NumberTheory 10

王胤雅

201911010205

201911010205@mail.bnu.edu.cn

2024 年 5 月 31 日

PROBLEM I Assume p, q are odd primes, $a > 1$ is integal. Prove:

1. $q \mid a^p - 1 \implies q \mid a - 1$ or $2p \mid q - 1$.
2. $q \mid a^p + 1 \implies q \mid a + 1$ or $2p \mid q - 1$.

SOLUTION.

1. Consider $a \in \mathbb{Z}_q^*$. Since $a^p - 1 = 0$ in $\mathbb{Z}_q^*$, then $o(a) \mid p$. So $o(a) = 1$ or $o(a) = p$. If $o(a) = 1$, then $a \equiv 1 \pmod q$, then $q \mid a - 1$. If $o(a) = p$, then $p = o(a) \mid o(\mathbb{Z}_q^*) = q - 1$. Since $2 \mid q - 1$, $(p, 2) = 1$, then $2p \mid q - 1$.
2. Consider $-a \in \mathbb{Z}_q^*$. Since $(-a)^p - 1 = 0$ in $\mathbb{Z}_q^*$, then $o(-a) \mid p$. So $o(-a) = 1$ or $o(-a) = p$. If $o(-a) = 1$, then $-a \equiv 1 \pmod q$, then $q \mid a+1$. If $o(-a) = p$, then $p = o(-a) \mid o(\mathbb{Z}_q^*) = q-1$. Since $2 \mid q - 1$, $(p, 2) = 1$, then $2p \mid q - 1$.

$\square$

PROBLEM II Find primitive root for each number $7, 49, 343, 686$.

SOLUTION.

1. Obviously, 3 is the primitive root of 7.
2. 3 is the primitive root of 49.
3. 3 is the primitive root of 343.
4. Since the primitive root of 686 is the odd one of $3, 3 + 343$, then 3 is the primitive root of 686.

$\square$