Elliptic Curve Cryptography

Tanja Lange

Coding Theory and Cryptology

Technische Universiteit Eindhoven

The Netherlands

tanja@hyperelliptic.org

05.02.2011

Data Protection

Many factors influence the security and privacy of data

- Secure storage, physical security.
- Access control.
- Protection against alteration of data
  $\Rightarrow$ digital signatures, message authentication codes.
- Protection of sensitive content against reading
  $\Rightarrow$ encryption.

Cryptology is the science that studies mathematical techniques in order to provide confidentiality, authenticity and related properties for digital information.

Encryption

Important Distinction

- Partners share a secret (key)
  $\Rightarrow$ use of *symmetric encryption* methods
  - classical methods (Caesar, ...) belong to this class
  - One-time pad
  - AES
- Partners have no initial secret
  $\Rightarrow$ use of public key cryptography
  - RSA
  - Diffie-Hellman key-exchange
  - ElGamal signatures

Most applications are hybrid, i.e., they use a combination of both (e.g. use public key cryptography to get session key).

Public Key cryptography

Each user has two keys

- a private key chosen by him which *never* leaves the secure environment,
- a public key which is made public in a kind of phone book.
- These keys are linked by a (computational) one-way function; the general principles are public.
- Sender uses public key of recipient to encrypt
  $\Rightarrow$ only recipient knows secret key and can decrypt.
- Sender uses his private key to sign a message
  $\Rightarrow$ signature must be due to him as only he knows the secret; every recipient can verify the signature using the sender's public key.

What do mathematicians do here?

- Find good candidates for computational one-way functions.
- Look for variants having better performance.
- Analysis of attacks.

Proposed candidates

- Multiplying two integers is easy while factoring is hard (RSA).

  primes $p, q \Rightarrow N = p \cdot q$ vs. integer $N \Rightarrow p, q$.
- In some groups computing exponentiation is easy while finding the corresponding exponent given two group elements is hard $\Rightarrow$ discrete logarithm problem (DLP).

  $g \in G,$ integer $a \Rightarrow h = g^a$ vs. $g \in G, h = g^a \Rightarrow a$.

Signatures in discrete logarithm systems

Public parameters: Group G, generator g, $\mathrm{ord}(g) = \ell$, some function $H : G \to \mathbb{Z}/\ell$.
Signer A has secret key a and public key $h_A = g^a$.

- Sign message $m \in \mathbb{Z}/\ell$
  - choose random integer k,
  - compute $r = g^k$ and $s \equiv am + kH(r) \bmod \ell$
  - send (r, s)
- Validate signature (r, s) on m
  - Check whether g^s equals $h_A^m \cdot r^{H(r)}$

A's signatures are valid:

$$g^s = g^{am+kH(r)} = (g^a)^m \cdot (g^k)^{H(r)} = h_A^m \cdot r^{H(R)}.$$

In practice, $h(m)$ for a hash function h is used instead of m.
Good for long messages and helps against forgery.

Signatures in discrete logarithm systems

Public parameters: Group G, generator g, $\mathrm{ord}(g) = \ell$, some function $H : G \to \mathbb{Z}/\ell$.
Signer A has secret key a and public key $h_A = g^a$.

- Sign message $m \in \mathbb{Z}/\ell$
  - choose random integer k, keep k secret!
  - compute $r = g^k$ and $s \equiv am + kH(r) \bmod \ell$
  - send (r, s)

If k becomes public, the long term secret key a can be computed from a single signature:

$$a \equiv (s - kH(r))/m \bmod \ell.$$

If the same k is used for two messages m_1 and m_2 then

$$s_1 - s_2 \equiv (am_1 + kH(r)) - (am_2 + kH(r)) = a(m_1 - m_2)$$

revealing a — but this would be a very non-random k!

Diffie-Hellman Key exchange

$$G = \langle g \rangle, \ell = \mathrm{ord}(g)$$

Alice		**Bob**
1. secretly generates $a < \ell$		1. secretly generates $b < \ell$
2. computes $h_A = g^a$		2. computes $h_B = g^b$
3. transmits h_A		3. transmits h_B
4. computes ${h_B}^a$	$= g^{ab} =$	4. computes ${h_A}^b$

A and B know $k = g^{ab} \in G$; k can be used in symmetric encryption. Anybody knowing a or b also knows k.

Choice of group matters!

- $G = (\mathbb{Z}, +), g = 1$

Choice of group matters!

- $G = (\mathbb{Z}, +), g = 1 \Rightarrow h_A = 1 + 1 + \cdots + 1 = a$, so everybody can compute $k = ab$.
- $G \leq (\mathbb{Q}, \cdot), g = 2$

Choice of group matters!

- $G = (\mathbb{Z}, +), g = 1 \Rightarrow h_A = 1 + 1 + \cdots + 1 = a$, so everybody can compute $k = ab$.
- $G \leq (\mathbb{Q}, \cdot), g = 2 \Rightarrow h_A = 2^a$ and a is easily computed as $a = \log_2(h_A)$ giving $k = h_b^a$.
  These two examples work with infinite groups, the growth of h_A reveals a.

Choice of group matters!

- $G = (\mathbb{Z}, +), g = 1 \Rightarrow h_A = 1 + 1 + \cdots + 1 = a$, so everybody can compute $k = ab$.
- $G \leq (\mathbb{Q}, \cdot), g = 2 \Rightarrow h_A = 2^a$ and a is easily computed as $a = \log_2(h_A)$ giving $k = h_b^a$.
  These two examples work with infinite groups, the growth of h_A reveals a.
- $G = (\mathbb{Z}/p, +), g = 1 + p\mathbb{Z}$ again reveals a as $h_A \equiv a \bmod p$.
- $G = (\mathbb{Z}/p, +), g = s + p\mathbb{Z}$

Choice of group matters!

- $G = (\mathbb{Z}, +), g = 1 \Rightarrow h_A = 1 + 1 + \cdots + 1 = a$, so everybody can compute $k = ab$.
- $G \leq (\mathbb{Q}, \cdot), g = 2 \Rightarrow h_A = 2^a$ and a is easily computed as $a = \log_2(h_A)$ giving $k = h_b^a$.
  These two examples work with infinite groups, the growth of h_A reveals a.
- $G = (\mathbb{Z}/p, +), g = 1 + p\mathbb{Z}$ again reveals a as $h_A \equiv a \bmod p$.
- $G = (\mathbb{Z}/p, +), g = s + p\mathbb{Z}$
  $\Rightarrow h_A \equiv as \bmod p \Rightarrow a \equiv h_A s^{-1} \bmod p$ again reveals a.
  Modular inversion is easily computed using the extended Euclidean algorithm.

Choice of group matters!

- $G = (\mathbb{Z}, +), g = 1 \Rightarrow h_A = 1 + 1 + \cdots + 1 = a$, so everybody can compute $k = ab$.
- $G \leq (\mathbb{Q}, \cdot), g = 2 \Rightarrow h_A = 2^a$ and a is easily computed as $a = \log_2(h_A)$ giving $k = h_b^a$.
  These two examples work with infinite groups, the growth of h_A reveals a.
- $G = (\mathbb{Z}/p, +), g = 1 + p\mathbb{Z}$ again reveals a as $h_A \equiv a \bmod p$.
- $G = (\mathbb{Z}/p, +), g = s + p\mathbb{Z}$
  $\Rightarrow h_A \equiv as \bmod p \Rightarrow a \equiv h_A s^{-1} \bmod p$ again reveals a.
  Modular inversion is easily computed using the extended Euclidean algorithm.
- $\langle g \rangle \leq ((\mathbb{Z}/p)^*, \cdot)$ can be easy to break if $\ell = \mathrm{ord}(g)$ is small or highly composite, but DLP is not always easy.

Proposed groups for real-world crypto

- $\mathbb{F}_p^*$, multiplicative group of prime field.
- $\mathbb{F}_q^*$ (same for arbitrary finite field).
- $E(\mathbb{F}_q)$, group of $\mathbb{F}_q$-rational points on elliptic curve E.
- $\mathrm{Pic}_C^0(\mathbb{F}_q)$, divisor class group of curve C over $\mathbb{F}_q$.

Difference in security:

- First two examples have attacks subexponential in q

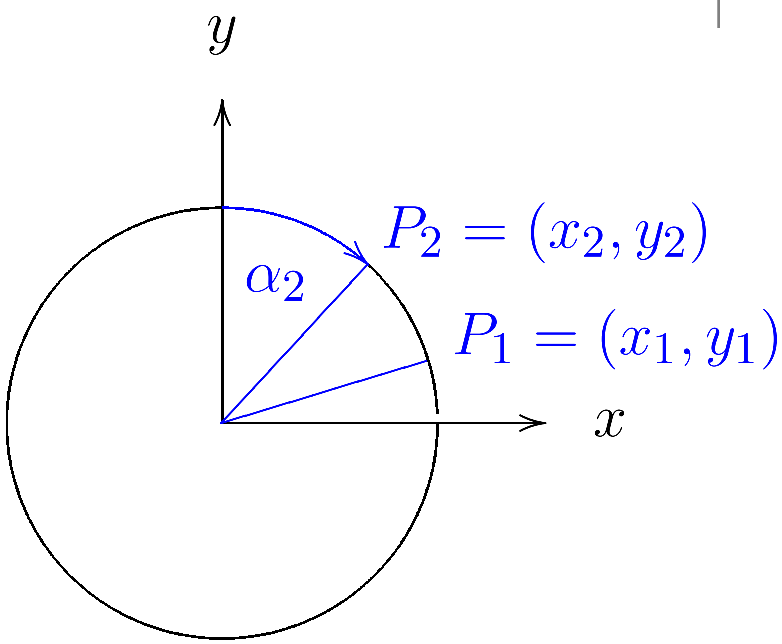
$$\exp((c + o(1))(\log q)^{1/3}(\log\log q)^{2/3}),$$

- for elliptic and small genus hyperelliptic curves the best attacks are exponential in group size ℓ

$$\Theta(\exp((1/2)\log \ell)) = \Theta(\ell^{1/2}).$$

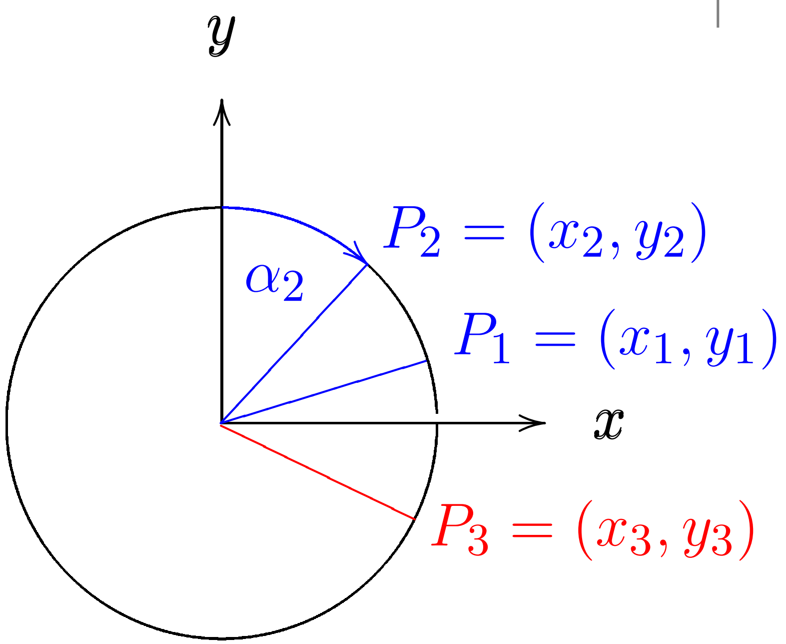
Do you know how to add on a circle?

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



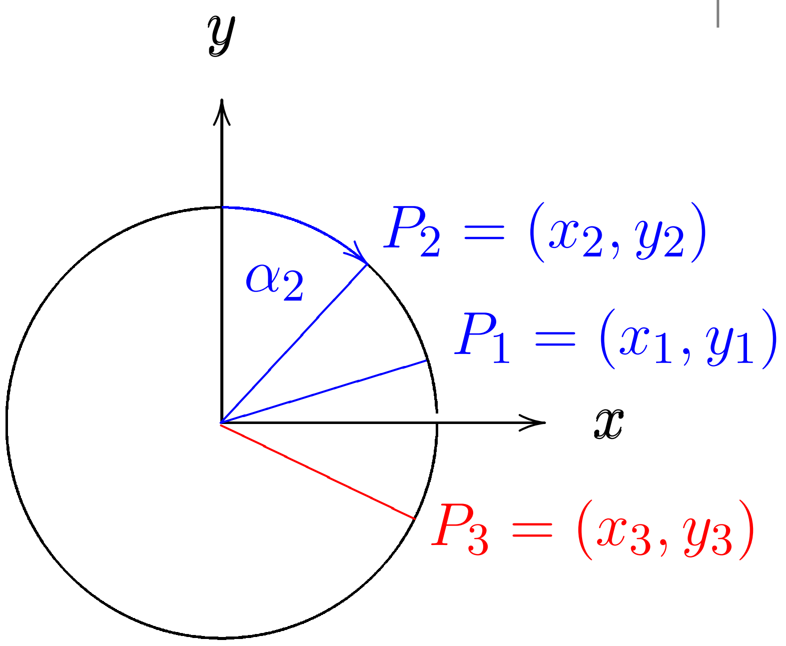
Do you know how to add on a circle?

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

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

Cryptography on the circle I

- Can use addition of hours on clock to motivate addition law.
- $(0, 1)$ is at $\alpha = 0$. Then $(0, 1) + Q = Q + (0, 1) = Q$.
- $R = (0, -1)$ is at angle $180°$. Then $[2]R = R + R$

Cryptography on the circle I

- Can use addition of hours on clock to motivate addition law.
- $(0, 1)$ is at $\alpha = 0$. Then $(0, 1) + Q = Q + (0, 1) = Q$.
- $R = (0, -1)$ is at angle $180°$. Then $[2]R = R + R(0, 1)$.
- What is the order of $(1, 0)$?

Cryptography on the circle I

- Can use addition of hours on clock to motivate addition law.
- $(0,1)$ is at $\alpha = 0$. Then $(0,1) + Q = Q + (0,1) = Q$.
- $R = (0,-1)$ is at angle 180°. Then $[2]R = R + R(0,1)$.
- What is the order of $(1,0)$? $[2](1,0) = (0,-1)$.

Cryptography on the circle I

- Can use addition of hours on clock to motivate addition law.
- $(0, 1)$ is at $\alpha = 0$. Then $(0, 1) + Q = Q + (0, 1) = Q$.
- $R = (0, -1)$ is at angle $180°$. Then $[2]R = R + R(0, 1)$.
- What is the order of $(1, 0)$? $[2](1, 0) = (0, -1)$.
- Negative of (x, y) is $(-x, y)$.
- These observations are clear from the angles on the circle, e.g. $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ is at $45°$ and has order 8.
- How about $S = (\frac{3}{5}, \frac{4}{5})$? Use $[n]P$ to denote n-fold of P.

Cryptography on the circle I

- Can use addition of hours on clock to motivate addition law.
- $(0,1)$ is at $\alpha = 0$. Then $(0,1) + Q = Q + (0,1) = Q$.
- $R = (0,-1)$ is at angle $180°$. Then $[2]R = R + R(0,1)$.
- What is the order of $(1,0)$? $[2](1,0) = (0,-1)$.
- Negative of (x,y) is $(-x,y)$.
- These observations are clear from the angles on the circle, e.g. $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ is at $45°$ and has order 8.
- How about $S = (\frac{3}{5}, \frac{4}{5})$? Use $[n]P$ to denote n-fold of P.
  Compute $[2]S$: $x_3 = \frac{3}{5}\frac{4}{5} + \frac{4}{5}\frac{3}{5} = \frac{24}{25}$, $y_3 = \frac{4}{5}\frac{4}{5} - \frac{3}{5}\frac{3}{5} = \frac{7}{25}$
  $[3]S = [2]S + S$: $x_3 = \frac{117}{125}$, $y_3 = \frac{-44}{125}$, $[4]P = (\frac{336}{625}, \frac{-527}{625})$

Cryptography on the circle II

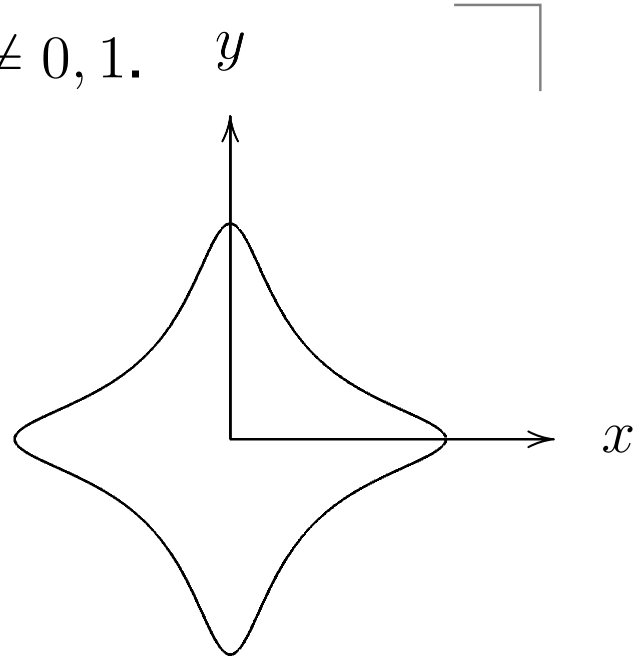
- Can use this to build a discrete logarithm system by using points over a finite field ($x, y \in \mathbb{F}_q$)
- Implementation a bit more complicated than in $\mathbb{F}_q^*$ – need to do 4 modular multiplications for each group operation (can optimize this down to 3 multiplications).
- Security? Not much better than in $\mathbb{F}_q^*$ because index calculus attacks apply.
  To achieve 192 bit security need to have q with at least 1024 bits (half the length as for $\mathbb{F}_q^*$).
- Mathematically the clock group is a torus over $\mathbb{F}_q$.

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:

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

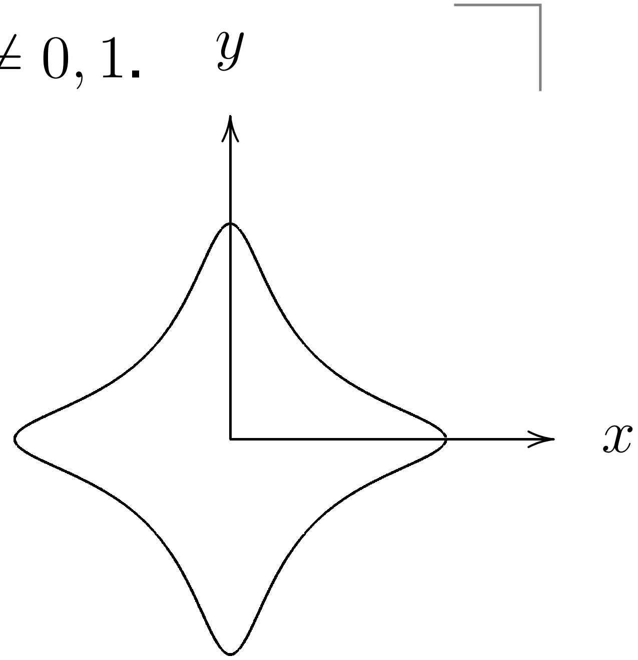
Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)



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)

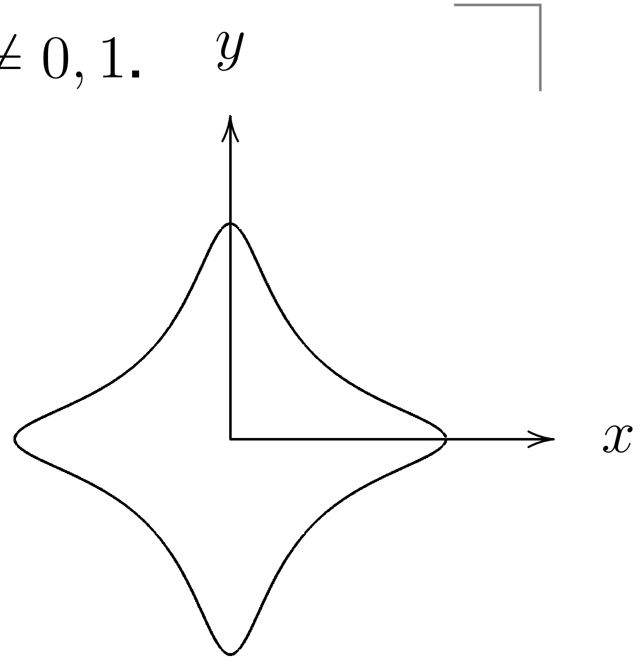
Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

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

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

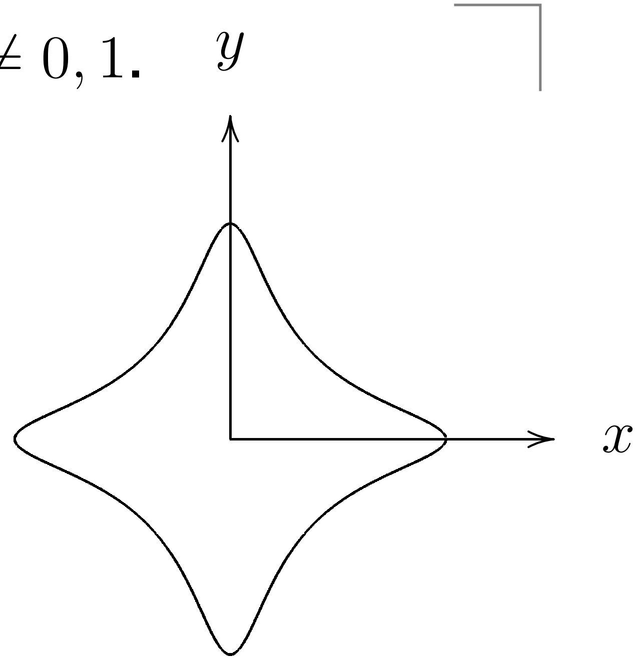
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- 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

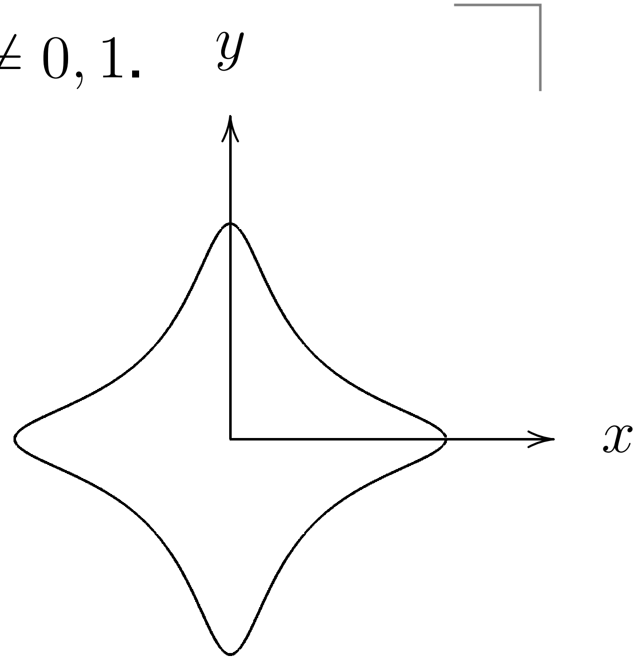
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- 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

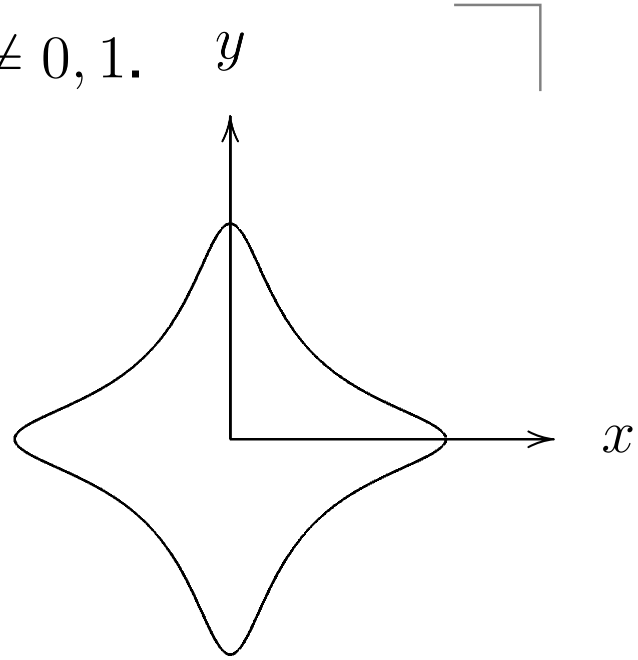
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- 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).

Explicit formulas: addition

- $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- Avoid inversions: Use $(X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$ to represent $(x_1, y_1) = (X_1/Z_1, Y_1/Z_1)$, i. e., $(X_1 : Y_1 : Z_1) = (\lambda X_1 : \lambda Y_1 : \lambda Z_1)$ for $\lambda \neq 0$.
- Addition formulas in projective coordinates:

$$\begin{aligned}
A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2; \\
E &= d \cdot C \cdot D;\ F = B - E;\ G = B + E; \\
X_3 &= A \cdot F \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D); \\
Y_3 &= A \cdot G \cdot (D - C); \\
Z_3 &= F \cdot G.
\end{aligned}$$

- Needs 10M + 1S + 1D + 7A, i.e. 10 multiplications, 1 squaring, 1 multiplication involving d, and 7 additions.

Faster dedicated doubling

- If $(x_2, y_2) = (x_1, y_1)$ we speak of doubling.
- Addition formulas work for doubling:
  $$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right).$$
- Doubling formulas in projective coordinates:
  $$\begin{aligned} B &= (X_1 + Y_1)^2;\ C = X_1^2;\ D = Y_1^2; \\ E &= C + D;\ H = Z_1^2;\ J = E - 2H; \\ X_3 &= (B - E) \cdot J;\ Y_3 = E \cdot (C - D);\ Z_3 = E \cdot J. \end{aligned}$$
- Needs 3M + 4S + 6A.
- Can compose any computation $[n]P$ from additions and doublings (use sliding window methods).

Why Edwards curves in this talk?

- Edwards curves are elliptic curves.
- Addition on Edwards curves easier to motivate than on Weierstrass curves (the usual representation).
- Edwards showed that any elliptic curve can be written in this form (possibly after a small field extension).
- Map between Edwards curves and Weierstrass curves explicit and efficient, so breaking DLPs in one representation breaks them in the other as well.
- Security studies of elliptic curves show:
  - Elliptic curves offer much higher security per bit compared to the clock group – the 1024-bit clock group corresponds to q having only 224 bits.
  - Much slower increase in size of q with the security level. The 1536-bit clock group matches 256-bits q.

Why Edwards curves?

- Very fast point addition 10M + 1S + 1D. Even faster with Inverted Edwards coordinates (9M+1S+1D) and Extended Edwards coordinates (8M+1S+1D).
- Dedicated doubling formulas need only 3M + 4S.
- Fastest scalar multiplication in the literature.
- For comparison: IEEE standard P1363 provides “the fastest arithmetic on elliptic curves” by using Jacobian coordinates on Weierstrass curves.
  - Point addition 12M + 4S.
  - Doubling formulas need only 4M + 4S.
- For more curve shapes, better algorithms (even for Weierstrass curves) and many more operations (mixed addition, re-addition, tripling, scaling,...) see `www.hyperelliptic.org/EFD`.

Beyond speed

- Neutral element of addition law is affine point.
- Addition law is symmetric in both inputs.
- $P + Q = \left(\dfrac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \dfrac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$

Beyond speed

- Neutral element of addition law is affine point.
- Addition law is symmetric in both inputs.
- $P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
  Can compute this using the same formulas as general addition; different for Jacobian coordinates.

Beyond speed

- Neutral element of addition law is affine point.
- Addition law is symmetric in both inputs.
- $P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
  Can compute this using the same formulas as general addition; different for Jacobian coordinates.
- If d is not a square in K the denominators $1 + d x_1 x_2 y_1 y_2$ and $1 - d x_1 x_2 y_1 y_2$ are never 0; addition law is complete.

Beyond speed

- Neutral element of addition law is affine point.
- Addition law is symmetric in both inputs.
- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1}, \frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$
  Can compute this using the same formulas as general addition; different for Jacobian coordinates.
- If d is not a square in K the denominators $1+dx_1x_2y_1y_2$ and $1-dx_1x_2y_1y_2$ are never 0; addition law is complete.
- Having addition law work for doubling removes some checks from the code; addition law also works for adding $P+(-P)$ or the neutral element.

Convenience and security

- Can reduce area by implementing only addition formula and using that for doublings. This is slower but ...
- ...has benefit that certain side-channel attacks are not feasible:
  - execution time of $[b]P$ does not depend on the chosen scalar (but does leak Hamming weight);
  - power traces of addition and doubling do not differ if addition formulas are used uniformly.
  - Still need to handle differential and template attacks.
- Attention: There are other formulas for Edwards curves that need distinguishing additions and doublings:

$$(x_3, y_3) = ((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2), (x_1y_1 - x_2y_2)/(x_1y_2 - y_1x_2))$$

is addition on Edwards curve ...and fails for doublings.

Weierstrass curves

$$E : v^2 + \underbrace{(a_1u + a_3)}_{h(u)} v = \underbrace{u^3 + a_2u^2 + a_4u + a_6}_{f(u)}, \;\; h, f \in \mathbb{F}_q[u].$$

Group: $E(\mathbb{F}_q) = \{ (u, v) \in \mathbb{F}_q^2 \, : \, v^2 + h(u)v = f(u) \} \cup \{ P_\infty \}$

Often $q = 2^r$ or $q = p$, prime. Isomorphic transformations lead to

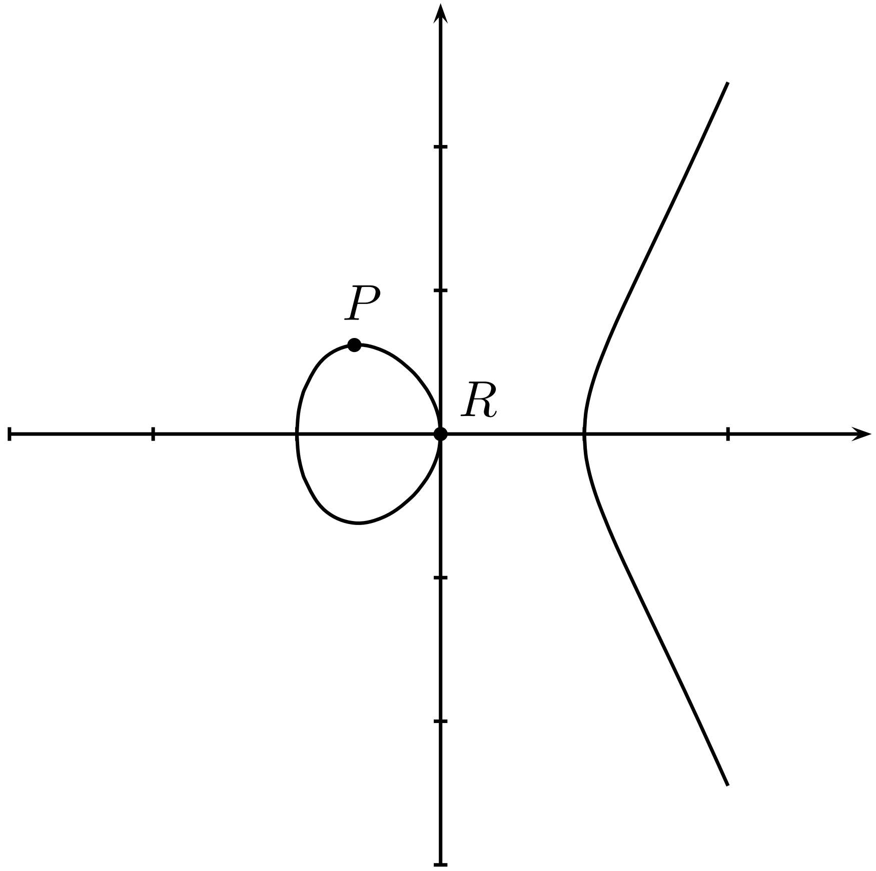
$$v^2 = f(u) \qquad q \text{ odd},$$

for

$$\begin{aligned} v^2 + uv &= u^3 + a_2u^2 + a_6 \\ v^2 + v &= u^3 + a_4u + a_6 \end{aligned} \qquad q = 2^r, \quad \begin{array}{l} \text{curve non-supersingular} \\ \text{curve supersingular} \end{array}$$

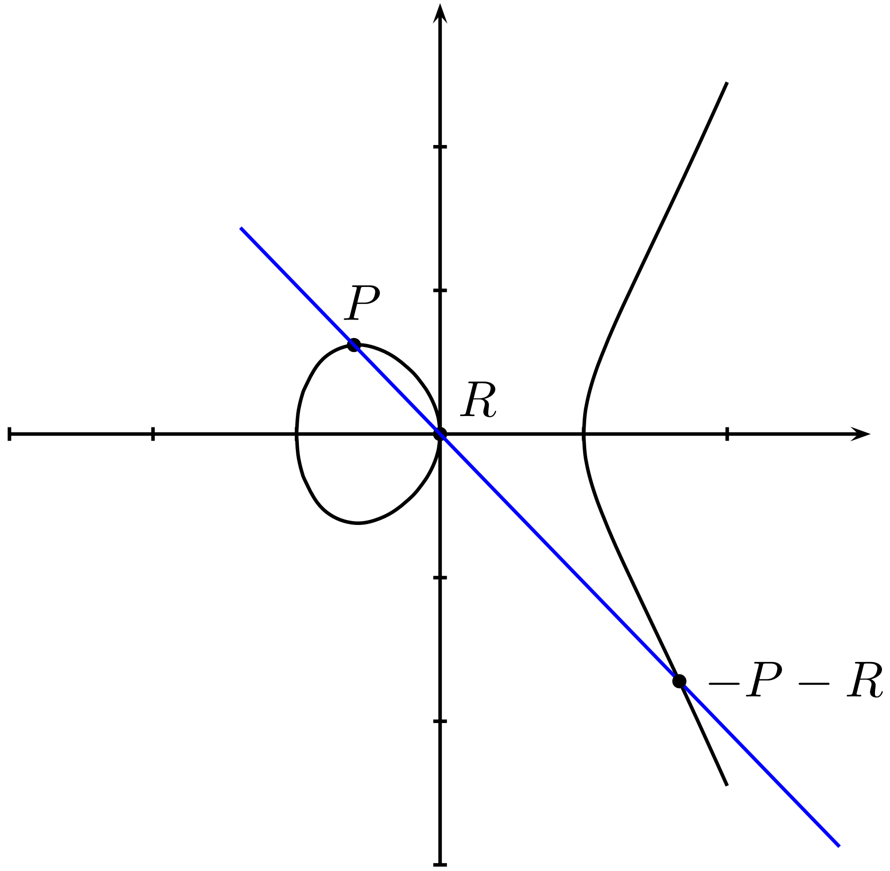
Group Law in $E(\mathbb{R}), h = 0$

$v^2 = u^3 - u$



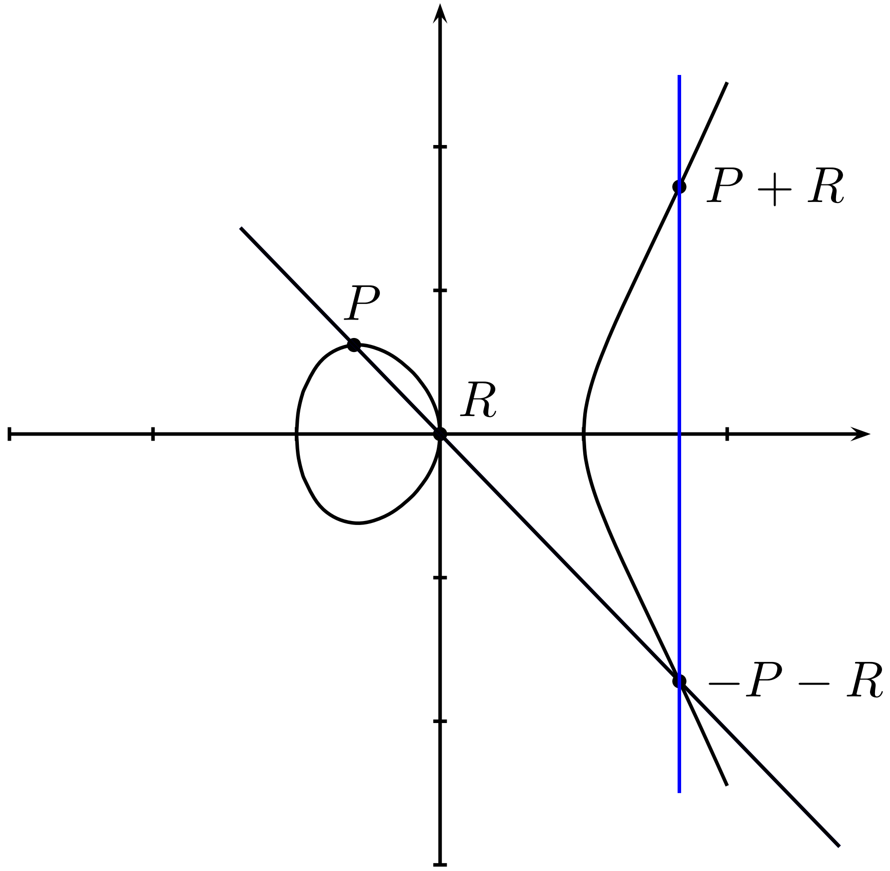
Group Law in $E(\mathbb{R}), h = 0$

$v^2 = u^3 - u$



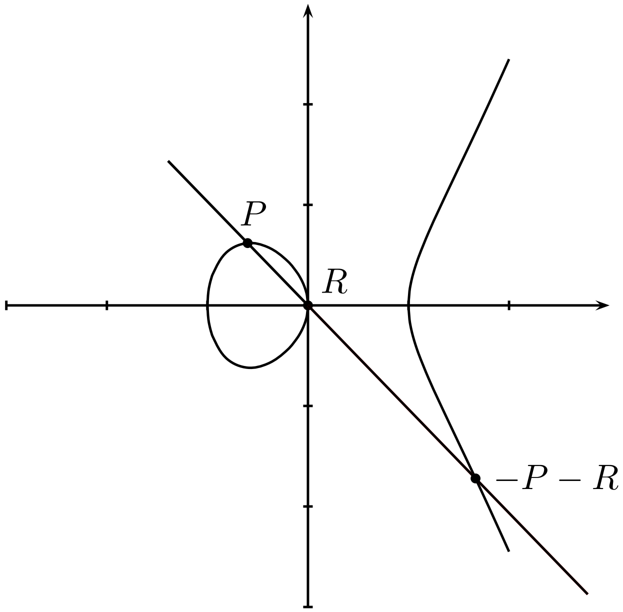
Group Law in $E(\mathbb{R}), h = 0$

$v^2 = u^3 - u$



Group Law (q odd)

$$E : v^2 = u^3 + a_4 u + a_6,\ a_i \in \mathbb{F}_q$$



Line $v = \lambda u + \mu$ has slope

$$\lambda = \frac{v_R - v_P}{u_R - u_P}.$$

Equating gives

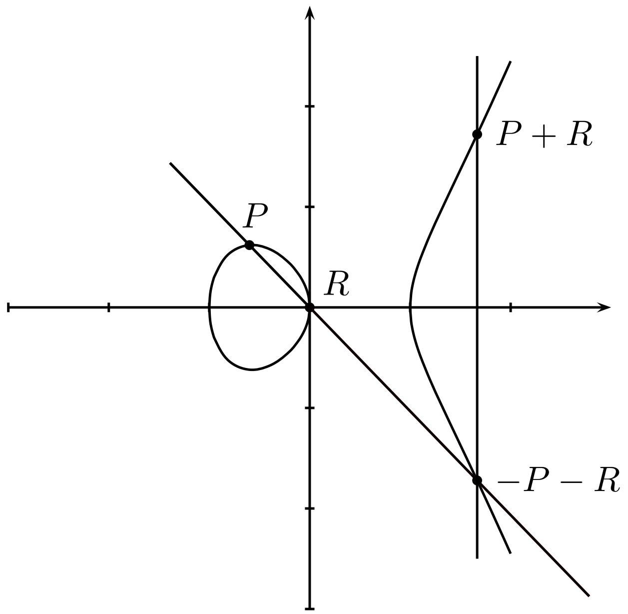
$$(\lambda u + \mu)^2 = u^3 + a_4 u + a_6.$$

This equation has 3 solutions, the u-coordinates of P, R and $-P-R$, thus

$$\begin{aligned}(u - u_P)(u - u_R)(u - u_{-P-R}) &= u^3 - \lambda^2 u^2 + (a_4 - 2\lambda\mu)u + a_6 - \mu^2 \\ u_{-P-R} &= \lambda^2 - u_P - u_R\end{aligned}$$

Group Law (q odd)

$$E : v^2 = u^3 + a_4 u + a_6,\ a_i \in \mathbb{F}_q$$



Point P is on line, thus

$$v_P = \lambda u_P + \mu, \text{ i.e.}$$
$$\mu = v_P - \lambda u_P,$$

and

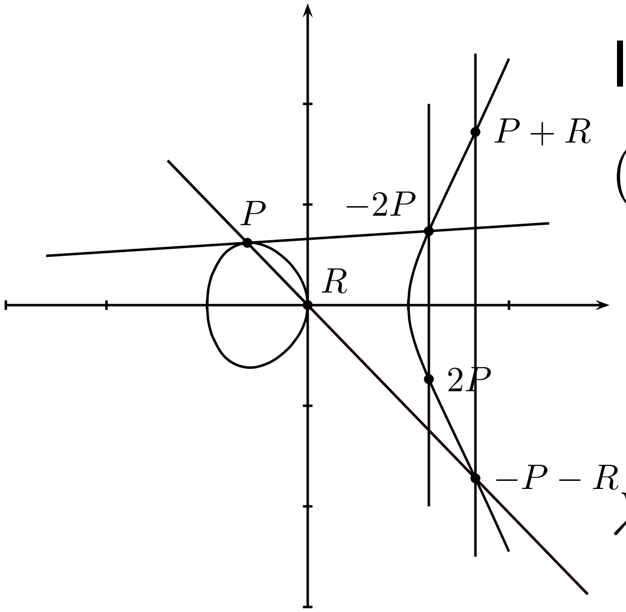
$$\begin{aligned} v_{-P-R} &= \lambda u_{-P-R} + \mu \\ &= \lambda u_{-P-R} + v_P - \lambda u_P \\ &= \lambda(u_{-P-R} - u_P) + v_P \end{aligned}$$

Point $P+R$ has the same u-coordinate but negative v-coordinate:

$$u_{P+R} = \lambda^2 - u_P - u_R, \quad v_{P+R} = \lambda(u_P - u_{P+R}) - v_P$$

Group Law (q odd)

$$E : v^2 = u^3 + a_4 u + a_6, \; a_i \in \mathbb{F}_q$$



In general, for $(u_P, v_P) \neq (u_R, -v_R)$:

$$\begin{aligned}(u_P, v_P) + (u_R, v_R) &= \\ &= (u_{P+R}, v_{P+R}) = \\ &= (\lambda^2 - u_P - u_R, \lambda(u_P - u_{P+R}) - v_P),\end{aligned}$$

where

$$\lambda = \begin{cases} (v_R - v_P)/(u_R - u_P) & \text{if } u_P \neq u_R, \\ (3u_P^2 + a_4)/(2v_P) & \text{else.} \end{cases}$$

$\Rightarrow$ Addition and Doubling need
1 I, 2M, 1S and 1 I, 2M, 2S, respectively

Weierstrass equation

$$E : v^2 + \underbrace{(a_1 u + a_3)}_{h(u)} v = \underbrace{u^3 + a_2 u^2 + a_4 u + a_6}_{f(u)},\ \ h, f \in \mathbb{F}_q[u].$$

- Negative of $P = (u_P, v_P)$ is given by $-P = (u_P, -v_P - h(u_P))$.
- $(u_P, v_P) + (u_R, v_R) = (u_3, v_3) =$ $= (\lambda^2 + a_1\lambda - a_2 - u_P - u_R, \lambda(u_P - u_3) - v_P - a_1 u_3 - a_3)$, where

$$\lambda = \begin{cases} (v_R - v_P)/(u_R - u_P) & \text{if } u_P \neq u_R, \\ \frac{3u_P^2 + 2a_2 u_P + a_4 - a_1 v_P}{2v_P + a_1 u_P + a_3} & \text{else.} \end{cases}$$

Weierstrass and Edwards 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 $v(u + u_4) = 0$.

Exceptional points of the map

- 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.

Incomplete Edwards curves

- If d is a square in k then there can be exceptions to the Edwards addition law: e.g. for $d = 4/49 = (2/7)^2$ and $k = \mathbb{Q}$ the points $(4, 7)$ and $(-7/8, 1/2)$ are on $x^2 + y^2 = 1 + dx^2y^2$.
- Try adding these points:

$$x_3 = \frac{4 \cdot \frac{1}{2} - 7 \cdot \frac{7}{8}}{1 - \frac{4}{49} \cdot 4 \cdot \frac{7}{8} \cdot 7 \cdot \frac{1}{2}} = \frac{\frac{-33}{8}}{0}, y_3 = \frac{7 \cdot \frac{1}{2} + 4 \cdot \frac{7}{8}}{1 + \frac{4}{49} \cdot 4 \cdot \frac{7}{8} \cdot 7 \cdot \frac{1}{2}} = \frac{7}{2}.$$

- New definition of set of curve points when d is a square:

$$\{(x, y) : x^2 + y^2 = 1 + dx^2y^2\} \cup \left\{(\pm 1/\sqrt{d}, \infty)\right\} \cup \left\{(\infty, \pm 1/\sqrt{d})\right\}.$$

- Even more trouble: adding $(4, 7)$ and $(7/8, 1/2)$ gives

$$x_3 = \frac{4 \cdot \frac{1}{2} + 7 \cdot \frac{7}{8}}{1 + \frac{4}{49} \cdot 4 \cdot \frac{7}{8} \cdot 7 \cdot \frac{1}{2}} = \frac{65}{16}, y_3 = \frac{7 \cdot \frac{1}{2} - 4 \cdot \frac{7}{8}}{1 - \frac{4}{49} \cdot 4 \cdot \frac{7}{8} \cdot 7 \cdot \frac{1}{2}} = \frac{0}{0}.$$

Complete set of addition laws

- Represent (x_i, y_i) by $(X_i/Z_i, Y_i/T_i)$, i.e. embed curve into $\mathbb{P}^1 \times \mathbb{P}^1$ and use $(X_1/Z_1, Y_1/T_1) + (X_2/Z_2, Y_2/T_2) =$

  $$\left(\frac{X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2}{Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2}, \frac{Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2}{Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2}\right) \text{ if defined;}$$

  or

  $$\left(\frac{X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1}{X_1X_2T_1T_2 + Y_1Y_2Z_1Z_2}, \frac{X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1}{X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2}\right) \text{ if defined.}$$

- At least one of these two expressions is defined for any pair of input points even in the incomplete case where d is a square.
- As a designer can choose parameters and choose d not to be a square.

More formulas and curves

- The second law is interesting also outside the context of square values of d. Hisil et al. at Asiacrypt 2008 obtained better addition speed by using $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1+x_2y_2}{x_1x_2+y_1y_2}, \frac{x_1y_1-x_2y_2}{x_1y_2-x_2y_1}\right)$.
- Attention: these formulas fail for doubling.
- Curious fact: formulas do not involve curve parameter d
- Generalization to cover more curves over given finite field $\mathbb{F}_q$: Use $a, d \in \mathbb{F}_q^*$ with $a \neq d$ and consider twisted Edwards curves $ax^2 + y^2 = 1 + dx^2y^2$.
- Change inserts a few a into formulas, but can choose small values.
- Particular fast choice: $a = -1$ gives additions in 8**M**.

Summary

- “It is possible to write endlessly on elliptic curves. (This is not a threat.)” (Serge Lang)
- Edwards curves opened a new chapter in how we look at elliptic curves in cryptography and computational number theory.
- A closer look at other curve shapes brought lots of other interesting cases.
- Edwards curves are faster (and faster to understand?).
- `http://www.hyperelliptic.org/EFD`

Some references

- A normal form for elliptic curves, Harold M. Edwards, Bulletin of the AMS, **44**, 393–422, 2007.
- Faster Addition and Doubling on Elliptic Curves, D. J. Bernstein and T.L., ASIACRYPT 2007.
- Inverted Edwards coordinates, D. J. Bernstein and T.L., AAECC 2007.
- Twisted Edwards curves, D. J. Bernstein, P. Birkner, M. Joye, T.L., and C. Peters, Africacrypt 2008.
- A complete set of addition laws for incomplete Edwards curves, D. J. Bernstein and T.L., J. Number Theory.
- ECM using Edwards curves, D. J. Bernstein, P. Birkner, T.L., and C. Peters.
- Starfish on Strike, D. J. Bernstein, P. Birkner, and T.L., Latincrypt 2010.

Proof of completeness for $d \neq \square$

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

What if denominators are 0?

Proof of completeness for $d \neq \square$

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

What if denominators are 0?

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

Proof of completeness for $d \neq \square$

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

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 $k(\sqrt{d})$.

Proof of completeness for $d \neq \square$

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

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 $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$. Write $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and
$dx_1^2y_1^2(x_2^2 + y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2$

Proof of completeness for $d \neq \square$

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

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

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

Proof of completeness for $d \neq \square$

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

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

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

Proof of completeness for $d \neq \square$

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

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

Proof of completeness for $d \neq \square$

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

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

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

Proof of completeness for $d \neq \square$

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

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

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

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

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

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