NTOUCS 1112 密碼學與應用作業三 繳交日期 112/03/23(四) 15:10

1. Which of the following congruences have solutions. If yes, what are the solutions?
   (a) $X^2 \equiv 153 \pmod{419}$?
   (b) $X^2 \equiv 53 \pmod{191}$?
   (c) $X^2 \equiv 52528 \pmod{80029}$
   Note: 419, 191, 65537 are primes, 80029=419*191

2. Find the last 3-digits of 1234^{5632}

3. Find all primes p for which the matrix $\begin{bmatrix} 3 & 6 \\ 5 & 3 \end{bmatrix}$ (mod p) is not invertible.

4. 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 $ord_n(a) \mid \phi(n)$.