Homework II

2021 年 3 月 18 日

谢远峰

网安一班

3019244283

习题 1

证明：如果素数 p=4n+1, 且 d|n, 则 $\left(\frac{d}{p}\right)$

$$
\begin{aligned}
(d,p)=1 \rightarrow & d^{p-1} \equiv 1(mod\ p) && \text{费马小定理}\\
\rightarrow & d^{4n} \equiv 1(mod\ p)\\
\rightarrow & (d^{2n})^2 \equiv 1^2(mod\ p) && \text{同余性质}\\
\rightarrow & d^{2n} \equiv 1(mod\ p)\\
\rightarrow & d^{\frac{p-1}{2}} \equiv 1(mod\ p) && \text{二次剩余理论}
\end{aligned}
$$

d 是模 p 的二次剩余，所以 $\left(\frac{d}{p}\right)$