椭圆曲线

网络空间安全学院

教师：胡丽琴

关于椭圆曲线

1984年，Hendrik Lenstra提出了依靠椭圆曲线性质分解整数的精妙算法。这一发现激发了学者进一步研究椭圆曲线在密码和计算数论的其它应用。

关于椭圆曲线

椭圆曲线密码在1985年分别由Neal Koblitz和Victor Miller提出。椭圆曲线密码方案为公钥机制，提供如同RSA一样的功能。但是，它的安全性依赖不同的困难问题，也就是椭圆曲线离散对数问题(ECDLP)。

关于椭圆曲线

解决大整数分解问题需要亚指数时间复杂度的算法，而目前已知计算椭圆曲线离散对数问题的最好方法都需要全指数时间复杂度。这意味着在椭圆曲线系统中我们只需要使用相对于RSA短得多的密钥就可以达到与其相同的安全强度。

关于椭圆曲线

- 例如，一般认为160比特的椭圆曲线密钥提供的安全强度与1024比特RSA密钥相当。
- 使用短的密钥的好处在于加解密速度快、节省能源、节省带宽、存储空间。

●椭圆曲线的一般形式

- 设**K**是一个域，满足$\chi(\mathbf{K}) \neq 2, 3$。当$4a^3+27b^2 \neq 0$时，域**K**上的点集

$$E(\mathbf{K}):=\{(x, y)\in \mathbf{K}\times\mathbf{K} \mid y^2=x^3+ax+b\}\cup\{O\}$$

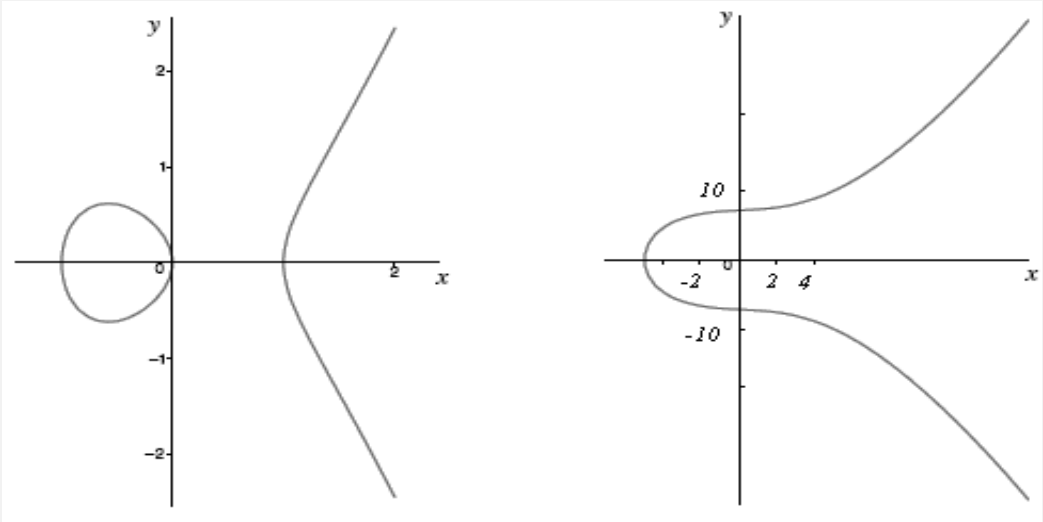
叫做域**K**上的椭圆曲线。

- 其中O表示无穷远点。

● 实数域上椭圆曲线的例子

例

- $E_1:=\{(x, y)\in\mathbf{R}\times\mathbf{R}|\ y^2=x^3-x\}\cup\{O\}$
- $E_2:=\{(x, y)\in\mathbf{R}\times\mathbf{R}|\ y^2=x^3+3\}\cup\{O\}$



● 有限域上椭圆曲线的点

- 设K=$\mathbf{F}_p$，其中$p\neq 2,3$，$4a^3+27b^2\neq 0$。

  $E(\mathbf{F}_p)=\{(x,y)\in\mathbf{F}_p\times\mathbf{F}_p \mid y^2=x^3+ax+b\}\cup\{O\}$是$\mathbf{F}_p$上的椭圆曲线。

- 对每个$x\in\mathbf{F}_p$，计算$z=x^3+ax+b$;

1. 若$y^2=z$在$\mathbf{F}_p$中没有解$y\in\mathbf{F}_p$，则椭圆曲线E上没有横坐标为x的点;
2. 若$y^2=z$在$\mathbf{F}_p$中有解，则有两个解，设为y_1，y_2，从而有

$$(x,y_1),(x,y_2)\in E(\mathbf{F}_p)$$

● 有限域上椭圆曲线的例子

- 设$\mathbf{F}_{17}$上的椭圆曲线为E：$y^2=x^3+2x+3$，求出该椭圆曲线的全部点。
- 对x=0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16，分别求出y。
  - x=0，计算$y^2\equiv3(\mathrm{mod}\ 17)$，无解；
  - x=1，计算$y^2\equiv6(\mathrm{mod}\ 17)$，无解；
  - x=2，计算$y^2\equiv15(\mathrm{mod}\ 17)$，解为：$y$=7和$y$=10；

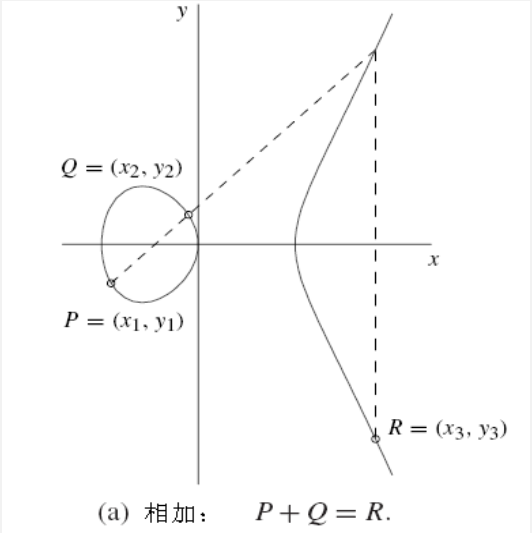
  ……
  - x=16，计算$y^2\equiv0(\mathrm{mod}\ 17)$，解为：$y$=0.

因此，$E(\mathbf{F}_p)=\{(2,7),(2,10),(3,6),(3,11),\ldots,(16,0),O\}$

● 加法原理

定义

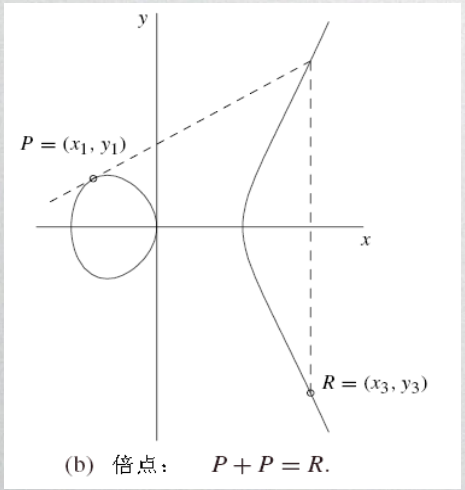
- 设P、Q是E上的两个不同的点，L是过点P和Q的直线，R'是L与曲线E相交的第三点。设L'是过R'和O的直线，则P⊕Q就是L'与E相交的第三点R。



(a) 相加： $P + Q = R$.

加法原理

- 若P=Q呢？
- 设P是E上的点，L是过点P的切线，R'是L与曲线E相交的第二点。设L'是过R'和O的直线，则P⊕P就是L'与E相交的第三点R。



(b) 倍点： $P + P = R$.

●加法原理

例

- 令椭圆曲线E由方程$y^2=x^3+ax+b$确定，并令P=(x_1, y_1)，Q=(x_2, y_2)，则

  P+Q=R=(x_3, y_3),

  这里$x_3=m^2-x_1-x_2$, $y_3=m(x_1-x_3)-y_1$，并且

$$m=\begin{cases}(y_2-y_1)/(x_2-x_1), & if\ P\neq Q\\ (3x_1^2+a)/2y_1, & if\ P=Q\end{cases}$$

  特别地，

- P+O=O+P=P；
- −P=$(x_1, -y_1)$

●加法原理

- E对于上述加法运算构成一个加法交换群

  单位元是什么？

- 无穷远点是有限域上椭圆曲线群的单位元

- 设$\mathbf{F}_{17}$上的椭圆曲线为E={$(x,y)|\ y^2=x^3+2x+3$}∪{O}，设P=(2,7)，Q=(11,8)，求P+Q，2P，8P。