第十一章

> 4. 证明命题11.4。

证明：

1. 对于

$$a \equiv b \pmod p$$

若

$$x^2 \equiv a \pmod p$$

有解，则必有

$$x^2 \equiv b \pmod p$$

故

$$(\frac{a}{p}) = (\frac{b}{p})$$

2.

- 若

$$x^2 \equiv a \pmod p$$

和

$$x^2 \equiv b \pmod p$$

均有解，则

$$x^2 \equiv (ab) \pmod p$$

有解

$$(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$$

成立

- 若

$$x^2 \equiv a \pmod p$$

和

$$x^2 \equiv b \pmod p$$

均无解，则由命题11.3中QNR*QNR=QR有

$$x^2 \equiv (ab) \pmod p$$

有解

$$(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$$

成立

- 使用欧拉准则

$$(\frac{a}{p})=a^{(p-1)/2}\pmod p\textcolor{red}{\backslash}(\frac{b}{p})=b^{(p-1)/2}\pmod p\textcolor{red}{\backslash}(\frac{ab}{p})=(ab)^{(p-1)/2}\pmod p$$

$$有(\frac{a}{p})(\frac{b}{p})=(\frac{ab}{p})成立$$

3. 显然

$$x^2\equiv a^2\pmod p有两个解：x\equiv\pm a\pmod p$$

则

$$(\frac{a^2}{p}=1)恒成立$$

> 5. 给出推论11.1的完整证明。

证明：由欧拉准则

$$(\frac{-1}{p})=(-1)^{(p-1)/2}$$

$$当p\equiv 1\pmod 4时，(p-1)/2为偶数，则(\frac{-1}{p})=1恒成立\textcolor{red}{\backslash当}p\equiv -1\pmod 4时，(p-1)/2为奇数，则(\frac{-1}{p})=-1恒成立$$

> 6. 设 p 是奇素数，请证明 Z_p^*的所有生成元都是模 p 的二次非剩余

证明：对于任意生成元a,若a为模p的二次剩余，则有 $x\in Z_p^*$且$x^2\equiv a\pmod p$ 有解

令$a^m\equiv x\pmod p$,则$a^{2m}\equiv a\pmod p$, $a^{2m-1}\equiv 1\pmod p$

因为x有两解，故存在两个不同的m，m小于p-1，使得$a^{2m-1}\equiv 1\pmod p$

不符合生成元的定义，故假设错误，a为模p的二次非剩余。