椭圆曲线

杨礼珍

同济大学计算机科学与技术系, 2018

Outline

6.5 椭圆曲线

阅读：《密码学原理与实践》P.201 6.5节。
作业：《密码学原理与实践》P.220 练习6.13(a)

定义6.3

设$a, b \in \mathbb{R}$是满足$4a^2 + 27b^2 \neq 0$的常实数。方程

$$y^2 = x^3 + ax + b \tag{1}$$

的所有解$(x, y) \in \mathbb{R} \times \mathbb{R}$连同一个无穷远点$\mathcal{O}$组成的集合E称为一个非奇异椭圆曲线。

Fact：

方程(1)有3个不同解 $\Longleftrightarrow 4a^2 + 27b^2 \neq 0$，则$E$是非奇异的；否则称为奇异椭圆曲线。

6.5 椭圆曲线

6.5.1 实数上的椭圆曲线

椭圆曲线的不同形状：

例：下图画出了实数域上的椭圆曲线$y^2 = x^3 - 4x$。

对非奇异椭圆曲线E定义二元运算$+$，使其成为一个Abel群：

1. 单位元设为$\mathcal{O}$，因此，有$\forall P \in E$有$P + \mathcal{O} = \mathcal{O} + P = P$。
2. 设$P = (x_1, y_1), Q = (x_2, y_2) \in E$，$P + Q = R$。分三种情形定义$R$：

- 情形1. $x_1 \neq x_2$：设$R = (x_3, y_3), R' = (x_3, -y_3)$。

6.5 椭圆曲线

6.5.1 实数上的椭圆曲线

6.5 椭圆曲线

6.5.1 实数上的椭圆曲线