Starfish on strike

Daniel J. Bernstein, Peter Birkner, Tanja Lange

2010.08.09

Edwards curves

An Edwards curve over a non-binary field k is a curve $x^2 + y^2 = 1 + dx^2y^2$ with $d \notin \{0, 1\}$.

Edwards addition law: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

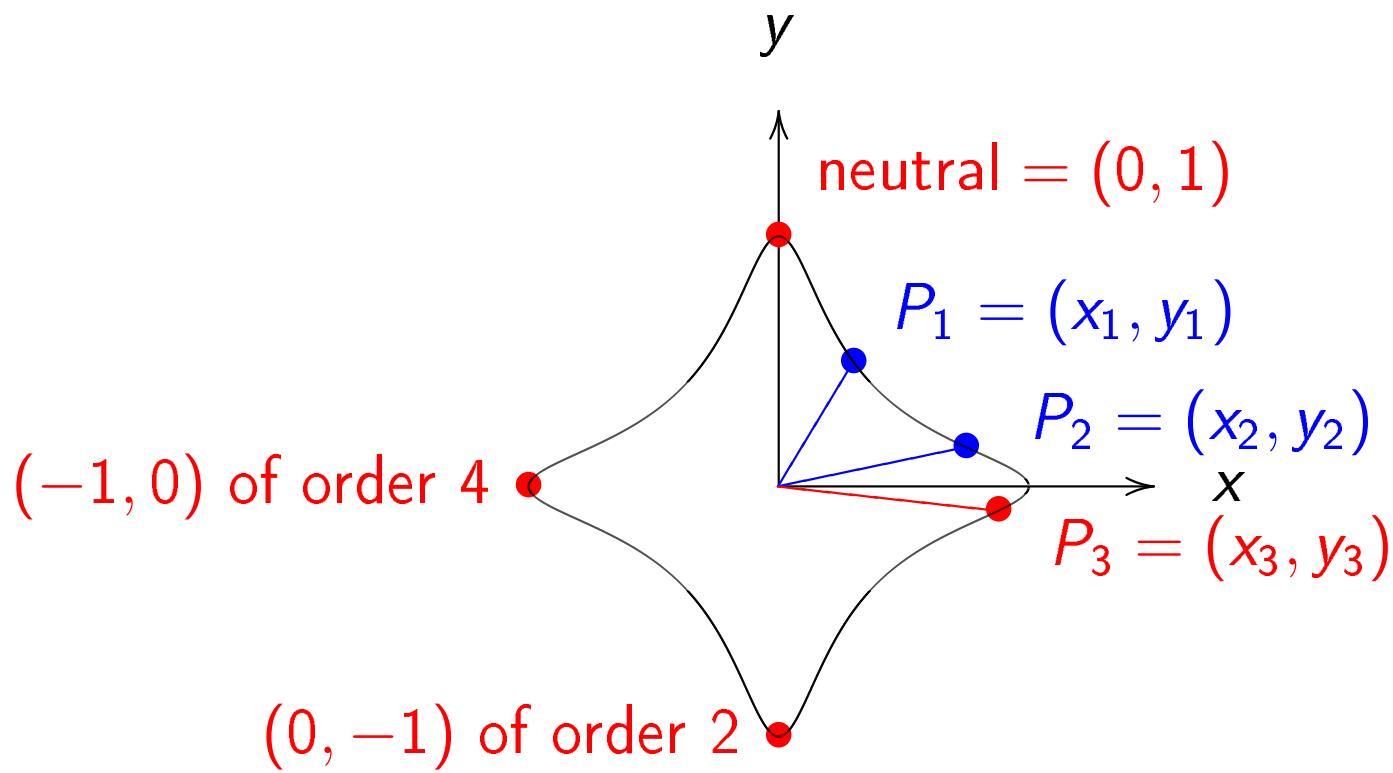
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \qquad y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Neutral element: $(0, 1)$. Negation: $-(x_1, y_1) = (-x_1, y_1)$.

Use projective representation to avoid divisions:

- $(X_1 : Y_1 : Z_1)$ represents $(X_1/Z_1, Y_1/Z_1)$.
- Addition costs $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{M}_d$.
- Doubling costs $3\mathbf{M} + 4\mathbf{S}$.

Example: $x^2 + y^2 = 1 - 30x^2y^2$



Compare to standard Jacobian $V^2 = U^3 - 3UW^4 + bW^6$:

- Addition $11\mathbf{M} + 5\mathbf{S}$. Edwards saves $4\mathbf{S} + 1\mathbf{M} - 1\mathbf{M}_d$.
- Doubling $3\mathbf{M} + 5\mathbf{S}$. Edwards saves $1\mathbf{S}$.

Example: $x^2 + y^2 = 1 - 30x^2y^2$

Compare to standard Jacobian $V^2 = U^3 - 3UW^4 + bW^6$:

- Addition $11\mathbf{M} + 5\mathbf{S}$. Edwards saves $4\mathbf{S} + 1\mathbf{M} - 1\mathbf{M}_d$.
- Doubling $3\mathbf{M} + 5\mathbf{S}$. Edwards saves $1\mathbf{S}$.

Twisted Edwards curves

2008 Bernstein–Birkner–Joye–Lange–Peters:
Generalize to "twisted Edwards curves"
$ax^2 + y^2 = 1 + dx^2y^2$ with $a \neq 0, d \neq 0, a \neq d$.

Addition law: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \qquad y_3 = \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}.$$

Advantages:

- More flexible: not necessarily a point of order 4.
- Covers all Montgomery curves.
- Covers even more curves with a 2-isogeny.
- Saves time when d is a ratio of small integers.

Speed of twisted Edwards curves

Projective addition: $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{M}_d + 1\mathbf{M}_a$.
Projective doubling: $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{M}_a$.

Speed of twisted Edwards curves

Projective addition: $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{M}_d + 1\mathbf{M}_a$.
Projective doubling: $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{M}_a$.

2008 Hisil–Wong–Carter–Dawson: dual addition law

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_1 + x_2 y_2}{a x_1 x_2 + y_1 y_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - y_1 x_2} \right);$$

extended coordinates $(X : Y : Z : T)$ with $T = XY/Z$;
bouncing between projective and extended coordinates.

Addition: $9\mathbf{M} + 1\mathbf{M}_a$. Only $8\mathbf{M}$ for $a = -1$.
Doubling: $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{M}_a$.

Note the addition speedup for $a = -1$.

The $p - 1$ method of factorization

$2^{232792560} - 1$ has prime divisors 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 103, 109, 113, 127, 131, 137, 151, 157, 181, 191, 199, etc.

An odd prime p divides $2^{232792560} - 1$
iff order of 2 in $\mathbf{F}_p^*$ divides 232792560.

Many ways for this to happen: 232792560 has 960 divisors.
Why so many?

$232792560 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$

Compute $\gcd\{2^{232792560} - 1, n\}$
to obtain the product of all primes p dividing n
such that the order of 2 in $\mathbf{F}_p^*$ divides 232792560.
(Assuming n squarefree for simplicity.)

ECM: the elliptic-curve method of factorization

Take a curve over $\mathbf{Q}$ with a point G.
E.g. Take any G, compute Edwards d from G.

Reduce this curve modulo n.
(Can recycle curve for many different n; ECM is green.)

Compute $[s]G$ modulo n for some very smooth s.
If the order of G in $E(\mathbf{F}_p)$ divides s
then the point $[s]G$ is the neutral element modulo p.
Detect by a suitable gcd computation.

E modulo p has order in $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$;
this may or may not be smooth but we can vary E.

Curve operations more expensive than in $p-1$ method;
but varying curves makes method much faster overall.

Torsion points

Curve over $\mathbf{Q}$ has some torsion points: points of finite order.
All possible torsion groups (Mazur's theorem):

- $\mathbf{Z}/m$ for $m \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$,
- $\mathbf{Z}/2 \times \mathbf{Z}/2m$ for $m \in \{1, 2, 3, 4\}$.

If a point has finite order on the curve over $\mathbf{Q}$ then
the point has the same finite order over $\mathbf{Z}/n$ and over $\mathbf{F}_p$.
Don't choose G as a torsion point.

Minimize trouble by choosing curve with torsion $\mathbf{Z}/1$?
No: people try to use curves with many torsion points.

e.g. 2008–2010 Bernstein–Birkner–Lange–Peters
"ECM using Edwards curves" (software: "EECM-MPFQ")
save time in ECM by using Edwards curves; construct
families of Edwards curves with torsion $\mathbf{Z}/12$ or $\mathbf{Z}/2 \times \mathbf{Z}/8$.

Why people want big torsion

Standard series of heuristic approximations when ECM uses a "random" elliptic curve:

Pr[prime $p \in [1, R]$ is found by this curve]

Why people want big torsion

Standard series of heuristic approximations when ECM uses a "random" elliptic curve:

$$\Pr[\text{prime } p \in [1, R] \text{ is found by this curve}]$$
$$\stackrel{?}{\approx} \Pr[\text{prime } p \in [1, R] \text{ has smooth } \#\langle G \text{ in } E(\mathbf{F}_p)\rangle]$$

Why people want big torsion

Standard series of heuristic approximations when ECM uses a "random" elliptic curve:

$\Pr[\text{prime } p \in [1, R] \text{ is found by this curve}]$
$\stackrel{?}{\approx} \Pr[\text{prime } p \in [1, R] \text{ has smooth } \#\langle G \text{ in } E(\mathbf{F}_p)\rangle]$
$\stackrel{?}{\approx} \Pr[\text{prime } p \in [1, R] \text{ has smooth } \#E(\mathbf{F}_p)]$

Why people want big torsion

Standard series of heuristic approximations when ECM uses a "random" elliptic curve:

$\Pr[\text{prime } p \in [1, R] \text{ is found by this curve}]$
$\stackrel{?}{\approx} \Pr[\text{prime } p \in [1, R] \text{ has smooth } \#\langle G \text{ in } E(\mathbf{F}_p)\rangle]$
$\stackrel{?}{\approx} \Pr[\text{prime } p \in [1, R] \text{ has smooth } \#E(\mathbf{F}_p)]$
$\stackrel{?}{\approx} \Pr[\text{integer} \in [1, R] \text{ is smooth}].$

Why people want big torsion

Standard series of heuristic approximations
when ECM uses a "random" elliptic curve:

Pr[prime $p \in [1, R]$ is found by this curve]
$\stackrel{?}{\approx}$ Pr[prime $p \in [1, R]$ has smooth $\#\langle G \text{ in } E(\mathbf{F}_p)\rangle$]
$\stackrel{?}{\approx}$ Pr[prime $p \in [1, R]$ has smooth $\#E(\mathbf{F}_p)$]
$\stackrel{?}{\approx}$ Pr[integer $\in [1, R]$ is smooth].

Standard series of heuristic approximations
when ECM uses a curve known to have t torsion points:

Pr[prime $p \in [1, R]$ is found by this curve]

Why people want big torsion

Standard series of heuristic approximations
when ECM uses a "random" elliptic curve:

$$\begin{aligned}
&\Pr[\text{prime } p \in [1, R] \text{ is found by this curve}] \\
&\overset{?}{\approx} \Pr[\text{prime } p \in [1, R] \text{ has smooth } \#\langle G \text{ in } E(\mathbf{F}_p)\rangle] \\
&\overset{?}{\approx} \Pr[\text{prime } p \in [1, R] \text{ has smooth } \#E(\mathbf{F}_p)] \\
&\overset{?}{\approx} \Pr[\text{integer} \in [1, R] \text{ is smooth}].
\end{aligned}$$

Standard series of heuristic approximations
when ECM uses a curve known to have t torsion points:

$$\begin{aligned}
&\Pr[\text{prime } p \in [1, R] \text{ is found by this curve}] \\
&\overset{?}{\approx} \Pr[\text{integer} \in t\mathbf{Z} \cap [1, R] \text{ is smooth}]
\end{aligned}$$

Why people want big torsion

Standard series of heuristic approximations
when ECM uses a "random" elliptic curve:

Pr[prime $p \in [1, R]$ is found by this curve]
$\stackrel{?}{\approx}$ Pr[prime $p \in [1, R]$ has smooth $\#\langle G \text{ in } E(\mathbf{F}_p)\rangle$]
$\stackrel{?}{\approx}$ Pr[prime $p \in [1, R]$ has smooth $\#E(\mathbf{F}_p)$]
$\stackrel{?}{\approx}$ Pr[integer $\in [1, R]$ is smooth].

Standard series of heuristic approximations
when ECM uses a curve known to have t torsion points:

Pr[prime $p \in [1, R]$ is found by this curve]
$\stackrel{?}{\approx}$ Pr[integer $\in t\mathbf{Z} \cap [1, R]$ is smooth]
$\stackrel{?}{\approx}$ Pr[integer $\in \mathbf{Z} \cap [1, R/t]$ is smooth].

Why people want big torsion

Standard series of heuristic approximations
when ECM uses a "random" elliptic curve:

$$\begin{aligned}
&\Pr[\text{prime } p \in [1,R] \text{ is found by this curve}] \\
&\stackrel{?}{\approx} \Pr[\text{prime } p \in [1,R] \text{ has smooth } \#\langle G \text{ in } E(\mathbf{F}_p)\rangle] \\
&\stackrel{?}{\approx} \Pr[\text{prime } p \in [1,R] \text{ has smooth } \#E(\mathbf{F}_p)] \\
&\stackrel{?}{\approx} \Pr[\text{integer} \in [1,R] \text{ is smooth}].
\end{aligned}$$

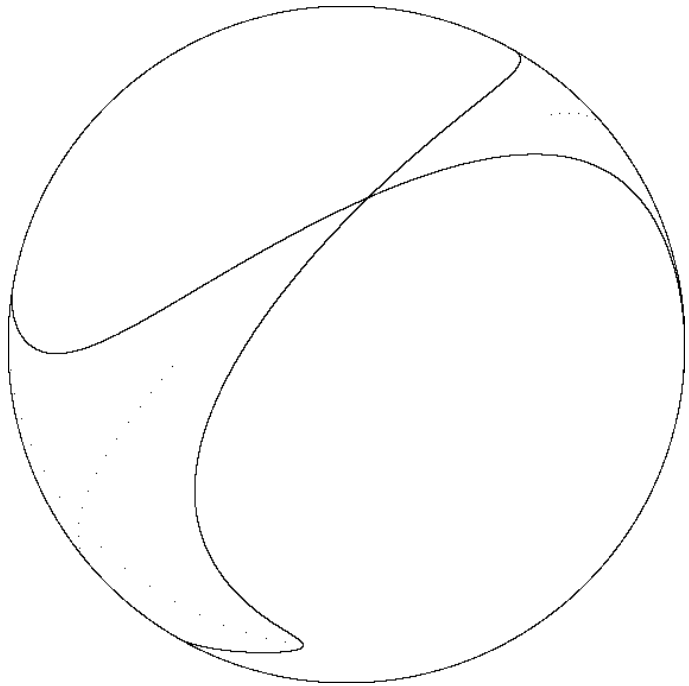
Standard series of heuristic approximations
when ECM uses a curve known to have t torsion points:

$$\begin{aligned}
&\Pr[\text{prime } p \in [1,R] \text{ is found by this curve}] \\
&\stackrel{?}{\approx} \Pr[\text{integer} \in t\mathbf{Z} \cap [1,R] \text{ is smooth}] \\
&\stackrel{?}{\approx} \Pr[\text{integer} \in \mathbf{Z} \cap [1,R/t] \text{ is smooth}].
\end{aligned}$$

Larger $t \Rightarrow$ smaller $R/t \Rightarrow$ larger Pr.

Starfish on strike

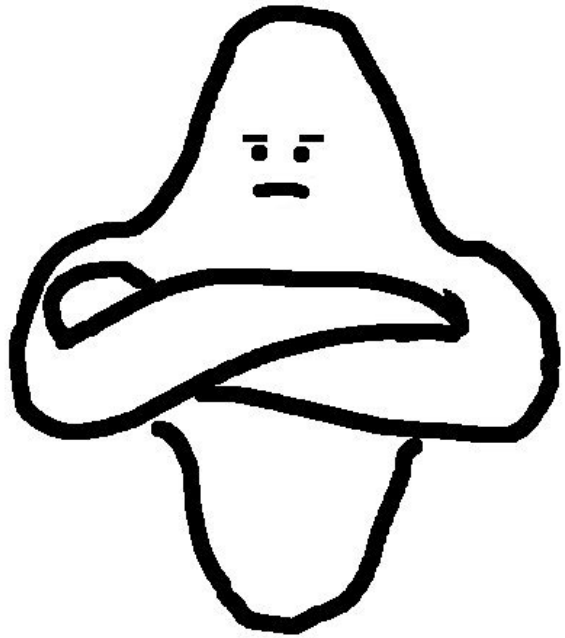
Would like to combine $a = -1$ speedup with large torsion.
Let's look closer at $-x^2 + y^2 = 1 - 30x^2y^2$:



Singularity at infinity blows up to two points of order 2.
EECM paper proved: arbitrary d with $a = -1$
cannot achieve highest torsion such as $\mathbf{Z}/12$ and $\mathbf{Z}/2 \times \mathbf{Z}/8$.

Starfish on strike

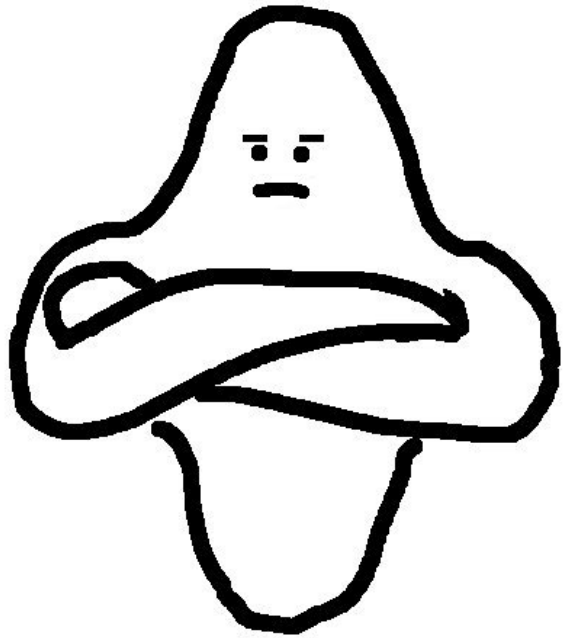
Would like to combine $a = -1$ speedup with large torsion.
Let's look closer at $-x^2 + y^2 = 1 - 30x^2y^2$:



Singularity at infinity blows up to two points of order 2.
EECM paper proved: arbitrary d with $a = -1$
cannot achieve highest torsion such as $\mathbf{Z}/12$ and $\mathbf{Z}/2 \times \mathbf{Z}/8$.

Starfish on strike

Would like to combine $a = -1$ speedup with large torsion.
Let's look closer at $-x^2 + y^2 = 1 - 30x^2y^2$:



Singularity at infinity blows up to two points of order 2.
EECM paper proved: arbitrary d with $a = -1$
cannot achieve highest torsion such as $\mathbf{Z}/12$ and $\mathbf{Z}/2 \times \mathbf{Z}/8$.
This paper: Does $a = -1$ speedup outweigh smaller torsion?

Example: Constructing $\mathbf{Z}/8$ with $a = -1$

Twisted Edwards curve has 1 affine point of order 2 at $(0, -1)$.
Points of order 4 doubling to $(0, -1)$ exist iff $a = \square$ or $d = \square$.
For $a = -1$ only possibility is $d = \square$.

Many more restrictions on d to construct points of order 8 and non-torsion point G. Resulting theorem:

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 $\boldsymbol{Q}$.
Define $u = 2r/s$, $v = (2r^3 - s^2)/s^2$, $d = (16u^4)/(4u^4 - 1)^2$.
Then the twisted Edwards curve $-x^2 + y^2 = 1 + dx^2y^2$ has torsion group $\boldsymbol{Z}/8$ and non-torsion point $(2u^2, (4u^4 - 1)/v)$.

Can take $(4, -16)$ and its multiples as values for (r, s).
Paper has similar constructions for $\mathbf{Z}/2 \times \mathbf{Z}/4$ and $\mathbf{Z}/6$; note that torsion groups are half-size compared to EECM paper.

Experiments and conclusions

We modified EECM-MPFQ to support our new curves.

EECM paper optimized EECM-MPFQ s etc. for old curves.
We tried those parameters with thousands of our curves
for all b-bit primes for each $b \in \{15, 16, \ldots, 26\}$.

Experiments and conclusions

We modified EECM-MPFQ to support our new curves.

EECM paper optimized EECM-MPFQ s etc. for old curves.
We tried those parameters with thousands of our curves
for all b-bit primes for each $b \in \{15, 16, \ldots, 26\}$.

Happy observation: Our new $\mathbf{Z}/6$ $a = -1$ curves
are the new price/performance leaders for ECM!
EECM-MPFQ now uses these curves by default.
Gain in # modular multiplications per curve
outweighs loss in # primes found per curve.

Experiments and conclusions

We modified EECM-MPFQ to support our new curves.

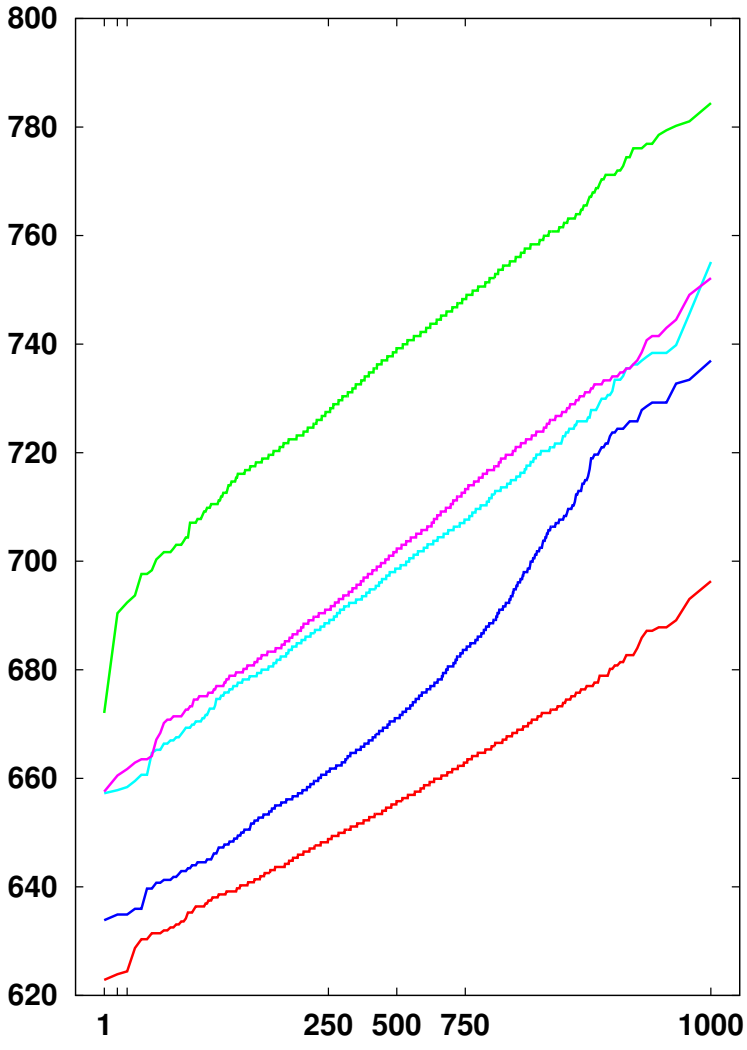
EECM paper optimized EECM-MPFQ s etc. for old curves.
We tried those parameters with thousands of our curves
for all b-bit primes for each $b \in \{15, 16, \ldots, 26\}$.

Happy observation: Our new $\mathbf{Z}/6$ $a = -1$ curves
are the new price/performance leaders for ECM!
EECM-MPFQ now uses these curves by default.
Gain in # modular multiplications per curve
outweighs loss in # primes found per curve.

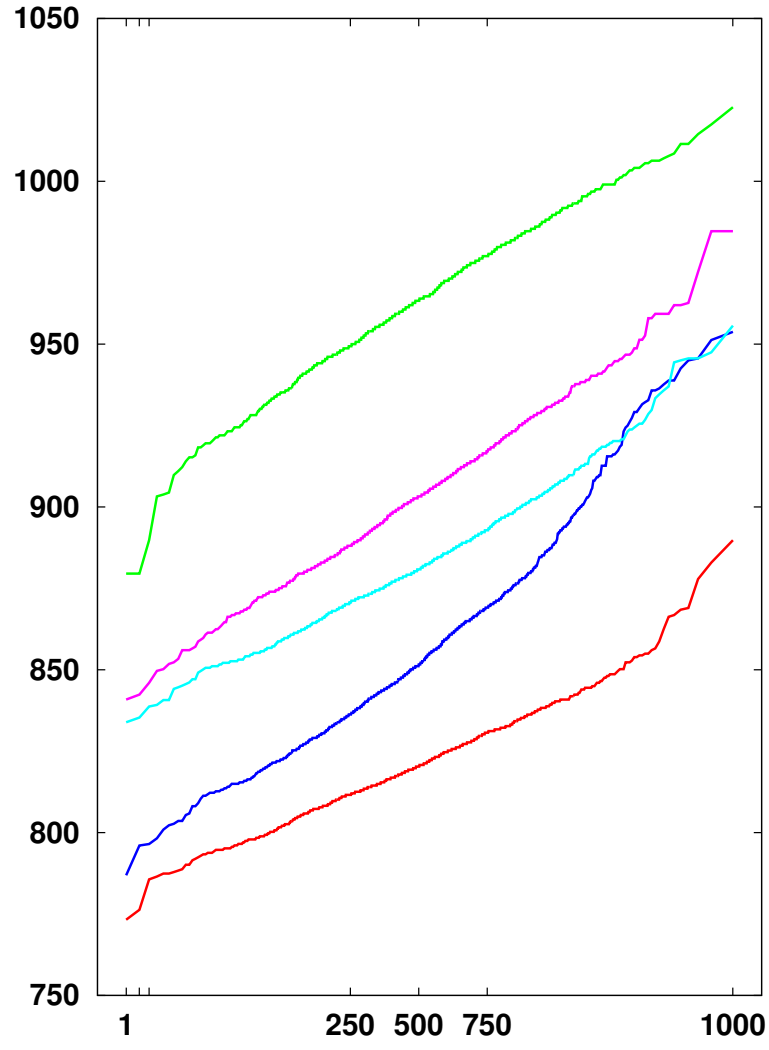
Surprising observation: It's a gain, not a loss!
Switching from $\mathbf{Z}/2 \times \mathbf{Z}/8$ to our new curves
decreases torsion but *increases* # primes found per curve.
Some particular curves are even more effective.

Number of modular multiplications per prime found

15-bit primes

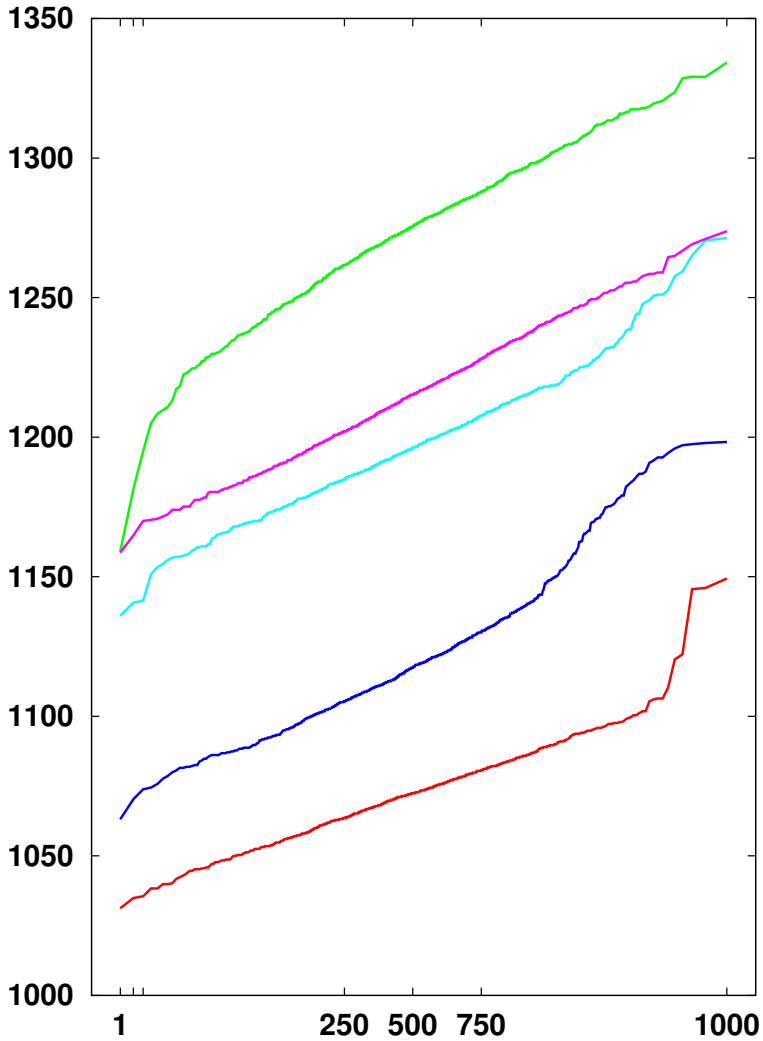


16-bit primes

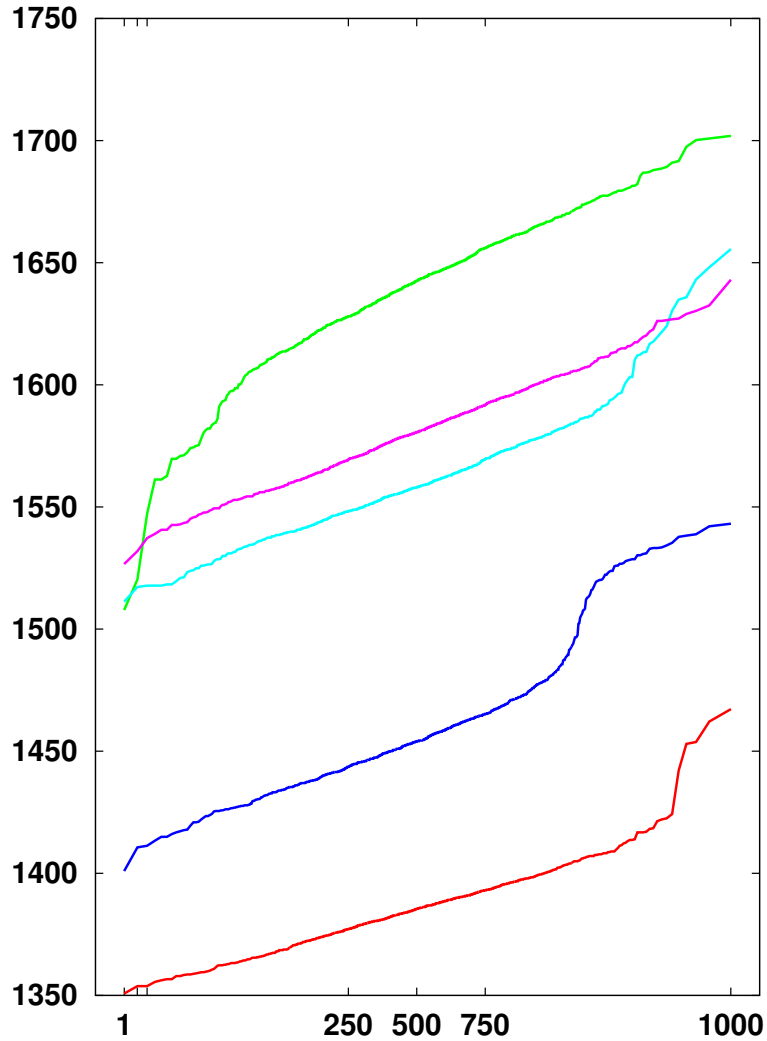


Number of modular multiplications per prime found

17-bit primes

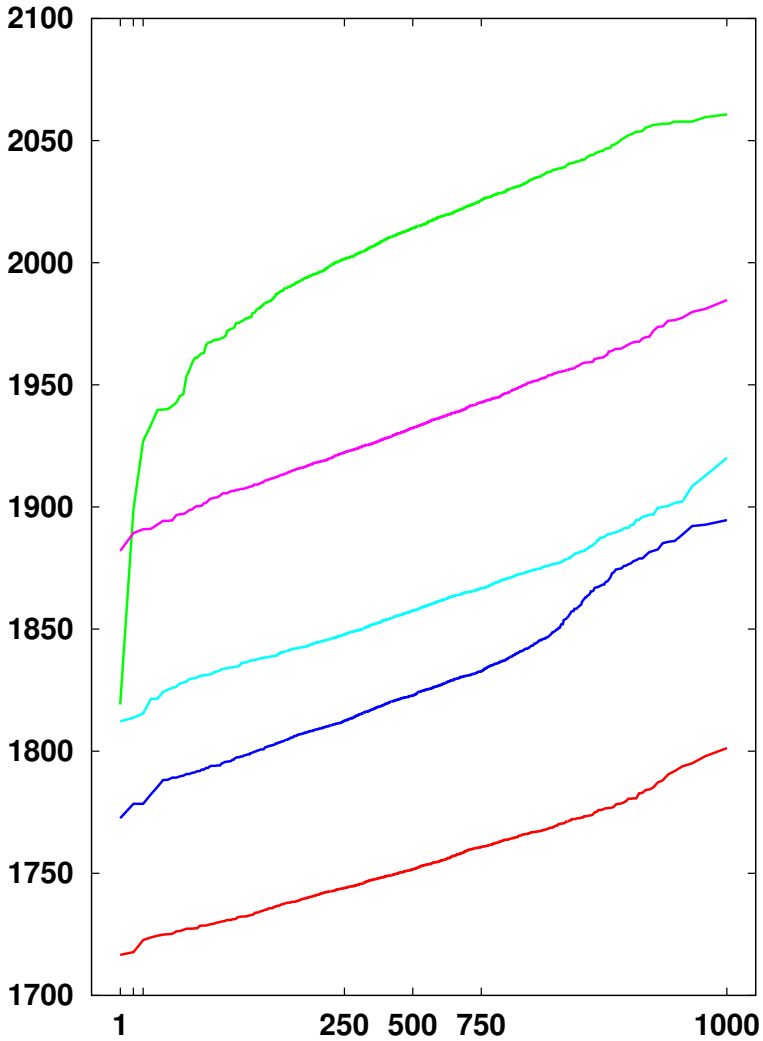


18-bit primes

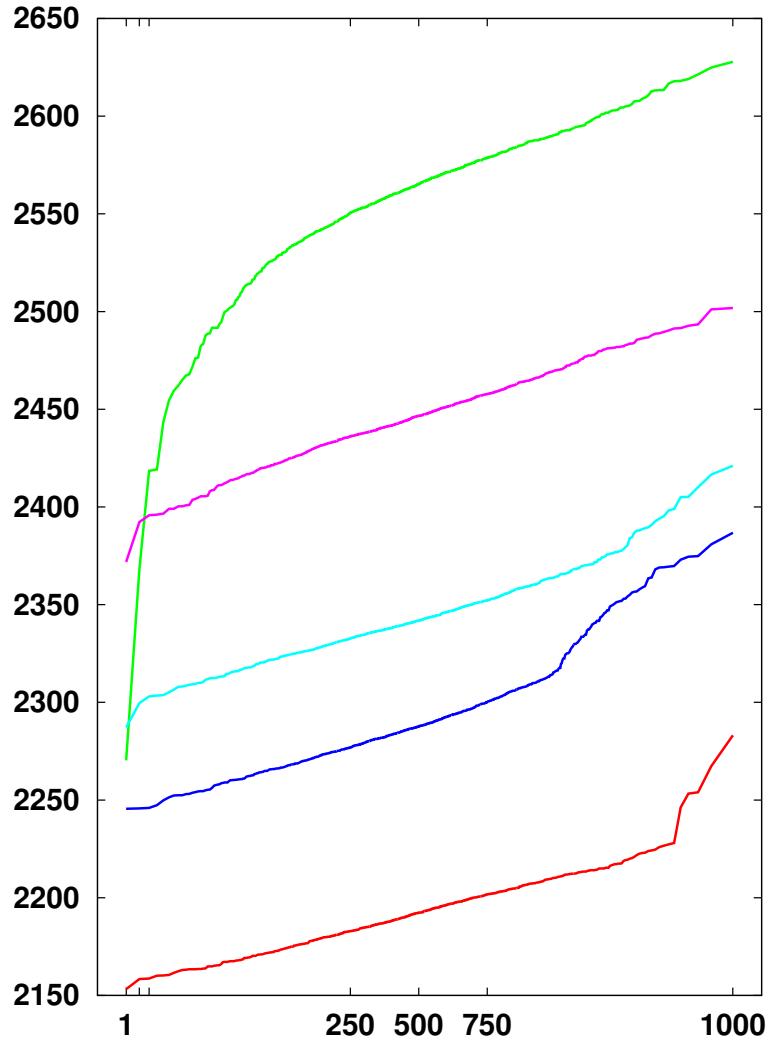


Number of modular multiplications per prime found

19-bit primes

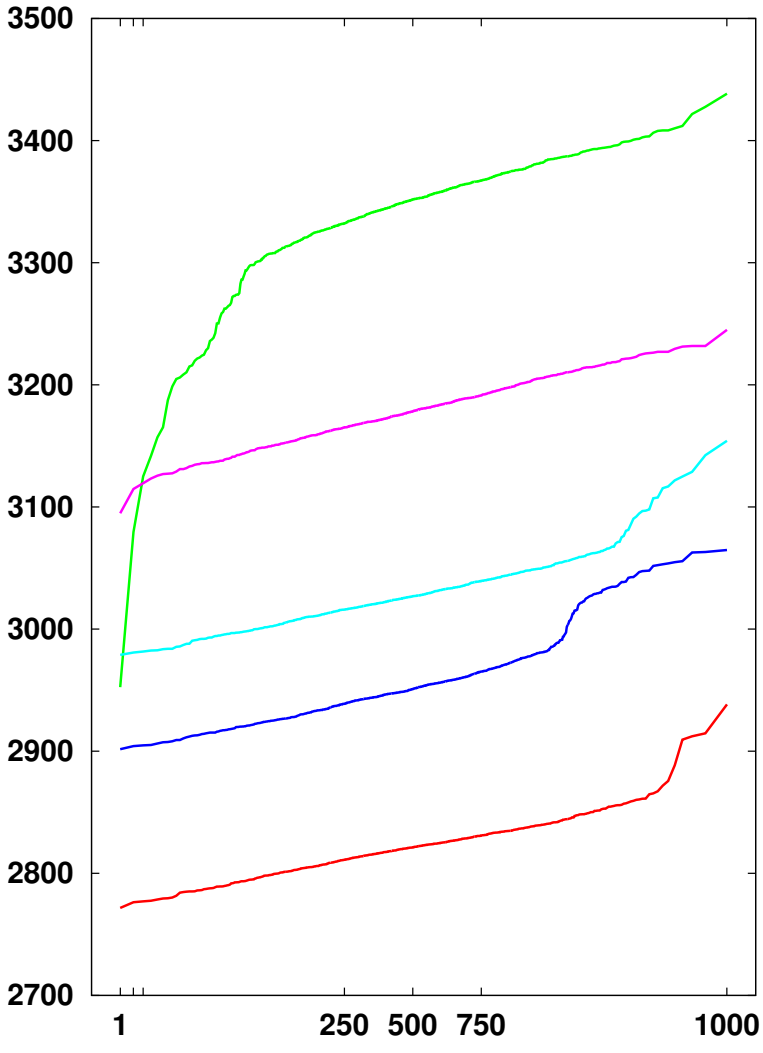


20-bit primes

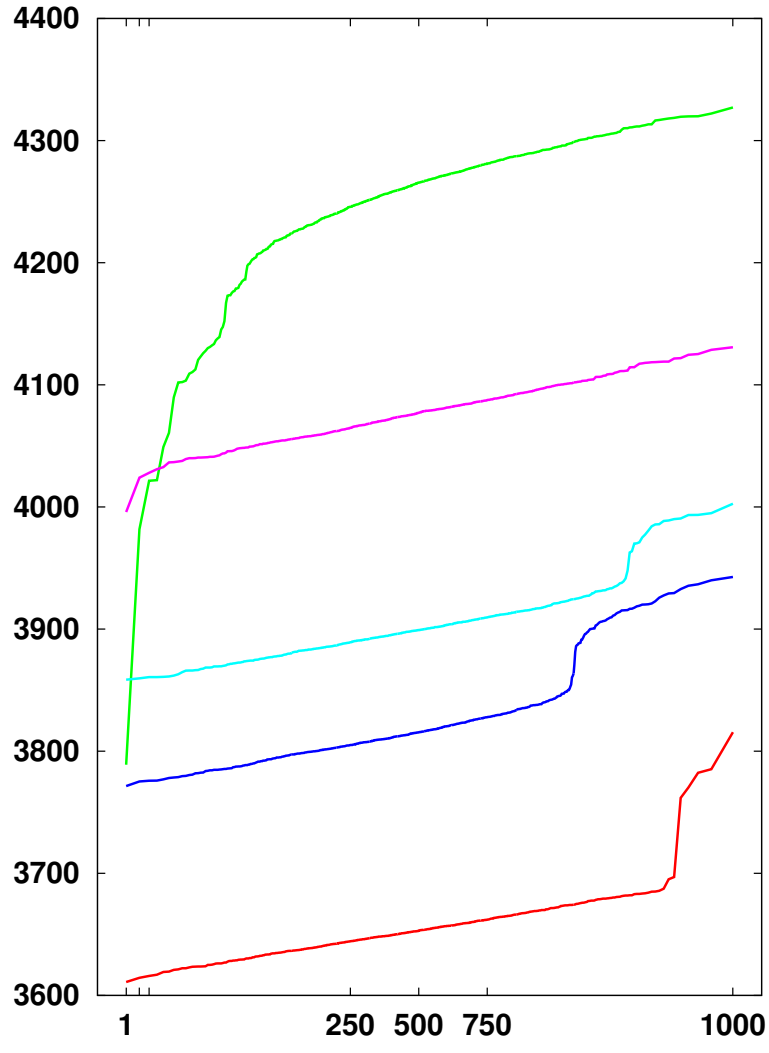


Number of modular multiplications per prime found

21-bit primes

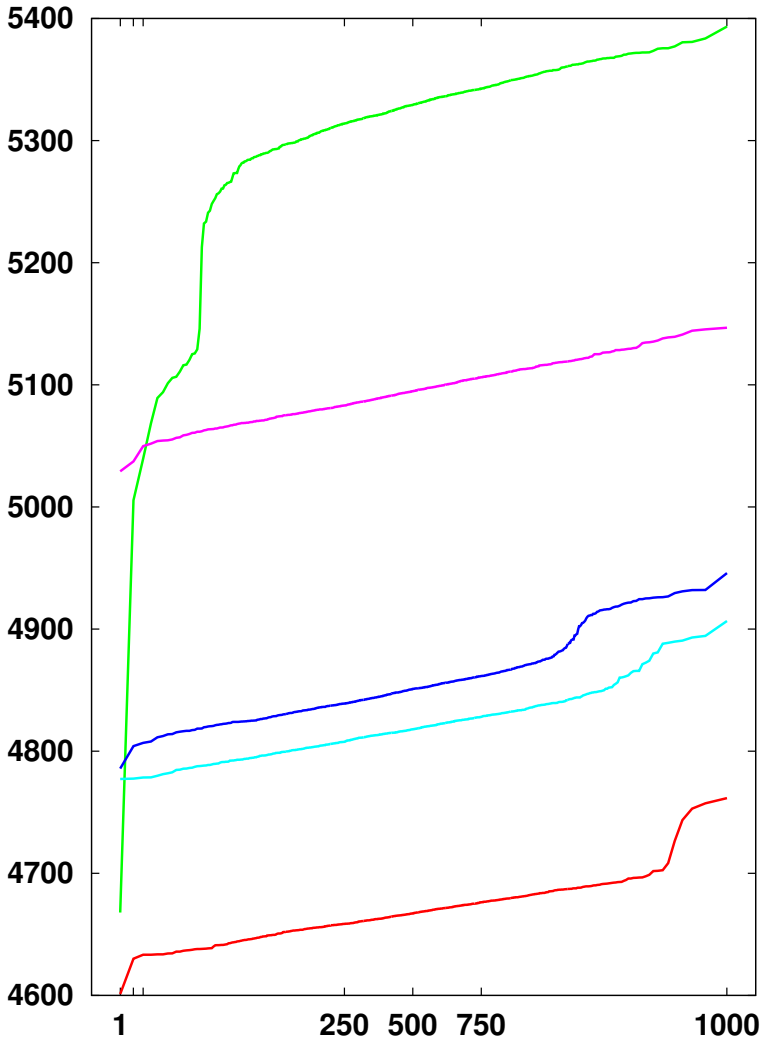


22-bit primes

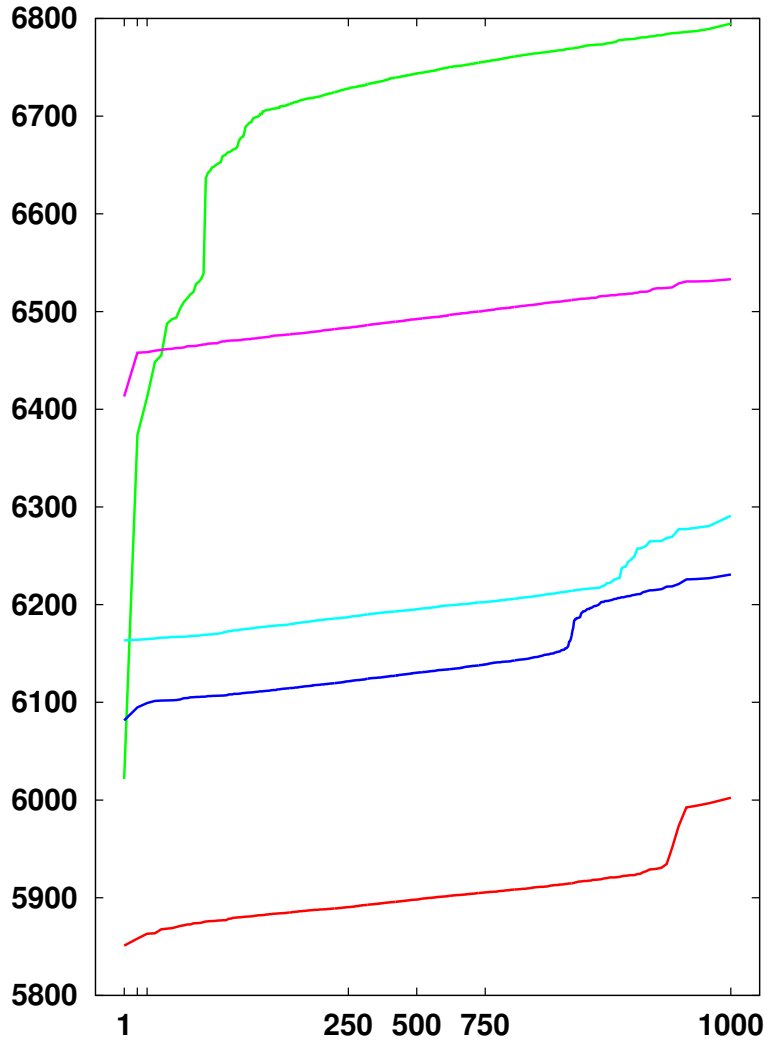


Number of modular multiplications per prime found

23-bit primes

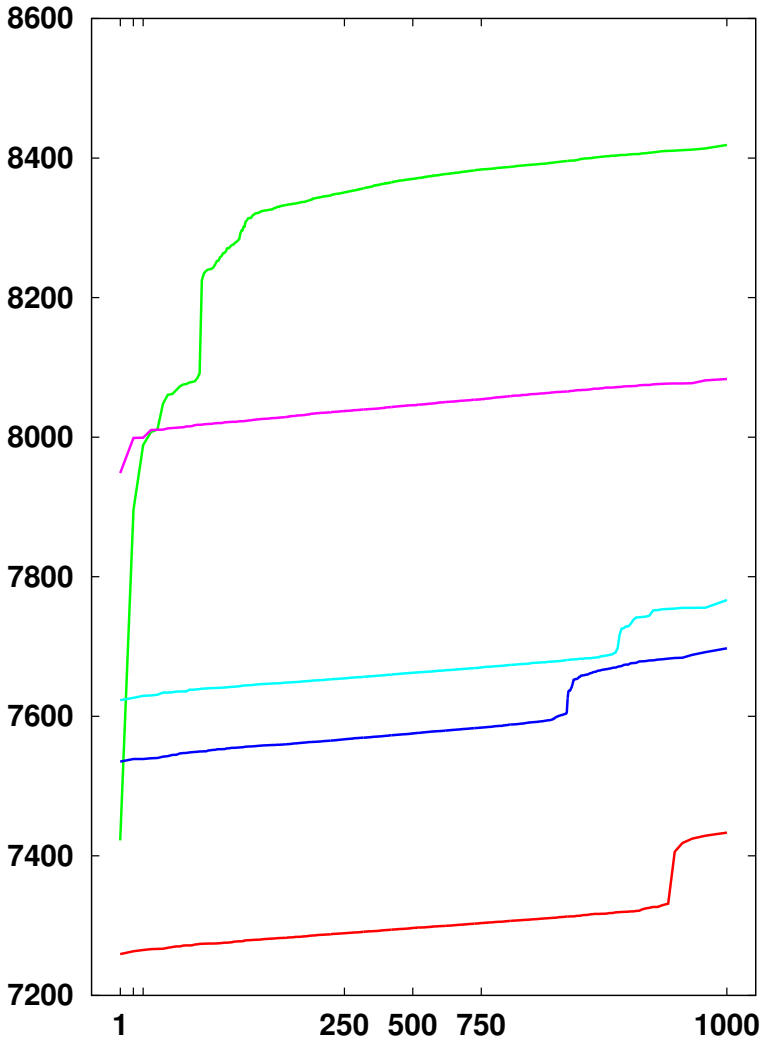


24-bit primes

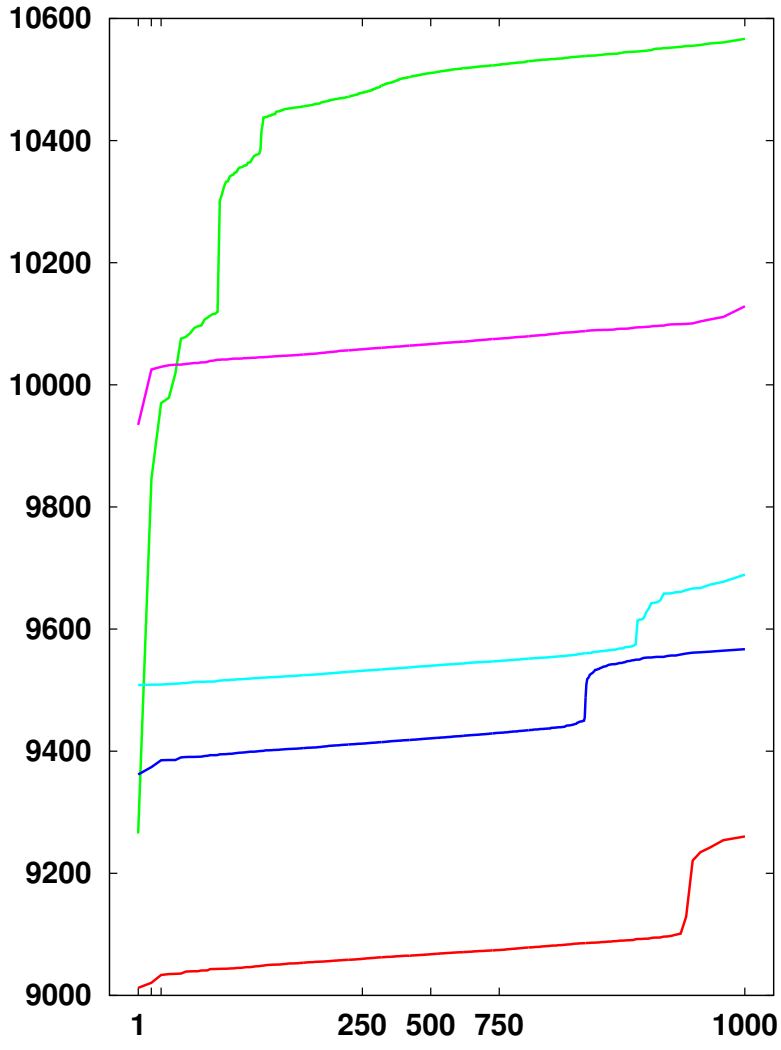


Number of modular multiplications per prime found

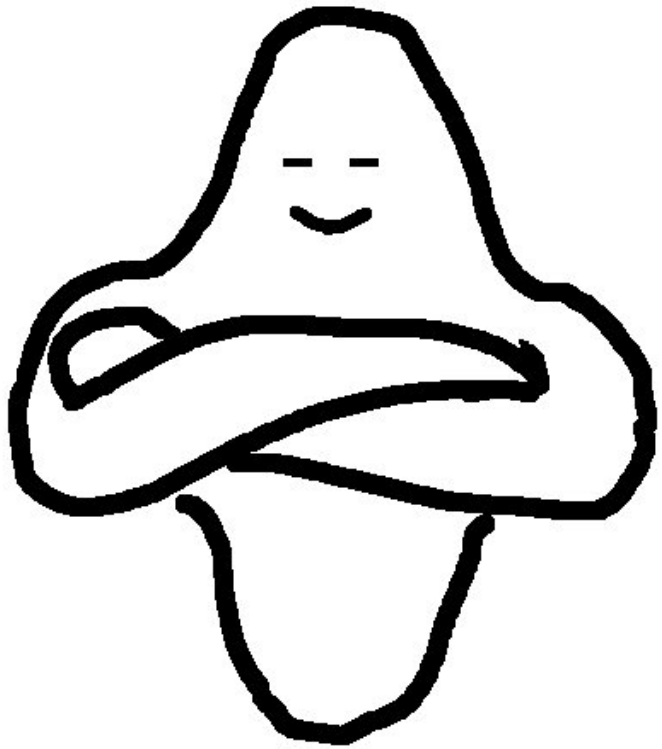
25-bit primes



26-bit primes



The end



Thanks!