MATH 1025: Introduction to Cryptography

Midterm Review

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

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

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

Problem 2.

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

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

Problem 3.

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

(b) Which abelian group is that?

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

Problem 5. Compute the discrete logarithm $\ell og_2(13)$ for the prime $p = 23$, i.e., you must solve the congruence $2^x \equiv 13 \pmod{23}$.

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 $\ell og_g(a)$ modulo p is even.

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

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

Problem 8.

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

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