Dartmouth College Department of Mathematics
Math 148 Introduction to Public Key Cryptography and Elliptic Curves
Spring 2025

Problem Set # 2 (due by Canvas upload by the end of Friday 2 May)

Problems:

1. Use the babystep-giantstep algorithm to solve $11^x = 21$ in $\mathbb{F}_{71}$. Explain all of the steps in your computation.

2. Let g be a generator in $\mathbb{F}_p^\times$. Suppose that $x = a$ and $x = b$ are both solutions to the congruence $g^x \equiv h \pmod{p}$. Show that $a \equiv b \pmod{p-1}$. Explain why this implies that the map

$$\log_g : \mathbb{F}_p^\times \to \mathbb{Z}/(p-1)\mathbb{Z} \tag{1}$$

is well-defined.

3. In this problem we will demonstrate an algorithm for determining square roots modulo a natural number m.

(a) Let p be a prime satisfying $p \equiv 3 \pmod{4}$. Let a be an integer such that the congruence $x^2 \equiv a \pmod{p}$ has a solution. Prove that $b \equiv a^{(p+1)/4} \pmod{p}$ is a solution, i.e., it satisfies $b^2 \equiv a \pmod{p}$.

(b) Let p be an odd prime. Given b such that $b^2 \equiv a \pmod{p}$, find another number x such that $x \not\equiv b \pmod{p}$ and $x^2 \equiv a \pmod{p}$.

(c) Given a composite number m which factors as $m = pq$ where p and q are distinct primes, explain how to solve $x^2 \equiv a \pmod{m}$ if you know solutions to $y^2 \equiv a \pmod{p}$ and $z^2 \equiv a \pmod{q}$.

(d) Find four square roots of 2833 modulo $4189 = 59 \cdot 71$. Note that your four square roots should be distinct modulo 4189.

4. Let $p = 1801$. Compute $\log_{11} 249$ using the Pohlig-Hellman algorithm. Explain all of the steps in your computation.

5. Find a twin pair of primes (a, b) smaller than 1000 such that solving the discrete log problem requires fewer computations for the larger one than for the smaller one when using the Pohlig-Hellman algorithm or determine that no such pair exists. You may want to write a short program for your computations.

6. An integer M is called *B-power-smooth* if every prime power p^e dividing M satisfies $p^e \leq B$. For example, $180 = 2^2 \cdot 3^2 \cdot 5$ is 10-power-smooth, since the largest prime power dividing 180 is 9, which is smaller than 10.

(a) Suppose that M is B-power-smooth. Prove that M is also B-smooth.

(b) Suppose that M is B-smooth. Is it true that M is also B-power-smooth? Either prove that it is true or give an example for which it is not true.

(c) The following is a list of 10 randomly chosen numbers between 1 and 1000, sorted from smallest to largest. Which of these numbers are 10-power-smooth? Which of them are 10-smooth?

$$\{84, 141, 208, 318, 366, 440, 530, 726, 765, 817\}$$

(d) Prove that M is B-power-smooth if and only if M divides the least common multiple of $\{1, 2, \ldots, B\}$.