网络空间安全数学基础（4）

网络空间安全学院

高莹

2020年 10 月 21日

本次课程内容目录

环理论回顾

回顾.

让我们构造一个具有8个元素的域。这点可以从$\mathbb{Z}_2[x]$的3次不可约多项式上得到。考虑常数项为1的多项式就足够，因为任何常数项为0的多项式都可以被x整除从而可约。考虑有以下4个多项式：

$$f_1(x) = x^3 + 1$$
$$f_2(x) = x^3 + x + 1$$
$$f_3(x) = x^3 + x^2 + 1$$
$$f_4(x) = x^3 + x^2 + x + 1$$

然后，$f_1(x) = x^3 + 1$是可约的因为：

$$x^3 + 1 = (x + 1)(x^2 + x + 1)$$

环理论回顾

f_4同样可约：

$$x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$$

f_2, f_3都不可约，任意其中一个可以用于构建8元域。我们用$f_2(x)$来构建域$\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$.域中的8个元素分别为：$0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x$和$x^2 + x + 1$。如果要计算域中两个元素的乘，直接将两个多项式相乘并模掉$x^3 + x^2 + 1$.

环理论回顾

示例.

比如在域$\mathbb{Z}_2[x]/(x^3+x^2+1)$中计算$(x^2+1)(x^2+x+1)$，我们首先得到乘积$x^4+x^3+x^2+1$。然后用$x^3+x+1$来除，得到

$$x^4+x^3+x^2+1=(x+1)(x^3+x+1)+x^2+x$$

因此在域$\mathbb{Z}_2[x]/(x^3+x^2+1)$中，有

$$(x^2+1)(x^2+x+1)=x^2+x$$

环理论回顾

接下来，我们展示一个完整非零元素相乘的乘法表，为了简洁，把$a_2x^2 + a_1x + a_0$记为$a_2a_1a_0$

	001	010	011	100	101	110	111
001	001	010	011	100	101	110	111
010	010	100	110	011	001	111	101
011	011	110	101	110	100	001	010
100	100	011	111	110	010	101	001
101	101	001	100	010	111	011	110
110	110	111	001	101	011	010	100
111	111	101	010	001	110	100	011

ElGamal密码体制

Cryptosystem 7.1: *ElGamal Public-key Cryptosystem in* $\mathbb{Z}_p^*$

Let p be a prime such that the **Discrete Logarithm** problem in $(\mathbb{Z}_p^*, \cdot)$ is infeasible, and let $\alpha \in \mathbb{Z}_p^*$ be a primitive element. Let $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$, and define

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod{p}\}.$$

The values p, α, and β are the public key, and a is the private key.

For $K = (p, \alpha, a, \beta)$, and for a (secret) random number $k \in \mathbb{Z}_{p-1}$, define

$$e_K(x, k) = (y_1, y_2),$$

where

$$y_1 = \alpha^k \bmod p$$

and

$$y_2 = x\beta^k \bmod p.$$

For $y_1, y_2 \in \mathbb{Z}_p^*$, define

$$d_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p.$$

椭圆曲线的发现

椭圆曲线是由Neil Koblitz和Victor Miller两位学者分别于1985年首先独立提出。椭圆曲线具有的性质：

- 有限域上椭圆曲线在点加运算下构成有限交换群，且其阶与基域规模相近；
- 类似于有限域乘法群中的乘幂运算，椭圆曲线多倍点运算构成一个单向函数。

密钥强度对比

RSA与ElGamal系统中需要使用长度为1024位的模数，才能达到足够的安全等级。而ECC只需使用长度为160位的模数即可，且传送密文或签章所需频宽较少，并已正式列入IEEE 1363标准，使ECC成为构造公开密钥密码体制一个有力的工具

RSA密钥强度（比特）	椭圆曲线密钥强度（比特）	攻破时间
768	132	2009. 12
829	140左右	2019. 12
1024	160	
2048	210	

椭圆曲线的定义

椭圆曲线并非椭圆，之所以称为椭圆曲线是因为它的曲线方程与计算椭圆周长的方程类似。

椭圆曲线的方程：$y^2 + axy + by = x^3 + cx^2 + dx + e$，其中a,b,c,d,e是满足某些条件的实数。

椭圆曲线有一个特殊的点，记为O，它并不在椭圆曲线E上，此点称为无穷远点。

一条椭圆曲线E(x,y)是由全体解(x,y)再加上一个无穷远点构成的集合。

$$E = \{(x, y) | Y^2 + aXY + bY = X^3 + cX^2 + dX + e\} \cup \{O\}$$

实数域上椭圆曲线的定义

在实数域上，椭圆曲线可定义成 $E : y^2 = x^3 + ax + b$
若方程式没有重复的因式或$4a^3 + 27b^2 \neq 0$，E（a,b）是一条非奇异椭圆曲线。
否则，E（a,b）是一条奇异椭圆曲线（某些数的逆元素(inverse)将不存在）。

多项式的判别式

多项式的判别式定义.

设f(x)是域上一个次数大于2的多项式，假定$f(x) = a_0(x-\alpha_1)...(x-\alpha_n)$，这里$\alpha_1, ..., \alpha_n$是它域上的根，则f的判别式定义为D(f):

$$D(f) = a_0^{2n-2} \prod_{1 \le i \le j \le n} (\alpha_i - \alpha_j)^2$$

n=2时.

$$f(x) = ax^2 + bx + c = a(x-\alpha_1)(x-\alpha_2)$$

$$D(f) = a^2(\alpha_1 - \alpha_2)^2 = a^2((\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2) = a^2(b^2a^{-2} - 4ca^{-1})$$

$$D(ax^2 + bx + c) = b^2 - 4ac$$

多项式的判别式

n=3时.

$$f(x) = ax^3 + bx^2 + cx + d = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

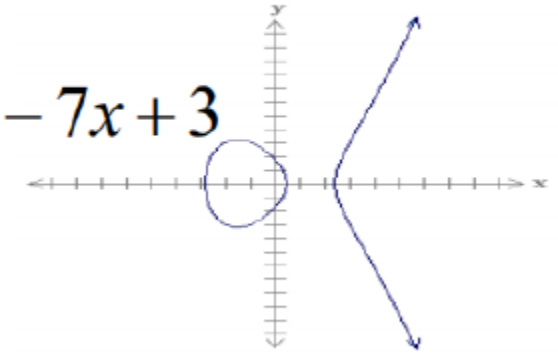
$$D(f) = a^4(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

$$D(ax^3 + bx^2 + cx + d) = b^2c^2 - 4b^3d - 4ac^3 - 27a^2d^2 + 18abcd$$

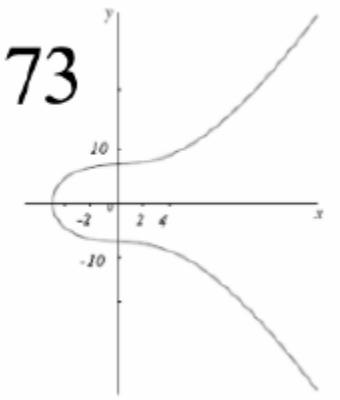
$$D(x^3 + ax + b) = 4a^3 + 27b^2$$

椭圆曲线的例子

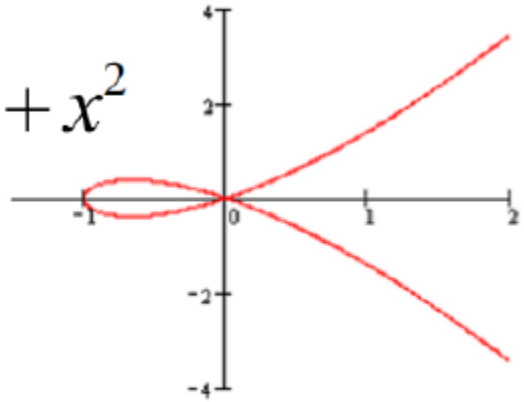
$E: y^2 = x^3 - 7x + 3$



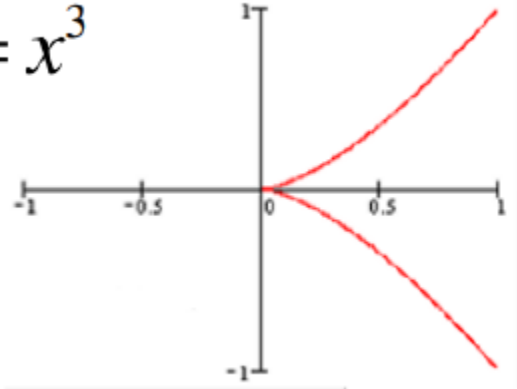
$E: y^2 = x^3 + 73$



$E: y^2 = x^3 + x^2$



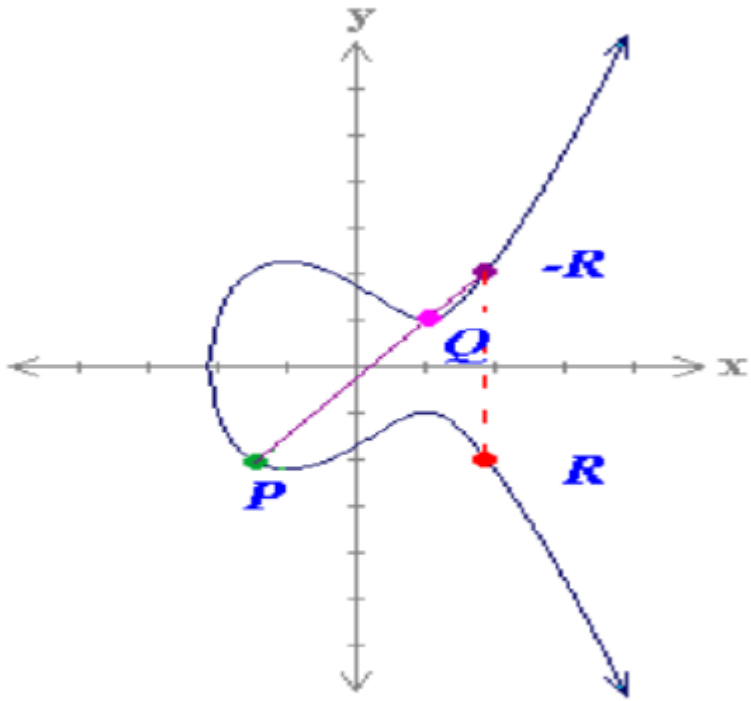
$E: y^2 = x^3$



满足方程的任意一点是否都存在切线?

椭圆曲线上的加法

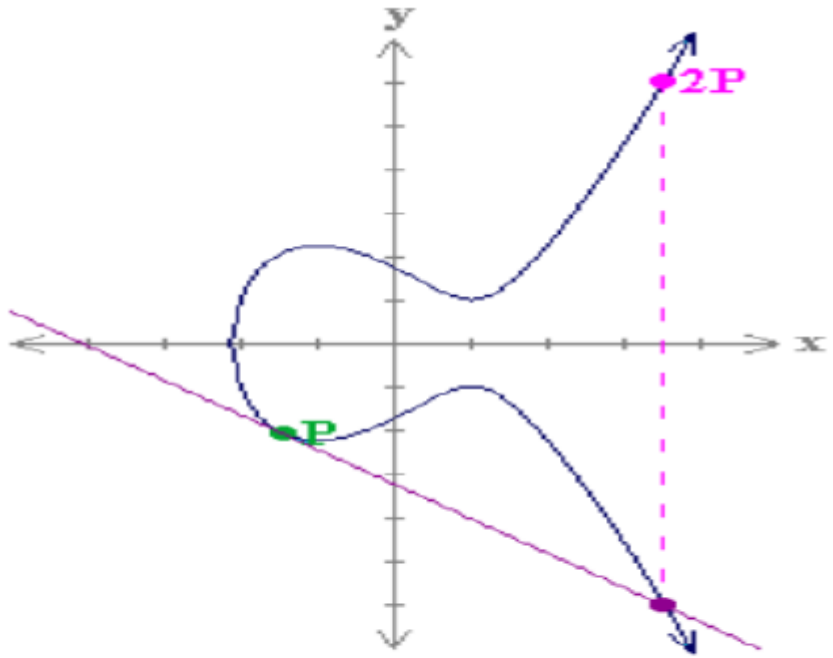
两异点相加：假设P和Q是椭圆曲线上两个相异的点，而且P不等于-Q 。若P+Q=R ，则点R是经过P、Q两点的直线与椭圆曲线相交之唯一交点的负点。



$y^2 = x^3 - 3x + 3$

椭圆曲线上的加法

双倍的点：令P +P=2P ，则点2P是经过P的切线与椭圆曲线相交之唯一交点的负点。



$y^2 = x^3 - 3x + 3$

椭圆曲线的定义

定义.

一条椭圆曲线E是一个Weierstrass方程

$$E : Y^2 = X^3 + AX^2 + B,$$

的一组解加上一个额外的点O，A,B两个常数满足：

$$4A^3 + 27B^2 \neq 0.$$

椭圆曲线的定义

定理.

E是一条椭圆曲线，则E上加法有如下性质(E上的点组成一个交换群)：

- P+O=O+P=P, for all $P \in E$ [Identity]
- P+(-P)=O, for all $P \in E$ [Inverse]
- (P+Q)+R=P+(Q+R), for all $P, Q, R \in E$ [Associate]
- P+Q=Q+P , for all $P, Q \in E$ [Commutative]

椭圆曲线的定义

定理(椭圆曲线加法定理).

$$E\text{æ}Y^2 = X^3 + AX + B$$

是一条椭圆曲线，P_1和P_2是E上的点。
(a)如果$P_1 = O$,则$P_1 + P_2 = P_2$.
(b)否则$P_2 = O$,则$P_1 + P_2 = P_1$.
(c)否则，记$P_1 = (x_1, y_1), P_2 = (x_2, y_2)$.
(d)若$x_1 = x_2, y_1 = -y_2$,则$P_1 + P_2 = O$
(e)否则定义λ:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, P_1 \neq P_2, \\ \dfrac{3x_1^2 + A}{2y_1}, P_1 = P_2 \end{cases} \tag{1}$$

然后让$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$.
$P_1 + P_2 = (x_3, y_3)$

本次课程内容目录

有限域上椭圆曲线的定义

定义.

$p \geq 3$为一个素数，一条在域$\mathbb{F}_p$上的椭圆曲线为如下形式的等式

$$E : Y^2 = X^3 + AX + B,\ A, B \in \mathbb{F}_p,\ 4A^3 + 27B^2 \neq 0$$

E上所有点的集合为：

$$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p,\ y^2 = x^3 + Ax + B\} \cup O$$

有限域上的椭圆曲线可以定义在任意有限域上，因二元域上的情形比较复杂，放在后面讲

椭圆曲线在模p下的运算规则

加法规则：

- 对所有的点$P \in E(\mathbb{F}_p)$, $P + O = O + P, P + (-P) = O$
- 记$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P \neq -Q$,则$P + Q = (x_3, y_3)$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, P_1 \neq P_2, \\ \dfrac{3x_1^2 + A}{2y_1}, P_1 = P_2 \end{cases} \tag{2}$$

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1.$$

如果$s, t \in \mathbb{F}_p$，则对所有$P \in E(\mathbb{F}_p)$,

$$(s + t)P = sP + tP$$

椭圆曲线在模p下的运算规则举例

例1.

有限域$\mathbb{F}_{23}$之下，点P=(0,1)是椭圆曲线

$$E : y^2 = x^3 + 12x + 1$$

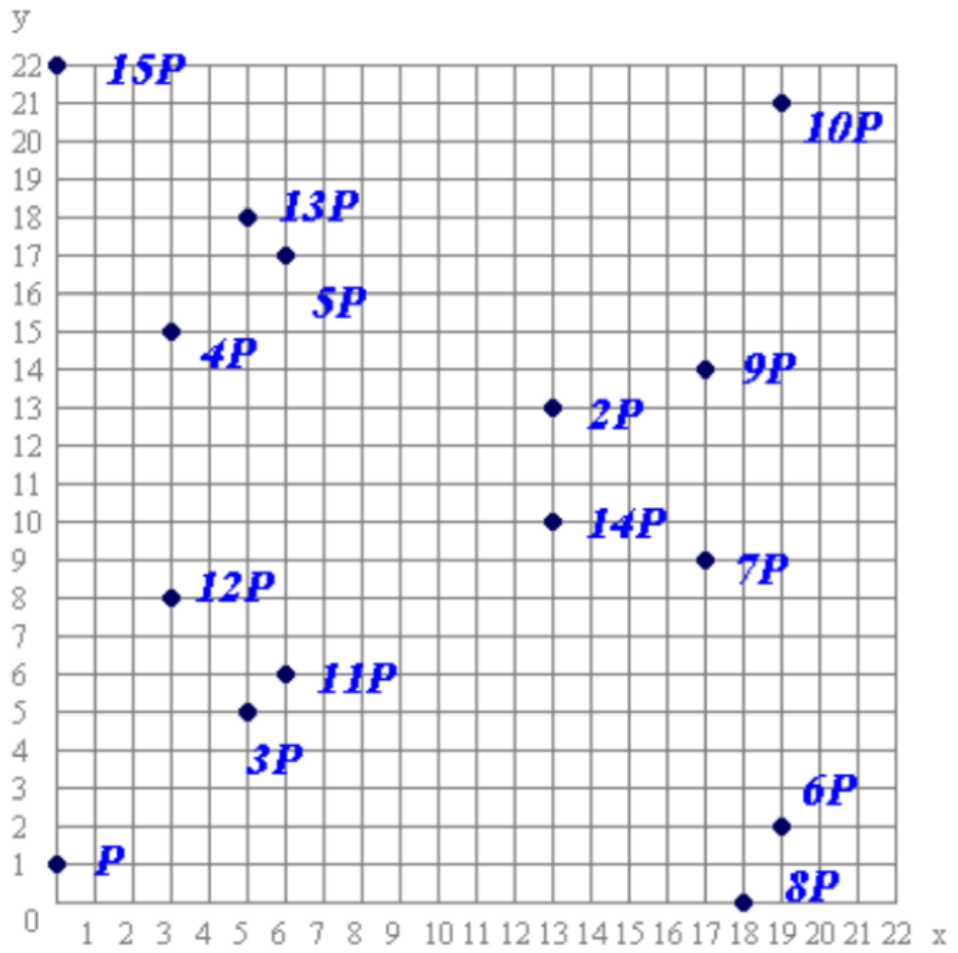
的生成数，求nP

$$
\begin{array}{l|l}
P = (0, 1) & 9P = (17, 14) \\
2P = (13, 13) & 10P = (19, 21) \\
3P = (5, 5) & 11P = (6, 6) \\
4P = (3, 15) & 12P = (3, 8) \\
5P = (6, 17) & 13P = (5, 18) \\
6P = (19, 2) & 14P = (13, 10) \\
7P = (17, 9) & 15P = (0, 22) \\
8P = (18, 0) &
\end{array}
$$

注：$|E(\mathbb{F}_{23})| = 15$，其实还要加上一个无穷远点，故E上共有16个点，点P的秩n=16。

椭圆曲线在模p下的运算规则

在坐标上画出，并观察图像特点



椭圆曲线在模p下的运算规则

例2.

有限域$\mathbb{F}_{23}$之下，取椭圆曲线

$$E : y^2 = x^3 + 16x + 10$$

上的两点P=(18,14), Q=(5,10), $R = P + Q = (x_3, y_3) = ?$

$$\lambda = \frac{3x^1 + A}{2y_1} mod\ p = 9$$

$$x_3 = \lambda^2 - x_1 - x_2 mod\ p = 22$$

$$y_3 = \lambda(x_1 - x_3) - y_1 mod\ p = 19$$

$$R = (22, 19)$$

椭圆曲线在模p下的运算规则

例3.

条件同例2，若$P+P=2P=R=(x_3,y_3)$，则R=?

$$x_3=\lambda^2-x_1-x_1 mod\ p=22$$

$$y_3=\lambda(x_1-x_3)-y_1 mod\ p=19$$

$$P+P=2P=R=(22,19)$$

椭圆曲线在模p下的点数

显然$E(\mathbb{F}_p)$是一个有限集，因为对X,Y分量来说都只有有限个可能。更确切地说，X取值一共有p中可能，对每一个X，等式

$$Y^2 = X^3 + AX + B$$

表明对应的Y最多只有两种可能，再加上一个点O，$E(\mathbb{F}_p)$最多只有2p+1个点。然而这一估计数值想当然的比实际大小要大。

椭圆曲线在模p下的点数

当我们为X赋一个值时，以下的三次多项式的值一共有三种可能

$$X^3 + AX + B$$

第一，它可能是一个模p的2次剩余，说明它有两个方根，因此我们得到$E(\mathbb{F}_p)$中的两个点。这件事50%会发生。第二，它可能是一个模p的非2次剩余，此时我们舍弃X，这件事50%发生。第三，它可能等于0，我们得到$E(\mathbb{F}_p)$中的一个点，但这概率非常非常低。因此我们期望$E(\mathbb{F}_p)$中点的个数约为

$$\#E(\mathbb{F}_p) \approx 50\% \cdot 2 \cdot p + 1 = p + 1$$

椭圆曲线在模p下的点数

Hasse提出了一个非常著名的定理，在之后被Weil和Deligne广义化，描述了在随机波动的情况下这是正确的

定理 (Hasse).

E是$\mathbb{F}_p$上的一条椭圆曲线，则

$$\#E(\mathbb{F}_p) = p + 1 - t_p \text{ with } |t_p| \leq 2\sqrt{p}$$

定义

$t_p = p + 1 - \#E(\mathbb{F}_p)$这个数称为$E/\mathbb{F}_p$的Frobenius迹(the trace of Frobenius)。这里不解释这个名字的由来，但要说的是t_p实际上是一个确定的2x2矩阵的迹，并且这个矩阵代表的是$E/\mathbb{F}_p$相关的2维向量空间一个线性变换。

p	$\#E(\mathbb{F}_p)$	t_p	$2\sqrt{p}$
3	4	0	3.46
5	8	−2	4.47
7	11	−3	5.29
11	16	−4	6.63
13	14	0	7.21
17	15	3	8.25

Figure: number of points and trace of Frobenius for E: $Y^2 = X^3 + 4X + 6$

注：若$\#E(\mathbb{F}_p) = p + 1$，曲线$E(\mathbb{F}_p)$称为超奇异的，否则称为非超奇异的

注释

Hasse的定理为$\#E(\mathbb{F}_p)$给了一个界限，但并没有给出具体计算的方法。原则上，一个人可以尝试所有的X，并计算$X^3 + AX + B$并检查，但这需要O(p)的复杂度，非常低效。Schoof找到了$O((log\ p)^6)$时间的多项式时间算法来计算$\#E(\mathbb{F}_p)$。他的算法之后被Elkies和Atkin改善并用于实际，现在这一算法被称为SEA算法。我们在此不描述SEA算法的内容，因为其中用到了椭圆曲线的高级技巧。