CSE 40622 Cryptography
Writing Assignment 02 (Lecture 02)

Name & netID: Walker Bagley (wbagley)

1. (10 pts) Calculate the remainders of these with the modulus 19. Simplify the operands before you conduct arithmetic calculations. You need to show how each operand is simplified with the modular reduction.

   1.1. $(138 + 38) \mod 19$
   Answer:

$$\begin{aligned}(138 + 38) &\equiv (5 + 0) \pmod{19} \\ &\equiv 5 \pmod{19}\end{aligned}$$

   1.2. $(19 - 50) \mod 19$
   Answer:

$$\begin{aligned}(19 - 50) &\equiv (0 - 12) \pmod{19} \\ &\equiv -12 \pmod{19} \\ &\equiv 7 \pmod{19}\end{aligned}$$

   1.3. $40 \cdot 22 \mod 19$
   Answer:

$$\begin{aligned}(40 \cdot 22) &\equiv (2 \cdot 3) \pmod{19} \\ &\equiv 6 \pmod{19}\end{aligned}$$

   1.4. $6 \cdot (21^{-1}) \mod 19$
   - Please find the multiplicative inverse of 21 modulo 19 first.

   Answer:

$$\begin{aligned}21^{-1} &\equiv 10 \pmod{19} \\ 6 \cdot (21^{-1}) &\equiv (6 \cdot 10) \pmod{19} \\ &\equiv 60 \pmod{19} \\ &\equiv 3 \pmod{19}\end{aligned}$$

   1.5. $20^{501} \mod 19$
   Answer:

$$\begin{aligned}20 &\equiv 1 \pmod{19} \\ 20^2 &\equiv 1 \pmod{19} \\ 20^n &\equiv 1 \pmod{19} \\ 20^{501} &\equiv 1 \pmod{19}\end{aligned}$$

2. (10 pts) Find an example (i.e., the values of x, y, c, n) to show that, even if $x \equiv y \pmod{n}$ and x/c and y/c are both integers, $x/c \not\equiv y/c \pmod{n}$.

Answer:

$$\begin{cases} x = 10 \\ y = 25 \\ c = 5 \\ n = 15 \end{cases}$$

$$\begin{aligned} 10 &\equiv 25 \pmod{15} \\ 10/5 &= 2 \\ 25/5 &= 5 \\ 2 &\not\equiv 5 \pmod{15} \end{aligned}$$

3. (10 pts) Use the Euclidean algorithm to calculate the GCD of 30 and 151.

Answer:

$$\begin{aligned} 151 &= 5 \cdot 30 + 1 \\ 30 &= 30 \cdot 1 + 0 \\ \gcd(30, 151) &= 1 \end{aligned}$$

4. (10 pts) Use the extended Euclidean algorithm to calculate the multiplicative inverse $30^{-1} \mod 151$.

Answer:

$$\begin{aligned} 151 &= 5 \cdot 30 + 1 \\ 1 &= 151 - 5 \cdot 30 \\ 1 &\equiv (151 - 5 \cdot 30) \pmod{151} \\ 1 &\equiv (0 - 5 \cdot 30) \pmod{151} \\ 1 &\equiv -5 \cdot 30 \pmod{151} \\ 1 &\equiv 146 \cdot 30 \pmod{151} \\ 30^{-1} &\equiv 146 \pmod{151} \end{aligned}$$

5. (10 pts) Use the squaring method discussed in the lecture to compute $117^{140} \mod 203$.

Answer:

$$
\begin{aligned}
117^1 &\equiv 117 \pmod{203} \\
117^2 &\equiv 88 \pmod{203} \\
117^4 &\equiv 88^2 \equiv 30 \pmod{203} \\
117^8 &\equiv 30^2 \equiv 88 \pmod{203} \\
117^{16} &\equiv 88^2 \equiv 30 \pmod{203} \\
117^{32} &\equiv 30^2 \equiv 88 \pmod{203} \\
117^{64} &\equiv 88^2 \equiv 30 \pmod{203} \\
117^{128} &\equiv 30^2 \equiv 88 \pmod{203} \\
117^{140} &\equiv 117^{128} \cdot 117^8 \cdot 117^4 \pmod{203} \\
&\equiv 88 \cdot 88 \cdot 30 \pmod{203} \\
&\equiv 88^2 \cdot 30 \pmod{203} \\
&\equiv 30 \cdot 30 \pmod{203} \\
&\equiv 30^2 \pmod{203} \\
&\equiv 88 \pmod{203}
\end{aligned}
$$