Edwards curves

D. J. Bernstein
University of Illinois at Chicago

The $p - 1$ factorization method

$2^{232792560} - 1$ 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.

These divisors include
70 of the 168 primes $\le 10^3$;
156 of the 1229 primes $\le 10^4$;
296 of the 9592 primes $\le 10^5$;
470 of the 78498 primes $\le 10^6$;
etc.

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

Many ways for this to happen:
232792560 has 960 divisors.

Why so many?
Answer: 232792560
$= \text{lcm}\{1, 2, 3, 4, 5, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$

Can compute $2^{232792560} - 1$
using 41 ring operations.
(Side note: 41 is not minimal.)

Ring operation: 0, 1, $+$, $-$, $\cdot$.

This computation: 1; $2 = 1 + 1$;
$2^2 = 2 \cdot 2$; $2^3 = 2^2 \cdot 2$; $2^6 = 2^3 \cdot 2^3$;
$2^{12} = 2^6 \cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54};
2^{55}; 2^{110}; 2^{111}; 2^{222}; 2^{444}; 2^{888}; 2^{1776};
2^{3552}; 2^{7104}; 2^{14208}; 2^{28416}; 2^{28417};
2^{56834}; 2^{113668}; 2^{227336}; 2^{454672}; 2^{909344};
2^{909345}; $2^{1818690}$; $2^{1818691}$; $2^{3637382}$;
$2^{3637383}$; $2^{7274766}$; $2^{7274767}$; $2^{14549534}$;
$2^{14549535}$; $2^{29099070}$; $2^{58198140}$;
$2^{116396280}$; $2^{232792560}$; $2^{232792560} - 1$.

Given positive integer n,
can compute $2^{232792560} - 1 \bmod n$
using 41 operations in $\mathbf{Z}/n$.
Notation: $a \bmod b = a - b \lfloor a/b \rfloor$.

e.g. $n = 8597231219$: ...

$$2^{27} \bmod n = 134217728;$$
$$2^{54} \bmod n = 134217728^2 \bmod n$$
$$= 935663516;$$
$$2^{55} \bmod n = 1871327032;$$
$$2^{110} \bmod n = 1871327032^2 \bmod n$$
$$= 1458876811; \ldots;$$
$$2^{232792560} - 1 \bmod n = 5626089344.$$

Easy extra computation (Euclid):
$\gcd\{5626089344, n\} = 991$.

This $p - 1$ method (1974 Pollard) quickly factored $n = 8597231219$. Main work: 27 squarings mod n.

Could instead have checked n's divisibility by $2, 3, 5, \ldots$. The 167th trial division would have found divisor 991.

Not clear which method is better. Dividing by small p is faster than squaring mod n. The $p - 1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up to larger exponent
$\operatorname{lcm}\{1, 2, 3, 4, 5, \ldots, 100\}$:
using 136 squarings mod n
find 2317 of the primes $\leq 10^5$.

Is a squaring mod n
faster than 17 trial divisions?

Or $\operatorname{lcm}\{1, 2, 3, 4, 5, \ldots, 1000\}$:
using 1438 squarings mod n
find 180121 of the primes $\leq 10^7$.

Is a squaring mod n
faster than 125 trial divisions?

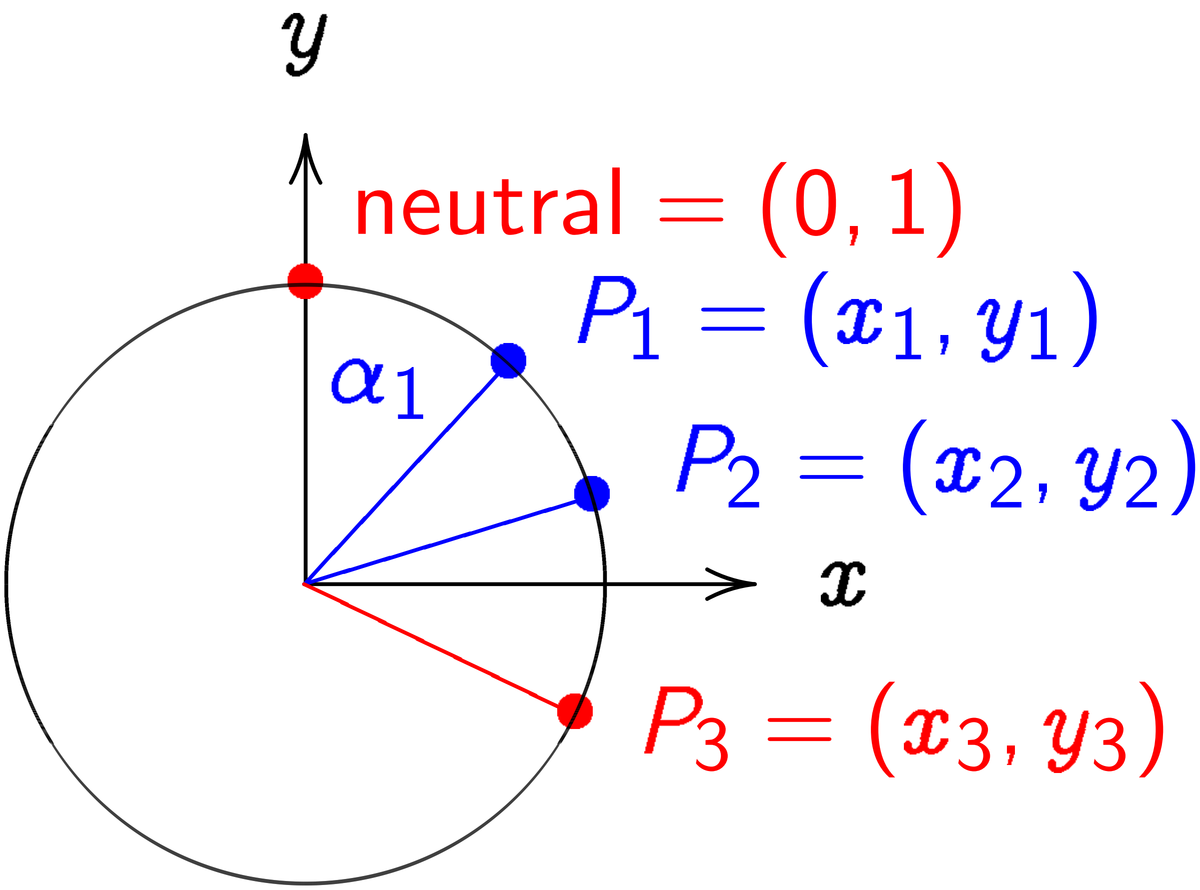
Plausible conjecture: if S is $\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log\log H}$ then $p-1$ divides $\text{lcm}\{1,2,\ldots,S\}$ for $H/S^{1+o(1)}$ primes $p \le H$.
Same if $p-1$ is replaced by order of 2 in $\mathbf{F}_p^*$.

So uniform random prime $p \le H$ divides $2^{\text{lcm}\{1,2,\ldots,S\}}-1$ with probability $1/S^{1+o(1)}$.

$(1.4\ldots+o(1))S$ squarings mod n produce $2^{\text{lcm}\{1,2,\ldots,S\}}-1 \bmod n$.

Similar time spent on trial division finds far fewer primes for large H.

Interlude: Addition on a clock



$x^2 + y^2 = 1$, parametrized by

$x = \sin\alpha, \quad y = \cos\alpha.$

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$.

Examples of clock addition:

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

Many equivalent formulations.

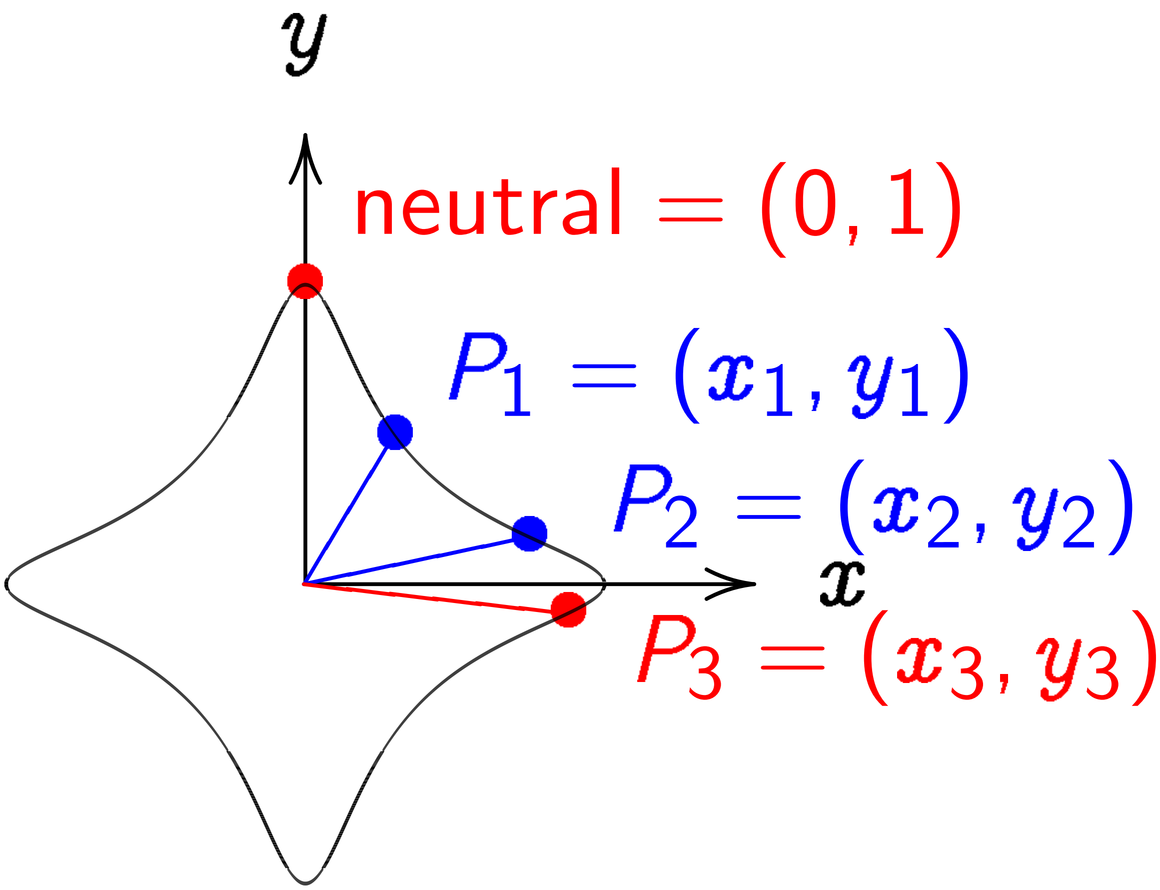
e.g. Clock addition represents multiplication of norm-1 elements of $\mathbf{C} = \mathbf{R}[i]/(i^2 + 1)$.

$(x, y) \mapsto y + ix$;

$(4/5 + 3i/5)^3$

$\quad = -44/125 + 117i/125.$

Addition on an Edwards curve



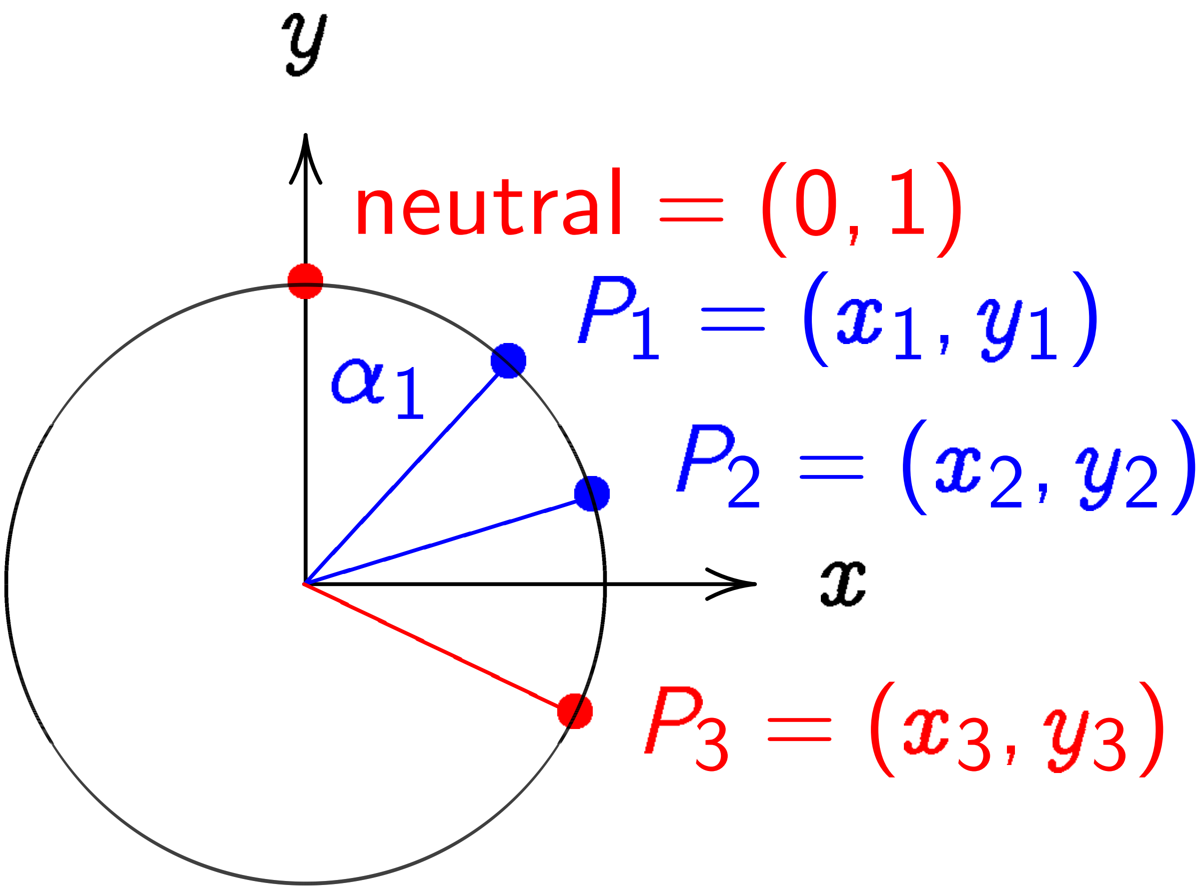
$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2) is

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$

$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The clock again, for comparison:



$x^2 + y^2 = 1.$

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1 y_2 + y_1 x_2,$
$\ y_1 y_2 - x_1 x_2).$

The $p+1$ factorization method

(1982 Williams)

Define $(X, Y) \in \mathbf{Q} \times \mathbf{Q}$ as the 232792560th multiple of $(3/5, 4/5)$ in the group $\text{Clock}(\mathbf{Q})$.

The integer $5^{232792560} X$
is divisible by
82 of the primes $\leq 10^3$;
223 of the primes $\leq 10^4$;
455 of the primes $\leq 10^5$;
720 of the primes $\leq 10^6$;
etc.

Given an integer n,
compute $5^{232792560}X \bmod n$
and compute gcd with n,
hoping to factor n.

Many p's not found by $\mathbf{F}_p^*$
are found by Clock($\mathbf{F}_p$).

If -1 is not a square mod p
and $p+1$ divides 232792560
then $5^{232792560}X \bmod p = 0$.

Proof: $\mathbf{F}_p[i]/(i^2+1)$ is a field
so $(p+1)(3/5, 4/5) = (0, 1)$
in the group Clock($\mathbf{F}_p$)
so $232792560(3/5, 4/5) = (0, 1)$.

ECM, the elliptic-curve method

(1987 Lenstra)

Analogous method using the elliptic curve $y^2 = x^3 - 3x + 10$ finds many new primes.

Analogous method using the elliptic curve $y^2 = x^3 - 3x + 11$ finds many new primes.

Analogous method using the elliptic curve $y^2 = x^3 - 3x + 12$ finds many new primes.

... As many curves as you want!

Good news: *All* primes $\le H$
seem to be found after a
reasonable number of curves.

Plausible conjecture: if S is
$\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H\log\log H}$
then, for each prime $p \le H$,
a uniform random curve mod p
has chance $\ge 1/S^{1+o(1)}$ to find p.

If a curve fails, try another.
Find p using, on average,
$\le S^{1+o(1)}$ curves;
i.e., $\le S^{2+o(1)}$ squarings.
Time subexponential in H.

Primality proofs

If $2^{n-1} = 1$ in $\mathbf{Z}/n$, and $n - 1$ has a prime divisor $q > \sqrt{n} - 1$ with $2^{(n-1)/q} - 1$ in $(\mathbf{Z}/n)^*$, then n is prime. (1876 Lucas, 1914 Pocklington, 1927 Lehmer)

What if we don't know a big prime q dividing $n - 1$?

Replace multiplicative group by random elliptic-curve group. (1986 Goldwasser/Kilian; point counting: 1985 Schoof)

Use complex-multiplication curves; faster point counting. (1988 Atkin; special: 1985 Bosma, 1986 Chudnovsky–Chudnovsky)

Conjectured time $\le (\lg n)^{4+o(1)}$ for fastECPP (1990 Shallit) to find certificate proving n prime. *Proven* time $\le (\lg n)^{3+o(1)}$ to verify certificate.

Newer methods prove primality in *proven* time $\le (\lg n)^{6+o(1)}$ (2002 Agrawal–Kayal–Saxena; 2005 Lenstra–Pomerance) but fastECPP is *conjecturally* faster.

Public-key cryptography

(1976 Diffie–Hellman)

Standardize $p = 2^{262} - 5081$.

Alice's secret key a

Bob's secret key b

Alice's public key $4^a \bmod p$

Bob's public key $4^b \bmod p$

{Alice, Bob}'s shared secret $4^{ab} \bmod p$ = {Bob, Alice}'s shared secret $4^{ab} \bmod p$

Bad news: Attacker can find a and b by "index calculus."

To protect against this attack, replace $2^{262} - 5081$ with a much larger prime. *Much* slower arithmetic.

Alternative (1985 Miller, independently 1987 Koblitz): Elliptic-curve cryptography! Replace the multiplicative group with an elliptic-curve group. *Somewhat* slower arithmetic.

What is an elliptic curve?

Fix an odd prime p.
Fix $a, b \in \mathbf{F}_p$ with $4a^3 + 27b^2 \neq 0$.

Well-known fact:
The points of the "elliptic curve"
$E : y^2 = x^3 + ax + b$ over $\mathbf{F}_p$
form a commutative group $E(\mathbf{F}_p)$.

"So the set of points is
$\{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p :$
$\quad y^2 = x^3 + ax + b\}$?"

Not exactly! The set is
$\{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p :$
$\quad y^2 = x^3 + ax + b\} \cup \{\infty\}$.

To add $(x_1, y_1), (x_2, y_2) \in E(\mathbf{F}_p)$:

Define $x_3 = \lambda^2 - x_1 - x_2$
and $y_3 = \lambda(x_1 - x_3) - y_1$
where $\lambda = (y_2 - y_1)/(x_2 - x_1)$.
Then $(x_3, y_3) \in E(\mathbf{F}_p)$.

Geometric interpretation:
$(x_1, y_1), (x_2, y_2), (x_3, -y_3)$ are
on the curve $y^2 = x^3 + ax + b$
and on a line;
$(x_3, y_3), (x_3, -y_3)$ are
on a vertical line.

"So that's the group law?
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$?"

Not exactly! Definition of λ assumes that $x_2 \neq x_1$.

To add $(x_1, y_1), (x_1, y_1) \in E(\mathbf{F}_p)$:

Define $x_3 = \lambda^2 - x_1 - x_2$
and $y_3 = \lambda(x_1 - x_3) - y_1$
where $\lambda = (3x_1^2 + a)/2y_1$.
Then $(x_3, y_3) \in E(\mathbf{F}_p)$.

Geometric interpretation:
The curve's tangent line at (x_1, y_1) passes through $(x_3, -y_3)$.

"So that's the group law?
One special case for doubling?"

Not exactly! More exceptions:
e.g., y_1 could be 0.

Six cases overall: $\infty + \infty = \infty$;
$\infty + (x_2, y_2) = (x_2, y_2)$;
$(x_1, y_1) + \infty = (x_1, y_1)$;
$(x_1, y_1) + (x_1, -y_1) = \infty$;
for $y_1 \neq 0$, $(x_1, y_1) + (x_1, y_1) =$
(x_3, y_3) with $x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = \lambda(x_1 - x_3) - y_1$,
$\lambda = (3x_1^2 + a)/2y_1$;
for $x_1 \neq x_2$, $(x_1, y_1) + (x_2, y_2) =$
(x_3, y_3) with $x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = \lambda(x_1 - x_3) - y_1$,
$\lambda = (y_2 - y_1)/(x_2 - x_1)$.

$E(\mathbf{F}_p)$ is a commutative group:

Has neutral element ∞, and $-$:
$-\infty = \infty$; $-(x, y) = (x, -y)$.

Commutativity: $P + Q = Q + P$.

Associativity:
$(P + Q) + R = P + (Q + R)$.
Straightforward but tedious:
use a computer-algebra system
to check each possible case.
Or relate each $P + Q$ case
to "ideal-class product."
Many other proofs,
but can't escape case analysis.

Do we need six cases? No!

Can cover $E \times E$
using three (open) addition laws.
(1985 H. Lange–Ruppert)

How about just *one* law
that covers $E \times E$?
One complete addition law?

Bad news: “Theorem 1.
The smallest cardinality of a
complete system of addition laws
on E equals two.”
(1995 Bosma–Lenstra)

Edwards curves

Fix an odd prime p.

Fix non-square $d \in \mathbf{F}_p$.

$$\{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

“What if denominators are 0?”

Answer: They aren’t!
If $x_1^2 + y_1^2 = 1 + dx_1^2 y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2 y_2^2$
then $dx_1 x_2 y_1 y_2$ can’t be ± 1.

Outline of proof:
If $(dx_1 x_2 y_1 y_2)^2 = 1$ then
curve equation implies
$(x_1 + dx_1 x_2 y_1 y_2 y_1)^2 =$
$dx_1^2 y_1^2 (x_2 + y_2)^2$.
Conclude that d is a square.
But d is not a square! Q.E.D.

Fact: $x^2 + y^2 = 1 + dx^2y^2$
is birationally equivalent
to an elliptic curve E with
$j(E) = 16(1+14d+d^2)^3/d(1-d)^4$.
The groups are isomorphic.

Can simplify and accelerate
elliptic-curve factorization,
elliptic-curve primality proving,
elliptic-curve cryptography
by switching to Edwards curves.

In factorization,
don't mind denominators being 0,
so also allow square d.

What about Bosma–Lenstra?

Recall "Theorem 1.
The smallest cardinality of a complete system of addition laws on E equals two."

"Complete" in the theorem means "covers $E(\overline{\mathbf{F}_p}) \times E(\overline{\mathbf{F}_p})$"; $\overline{\mathbf{F}_p}$ is the algebraic closure of $\mathbf{F}_p$.

The Edwards addition law has exceptions defined over $\overline{\mathbf{F}_p}$, but no exceptions defined over $\mathbf{F}_p$.
Critical (but not sufficient!): all points at ∞ on curve are singular and blow up irrationally.

Historical notes
on the addition law:

1761 Euler, 1866 Gauss:
$d = -1$ over field with $\sqrt[4]{-1}$.
"The lemniscatic elliptic curve."

2007 Edwards: any 4th power d.
Theorem: have now obtained
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–T. Lange:
general d; proof of
completeness for non-square d;
new elliptic-curve speed records!

Faster adds using $(Z/X, Z/Y)$,
"inverted Edwards coordinates."
Also built a computer-verified
"Explicit-Formulas Database."
(2007 Bernstein–Lange)

First software implementation:
new speed records for ECM!
Also found better ECM curves:
smaller curves with large torsion.
(2008 B.–Birkner–L.–Peters)

Twists and isogenies bring same
speeds to more curves over $\mathbf{F}_p$.
(2008 B.–Birkner–Joye–L.–Peters)

Current project (B.–L.):
for *every* elliptic curve E,
find complete addition law for E
with best possible speeds.

First step:
Found fast complete addition law
for "binary Edwards curves"

$$d_1(x+y)+d_2(x^2+y^2) \\ = (x+x^2)(y+y^2).$$

If $m \geq 3$ then these cover all
ordinary elliptic curves over $\mathbf{F}_{2^m}$.
(2008 B.–L.–Rezaeian Farashahi)

Last slide: Advertisement

ECC 2008: 12th Workshop on Elliptic-Curve Cryptography.

22–24 September 2008, Trianon Zalen, Utrecht (on the Oudegracht!).

http://www.hyperelliptic.org/tanja/conf/ECC08/

Also ECC summer school: 15–19 September 2008, Technische Universiteit Eindhoven.