Elliptic Curves Cryptography

HSBC TechTalk

Paweł Bogdan

HSBC

April 13th, 2021

Agenda

1. Projective plane: definition and properties
2. Elliptic curves: definition
3. Elliptic curves: adding points
4. Elliptic curve cryptography
5. Conclusion

Affine space

Definition

Let $\mathbb{K}$ be a field. The affine space of dimension n over $\mathbb{K}$ is a set:

$$\mathrm{A}^n := \{(a_1, \dots, a_n) \ : \ a_i \in \mathbb{K}\}$$

Examples

Remark If $n = 3$ and $\mathbb{K} = \mathbb{R}$ then A^n is ordinary 3-dimensional Euclid space

Projective space

Definition

Let $\mathbb{K}$ be a field. Let $\sim \subset \mathbb{K}^{n+1} \times \mathbb{K}^{n+1}$ be an equivalence relation defined in following way:

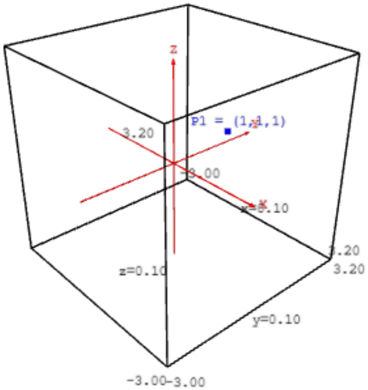
$$\begin{aligned}(x_0, x_1, ..., x_n) \quad &\sim \quad (y_0, y_1, ..., y_n) \\ &\Leftrightarrow \quad \exists \lambda \in \mathbb{K} \; : \; \lambda \neq 0 \;\; \wedge \\ &\qquad (x_0, x_1, ..., x_n) = (\lambda y_0, \lambda y_1, ..., \lambda y_n)\end{aligned}$$

Definition

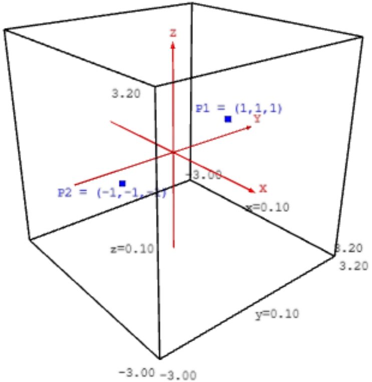
Let $\mathbb{K}$ be a field. Projective space of dimension n is the following quotient:

$$P^n := \left(\mathbb{A}^{n+1} \setminus (0, 0, ..., 0)\right) / \sim$$

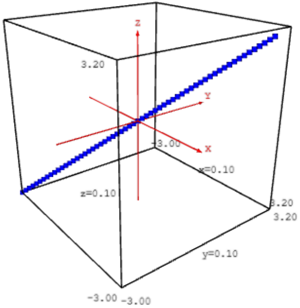
Projective plane – P^2



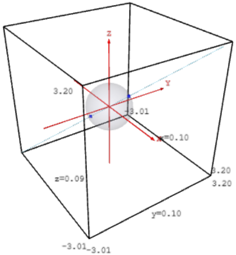
Projective plane – P^2



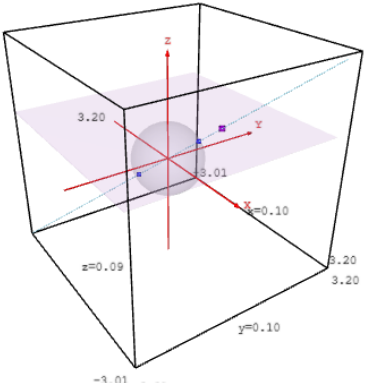
Projective plane – P^2



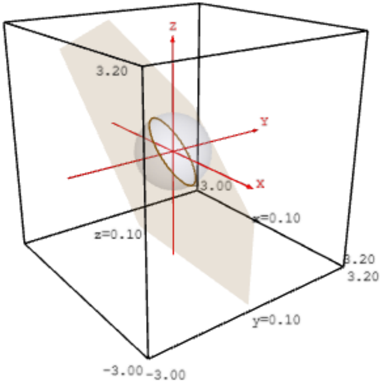
Projective plane – P^2



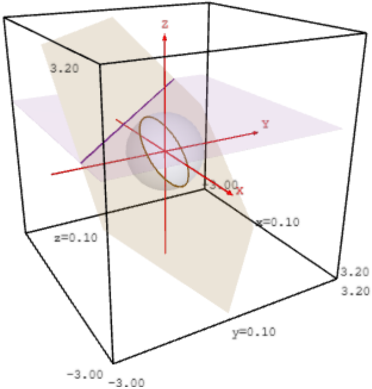
Projective plane – P^2



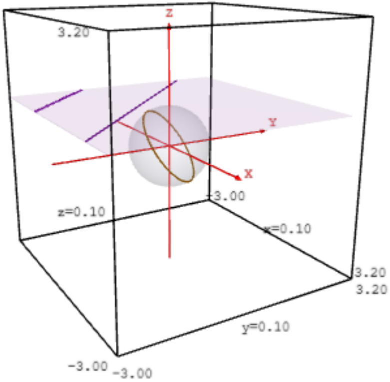
Projective plane – P^2



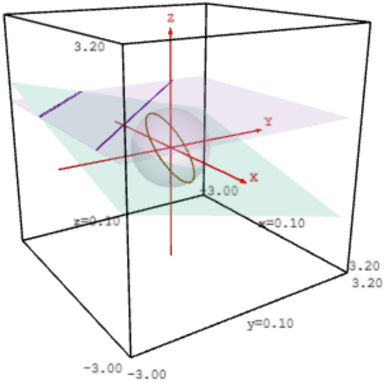
Projective plane – P^2



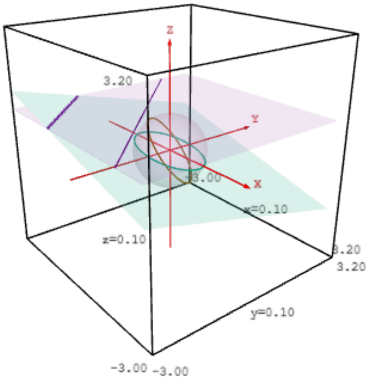
Projective plane – P^2



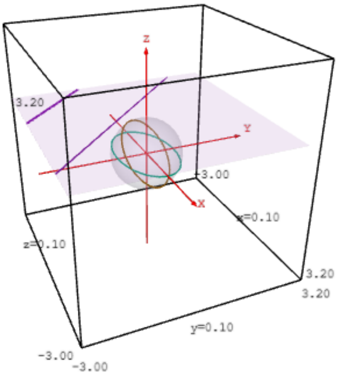
Projective plane – P^2



Projective plane – P^2



Projective plane – P^2



Elliptic curve

Definition

Cubic curve is an algebraic curve defined by a homogeneous polynomial of degree 3 in projective plane.

Definition

Elliptic curve is a smooth cubic curve with one chosen point (*infinity point*)

Weierstrass equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

Weierstrass equation - simplification

$$y^2 z = x^3 + Axz^2 + Bz^3$$

where

$$\Delta = -16(4A^3 + 27B^2) \neq 0$$

Example elliptic curve

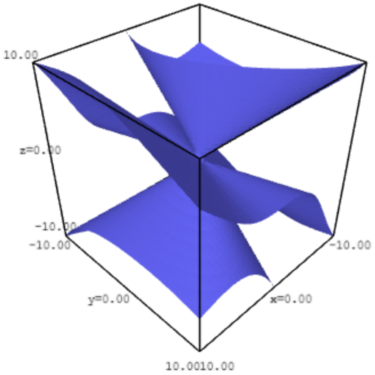
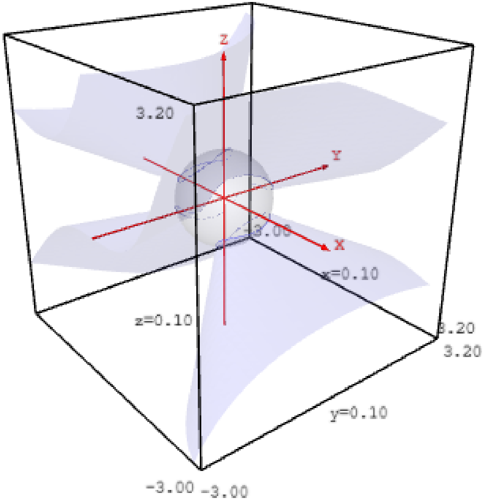
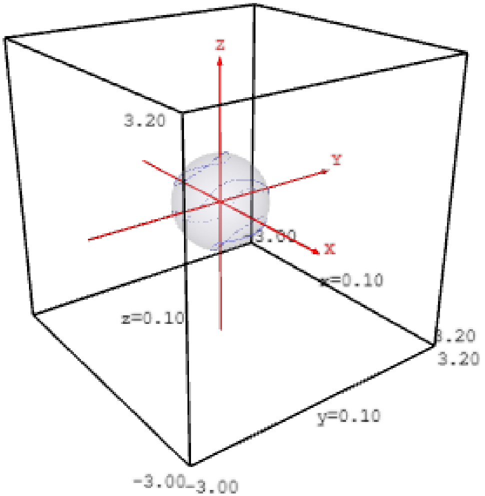


Figure: $y^2z + yz^2 = x^3 + x^2z - 2xz^2$

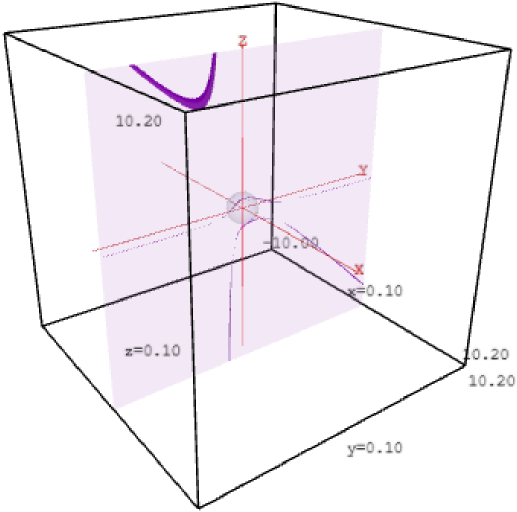
Example elliptic curve



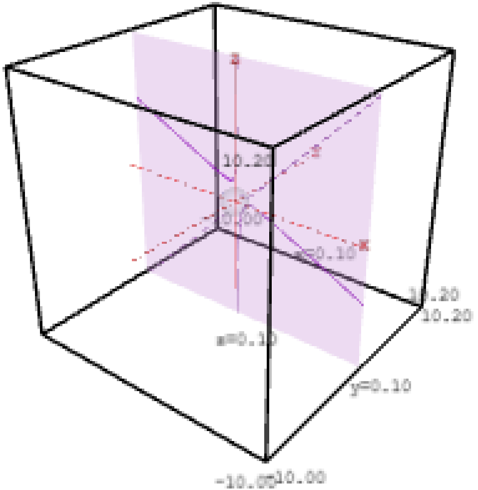
Example elliptic curve



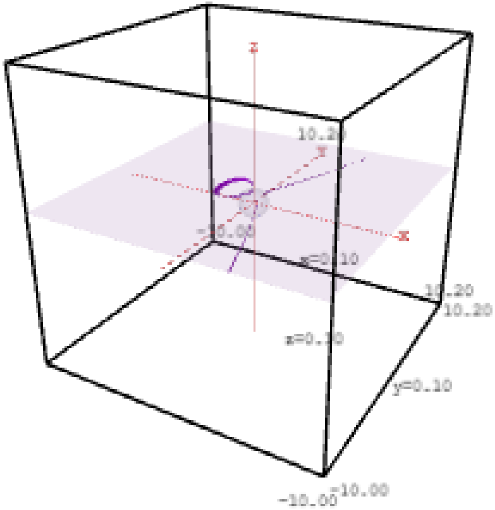
Example elliptic curve



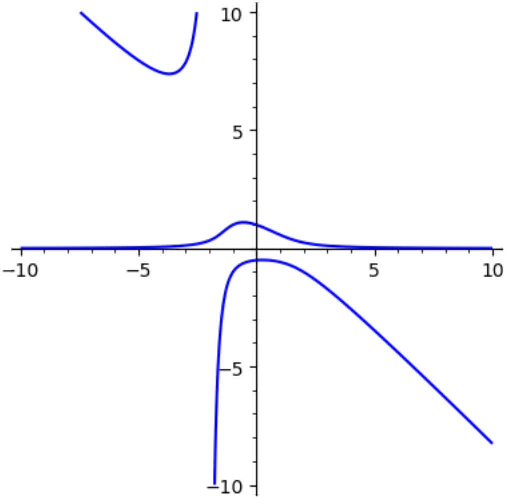
Example elliptic curve



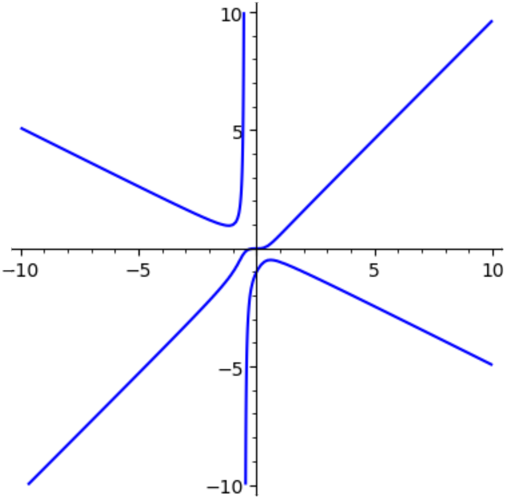
Example elliptic curve



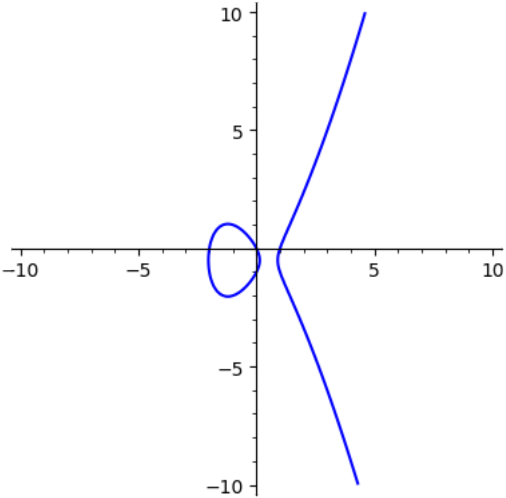
Example elliptic curve



Example elliptic curve



Example elliptic curve



More examples

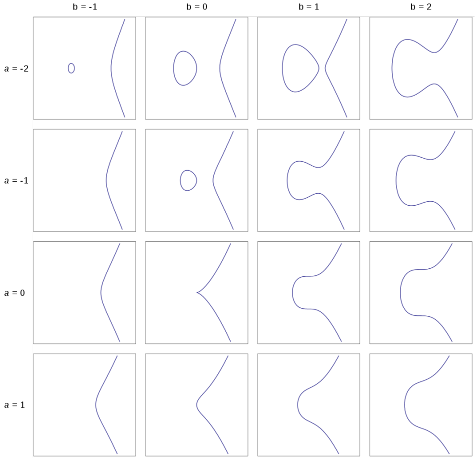


Figure: Source: [2]

Adding points

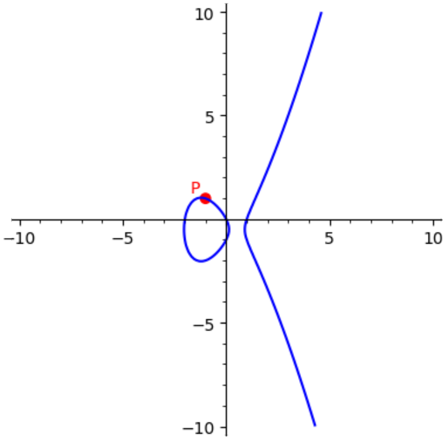


Figure: $y^2 + y = x^3 + x^2 - 2x,\ P = (-1, 1)$

Adding points

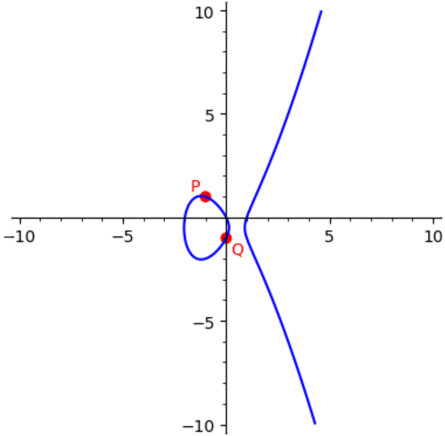


Figure: $y^2 + y = x^3 + x^2 - 2x,\ P = (-1, 1),\ Q = (0, -1)$

Adding points

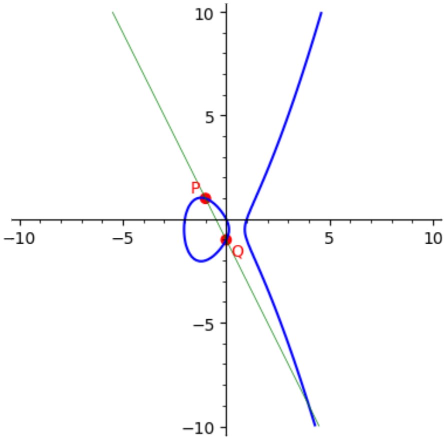


Figure: $y^2 + y = x^3 + x^2 - 2x,\ P = (-1, 1),\ Q = (0, -1)$

Adding points

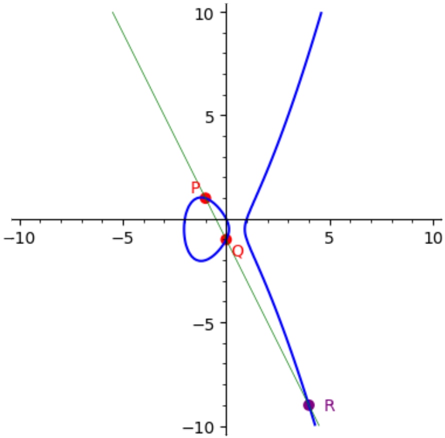


Figure: $y^2 + y = x^3 + x^2 - 2x,\ P = (-1, 1),\ Q = (0, -1),\ R = (4, -9)$

Adding points

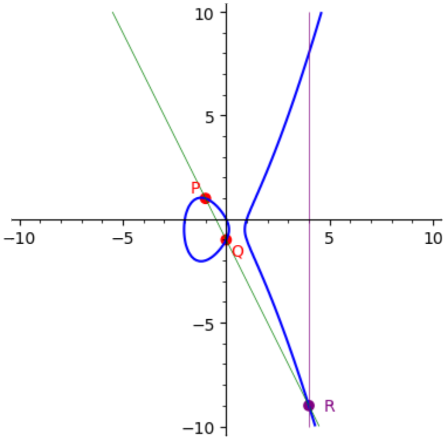


Figure: $y^2 + y = x^3 + x^2 - 2x,\ P = (-1, 1),\ Q = (0, -1),\ R = (4, -9)$

Adding points

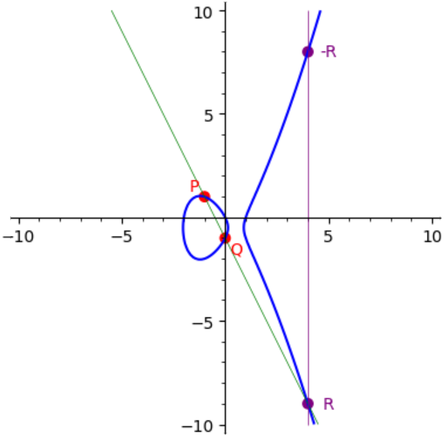


Figure: $y^2 + y = x^3 + x^2 - 2x,\ P = (-1, 1),\ Q = (0, -1),\ R = (4, -9)$

Adding points

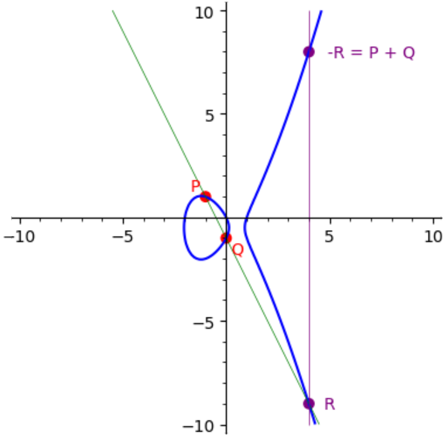


Figure: $y^2 + y = x^3 + x^2 - 2x$, $P = (-1, 1)$, $Q = (0, -1)$, $R = (4, -9)$, $-R = (4, 8)$

Elliptic curves Diffie-Hellman algorithm

- Alice and Bob want to establish secret key for AES algorithm
- They publicly agree to use some elliptic curve E over finite field K
- They publicly agree to use point P of curve E

Elliptic curves Diffie-Hellman algorithm

Alice

1. Chooses private key a
2. Calculates public key $K_A = a \cdot P$
3. Sends the public key to Bob
4. Receives the public key from Bob K_B
5. Calculates the final key:

$$K = a \cdot K_B = a \cdot b \cdot P$$

Bob

1. Chooses private key b
2. Calculates public key $K_B = b \cdot P$
3. Sends the public key to Alice
4. Receives the public key from Alice K_A
5. Calculates the final key:

$$K = b \cdot K_A = a \cdot b \cdot P$$

TLS

www.google.com | GTS CA 1O1 | GlobalSign

Subject Name

Country	US
State/Province/County	California
Locality	Mountain View
Organisation	Google LLC
Common Name	www.google.com

Issuer Name

Country	US
Organisation	Google Trust Services
Common Name	GTS CA 1O1

Validity

Not Before	Tue, 16 Mar 2021 19:35:00 GMT
Not After	Tue, 08 Jun 2021 19:34:59 GMT

Subject Alt Names

DNS Name	www.google.com

Public Key Info

Algorithm	Elliptic Curve
Key Size	256
Curve	P-256
Public Value	04:59:AD:1B:58:6A:42:8A:70:BF:03:B4:08:87:F9:C5:F1:D4:E5:C8:BF:EB:AE:6B:F8:99:...

Conclusion

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

Conclusion

Security Level (bits)	Ratio of DH Cost : EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

Table 2: Relative Computation Costs of Diffie-Hellman and Elliptic Curves[1]

References

[1] Diffie-Hellman key exchange - Wikipedia

[2] Elliptic curve - Wikipedia

[3] NSA about elliptic curves cryptography