MATH 1025: Introduction to Cryptography

Midterm Review

Solutions

Problem 1. Solve each of the following systems of congruences (or explain why no solution exists).

(a) $x \equiv 3 \pmod 7$ and $x \equiv 4 \pmod 9$.

Solution. The first congruence gives $x = 3 + 7k, k \in \mathbb{Z}$. Substituting into the second congruence, we get $3 + 7k \equiv 4 \pmod 9$ or $k \equiv 4 \pmod 9$, since $4 \equiv 7^{-1} \pmod 9$. Hence, $x \equiv 31 \pmod{63}$.

(b) $x \equiv 4 \pmod 6$ and $x \equiv 5 \pmod{14}$.

Solution. The first congruence gives $x = 4 + 6k, k \in \mathbb{Z}$. Substituting into the second congruence, we get $4 + 6k \equiv 5 \pmod{14}$ or $6k \equiv 1 \pmod{14}$. As $\gcd(6, 14) = 2 \neq 1$, we have that 6 is not invertible modulo 14, hence, there are no solutions.

Problem 2.

(a) Using that $16399 = 23^2 \cdot 31$ and the properties of Euler's totient function, find $\varphi(16399)$.

Solution. $\varphi(16399) = \varphi(23^2)\varphi(31) = 23 \cdot (23 - 1) \cdot 30 = 15180$.

(b) What is the order of the multiplicative group $\mathbb{Z}^\times_{16399}$?

Solution. $|\mathbb{Z}^\times_{16399}| = \varphi(16399) = 15180$.

Problem 3.

(a) What is the order of the multiplicative group $\mathbb{Z}^\times_{15}$?

Solution. $|\mathbb{Z}^\times_{15}| = \varphi(3)\varphi(5) = 8$.

(b) Which abelian group is that?

Solution. There are 3 nonisomorphic abelian groups of order 8: $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. We need to find out, which one of them $\mathbb{Z}^\times_{15}$ is isomorphic to. First as a set $\mathbb{Z}^\times_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Notice that the order of 2 is 4, as $2^4 = 16 \equiv 1 \pmod{15}$, but $2^2 = 4 \not\equiv 1 \pmod{15}$. The presence of an element of order 4 allows to conclude that the group under consideration is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (the latter contains only elements of order 2 and isomorphisms preserve orders). Similarly, $\mathbb{Z}_8$ contains only one element of order 2, but $4^2 \equiv 1 \pmod{15}$ and $11^2 \equiv 1 \pmod{15}$, hence, the only remaining possibility is $\mathbb{Z}^\times_{15} \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.

Problem 4. Let p be an odd prime number and $k \in \mathbb{Z}_{>0}$. Show that $\varphi(p^k) = p^k - p^{k-1}$.

Solution. Each p's element is divisible by p and not coprime to p^k. As the total number of such elements between 1 and $p^k - 1$ is equal to $p^k : p = p^{k-1}$, we get $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$.

Problem 5. Compute the discrete logarithm $\log_2(13)$ for the prime $p = 23$, i.e., you must solve the congruence $2^x \equiv 13 \pmod{23}$.

Solution. $2^7 = 128 \equiv 13 \pmod{23}$.

Problem 6. Let p be an odd prime and let g be a primitive root modulo p. Prove that a has a square root modulo p if and only if its discrete logarithm $\log_g(a)$ modulo p is even.

Solution. Recall that a is a square if and only if there is $b = g^k$, s.t. $a = b^2 = g^{2k}$. Let a be a square, then $\log_g(a) = \log_g(g^{2k}) = 2k$ is an even number.

Problem 7. Use Shanks' baby-step giant-step method to solve the following discrete logarithm problem:

$$11^x = 21 \text{ in } \mathbb{F}_{71}.$$

Solution.

Step 1. We find $n = \lfloor\sqrt{70}\rfloor + 1 = 9$.

Step 2. Then compute $11^{-1} \equiv 13 \pmod{71}$ and $11^{-9} \equiv 13^9 \equiv 7 \pmod{71}$ and obtain the lists

'Baby-step list' $L_1 = \{11^0, 11^1, 11^2, \ldots, 11^8, 11^9\} = \{1, 11, 50, 53, 15, 23, 40, 14, 12, 61\}$;

'Giant-step list': $L_2 = \{21, 21 \cdot 7, 21 \cdot 7^2, \ldots, 21 \cdot 7^8, 21 \cdot 7^9\} = \{21, 5, 35, 32, 11, 6, 42, 10, 70, 64\}$.

Step 3. The element in the intersection is $11 \in L_1 \cap L_2$, giving rise to the congruence $11 = 11^1 \equiv 21 \cdot 11^{-9 \cdot 4}$ or $11^{1+36} \equiv 21$. The answer is 37.

Problem 8.

(a) Compute the Legendre symbol $\left(\frac{5670}{10007}\right)$ (use that $5670 = 2 \cdot 3^4 \cdot 5 \cdot 7$).

Solution. $\left(\frac{5670}{10007}\right) = \left(\frac{2 \cdot 3^4 \cdot 5 \cdot 7}{10007}\right) = \left(\frac{2}{10007}\right)\left(\frac{3}{10007}\right)^4\left(\frac{5}{10007}\right)\left(\frac{7}{10007}\right) = \left(\frac{2}{10007}\right)\left(\frac{5}{10007}\right)\left(\frac{7}{10007}\right) =$ (one has $\left(\frac{3}{10007}\right)^4 = 1$ as $(\pm 1)^4 = 1$ regardless of the sign). Using the law of quadratic reciprocity, we compute

$$\left(\frac{2}{10007}\right) = 1 \text{ as } 10007 \equiv 7 \pmod{8},$$
$$\left(\frac{5}{10007}\right) = (-1)^{\frac{(10007-1)(5-1)}{4}}\left(\frac{10007}{5}\right) = \left(\frac{2}{5}\right) = -1 \text{ and}$$
$$\left(\frac{7}{10007}\right) = (-1)^{\frac{(10007-1)(7-1)}{4}}\left(\frac{10007}{7}\right) = -\left(\frac{4}{7}\right) = -1.$$

Finally, $\left(\frac{5670}{10007}\right) = 1 \cdot (-1) \cdot (-1) = 1$.

(b) Compute the Jacobi symbol $\left(\frac{462}{1781}\right)$ (use that $462 = 2 \cdot 3 \cdot 7 \cdot 11$ and $1781 = 5^3 \cdot 11$).

Solution. $\left(\frac{462}{1781}\right) = \left(\frac{462}{5}\right)^3 \left(\frac{462}{11}\right) = \left(\frac{462}{5}\right)^3 \left(\frac{2}{11}\right) \left(\frac{3}{11}\right) \left(\frac{7}{11}\right) \left(\frac{11}{11}\right) = 0.$