NumberTheory 10

白永乐

202011150087

202011150087@mail.bnu.edu.cn

2024 年 5 月 24 日

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

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

SOLUTION .

1. Consider $o(a)$ in $\mathbb{Z}_q^*$. We know that $o(a) \mid p$. So $o(a) = 1 \vee o(a) = p$. When $o(a) = 1$, we get $q \mid a - 1$. Besides, $o(a) \mid o(\mathbb{Z}_q^*) = q - 1$. So when $o(a) = p$, we get $p \mid q - 1$. Since q is odd, we know $2 \mid q - 1$. And $\gcd(2, p) = 1$, so $2p \mid q - 1$.
2. Consider $o(-a)$ in $\mathbb{Z}_q^*$. We know that $o(-a) \mid p$. So $o(-a) = 1 \vee o(-a) = p$. When $o(-a) = 1$, we get $q \mid a + 1$. Besides, $o(-a) \mid o(\mathbb{Z}_q^*) = q - 1$. So when $o(-a) = p$, we get $p \mid q - 1$. Since q is odd, we know $2 \mid q - 1$. And $\gcd(2, p) = 1$, so $2p \mid q - 1$.

□

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

SOLUTION . By calculating we get that 3 is primitive root of 7. So we know there exists a primitive root x of 49 such that $x = 3 + 7y$. By calculating we get that 3 is primitive root of 49. So we know there exists a primitive root x of 49 such that $x = 3 + 49y$. By calculating we get that 3 is primitive root of 343. So we know that the odd one of $3, 346$ is primitive root of 686. So 3 is primitive root of 686. □