Faster arithmetic on elliptic curves – blessing to ECC, harm to RSA

Tanja Lange

Coding Theory and Cryptology

EIPSI

Department of Mathematics and Computer Science

tanja@hyperelliptic.org

22.04.2008

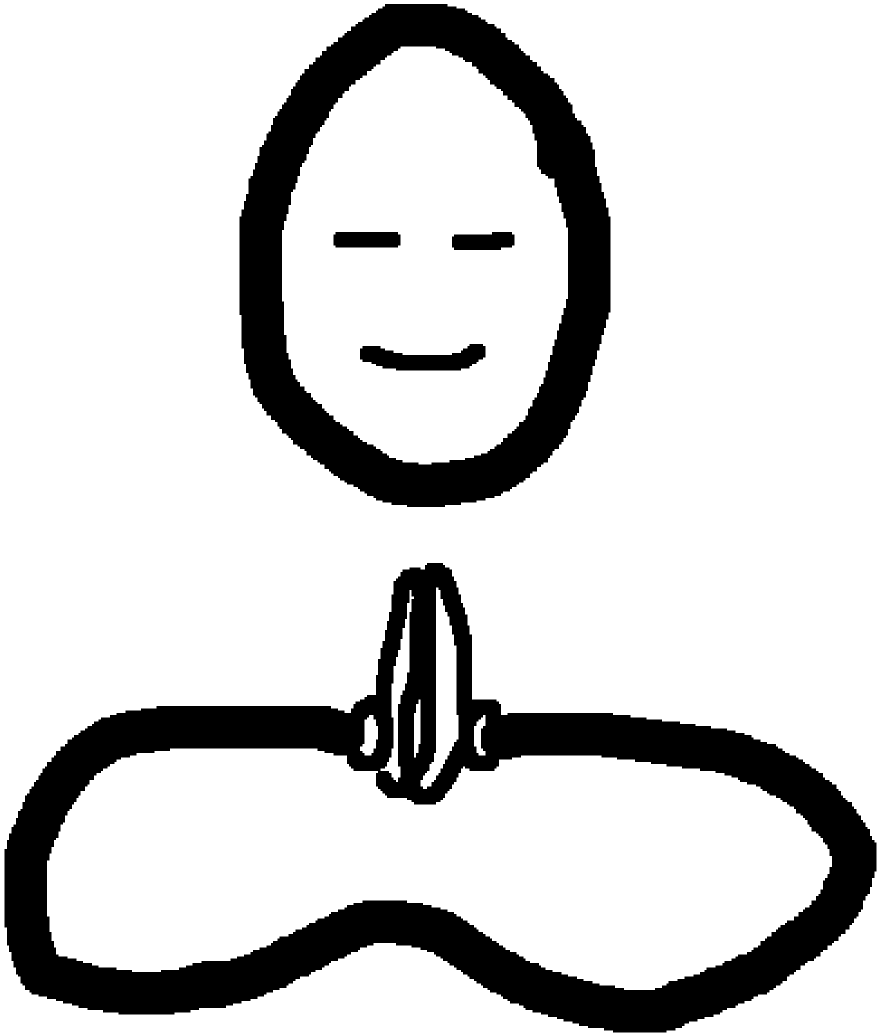
It all started with the fight between elliptic and hyperelliptic curves . . .

To face the challenge, to take the competition to a completely new level . . .

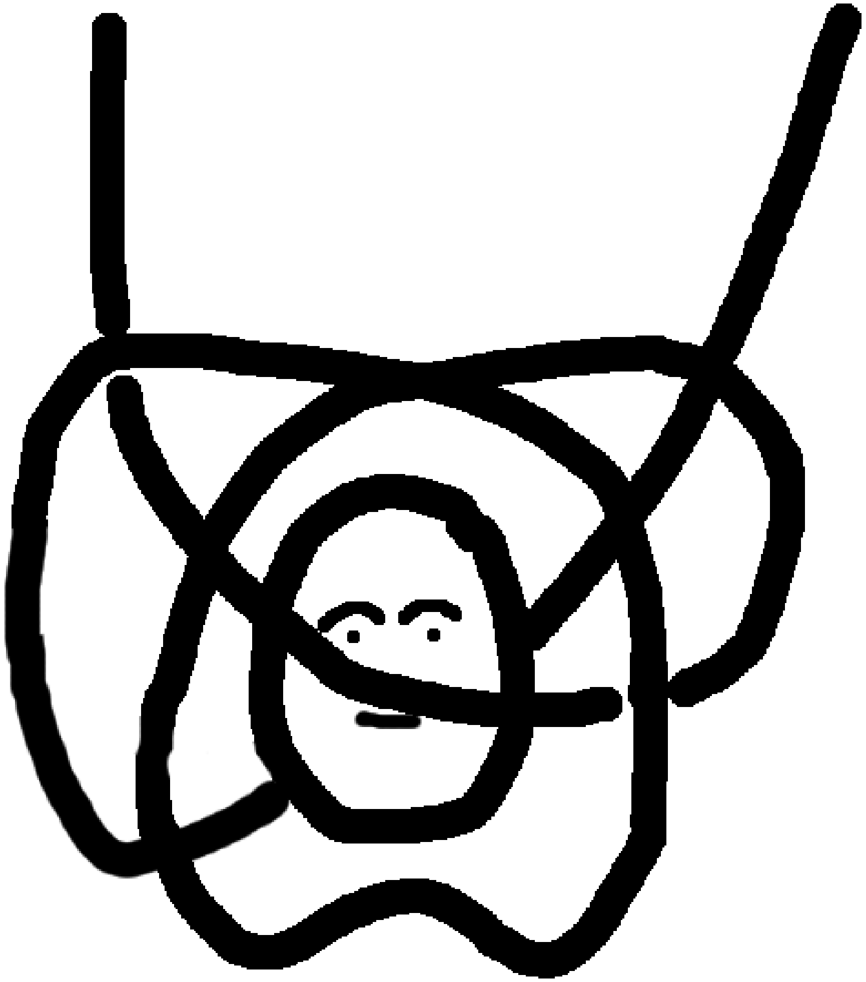
$$y^2 = x^3 + ax + b$$

…elliptic has to reconsider its form …

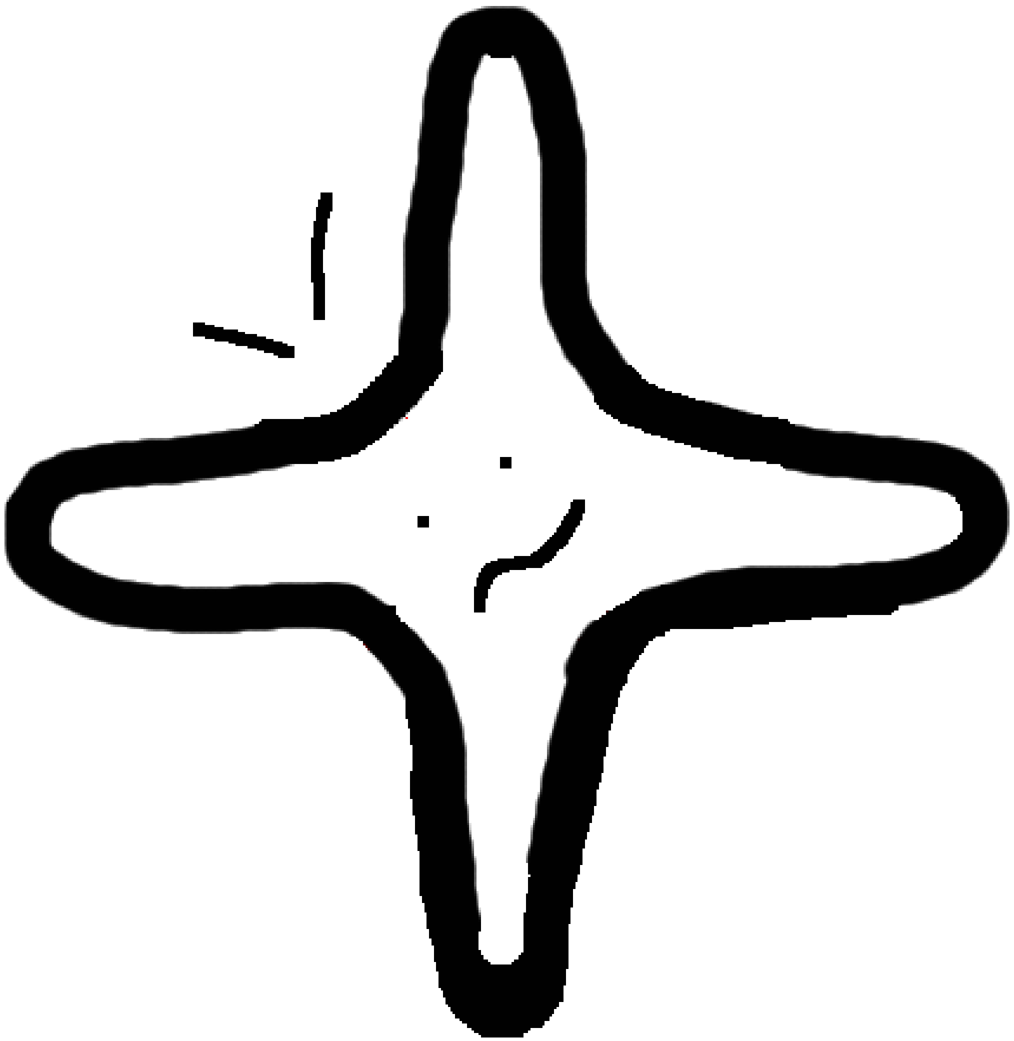
. . . has to abstract from its Weierstrass form . . .



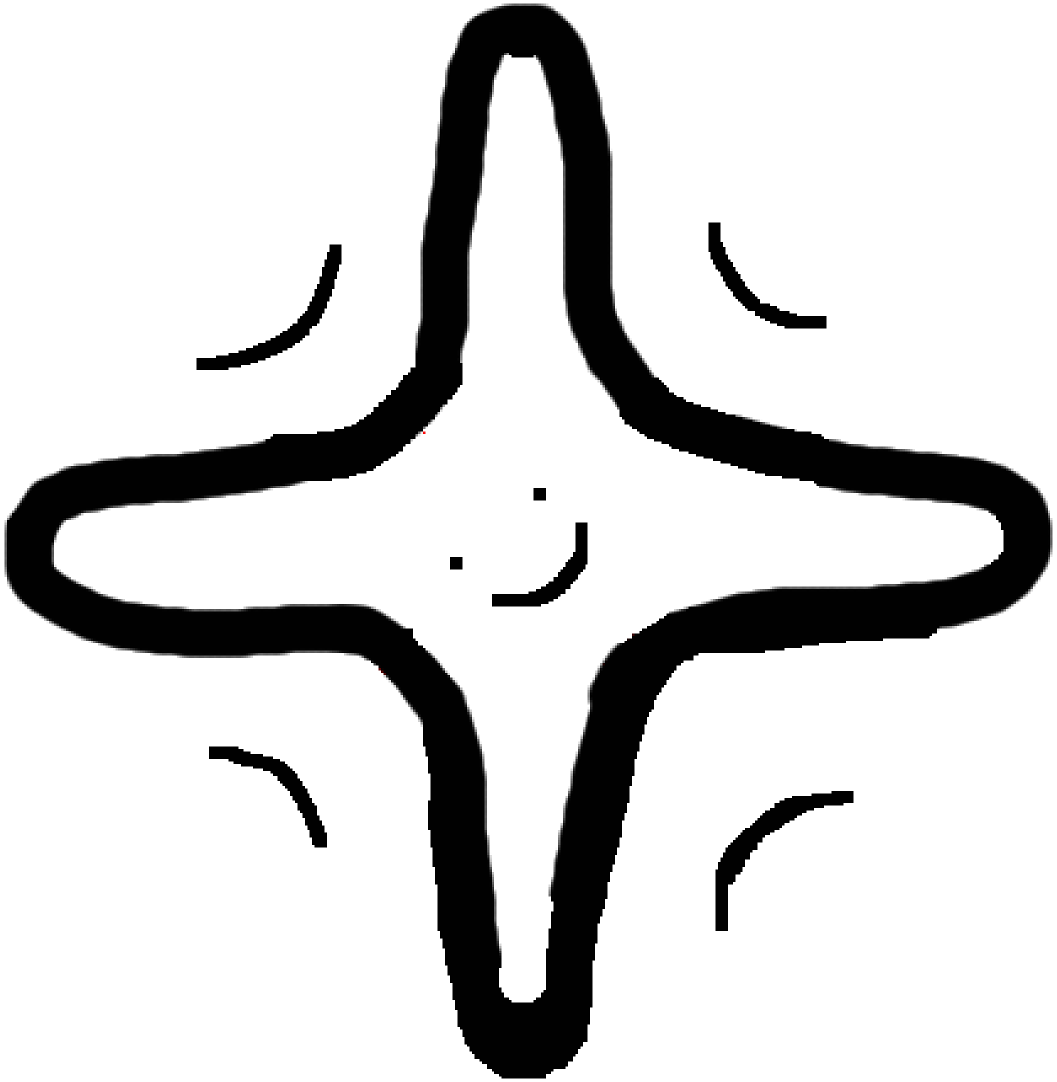
. . . has to undergo severe isomorphic transformations . . .



. . . until it finds . . .



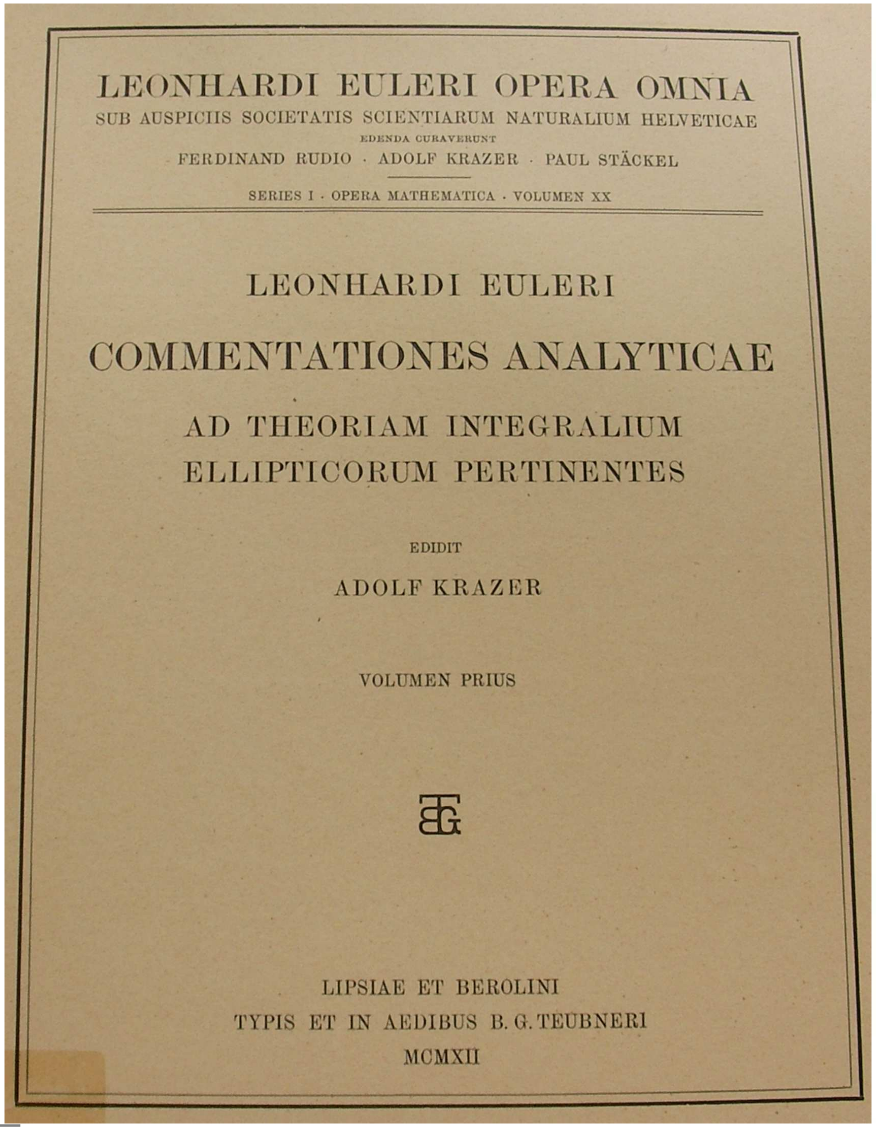
...its true ...



…normal form!

$$x^2+y^2=c^2(1+dx^2y^2)$$

Long, long ago . . .



LEONHARDI EULERI OPERA OMNIA
SUB AUSPICIIS SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE
EDENDA CURAVERUNT
FERDINAND RUDIO · ADOLF KRAZER · PAUL STÄCKEL

SERIES I · OPERA MATHEMATICA · VOLUMEN XX

LEONHARDI EULERI

COMMENTATIONES ANALYTICAE

AD THEORIAM INTEGRALIUM
ELLIPTICORUM PERTINENTES

EDIDIT

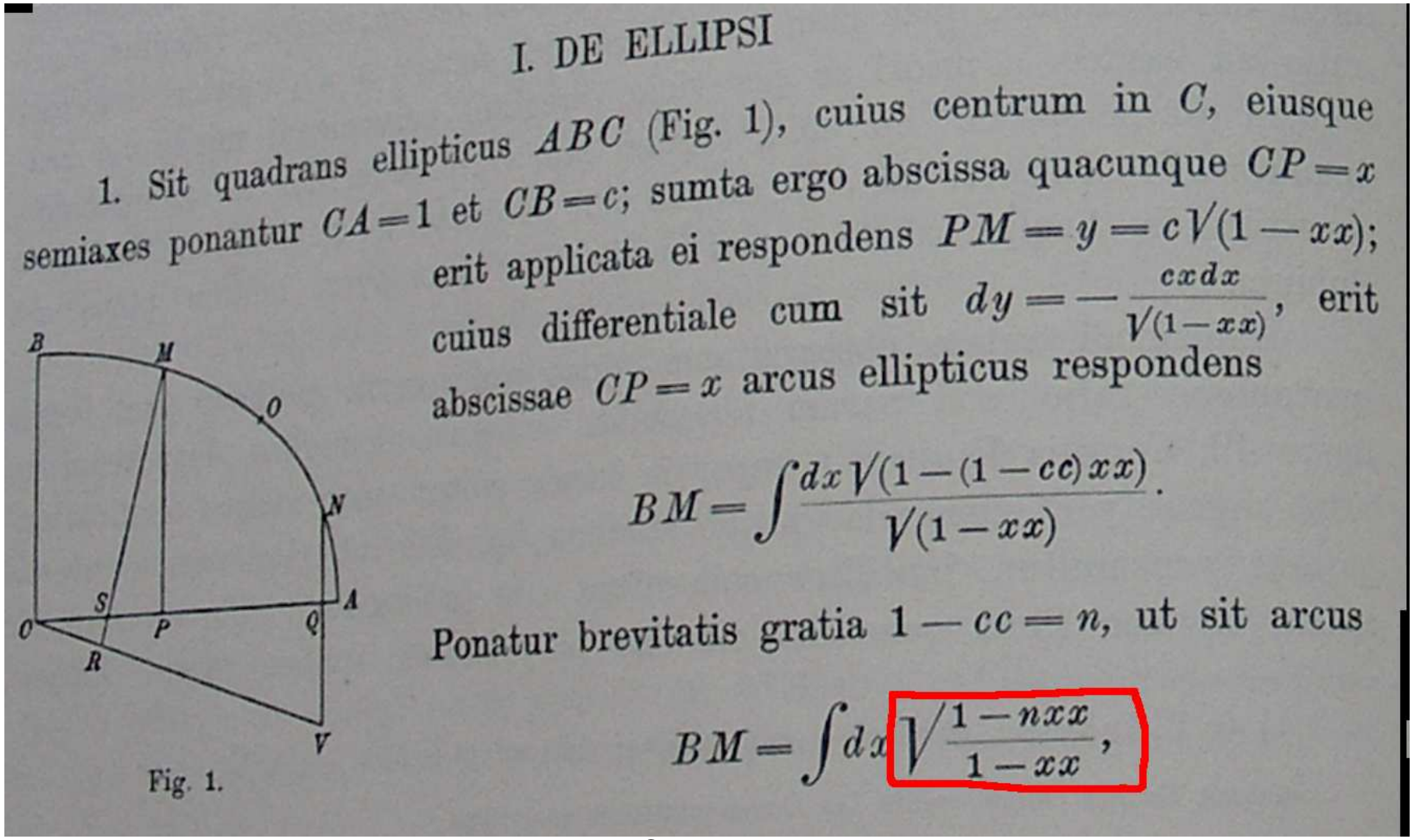
ADOLF KRAZER

VOLUMEN PRIUS

LIPSIAE ET BEROLINI
TYPIS ET IN AEDIBUS B. G. TEUBNERI
MCMXII

Euler 1761

" Observationes de Comparatione Arcuum Curvarum Irrectificabilium"



I. DE ELLIPSI

1. Sit quadrans ellipticus ABC (Fig. 1), cuius centrum in C, eiusque semiaxes ponantur $CA = 1$ et $CB = c$; sumta ergo abscissa quacunque $CP = x$ erit applicata ei respondens $PM = y = c\sqrt{(1 - xx)}$; cuius differentiale cum sit $dy = -\frac{cxdx}{\sqrt{(1-xx)}}$, erit abscissae $CP = x$ arcus ellipticus respondens

$$BM = \int \frac{dx\sqrt{(1-(1-cc)xx)}}{\sqrt{(1-xx)}}.$$

Ponatur brevitatis gratia $1 - cc = n$, ut sit arcus

$$BM = \int dx \boxed{\sqrt{\frac{1-nxx}{1-xx}},}$$

Fig. 1.

$$\frac{1}{y^2} = \frac{1-nx^2}{1-x^2} \Leftrightarrow x^2 + y^2 = 1 + nx^2y^2.$$

Euler 1761

COROLLARIUM 3

43. Inventio ergo cordarum arcuum quorumvis multiplorum una cum cordis complementi ita se habebit:

Corda arcus	Corda complementi
simpli $= a$	simpli $= A$
dupli $= b = \dfrac{2aA}{1 - aaAA}$	dupli $= \dfrac{AA - aa}{1 + aaAA} = B$
tripli $= c = \dfrac{aB + bA}{1 - abAB}$	tripli $= \dfrac{AB - ab}{1 + abAB} = C$
quadrupli $= d = \dfrac{aC + cA}{1 - acAC}$	quadrupli $= \dfrac{AC - ac}{1 + acAC} = D$
quintupli $= e = \dfrac{aD + dA}{1 - adAD}$	quintupli $= \dfrac{AD - ad}{1 + adAD} = E$
etc.	etc.

Euler gives doubling and (special) addition for (a, A) on $a^2 + A^2 = 1 - a^2A^2$.

Gauss, posthumously

ELEGANTIORES INTEGRALIS $\int \frac{dx}{\sqrt{(1-x^4)}}$ PROPRIETATES.

[2.]

$$1 = ss + cc + sscc \quad \text{sive} \quad 2 = (1+ss)(1+cc) = \left(\tfrac{1}{ss} - 1\right)\left(\tfrac{1}{cc} - 1\right)$$

$$s = \sqrt{\frac{1-cc}{1+cc}}, \qquad c = \sqrt{\frac{1-ss}{1+ss}}$$

$$\sin \operatorname{lemn}(a \pm b) = \frac{sc' \pm s'c}{1 \mp scs'c'}$$

$$\cos \operatorname{lemn}(a \pm b) = \frac{cc' \mp ss'}{1 \pm ss'cc'}$$

$$\sin \operatorname{lemn}(-a) = -\sin \operatorname{lemn} a, \qquad \cos \operatorname{lemn}(-a) = \cos \operatorname{lemn} a$$

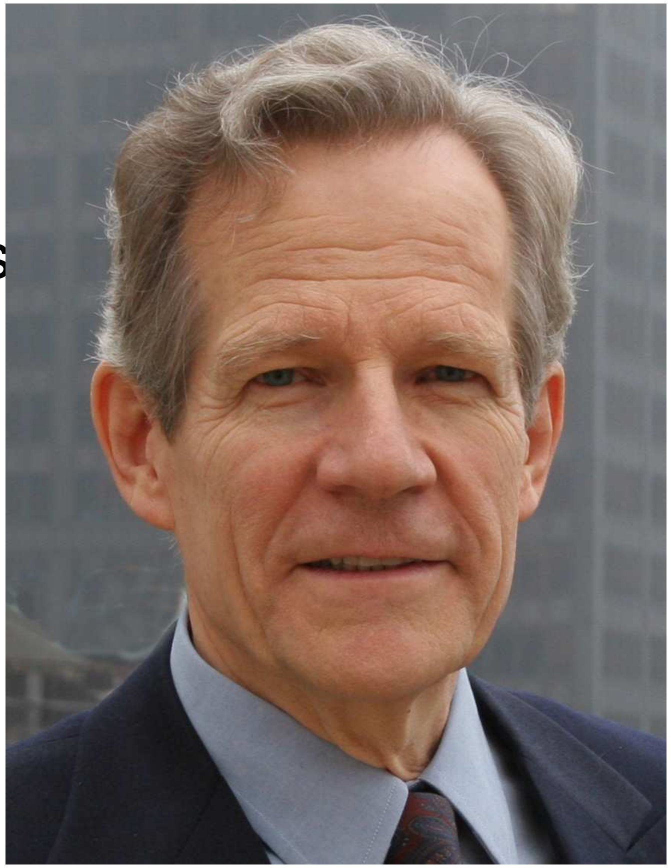
$$\sin \operatorname{lemn} k\varpi = 0 \qquad \sin \operatorname{lemn}(k+\tfrac{1}{2})\varpi = \pm 1$$

$$\cos \operatorname{lemn} k\varpi = \pm 1 \qquad \cos \operatorname{lemn}(k+\tfrac{1}{2})\varpi = 0$$

Gauss gives general addition for arbitrary points on

$$1 = s^2 + c^2 + s^2c^2.$$

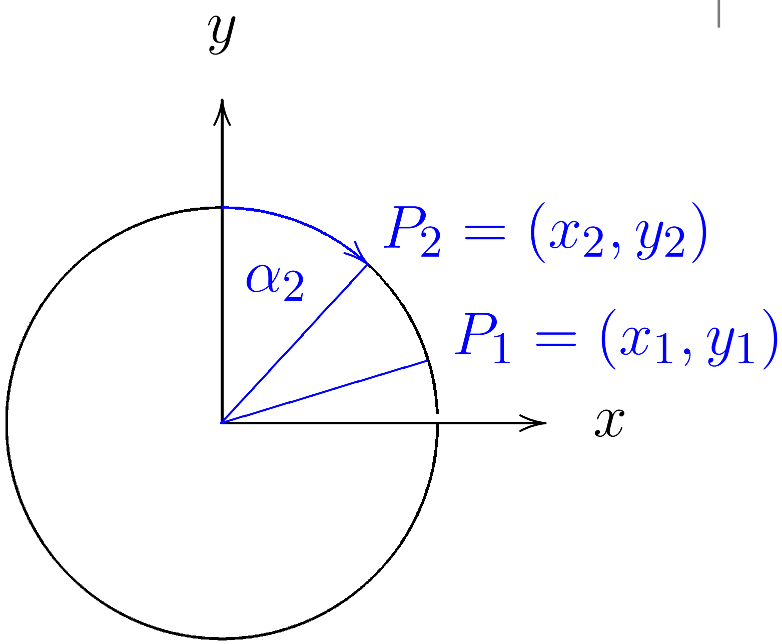
Harold M. Edwards



- The Gauss/Euler example is mentioned in some books.
- Edwards generalized this single example to whole class of curves
- Showed how to do arithmetic on this curve.
- Shows that – after some field extensions – every elliptic curve over field k of odd characteristic is birationally equivalent to a curve of the form
  $x^2 + y^2 = a^2(1 + x^2y^2), a^5 \neq a$
- Many more properties in his paper Bulletin of the AMS, **44**, 393–422, 2007

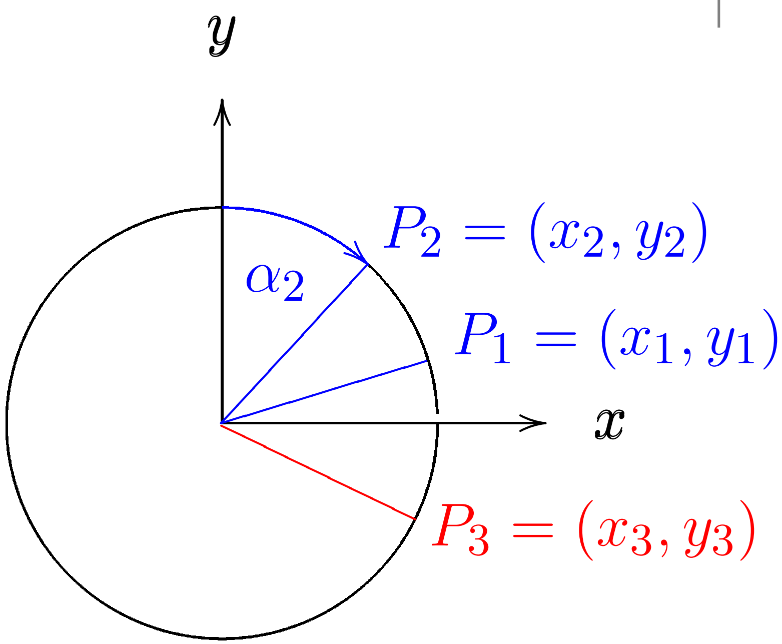
Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x, y) \in k \times k | x^2 + y^2 = 1\}$



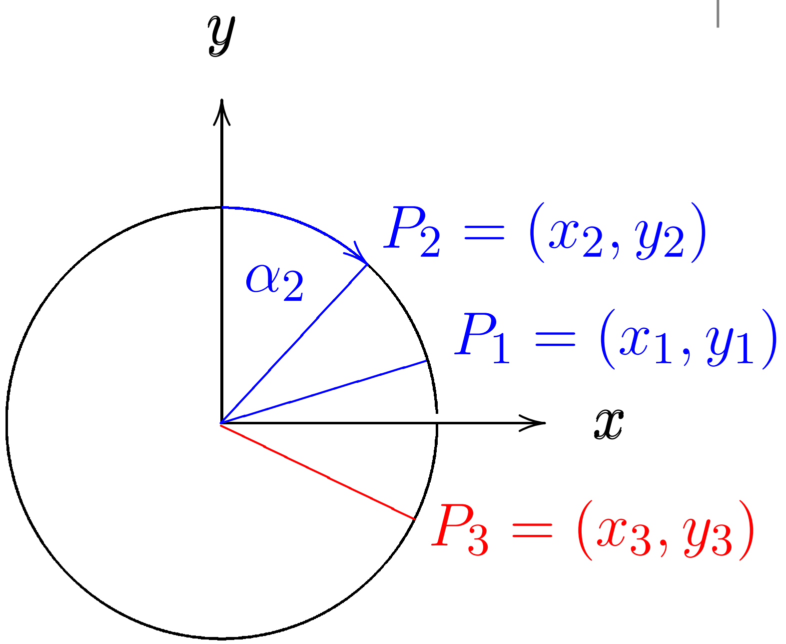
Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x, y) \in k \times k | x^2 + y^2 = 1\}$



Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x, y) \in k \times k | x^2 + y^2 = 1\}$
$x_i = \sin(\alpha_i),\ y_i = \cos(\alpha_i)$



$$\begin{aligned} x_3 &= \sin(\alpha_1 + \alpha_2) \\ &= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \end{aligned}$$

$$\begin{aligned} y_3 &= \cos(\alpha_1 + \alpha_2) \\ &= \cos(\alpha_1)\cos(\alpha_2) - \sin(\alpha_1)\sin(\alpha_2) \end{aligned}$$

Addition of angles defines commutative group law
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

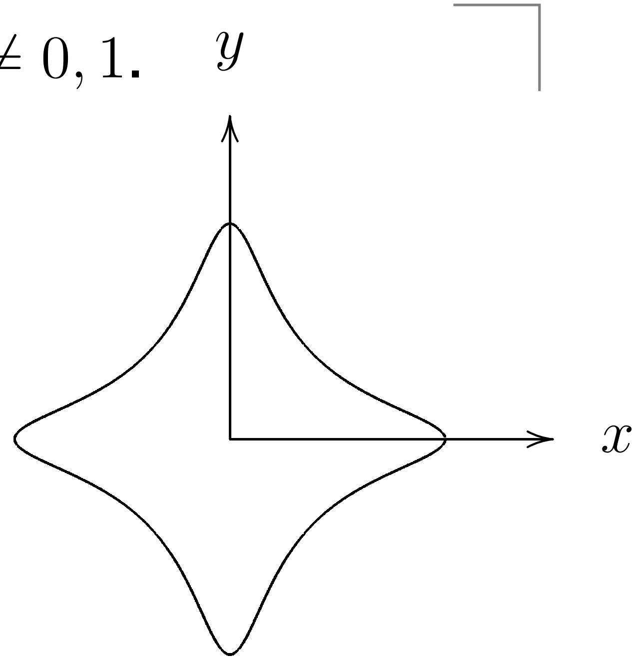
$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2.$$

Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$

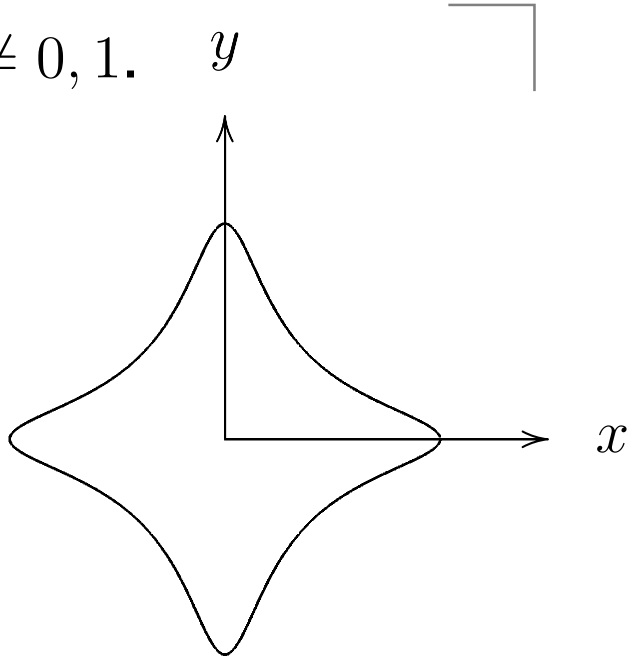
Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)



Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

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

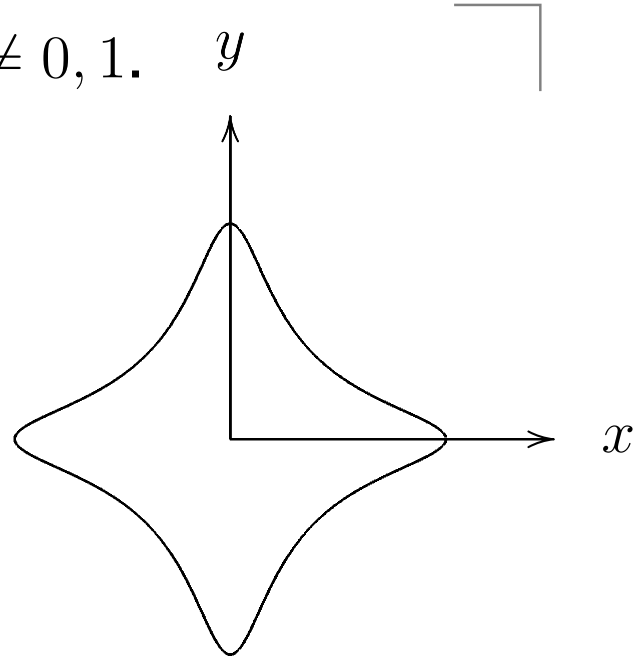
Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$

Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law



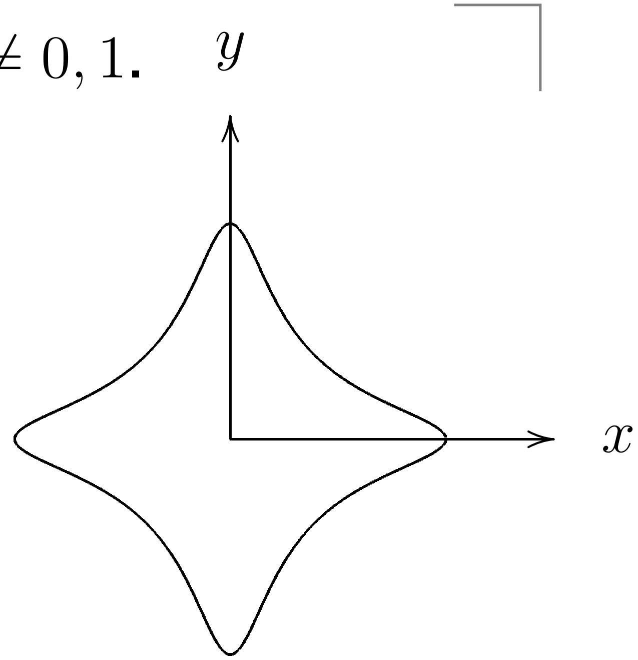
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is

Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

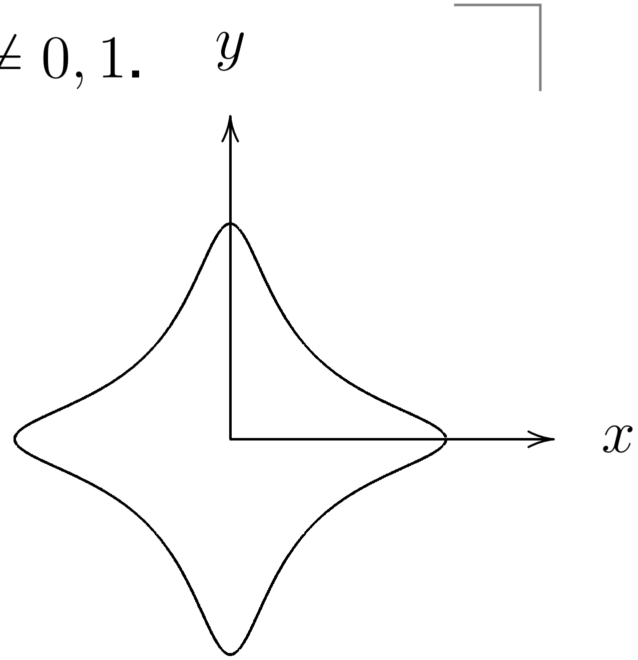
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$ (like on circle).

Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

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

- Neutral element is $(0, 1)$ (like on circle).
- $-(x_1, y_1) =$

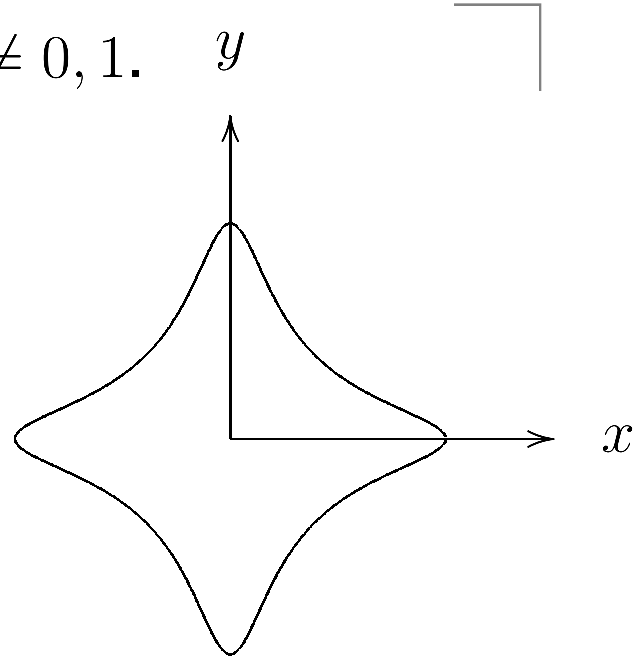
Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$

Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law



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

- Neutral element is $(0, 1)$ (like on circle).
- $-(x_1, y_1) = (-x_1, y_1)$ (like on circle).

Relationship to elliptic curves

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- Let $P_4 = (u_4, v_4)$ have order 4 and shift u s.t. $2P_4 = (0,0)$. Then Weierstrass form:
$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$
- Define $d = 1 - (4u_4^3/v_4^2)$.
- The coordinates $x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$ satisfy
$$x^2 + y^2 = 1 + dx^2y^2.$$
- Inverse map $u = u_4(1+y)/(1-y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q=\left(\dfrac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \dfrac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\dfrac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1}, \dfrac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q = \left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P = \left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1}, \frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\dfrac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \dfrac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!

Nice features of the addition law

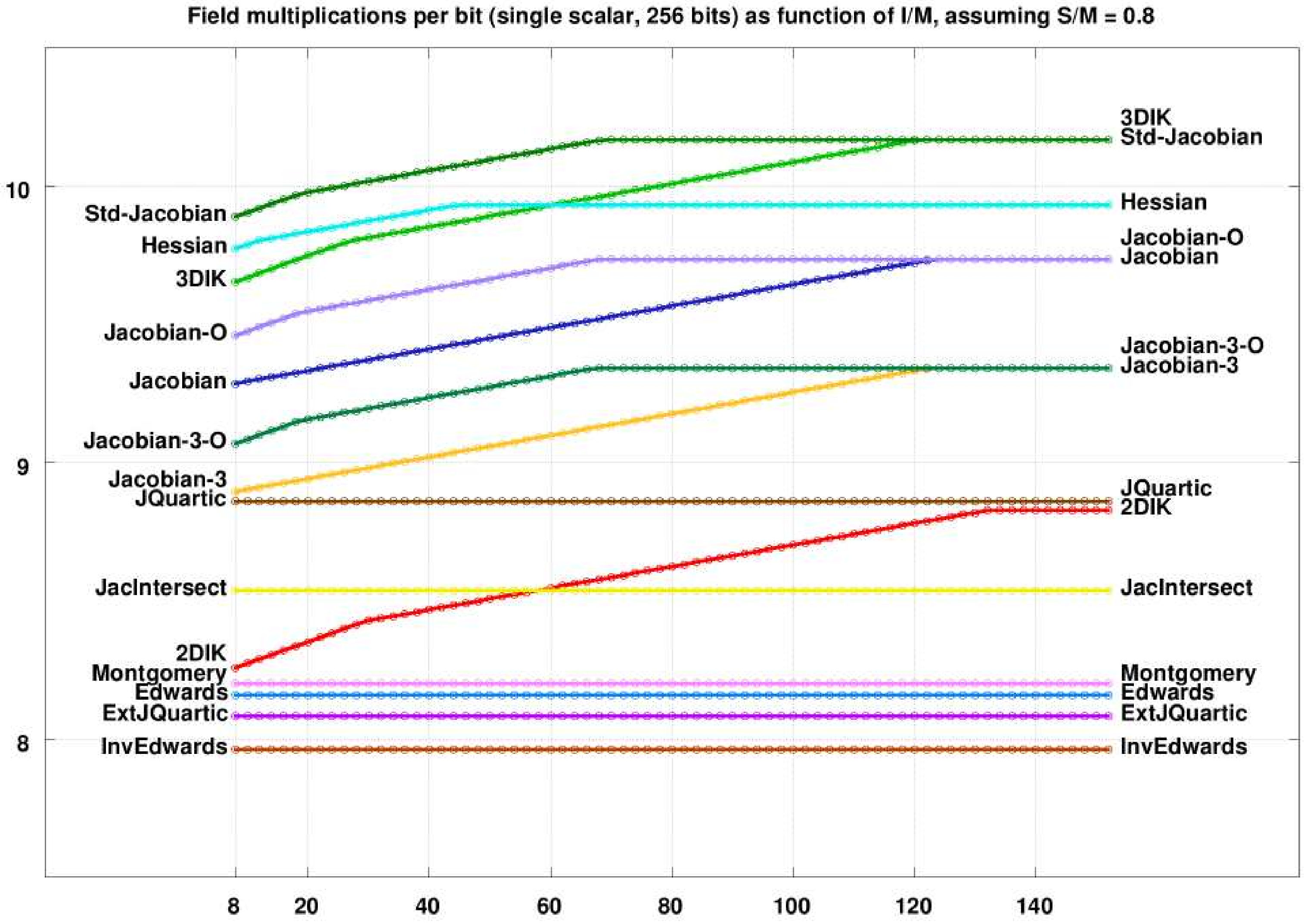
- Neutral element of addition law is affine point, this avoids special routines (for $(0, 1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right).$
- $[2]P = \left(\dfrac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \dfrac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!
- Having addition law work for doubling removes some checks from the code.

Complete addition law

- For d not a square in k, the Edwards addition law is complete, there are no exceptional cases.
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on curve.
  - Addition works to add P and P.
  - Addition works to add P and $-P$.
  - Addition just works to add P and any Q.
- Only complete addition law in the literature.
- Very fast point addition 10M + 1S + 1D.
- Dedicated doubling formulas need only 3M + 4S.
- Fastest scalar multiplication in the literature, in particular in 'Inverted Edwards' representation.

Speed comparison & influence of inversions

Joint work with D.J. Bernstein



Consequences

- Speed records for Diffie-Hellman key exchange.
- Faster signature computation (additions in this form are easy).
- Can afford larger key length for same speed (or get faster for same level of security).
- Applications using scalar multiplication on elliptic curves get faster . . .

Consequences

- Speed records for Diffie-Hellman key exchange.
- Faster signature computation (additions in this form are easy).
- Can afford larger key length for same speed (or get faster for same level of security).
- Applications using scalar multiplication on elliptic curves get faster ...
- ...which brings us to the second topic of this talk

RSA Cryptosystem

Secret computation – key generation:

- pick two primes p, q,
- compute $N = p \cdot q$,
- compute $\varphi(N) = (p-1)(q-1)$, where φ is the Euler-φ function,
- pick integer e co-prime to $\varphi(N)$,
- compute d with $de \equiv 1 \bmod \varphi(N)$.

Note that for any m with $\gcd(m, N) = 1$ the order of m modulo N is $\varphi(N)$.
So we have

$$(m^e)^d \equiv m^{ed} \equiv m^{k\varphi(N)+1} \equiv m \bmod N,$$

for some integer k.

Parameters & common pitfalls

- Factorization hardest if p and q have same size.
- Current choice (bleeding edge security): N has 1024 bits and p and q have 512 bits.
- Better security 2048 bits and not too painful performance (if one really wants to stick to RSA ...).
- Problem if one takes 'same size' too literally:

$$
\begin{aligned}
N = {} & 1000000000000000000000000000000000000000000000000000000\\
& 0000000000000000000000000000000000000000000000000000000000\\
& 0000000000000000000000000000000000000000000000000000000029\\
& 9999999999999999999999999999999999999999999999999999999999\\
& 9999999999999999999999999999999999999999999999999999999999\\
& 99999999999999999999999999999999999999999999999999997921.
\end{aligned}
$$

Factorization by inspection?!

Pitfalls ctd.

- Yes, this looks like very close to a power of 10, actually close to 10^{340}. Squareroot $\sqrt{N}$ is almost an integer, almost 10^{170}.

Pitfalls ctd.

- Yes, this looks like very close to a power of 10, actually close to 10^{340}. Squareroot $\sqrt{N}$ is almost an integer, almost 10^{170}.
- Brute-force search $\gcd(N, 10^{170} - i)$ finds factor $q = 10^{170} - 33$ and then $p = N/q = 10^{170} + 63$.

Pitfalls ctd.

- Yes, this looks like very close to a power of 10, actually close to 10^{340}. Squareroot $\sqrt{N}$ is almost an integer, almost 10^{170}.
- Brute-force search $\gcd(N, 10^{170} - i)$ finds factor $q = 10^{170} - 33$ and then $p = N/q = 10^{170} + 63$.
- This attack is well known and mentioned e.g. in the Handbook of Applied Cryptography. Yet it is found in practice by amateurs, usually with powers of 2 rather than 10.
- Famous example: letter bomber Franz Fuchs in Austria (6 attack series between 1993 and capture in 1997) send RSA-encrypted letter to Austrian magazine 'Profil'. Modulus N had 1024 bits, i.e. full size, but both primes were extremely close to 2^{512}. Found by Hans Dobbertin.

Attacks against generic RSA

Best known attacks against generic RSA try to find a, b with

$$a^2 \equiv b^2 \bmod N, \text{ i.e., } N|(a^2 - b^2). \tag{1}$$

If $N \nmid (a \pm b)$ then

$$1 < \gcd(N, a - b) < N$$

finds nontrivial factor.
The quadratic sieve finds such a relation by computing for many integers a_i

$$(a_i^2 \bmod N) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} a_i', \tag{2}$$

where p_j in factor base F and $\gcd(a_i', p_j) = 1$ for all $p_j \in F$.
Collect relations of form (2) with $a_i' = 1$; construct relation (1) using linear algebra. Number field sieve is similar.

Computational issues in factorization

- The factorization $N = p \cdot q$ is broken down into many factorizations of the form

$$(a_i^2 \bmod N) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} a_i'.$$

- Find small factors $p_i < 2^{20}$ by trial division/sieving.
- Find larger factors $p_i < 2^{40}$ by using ECM - the Elliptic Curve Method of factorization.
- Main idea of ECM: to factor $b = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ compute $[k]P$ for some point P on an elliptic curve E modulo b; hope that k is a multiple of the order of P on E modulo p_i and not on E modulo p_j for some i and j.
- Retrieve p_i by a gcd computation (technically all factors p_i such that k is a multiple of the group order of E modulo p_i.)

Impact of faster arithmetic on EC

- Traditionally the computation $[k]P$ was carried out in Montgomery form elliptic curves; Edwards curves are solidly faster.
- Previously fastest implementation was GMP-ECM by Zimmerman et al.
- Using Edwards curves and some new ideas we (joint work with D.J. Bernstein, P. Birkner, C. Peters) sped up the best known ECM implementation; faster arithmetic alone gives 7%; we also found more effective curves.
- Latest results: our cluster is warming up with some EECM (Edwards-ECM) computations (stage 1 and 2 working) seaching for 40-bit factors.

Edwards curves

–

blessing to ECC, harm to RSA

References

- Bernstein/L. “Faster addition and doubling on elliptic curves”, Asiacrypt 2007, pp. 29-50. Online.
- Bernstein/Birkner/L./Peters, “Optimizing double-base elliptic-curve single-scalar multiplication”, Indocrypt 2007, pp. 167–182. Online.
- Bernstein/L. “Analysis and optimization of elliptic-curve single-scalar multiplication”, Proceedings of Fq8.
- Bernstein/Birkner/L./Peters, “Twisted Edwards Curves”, Africacrypt.
- Bernstein/Birkner/L./Peters, “ECM using Edwards curves”.
- Bernstein/L./Rezaeian Farashahi, “Binary Edwards Curves”.

Details on the blow-up

- Points with $v(u+u_4)=0$ on Weierstrass curve map to points at infinity on desingularization of Edwards curve.
- Reminder: $d = 1-(4u_4^3/v_4^2)$.
- $u=-u_4$ is u-coordinate of a point iff

$$\begin{aligned} & (-u_4)^3 + (v_4^2/u_4^2 - 2u_4)(u_4)^2 + u_4^2(u_5) \\ = \ & v_4^2 - 4u_4^3 = v_4^2 d \end{aligned}$$

  is a square, i. e., iff d is a square.
- $v=0$ corresponds to $(0,0)$ which maps to $(0,-1)$ on Edwards curve and to solutions of $u^2+(v_4^2/u_4^2-2u_4)u+u_4^2=0$. Discriminant is

$$(v_4^2/u_4^2-2u_4)^2-4u_4^2 = v_4^4 d,$$

  i. e., points defined over k iff d is a square.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Intuitive explanation:
The points at infinity (for which the addition law must fail) have minimal field of definition $k(\sqrt{d})$.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} d x_1^2 y_1^2 (x_2^2 + y_2^2) &= d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2 \\ &= d x_1^2 y_1^2 + \epsilon^2 \end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} d x_1^2 y_1^2 (x_2^2 + y_2^2) &= d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2 \\ &= d x_1^2 y_1^2 + \epsilon^2 \\ &= 1 + d x_1^2 y_1^2 = x_1^2 + y_1^2 \end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

$$\begin{aligned}(x_1 + \epsilon y_1)^2 &= x_1^2 + y_1^2 + 2\epsilon x_1 y_1 = d x_1^2 y_1^2 (x_2^2 + y_2^2) + 2 x_1 y_1 d x_1 x_2 y_1 y_2 \\ &= d x_1^2 y_1^2 (x_2^2 + 2 x_2 y_2 + y_2^2) = d x_1^2 y_1^2 (x_2 + y_2)^2.\end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

$$(x_1 + \epsilon y_1)^2 = x_1^2 + y_1^2 + 2\epsilon x_1 y_1 = d x_1^2 y_1^2 (x_2^2 + y_2^2) + 2 x_1 y_1 d x_1 x_2 y_1 y_2$$

$$= d x_1^2 y_1^2 (x_2^2 + 2 x_2 y_2 + y_2^2) = d x_1^2 y_1^2 (x_2 + y_2)^2.$$

$x_2 + y_2 \neq 0 \Rightarrow d = ((x_1 + \epsilon y_1)/x_1 y_1 (x_2 + y_2))^2 \Rightarrow d = \square$

$x_2 - y_2 \neq 0 \Rightarrow d = ((x_1 - \epsilon y_1)/x_1 y_1 (x_2 - y_2))^2 \Rightarrow d = \square$

If $x_2 + y_2 = 0$ and $x_2 - y_2 = 0$ then $x_2 = y_2 = 0$, contradiction.