601.445/601.645: Practical Cryptographic Systems September 28, 2021

Weekly Homework 2

Instructor: Matthew Green and Alishah Chator *Due: 11:59pm, October 5*

Name: ____

The assignment should be completed individually. You are permitted to use the Internet and any printed references. You may find Katz-Lindell §11.5 (§10.4 in the first edition) or Handbook of Applied Cryptography §8.2 (in the online public edition) helpful.

Please submit the completed assignment via Gradescope.

Problem 1: Determine whether the following are Groups. Justify your claims.

1. The integers under addition, $(\mathbb{Z}, +)$
2. The integers under multiplication, $(\mathbb{Z}, \cdot)$
3. The real numbers under multiplication, $(\mathbb{R}, \cdot)$
4. The positive integers under addition, $(\mathbb{Z}^+, +)$
5. The positive integers under subtraction, $(\mathbb{Z}^+, -)$

Problem 2: Do the following problems. Show your work.

1. Apply the extended Euclidean algorithm to primes 59 and 17 to find x and y such that $59x + 17y = 1$.
2. What is the inverse of 59 (*i.e.,* 8) modulo 17 and what is the inverse of 17 modulo 59?
3. Prove that 2 is a generator of $\mathbb{Z}_{59}^*$, while 4 is not a generator of $\mathbb{Z}_{59}^*$. (HINT: Recall, g is a generator of $\mathbb{Z}_{59}^*$, where p is prime, if and only if $g^a \neq 1 \ mod \ p$ for every non-trivial divisor $1 < a < p-1$ of $(p-1)$.
4. List all of the subgroups of $\mathbb{Z}_{23}^*$ and provide one generator for each subgroup.[1] See HAC §2.5 for definitions if this is helpful.

[1]Note: a subgroup is a cyclic group that is contained within the larger group. You can find subgroups by doing what we did in class: picking an element of the group and seeing whether it generates the whole group or just a subset.

Problem 3: Use the Chinese Remainder Theorem to solve the following problems. You may find the constructive proof of the theorem[2] useful in computing the solutions.

1. Find the unique $x \in \mathbb{Z}_{35}$ such that $x \equiv 4 \ mod \ 5$ and $x \equiv 3 \ mod \ 7$.

2. Find the unique $x \in \mathbb{Z}_{110}$ such that $x \equiv 2 \ mod \ 10$ and $x \equiv 9 \ mod \ 11$.

3. Find the unique $x \in \mathbb{Z}_{385}$ such that $x \equiv 3 \ mod \ 5$, $x \equiv 4 \ mod \ 7$ and $x \equiv 8 \ mod \ 11$.

4. **Quadratic Residues.** An integer x is called a *quadratic residue* modulo n if $\exists y \in \mathbb{Z}$ s.t. $y^2 \equiv x \ mod \ n$. That is, an integer is a quadratic residue if it is equivalent to a perfect square modulo n. In this problem, we will walk through solving problems with quadratic residues of the form $x^2 \equiv a \ mod \ n$ where p, q are primes, $n = pq$, and $p \equiv q \equiv 3 \ mod \ 4$. Suppose we have $x^2 \equiv 11 \ mod \ 133$. Let us find all the possible values of x (there are four!).

   (a) First factor $n = 133$.

   (b) Now we should have a p, q such that $n = pq$ and $p \equiv q \equiv 3 \ mod \ 4$. For this problem label the smaller factor of n as p and the larger one as q. Solve $y^2 \equiv 11 \ mod \ p$. It should be straight forward to compute the square root of this value. You should find two distinct positive integers $< p$ such that this equation holds (remember you can rewrite negative values modulo p as a positive integer $< p$). We will refer to these two square roots as y_1, y_2

   (c) Now let us attempt do do the same to solve $z^2 \equiv 11 \ mod \ q$. Here we will see it is not as clear how to compute a square root. Instead we can use something called *Euler's Criterion*, which gives us a way to compute the square roots of a quadratic residue $z^2 \equiv a \ mod \ q$ as long as it is modulo a prime $q \equiv 3 \ mod \ 4$. The two square roots are $z_1 \equiv a^{(q+1)/4} \ mod \ q$ and $z_2 = q - x_1$.

   (d) Now to compute the four square roots of $x^2 \equiv 11 \ mod \ 133$ we have to apply the Chinese Remainder Theorem to solve each of the resulting 4 equations:

$$x_1 \equiv y_1 \ mod \ p, \ \ x_1 \equiv z_1 \ mod \ q$$

$$x_2 \equiv y_1 \ mod \ p, \ \ x_2 \equiv z_2 \ mod \ q$$

$$x_3 \equiv y_2 \ mod \ p, \ \ x_3 \equiv z_1 \ mod \ q$$

$$x_4 \equiv y_2 \ mod \ p, \ \ x_4 \equiv z_2 \ mod \ q$$

[2] https://en.wikipedia.org/wiki/Chinese_remainder_theorem#Existence_(constructive_proof)