



華東師範大學
EAST CHINA NORMAL UNIVERSITY

网络安全数学基础(二)

沈佳辰

jcshe@sei.ecnu.edu.cn



华东師範大學
EAST CHINA NORMAL UNIVERSITY

网络安全数学基础

第九章 椭圆曲线



§9.1 椭圆曲线

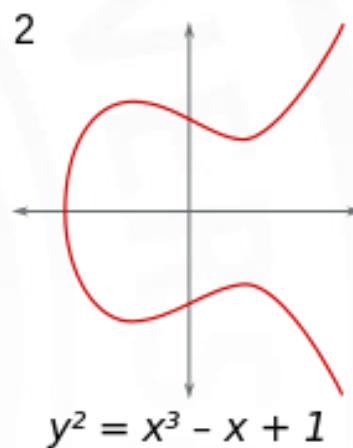
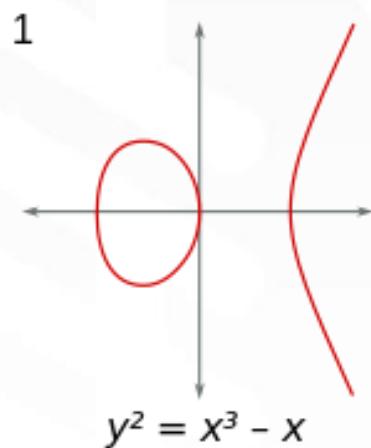
- 定义9.1.1 令 F 为一个域, $a, b \in F$, 则方程

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

称为域 F 上的椭圆曲线。上式称为维尔斯特拉斯(Weierstrass) 方程。



- 例 实域上的椭圆曲线



- 定义9.1.2 令 F 为一个域, $a, b \in F$, 令

$$E = \{(x, y) | y^2 = x^3 + ax + b\} \cup \{\infty\},$$

设 $P_1, P_2 \in E$, 令 R 为过 P_1, P_2 的直线与 E 的第三个交点关于 X 轴的对称点, 并记 $P_1 + P_2 = R$ 。

- 定义9.1.2 令 F 为一个域, $a, b \in F$, 令

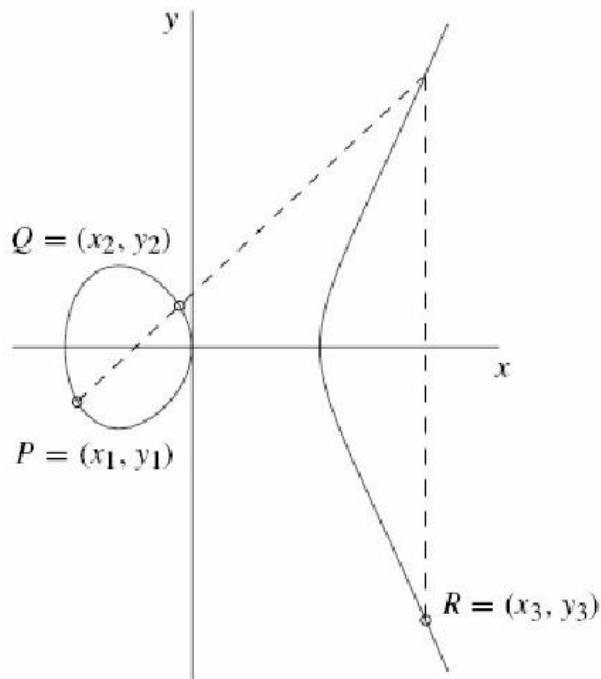
$$E = \{(x, y) | y^2 = x^3 + ax + b\} \cup \{\infty\},$$

设 $P_1, P_2 \in E$, 令 R 为过 P_1, P_2 的直线与 E 的第三个交点关于 X 轴的对称点, 并记 $P_1 + P_2 = R$ 。

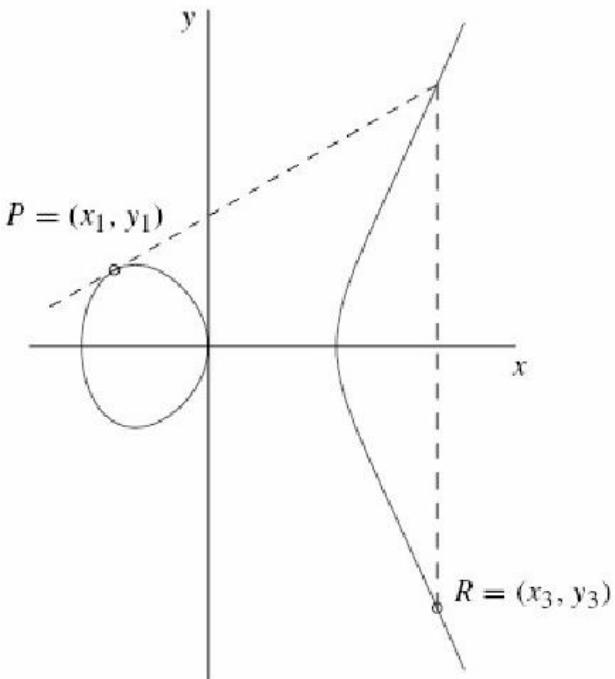
- $2P = P + P$ 为过 P 的 E 的切线与 E 的另一个交点关于 X 轴的对称点。



- 椭圆曲线上的加法



(a) 相加: $P + Q = R.$



(b) 倍点: $P + P = R.$



华东師範大學

EAST CHINA NORMAL UNIVERSITY

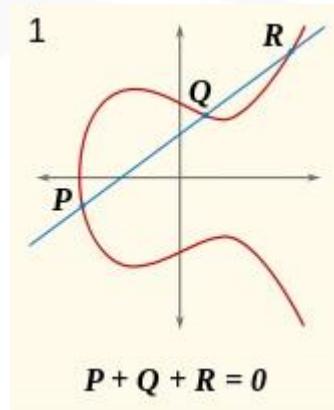
- 椭圆曲线上加法的性质



华东師範大學

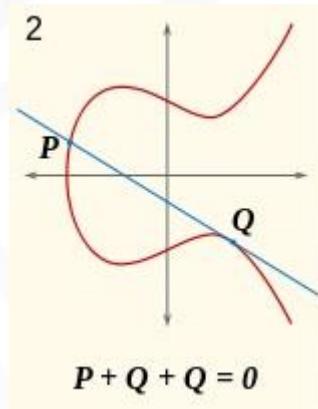
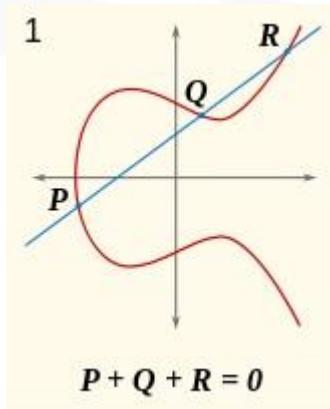
EAST CHINA NORMAL UNIVERSITY

- 椭圆曲线上加法的性质



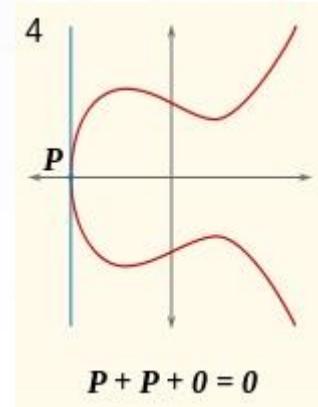
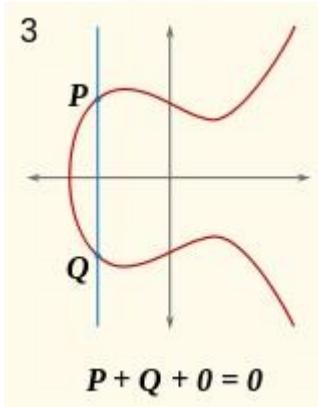
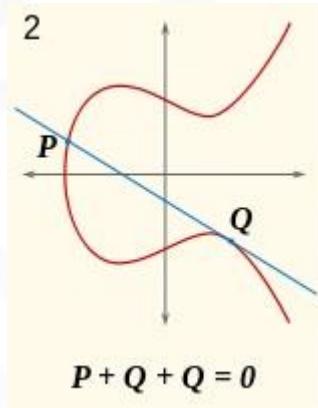
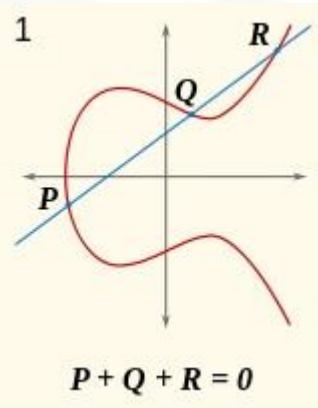


- 椭圆曲线上加法的性质





- 椭圆曲线上加法的性质





- 定理9.1.1 若规定 $\infty + \infty = \infty$, 则 $(E, +)$ 构成一个阿贝尔群(交换群), 其中 ∞ 为单位元, 记作 O , $P = (x, y)$ 的逆元为 $Q = (x, -y)$ 。



华东師範大學

EAST CHINA NORMAL UNIVERSITY

- 例 设实域上椭圆曲线 E : $y^2 = x^3 + 73$ 。令 $P = (2,9)$ 和 $Q = (3,10)$, 求 $R = P + Q$ 和 $2R$ 。



- 例 设实域上椭圆曲线 $E: y^2 = x^3 + 73$ 。令 $P = (2,9)$ 和 $Q = (3,10)$ ，求 $R = P + Q$ 和 $2R$ 。

解：易知过 P, Q 的直线为 $y = x + 7$ ，代入椭圆曲线方程得 $(x + 7)^2 = x^3 + 73$ ，可求得直线与椭圆曲线的第三个交点为 $(-4,3)$ ，因此 $R = (-4, -3)$ 。

- 例 设实域上椭圆曲线 $E: y^2 = x^3 + 73$ 。令 $P = (2,9)$ 和 $Q = (3,10)$, 求 $R = P + Q$ 和 $2R$ 。

解：易知过 P, Q 的直线为 $y = x + 7$, 代入椭圆曲线方程得 $(x + 7)^2 = x^3 + 73$, 可求得直线与椭圆曲线的第三个交点为 $(-4,3)$, 因此 $R = (-4, -3)$ 。

对椭圆曲线求微分可知 $2ydy = 3x^2dx$, 因此 E 在 R 的斜率为 $\frac{dy}{dx}\Big|_{\substack{x=-4 \\ y=-3}} = -8$, 因此过 R 的 E 的切线为 $y = -8(x + 4) - 3$, 代入椭圆曲线并求解可得另一个交点为 $(72, -611)$, 因此 $2R = (72, 611)$ 。

§9.2 椭圆曲线密码

- 以下三类公钥系统被认为是安全有效的
 - 基于大整数分解问题的RSA型公钥密码；
 - 基于有限域上离散对数问题的ElGamal型公钥密码；
 - 基于椭圆曲线离散对数问题的椭圆曲线公钥密码。



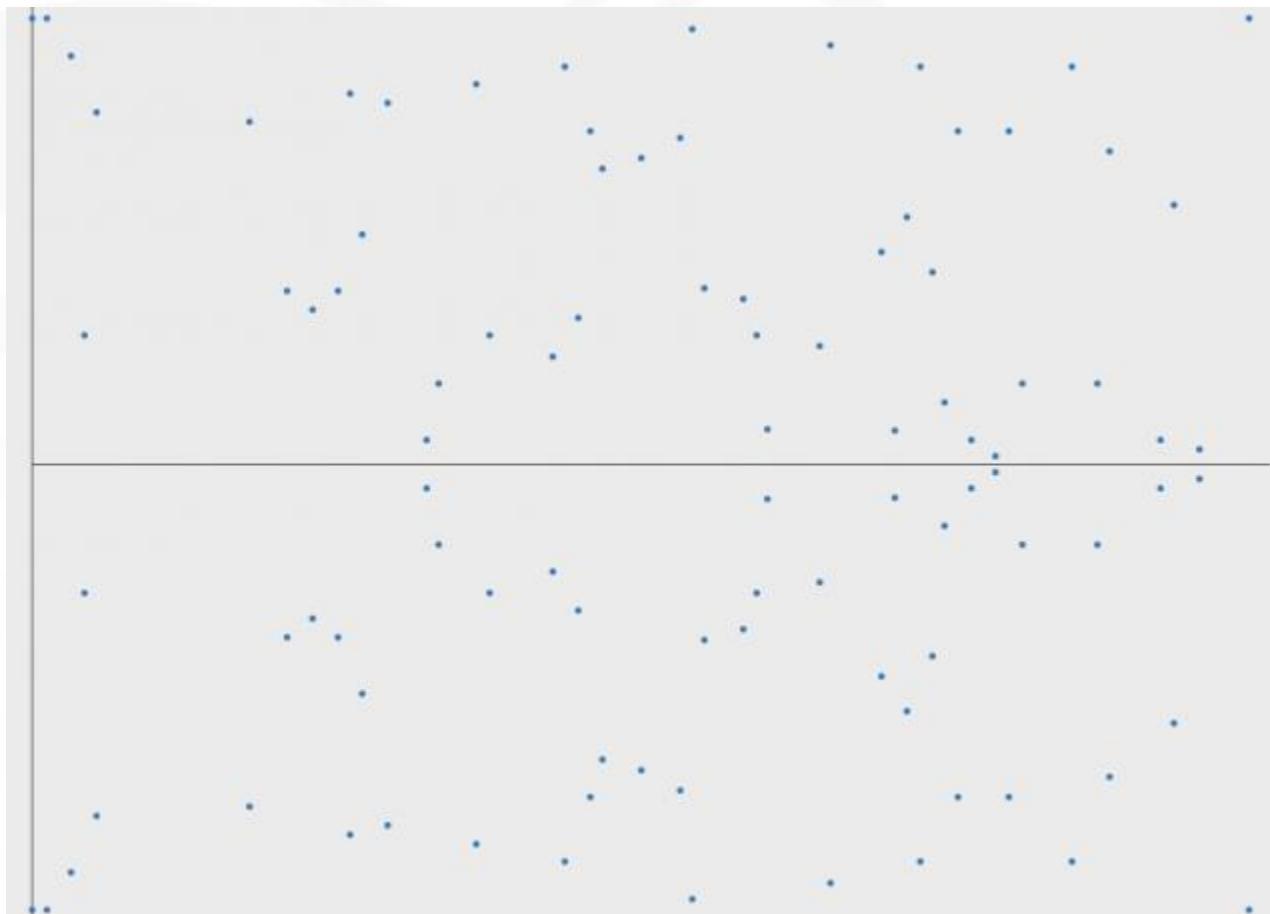
- 椭圆曲线公钥密码优势：对于椭圆曲线离散对数问题，目前不存在亚指数时间算法，从而为达到相同安全性所需的密钥尺寸更小
 - RSA 密码体制：模长1024 比特；
 - 椭圆曲线密码体制：模长160 比特。
- 椭圆曲线密码体制适用于计算、存储、带宽受限，但又要求高速实现的应用领域，例如智能卡、无线通讯等。



华东師範大學

EAST CHINA NORMAL UNIVERSITY

- 有限域上椭圆曲线

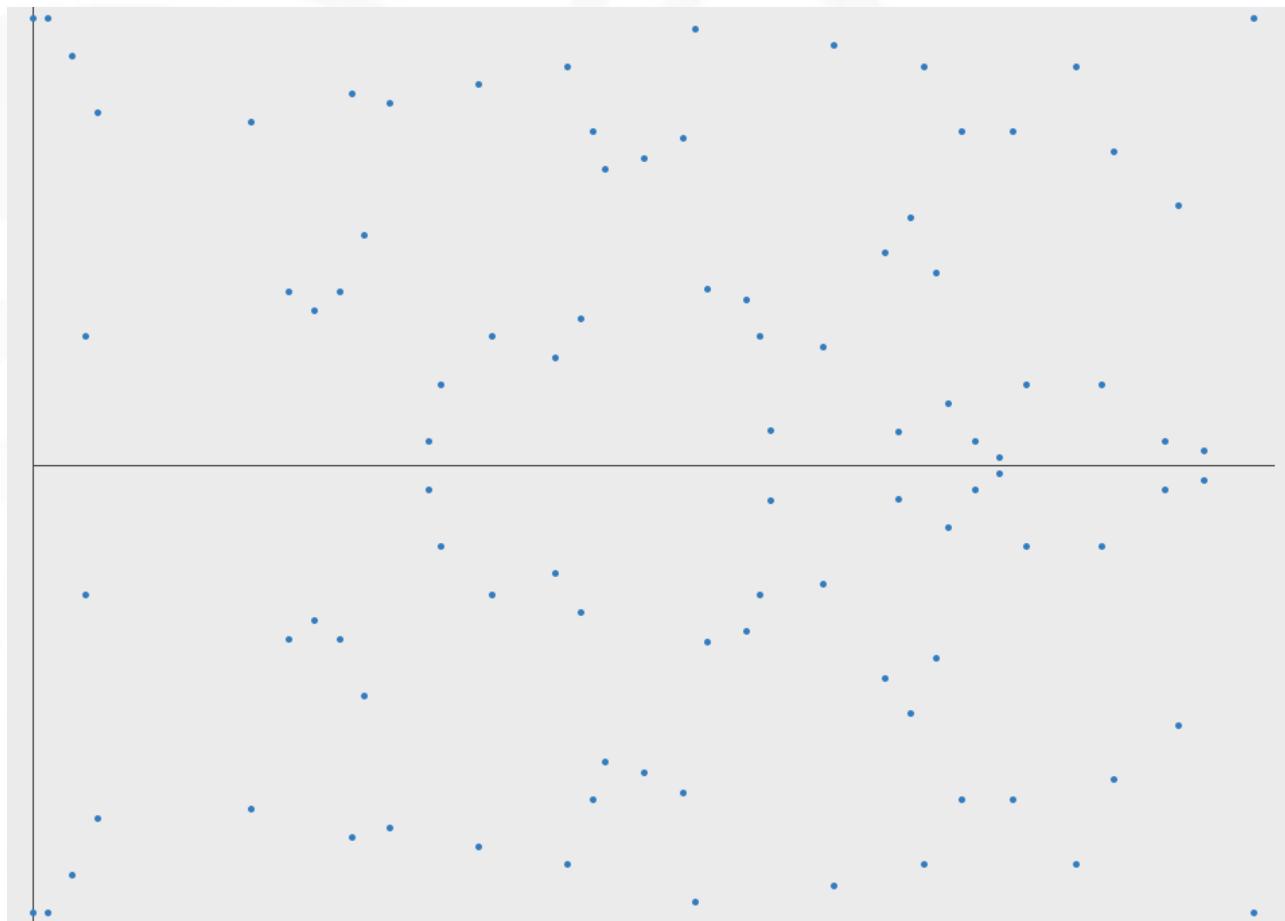




华东師範大學

EAST CHINA NORMAL UNIVERSITY

- 有限域上椭圆曲线加法





- El'Gamal密码方案的椭圆曲线形式

- 设 E 为 F_q 上的椭圆曲线，一般记为 $E(F_q)$ ，设 $P = (x_p, y_p) \in E(F_q)$ ，且 P 的次数足够大，任取 $1 < s < \text{ord}(P)$ ，令 $Q = (x_q, y_q) = sP$ ，则 $E(F_q), P, Q$ 为公钥， s 为私钥。
- 消息 m 满足 $0 \leq m < F_q$ ，任取 $1 < r < F_q$ ，计算 $(x_1, y_1) = rP, (x_2, y_2) = rQ, c = m \cdot x_2$ ，则密文为 (x_1, y_1, c) 。
- 解密时，计算 $(x', y') = s(x_1, y_1)$ ，再计算 $m' = c \cdot x'^{-1}$ ，解得明文。



- 方案的正确性

证明：因为 $(x', y') = s(x_1, y_1) = srP = rsP = rQ = (x_2, y_2)$ ，因此 $x' = x_2$ ，故 $m' = c \cdot {x'}^{-1} = c \cdot {x_2}^{-1} = m$ ，得证。



- 方案的正确性

证明：因为 $(x', y') = s(x_1, y_1) = srP = rsP = rQ = (x_2, y_2)$ ，因此 $x' = x_2$ ，故 $m' = c \cdot x'^{-1} = c \cdot x_2^{-1} = m$ ，得证。

- 方案的安全性依赖于椭圆曲线上的离散对数问题。

上机练习

- El'Gamal密码方案的椭圆曲线形式
 - 取 $p = 613, q = 827$ 都是10位的素数, $n = pq = 506951$, 令 x 满足 $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$, 则公钥为 n, x , 私钥为 p, q 。
 - 消息 m 为一个比特, 随机取 $y, (y, n) = 1$, 则 $c = E(m) = y^2 x^m \pmod{n}$
 - 解密时, 求 $\left(\frac{c}{p}\right)$ 和 $\left(\frac{c}{q}\right)$, 如果 $\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = 1$, 则 $m' = D(c) = 0$, 否则 $m' = D(c) = 1$ 。
- 要求输出中间结果, 包括 $x, y, c, \left(\frac{c}{p}\right), \left(\frac{c}{q}\right), m'$



上机练习

- 作业：实现算法4.1（模 p 平方根算法）并计算同余式 $x^2 \equiv 315 \pmod{907}$ 的所有解。
- 要求输出所有中间结果和最终结果。