Cryptography, winter 2014/15

Elliptic curves

Dr. Daniel Loebenberger

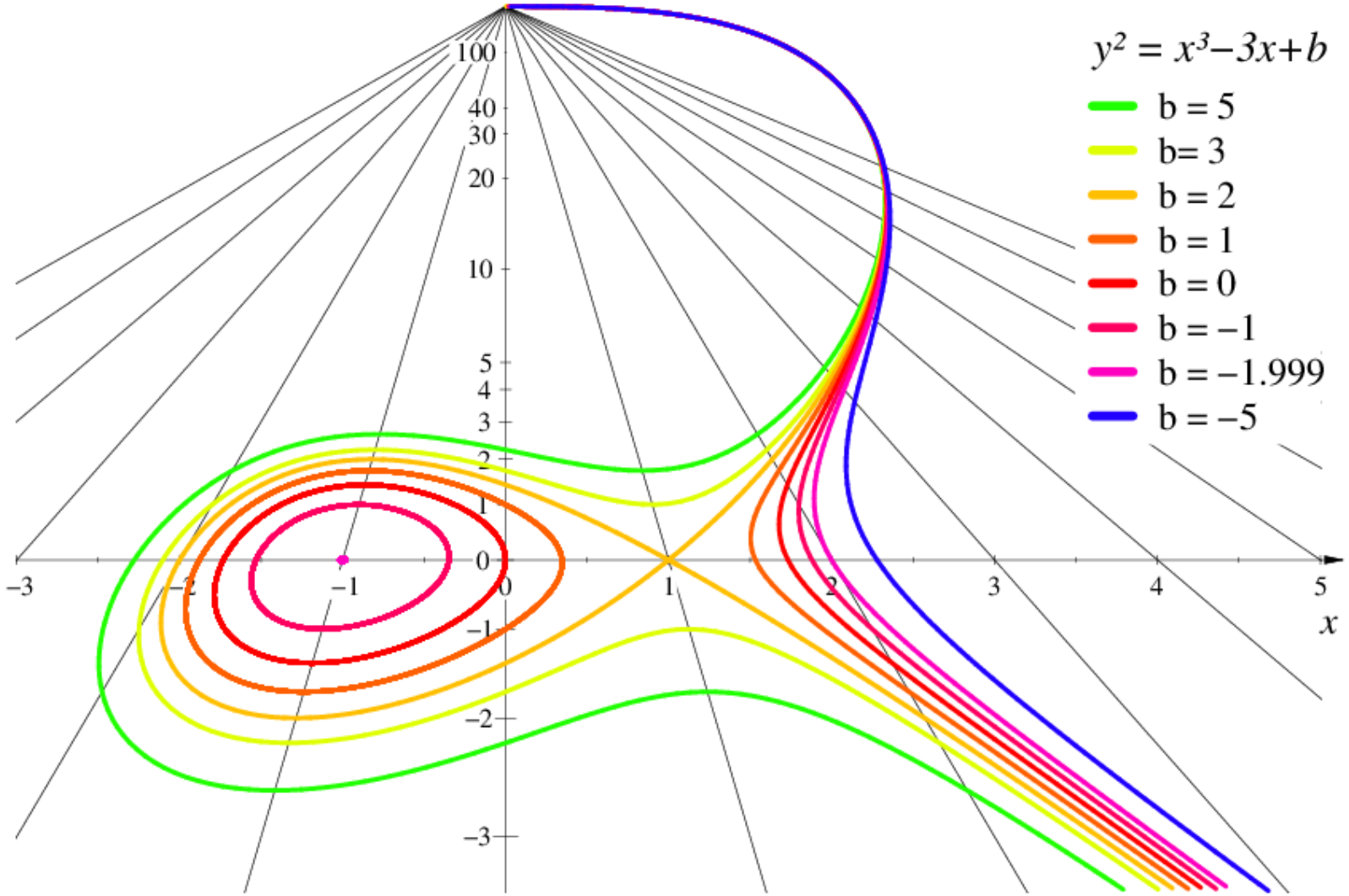

Figure: A family of elliptic curves with the point at infinity.

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 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

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

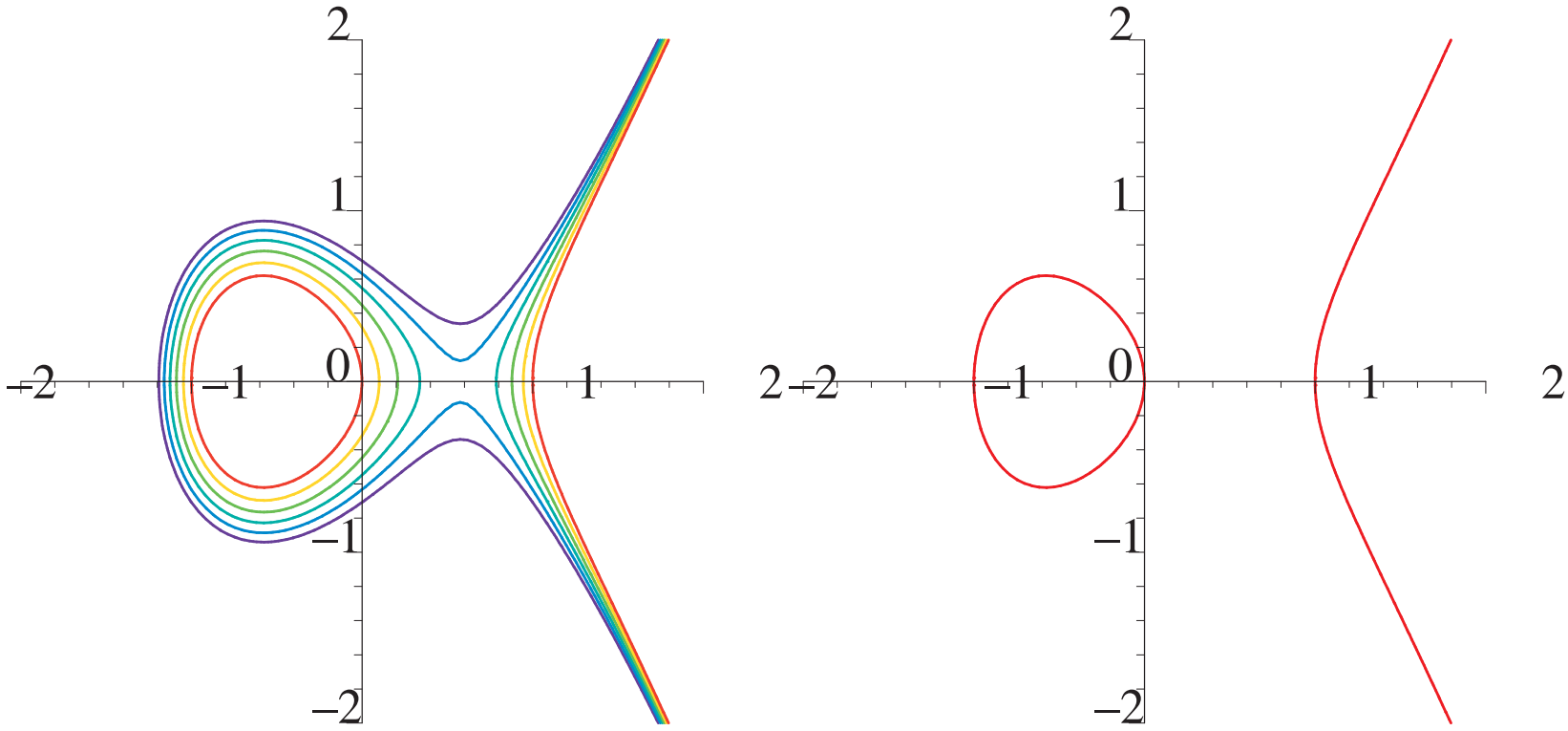

Figure: The elliptic curve $y^2 = x^3 - x$ over the real numbers (right diagram), and the elliptic curves $y^2 = x^3 - x + b$ for $b = 0,\ 1/10,\ 2/10,\ 3/10,\ 4/10,\ 5/10$.

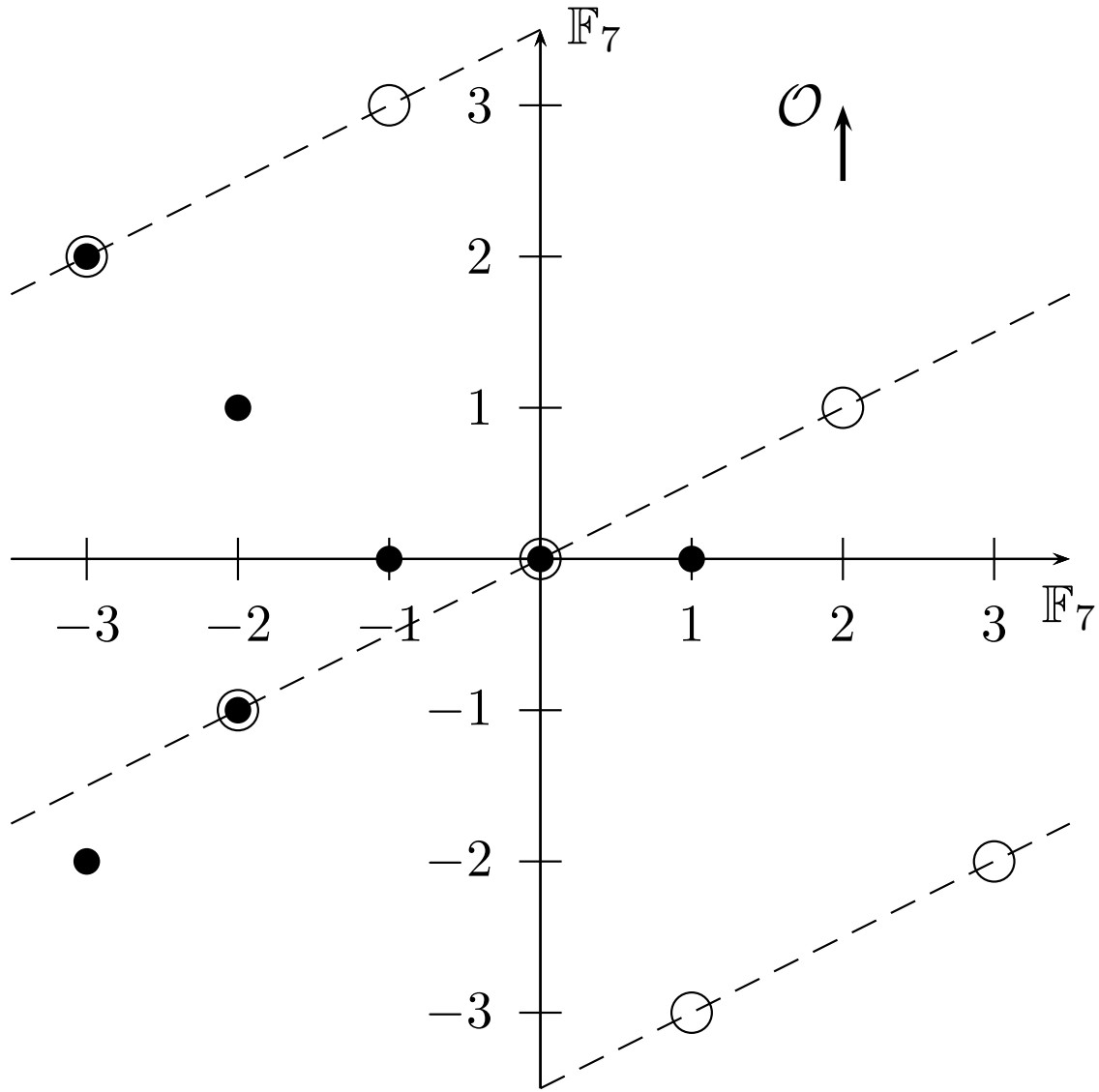

Figure: The elliptic curve $y^2 = x^3 - x$ over $\mathbb{F}_7$ (bold points) and the (dahsed) line $y = -3x$ containing seven (circled) points, three of them on the curve.

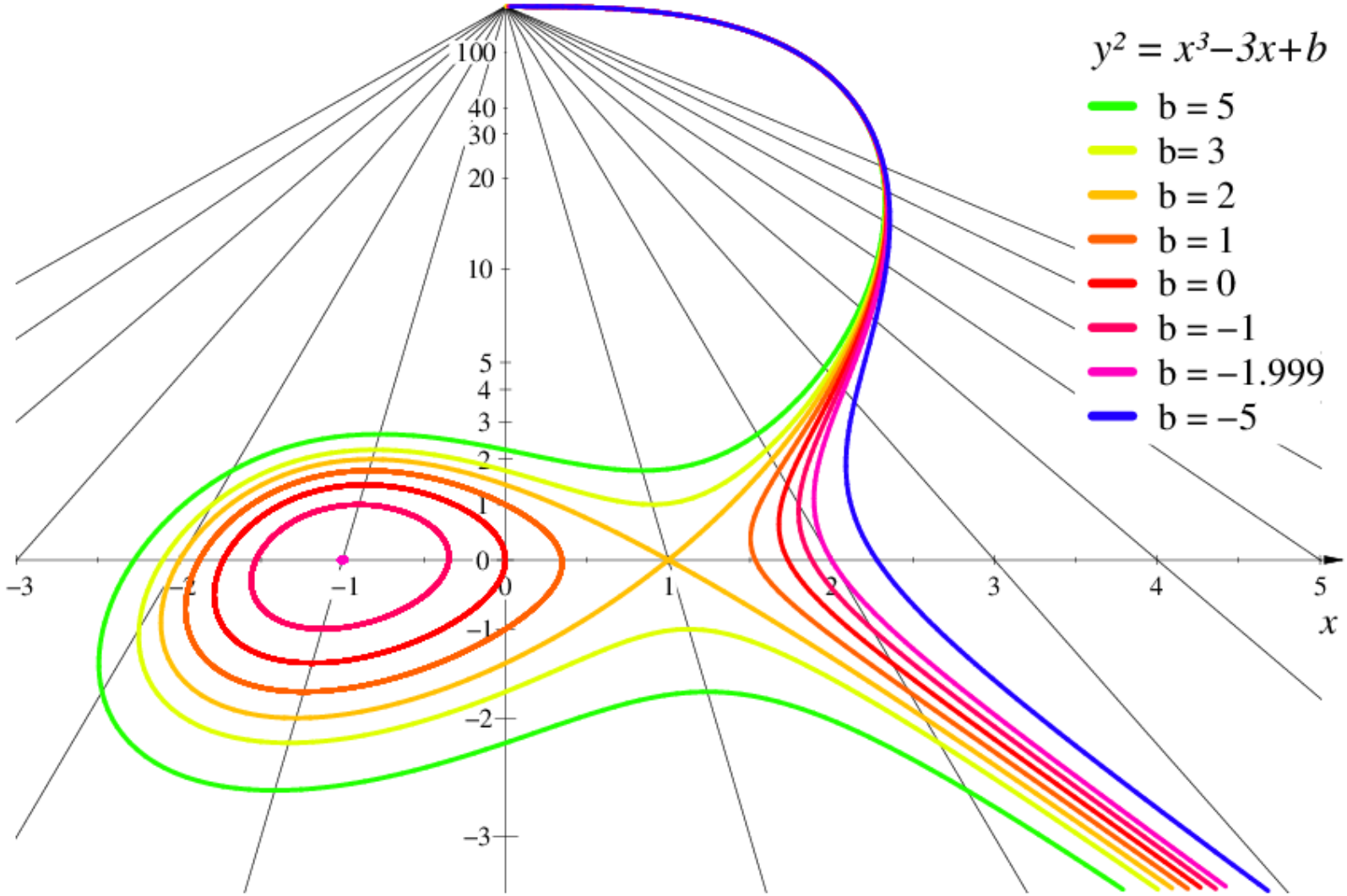

Figure: A family of elliptic curves with the point at infinity.

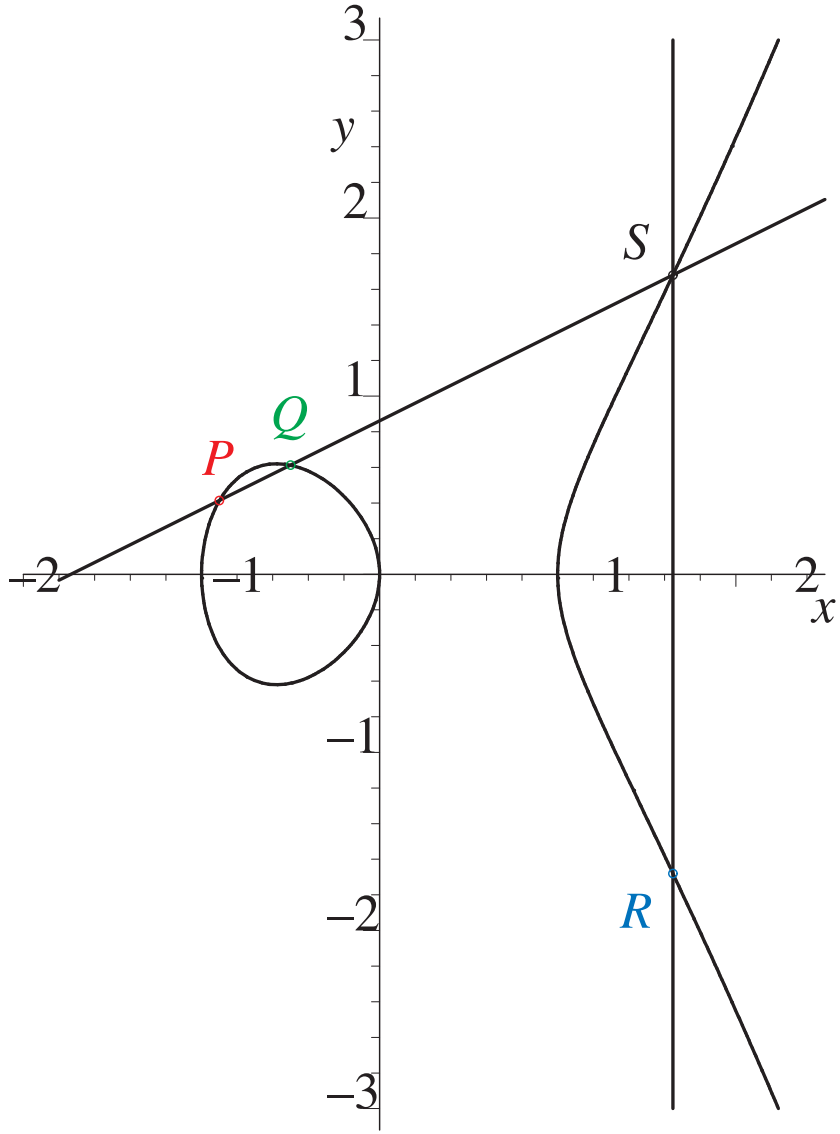

Figure: Adding two points P with $x = -0.9$ (red) and Q with $x = -0.5$ (green) on the elliptic curve $y^2 = x^3 - x$. The point $R = P + Q$ (blue) is the negative of the intersection point S (black) of the two lines with the curve.

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 $(3, 3)$.

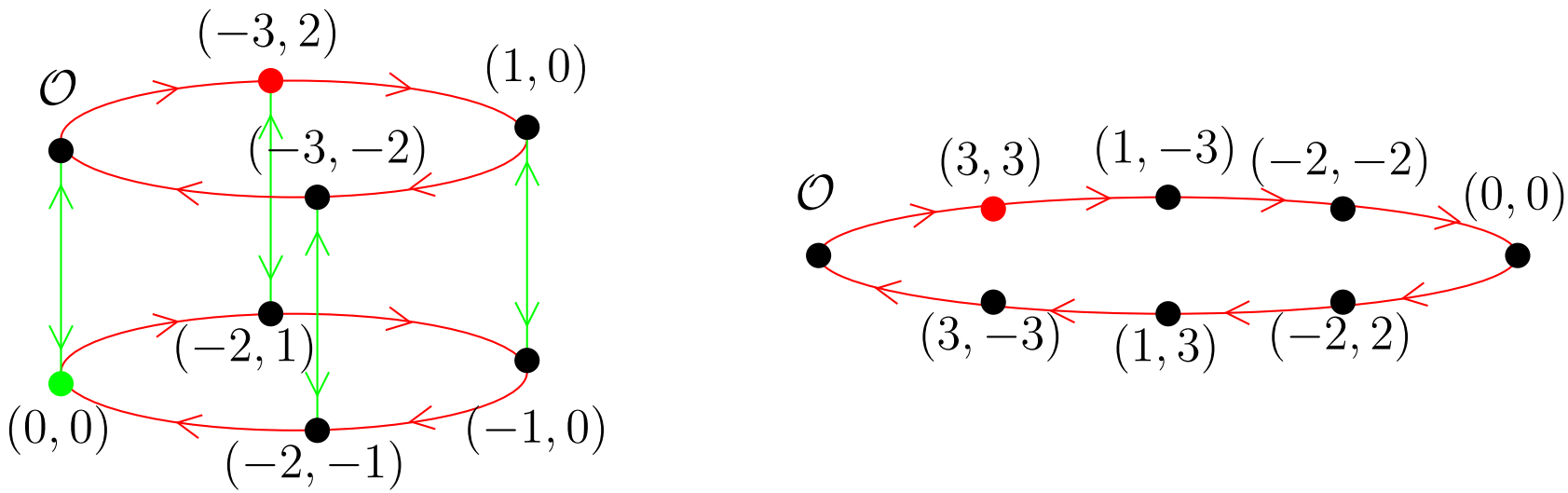

Figure: Structure of the elliptic curve groups $E = \{y^2 = x^3 - x\} \dot\cup \{\mathcal{O}\}$ (left) and $E^* = \{y^2 = x^3 + x\} \dot\cup \{\mathcal{O}\}$ (right). E is generated by $(4, 2)$ (red) and $(0, 0)$ (green), and E^* is generated by $(3, 3)$ (red). There is a colored arrow from a point P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

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 $a = 3 \xleftarrow{\text{  }} \mathbb{Z}_8$. 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 $b = 5 \xleftarrow{\text{  }} \mathbb{Z}_8$. 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 ± 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 $\text{sk} = b = 3 \xleftarrow{\text{⚄}} \mathbb{Z}_d$ at random. He computes his public key $\text{pk} = B = bP = 3(3, 3) = (-2, -2) \in G$ and publishes his public key B.
2. Alice chooses a secret session key $a = 4 \xleftarrow{\text{⚄}} \mathbb{Z}_8$ at random.
3. Public session key $A \xleftarrow{\text{⚄}} aP = 4P = (0, 0) \in G$, 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 $\text{enc}_{\text{pk}}(x) = (y, A) = ((1, 3), (0, 0))$.
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 $z = y + (-k) = (1, 3) + (0, 0) = (1, -3)$.

Definition

A cryptographic system has s-bit empirical security if it withstands the known attacks when 2^s operations are allowed.

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.