. The quantity

$$z = 4f^4 - 20f^3 + 20f^2 - 8f + 1$$

must be a square. The quartic

$$\mathcal{C} : y^2 = 4x^4 - 20x^3 + 20x^2 - 8x + 1$$

has the rational point $(0,1)$ and so is birationally equivalent to

$$T^2 = S^3 + \frac{2}{3}S - \frac{53}{108}$$

on which $(2/3, 1/2)$ is a point of infinite order. The transformation formulas are

$$x = \frac{1}{X+2}, y = Yx^2$$

and

$$X = \frac{T+1/2}{S-2/3}, Y = -X^2 + 2S + 2/3.$$

3.6 Summary

For practical application, one may as well use the largest group available, namely the group $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ of §3.1, giving a prescribed factor of 16 in k. It is possible *a priori* that the infinite family we use is too particularly defined to be random, but in practice we have not found this to be so. An unusual feature in one or two instances was that a small factor of N was found during the preparation of the curve E, i.e., by virtue of the smoothness of the number of points on the curve

$$T^2 = S^3 - 8S - 32$$

modulo p.

4 The use of curves with complex multiplication

If E is a curve defined over the field of p elements with complex multiplication by $-D$, then $k = p+1$ for $(-D/p) = -1$, and k is a norm in $\mathbf{Q}(\sqrt{-D})$ when $(-D/p) = +1$. In the latter case k cannot be divisible by any odd power of a prime q for which $(-D/q) = -1$, but there is no restriction for primes r with $(-D/r) = +1$.

Thus in the implementation of ECM one should in the first stage use for the large exponent a product of the form

$$F = \prod_{r^\alpha \leq B} r^\alpha \prod_{q^{2\beta} \leq B} q^{2\beta},$$

and in the second stage only consider single primes r. For a given B, this cuts the time to approximately half as compared with a general elliptic curve. On the other hand, the (unknown) factor p of a given composite N for which we hope to find a smooth k will with probability 1/2 have $(-D/p) = -1$, in which case we are merely repeating the $(P+1)$-factorization method [11]. Presumably that method has already been tried, and even if it has not our product F is quite unsuitable. So on balance it seems that we gain nothing in the general case.

However, there are two cases where it can be guaranteed that *all* the prime factors of our composite N will be norms in some quadratic field $\mathbf{Q}(\sqrt{-D})$. First, in the slightly artificial environment of the Cunningham Project [2], we may have many square roots and discriminants available. For example, if N is the result of removing the algebraic factors from $7^{660}+1$, then all primes p dividing N have $p = 1320n+1$ with $(7/p) = (-1)^n$. Thus we can use $\mathbf{Q}(\sqrt{-D})$ for $D = 3, 4, 8, 11, 15, 20, 24, 40, 88, 120, 132, 660$ and 1320. The reason is that the singular values of the modular invariant j for all these discriminants are expressible in terms of the square roots which we can find modulo N. But $D = 55$, for example, is not usable since it is not idoneal in the sense of Euler [10]; its j-invariant requires a further square root in $\mathbf{Q}(\sqrt{5})$.

We also face a limitation similar to that of the $(P+1)$-method of factorization; if we twist our curve by the character $(./N)$ we shall certainly also twist it modulo p for at least one prime divisor p of N, but this may not be the divisor p for which the twist modulo p has a smooth number of points. Thus for $D > 4$ it is not worth using a twist of a curve that has already been used, rather than a wholly independent curve; the saving of half the time is balanced by the probability $1/2$ that we are merely repeating the curve modulo p. However for $D = 3$ it is worth using up to three curves (from a total of six curves related by twists), and for $D = 4$ up to two curves (from a total of four curves). Thus in the present example we can use three curves for $D = 3$, two for $D = 4$, and one each for the others, giving a total of 16 specially favorable curves.

The other case is in the elliptic curve primality proving method described in the authors' paper [1], which can also be consulted for more theoretical details of the above. There at each stage of the "downrun" one attempts to factorize norms in $\mathbf{Q}(\sqrt{-D})$; however the only square root not available is $\sqrt{-D}$ itself, so that only the nine D of class number one can be used.

5 Conclusion

We have described the construction of families of elliptic curves over $\mathbf{Q}$ which have simultaneously nontrivial torsion and nontrivial rank. These curves are then used to speed up the ECM algorithm. We have also indicated a limited use of elliptic curves with complex multiplication.

Acknowledgment. We wish to thank P. Montgomery for pointing out several misprints in an earlier version of the manuscript.

References

[1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. Research Report 1256, INRIA, Juin 1990. Submitted to *Math. Comp.*

[2] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, 2 ed. No. 22 in Contemporary Mathematics. AMS, 1988.

[3] J. S. Chahal. *Topics in number theory.* Plenum Press, 1988.

[4] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. 3*, 33 (1976), 193–237.

[5] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Math. 126* (1987), 649–673.

[6] B. Mazur. Rational points on modular curves. In *Modular forms of one variable V* (1977), vol. 601 of *Lect. Notes in Math.*, Springer Verlag, pp. 107–148. Proceedings International Conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik, July 2-14, 1976.

[7] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp. 48*, 177 (January 1987), 243–264.

[8] M. A. Reichert. Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields. *Math. Comp. 46*, 174 (April 1986), 637–658.

[9] H. Suyama. Informal preliminary report (8). 25 Oct 1985.

[10] H. Weber. *Lehrbuch der Algebra*, vol. I, II, III. Chelsea Publishing Company, New York, 1902.

[11] H. C. Williams. A $p+1$ method of factoring. *Math. Comp. 39*, 159 (July 1982), 225–234.