Elliptic Curves in Montgomery Form with $B = 1$ and Their Low Order Torsion

Richard Moloney[1], Gary McGuire[2], and Michael Markowitz[3] *

[1] School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4, Ireland
richard.moloney@ucd.ie

[2] School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4, Ireland
gary.mcguire@ucd.ie

[3] Information Security Corp.
1011 Lake St., Suite 425
Oak Park, IL 60301 USA
markowitz@infoseccorp.com

Abstract. This paper proves that the Montgomery form elliptic curves that are cheaply transformable into short Weierstrass form by a simple change of variables $(x, y) \mapsto (x + \alpha, y)$ (instead of a more general affine change of variables) are precisely the curves with $B = 1$. The points of order 2 and 4 on these curves are described, and it is observed that the x-coordinates of these points are consecutive field elements. Finally, it is shown that two elliptic curves specified (in short Weierstrass form) in the SECG standard can be transformed into $B = 1$ Montgomery form, and also into Edwards form.

1 Introduction

It is well-known that every elliptic curve E over a field k of characteristic p, with $p > 3$, can be transformed into *short Weierstrass form*

$$y^2 = x^3 + ax + b \tag{1}$$

by a birational transformation over k. In [6] Montgomery considered elliptic curves that can be written in what has since become known as *Montgomery form*

$$BY^2 = X^3 + AX^2 + X. \tag{2}$$

* The first and second authors were supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006, the Irish Research Council for Science, Engineering and Technology, and are members of UCD CASL.

More recently Bernstein and Lange [3] initiated a study of curves that can be written in *Edwards form* [5]

$$\bar{x}^2 + \bar{y}^2 = 1 + d\bar{x}^2\bar{y}^2. \tag{3}$$

The special forms (2) and (3) are particularly well suited for certain computations and many authors have used them to improve the efficiency of diverse cryptographic applications (see, for example, [1], [2], [4], [7], and references therein). In general, however, a transformation between elliptic curve forms requires passage to a finite extension of k, the cost of which can outweigh any advantages the special forms might otherwise afford. (For example, it is unlikely one would consider applying Montgomery's method [6] to protocols based on NSA Suite B curves.)

Even when transformations between different forms exist over k, their complexity may prove to be prohibitive for use in certain algorithms. Thus it is natural to ask which Montgomery curves (other than $y^2 = x^3 + x$, of course) are transformable *in the simplest possible manner* into short Weierstrass form over k. We consider the *simplest possible manner* to mean a k-translation of the x coordinate, i.e., a map $(x, y) \mapsto (x + c, y)$ where $c \in k$.

In this note, we prove that the Montgomery curves which are mapped to Weierstrass form by a translation of the x-coordinate are precisely those which are of the form

$$Y^2 = X^3 + AX^2 + X,$$

which we call $B = 1$ Montgomery curves. Any Montgomery form (2) where B is a square is of course isomorphic to a $B = 1$ Montgomery curve, so up to k-isomorphism there are only two cases, $B = 1$ and B a non-square in k. If k has characteristic p, and $p \equiv 3 \bmod 4$, then the non-square can be taken to be -1.

We also show that two such curves are specified in the SEC 2 standards [8]. These are the only curves of which the authors are aware to be both specified in a standards document and to be transformable to Edwards form over their field of definition. These curves are already know to be insecure.

We are aware that most, if not all, of our results are already in the literature. The purpose of this note is to make a couple of simple observations, which we believe have not been pointed out before.

2 The Simplest Montgomery Curves

The following is already known, see the remark afterwards. We wish to know which Montgomery form curves can be mapped to short Weierstrass form *by a map of the form* $(x, y) \mapsto (x + c, y)$.

Proposition 1. *An elliptic curve over k in Montgomery form can be mapped into short Weierstrass form by a simple translation $(x, y) = (X+\alpha, Y)$ of the x-coordinate for some $\alpha \in k$ if and only if $B = 1$. If $B = 1$, then the displacement α is a root of the polynomial $f(x) = x^3 + ax + b$.*

Proof. First, suppose that E_M is an elliptic curve in Montgomery form with $B = 1$, *i.e.*, that E is given by an equation of the form $Y^2 = X^3 + AX^2 + X$ for some $A \in k$. If we set $\alpha = A/3 \in k$, then the translation $(X, Y) = (x - \alpha, y)$ clearly transforms E_M into the short Weierstrass form E_W

$$y^2 = x^3 + (1 - 3\alpha^2)x + (2\alpha^3 - \alpha). \tag{4}$$

Conversely, suppose that the Montgomery curve E_M given by (2) is transformed into short Weierstrass form E_W as in (1) by the translation $(x, y) = (X + \alpha, Y)$ for some displacement $\alpha \in k$. Substituting this into (2) yields

$$By^2 = (x - \alpha)^3 + A(x - \alpha)^2 + (x - \alpha)$$

and for this equation to be of the form (1), we must have $B = 1$ and $A = 3\alpha$ (multiply (1) through by B and compare x^3 and x^2 terms).

Now under the translation $(X, Y) = (x - \alpha, y)$, $(0, 0) \in E_M \mapsto (\alpha, 0)$ and for the latter point to be on E_W, we must have $f(\alpha) = 0$.

Remark 1. This proposition may be viewed as a corollary of the proof of the related result [7, Prop.1] which states that the general Montgomery curve (2) is transformable into short Weierstrass form (1) (by an affine transformation) over k if and only if the following two conditions are satisfied:

- $f(x) = x^3 + ax + b$ has at least one root $\alpha \in k$, and for this root

(5)

- $3\alpha^2 + a$ is a quadratic residue in k.

3 The Low Order Torsion of $B = 1$ Montgomery Curves

Recall that a point P on an elliptic curve E is a *torsion point of order n* (possibly defined over the algebraic closure $\bar{k}$) if $nP = 0$ and $n > 0$ is the least such integer with this property. In this section we give explicit formulae for the Weierstrass coordinates of the points of order 2 and 4 on a $B = 1$ Montgomery curve. Our results provide an explanation of the rather surprising configuration of these points on the "random" SECG standard curves presented in the next section.

For the remainder of this section, let E_W be an elliptic curve in Weierstrass form (4) (where $\alpha \in k$) which is k-isomorphic to a $B = 1$ Montgomery curve.

Points of Order 2

The points of order 2 on a curve in Weierstrass coordinates are those points on the curve with $y=0$. Factoring the right hand side of (4) as

$$(x-\alpha)(x^2+\alpha x-2\alpha^2+1), \tag{6}$$

we see that $(\alpha, 0)$ is always a point of order 2 defined over k on E_W.

Considering the other two roots of the cubic (6), we observe that

$$\left(\frac{-\alpha \pm \sqrt{9\alpha^2-4}}{2}, 0\right)$$

are the remaining points of order 2 and they are defined over k only when $9\alpha^2-4$ is a quadratic residue.

Points of Order 4

The x-coordinates of the points of order 4 on E_W are given by the roots of the fourth division polynomial ψ_4 that are not also roots of the second division polynomial ψ_2. On our $B{=}1$ curve given in short Weierstrass form by (4), we have

$$\begin{aligned}\psi_4/2\psi_2(x) = {} & x^6+5(1-3\alpha^2)x^4+20(2\alpha^3-\alpha)x^3-5(9\alpha^4-6\alpha^2+1)x^2 \\ & +4\alpha(6\alpha^4-5\alpha^2+1)x-5\alpha^6+5\alpha^4+\alpha^2-1.\end{aligned}$$

This polynomial factors as

$$(x-\alpha+1)(x-\alpha-1)\left[x^4+2\alpha x^3+6(1-2\alpha^2)x^2-2\alpha(3-7\alpha^2)x+(1-5\alpha^4)\right]$$

showing that $\alpha \pm 1$ are x-coordinates of points of order 4. Substituting $x=\alpha{+}1$ into (4) gives $y^2=3\alpha+2$, so we see that $\left(\alpha{+}1, \pm\sqrt{3\alpha+2}\right)$ are points of order 4 and are defined over k when $3\alpha{+}2$ is a quadratic residue. Similarly, we find that $\left(\alpha{-}1, \pm\sqrt{3\alpha-2}\right)$ are points of order 4 defined over k when $3\alpha{-}2$ is a quadratic residue.

In particular, we have the

Proposition 2. *On a $B{=}1$ Montgomery curve in short Weierstrass form* (4)*, the displacement α is the x-coordinate of a point of order* 2 *defined over k. Furthermore, $\alpha{+}1$, resp. $\alpha{-}1$, is the x-coordinate of a point of order* 4 *that is defined over k when $3\alpha{+}2$, resp. $3\alpha{-}2$, is a quadratic residue.*

4 Montgomery and Edwards Coordinates For Two SECG Curves

In this section we show that the two "verifiably random" curves `secp112r2` and `secp128r2` in the SEC 2 standard [8], which were originally specified there in short Weierstrass form, are in fact Montgomery curves with $B=1$. We also show that these two curves may be transformed into Edwards form (3) by simple linear fractional transformations over their respective ground fields (not a new result) and we give the transformation.

As stated in [3], more than 25% (perhaps 30-40%) of elliptic curves over k in short Weierstrass form are k-isomorphic to a curve in Edwards form. An extension of Edwards form, called twisted Edwards form, covers more curves in Weierstrass form and is known to cover exactly the class of Montgomery curves. See [2] for a discussion of the relations between (twisted) Edwards and Montgomery.

The characteristic primes in the two SECG examples below are 3 mod 4. In this case, $p \equiv 3 \bmod 4$, a Weierstrass curve can be transformed to Montgomery form if and only if the curve has a point of order 4. So it is already known that the curves below can be transformed into Montgomery form, however we are pointing out that the transformation has the simplest possible form, and giving the explicit formulae.

These two curves are already considered to be insecure. Their group orders are 112-bit and 128-bit, which is too small. Also they are not "twist secure.".

secp112r2

(See [8, Section 2.2.2]) This curve, defined over $k = GF((2^{128}-3)/76439)$, is given in short Weierstrass form (1) with

$$a = 1970543761890640310119143205433388,$$
$$b = 1660538572255285715897238774208265.$$

Set $\alpha = 3610075134545239076002374364665933 \in k$.

secp128r2

(See [8, Section 2.3.2]) This curve, defined over $k = GF(2^{128}-2^{97}-1)$, is given in short Weierstrass form (1) with

$$a = 284470887156368047300405921324061011681,$$
$$b = 126188322377389722996253562430093625949.$$

In this case, choose $\alpha = 311198077076599516590082177721943503641 \in k$.

For each of these curves, the translation $(x, y) \mapsto (X + \alpha, Y)$ with the indicated choice of displacement α transforms the given Weierstrass equation into the Montgomery form (2) with $B = 1$ and $A = 3\alpha$. The values $3\alpha - 2$ are quadratic residues in their respective fields, the values $3\alpha + 2$ are not. Taking β to be a square root of $3\alpha - 2$ in the appropriate field, it is easy to check that the transformation

$$(\bar{x}, \bar{y}) = \left(\frac{\beta(x-\alpha)}{y}, \frac{x+1-\alpha}{x-1-\alpha} \right)$$

maps `secp112r2` (resp. `secp128r2`) into Edwards form (3) with $d = (3\alpha+2)/(3\alpha-2)$.

5 Conclusion

We have seen that the two propositions of the present paper apply to the SECG curves `secp112r2` and `secp128r2`. This answers a question raised by the third author who wondered how likely it was that a curve chosen "verifiably at random" would have a fourth division polynomial that vanished on three consecutive field elements. In [8], it was asserted that these curves were chosen "so that scalar multiplication of points on the associated elliptic curve can be accelerated using Montgomery's method [6]". In light of Prop. 1, we somewhat wildly speculate that at least one additional (and unspecified) design criterion was applied in the choice of these curves, namely the condition $B = 1$, in order to minimize the cost of change of coordinate transformations between the Montgomery and Weierstrass forms.

When one intends to use the Montgomery form for computational efficiency, one would like "cheap" change of coordinate transformations between the Montgomery and Weierstrass forms since parameters, keys, signatures, key agreement data, etc. are normally presented or exchanged in Weierstrass coordinates. A similar statement applies to Edwards form, which recent work [1], [3] has shown may be faster than other forms in software and hardware implementations. Also, Edwards form gives better security with respect to side channel analysis.

In any case, the following brief SAGE script should allow the reader to check that $\alpha-1$, α, $\alpha+1$ are indeed roots of ψ_4 for the curve `secp112r2`, as assured by Prop. 2.

```
p = 4451685225093714772084598273548427
k = GF(p)
a = k(1970543761890640310119143205433388)
b = k(1660538572255285715897238774208265)
```

```
s = sqrt((1 - a)/3)
if 2 * s^3 - s == b :
    alpha = s
else:
    alpha = -s
E = EllipticCurve([a, b])
(alpha - 1, 1) in E.division_polynomial(4).roots()
(alpha, 1) in E.division_polynomial(4).roots()
(alpha + 1, 1) in E.division_polynomial(4).roots()
```

With the appropriate inputs p, a and b, the same script verifies the result of Prop. 2 for `secp128r2`.

Acknowledgement. We thank Tanja Lange for helpful comments on an earlier version.

References

1. Brian Baldwin, Richard Moloney, Andrew Byrne, Gary McGuire and William P. Marnane, *A Hardware Analysis of Twisted Edwards Curves for an Elliptic Curve Cryptosystem*, To appear in ARC 2009, available at `http://eprint.iacr.org/2009/001`
2. D. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, *Twisted Edwards Curves*, AFRICACRYPT 2008, Lecture Notes in Computer Science **5023**, Springer-Verlag, New York (2008), 389–405. `http://cr.yp.to/newelliptic/twisted-20080313.pdf`
3. D. Bernstein and T. Lange, *Faster addition and doubling on elliptic curves*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science **4833**, Springer-Verlag, New York (2007), 29–50. `http://cr.yp.to/newelliptic/newelliptic-20070906.pdf`
4. W. Castryck, S. Galbraith, and R. Rezaeian Farashahi, *Efficient arithmetic on elliptic curves using a mixed Edwards-Montgomery representation*, Cryptology ePrint Archive, Report 2008/218 (2008). `http://eprint.iacr.org/2008/218.pdf`
5. H. Edwards, *A normal form for elliptic curves*, Bulletin A.M.S. **44** (2007), 393–422. `http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/S0273-0979-07-01153-6.pdf`
6. P.L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorizations*, Math. Comp. **48** (1987), 243–264. `http://links.jstor.org/sici?sici=0025-5718(198701)48:177<243:STPAEC>2.0.CO;2-3`
7. K. Okeya, H. Kurumatani, K. Sakurai, *Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications*, in: *PKC '00: Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography*, Lecture Notes In Computer Science **1751**, Springer-Verlag, London (2000), 238–257. `http://www.sdl.hitachi.co.jp/crypto/ok-ecdh/PKC2K_ECMF.ps`
8. *SEC 2: Recommended Elliptic Curve Domain Parameters*, Standards for Efficient Cryptography Group (SECG), Sept. 2000. `http://www.secg.org/download/aid-386/sec2_final.pdf`