Cipolla's algorithm*

张晴川
qzha536@aucklanduni.ac.nz

June 15, 2020

1 问题

给定素数 p 和整数 n，在 $\mathbb{F}_p$ 上求平方根 $\sqrt{n}$，p 是素数。

2 核心思路

我们在 $\mathbb{F}_p$ 的二次扩张上求平方根，如果 n 在 $\mathbb{F}_p$ 上已经有平方根，那么求出的结果一定也在 $\mathbb{F}_p$ 内，这是因为任意一个域中 $x^2 = n$ 都最多只有两个根（拉格朗日定理）。

3 做法

Lemma (欧拉准则)**.**

$$x^{\frac{p-1}{2}} = \begin{cases} 1 & x\text{是二次剩余} \\ -1 & x\text{不是二次剩余} \end{cases}$$

首先考虑在 $\mathbb{F}_p$ 中随机选取一个数 a 满足 $\omega = a^2 - n$ 不是二次剩余，由于 $\mathbb{F}_p$ 有一半的数不是二次剩余，这一步很快，判定用欧拉准则即可。

现在考虑 $\mathbb{F}_p$ 的二次扩张 $\mathbb{F}_p(\sqrt{\omega})$。

我们来证明 n 的一个平方根是：

$$(a + \sqrt{\omega})^{\frac{p+1}{2}}$$

*更多内容请访问：`https://github.com/SamZhangQingChuan/Editorials`

Proof. 只需要证明 $(a+\sqrt{\omega})^{p+1}=n$ 即可：

$$
\begin{aligned}
(a+\sqrt{\omega})^{p+1} &= (a+\sqrt{\omega})^p(a+\sqrt{\omega}) \\
&= (a^p+\sqrt{\omega}^p)(a+\sqrt{\omega}) && \because 1<i<p \implies \binom{p}{i}=0 \\
&= (a+\sqrt{\omega}^{p-1}\sqrt{\omega})(a+\sqrt{\omega}) \\
&= (a+\omega^{\frac{p-1}{2}}\sqrt{\omega})(a+\sqrt{\omega}) \\
&= (a-\sqrt{\omega})(a+\sqrt{\omega}) && \because \omega\text{不是二次剩余} \implies \omega^{\frac{p-1}{2}}=-1 \\
&= a^2-\omega^2 \\
&= a^2-(a^2-n) \\
&= n
\end{aligned}
$$

□

所以 $(a+\sqrt{\omega})^{\frac{p+1}{2}}$ 确实是 n 的平方根。如果 n 在 $\mathbb{F}_p$ 中是二次剩余，那么我们得到的结果一定也在 $\mathbb{F}_p$ 中。