1082 作業三

繳交日期 109/04/10(五) 13:10

1. Calculate the following (please write down the detail calculation process)
   (a) Divide 2^{12345} by 120. What is the remainder?
   (b) What is the last 3 digits of 321^{2439}?
   (c) Evaluate $7^{999} \pmod{8}$?
   (d) Use part (c) to find $6^{7^{999}}$ (mod 30)?

2. Let $p \equiv 3 \pmod 4$ be prime. Show that $x^2 \equiv -1 \pmod p$ has no solution, i.e. -1 or p-1 is a quadratic non-residue. (Hint: by contradiction, i.e. assume that the solution x exists. Raise both sides to the power (p-1)/2 and use Fermat's theorem.)

3. Let a and $n > 1$ be integers with $\gcd(a, n) = 1$. The order of a mod n is the smallest positive integer r such that $a^r \equiv 1 \pmod n$. Denote $r = ord_n(a)$.
   (a) Show that $r \le \phi(n)$
   (b) Show that if $m = r\,k$ is a multiple of r, then $a^m \equiv 1 \pmod n$
   (c) Suppose $a^t \equiv 1 \pmod n$. Write $t = q\,r + s$ with $0 \le s < r$ (this is just division with remainder). Show that $a^s \equiv 1 \pmod n$.
   (d) Using the definition of r and the fact that $0 \le s < r$, show that $s = 0$ and therefore $r \mid t$. This, combined with part (b), yields the result that $a^t \equiv 1 \pmod n$ if and only if $ord_n(a) \mid t$.
   (e) Show that $ord_n(a) \mid \phi(n)$.