Topics in CS: Problem Set 2

Due date: November 16, 2025.

Question 1. (30 points)

1. Does 5 divide $2^{12345} - 8^{4328}$?
2. Does 7 divide $2^{12345} - 8^{4328}$?
3. Compute $7^{(3^{10000})} \bmod 101$.

   You can rely on the facts that $3^{40} \equiv 1 \bmod 100$ and $7^{100} \equiv 1 \bmod 101$. We will soon prove Fermat's little theorem and Euler's totient theorem, justifying these congruences.

Question 2. (30 points) Let $a, b \in \mathbb{Z} \setminus \{0\}$. The *least common multiplier* of a and b, denoted $\mathsf{lcm}(a, b)$, is defined as

$$\mathsf{lcm}(a, b) = \min\{k \in \mathbb{N} \ : \ a \mid k \wedge b \mid k\}.$$

1. Prove that $\mathsf{lcm}(a, b)$ is well defined.
2. Suppose that $a, b > 0$. Prove that $\mathsf{lcm}(a, b) = a$ if and only if $b \mid a$.
3. Let $c \in \mathbb{Z}$ and suppose that $a, b, c > 0$. Prove that $\mathsf{lcm}(ca, ca) = c \cdot \mathsf{lcm}(a, b)$.

Question 3. (20 points)

1. Implement the division algorithm $\mathsf{Div}(x, y)$ for inputs of arbitrary length.
2. Sample an 8 bit number and compute its quotient and remainder with respect to 23.
3. Sample a 512 bit number and compute its quotient and remainder with respect to 12345.

Question 4. (20 points)

1. Implement the multiplication-modulo-N algorithm $\mathsf{ModMult}(x, y, N)$ for inputs of arbitrary length. Use the algorithm Div you implementer in the previous item.
2. Sample an 8 bit number N and $x, y \in \mathbb{Z}_N$ and compute $xy \bmod N$.
3. Sample a 512 bit number N and $x, y \in \mathbb{Z}_N$ and compute $xy \bmod N$.

Good luck!