Starfish on Strike

Daniel J. Bernstein[1], Peter Birkner[2], and Tanja Lange[3]

[1] Department of Mathematics, Statistics, and Computer Science (M/C 249)
University of Illinois at Chicago, Chicago, IL 60607–7045, USA
djb@cr.yp.to
[2] Laboratoire PRiSM, Université de Versailles Saint-Quentin-en-Yvelines, France
pbirkner@fastmail.fm
[3] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands
tanja@hyperelliptic.org

Abstract. This paper improves the price-performance ratio of ECM, the elliptic-curve method of integer factorization. In particular, this paper constructs "$a = -1$" twisted Edwards curves having $\mathbf{Q}$-torsion group $\mathbf{Z}/2 \times \mathbf{Z}/4$, $\mathbf{Z}/8$, or $\mathbf{Z}/6$ and having a known non-torsion point; demonstrates that, compared to the curves used in previous ECM implementations, some of the new curves are more effective at finding small primes despite being faster; and precomputes particularly effective curves for several specific sizes of primes.

Keywords: Factorization, ECM, elliptic-curve method, curve selection, Edwards coordinates, twisted Edwards curves, Suyama curves.

1 Introduction

ECM, Lenstra's elliptic-curve method of integer factorization [11], does not find the secret prime factors of an RSA modulus as quickly as the number-field sieve (NFS) does. However, ECM is an increasingly important tool *inside* NFS as a method of finding many smaller primes.

This paper proposes a new two-part strategy to choose curves in ECM. We have implemented the strategy as a patch to the state-of-the-art "EECM-MPFQ" software, and demonstrated through extensive computer experiments that the new strategy achieves better ECM price-performance ratios than anything in the previous literature.

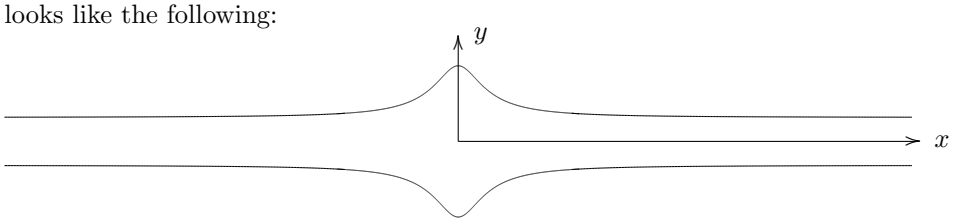
1.1. Background: Edwards curves in ECM. Edwards curves were first described by Edwards in [7]. Bernstein and Lange [5] gave inversion-free formulas for addition and doubling, showing that Edwards curves allow faster scalar multiplication than all other known curve shapes.

Permanent ID of this document: 44c7b02bb6796bb931f85794f77ef1b0. Date of this document: 2010.06.14. This work has been supported in part by the European Commission through the IST Programme under Contract ICT–2007–216676 ECRYPT II, and in part by the National Science Foundation under grant ITR–0716498.

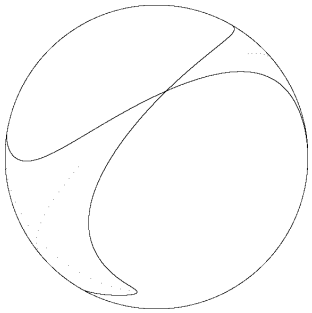
Edwards curves save time in many applications in cryptography and number theory — provided that the underlying curve is allowed to have a point of order 4. This 4-torsion requirement does not sound troublesome for ECM: the conventional wisdom is that torsion points increase the chance of factorization. This conventional wisdom is based on the heuristic that, for a curve having a torsion group of size r, the group order modulo p has the same smoothness probability as an integer divisible by r in the Hasse interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, or equivalently an integer in $[(p+1-2\sqrt{p})/r, (p+1+2\sqrt{p})/r]$, so increasing r increases the smoothness chance. For more details on this heuristic and the extent to which it holds, see [4, Section 9].

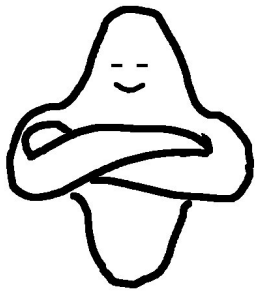
Bernstein, Birkner, Lange, and Peters demonstrated in [4] the speed of Edwards curves inside ECM. The same paper introduced new small-coefficient high-torsion positive-rank Edwards curves and reported measurements of the effectiveness of two representative curves, i.e., the success chance of the curves at finding primes of various sizes. One curve was the smallest-coefficient positive-rank Edwards curve having torsion group isomorphic to $\mathbf{Z}/12$; the other, $\mathbf{Z}/2 \times \mathbf{Z}/8$. Those curves turned out to be simultaneously faster and more effective than the standard ECM choices described in detail in [17], namely Montgomery curves (specifically Suyama curves) for stage 1 and Weierstrass curves for stage 2.

Twisted Edwards curves $ax^2 + y^2 = 1 + dx^2y^2$ were introduced in [3] as a generalization of Edwards curves; they do not necessarily have a point of order 4. For a twisted Edwards curve with $a = -1$ and negative d the affine graph looks like the following:



To visualize the behavior at infinity we map a sphere to $\mathbf{P}^2(\mathbf{R})$, rotate the sphere to an angle that makes the relevant points at infinity visible at the same time as $(0,0)$, and then project the front half of the sphere onto a circle. This first picture shows that there is a single point at infinity and that the curve has two different tangent lines at this point — but only the second picture shows the true nature of things:





Clearly our all-time-favorite starfish has gone on strike! This might explain the results of [4] that curves over $\mathbf{Q}$ with $a = -1$ cannot have 12 or more rational torsion points. Twisted Edwards curves with this parameter choice are refusing to work for ECM!

The interest in curves with $a = -1$ comes from a curve-addition speedup found by Hisil et al. in [9]. The addition formulas in [9] use $9\mathbf{M}$ for $a = 1$ but only $8\mathbf{M}$ for $a = -1$, where $\mathbf{M}$ is the cost of a field multiplication; these formulas hold the speed records for elliptic-curve addition, and one might even speculate that they are optimal. The speed of *doubling* is unaffected by $a = -1$, and scalar multiplication (using standard "window" methods) consists *asymptotically* of 100% doublings and 0% additions; however, additions are a significant fraction of the cost of ECM stage 1, as illustrated by [4, Table 4.1], and are even more important for ECM stage 2.

Unfortunately [4] showed that there are no twisted Edwards curves with $a = -1$ and torsion group isomorphic to $\mathbf{Z}/10$, or to $\mathbf{Z}/12$, or to $\mathbf{Z}/2 \times \mathbf{Z}/8$, or (even for general a) to $\mathbf{Z}/2 \times \mathbf{Z}/6$.

1.2. Contributions of this paper. It is natural to ask whether the speedup in curve additions might be worth a sacrifice in size of the torsion subgroup. To answer this question we first construct twisted Edwards curves with $a = -1$, with positive rank, and with 8 or 6 $\mathbf{Q}$-rational torsion points, and we then carry out extensive computer experiments to analyze the effectiveness of the curves at finding various sizes of primes. The constructions cover three torsion groups, discussed in Sections 3, 4, and 5; for each torsion group we give a fast search method for small-coefficient curves, an explicit infinite family of suitable curves, and the best curves we found. Section 7 compares our curves to previous curves.

We were initially hoping, and were pleased to discover, that the speedup in curve additions *is* worthwhile. Some of our $a = -1$ curves are the new price-performance leaders for ECM: they cost fewer modular multiplications per prime found than the curves used in [12], [13], [17], and [4]. The loss of effectiveness, compared to previous curves with 12 or 16 torsion points, is outweighed by the $a = -1$ gain in speed.

We were surprised to learn that some of our $a = -1$ curves are *more effective* than previous curves with 12 or 16 torsion points. These curves establish new price-performance records for ECM in Montgomery form, even without the Edwards speedups and without the $a = -1$ speedups. In twisted Edwards form, with $a = -1$, these curves require fewer modular multiplications than previous curves *and* find more primes. Evidently the starfish has found a better job working for smaller torsion!

1.3. Sizes of primes used in our paper. We do not claim to be able to *prove* the effectiveness of our curves except through computation. There is a common belief that one can estimate the effectiveness of a curve E by counting the average number of powers of 2 and 3 in $\#E(\mathbf{F}_p)$, as in [13], [17], [2], etc.; but this belief cannot be correct, because it suggests that our curves have, at best, the *same* effectiveness as previous $\mathbf{Z}/12$ curves.

To ensure the comprehensiveness of our computations we try a huge number of curves on *all* b-bit primes, for various values of b. Of course, the cost of this computation increases exponentially with b, and this paper reports results only for $15 \leq b \leq 26$, but these results are enough to demonstrate the impact of the ECM variations considered in this paper.

We do not claim that ECM is useful for $b = 15$; presumably Pollard's rho method is better at that size. We also do not claim that our quantitative improvements are independent of b; it seems obvious that the gains decrease slowly with b. We are continuing our computations and do not anticipate problems pushing the computations past $b = 30$, i.e., solidly into the range where ECM is used in cryptanalysis.

2 Summary of results on points of small order

Let k be a field of characteristic different from 2. A twisted Edwards curve over k has the form $E : ax^2 + y^2 = 1 + dx^2y^2$, for some $a, d \in k \setminus \{0\}$ with $a \neq d$. The Edwards addition law is given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

See [6] for a simple definition of a group law on the completed twisted Edwards curve

$$\overline{\mathrm{E}}_{\mathrm{E},a,d} = \left\{ ((X : Z), (Y : T)) \in \mathbf{P}^1 \times \mathbf{P}^1 : aX^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2 \right\}.$$

We abbreviate $((x_1 : 1), (y_1 : 1))$ as (x_1, y_1).

We describe points of small order in the special case $a = -1$; see [4, Sections 2 and 3] for proofs in the general case. The picture in the previous section shows the case of $a = -1$ and $d < 0$. The three points $(0, -1)$ and $((1 : 0), (1 : \pm\sqrt{-d}))$ have order 2, so $E(\mathbf{Q})$ contains a subgroup isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/2$ if and only if $-d$ is a square. Points of order 4 doubling to $(0, -1)$ are $(\pm\sqrt{-1}, 0)$ (which do not exist over $\mathbf{Q}$) and $((1 : \pm\sqrt{d}), (1 : 0))$ which exist if and only if d is a square. Over $\mathbf{Q}$, the values of d and $-d$ cannot simultaneously be squares, so the only way that $\mathbf{Z}/2 \times \mathbf{Z}/4$ can be achieved is with points of order 4 doubling to $((1 : 0), (1 : \pm\sqrt{-d}))$. These are $(\pm\sqrt[4]{-1/d}, \pm\sqrt[4]{-1/d})$. Order-8 points doubling to $((1 : \pm\sqrt{d}), (1 : 0))$ are of the form $(x_8, \pm 1/(x_8\sqrt{d}))$, where $d = 1/(x_8^4 + 2x_8^2)$.

Note that there is no other way a twisted Edwards curve with $a = -1$ can have torsion group isomorphic to $\mathbf{Z}/8$: There is only one element of order 2 in $\mathbf{Z}/8$, so $-d$ must not be a square. The only points of order 4 are $((1 : \pm\sqrt{d}), (1 : 0))$, so d must be a square and any point of order 8 must double to $((1 : \pm\sqrt{d}), (1 : 0))$.

If $y_3 \in \mathbf{Q} \setminus \{-2, -1/2, 0, 1\}$ and $x_3 \in \mathbf{Q}$ satisfy the equation $x_3^2 = y_3^2 + 2y_3$ then the twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where $d = -(2y_3 + 1)/(x_3^2y_3^2)$, has $(\pm x_3, y_3)$ as points of order 3 and $(\pm x_3, -y_3)$ as points of order 6.

3 Torsion group isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/4$

In this section we present two approaches to finding curves with torsion group isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/4$. In the first we find curves with non-torsion points of small height; in the second we present a family of such curves for which d and the coordinates of a non-torsion point are parameterized in terms of points on a related elliptic curve, the "generating curve". We then study the effectiveness of the curves in finding primes.

3.1. Finding curves with small parameters. To find curves with torsion group isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/4$ and rank at least 1 we need to choose d so that $d = -e^4$ for some $e \in \mathbf{Q}$ and so that there exists a point which has infinite order. All points of finite order are listed in the previous section, so this task amounts to putting $d = -a^4/b^4$ for some positive a, b, and letting the coordinates of the non-torsion point be $x_1 = b/c$ and $y_1 = b/f$ for $c \neq \pm f$ and $c, f \neq 0$. Such points correspond to solutions of $(c^2 + b^2)(f^2 - b^2) = a^4 - b^4$. We iterated over many small pairs (a, b) and tested for each divisor A_1 of $a^4 - b^4$ whether $A_1 - b^2$ and $(a^4 - b^4)/A_1 + b^2$ are squares; after testing fewer than 10^{10} divisors we had found 793 different curves.

3.2. Infinite families. The point $Q = (36, -864/5)$ is a non-torsion point on the curve C in the following theorem. Almost all $(u, v) = [i]Q$ satisfy the hypotheses and generate curves with torsion group $\mathbf{Z}/2 \times \mathbf{Z}/4$ and rank at least 1.

Theorem 3.3. *Let (u, v) with $u \neq -324/25, (25v-1944)/30, -(25v+1944)/270, -5v/24, (-25v+972)/45$ or $(25v-3888)/180$ be a rational point on the elliptic curve $C : V^2 = U^3 - 11664U/25$ over $\mathbf{Q}$. Define $e = (270u+25v+1944)/(30u-25v+1944)$ and $y_1 = (30u-25v+1944)^2/(-625v^2+77760v+1250u^3+24300u^2-3779136)$. Then the twisted Edwards curve $E : -x^2+y^2 = 1-e^4x^2y^2$ has torsion group $\mathbf{Z}/2 \times \mathbf{Z}/4$ and $(1/3, y_1)$ is a non-torsion point on the curve.*

Proof. For $u \neq -324/25, (25v - 1944)/30, -(25v + 1944)/270, -5v/24$ the value e is defined and not equal to $0, \pm 1$. The twisted Edwards curve E has the desired torsion group, because $a = -1$, $d = -e^4$ for some rational e and d is different from 0 and -1.

If we require $d = -e^4$ and that $x = 1/3$ is the x-coordinate of a point on E we obtain $-1/9 + y_1^2 = 1 - (1/9)e^4y_1^2$ which is a quadratic equation in y_1 with the two solutions $y_1 = \pm 10/\sqrt{90 + 10e^4}$. These solutions are rational only if $90 + 10e^4 = r^2$. This defines an elliptic curve which is isomorphic to $C : V^2 = U^3 - 11664U/25$ and every point (u, v) on C gives a solution, namely $e = (270u+25v+1944)/(30u-25v+1944)$ and $y_1 = (30u-25v+1944)^2/(-625v^2 + 77760v + 1250u^3 + 24300u^2 - 3779136)$. This solution has been constructed to have $(1/3, y_1)$ on the curve.

Section 2 lists all torsion points. The point $(1/3, y_1)$ is a non-torsion point, unless $e = \pm 3$, i.e., unless $u = (-25v + 972)/45$ or $(25v - 3888)/180$. □

It is possible to obtain more elliptic families by choosing different values for the x-coordinate of the non-torsion point. Several, but not all, choices lead to parameterizing curves of rank > 0.

bits	#1	#2	#3	#250	#500	#750	#1000	ratio
15	$(\frac{12}{91},\frac{27}{29})$ 1089	$(\frac{23}{14},\frac{49}{578})$ 1060	$(\frac{27}{11},\frac{5}{13})$ 1057	$(\frac{1448}{2151},\frac{1448}{3697})$ 1006	[72] 990	$(\frac{1}{8},\frac{196}{689})$ 978	$(\frac{47}{129},\frac{47}{89})$ 933	1.16720
16	$(\frac{27}{11},\frac{5}{13})$ 1564	$(\frac{12}{343},\frac{1404}{1421})$ 1564	$(\frac{12}{41},\frac{16}{461})$ 1546	$(\frac{57}{176},\frac{703}{1252})$ 1449	$(\frac{178}{729},\frac{445}{477})$ 1428	$(\frac{1122}{949},\frac{187}{2405})$ 1408	$(\frac{21}{38},\frac{7}{34})$ 1345	1.16283
17	$(\frac{12}{343},\frac{1404}{1421})$ 2985	$(\frac{27}{11},\frac{5}{13})$ 2928	$(\frac{12}{91},\frac{27}{29})$ 2895	$(\frac{949}{1122},\frac{73}{1110})$ 2742	[17] 2712	[135] 2686	$(\frac{304}{44187},\frac{76}{85})$ 2593	1.15118
18	$(\frac{27}{11},\frac{5}{13})$ 5575	$(\frac{12}{343},\frac{1404}{1421})$ 5529	$(\frac{13}{16},\frac{64}{233})$ 5433	[18] 5163	$(\frac{888}{539},\frac{111}{401})$ 5117	$(\frac{237}{518},\frac{79}{241})$ 5076	$(\frac{133}{219},\frac{665}{877})$ 4939	1.12877
19	$(\frac{12}{343},\frac{1404}{1421})$ 10200	$(\frac{27}{11},\frac{5}{13})$ 9770	$(\frac{3}{14},\frac{1}{17})$ 9629	$(\frac{1173}{161896},\frac{391}{392})$ 9271	$(\frac{9}{13},\frac{405}{12277})$ 9212	$(\frac{946}{11529},\frac{473}{1017})$ 9160	$(\frac{154}{309},\frac{154}{339})$ 9004	1.13283
20	$(\frac{12}{343},\frac{1404}{1421})$ 15486	$(\frac{27}{11},\frac{5}{13})$ 14845	$(\frac{63}{20},\frac{1}{244})$ 14537	$(\frac{19}{1328},\frac{19}{10064})$ 13785	$(\frac{119}{62},\frac{119}{194})$ 13706	[168] 13634	$(\frac{539}{1278},\frac{539}{1154})$ 13379	1.15749
21	$(\frac{12}{343},\frac{1404}{1421})$ 22681	$(\frac{27}{11},\frac{5}{13})$ 21745	$(\frac{3}{14},\frac{1}{17})$ 21428	[29] 20095	$(\frac{106}{555},\frac{106}{771})$ 19979	$(\frac{28}{101},\frac{1456}{2777})$ 19886	$(\frac{7}{6},\frac{7}{1385})$ 19475	1.16462
22	$(\frac{12}{343},\frac{1404}{1421})$ 46150	$(\frac{27}{11},\frac{5}{13})$ 43916	$(\frac{3}{14},\frac{1}{17})$ 43482	$(\frac{583}{391986},\frac{583}{585})$ 41185	$(\frac{2755}{10816},\frac{551}{676})$ 40993	$(\frac{59}{133},\frac{59}{377})$ 40843	$(\frac{371}{768},\frac{371}{5440})$ 40410	1.14204
23	$(\frac{12}{343},\frac{1404}{1421})$ 82743	$(\frac{27}{11},\frac{5}{13})$ 77161	$(\frac{3}{14},\frac{1}{17})$ 76640	[45] 72681	$(\frac{671}{234},\frac{671}{11169})$ 72475	$(\frac{2}{309},\frac{26}{519})$ 72293	$(\frac{237}{24256},\frac{79}{164})$ 71612	1.15543
24	$(\frac{12}{343},\frac{1404}{1421})$ 187596	$(\frac{27}{11},\frac{5}{13})$ 177237	$(\frac{12}{91},\frac{27}{29})$ 176170	[74] 167895	$(\frac{8}{39},\frac{1352}{1385})$ 167509	$(\frac{96}{41},\frac{864}{1241})$ 167209	$(\frac{68}{609},\frac{17}{105})$ 166251	1.12839
25	$(\frac{12}{343},\frac{1404}{1421})$ 311864	$(\frac{27}{11},\frac{5}{13})$ 293153	$(\frac{12}{91},\frac{27}{29})$ 289748	$(\frac{20}{11},\frac{80}{10909})$ 277183	$(\frac{119}{11649},\frac{119}{339})$ 276546	$(\frac{959}{3655},\frac{959}{3845})$ 276098	$(\frac{231}{5780},\frac{231}{289})$ 274946	1.13427
26	$(\frac{12}{343},\frac{1404}{1421})$ 480006	$(\frac{27}{11},\frac{5}{13})$ 451692	$(\frac{12}{91},\frac{27}{29})$ 446071	$(\frac{133}{2419},\frac{95}{101})$ 424437	$(\frac{1199}{13392},\frac{1199}{1233})$ 423131	$(\frac{322}{251},\frac{161}{353})$ 422585	$(\frac{12}{731},\frac{27}{29})$ 420891	1.14045

Table 3.1. Number of b-bit primes found by various curves having torsion group $\mathbf{Z}/2 \times \mathbf{Z}/4$ and having $a = -1$, using standard EECM parameters. The "bits" column is b. The "#1" column specifies a non-torsion point (x_1, y_1) on the curve that, out of a pool of 1000 curves, was most effective at finding b-bit primes; and the number of b-bit primes found by that curve. The "#2" column provides similar data for the second-best curve out of the same pool. The "#1000" column provides similar data for the worst curve out of the same pool. If $[i]$ appears in place of (x_1, y_1) then it means the curve generated by Theorem 3.3 using $[i](36, -864/5)$. The "ratio" column is the #1 number of primes divided by the #1000 number of primes.

3.4. Effectiveness. We modified the EECM-MPFQ software from [4] to test 1000 curves having torsion group $\mathbf{Z}/2 \times \mathbf{Z}/4$ and having $a = -1$. These 1000 curves include the 793 small-coefficient curves mentioned above, and an additional 207 curves generated modulo n from the infinite family stated in Theorem 3.3.

For each $b \in \{15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$ we tried all 1000 of these curves on all b-bit primes, i.e., all primes between 2^{b-1} and 2^b. To simplify comparisons we used the EECM parameters B_1, d_1 suggested in [4, Table 10.1]: specifically, $(16, 60)$ for $b \in \{15, 16\}$; $(27, 60)$ for $b = 17$; $(27, 90)$ for $b = 18$;

$(37, 90)$ for $b \in \{19, 20, 21\}$; $(47, 120)$ for $b = 22$; $(64, 120)$ for $b = 23$; $(81, 210)$ for $b = 24$; and $(97, 210)$ for $b \in \{25, 26\}$.

Table 3.1 shows that curves with this torsion group vary quite dramatically in effectiveness (number of primes found). The improvement from the worst curve to the best curve fluctuates somewhat with b, hinting at interactions between curve effectiveness and parameter choice, but is typically around 15%; see the "ratio" column in the table. This improvement is not merely a matter of luck: in particular, the interesting curve $-x^2 + y^2 = 1 - (77/36)^4 x^2 y^2$, with torsion group $\mathbf{Z}/2 \times \mathbf{Z}/4$ and non-torsion point $(12/343, 1404/1421)$, easily outperforms the other 999 curves for $b \geq 19$, for example finding 46150 primes for $b = 22$.

For comparison, [4] reported finding 46323 of the 22-bit primes using the curve $x^2 + y^2 = 1 - (24167/25)x^2y^2$ with torsion group $\mathbf{Z}/12$ and non-torsion point $(5/23, -1/7)$. Switching to our curve $-x^2+y^2 = 1-(77/36)^4x^2y^2$ produces only a tiny decrease in effectiveness, 0.4%, while reducing the total ECM stage-1-and-stage-2 cost from $1016\mathbf{M}+276\mathbf{S}$ to $970\mathbf{M}+276\mathbf{S}$, a speedup of nearly 4%. This is only the beginning of the comparison between $a = -1$ and $a = 1$: we have identified better $\mathbf{Z}/12$ curves, and better $\mathbf{Z}/2 \times \mathbf{Z}/8$ curves, but as described in subsequent sections we have also identified better $a = -1$ curves.

4 Torsion group isomorphic to Z/8

We start this section by giving a parameterization of all curves having torsion group isomorphic to $\mathbf{Z}/8$ and then show how to construct these curves and how effective they are.

Theorem 4.1. *If $u \in \mathbf{Q} \setminus \{0\}$ then the twisted Edwards curve $E : -x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where*

$$x_8 = \frac{2u^2 - 1}{2u}, \qquad y_8 = \frac{2u^2 + 1}{2u}, \qquad d = \frac{16u^4}{(4u^4 - 1)^2},$$

has (x_8, y_8) as a point of order 8 and has torsion group isomorphic to $\mathbf{Z}/8$.

Conversely, every twisted Edwards curve over $\mathbf{Q}$ with $a = -1$ and torsion group isomorphic to $\mathbf{Z}/8$ is expressible in this way.

The parameters $u, -u, 1/(2u)$, and $-1/(2u)$ give the same value of d and they are the only values giving this d.

Proof. Note that $d = ((4u^2)/(4u^4 - 1))^2$ is a square, that $1/(x_8^4 + 2x_8^2) = (2u)^4/((2u^2 - 1)^4 + 2(2u^2 - 1)^2(2u)^2) = d$, and that $1/(x_8\sqrt{d}) = (2u(4u^4 - 1))/(4u^2(2u^2 - 1)) = (2u^2 + 1)/(2u) = y_8$. By Section 2, the curve E has (x_8, y_8) as a point of order 8, and has torsion group isomorphic to $\mathbf{Z}/8$.

Conversely, assume that a twisted Edwards curve with $a = -1$ has torsion group isomorphic to $\mathbf{Z}/8$ and has a point of order 8. So the curve can be expressed in this form for some $x_8 \in \mathbf{Q} \setminus \{0\}$ such that $d = 1/(x_8^4 + 2x_8^2)$ is a square in $\mathbf{Q}$. In other words, x_8 is a root of $x_8^4 + 2x_8^2 - 1/d$. Put $x_8^2 = T$, then T is a root of $T^2 + 2T - 1/d$ which means that $(d + 1)/d$ is a square, i.e. that $d + 1$ is also a

square. Thus $1, d$, and $d+1$ form a Pythagorean triple and can be parameterized as $d = (r^2-1)^2/(2r)^2$ and $d+1 = (r^2+1)^2/(2r)^2$ for $r \neq 0$. The solutions for T are then $2/(r^2-1)$ and $-2r^2/(r^2-1)$. Obviously only one of them can be positive for each choice of r, in particular the first one requires $r^2 > 1$ while the second one requires $r^2 < 1$; changing r to $1/r$ changes from one value to the other and if one is a square for r_1 then the other one becomes one for $1/r_1$; d is left invariant by this change.

It is thus sufficient to restrict to one case, so request that $2/(r^2-1)$ is a square in $\mathbf{Q}$, i.e. $r^2 = 2s^2+1$. Define u as the slope of the line between $(1,0)$ and (r,s): i.e., $u = s/(r-1)$. Substitute $s = u(r-1)$ into $r^2 = 2s^2+1$ to obtain $r = (2u^2+1)/(2u^2-1)$. This gives $d = (r^2-1)^2/(2r)^2 = (2u^2-1)^2((2u^2+1)^2-(2u^2-1)^2)^2/(4(2u^2+1)^2(2u^2-1)^4) = 16u^4/(4u^4-1)^2$, $T = 2/(r^2-1) = 2(2u^2-1)^2/((2u^2+1)^2-(2u^2-1)^2) = (2u^2-1)^2/(4u^2)$, i.e. $x_8 = (2u^2-1)/(2u)$, and $y_8 = 2u(4u^4-1)/((2u^2-1)4u^2) = (2u^2+1)/(2u)$.

The numerator of $(d(u)-d(v))$ factors as $(u-v)(u+v)(uv-1/2)(uv+1/2)(u^2+v^2)(u^2v^2+1/4)$ showing that if v is any of the listed values $u, -u, 1/(2u)$, and $-1(2u)$ then $d(v) = d(u)$. Conversely, if v is not one of those values then none of the factors $u-v, u+v, uv-1/2$, and $uv+1/2$ are 0 so $d(v) \neq d(u)$. □

4.2. Finding curves with small parameters. Theorem 4.1 gives a complete parameterization of all twisted Edwards curves with $a = -1$ and torsion subgroup isomorphic to $\mathbf{Z}/8$. To find such curves of rank at least 1, i.e. with some point (x_1, y_1) which is not a point of finite order, write $u = a/b$, $x_1 = (2a^2-b^2)/e$, and $y_1 = (2a^2+b^2)/f$ where a, b, e, f are non-zero integers. Then a, b, e, f satisfy

$$((2a^2-b^2)^2+e^2)((2a^2+b^2)^2-f^2) = (2ab)^4.$$

We searched for solutions by considering a range of positive integers a and integers $1 < b < a\sqrt{2}$; this ensures $u > 1/\sqrt{2}$ which does not lose any generality by Theorem 4.1. For each (a,b) we enumerated all divisors of $(2ab)^4$, subtracted $(2a^2-b^2)^2$ from each divisor, and searched for squares. As one would expect from the degree of the equation, this search was less productive than the search in Section 3: after a comparably fast test of $10^{10.66}$ divisors we had found just 3 curves, such as the curve $-x^2+y^2 = 1+(784/2337)^2x^2y^2$ with non-torsion point $(8/49, 2337/2303)$.

4.3. Infinite families. The following theorem, applied to multiples of the non-torsion point $(4,-16)$ on the specified curve, produces infinitely many curves with positive rank and torsion group isomorphic to $\mathbf{Z}/8$.

Theorem 4.4. *Let (r,s) be a rational point with $r, s \neq 0$ and $s \neq \pm 4r$ on the elliptic curve $S^2 = R^3+48R$ over $\mathbf{Q}$. Let $u = 2r/s$, $v = (2r^3-s^2)/s^2$ and $d = (16u^4)/(4u^4-1)^2$. The twisted Edwards curve $-x^2+y^2 = 1+dx^2y^2$ has torsion subgroup $\mathbf{Z}/8$ and $(x_1,y_1) = (2u^2, (4u^4-1)/v)$ as a non-torsion point.*

Proof. The conditions on r and s ensure that d is defined and $\neq 0, -1$; Theorem 4.1 shows that the torsion group equals $\mathbf{Z}/8$.

bits	#1	#2	#3	#250	#500	#750	#1000	ratio
15	[455] 1113	[763] 1108	[903] 1106	[580] 1059	[773] 1042	[73] 1026	[86] 973	1.14388
16	[899] 1636	[986] 1633	[880] 1626	[641] 1549	[648] 1523	[269] 1500	$(\frac{133}{156}, \frac{697}{528})$ 1397	1.17108
17	[954] 2986	[985] 2970	[314] 2957	[830] 2878	[305] 2847	[641] 2817	[23] 2716	1.09941
18	[583] 5506	[585] 5487	[891] 5468	[722] 5356	[84] 5318	[57] 5281	[483] 5116	1.07623
19	[506] 9859	[825] 9821	[844] 9813	[932] 9652	[233] 9603	[256] 9551	[32] 9349	1.05455
20	$(\frac{27692}{361875}, \frac{362933}{352275})$ 14823	[456] 14696	[765] 14675	[394] 14432	[466] 14370	[565] 14305	[475] 14053	1.05479
21	$(\frac{27692}{361875}, \frac{362933}{352275})$ 21637	[670] 21499	[904] 21467	[128] 21157	[549] 21069	[604] 20983	[69] 20636	1.04851
22	$(\frac{27692}{361875}, \frac{362933}{352275})$ 43760	[903] 43454	[704] 43411	[105] 43018	[690] 42888	[801] 42779	[893] 42331	1.03376
23	$(\frac{27692}{361875}, \frac{362933}{352275})$ 76798	[887] 76675	[668] 76484	[989] 75983	[555] 75809	[87] 75640	[43] 75044	1.02337
24	$(\frac{27692}{361875}, \frac{362933}{352275})$ 176146	[970] 174926	[554] 174911	[15] 174235	[791] 173994	[986] 173767	[47] 172910	1.01871
25	$(\frac{27692}{361875}, \frac{362933}{352275})$ 291211	[655] 289378	[713] 289365	[950] 287993	[176] 287690	[247] 287384	[330] 286355	1.01696
26	$(\frac{27692}{361875}, \frac{362933}{352275})$ 447683	[793] 443619	[457] 443432	[490] 442162	[468] 441787	[585] 441398	[721] 439094	1.01956

Table 4.1. Number of b-bit primes found by various curves having torsion group $\mathbf{Z}/8$ and having $a = -1$, using standard EECM parameters. Columns are defined as in Table 3.1, except that if $[i]$ appears in place of (x_1, y_1) then it means the curve generated by Theorem 4.4 using $[i](4, -16)$.

If we require $d = (16u^4)/(4u^4 - 1)^2$ as in Theorem 4.1 and $x_1 = 2u^2$ then y_1 has to satisfy $y_1^2 = (4u^4-1)^2(1+4u^4)/((4u^4-1)^2-64u^8) = (4u^4-1)^2/(-12u^4+1)$. So $-12u^4 + 1$ must be a rational square. This leads to the elliptic curve $v^2 = -12u^4+1$, which is isomorphic to the Weierstrass curve $C : S^2 = R^3+48R$ via $u = 2R/S$ and $v = (2R^3 - S^2)/S^2$. Any point (r, s) on C gives a point $(x_1, y_1) = (2u^2, (4u^4 - 1)/v)$ on the twisted Edwards curve.

Since $u \neq 0$ also $x_1 \neq 0$ and then $x_8 = x_1$ implies $2u^2 = \pm(2u^2 - 1)/(2u)$ which is excluded by $s \neq \pm 4r$. This means that (x_1, y_1) is different from all torsion points listed in Section 2. □

4.5. Effectiveness. We tried 1000 curves having torsion group $\mathbf{Z}/8$ and having $a = -1$, and measured their effectiveness by the procedures described in Section 3. Table 4.1 reports the results. There is again a clear curve #1 whose performance cannot be explained by random fluctuation. The average effectiveness of $\mathbf{Z}/8$ curves is higher than the average effectiveness of $\mathbf{Z}/2 \times \mathbf{Z}/4$ curves,

but the variation is smaller, and the best $\mathbf{Z}/8$ curve is not as good as the best $\mathbf{Z}/2 \times \mathbf{Z}/4$ curve.

5 Torsion group isomorphic to Z/6

The structure of this section follows closely that of the previous one.

Theorem 5.1. *If $u \in \mathbf{Q} \setminus \{0, \pm 1\}$ then the twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where*

$$x_3 = \frac{u^2-1}{2u}, \quad y_3 = \frac{(u-1)^2}{2u}, \quad d = -16\frac{u^3(u^2-u+1)}{(u-1)^6(u+1)^2},$$

has (x_3, y_3) as a point of order 3 and has torsion group isomorphic to $\mathbf{Z}/6$. Conversely, every twisted Edwards curve over $\mathbf{Q}$ with $a = -1$ and a point of order 3 arises in this way.

The parameters u and $1/u$ give the same value of d.

Proof. For $u \in \mathbf{Q} \setminus \{0, \pm 1\}$ the value d is defined and not equal to 0 or -1. Use $-x_3^2 + y_3^2 = -\frac{(u^2-1)^2}{(2u)^2} + \frac{(u-1)^4}{(2u)^2} = \frac{-4u^3+8u^2-4u}{(2u)^2} = -\frac{2(u-1)^2}{2u} = -2y_3$ to see that (x_3, y_3) is a point of order 3. Further observe that

$$-\frac{2y_3+1}{x_3^2y_3^2} = -\frac{(2(u-1)^2+2u)(2u)^4}{2u(u^2-1)^2(u-1)^4} = \frac{16u^3(u^2-u+1)}{(u+1)^2(u-1)^6} = d.$$

Furthermore $y_3 \notin \{-2, -1/2, 0, 1\}$ since $u \in \mathbf{Q} \setminus \{0, \pm 1\}$. By Section 2, the twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$ has (x_3, y_3) as a point of order 3 and has torsion group isomorphic to $\mathbf{Z}/6$.

Conversely, let $x_3^2 = y_3^2 + 2y_3$, then $1 = (y_3+1)^2 - x_3^2 = (y_3+1-x_3)(y_3+1+x_3)$. Splitting 1 as $u \cdot 1/u$ gives $(y_3 + 1 + x_3) = u$ and $(y_3 + 1 - x_3) = 1/u$ and thus $2(y_3 + 1) = u + 1/u$ and $2x_3 = u - 1/u$. The value for d follows from $d = -(2y_3 + 1)/(x_3^2y_3^2)$.

The numerator of $(d(u) - d(v))$ factors as $(u - v)(uv - 1)$ times a polynomial of degree 6 in u and v which does not factor over $\mathbf{Q}$, showing there are no other rational transformations leaving d invariant that work independently of u. □

5.2. Finding curves with small parameters. Theorem 5.1 gives a complete parameterization of all Edwards curves with torsion group isomorphic to $\mathbf{Z}/6$.

Write $u = a/b$ for integers a, b satisfying $0 < |b| < a$, so $|u| > 1$ ensuring that d is defined and avoiding repetitions of d by Theorem 5.1. Define $e = (a^2-b^2)/x_1$ and $f = -(a-b)^2/y_1$, with integers $e \neq f$. Any solution to $-x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ corresponds to a point (a, b, e, f) on

$$((a^2 - b^2)^2 + e^2)((a - b)^4 - f^2) = (a^2 + b^2)^3(b^2 - 4ab + a^2).$$

We searched for solutions following the same strategy as in the previous sections and within $10^{10.7}$ divisors had found 12 curves.

5.3. Infinite families. Suyama [15] presented a rational family of Montgomery curves with torsion containing $\mathbf{Z}/6$. All Suyama curves can be translated to twisted Edwards curves as shown in [4] but here we additionally require $a = -1$. We now present an elliptic family that is a subfamily of Suyama's construction and satisfies $a = -1$.

Theorem 5.4. *Let (u, v) be a rational point with $u, v \neq 0$ and $u \neq 1/96$, $1/192$, $-1/384$, $1/576$ on the curve $C : V^2 = U^3 - U^2/2304 - 5U/221184 + 1/28311552$. Define $\sigma = (1-96u)/(96u)$ and $r = v/u^2$. Define $\alpha = \sigma^2 - 5$ and $\beta = 4\sigma$. Define $d = (\beta+\alpha)^3(\beta-3\alpha)/(r(\beta-\alpha))^2$. Then the twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ has torsion group isomorphic to $\mathbf{Z}/6$ and a non-torsion point (x_1, y_1) with $x_1 = 2r\sigma/((\sigma-1)(\sigma+5)(\sigma^2+5))$ and $y_1 = (\alpha^3 - \beta^3)/(\alpha^3 + \beta^3)$. A point of order 3 is given by $(x_3, y_3) = (-r/((\sigma-1)(\sigma+5)), (\alpha-\beta)/(\alpha+\beta))$.*

Proof. The twisted Edwards curves $-c^2x^2 + y^2 = 1 + dx^2y^2$ and $-\bar{x}^2 + \bar{y}^2 = 1 + (d/c^2)\bar{x}^2\bar{y}^2$ are isomorphic with $\bar{x} = cx$. By Theorem 7.6 of [4] the Edwards curves corresponding to Suyama curves have $a = (\beta-\alpha)^3(3\alpha+\beta)$ and $d = (\beta+\alpha)^3(\beta-3\alpha)$. To get an isomorphic curve with $a = -1$ we thus need that $(\beta-\alpha)(3\alpha+\beta)$ is the negative of a rational square. Expanding gives $3\sigma^4 - 8\sigma^3 - 46\sigma^2 + 40\sigma + 75 = r^2$. This defines an elliptic curve isomorphic to $C : V^2 = U^3 - U^2/2304 - 5U/221184 + 1/28311552$, with $\sigma = -(U - 1/96)/U$ and $r = V/U^2$. The values for x_1, y_1, and d in terms of s and t follow from $c = r(\beta-\alpha)$ and the expressions in [4].

By the conditions on u, v all expressions are defined and $d \neq 0, -1$; furthermore (x_1, y_1) does not match any of the points of finite order. To verify the statements on (x_3, y_3) observe that $-x_3^2 + y_3^2 = 1 + dx_3^2y_3^2$ and that $-x_3^2 + y_3^2 = -2y_3$, showing that the point is on the curve and has order 3. □

The elliptic curve C from the proof has rank 1 and torsion subgroup isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/2$. A non-torsion point is given by $Q = (1/192, 1/4608)$, so (u, v) can be chosen as a multiple $[i]Q$ of Q with $i > 1$. One can also add points of order 2 to these multiples; in particular, $(1/1152, 7/55296)$ is $-Q$ plus a point of order 2, and generates $\sigma = 11$, a Suyama case that has already drawn attention for being more effective than typical Suyama curves, as discussed in [2].

5.5. Effectiveness. We tried 1000 curves having torsion group $\mathbf{Z}/6$ and having $a = -1$, and measured their effectiveness as in Sections 3 and 4. Table 5.1 shows that these curves are extremely effective, even better than the $\mathbf{Z}/12$ curve measured in [4]. See Sections 6 and 7 for further discussion.

6 Effectiveness for Z/12 and Z/2 × Z/8

This paper proposes that the ECM curves used to find b-bit primes should be selected by precomputing the most effective curves. Of course, this proposal is not limited to the fast $a = -1$ curves analyzed in this paper; one can instead precompute, e.g., the most effective $\mathbf{Z}/2 \times \mathbf{Z}/8$ curve.

bits	#1	#2	#3	#250	#500	#750	#1000	ratio
15	[58] 1175	[348] 1173	[853] 1172	[850] 1128	[799] 1116	[74] 1104	$(\frac{176}{321}, \frac{2}{123})$ 1051	1.11798
16	[519] 1779	[532] 1772	[711] 1751	[170] 1695	[38] 1677	[460] 1656	$(\frac{864}{403}, \frac{343}{143})$ 1546	1.15071
17	[745] 3355	[868] 3343	[971] 3341	[539] 3253	[425] 3226	[166] 3202	$(\frac{176}{321}, \frac{2}{123})$ 3010	1.11462
18	[424] 6223	[310] 6209	[18] 6209	[379] 6104	[634] 6067	[463] 6034	$(\frac{147}{1696}, \frac{14336}{10229})$ 5729	1.08623
19	[615] 10809	$(\frac{825}{2752}, \frac{1521}{1504})$ 10802	[96] 10771	[175] 10640	[375] 10593	[497] 10538	$(\frac{864}{403}, \frac{343}{143})$ 10301	1.04932
20	[932] 16328	[94] 16289	[785] 16287	[334] 16106	[107] 16037	[466] 15969	$(\frac{176}{321}, \frac{2}{123})$ 15399	1.06033
21	$(\frac{825}{2752}, \frac{1521}{1504})$ 24160	[982] 24119	[265] 24113	[194] 23821	[669] 23735	[869] 23654	$(\frac{749}{3420}, \frac{17199}{122324})$ 22790	1.06011
22	$(\frac{336}{527}, \frac{80}{67})$ 48424	$(\frac{825}{2752}, \frac{1521}{1504})$ 48378	[306] 48357	[565] 47982	[960] 47867	[474] 47749	$(\frac{147}{1696}, \frac{14336}{10229})$ 45828	1.05665
23	$(\frac{336}{527}, \frac{80}{67})$ 83943	[604] 83417	[879] 83360	[861] 82907	[658] 82755	[3] 82593	$(\frac{864}{403}, \frac{343}{143})$ 81114	1.03488
24	$(\frac{825}{2752}, \frac{1521}{1504})$ 193069	[119] 192831	[90] 192667	[618] 191776	[728] 191526	[513] 191288	$(\frac{147}{1696}, \frac{14336}{10229})$ 188198	1.02588
25	$(\frac{825}{2752}, \frac{1521}{1504})$ 318865	[290] 318680	[149] 318605	[453] 317555	[708] 317228	[217] 316924	$(\frac{176}{321}, \frac{2}{123})$ 311394	1.02399
26	$(\frac{825}{2752}, \frac{1521}{1504})$ 493470	$(\frac{336}{527}, \frac{80}{67})$ 493015	[337] 492320	[303] 490886	[198] 490477	[577] 490104	$(\frac{176}{321}, \frac{2}{123})$ 480263	1.02750

Table 5.1. Number of b-bit primes found by various curves having torsion group $\mathbf{Z}/6$ and having $a = -1$, using standard EECM parameters. Columns are defined as in Table 3.1, except that if $[i]$ appears in place of (x_1, y_1) then it means the curve generated by Theorem 5.4 from $[i](1/192, 1/4608)$.

We carried out computations for 1000 curves having $\mathbf{Z}/2 \times \mathbf{Z}/8$ torsion with $a = 1$, and 1000 curves having $\mathbf{Z}/12$ torsion with $a = 1$. For $\mathbf{Z}/2 \times \mathbf{Z}/8$ we used 975 curves from the (rank-1 elliptic) Atkin–Morain family [1], translated to Edwards form in [4, Theorem 7.3], and 25 small-coefficient curves from [4, Section 8]. For $\mathbf{Z}/12$ we used 922 curves from a (rank-1 elliptic) family introduced by Montgomery in [12], translated analogously to Edwards form, and 78 small-coefficient curves from [4, Section 8].

The results appear in Tables 6.1 and 6.2. It is clear from the tables that $\mathbf{Z}/12$ $a = 1$ is very close in effectiveness to $\mathbf{Z}/6$ $a = -1$, while $\mathbf{Z}/2 \times \mathbf{Z}/8$ $a = 1$ is noticeably worse: for example, the median $\mathbf{Z}/2 \times \mathbf{Z}/8$ curve finds 46501 22-bit primes, the median $\mathbf{Z}/12$ curve finds 47521 22-bit primes, and the median $\mathbf{Z}/6$ curve finds 47687 22-bit primes.

Recall that the small-coefficient $\mathbf{Z}/12$ curve measured in [4] finds only 46323 22-bit primes. The $\mathbf{Z}/12$ median reported here is dominated by the infinite family

bits	#1	#2	#3	#250	#500	#750	#1000	ratio
15	[792] 1165	[921] 1164	[389] 1163	[364] 1112	[647] 1096	[608] 1082	$(\frac{29573281}{31533721}, \frac{29573281}{79031041})$ 1014	1.14892
16	[642] 1726	[915] 1723	[855] 1716	[537] 1653	[532] 1634	[467] 1612	$(\frac{305}{851}, \frac{305}{319})$ 1506	1.14608
17	[920] 3176	[931] 3163	[908] 3161	[694] 3045	[929] 3016	[103] 2988	$(\frac{89623}{51987}, \frac{33019}{31961})$ 2838	1.11910
18	[758] 5804	[22] 5781	[906] 5779	[868] 5665	[297] 5630	[392] 5588	$(\frac{4913}{377}, \frac{51}{19})$ 5298	1.09551
19	[955] 10644	[370] 10635	[871] 10625	[564] 10439	[700] 10384	[747] 10333	[2] 10046	1.05953
20	[942] 15980	[350] 15893	[707] 15870	[654] 15668	[426] 15607	[596] 15538	$(\frac{1025}{1032}, \frac{41}{265})$ 15096	1.05856
21	[943] 23369	[316] 23354	[369] 23347	[43] 23081	[764] 22998	[443] 22903	$(\frac{1009}{15801}, \frac{41369}{41441})$ 22070	1.05886
22	[846] 46990	[724] 46977	[869] 46964	[743] 46620	[430] 46501	[46] 46377	$(\frac{86866}{18259}, \frac{8481}{4001})$ 45299	1.03733
23	[972] 83712	[590] 83706	[261] 83691	[483] 83181	[367] 83005	[919] 82828	$(\frac{18096}{9793}, \frac{62959}{30191})$ 81505	1.02708
24	[95] 189700	[485] 189678	[950] 189660	[637] 188973	[239] 188724	[116] 188502	$(\frac{29573281}{31533721}, \frac{29573281}{79031041})$ 185854	1.02069
25	[657] 313857	[723] 313718	[667] 313600	[938] 312577	[629] 312253	[328] 311942	$(\frac{7825}{12866}, \frac{22223}{27025})$ 308060	1.01882
26	[594] 483474	[269] 483440	[638] 483431	[801] 482285	[887] 481868	[631] 481471	$(\frac{28577}{34343}, \frac{527}{943})$ 474443	1.01903

Table 6.1. Number of b-bit primes found by various curves having torsion group $\mathbf{Z}/2 \times \mathbf{Z}/8$ and having $a = 1$, using standard EECM parameters. Columns are defined as in Table 3.1.

of $\mathbf{Z}/12$ curves, and it turns out that the average curves in that family are more effective than most of the small-coefficient $\mathbf{Z}/12$ curves. A similar effect occurs for $\mathbf{Z}/2 \times \mathbf{Z}/8$. Countering this effect is a speedup mentioned in [4]: additions of small-coefficient base points are much faster than additions of general points. In this paper we ignore this speedup and count multiplications by small coefficients as if they were as expensive as full multiplications.

7 Comparison

Among all of the 5000 curves measured here, the overall winner in effectiveness for 22-bit primes is the curve $-x^2 + y^2 = 1 - (6517/196608)x^2y^2$, with torsion group $\mathbf{Z}/6$ and non-torsion point $(336/527, 80/67)$. The runner-up for 22-bit primes is the curve $-x^2 + y^2 = 1 - (13312/18225)x^2y^2$, with torsion group $\mathbf{Z}/6$ and non-torsion point $(825/2752, 1521/1504)$. Compared to the $\mathbf{Z}/12$ curve measured in [4], both of these curves find 4% more primes and gain a further 4%

bits	#1	#2	#3	#250	#500	#750	#1000	ratio
15	[636] 1208	[872] 1206	[840] 1206	[516] 1158	[539] 1141	[218] 1120	$(\frac{1159}{191}, \frac{3971}{33239})$ 1039	1.16266
16	[903] 1829	[884] 1808	[662] 1807	[385] 1721	[684] 1690	[170] 1656	$(\frac{514917}{463733}, \frac{507}{277})$ 1509	1.21206
17	[780] 3394	[893] 3371	[850] 3360	[686] 3264	[172] 3229	[15] 3193	$(\frac{424}{18299}, \frac{316}{34075})$ 3011	1.12720
18	[878] 6261	[671] 6218	[666] 6215	[678] 6076	[99] 6032	[82] 5986	$(\frac{2511}{4931}, \frac{549}{3301})$ 5684	1.10151
19	[799] 10882	[918] 10846	[696] 10846	[203] 10643	[539] 10582	[253] 10525	$(\frac{2223}{1165}, \frac{3887}{4055})$ 10181	1.06885
20	[918] 16276	[811] 16275	[719] 16273	[536] 16052	[165] 15977	[441] 15890	$(\frac{1817}{4267}, \frac{2401}{10081})$ 15313	1.06289
21	[772] 23991	[663] 23970	$(\frac{285}{293}, \frac{153}{569})$ 23965	[386] 23687	[449] 23590	[737] 23476	$(\frac{15375}{31217}, \frac{149609}{124766})$ 22714	1.05622
22	[861] 48076	[400] 48028	[648] 48020	[923] 47651	[421] 47521	[11] 47367	$(\frac{4272}{3007397}, \frac{80}{323})$ 45987	1.04543
23	$(\frac{1856}{1735}, \frac{396}{445})$ 83563	[662] 83242	[888] 83196	[799] 82643	[858] 82439	[695] 82260	$(\frac{217}{2687}, \frac{8649}{8599})$ 80858	1.03345
24	$(\frac{285}{293}, \frac{153}{569})$ 192256	[705] 191836	[673] 191693	[275] 190997	[161] 190725	[907] 190459	$(\frac{31293}{105533}, \frac{160003}{307178})$ 187647	1.02456
25	$(\frac{285}{293}, \frac{153}{569})$ 317527	[556] 317372	[575] 317368	[371] 316185	[463] 315835	[457] 315485	$(\frac{192061}{196355}, \frac{2775125}{13288277})$ 310830	1.02155
26	$(\frac{285}{293}, \frac{153}{569})$ 491042	$(\frac{1856}{1735}, \frac{396}{445})$ 490405	[85] 489815	[865] 488399	[695] 487954	[278] 487484	$(\frac{2349}{199}, \frac{11907}{21733})$ 480509	1.02192

Table 6.2. Number of b-bit primes found by various curves having torsion group $\mathbf{Z}/12$ and having $a = 1$, using standard EECM parameters. Columns are defined as in Table 3.1.

from the $a = -1$ speedup, for an overall improvement of 8% in price-performance ratio. Our best $\mathbf{Z}/12$ curves close only about half of the gap.

It is easy to point to algebraic reasons for the effectiveness of $\mathbf{Z}/6$ $a = -1$ curves. Like all Suyama curves these curves have order divisible by 12 modulo any prime. For primes $p \in 1 + 4\mathbf{Z}$ more is true, thanks to $a = -1$: the point $(\sqrt{-1}, 0)$ is defined over $\mathbf{F}_p$ and has order 4; if d is a square then there are extra points of order 2 and 4; and if d is a 4th power then there is full 4-torsion. These reasons suggest that the $\mathbf{Z}/6$ curves with $a = -1$ are more effective than most Suyama curves, and *as effective* as $\mathbf{Z}/12$ curves, but do not explain why the curves are *more effective* than $\mathbf{Z}/12$ curves.

Figure 7.1 plots the price-performance ratio of all 5000 curves for $b = 15$: the number of multiplications per prime found (but counting all multiplications in stage 1 and stage 2 even for primes that actually skip stage 2), as in [4]. Figures 7.2, 7.3, and 7.4 plot data for $b \in \{15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$. These plots are directly comparable to the "ratio" column in [4, Table 10.1],

reporting (e.g.) 1519.3 multiplications for $b = 18$ and 3914.1 multiplications for $b = 22$. The "bumps" on the sides of several graphs are not random: they illustrate the family effects mentioned above.

7.1. Further computations. We plan to extend our precomputations to other choices of EECM-MPFQ parameters (B_1, d_1), to larger values of b, and to a larger pool of curves for each b. We expect that our continuing computations will gradually identify better and better curves for each b, mostly by luck for smaller values of b but also by locating special curves such as $-x^2 + y^2 = 1 - (13312/18225)x^2y^2$. Rather than constantly updating this paper we will maintain a web page showing the best results. Some of the other $\mathbf{Z}/2 \times \mathbf{Z}/8$ families listed in [13] have rank 1; our guess is that none of the families will be competitive with $\mathbf{Z}/6$ but we plan to check this through computation.

Note that each of the curves we consider can be efficiently computed modulo any desired n. The expense of this computation is at most the cost of a small number of additions (modulo n) on a parameterizing elliptic curve. This cost is noticeable only for very small b; it decreases rapidly as b increases.

ECM is normally applied as part of a series of computations: typically $p-1$, then $p+1$, then one ECM curve, then another ECM curve, etc. We plan to compute the best ECM curve for primes not found by the $p-1$ method, the best ECM curve for primes not found by the first curve, etc. Note that there are some known correlations between ECM curves; for example, $\mathbf{Z}/12$ prefers to find primes in $1 + 3\mathbf{Z}$, while $\mathbf{Z}/2 \times \mathbf{Z}/8$ prefers to find primes in $2 + 3\mathbf{Z}$. Our greedy approach might not be optimal but we expect it to produce noticeably better ECM sequences than choosing curves independently.

References

[1] A. O. L. Atkin, François Morain, *Finding suitable curves for the elliptic curve method of factorization*, Mathematics of Computation **60** (1993), 399–405. ISSN 0025–5718. MR 93k:11115. URL: http://www.lix.polytechnique.fr/~morain/Articles/articles.english.html. Citations in this document: §6.

[2] Răzvan Bărbulescu, *Familles de courbes adaptées à la factorisation des entiers* (2009). URL: http://hal.inria.fr/inria-00419218/PDF/Familles_version2.pdf. Citations in this document: §1.3, §5.3.

[3] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters, *Twisted Edwards curves*, in Africacrypt 2008 [16] (2008), 389–405. URL: http://eprint.iacr.org/2008/013. Citations in this document: §1.1.

[4] Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters, *ECM using Edwards curves (24 Jan 2010 version)* (2010). URL: http://eprint.iacr.org/2008/016. Citations in this document: §1.1, §1.1, §1.1, §1.1, §1.1, §1.2, §2, §3.4, §3.4, §3.4, §5.3, §5.3, §5.3, §5.5, §6, §6, §6, §6, §6, §7, §7, §7.

[5] Daniel J. Bernstein, Tanja Lange, *Faster addition and doubling on elliptic curves*, in Asiacrypt 2007 [10] (2007), 29–50. URL: http://cr.yp.to/papers.html#newelliptic. Citations in this document: §1.1.

[6] Daniel J. Bernstein, Tanja Lange, *A complete set of addition laws for incomplete Edwards curves* (2009). URL: http://eprint.iacr.org/2009/580. Citations in this document: §2.

[7] Harold M. Edwards, *A normal form for elliptic curves*, Bulletin of the American Mathematical Society **44** (2007), 393–422. URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html. Citations in this document: §1.1.

[8] Florian Hess, Sebastian Pauli, Michael E. Pohst (editors), *Algorithmic number theory, proceedings of the 7th international symposium (ANTS-VII) held at the Technische Universität Berlin, Berlin, July 23–28, 2006*, Lecture Notes in Computer Science, 4076, Springer, Berlin, 2006. ISBN 3-540-36075-1. MR 2007h:11001. See [17].

[9] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, Ed Dawson, *Twisted Edwards curves revisited*, in Asiacrypt 2008 [14] (2008). URL: http://eprint.iacr.org/2008/522. Citations in this document: §1.1, §1.1.

[10] Kaoru Kurosawa (editor), *Advances in cryptology—ASIACRYPT 2007, 13th international conference on the theory and application of cryptology and information security, Kuching, Malaysia, December 2–6, 2007, proceedings*, Lecture Notes in Computer Science, 4833, Springer, 2007. ISBN 978-3-540-76899-9. See [5].

[11] Hendrik W. Lenstra, Jr., *Factoring integers with elliptic curves*, Annals of Mathematics **126** (1987), 649–673. ISSN 0003–486X. MR 89g:11125. URL: http://links.jstor.org/sici?sici=0003-486X(198711)2:126:3<649:FIWEC>2.0.CO;2-V. Citations in this document: §1.

[12] Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of Computation **48** (1987), 243–264. ISSN 0025–5718. MR 88e:11130. URL: http://links.jstor.org/sici?sici=0025-5718(198701)48:177<243:STPAEC>2.0.CO;2-3. Citations in this document: §1.2, §6. See [15].

[13] Peter L. Montgomery, *An FFT extension of the elliptic curve method of factorization*, Ph.D. thesis, University of California at Los Angeles, 1992. URL: ftp://ftp.cwi.nl/pub/pmontgom/ucladissertation.psl.gz. Citations in this document: §1.2, §1.3, §7.1.

[14] Josef Pieprzyk (editor), *Advances in cryptology — ASIACRYPT 2008, 14th international conference on the theory and application of cryptology and information security, Melbourne, Australia, December 7–11, 2008*, Lecture Notes in Computer Science, 5350, 2008. ISBN 978-3-540-89254-0. See [9].

[15] Hiromi Suyama, *Informal preliminary report (8)*, cited in [12] (1985). Citations in this document: §5.3.

[16] Serge Vaudenay (editor), *Progress in cryptology — AFRICACRYPT 2008, First international conference on cryptology in Africa, Casablanca, Morocco, June 11-14, 2008, proceedings*, Lecture Notes in Computer Science, 5023, Springer, 2008. ISBN 978-3-540-68159-5. See [3].

[17] Paul Zimmermann, Bruce Dodson, *20 years of ECM*, in ANTS VII [8] (2006), 525–542. URL: http://www.loria.fr/~zimmerma/papers/40760525.pdf. Citations in this document: §1.1, §1.2, §1.3.

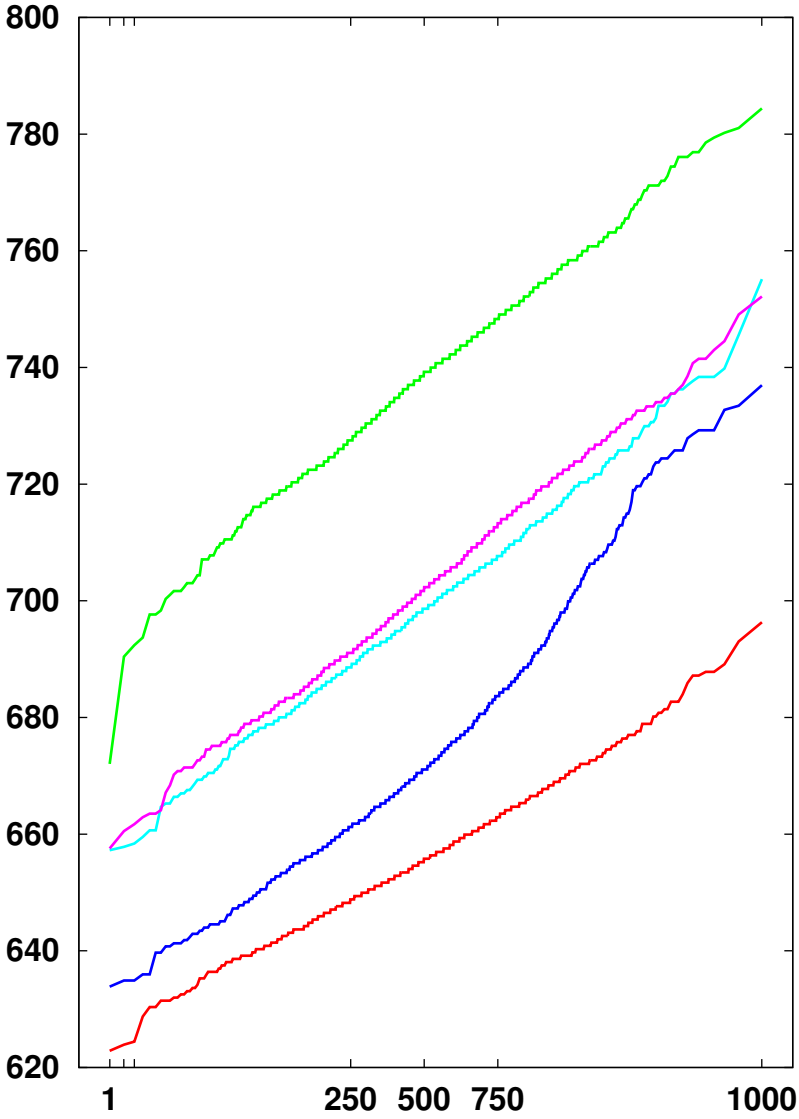


Fig. 7.1. Cost ratio for finding b-bit primes for $b = 15$. The horizontal axis is the curve number c within a pool of 1000 curves, with the most effective curve on the left and the least effective curve on the right. Horizontal tic marks appear at $c \in \{1, 2, 3, 250, 500, 750, 1000\}$. The horizontal scale is $\mathrm{erf}^{-1}((c - 500)/501)$, so a normal distribution would appear as approximately a straight line. The vertical axis is the total number of multiplications and squarings used in stage 1 and stage 2 of EECM with standard parameters, times the total number of b-bit primes, divided by the number of b-bit primes found by the curve. The five graphs are, from top to bottom in the middle, (green) $\mathbf{Z}/2 \times \mathbf{Z}/4$ with $a = -1$; (magenta) $\mathbf{Z}/8$ with $a = -1$; (cyan) $\mathbf{Z}/2 \times \mathbf{Z}/8$ with $a = 1$; (blue) $\mathbf{Z}/12$ with $a = 1$; and (red) $\mathbf{Z}/6$ with $a = -1$.

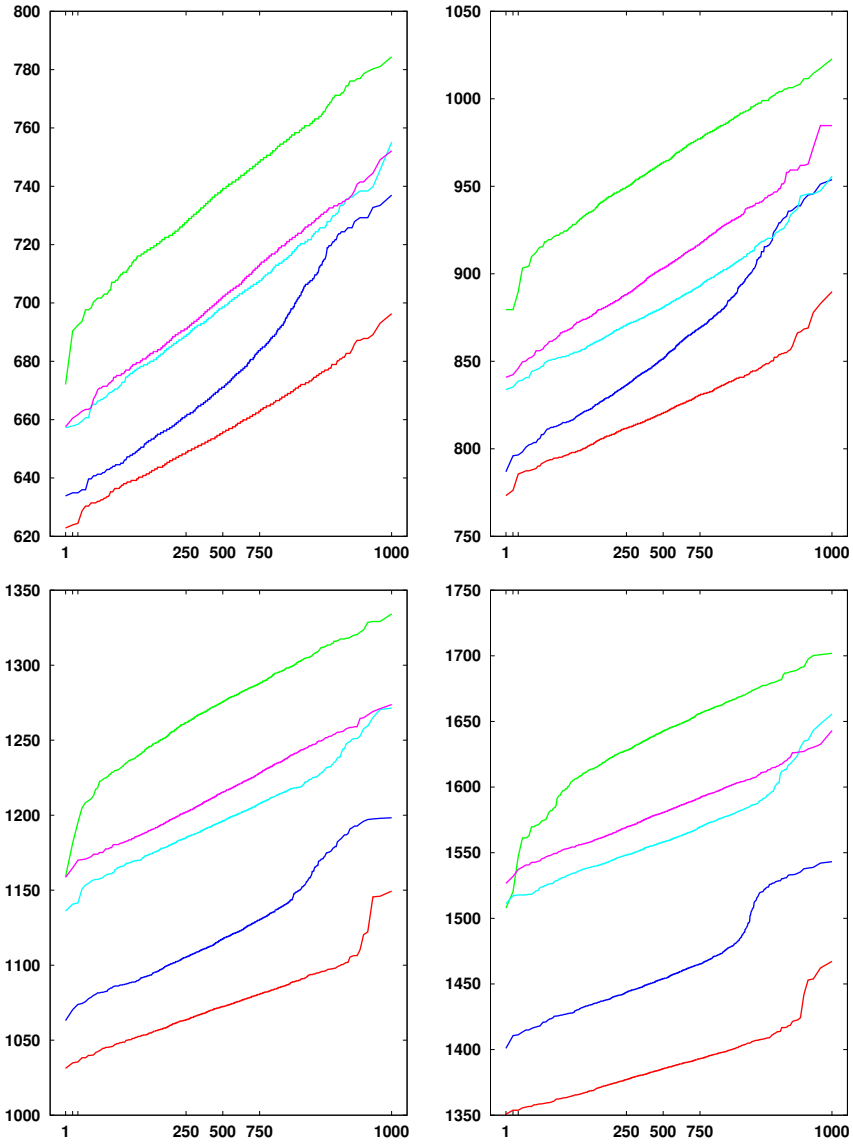


Fig. 7.2. Cost ratio for finding b-bit primes for $b \in \{15, 16, 17, 18\}$. See Figure 7.1 for explanation.

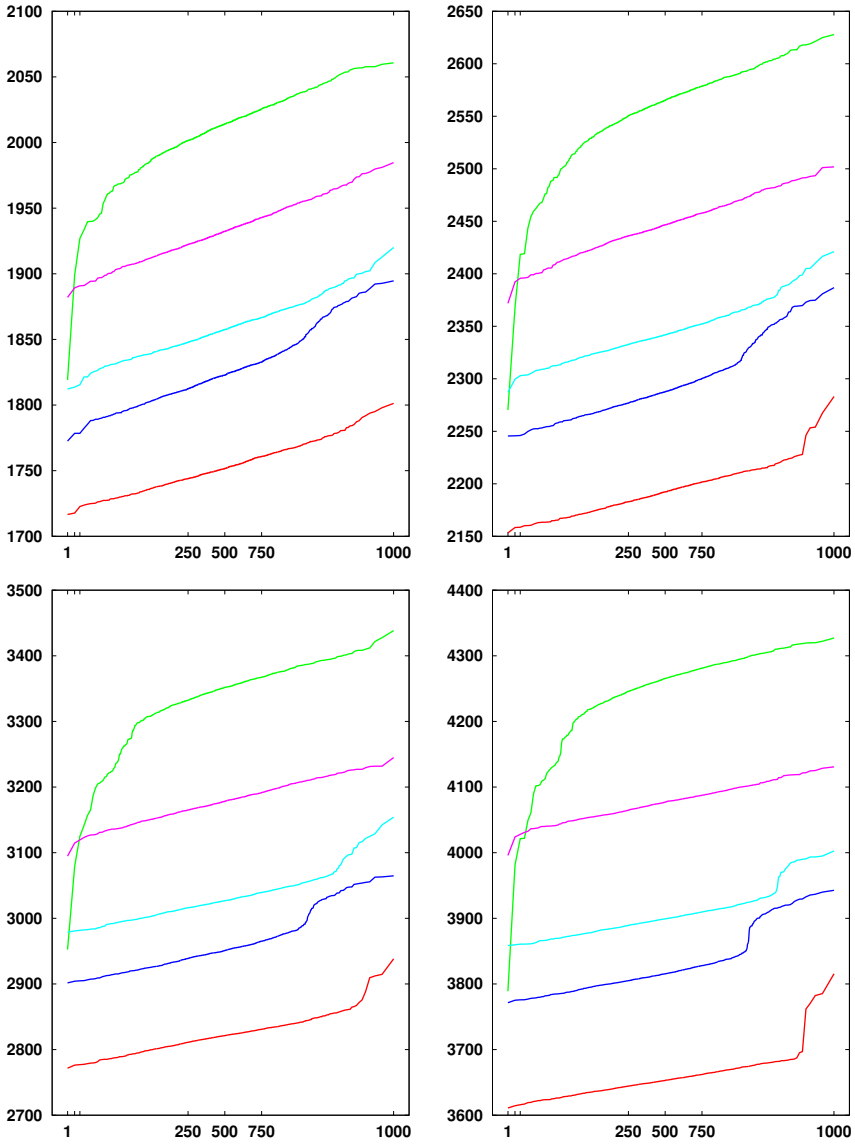


Fig. 7.3. Cost ratio for finding b-bit primes for $b \in \{19, 20, 21, 22\}$. See Figure 7.1 for explanation.

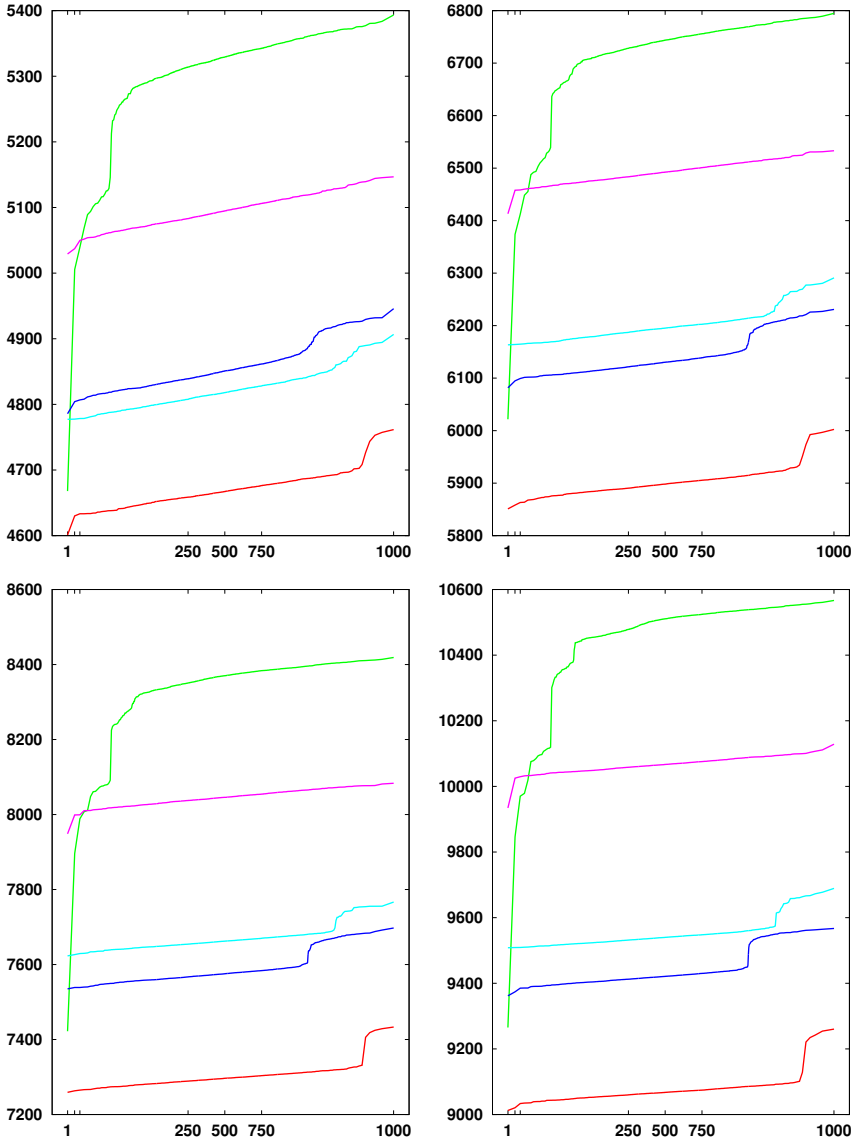


Fig. 7.4. Cost ratio for finding b-bit primes for $b \in \{23, 24, 25, 26\}$. See Figure 7.1 for explanation. The graph for $b = 23$ has $\mathbf{Z}/2 \times \mathbf{Z}/8$ below $\mathbf{Z}/12$.