Algorithms for primes

D. J. Bernstein
University of Illinois at Chicago

Some literature:

Recognizing primes:
1982 Atkin–Larson "On a primality test of Solovay and Strassen"; 1995 Atkin "Intelligent primality test offer"

Proving primes to be prime:
1993 Atkin–Morain "Elliptic curves and primality proving"

Factoring integers into primes:
1993 Atkin–Morain "Finding suitable curves for the elliptic curve method of factorization"

Enumerating small primes:
2004 Atkin–Bernstein "Prime sieves using binary quadratic forms"

Recognizing primes

Fermat: $w \in \mathbf{Z}$, prime $n \in \mathbf{Z}$
$\Rightarrow w^n - w = 0$ in $\mathbf{Z}/n$.

e.g. Fast proof of compositeness
of $n = 314159265358979323$:
in $\mathbf{Z}/n$ compute $2^n - 2$
$= 198079119221837430 \neq 0$.

Recognizing primes

Fermat: $w \in \mathbf{Z}$, prime $n \in \mathbf{Z}$
$\Rightarrow w^n - w = 0$ in $\mathbf{Z}/n$.

e.g. Fast proof of compositeness
of $n = 314159265358979323$:
in $\mathbf{Z}/n$ compute $2^n - 2$
$= 198079119221837430 \neq 0$.

"Carmichael numbers" are
composites that cannot be
proven composite this way.
1994 Alford–Granville–Pomerance:
$\#\{\text{Carmichael numbers}\} = \infty$.

Refined Fermat:

$w \in \mathbf{Z}$, prime $n \in 1 + 2\mathbf{Z}$

$\Rightarrow w = 0$ in $\mathbf{Z}/n$

or $w^{(n-1)/2} + 1 = 0$ in $\mathbf{Z}/n$

or $w^{(n-1)/2} - 1 = 0$ in $\mathbf{Z}/n$.

Proof:

$w^n - w$

$= w(w^{n-1} - 1)$

$= w(w^{(n-1)/2} + 1)(w^{(n-1)/2} - 1)$.

■

Doubly refined Fermat:

$w \in \mathbf{Z}$, prime $n \in 1 + 4\mathbf{Z}$

$\Rightarrow w = 0$ in $\mathbf{Z}/n$

or $w^{(n-1)/2} + 1 = 0$ in $\mathbf{Z}/n$

or $w^{(n-1)/4} + 1 = 0$ in $\mathbf{Z}/n$

or $w^{(n-1)/4} - 1 = 0$ in $\mathbf{Z}/n$.

Proof:

$$
\begin{aligned}
&w^n - w \\
&= w(w^{n-1} - 1) \\
&= w(w^{(n-1)/2} + 1)(w^{(n-1)/2} - 1); \\
&= w(w^{(n-1)/2} + 1) \\
&\qquad (w^{(n-1)/4} + 1)(w^{(n-1)/4} - 1).
\end{aligned}
$$

■

1966 Artjuhov:

$w \in \mathbf{Z}$, prime $n \in 1 + 2^u + 2^{u+1}\mathbf{Z}$

$\Rightarrow w = 0$ in $\mathbf{Z}/n$

or $w^{(n-1)/2} + 1 = 0$ in $\mathbf{Z}/n$

or $w^{(n-1)/4} + 1 = 0$ in $\mathbf{Z}/n$

$\vdots$

or $w^{(n-1)/2^u} + 1 = 0$ in $\mathbf{Z}/n$

or $w^{(n-1)/2^u} - 1 = 0$ in $\mathbf{Z}/n$.

e.g. Proof that 2821 is not prime:

in $\mathbf{Z}/2821$ have $2^{1410} + 1 = 1521$;

$2^{705} + 1 = 2606$; $2^{705} - 1 = 2604$.

Non-prime $n \in 1 + 2\mathbf{Z}$
$\Rightarrow$ uniform random
$w \in \{1, 2, \ldots, n - 1\}$
has $\geq$75% chance to prove
n non-prime by this test.

Try $\lceil \lg n \rceil$ choices of w.
Conjecture: If this doesn't prove
n non-prime then n is prime.

Messy history: Dubois, Selfridge,
Miller, Rabin, Lehmer, Solovay–
Strassen, Monier, Atkin–Larson.

Time $(\lg n)^{3+o(1)}$ for
$(\lg n)^{1+o(1)}$ exponentiations.
Can we do better?

e.g. Only $\lceil\sqrt{\lg n}\rceil$ choices of w?

Time $(\lg n)^{3+o(1)}$ for
$(\lg n)^{1+o(1)}$ exponentiations.
Can we do better?

e.g. Only $\lceil\sqrt{\lg n}\rceil$ choices of w?

No! There are too many n's
that have too many failing w's.

e.g. 1982 Atkin–Larson:
If $4k+3, 8k+5$ are prime
then $n=(4k+3)(8k+5)$ has
$(2k+1)(4k+2)$ failing w's.

Do better by extending $\mathbf{Z}/n$?

Main credits: Lucas, Selfridge.

e.g. Prime $n \in 1 + 2\mathbf{Z}$, $w \in \mathbf{Z}$, $w^2 - 4$ has Jacobi symbol -1 in $\mathbf{Z}/n \Rightarrow t^{(n+1)/2} \in \{1, -1\}$ in $(\mathbf{Z}/n)[t]/(t^2 - wt + 1)$.

Proof: $k = (\mathbf{Z}/n)[t]/(t^2 - wt + 1)$ is a field. In $k[u]$ have $u^2 - wu + 1 = (u - t)(u - t^n)$ so in k have $t^{n+1} = 1$. ■

Geometric view: group scheme G
$= \{(x, y) : x^2 - wxy + y^2 = 1\}$;
addition of (x, y) induced by
mult of $y + xt$ modulo $t^2 - wt + 1$.

$w^2 - 4$ has Jacobi symbol -1
so $\#G(\mathbf{Z}/n) = n + 1$ so
$(n + 1)(1, 0) = (0, 1)$ in $G(\mathbf{Z}/n)$.

Faster than $(\mathbf{Z}/n)^*$? No.
More reliable than $(\mathbf{Z}/n)^*$?

Geometric view: group scheme G $= \{(x, y) : x^2 - wxy + y^2 = 1\}$; addition of (x, y) induced by mult of $y + xt$ modulo $t^2 - wt + 1$.

$w^2 - 4$ has Jacobi symbol -1 so $\#G(\mathbf{Z}/n) = n + 1$ so $(n + 1)(1, 0) = (0, 1)$ in $G(\mathbf{Z}/n)$.

Faster than $(\mathbf{Z}/n)^*$? No.
More reliable than $(\mathbf{Z}/n)^*$?
No. Easily construct many n that have many bad w.

Try another group scheme?
e.g. $E : x^2 + y^2 = 1 - 30x^2y^2$.
Main obstacle: Find $\#E(\mathbf{Z}/n)$,
assuming that n is prime.

1986 Chudnovsky–Chudnovsky,
1987 Gordon: Build E here
using CM with class number 1.

Faster than $(\mathbf{Z}/n)^*$? No.
More reliable than $(\mathbf{Z}/n)^*$?

Try another group scheme?
e.g. $E : x^2 + y^2 = 1 - 30x^2y^2$.
Main obstacle: Find $\#E(\mathbf{Z}/n)$,
assuming that n is prime.

1986 Chudnovsky–Chudnovsky,
1987 Gordon: Build E here
using CM with class number 1.

Faster than $(\mathbf{Z}/n)^*$? No.
More reliable than $(\mathbf{Z}/n)^*$?
No. Easily construct many
"elliptic pseudoprimes."

1980 Baillie–Wagstaff, 1980
Pomerance–Selfridge–Wagstaff:

One $x^2 - wxy + y^2 = 1$ test
plus one $(\mathbf{Z}/n)^*$ exponentiation.
Time $(\lg n)^{2+o(1)}$.

Much more reliable than
two $(\mathbf{Z}/n)^*$ exponentiations!

\$620 for a counterexample,
i.e., a non-proved non-prime.

1995 Atkin:
one $(\mathbf{Z}/n)^*$ exponentiation
plus one $x^2 - wxy + y^2 = 1$ test
plus one cubic test.
$2500 for a counterexample.

Bad news: There should be
infinitely many counterexamples
to the 1980 tests
(1984 Pomerance, adapting
heuristic from 1956 Erdős)
and to Atkin's test.

Conjecture (new?):

Continuing this series becomes perfectly reliable after only $(\lg n)^{o(1)}$ tests.

Resulting algorithm determines primality of n in time $(\lg n)^{2+o(1)}$.

Conjecture (new?):

Continuing this series becomes perfectly reliable after only $(\lg n)^{o(1)}$ tests.

Resulting algorithm determines primality of n in time $(\lg n)^{2+o(1)}$.

To optimize $o(1)$: replace high-degree extensions with many elliptic curves.

1956 Erdős heuristic:

For each prime divisor p of n:
Force frequent $w^{n-1} = 1$ in $\mathbf{Z}/p$
by forcing $n - 1 \in (p - 1)\mathbf{Z}$ or
maybe $n - 1 \in ((p - 1)/2)\mathbf{Z} \ldots$

1956 Erdős heuristic:

For each prime divisor p of n:
Force frequent $w^{n-1} = 1$ in $\mathbf{Z}/p$
by forcing $n - 1 \in (p - 1)\mathbf{Z}$ or
maybe $n - 1 \in ((p - 1)/2)\mathbf{Z}$ . . .

"Chance" $\approx 1/\text{lcm}\{p - 1\}$.

1956 Erdős heuristic:

For each prime divisor p of n:
Force frequent $w^{n-1} = 1$ in $\mathbf{Z}/p$
by forcing $n - 1 \in (p - 1)\mathbf{Z}$ or
maybe $n - 1 \in ((p - 1)/2)\mathbf{Z}$ ...

"Chance" $\approx 1/\text{lcm}\{p - 1\}$.

Force small lcm by
restricting to primes p
with $p - 1 = \prod$ subset of Q_1,
where Q_1 is set of small primes.

1984 Pomerance heuristic:

Choose disjoint Q_1, Q_2.
Restrict to primes p
with $p - 1 = \prod$ subset of Q_1
and $p + 1 = \prod$ subset of Q_2.
Build n from these primes p.

Large chance that
$n - 1 \in (p - 1)\mathbf{Z}$ for all p and
$n + 1 \in (p + 1)\mathbf{Z}$ for all p.

Obvious extension:
Can similarly fool t tests
starting with $Q_1, Q_2, \ldots, Q_t$.

…but quantitative analysis,
generalizing Pomerance analysis,
suggests that smallest n
is *doubly* exponential in t,
i.e., $t \in O(\lg \lg n)$.

My conjecture: $t \in (\lg n)^{o(1)}$.

Interlude: Building E by CM

How quickly can we build t elliptic curves E with known $\#E(\mathbf{Z}/n)$, assuming n is prime? (Maybe best: 4 extensions and $t-4$ elliptic curves.)

Assume $t \le (\lg n)^{0.3}$. Compare to ECPP situation: $t \in (\lg n)^{1+o(1)}$ to find near-prime order.

Adapting idea of FastECPP
(1990 Shallit):

Compute square roots
of $\{1, 2, \ldots, \lfloor t^{1/2} \rfloor\}$ in $\mathbf{Z}/n$.
Time $t^{1/2}(\lg n)^{2+o(1)}$.
(Surely $t^{1/2}$ isn't optimal.)

Multiply to obtain square roots
of all $t^{1/2}$-smooth
discriminants $\le t^2$.
Time $t^2(\lg n)^{1+o(1)}$.

Apply Cornacchia.
Time $t^2(\lg n)^{1+o(1)}$.

Now have $\approx t$
CM discriminants for n,
assuming standard heuristics.
If $< t$: tweak "$\le t^2$."

Find the curves by fast CM:
$t^2(\lg n)^{1+o(1)} + t(\lg n)^{2+o(1)}$?
Latest news: 2010.09 Sutherland.

Proving primes to be prime

ECPP finds *proof* of primality in conjectured time $(\lg n)^{5+o(1)}$.

FastECPP: $(\lg n)^{4+o(1)}$. (1990 Shallit)

Verifying proof: time $(\lg n)^{3+o(1)}$.

Current project, Bernstein–Lange–Peters–Swart: Accelerate (and simplify!) verification. $(\lg n)^{3+o(1)}$, but better $o(1)$.

Standard proof structure:
elliptic curve E over $\mathbf{Z}/n$;
point $W \in E(\mathbf{Z}/n)$
of prime order $q > (n^{1/4} + 1)^2$;
recursive proof that q is prime.

Verifier checks
that $qW = 0$ in $E(\mathbf{Z}/n)$
(so $qW = 0$ in each $E(\mathbf{Z}/p)$);
that W is "stably nonzero"
(so $W \neq 0$ in each $E(\mathbf{Z}/p)$);
that $q > (n^{1/4} + 1)^2$;
and that q is prime.

Bad news, part 1:
Findable q's are close to n,
so recursion has many levels.

Bad news, part 2:
Arithmetic in $E(\mathbf{Z}/n)$ is slow!

Engineer's defn of $E(\mathbf{Z}/n)$
(e.g., 1986 Goldwasser–Kilian)
computes gcd at each step.

Bad news, part 1:
Findable q's are close to n,
so recursion has many levels.

Bad news, part 2:
Arithmetic in $E(\mathbf{Z}/n)$ is slow!

Engineer's defn of $E(\mathbf{Z}/n)$
(e.g., 1986 Goldwasser–Kilian)
computes gcd at each step.

Mathematician's defn of $E(\mathbf{Z}/n)$
(e.g., 1987 Lenstra)
computes gcd at each step.

Division-polynomial ECPP
(e.g., 2005 Morain)
uses many mults per bit.

Division-polynomial ECPP
(e.g., 2005 Morain)
uses many mults per bit.

Jacobian coordinates are
somewhat faster but still
$(9 + o(1)) \lg n$ mults, including
$(1 + o(1)) \lg n$ for multi-gcd.

Division-polynomial ECPP
(e.g., 2005 Morain)
uses many mults per bit.

Jacobian coordinates are
somewhat faster but still
$(9 + o(1)) \lg n$ mults, including
$(1 + o(1)) \lg n$ for multi-gcd.

"Montgomery ladder, $\infty \mapsto 0$"
(2006 Bernstein) reduces 9 to 8
but proof is an unholy mess.

Edwards to the rescue!

Edwards addition law for
$x^2 + y^2 = 1 + dx^2y^2$
is complete for non-square d.
(2007 Bernstein–Lange)
Can skip the multi-gcd.

$(7 + o(1)) \lg n$ mults,
with very small $o(1)$.
State of the art: 2010 Hisil.

Need correct computations in $E(\mathbf{Z}/p)$ for every prime p in n.

Is d non-square in $\mathbf{Z}/p$?

Need correct computations in $E(\mathbf{Z}/p)$ for every prime p in n.
Is d non-square in $\mathbf{Z}/p$?

Solution: Take d with Jacobi symbol -1 in $\mathbf{Z}/n$.
Must be non-square in *some* $\mathbf{Z}/p$.
Deduce $p \geq (q^{1/2} - 1)^2$.
Verify: no small primes in n.
Conclude that n is prime.

Can check larger order to reduce "small." Many optimizations.

Interlude: addition laws

1985 H. Lange–Ruppert:
$A(\overline{k})$ has a complete system
of addition laws, degree $\leq (3, 3)$.
Symmetry $\Rightarrow$ degree $\leq (2, 2)$.

"The proof is nonconstructive. . .
To determine explicitly a
complete system of addition laws
requires tedious computations
already in the easiest case
of an elliptic curve
in Weierstrass normal form."

1985 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for short Weierstrass curves.

Reduce formulas to 53 monomials
by introducing extra variables
$x_i y_j + x_j y_i$, $x_i y_j - x_j y_i$.

1987 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for long Weierstrass curves.

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3) X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4) X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1) X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2) X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6) X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1) Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6) Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6) X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6) X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2) Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2) Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1) Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1) Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1) Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1) Z_1 Z_2 + (a_3^3 + 3a_3 a_6) Z_1^2 Z_2^2.
\end{aligned}
$$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:

$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2].$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2]$.

My previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2]$.

My previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.
Actually, slide shows
$\text{Publish}(Y_3'), \text{Publish}(Z_3')$,
where Publish introduces typos.

What this means:

For all fields k,
all $\mathbf{P}^2$ Weierstrass curves
$E/k : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$,
all $P_1 = (X_1 : Y_1 : Z_1) \in E(k)$,
all $P_2 = (X_2 : Y_2 : Z_2) \in E(k)$:

$(X_3 : Y_3 : Z_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
$(X_3' : Y_3' : Z_3')$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
at most one of these is $(0 : 0 : 0)$.

2009 Bernstein–T. Lange:

For all fields k with $2 \neq 0$,
all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwards curves E/k:
$X^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2$,
all $P_1, P_2 \in E(k)$,
$P_1 = ((X_1 : Z_1), (Y_1 : T_1))$,
$P_2 = ((X_2 : Z_2), (Y_2 : T_2))$:

$(X_3 : Z_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(X_3' : Z_3')$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3 : T_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3' : T_3')$ is $y(P_1 + P_2)$ or $(0 : 0)$;
at most one of these is $(0 : 0)$.

$$X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2,$$
$$Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2,$$
$$Y_3 = Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2,$$
$$T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2,$$

$$X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1,$$
$$Z_3' = X_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,$$
$$Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1,$$
$$T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.$$

Much, much, much simpler than Lange–Ruppert, Bosma–Lenstra.

Also much easier to prove.

5. Explicit Formulae

From [5, Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1 Z_2 + X_2 Z_1}{Z_1 Z_2} - a_2, \qquad g = -(\lambda + a_1) f - \nu - a_3,$$

where

$$\lambda = \frac{Y_1 Z_2 - Y_2 Z_1}{X_1 Z_2 - X_2 Z_1} \qquad \text{and} \qquad \nu = -\frac{Y_1 X_2 - Y_2 X_1}{X_1 Z_2 - X_2 Z_1}.$$

Applying the automorphism of $E \times E$ mapping (P_1, P_2) to $(P_1, -P_2)$ we find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1 Z_2 + X_2 Z_1}{Z_1 Z_2} - a_2$$

and

$$s^*(Y/Z) = -(\kappa + a_1)\, s^*(X/Z) - \mu - a_3,$$

where

$$\kappa = \frac{Y_1 Z_2 + Y_2 Z_1 + a_1 X_2 Z_1 + a_3 Z_1 Z_2}{X_1 Z_2 - X_2 Z_1}$$

and

$$\mu = -\frac{Y_1 X_2 + Y_2 X_1 + a_1 X_1 X_2 + a_3 X_1 Z_2}{X_1 Z_2 - X_2 Z_1}.$$

The bijection of Theorem 2 maps (0:0:1) to the addition law given by $X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is found to be given by

$$\begin{aligned} X_3^{(1)} = {} & (X_1 Y_2 - X_2 Y_1)(Y_1 Z_2 + Y_2 Z_1) + (X_1 Z_2 - X_2 Z_1)\, Y_1 Y_2 \\ & + a_1 X_1 X_2 (Y_1 Z_2 - Y_2 Z_1) + a_1 (X_1 Y_2 - X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\ & - a_2 X_1 X_2 (X_1 Z_2 - X_2 Z_1) + a_3 (X_1 Y_2 - X_2 Y_1)\, Z_1 Z_2 \\ & + a_3 (X_1 Z_2 - X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\ & - a_4 (X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\ & - 3a_6 (X_1 Z_2 - X_2 Z_1)\, Z_1 Z_2, \end{aligned}$$

$$\begin{aligned}
Y_3^{(1)} = & -3X_1X_2(X_1Y_2 - X_2Y_1) \\
& - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - 2a_1(X_1Z_2 - X_2Z_1)\,Y_1Y_2 \\
& + (a_1^2 + 3a_2)\,X_1X_2(Y_1Z_2 - Y_2Z_1) \\
& - (a_1^2 + a_2)(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1a_2 - 3a_3)\,X_1X_2(X_1Z_2 - X_2Z_1) \\
& - (2a_1a_3 + a_4)(X_1Y_2 - X_2Y_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + (a_1a_4 - a_2a_3)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_3^2 + 3a_6)(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2 \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 - X_2Z_1)\,Z_1Z_2, \\
Z_3^{(1)} = & \; 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + a_1(X_1Y_2 - X_2Y_1)\,Z_1Z_2 - a_1(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) - a_3(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 - X_2Z_1)\,Z_1Z_2.
\end{aligned}$$

The corresponding exceptional divisor is $3 \cdot \Delta$, so a pair of points P_1, P_2 on E is exceptional for this addition law if and only if $P_1 = P_2$.

Multiplying the addition law just given by $s^*(Y/Z)$ we obtain the addition law corresponding to $(0:1:0)$. It reads as follows:

$$\begin{aligned}
X_3^{(2)} = & \; Y_1Y_2(X_1Y_2 + X_2Y_1) + a_1(2X_1Y_2 + X_2Y_1)\,X_2Y_1 + a_1^2X_1X_2^2Y_1 \\
& - a_2X_1X_2(X_1Y_2 + X_2Y_1) - a_1a_2X_1^2X_2^2 + a_3X_2Y_1(Y_1Z_2 + 2Y_2Z_1) \\
& + a_1a_3X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& - a_4X_1X_2(Y_1Z_2 + Y_2Z_1) - a_4(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& - a_1^2a_3X_1^2X_2Z_2 - a_1a_4X_1X_2(2X_1Z_2 + X_2Z_1) \\
& - a_2a_3X_1X_2^2Z_1 - a_3^2X_1Z_2(2Y_2Z_1 + Y_1Z_2) \\
& - 3a_6(X_1Y_2 + X_2Y_1)\,Z_1Z_2 \\
& - 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) - a_1a_3^2X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - 3a_1a_6X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_3a_4(X_1Z_2 - 2X_2Z_1)\,X_2Z_1 \\
& - (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(Y_1Z_2 + Y_2Z_1)\,Z_1Z_2 \\
& - (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1a_2a_6 - a_1a_4^2)\,X_1Z_1Z_2^2 \\
& - a_3^3(X_1Z_2 + X_2Z_1)\,Z_1Z_2 - 3a_3a_6(X_1Z_2 + 2X_2Z_1)\,Z_1Z_2 \\
& - (a_1^2a_3a_6 - a_1a_3^2a_4 + a_2a_3^3 + 4a_2a_3a_6 - a_3a_4^2)\,Z_1^2Z_2^2,
\end{aligned}$$

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3) X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4) X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1) X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2) X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6) X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1) Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6) Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6) X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6) X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2) Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2) Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1) Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1) Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1) Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1) Z_1 Z_2 + (a_3^3 + 3a_3 a_6) Z_1^2 Z_2^2.
\end{aligned}
$$

1987 Lenstra: Use Lange–Ruppert complete system of addition laws to computationally define $E(R)$ for more general rings R.

Define $\mathbf{P}^2(R) = \{(X : Y : Z) : X, Y, Z \in R;\ XR + YR + ZR = R\}$ where $(X : Y : Z)$ is the module $\{(\lambda X, \lambda Y, \lambda Z) : \lambda \in R\}$.

Define $E(R) = \{(X : Y : Z) \in \mathbf{P}^2(R) : Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3\}$.

To define (and compute) sum $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$:

Consider (and compute) Lange–Ruppert $(X_3 : Y_3 : Z_3)$, $(X_3' : Y_3' : Z_3')$, $(X_3'' : Y_3'' : Z_3'')$.

Add these R-modules:

$$\{ \quad (\lambda X_3, \lambda Y_3, \lambda Z_3) + (\lambda' X_3', \lambda' Y_3', \lambda' Z_3') + (\lambda'' X_3'', \lambda'' Y_3'', \lambda'' Z_3'') : \lambda, \lambda', \lambda'' \in R\}.$$

Express as $(X : Y : Z)$; assume trivial class group of R.

Factoring integers into primes

1993 Atkin–Morain "Finding suitable curves for the elliptic curve method of factorization":

"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."

2010 Bernstein–Birkner–Lange:

Better to switch to a family of twisted Edwards curves
$-x^2 + y^2 = 1 + dx^2y^2$
with $\mathbf{Z}/6$ torsion.

Expected benefit:
These curves are very fast.

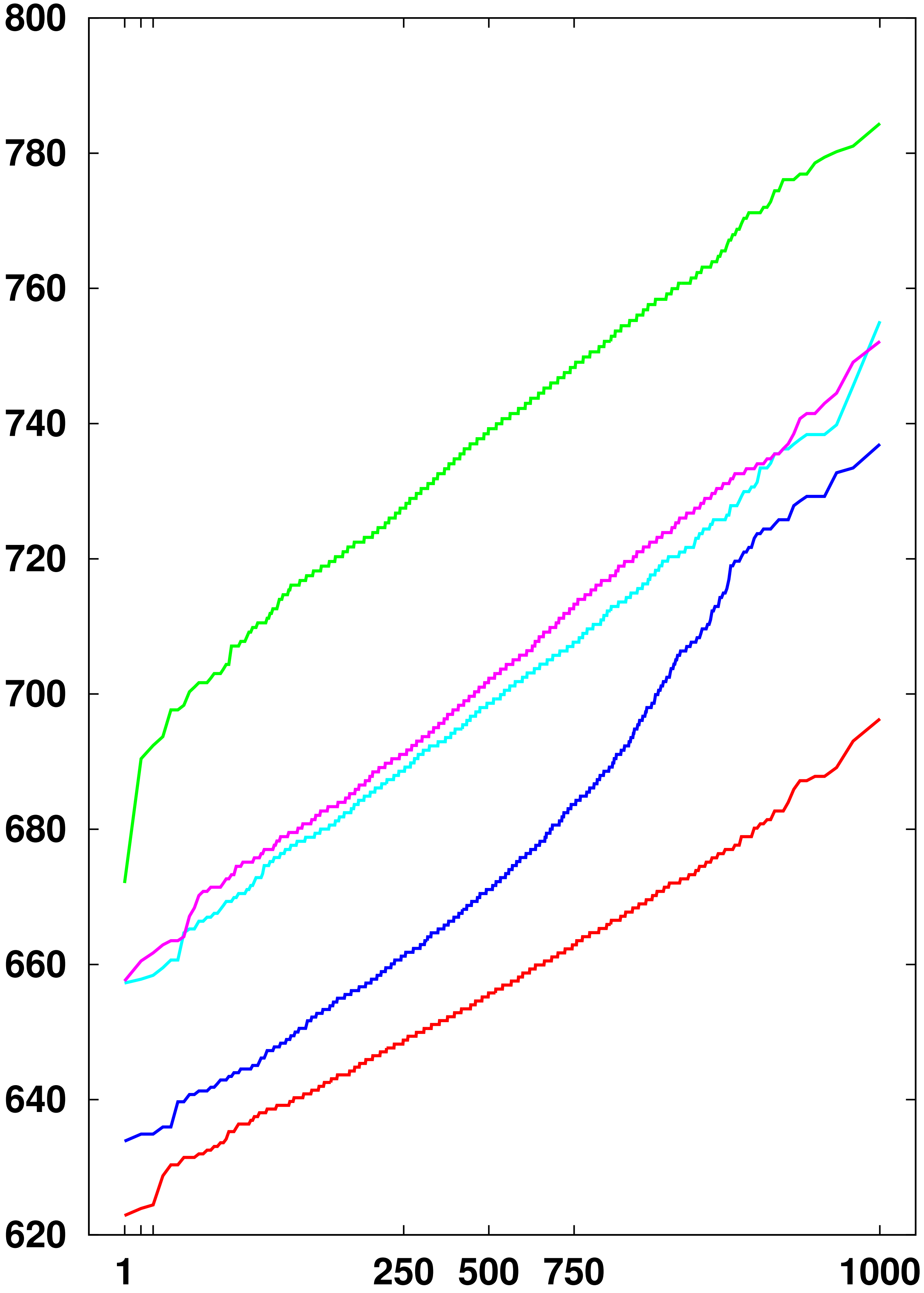
2010 Bernstein–Birkner–Lange:

Better to switch to a family of twisted Edwards curves
$-x^2 + y^2 = 1 + dx^2y^2$
with $\mathbf{Z}/6$ torsion.

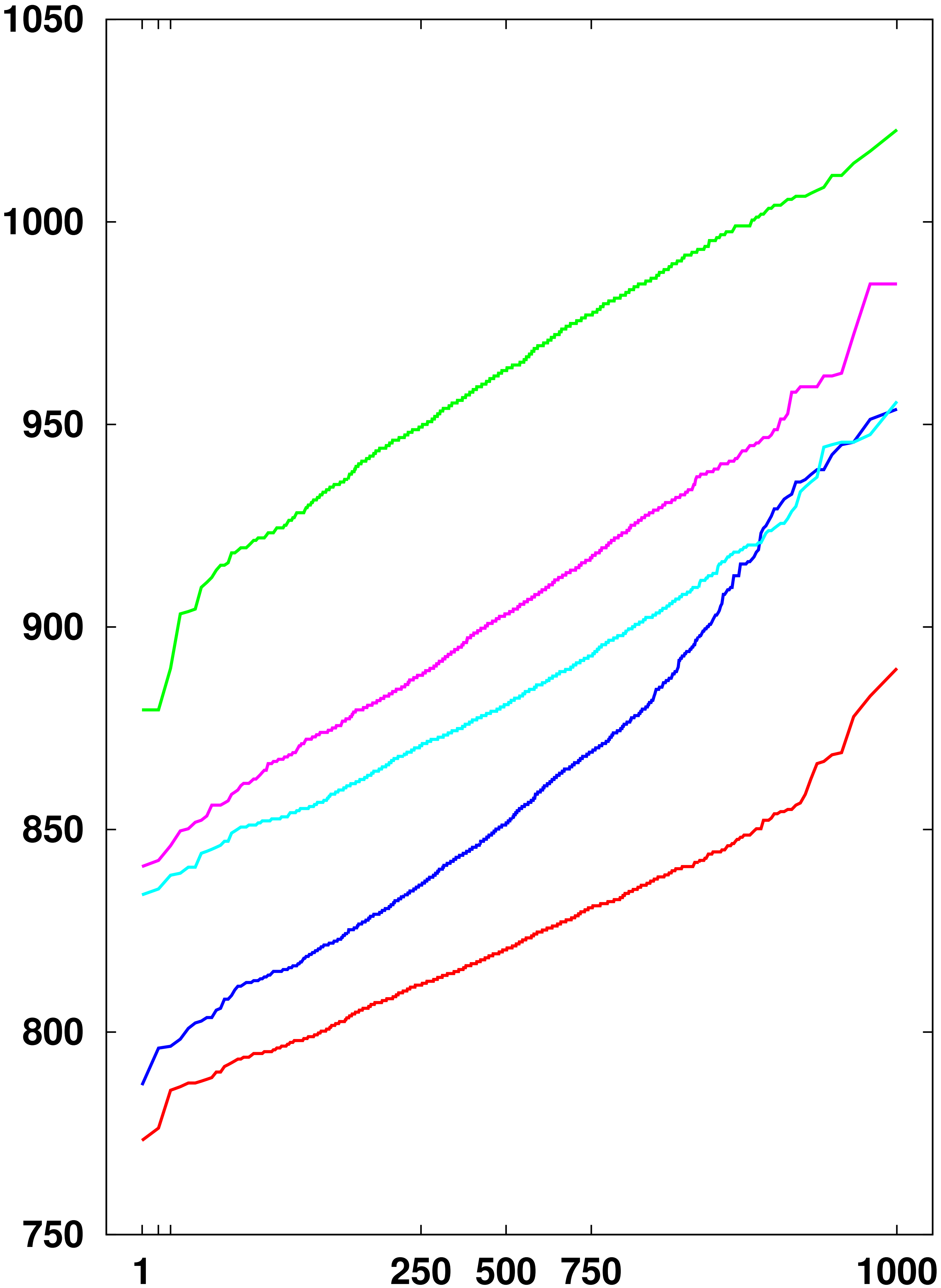
Expected benefit:
These curves are very fast.

Unexpected benefit:
These curves find *more* primes despite smaller torsion.

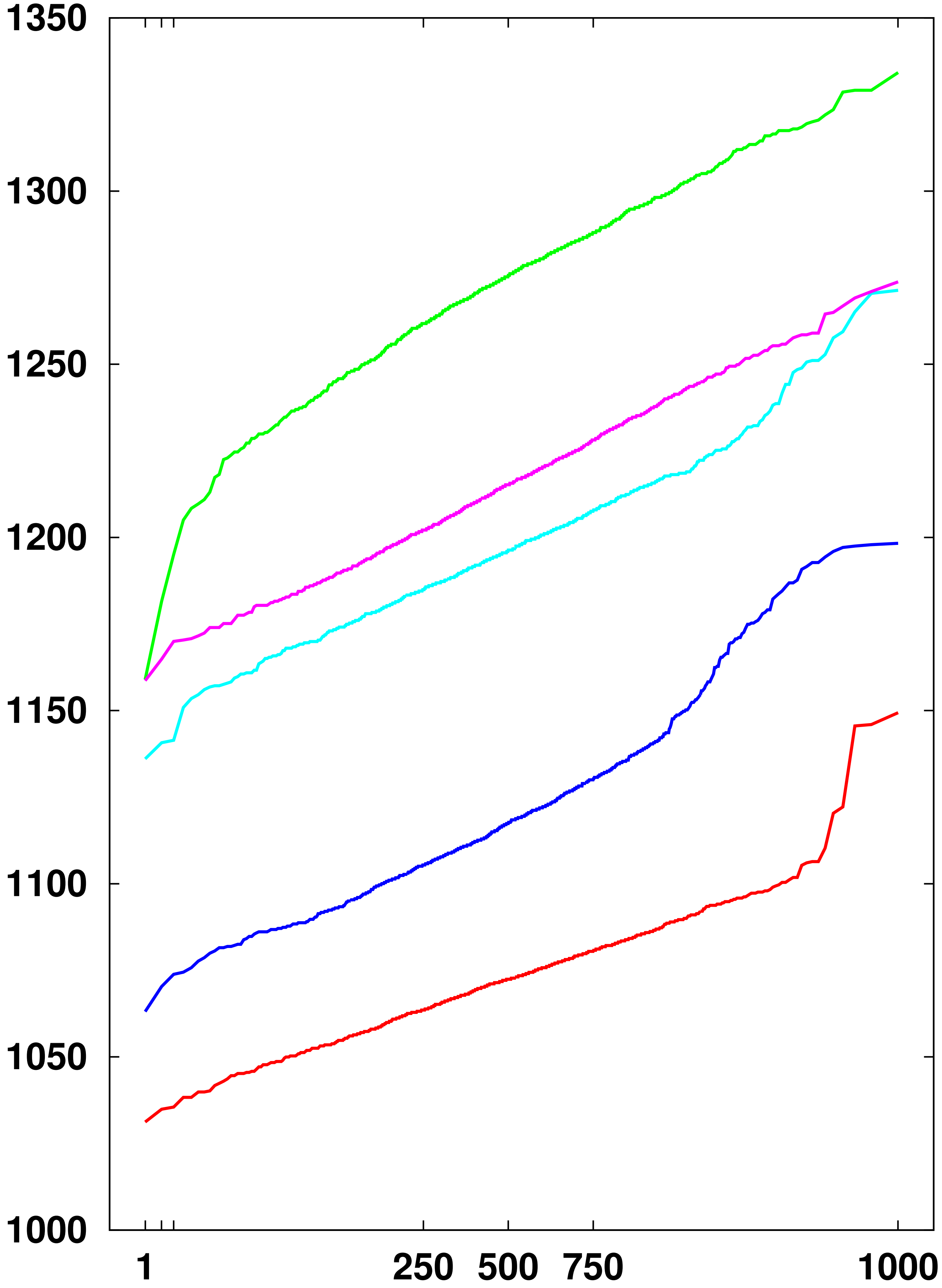
Mulmods/15-bit prime found:



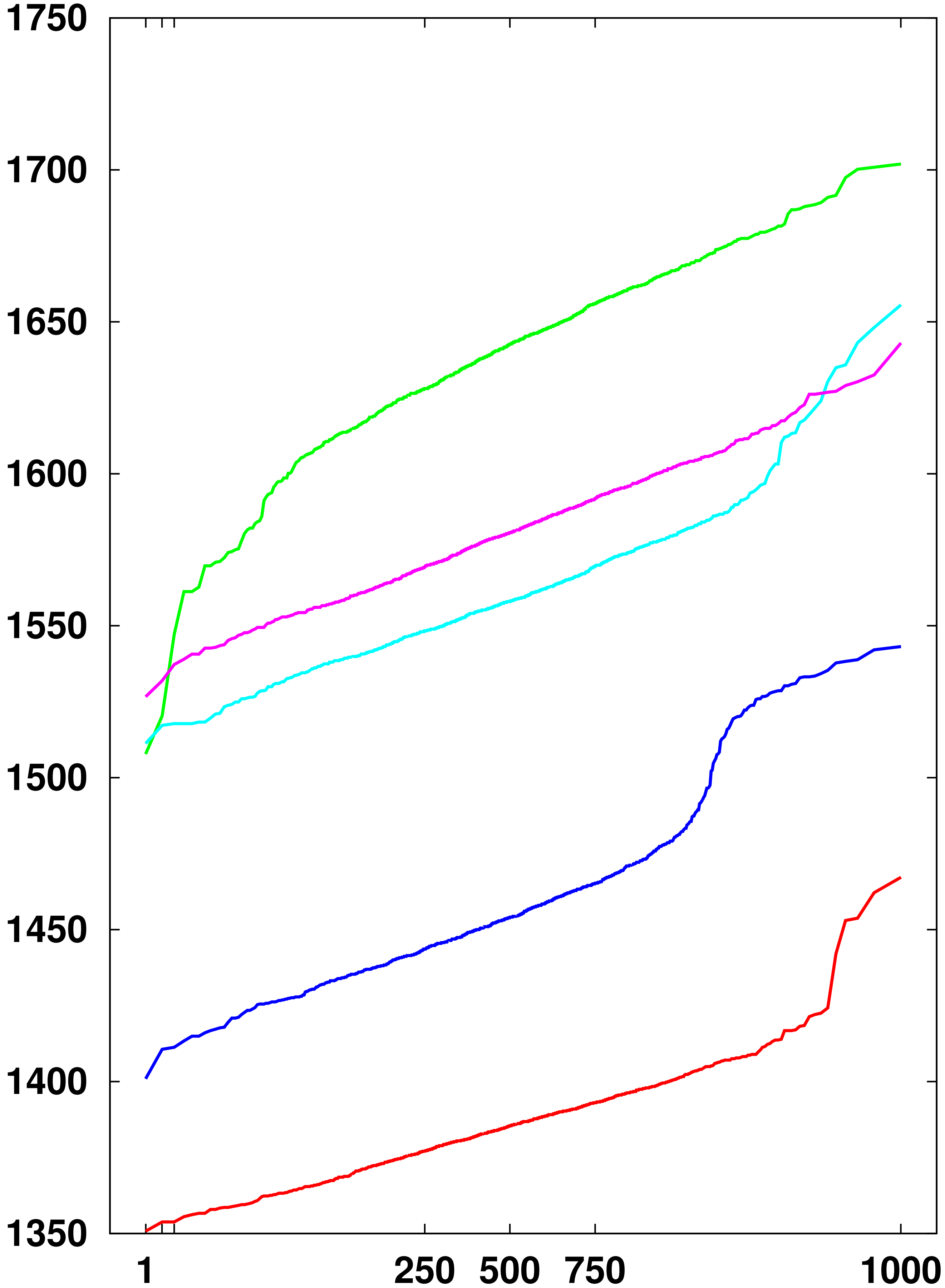
Mulmods/16-bit prime found:



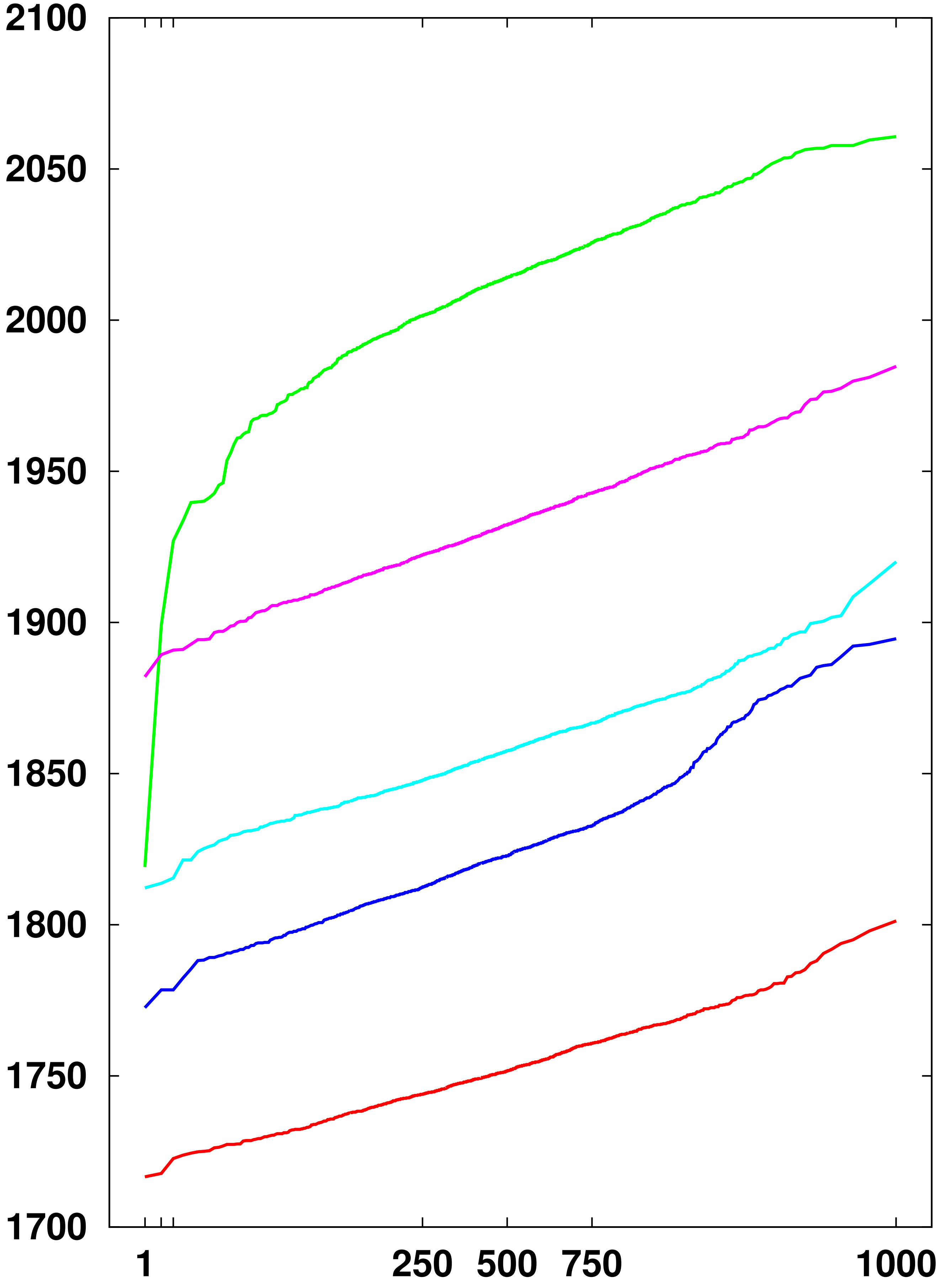
Mulmods/17-bit prime found:



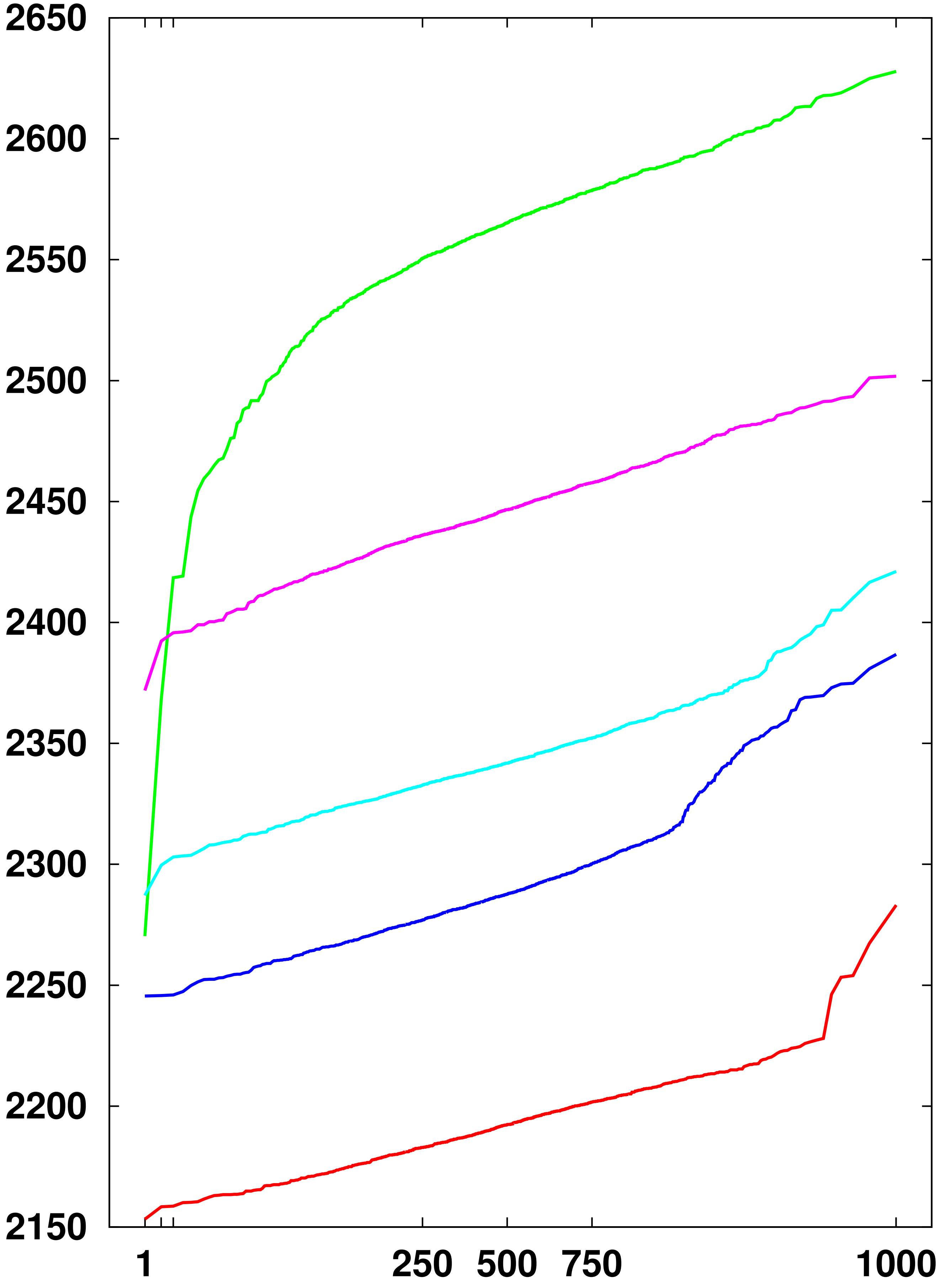
Mulmods/18-bit prime found:



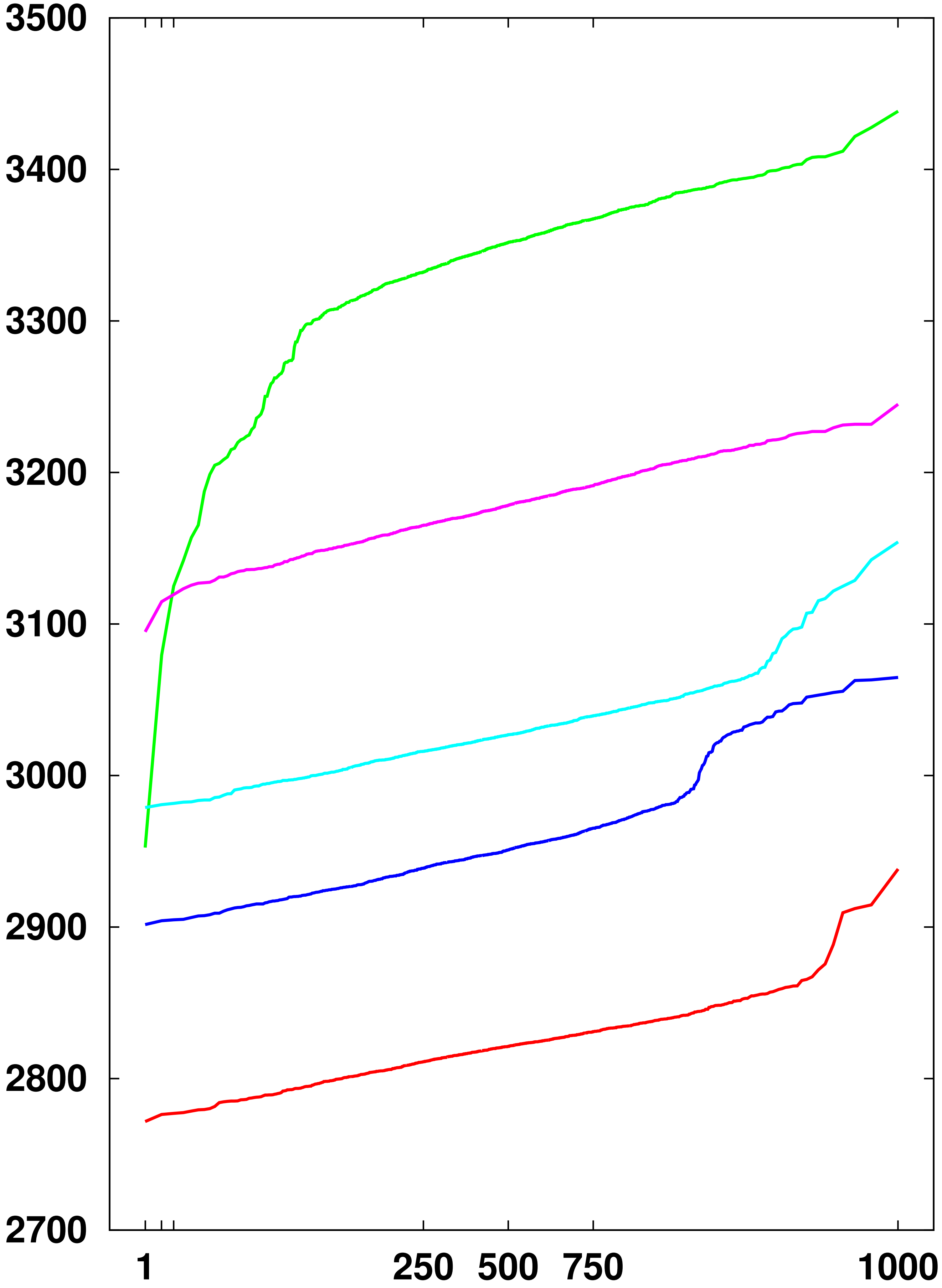
Mulmods/19-bit prime found:



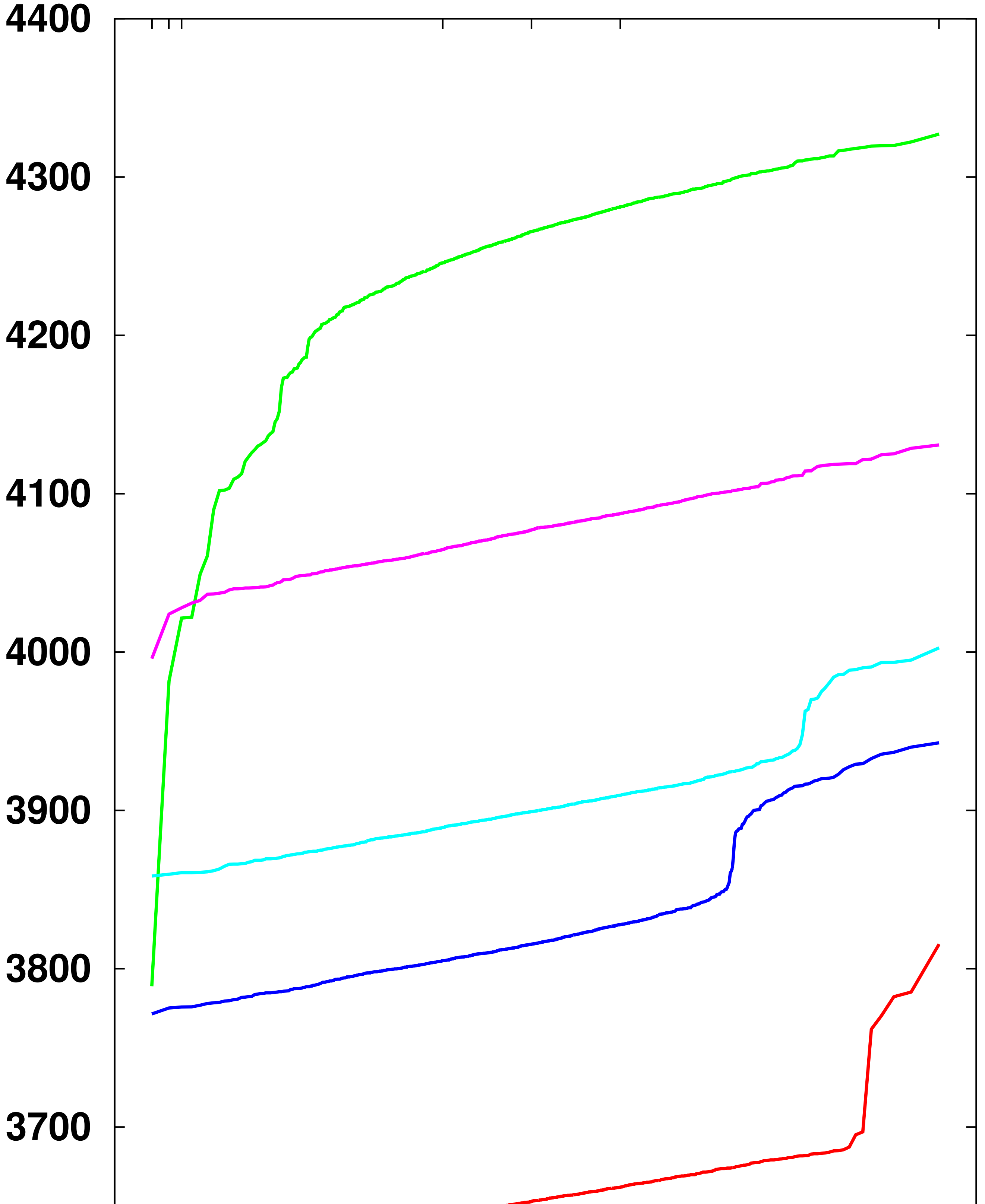
Mulmods/20-bit prime found:



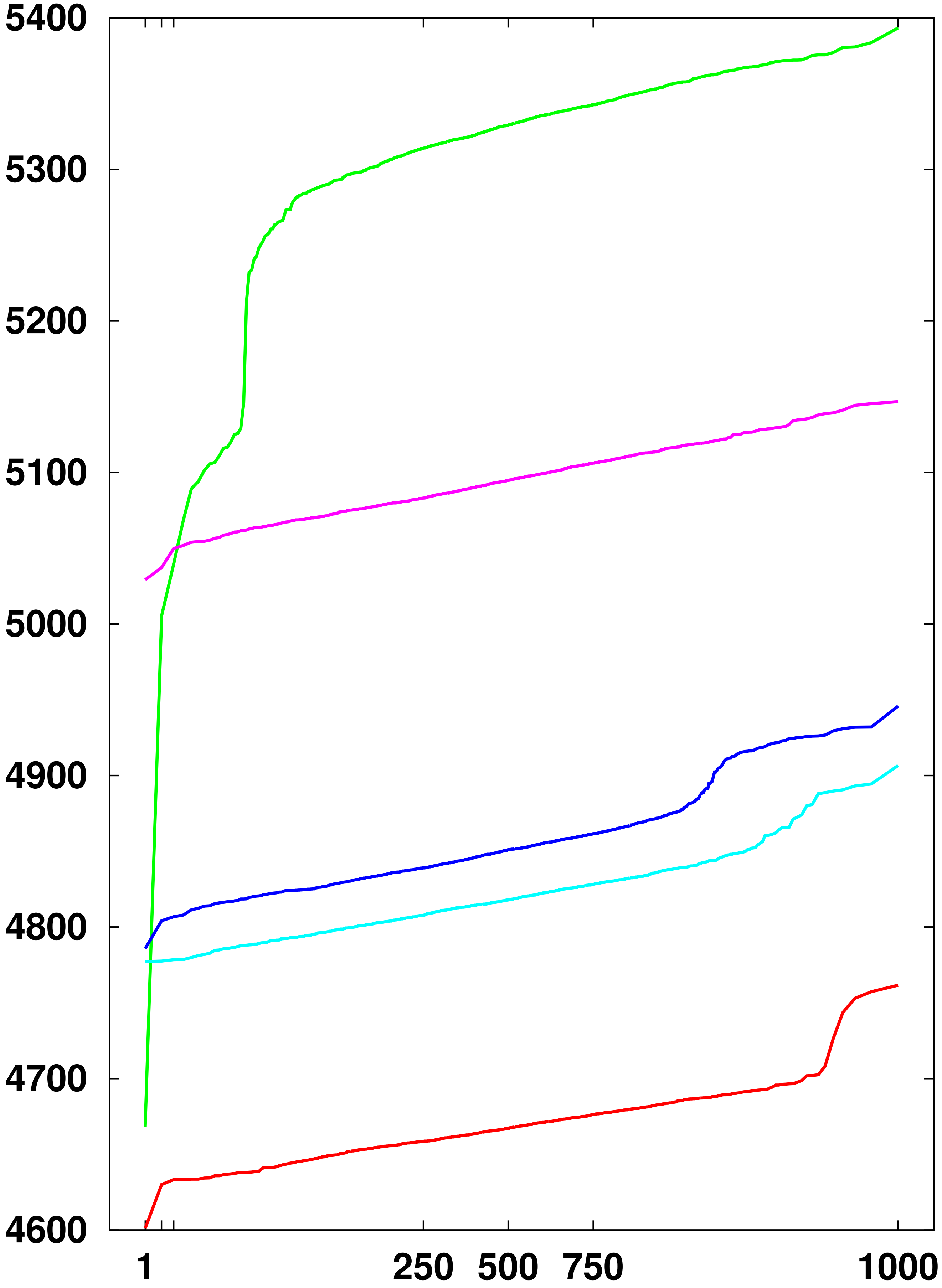
Mulmods/21-bit prime found:



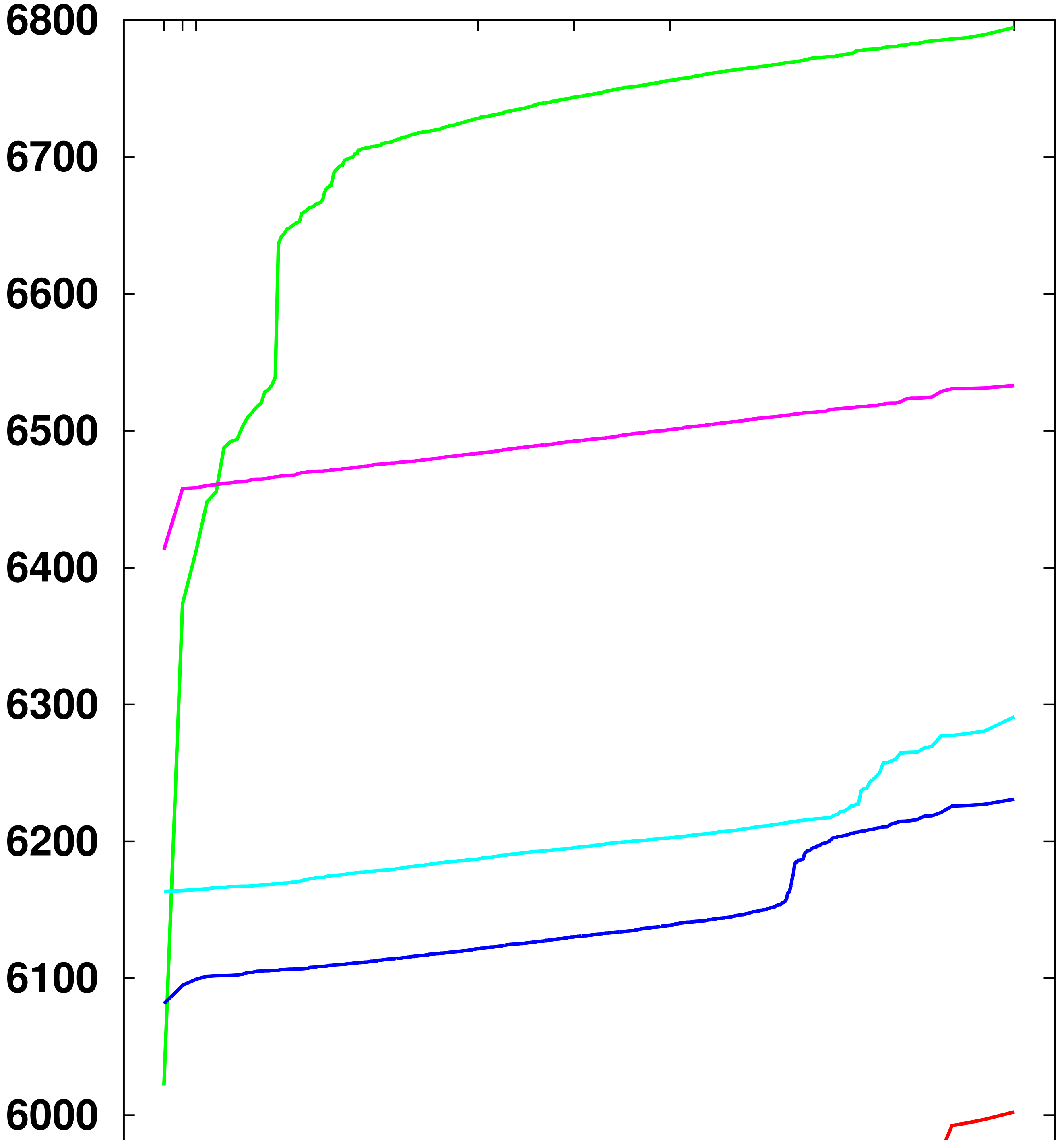
Mulmods/22-bit prime found:



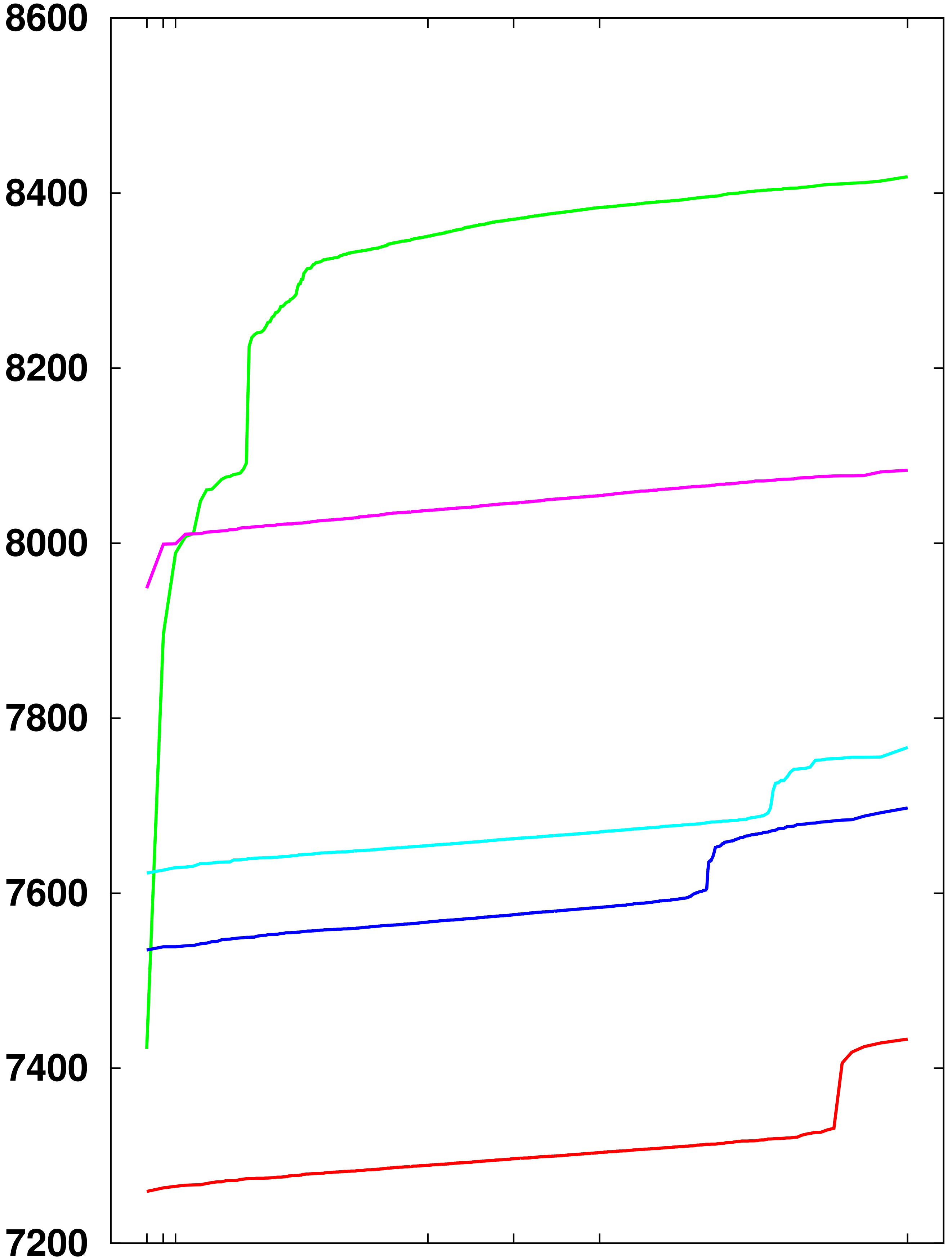
Mulmods/23-bit prime found:



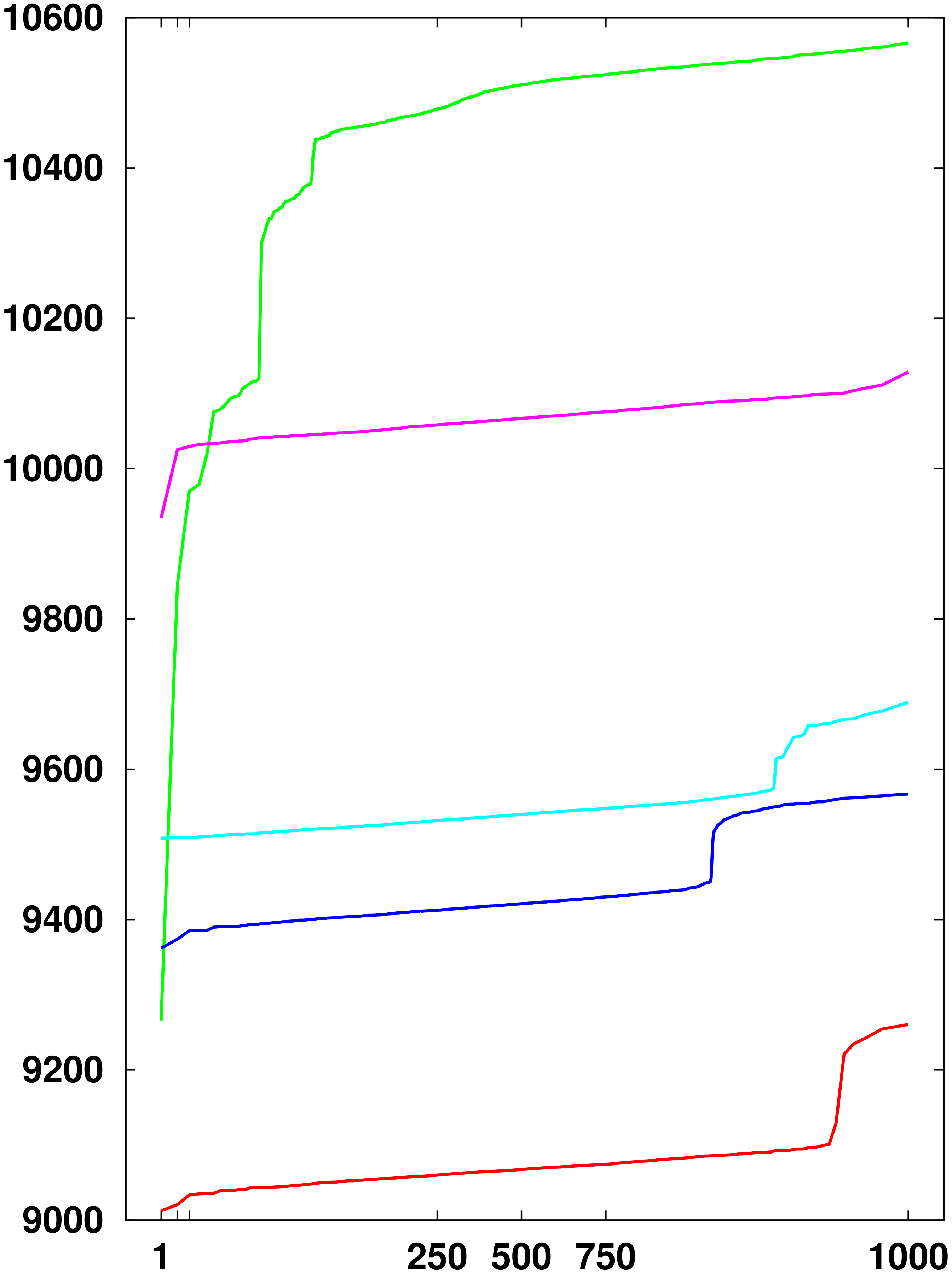
Mulmods/24-bit prime found:



Mulmods/25-bit prime found:



Mulmods/26-bit prime found:



Enumerating small primes

Sieve of Eratosthenes
enumerates products ij;
i.e., enumerates values $-x^2 + y^2$;
i.e., enumerates norms of
elements $y + xt$ of $\mathbf{Z}[t]/(t^2 - 1)$.

Determines primality of n
by counting representations
of n as such norms.

Fast computation if batched
across all $n \in \{1, 2, \ldots, H\}$.

Sieve of Atkin enumerates
$4x^2 + y^2$ for $n \in 1 + 4\mathbf{Z}$,
$3x^2 + y^2$ for $n \in 7 + 12\mathbf{Z}$,
$3x^2 - y^2$ for $n \in 11 + 12\mathbf{Z}$.

Fundamentally more efficient
than sieve of Eratosthenes:
$\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{3})$ are
smaller than "$\mathbf{Q}(\sqrt{1})$" $= \mathbf{Q} \times \mathbf{Q}$.

(Can we determine primality
by enumerating points
on elliptic curves?)

Consequence: Can print the primes in $\{1, 2, \ldots, H\}$, in order, using $\Theta(H/\lg\lg H)$ ops on $\Theta(\lg H)$-bit integers and $H^{1/2+o(1)}$ bits of memory.

Galway: $H^{1/3+o(1)}$.

$H^{1/4+o(1)}$ should be doable with LLL, Coppersmith, etc.

But is this a meaningful game?

Radeon 5970 graphics card:
2 320 000 000 000 mults/second.
$600; consumes 300 watts.

Can run at even higher speed
using more power, more fans:

Need better algorithms
with massive parallelism,
very little communication.

Good example, 2006 Sorenson
"The pseudosquares prime sieve":

$\Theta(H \lg H)$ operations,
$\Theta((\lg H)^2)$ bits of memory,
assuming standard conjectures.
Output is always correct:
primes in $\{1, 2, \ldots, H\}$.