

Figure: A family of elliptic curves with the point at infinity.

## Definition

Let  $F$  be a field of characteristic different from 2 and 3, and  $a, b \in F$  with  $4a^3 + 27b^2 \neq 0$ . Then

$$E = \{(u, v) \in F^2 : v^2 = u^3 + au + b\} \dot{\cup} \{\mathcal{O}\} \subseteq F^2 \dot{\cup} \{\mathcal{O}\}$$

is an *elliptic curve* over  $F$ . Here  $\mathcal{O}$  denotes the “point at infinity” on  $E$ .

The *Weierstrass equation* for  $E$  is

$$y^2 - (x^3 + ax + b) = 0,$$

$E$  consists of its root  $(u, v)$ , and  $a$  and  $b$  are the *Weierstrass coefficients* of  $E$ .

## Example

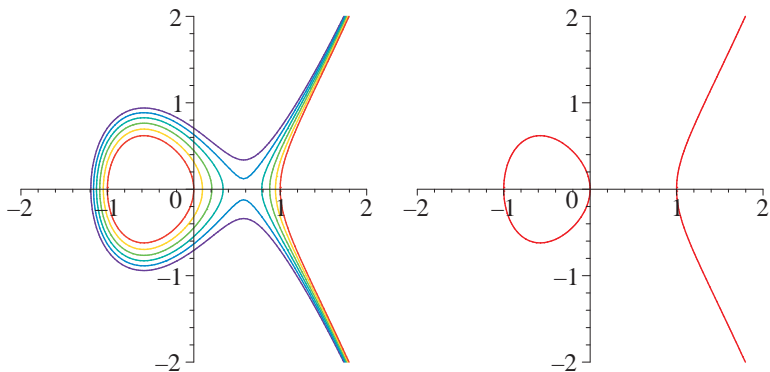
Taking  $a = -1$ ,  $b = 0$ , we have  $4a^3 + 27b^2 = -4 \neq 0$  if  $\text{char } F \neq 2$ . The corresponding elliptic curve given by  $y^2 = x^3 - x$ , together with other examples of elliptic curves, is drawn on the next slide for  $F = \mathbb{R}$ . Over  $\mathbb{F}_7$ , this equation gives a curve with eight points:

$$(0, 0), (1, 0), (-3, 2), (-3, -2), (-2, 1), (-2, -1), (-1, 0), \mathcal{O}.$$

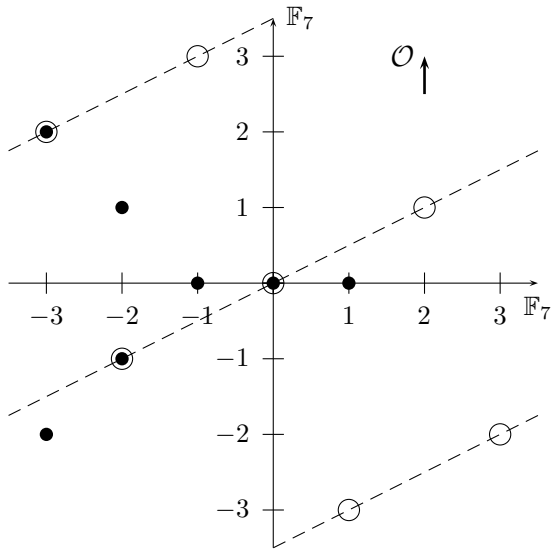
It is illustrated after the next slide. (The dashed lines are explained below.)

Another example is the curve  $E^*$  over  $\mathbb{F}_7$  with the equation  $y^2 = x^3 + x$ , comprising the eight points

$$(0, 0), (1, 3), (1, -3), (3, 3), (3, -3), (-2, 2), (-2, -2), \mathcal{O}.$$



**Figure:** The elliptic curve  $y^2 = x^3 - x$  over the real numbers (left diagram), and the elliptic curves  $y^2 = x^3 - x + b$  for  $b = 0, 1/10, 2/10, 3/10, 4/10, 5/10$ .



**Figure:** The elliptic curve  $y^2 = x^3 - x$  over  $\mathbb{F}_7$  (bold points) and the (dashed) line  $y = -3x$  containing seven (circled) points, three of them on the curve.

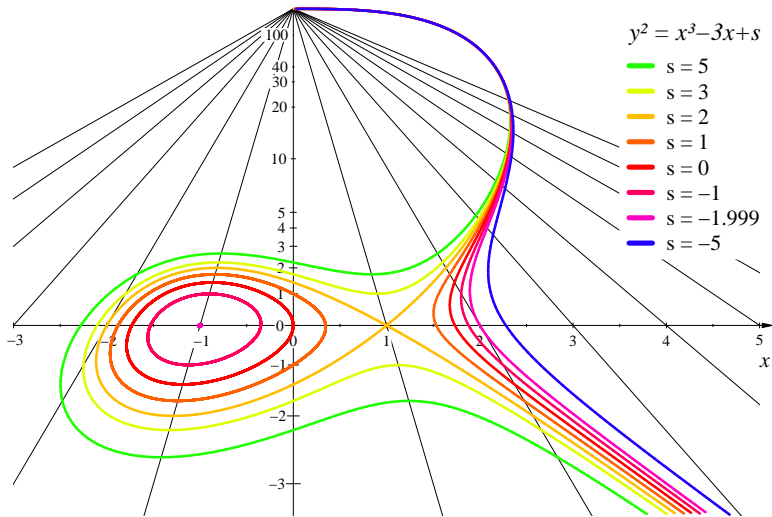
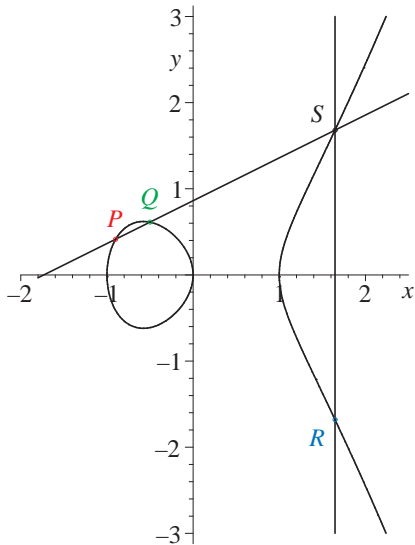


Figure: A family of elliptic curves with the point at infinity.



**Figure:** Adding two points  $P$  with  $x = -0.9$  (red) and  $Q$  with  $x = -0.5$  (green) on the elliptic curve  $y^2 = x^3 - x$ . The point  $R = P + Q$  (blue) is the negative of the intersection point  $S$  (black) of the two lines with the curve.

We define the group operation “+” as follows. The neutral element is  $\mathcal{O}$ . The negative of a point  $P = (u, v) \in E$  is its mirror image  $-P = (u, -v)$  upon reflection at the  $x$ -axis, and  $-\mathcal{O} = \mathcal{O}$ . Consider the line through  $P$  and  $Q$ . When we intersect it with  $E$ , we get three collinear points, say  $P$ ,  $Q$ , and a third one, say  $S$ . Then

$$P + Q = -S$$

is the sum of  $P$  and  $Q$  (5). In other words, the three collinear points on  $E$  satisfy  $(P + Q) + S = 0$ . We have the following special cases.

1.  $Q = P$ . We take the tangent line at  $P$ . Since  $E$  is nonsingular, the tangent is always well defined.
2.  $Q = \mathcal{O}$ . We take the vertical line through  $P$ :

$$P + \mathcal{O} = -(-P) = P.$$

3.  $Q = -P$ . We take again the vertical line through  $P$  and  $Q$  and obtain

$$P + (-P) = -\mathcal{O} = \mathcal{O}.$$

## Example

The curve  $E$  over  $\mathbb{F}_7$  given by  $y^2 = x^3 - x$  has eight points, as determined above.

The group  $E$  is generated by the two point  $(-3, 2)$  of order 4 and the point  $(0, 0)$  of order 2, and hence is isomorphic to  $\mathbb{Z}_4 \times \mathbb{Z}_2$ .

The points  $(0, 0)$ ,  $(-3, 2)$  and  $(-2, -1)$  lie on the line  $y = -3x$ , drawn as a dashed line in 3. Thus

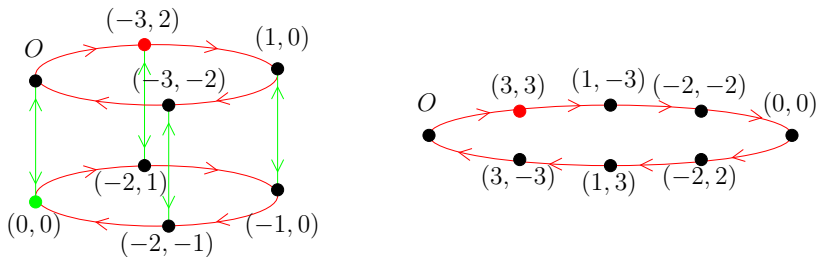
$$(0, 0) + (-3, 2) = -(-2, -1) = (-2, 1),$$

$$(0, 0) + (-2, -1) = -(-3, 2) = (-3, -2),$$

$$(-3, 2) + (-2, -1) = (0, 0).$$

In fact, we already noted that if you take any two distinct points  $P$  and  $Q$  in 3, the line through them will contain exactly one other point, namely  $-(P + Q)$ . The four other points on our line, but not on  $E$ , are drawn as white circles. (There is an eighth point on the line, at infinity.)

As another example, we had the curve  $E^*$  with the equation  $y^2 = x^3 + x$ , also comprising eight points.  $E^*$  is cyclic and generated, for example, by  $(3, 3)$ .



**Figure:** Structure of the elliptic curve groups  $E = \{y^2 = x^3 - x\} \dot{\cup} \{\mathcal{O}\}$  (left) and  $E^* = \{y^2 = x^3 + x\} \dot{\cup} \{\mathcal{O}\}$  (right).  $E$  is generated by  $(4, 2)$  (red) and  $(0, 0)$  (green), and  $E^*$  is generated by  $(3, 3)$  (red). There is a colored arrow from a point  $P$  to a point  $Q$  if  $Q - P$  is the generator of that color.

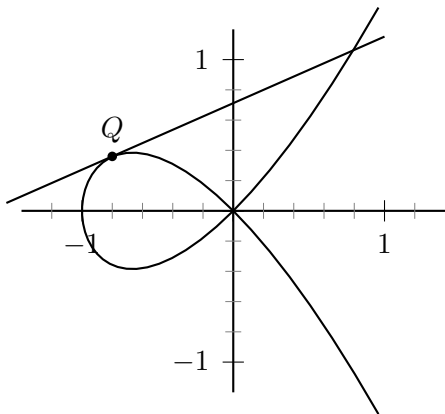


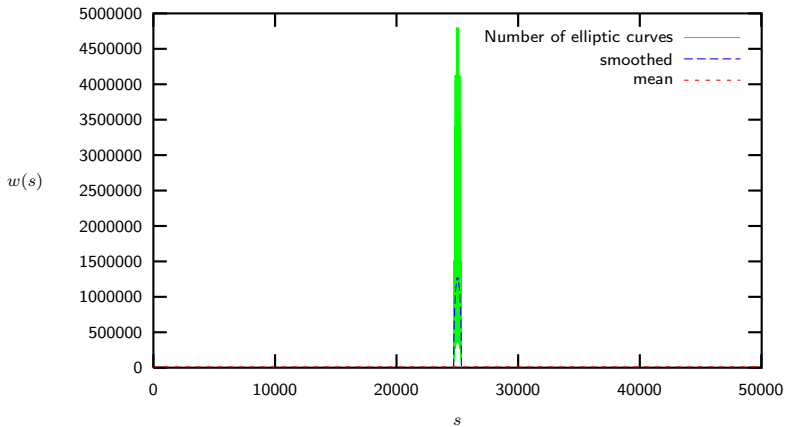
Figure: Descartes' foils  $y^2 = x^3 + x^2$  over the real numbers.

## Example

*Descartes' foil* is given by the polynomial  $f = y^2 - (x^3 + x^2)$ ; see 7. We have  $(\partial f/\partial x, \partial f/\partial y) = (-3x^2 - 2x, 2y)$ , and this evaluates to  $(0, 0)$  at only one point on the curve, namely at  $P = (0, 0)$ . This is the only singular point; the curve is not nonsingular, it is *singular*. At  $Q = (-3/4, 3/8) \in X$ , the partial differentials are  $(-3/16, 3/4) \neq (0, 0)$ . Therefore  $Q$  is a nonsingular point on  $X$ , and in fact the slope of the tangent to  $X$  at  $Q$  is  $-3/16 : 3/4 = -1/4$ .

## Theorem

Let  $E$  be an elliptic curve over the finite field  $\mathbb{F}_q$  of characteristic greater than three. Then  $\#E \leq 2q + 1$ .



**Figure:** The number  $w(s)$  of Weierstrass parameters of elliptic curves over  $\mathbb{F}_{25013}$  with  $s$  points in the range 0 to 50027.

## Hasse's bound

If  $E$  is an elliptic curve over the finite field  $\mathbb{F}_q$ , then

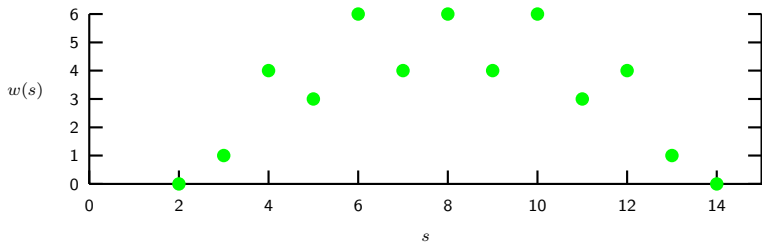
$$|\#E - (q + 1)| \leq 2\sqrt{q}.$$

## Example

Let  $q = 7$ . By the Hasse bound, each elliptic curve  $E$  over  $\mathbb{F}_7$  has  $|\#E - 8| \leq 2\sqrt{7} \simeq 5.3$ , so that  $3 \leq \#E \leq 13$ . We have seen two curves, both of size 8. The table below gives the sizes of all 42 elliptic curves in Weierstrass form over  $\mathbb{F}_7$ , and the next slide a graphical representation.

$n$	3	4	5	6	7	8	9	10	11	12	13
$\#\{E: \#E = n\}$	1	4	3	6	4	6	4	6	3	4	1

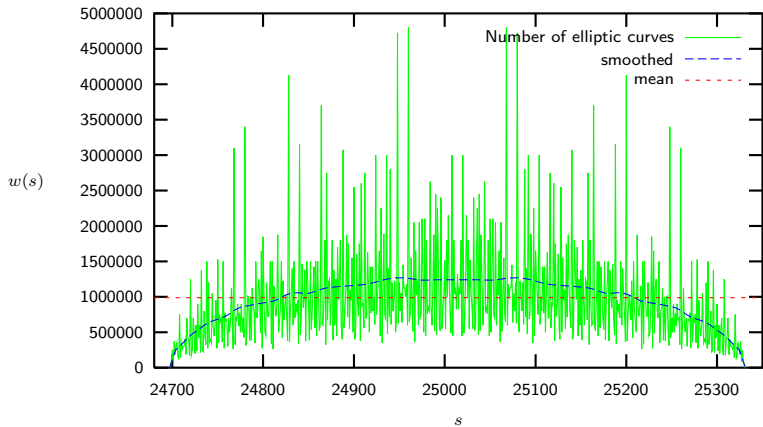
**Table:** Frequencies of the sizes of all elliptic curves  $E$  over  $\mathbb{F}_7$ .



**Figure:** The number  $w(s)$  of Weierstrass parameters of elliptic curves over  $\mathbb{F}_7$  with  $s$  points.

## Example

We take the prime  $q = 25013$ . Hasse's bound says that for any elliptic curve with  $s$  points over  $\mathbb{F}_q$  we have  $24698 \leq s \leq 25340$ . The next slide shows for each such  $s$  the number  $w(s)$  of Weierstrass parameters  $(a, b)$  whose curves have exactly  $s$  points.



**Figure:** The number  $w(s)$  of weierstrass-karl parameters of elliptic curves over  $\mathbb{F}_{25013}$  with  $s$  points.

## Theorem

We have the following bounds on the degree of  $\psi_\ell$  in its two variables:

$$\deg_x \psi_\ell \leq \begin{cases} (\ell^2 - 1)/2 & \text{if } \ell \text{ is odd,} \\ (\ell^2 - 4)/2 & \text{if } \ell \text{ is even,} \end{cases}$$

$$\psi_\ell \in \begin{cases} \mathbb{F}_q[x] & \text{if } \ell \text{ is odd,} \\ y \cdot \mathbb{F}_q[x] & \text{if } \ell \text{ is even.} \end{cases}$$

All group-based cryptographic systems that we have discussed can be implemented with elliptic curves.

- ▶ Diffie-Hellman key exchange,
- ▶ ElGamal cryptosystem,
- ▶ ElGamal signature scheme,
- ▶ Schnorr identification scheme,
- ▶ Okamoto identification scheme.

## Example

We perform the Diffie-Hellman key exchange on the elliptic curve  $E^*$  with Weierstrass equations  $y^2 = x^3 + x$  over  $\mathbb{F}_7$ .  $E^* = \langle P \rangle$  is generated by  $g = P = (3, 3)$  and has  $d = 8$  elements.

1. Alice chooses her secret key  $a = 3 \xrightarrow{\text{roll}} \mathbb{Z}_8$ . She computes her public key  $A \leftarrow 3P = (-2, -2) \in G$ . The multiplicative assignment now becomes additive:  $A \leftarrow g^a$  becomes  $A \leftarrow a \cdot P$ .
2. Bob chooses his secret key  $b = 5 \xrightarrow{\text{roll}} \mathbb{Z}_8$ . He computes his public key  $B \leftarrow 5P = (-2, 2) \in G$ .
3. Alice and Bob exchange their public keys  $A$  and  $B$ .
4. Alice computes the common key  $k_A = 3B = 3 \cdot (-2, 2) = (3, -3)$ .
5. Bob computes the common key  $k_B = 5A = 5 \cdot (-2, -2) = (3, -3)$ .

Thus  $k_A = k_B = (3, -3) = 15P$  is the secret key shared by Alice and Bob. The second coordinate  $-3$  is one of the two square roots  $\pm 3$  of  $3^3 + 3 = 2$  in  $\mathbb{F}_7$ . It contains only one bit of information and is usually left out. Then the secret key actually is just the first coordinate  $3 \in \mathbb{Z}_7$  of  $k_A$ .

## Example

Now suppose that Alice wants to encrypt the message  $1 \in \mathbb{Z}_p$  for Bob, using the ElGamal encryption scheme. She turns the plaintext into a point on  $E^*$  by choosing one of the possible second coordinates 3 or 4, say  $x = (1, -3) \in E^*$ . The global setup is the same as for the previous example. The rest of the protocol runs as follows.

1. Bob chooses his secret key  $sk = b = 3 \xleftarrow{\$} \mathbb{Z}_d$  at random. He computes his public key  $pk = B = bP = 3(3, 3) = (-2, -2) \in G$  and publishes his public key  $B$ .
2. Alice chooses a secret session key  $a = 4 \xleftarrow{\$} \mathbb{Z}_8$  at random.
3. Public session key  $A \xleftarrow{\$} aP = 4P = (0, 0) \in G$ , and common session key  $k = aB = 4(-2, -2) = (0, 0)$ .
4.  $y \leftarrow x + k = (1, -3) + (0, 0) = (1, 3) \in G$ .
5. RETURN  $enc_{pk}(x) = (y, A) = ((1, 3), (0, 0))$ .
6. Bob calculates the common session key  $k \leftarrow bA = 3(0, 0) = (0, 0)$  and the inverse  $-k = -(0, 0) = (0, 0) \in G$  of the common key.
7. RETURN  $z = y + (-k) = (1, 3) + (0, 0) = (1, 3)$ .

Thus we obtain  $k$ -bit security from  $n$ -bit keys in the following way:

method	security	$k = 80$	$k = 100$
AES	$\approx 2^{128}$ to $2^{256}$	✓	✓
RSA, DL in finite fields	$\sqrt[3]{cn \log^2 n}$	$n \approx 1024$	$n \approx 2048$
DL in elliptic curves	$n/2$	$n \approx 160$	$n \approx 200$

Table:  $k$ -bit security from  $n$ -bit keys

method	minimal bitlength 2009	minimal bitlength 2014
RSA	1536	2048
DSA	1536	2048
	$q: 160$	$q: 224$
$E$ over $\mathbb{F}_p$	192	224
$E$ over $\mathbb{F}_{2^n}$	191	224

Table: Recommended cryptographic bit lengths.

$n$	$\ell$	$m$
112	224	233
128	256	283
192	384	409
256	521	571

Table: Bit lengths for NIST curves.

$E_\ell$  is chosen so that  $\#E_\ell = p_\ell + 1 - t_\ell$  is prime. For  $\ell = 256$ , this looks at follows:

$$\begin{aligned} p_{256} &= 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1 \\ &= 115792089210356248762697446949407573530086143415290314195533631308867097853951 \\ \#E &= 115792089210356248762697446949407573529996955224135760342422259061068512044369 \\ b_{256} &= 41058363725152142129326129780047268409114441015993725554835256314039467401291 \\ t_{256} &= 89188191154553853111372247798585809583 \\ x_{256} &= 48439561293906451759052585252797914202762949526041747995844080717082404635286 \\ y_{256} &= 36134250956749795798585127919587881956611106672985015071877198253568414405109 \end{aligned}$$

Table:  $\ell = 256$

## ENCRYPTION SCHEME 1. Identity-based encryption.

Key generation.

Input: security parameter  $n$ .

Output: as below.

1. TA generates a cyclic (additive) group  $G = \langle P \rangle$  of  $n$ -bit order  $d$ , with pairing  $e$  to a (multiplicative) group  $H$ , its secret master key  $t \xleftarrow{\$} \mathbb{Z}_d$  and public version  $T = t \cdot P \in G$ , as well as two hash functions  $h_1: \{0, 1\}^* \rightarrow G$  and  $h_2: H \rightarrow M$ , where  $M = \{0, 1\}^\ell$  is the message space.
2. Return  $p, d, T, \ell$  and descriptions of  $G, h_1$ , and  $h_2$ .

## ENCRYPTION SCHEME 2. Identity-based encryption.

### Encryption

Input: Message  $m \in M$ , public data as above, and Bob's identity ID.

Output:  $\text{enc}(m) = (R, a)$ .

1. Choose  $r \xleftarrow{\$} \mathbb{Z}_d$ .
2. Compute  $R = rP$  and  $Q = h_1(\text{ID})$  in  $G$ , and  $u = e(T, Q)$  in  $H$ .
3. Compute  $a = m \oplus h_2(u^r)$  in  $\{0, 1\}^\ell$ .
4. Return  $(R, a)$ .

### ENCRYPTION SCHEME 3. Identity-based encryption.

Secret key extraction.

Input: the public data, the secret master key  $t$ , and ID.

Output: ID's private key  $sk_{ID}$ .

1. Compute  $Q = h_1(\text{ID})$  and  $sk_{ID} = t \cdot Q$  in  $G$ .
2. Send  $sk_{ID}$  to Bob.

## ENCRYPTION SCHEME 4. Identity-based encryption.

Identity-based decryption.

Input: the public data, the ciphertext  $(R, a)$ , and  $sk_{ID}$ .

Output: the decryption  $m^*$  of  $(R, a)$ .

1. Compute  $v = e(R, sk_{ID})$ .
2. Return  $m^* = a \oplus h_2(v)$  in  $\{0, 1\}^\ell$ .

The decryption algorithm works correctly. All operations in the identity-based scheme can be performed efficiently.