> 1．请证明：
>
> 命题11.4．设p是奇素数，$a,b\in\mathbb{Z}$且不被p整除。则有：
>
> 1.如果$a\equiv b\pmod p$，则$(\frac{a}{p})=(\frac{b}{p})$
>
> 2.$(\frac{a}{p})(\frac{b}{p})=(\frac{ab}{p})$
>
> 3.$(\frac{a^2}{p})=1$

证明：

1．**如果**$a\equiv b\pmod p$**，则**$(\frac{a}{p})=(\frac{b}{p})$

1)若a,b为模p的$\boldsymbol{QR}$，则必存在$x\in\mathbb{Z},s.t.\ a\equiv x^2\pmod p$，又$a\equiv b\pmod p$，故

$$a\equiv x^2\equiv b\pmod p\Rightarrow(\frac{a}{p})=(\frac{b}{p})=1$$

2)若a,b为模p的$\boldsymbol{QNR}$，对于$\forall x\in\mathbb{Z},s.t.a\not\equiv x^2\pmod p$**,**又$a\equiv b\pmod p$，故

$$a\equiv b\not\equiv x^2\pmod p\Rightarrow(\frac{a}{p})=(\frac{b}{p})=-1$$

综上：$(\frac{a}{p})=(\frac{b}{p})$证毕。

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

1)若a,b为模p的$\boldsymbol{QR}$，根据$\boldsymbol{QR}\times\boldsymbol{QR}=\boldsymbol{QR}$，$ab$也为模$p$的$\boldsymbol{QR}$，所以

$$(\frac{a}{p})(\frac{b}{p})=1\times1=1=(\frac{ab}{p})$$

2)若a,b为模p的$\boldsymbol{QNR}$，根据$\boldsymbol{QNR}\times\boldsymbol{QNR}=\boldsymbol{QR}$，所以

$$(\frac{a}{p})(\frac{b}{p})=(-1)\times(-1)=1=(\frac{ab}{p})$$

3)若a,b其中一个为模p的$\boldsymbol{QNR}$，另一个为模p的$\boldsymbol{QR}$，根据$\boldsymbol{QNR}\times\boldsymbol{QR}=\boldsymbol{QNR}$，所以

$$(\frac{a}{p})(\frac{b}{p}) = -1 = (\frac{ab}{p})$$

综上：$(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$证毕。

3.$(\frac{a^2}{p}) = 1$

由于a^2为平方数，故a^2为模p的$\boldsymbol{QR}$，故$(\frac{a^2}{p}) = 1$证毕。

> 2．给出推论11.1的完整证明。
>
> 推论11.1:设p是一个奇素数，则:
>
> $$(\frac{-1}{p}) = \begin{cases} 1 & \text{如果} p \equiv 1 \pmod 4; \\ -1 & \text{如果} p \equiv -1 \pmod 4. \end{cases}$$

证明:

因为$p \equiv 1 \pmod 4$，故$\exists k \in \mathbb{Z}, s.t.\ p = 4k+1$。则根据欧拉准则

$$(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} \equiv (-1)^{(4k+1-1)/2} \equiv (-1)^{2k} \equiv 1 \pmod p$$

因为$p \equiv -1 \pmod 4$，故$\exists k \in \mathbb{Z}, s.t.\ p = 4k+3$。则根据欧拉准则

$$(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} \equiv (-1)^{(4k+3-1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

证毕。

> 3．设p是奇素数，请证明$\mathbb{Z}_p^*$的所有生成元都是模p的二次非剩余。

证明:

假设存在一个生成元$a \in \mathbb{Z}_p^*$，a是模p的$\boldsymbol{QR}$。

则有：

$$(\frac{a}{p}) = 1 \Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod p$$

由于a是$\mathbb{Z}_p^*$的生成元，故a为模p的原根，根据定义：

$$a^{\phi(p)} \equiv 1 \pmod p$$

即a模p的阶为$\phi(p) = p - 1$，即存在**最小的整数**e，使得：

$$e = \phi(p) = p - 1 且 a^e \equiv 1 \pmod p$$

而

$$(p-1)/2 < e$$

说明e不为最小的整数，故假设不成立，原命题得证。