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 congruence relations 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 are primes, 80029=419*191

Sol:

(a) $419 \equiv 3 \pmod 4$

$$153^{\frac{419-1}{2}} \equiv 153^{209} \equiv 153^{128+64+16+1} \equiv 252 \cdot 154 \cdot 352 \cdot 153 \equiv 418 \equiv -1 \pmod{419}$$

$x^2 \equiv 153 \pmod{419}$ has no solution.

(b) $191 \equiv 3 \pmod 4$

$$53^{\frac{191-1}{2}} \equiv 53^{95} \equiv 53^{64+16+8+4+2+1} \equiv 98 \cdot 50 \cdot 97 \cdot 80 \cdot 135 \cdot 53 \equiv 190 \equiv -1 \pmod{191}$$

$x^2 \equiv 53 \pmod{191}$ has no solution.

(c) This problem is equivalent to the system of congruence equations

$x^2 \equiv 153 \pmod{419}$ and $x^2 \equiv 3 \pmod{191}$.

From part (a), the first congruence has no solution, means that 153 or 52528 is not a quadratic residue modulo 419. Thus the congruence relation $x^2 \equiv 52528 \pmod{80029}$ has no solution, i.e. not a quadratic residue modulo 80029, even though $3^{\frac{191-1}{2}} \equiv 3^{95} \equiv 3^{64+16+8+4+2+1} \equiv 12 \cdot 96 \cdot 67 \cdot 81 \cdot 9 \cdot 3 \equiv 1$ (mod 191) means that 3 or 52528 is a quadratic residue mod 191.

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

Sol:

$1000 = 2^3 \cdot 5^3$

$\phi(1000) = 1000 \cdot (1-1/2) \cdot (1-1/5) = 400$

We would really like to use the Euler's Theorem $a^{\phi(n)} \equiv 1 \pmod n$ to simplify the modulo exponentiation. However, the catch is that gcd(a, n)=1 or $a \in Z_n^*$ must be satisfied and unfortunately gcd(1234,100)=2. In this case we still can use Fermat's Little Theorem and Chinese Remainder Theorem to speed up the calculation of the modular exponentiation, which takes $O((\log n)^3)$ of time and is large if log n goes to several thousands. 1234^{5632} (mod 1000) is equivalent to the following system of congruence equations

$x \equiv 1234^{5632} \pmod 8) \equiv 1234^{5632} \pmod{125}$ where gcd(8,125)=1

Now the first congruence relation becomes $x \equiv (1234 \bmod 8)^{5632} \equiv 2^{5632} \equiv 8 \cdot 2^{5629} \equiv 0 \pmod 8$ and the second congruence relation becomes $x \equiv (1234 \bmod 125)^{(5632 \bmod 100)} \equiv 109^{32} \equiv 81 \pmod{125}$, where gcd(1234,125)=1 and $\phi(125) = 125 \cdot (1-1/5) = 100$.

Now we use CRT to solve the following system of equations

$x \equiv 0 \pmod 8 \equiv 81 \pmod{125}$ where gcd(8,125)=1

Because we have $8 \cdot (8^{-1})_{\text{mod } 125} + 125 \cdot (125^{-1})_{\text{mod } 8} = 1$, i.e. $8 \cdot (-78) + 125 \cdot 5 = 1$ and the CRT solution for the above system of congruence relations is

$x \equiv 81 \cdot 8 \cdot (-78) + 0 \cdot 125 \cdot 5 \equiv 456 \pmod{1000}$

A last note, although if we neglect the fact that gcd(1234, 1000)=2 and apply Euler's Theorem anyway, $1234^{5632} \equiv 234^{5632 \pmod{400}} \equiv 234^{32} \equiv (((((234^2)^2)^2)^2)^2) \equiv 456 \pmod{1000}$. This happens by chance or maybe some extra conditions are satisfied and is not guaranteed.

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

Sol:

If gcd(det(A),p)>1 then a matrix A is not invertible modulo p.

$\det(\begin{bmatrix} 3 & 6 \\ 5 & 3 \end{bmatrix}) = 3\times 3 - 5\times 6 = -21 \equiv p\text{-}21 \pmod{p}$

If p is greater than 21 then gcd(p-21, p) = 1 since p is a prime number. Thus, A is always invertible modulo p. Now we need to consider all primes less than 21, i.e. {2,3,5,7,11,13,17,19}, one by one to see if any one satisfies gcd(p-21,p)>1. Since p is a prime number, only its multiples are not relative prime to itself, which implies that p-21≡0 (mod p), or equivalently prime p that divides 21

(1) p=19 ⇒ 19-21 ≡ -2 ≡ 17 (mod 19)
(2) p=17 ⇒ 17-21 ≡ -4 ≡ 13 (mod 17)
(3) p=13 ⇒ 13-21 ≡ -8 ≡ 5 (mod 13)
(4) p=11 ⇒ 11-21 ≡ -10 ≡ 1 (mod 11)
(5) p=7 ⇒ 7-21 ≡ -14 ≡ 0 (mod 7)
(6) p=5 ⇒ 5-21 ≡ -16 ≡ 4 (mod 5)
(7) p=3 ⇒ 3-21 ≡ -18 ≡ 0 (mod 3)
(8) p=2 ⇒ 2-21 ≡ -19 ≡ 1 (mod 2)

Hence, the only prime numbers that make the matrix $\begin{bmatrix} 3 & 6 \\ 5 & 3 \end{bmatrix}$ (mod p) not invertible are 3 and 7.

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

Sol.

(a) Since r is the smallest positive integer such that $a^r \equiv 1$ (mod n) and Euler theorem says that the integer $\phi(n)$ satistfies $a^{\phi(n)} \equiv 1$ (mod n) for all $a \in Z_n^*$, we obtain that $r \leq \phi(n)$.

(b) Since $a^r \equiv 1$ (mod n), $a^m \equiv a^{rk} \equiv (a^r)^k \equiv 1^k \equiv 1$ (mod n).

(c) Since $a^t \equiv a^{qr+s} \equiv a^{qr} \cdot a^s \equiv 1 \cdot a^s \equiv a^s$ (mod n), $a^t \equiv 1$ (mod n) implies $a^s \equiv 1$ (mod n).

(d) We want to prove that "$a^t \equiv 1 \pmod{n} \Leftrightarrow ord_n(a) \mid t$"

($\Rightarrow$): part (c) shows that if $t = qr + s$, $0 \leq s < r$ then $a^t \equiv 1 \pmod{n} \Rightarrow a^s \equiv 1 \pmod{n}$. Since by definition r is the smallest number such that $a^r \equiv 1$ (mod n), we must have $s = 0$ and $t = qr + 0 = qr$ and therefore $r \mid t$.

($\Leftarrow$): part (b) shows exactly that if $r \mid t$ then $a^t \equiv 1$ (mod n).

(e) Assume $\phi(n) = qr + s$. From the Euler theorem $a^{\phi(n)} \equiv 1$ (mod n) and the result of part (d), we concludes that $s = 0$ and thus $ord_n(a) \mid \phi(n)$.