Homework Assignment 2 - Introduction To Cryptography

Ton That Tam Dinh

October 7, 2017

Problem 1.17. Find all values of x between 0 and m - 1that are solutions of the following congruences.
a) $x + 7 \equiv 23(mod 37)$

Proof. a) $x + 7 \equiv 23(mod 37) \leftrightarrow x \equiv 16(mod 37)$. So x = 16.
b) $x + 42 \equiv 19(mod 51) \leftrightarrow x \equiv -23(mod 51) \leftrightarrow x \equiv 28(mod 51)$. So the solution is x = 28.
c) $x^2 \equiv 3(mod 11)$
Try all x from 0 to 10 we have x = 5, 6.
d)$x^2 \equiv 2(mod 13)$
Try all x from 0 to 12 we don't find any solutions.
e)$x^2 \equiv 1(mod 8)$
Try all x from 0 to 7 we find that x = 1, 3, 5, 7 are the solutions for this equation.
f)$x^3 - x^2 + 2x - 2 \equiv 0(mod 11)$
We have $x^3 - x^2 + 2x - 2 = (x - 1)(x^2 + 2)$
Because 11 is prime number so $x^3-x^2+2x-2 \equiv 0(mod 11) \leftrightarrow (x-1) \equiv 0(mod 11) or (x^2+2) \equiv 0(mod 11)$. We found that when x = 3 or x = 8, $x^2 + 2 \equiv 0(mod 11)$. So x = 3 and x = 8 are two solutions. Otherwise, when x = 1 it made $x - 1 \equiv 0(mod 11)$. So x = 1 also the solution for this conguences. In conclusion, this congruences has three solutions: x = 1, x = 3 and x = 8. g)

$$x \equiv 1(mod 5)$$
$$x \equiv 2(mod 7)$$

We have 5 and 7 are relative primes so it exist a = 3 is the inverse of 7 in modulo 5, and b = 3 is the inverse of 5 in modulo 7. We found that when $x \equiv 1*7*3+2*5*3 \equiv 36 \equiv 1(mod 35)$. So x = 1 is the solution.

□

Problem 1.18. Suppose that $g^a \equiv 1(mod m)$ and that $g^b \equiv 1(mod m)$. Prove that $g^{gcd(a,b)} \equiv 1(mod m)$

Proof. By Euclide Algorithm we have:
$\exists u, v$ such that au + bv = gcd(a,b). So, $g^{gcd(a,b)} \equiv g^{au+bv} \equiv (g^a)^u.(g^b)^v \equiv 1(mod m)$. □

Problem 1.19. Prove that if a_1 and a_2 are units modulo m, then a_1a_2 is a unit modulo m.

Proof. We have a_1 is a unit modulo m it means gcd(a_1, m) = 1 so when we factorize a_1 and m it doesn't have any common prime number. The same thing occur with a_2 and m. So when we multiply a_1 and a_2, no prime number belong to factorization of m appear in a_1*a_2. It means gcd(m, a_1a_2) = 1, so a_1a_2 is a unit modulo m. □

.

Problem 1.23.d. Prove that if gcd(m,n) = 1, then the pair of congruences $x \equiv a(modm)$ and $x \equiv b(modn)$ has a solution for any choice of a and b. Also give an example to show that the condition gcd(m, n) = 1 is necessary.

Proof. Because (m,n) = 1 so it exist u and v such that: $u*m \equiv 1(modn)$ and $v*n \equiv 1(modm)$.
When we chose x = a*u*m + b*v*n, it will sastify two congruences.
Example:
Let's choose m = 3, n = 9. There is no x sastify $x \equiv 0(mod3)andx \equiv 1(mod9)$.

□

Problem 1.24. Let N, g, and A be positive integers (note that N need not be prime). Prove that the following algorithm, which is a low-storage variant of the square-and-multiply algorithm described in Section 1.3.2, return the value $g^A(modN)$.

Input. Positive integer N, g, and A.
1. Set a = g and b = 1.
2. Loop while $A > 0$.
3.If $A \equiv 1(mod2)$, set b = b.a(mod N)
4.Set $a = a^2(modN)$ and A = A div 2.
5.If $A > 0$, continue with loop at Step 2.
6.Return the number b, which equals $g^A(modN)$

Proof. Firsly, we should compute the binary expansion of A as
$A = A_0 + A_1 * 2 + A_2 * 2^2 + ... + A_r * 2^r$ with $A_0, A_1, ..., A_r \in 0, 1$
The loop will generate all $a_0 \equiv g(modN), a_1 \equiv g^2(modN), ..., a_i \equiv g^{2^i}(modN)$, and it will save in the variable a on each step.
On i th step, when $A \equiv 1(mod2)$ it mean $A_i = 1$ so we will multiply g^{2^i} with b. When we finish the loop, b is the answer of g^A (mod N).

□