ECC加密算法

Elliptic Curve Cryptography

–可厉害的土豆

参考资料：[1]

椭圆曲线离散对数问题
（Elliptic Curve Discrete Logarithm Problem，ECDLP）

椭圆曲线上的两个点P和Q，k为整数。

$$Q = kP$$

椭圆曲线加密的数学原理：
点P称为基点（base point）；k为私钥（private key）；Q为公钥（public key）

- ★ 给定k和P，根据加法法则，计算Q很容易。
- ★ 但给定P和Q，求k非常困难（实际应用ECC，质数p取的非常大，穷举出k非常困难）。

图片来源：[2]

椭圆曲线

$$y^2 = x^3+ax+b \quad (4a^3+27b^2 \neq 0)$$

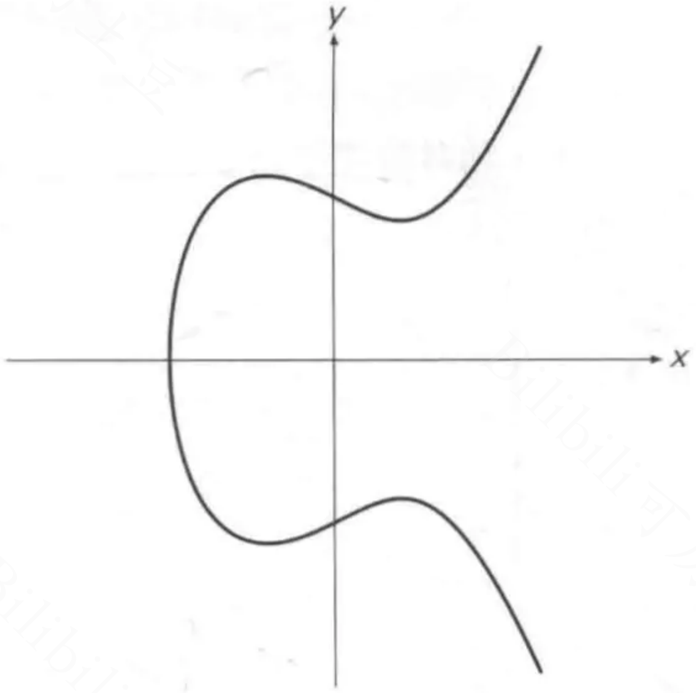
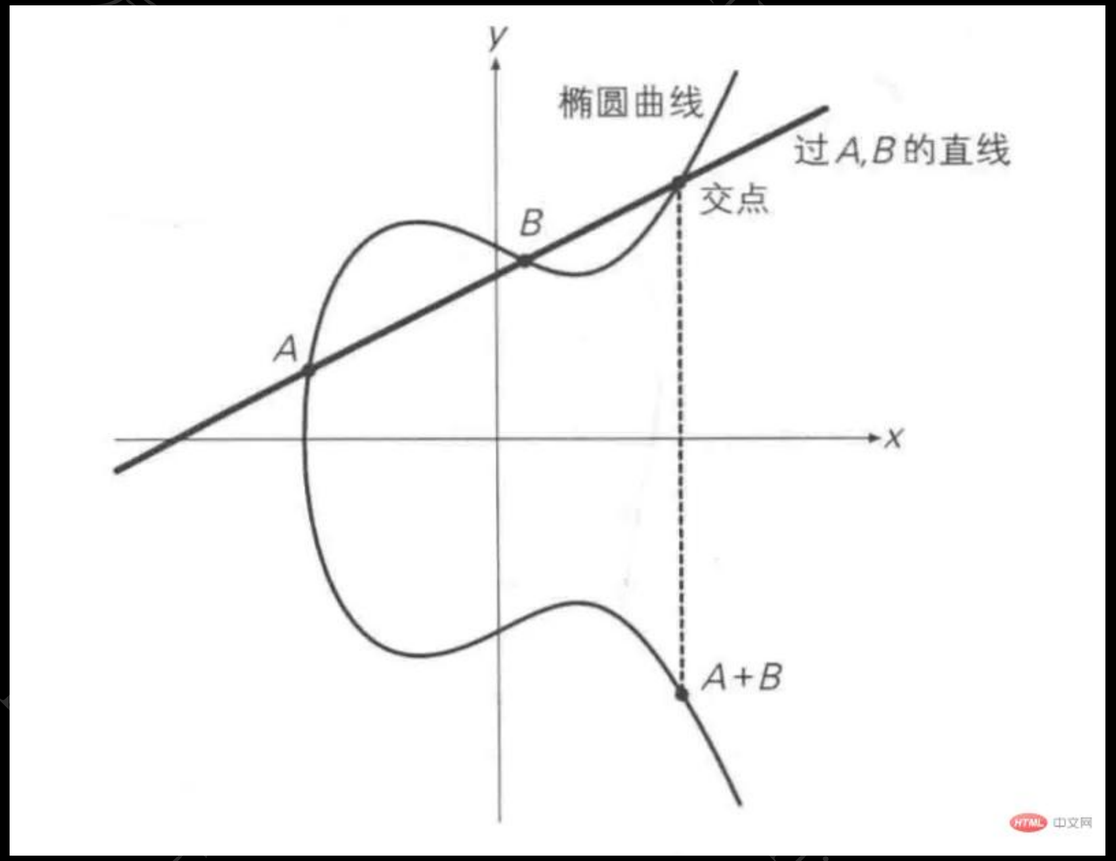
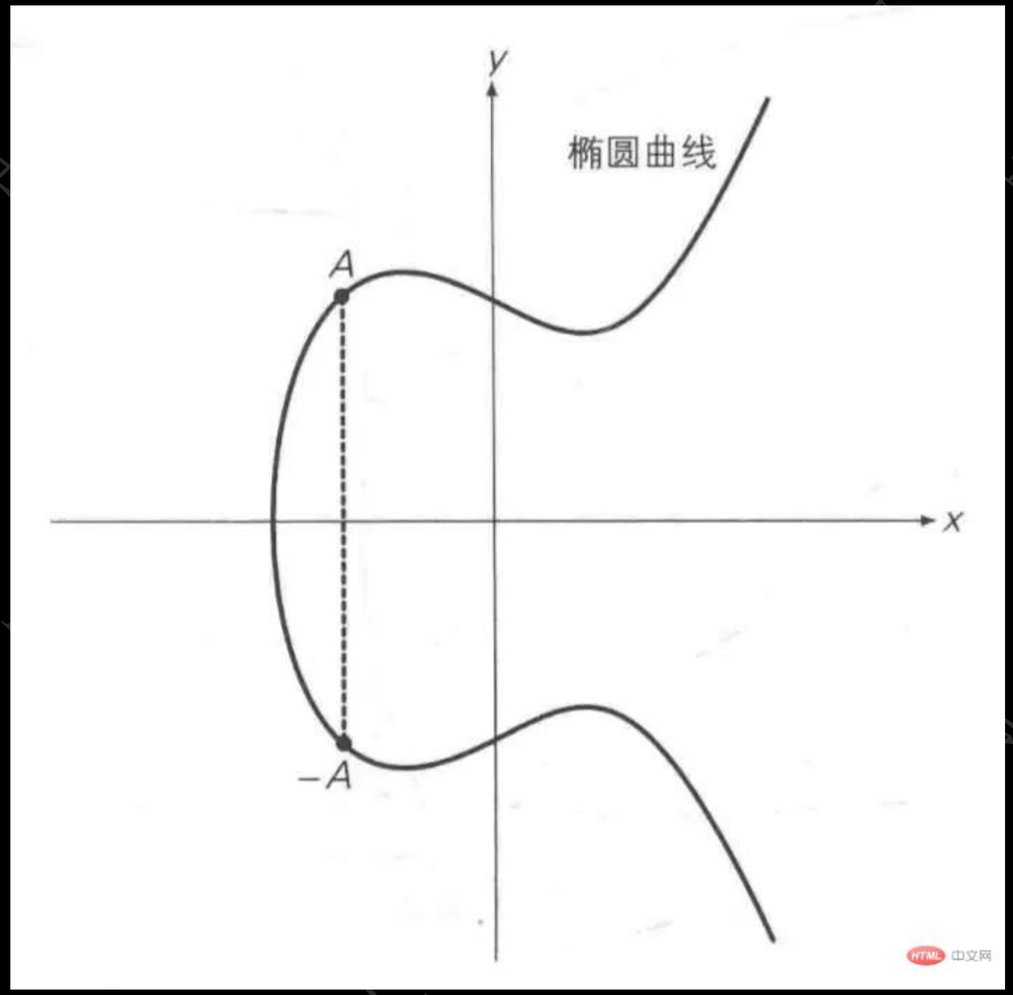


图 X-1　椭圆曲线示例（E_1: $y^2 = x^3 - 2x + 4$）

图片来源：[2]

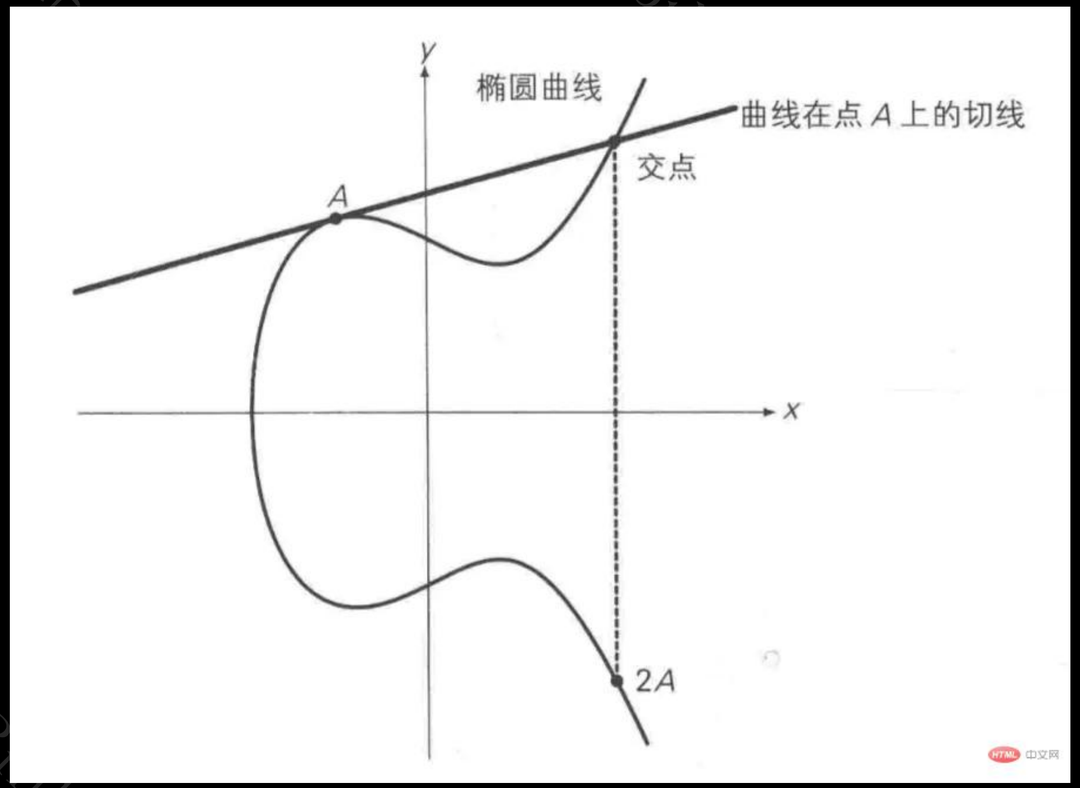
椭圆曲线

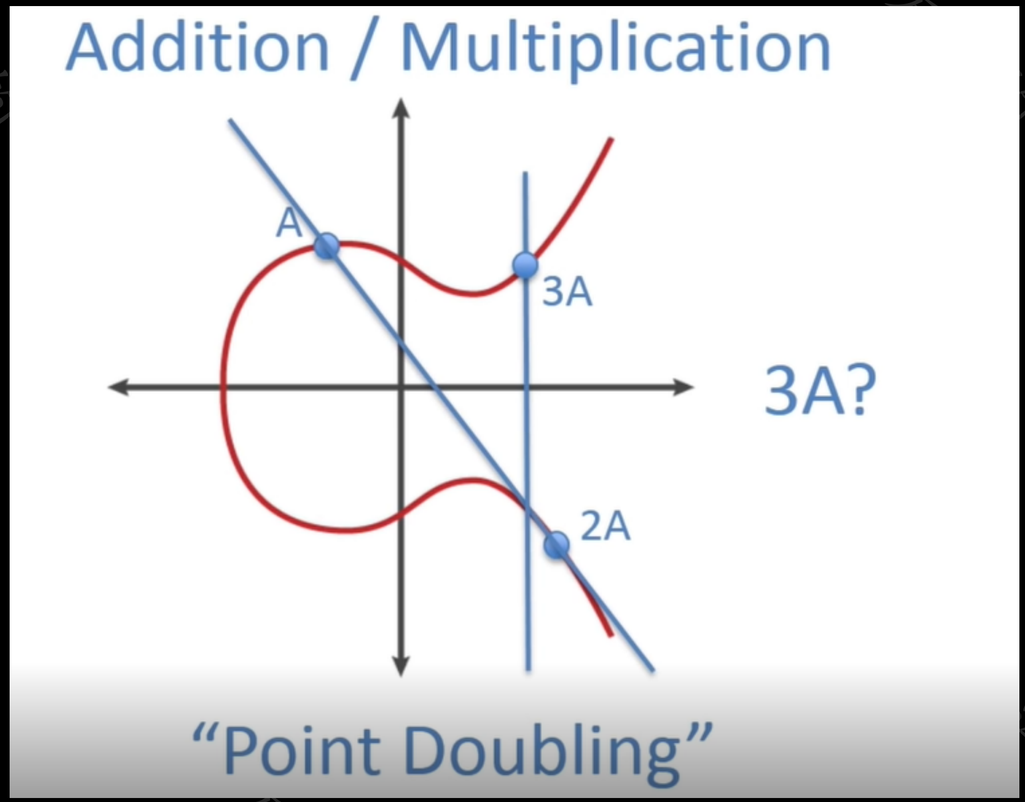




图片来源：[2,3]

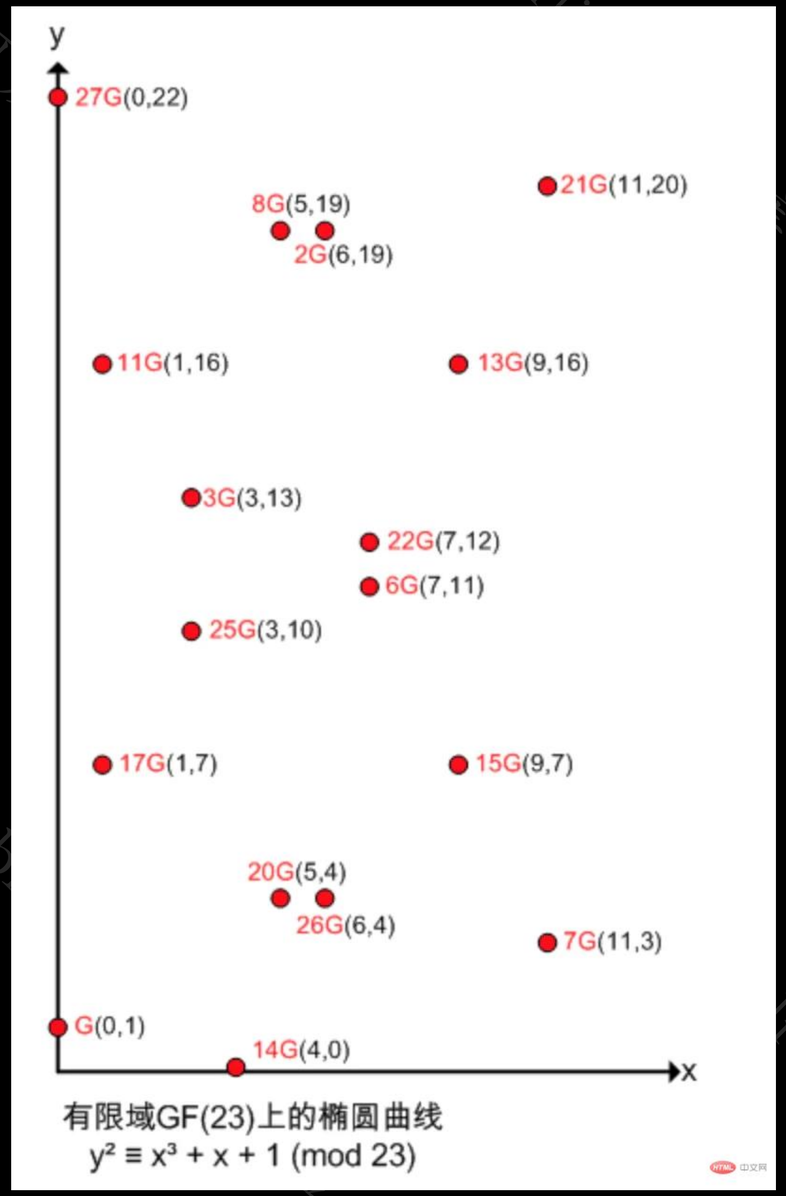
椭圆曲线

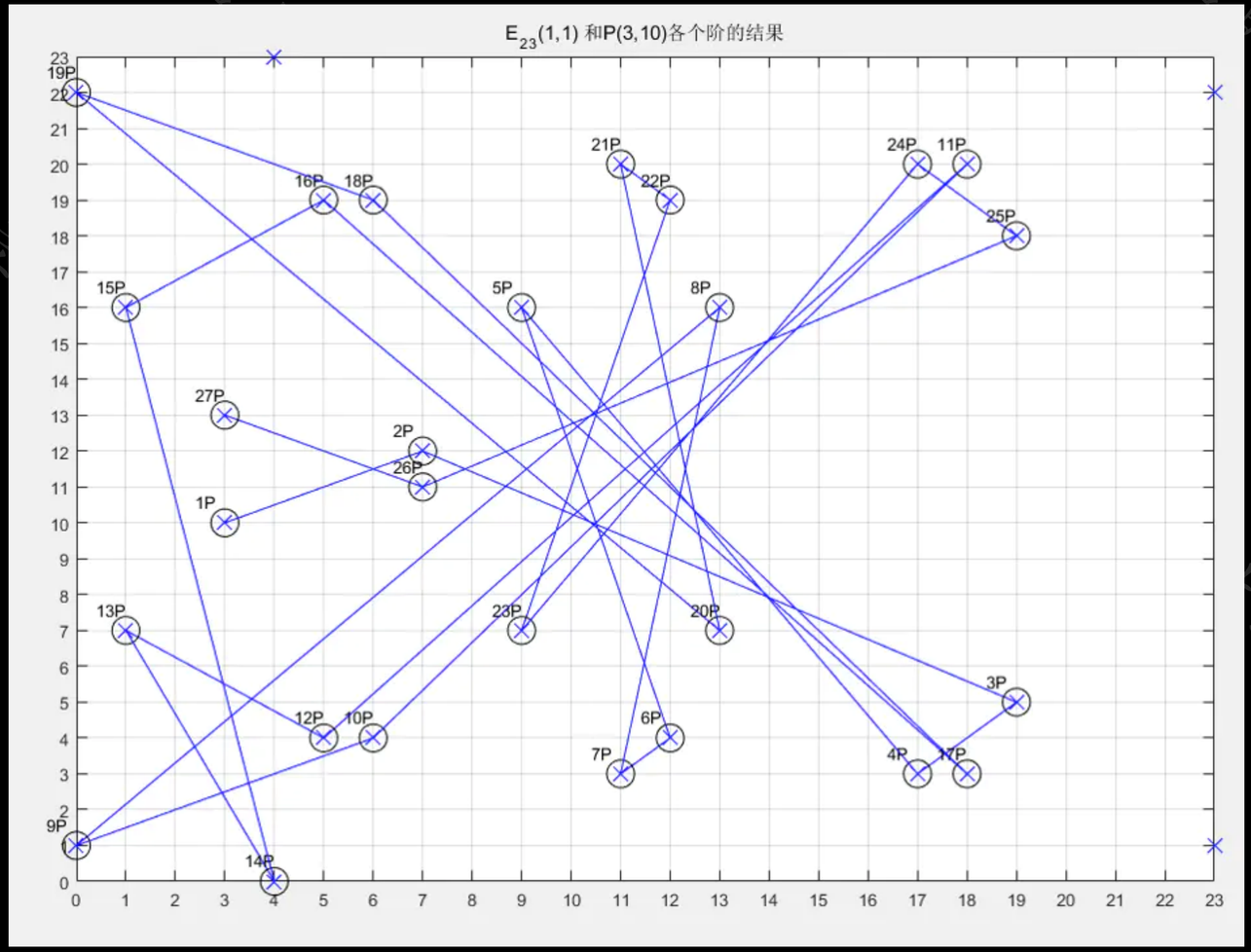

y
椭圆曲线
曲线在点 A 上的切线
交点
A
x
2A


Addition / Multiplication
A
3A
2A
3A?
“Point Doubling”

图片来源：[2,4]

椭圆曲线


y
27G(0,22)
21G(11,20)
8G(5,19)
2G(6,19)
11G(1,16)
13G(9,16)
3G(3,13)
22G(7,12)
6G(7,11)
25G(3,10)
17G(1,7)
15G(9,7)
20G(5,4)
26G(6,4)
7G(11,3)
G(0,1)
14G(4,0)
x
有限域GF(23)上的椭圆曲线
y² ≡ x³ + x + 1 (mod 23)


E23(1,1) 和P(3,10)各个阶的结果
19P
21P
24P
11P
16P
18P
22P
25P
15P
5P
8P
27P
2P
26P
1P
13P
23P
20P
3P
12P
10P
6P
7P
4P
17P
9P
14P

加密过程

$$Q = kP$$

1、选一条椭圆曲线Ep(a,b), 并取椭圆曲线上一点作为基点P。
2、选定一个大数k作为私钥，并生成公钥Q=kP。
3、加密：选择随机数r，将消息M生成密文C。 密文是一个点对，即C=(rP, M+rQ)。
4、解密： M+rQ-k(rP) = M+r(kP)-k(rp) = M

？！

椭圆曲线是连续的，并不适合加密。

我们要把椭圆曲线变成离散的点。

把椭圆曲线定义在有限域上！

参考资料：[5]

域

域是一个可以在其上进行加法、减法、乘法、和除法运算，而结果不会超出域的集合。

如：有理数集合、实数集合、复数集合都是域，但整数集合不是。

（很明显，使用除法得到的分数或者小数已超出整数集合）。

参考资料：[6]

有限域

如果域F只包含有限个元素，则称其为有限域。

有限域中元素的个数称为有限域的阶。

每个有限域的阶必为素数的幂，即有限域的阶可表示为p^n(p 是素数，n是正整数)，

该有限域通常称为Galois域(Galois Fields)，记为$GF(p^n)$。

参考资料：[7]

有限域上的椭圆曲线

在域的定义基础上，作如下修改：

1. 定义**模p加法**和**模p乘法**（加或乘的结果超过p时，模p取余数，p为素数）。
2. 集合内的元素经过加法和乘法计算，**结果仍然在集合内**。
3. 计算符合**交换率**、**结合率**、**分配率**。
4. 加法和乘法有**单位元素**（所有的集合内的值都有对应的负数，所有集合内非零值都有倒数）。

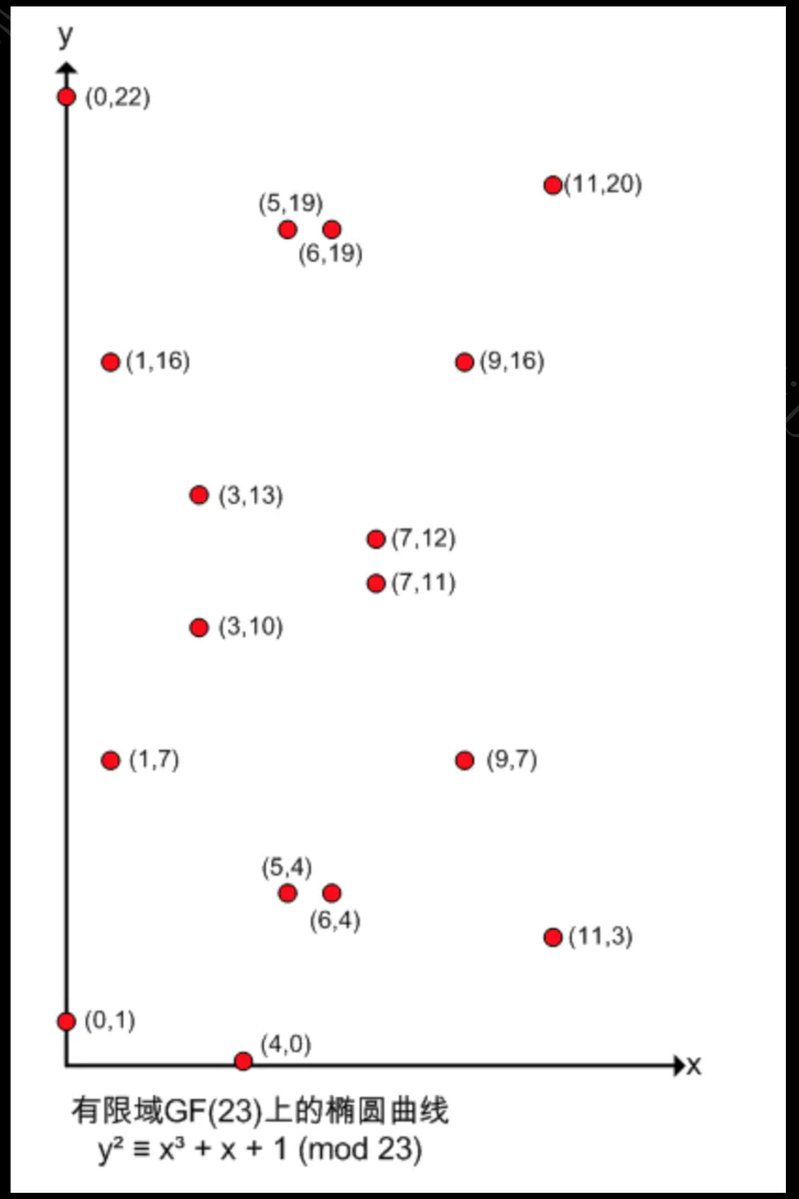
图片来源：[2]

有限域上的椭圆曲线运算

椭圆曲线：$y^2 = x^3+x+1$

有限域：GF(23)

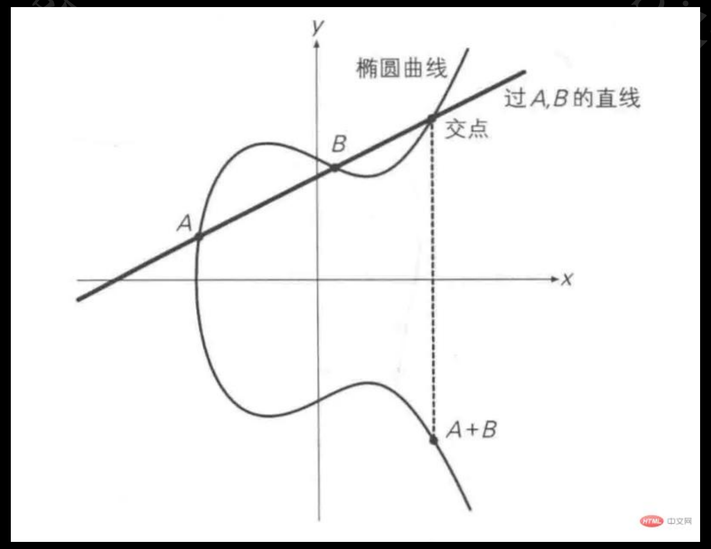
$$y^2 \equiv x^3 + x + 1 \pmod{23}$$

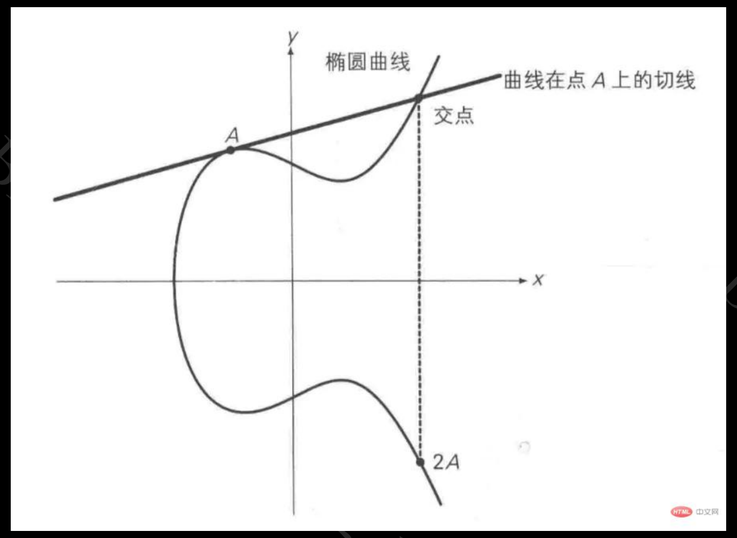


有限域GF(23)上的椭圆曲线
$y^2 \equiv x^3 + x + 1 \pmod{23}$

图片来源：[2,8]

有限域上的椭圆曲线运算





$$x_3 \equiv k^2 - x_1 - x_2 \pmod{p}$$

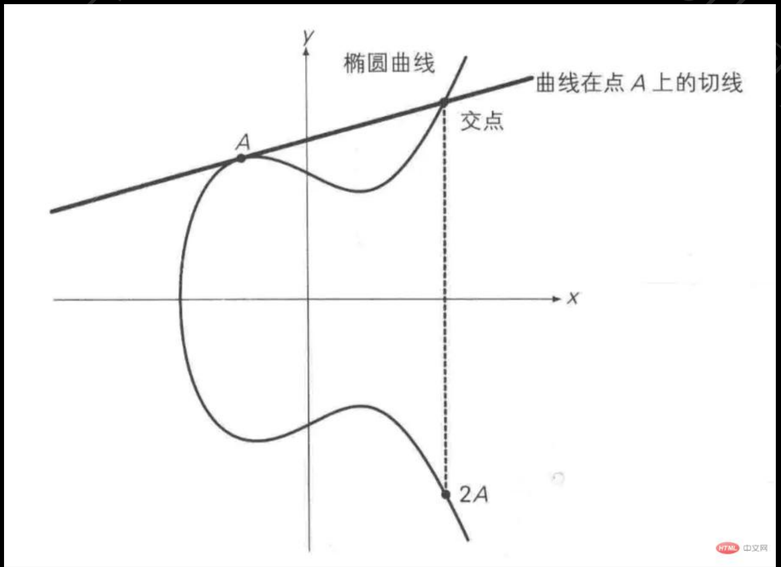
$$y_3 \equiv k(x_1 - x_3) - y_1 \pmod{p}$$

$$\text{若} P = Q, \text{则} k = \frac{3x_1^2 + a}{2y_1} \pmod{p}$$

$$\text{若} P \neq Q, \text{则} k = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}$$

图片来源：[2,8]

有限域上的椭圆曲线运算



$$x_3 \equiv k^2 - x_1 - x_2 \pmod{p}$$
$$y_3 \equiv k(x_1 - x_3) - y_1 \pmod{p}$$
$$\text{若} P = Q, \text{则} k = \frac{3x_1^2 + a}{2y_1} \pmod{p}$$
$$\text{若} P \neq Q, \text{则} k = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}$$

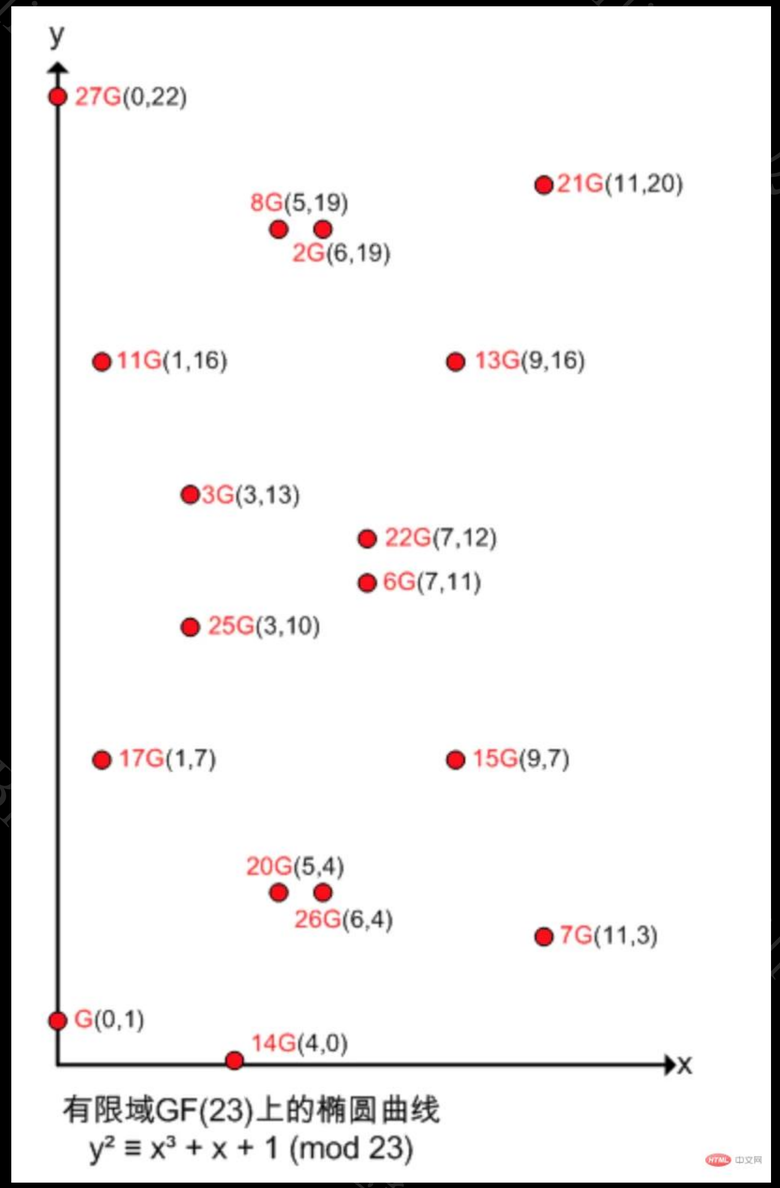
$y^2 \equiv x^3 + x + 1 \pmod{23}$

基点：A (0,1)

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

图片来源：[2,9]

有限域上的椭圆曲线运算



先做倍数再做加法。假设n=151，其对应的二进制是10010111。而二进制数字可以转化为：

$$\begin{aligned} 151 &= 1\cdot 2^7 + 0\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 \\ &= 2^7 + 2^4 + 2^2 + 2^1 + 2^0 \end{aligned}$$

$$151P = 2^7P + 2^4P + 2^2P + 2^1P + 2^0P$$

参考资料

[1] 刘启林. ECC椭圆曲线密码学的原理、公式推导、例子、Python实现和应用[DB/OL].https://zhuanlan.zhihu.com/p/42629724. 知乎. 2020-12-13.
[2] 李_MAX. ECC椭圆曲线加密算法[DB/OL]. https://www.jianshu.com/p/e41bc1eb1d81. 简书. 2020-08-14.
[3]James Early. Elliptic Curve Cryptography & Diffie-Hellman[DB/OL]. https://www.youtube.com/watch?v=yDXiDOJgxmg. Youtube. 日期不详.
[4] 已不再更新. ECC椭圆曲线加密算法(二)[DB/OL]. https://www.jianshu.com/p/8fbd8cd84e1e. 简书. 2018-12-19.
[5] 李浪，邹祎，郭迎. 密码工程学[M]：清华大学出版社，2014.12
[6] 百度百科. 有限域词条[DB/OL]. https://baike.baidu.com/item/%E6%9C%89%E9%99%90%E5%9F%9F/4273049?fr=aladdin. 2018-07-18.
[7] 继舜. 有限域计算概述[DB/OL]. https://zhuanlan.zhihu.com/p/262267121. 知乎. 2020-10-08.
[8] SlteBus. ECC椭圆曲线加解密原理详解. [DB/OL], https://blog.csdn.net/sitebus/article/details/82835492.CSDN. 2018-09-26.
[9] Avery. ECC椭圆曲线加密算法：介绍[DB/OL]. https://zhuanlan.zhihu.com/p/36326221. 知乎. 2018-5-08.

-可厉害的土豆

“谢谢观看
祝你每天吃好
每晚睡饱
身体健康
学业有成
”

–可厉害的土豆