CSE 40622 Cryptography, Spring 2018
Written Assignment 01 (Lecture 01-02)

Name: **Jasmine Walker**

1. (10 pts) Calculate the remainders of these with the modulus 17. You can calculate modulo operations without finding q, r explicitly.

   (a) $(38 + 17) \mod 17$
   Answer:
   $(38 + 17) \mod 17 = 55 \mod 17 =$ **4**

   (b) $(11 - 82) \mod 17$
   Answer:
   $(11 - 82) \mod 17 = -71 \mod 17 =$ **-14**

   (c) $5 \cdot 33 \mod 17$
   Answer:
   $5 \cdot 33 \mod 17 = 165 \mod 17 =$ **12**

   (d) $5 \cdot 33^{-1} \mod 17$

   - Please find the multiplicative inverse modulo 17 for 33^{-1}.

   Answer:
   $5 \cdot 33^{-1} \mod 17 = ((5 \mod 17) \cdot (33^{-1} \mod 17)) \mod 17$
   $33 \mod 17 = (34 - 1) \mod 17 = -1 \mod 17;$
   If we insert a := $33^{-1} \mod 17$, $(33 \cdot a) \mod 17 = (-1 \cdot a) \mod 17 = 1$
   By inspection of the second term, a = **16**
   $((5 \mod 17) \cdot (33^{-1} \mod 17)) \mod 17 = (5 \cdot 16) \mod 17 = 80 \mod 17 =$ **12**

   (e) $8^3 \mod 17$
   Answer:
   $8^3 \mod 17 = 512 \mod 17 =$ **2**

2. (10 pts) Prove or disprove the following proposition:

   Suppose x, y, n are positive integers. If $x \equiv y \pmod{n}$ and c is an integer that divides both x and y (*i.e.,* x/c and y/c are integers), then we have

   $$x/c \equiv y/c \pmod{n}$$

   * Please allow yourself to recognize the division / while you answer this question (but you'll forget it completely again, right?).

   Answer:
   Counterexample:
   $15 \equiv 3 \pmod{12}$; c = 3
   $(15/3) \not\equiv (3/3) \pmod{12}$
   $5 \not\equiv 1 \pmod{12}$
   This proposition is false.

3. (10 pts) Use the Euclidean algorithm to calculate the GCD of 17 and 131.

   Answer:
   Euclidean algorithm : if $x = q \cdot d + r$, then gcd(x, d) = gcd(d, r)
   $131 = 17 \cdot 7 + 12$
   $17 = 1 \cdot 12 + 5$
   $12 = 2 \cdot 5 + 2$
   $5 = 2 \cdot 2 + 1$
   $2 = 2 \cdot 1 + 0$
   So, the GCD of 17 and 131 is **1**.

4. (10 pts) Use the extended Euclidean algorithm to calculate the multiplicative inverse $17^{-1} \mod 131$.

   Answer:
   From above,
   $131 = 17 \cdot 7 + 12 \Rightarrow 12 = 131 - 17 \cdot 7$
   $17 = 1 \cdot 12 + 5 \Rightarrow 5 = 17 - 1 \cdot 12$
   $12 = 2 \cdot 5 + 2 \Rightarrow 2 = 12 - 2 \cdot 5$
   $5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2$

   $1 = 5 - 2(12 - 5(2)) = 12(-2) + 5(5)$
   $1 = 12(-2) + 5(17 - 1(12)) = 12(-7) + 17(5)$
   $1 = 17(5) + (131 - 17(7))(-7) = 131(-7) + 17(54)$
   So, $17^{-1} \mod 131 = \mathbf{54}$

5. (10 pts) Use the squaring method discussed in the lecture to compute $137^{100} \mod 201$.

   Answer:
   $137^2 \mod 201 = 76$
   $137^4 \mod 201 = ((137^2 \mod 201) \cdot (137^2 \mod 201)) \mod 201 = 148$
   $137^8 \mod 201 = ((137^4 \mod 201) \cdot (137^4 \mod 201)) \mod 201 = 196$
   $137^{16} \mod 201 = ((137^8 \mod 201) \cdot (137^8 \mod 201)) \mod 201 = 25$
   $137^{32} \mod 201 = ((137^{16} \mod 201) \cdot (137^{16} \mod 201)) \mod 201 = 22$
   $137^{64} \mod 201 = ((137^{32} \mod 201) \cdot (137^{32} \mod 201)) \mod 201 = 82$

   $137^{100} \mod 201 = ((137^{64} \mod 201) \cdot (137^{32} \mod 201) \cdot (137^4 \mod 201)) \mod 201$
   $= (82 \cdot 22 \cdot 148) \mod 201 = 266992 \mod 201 = \mathbf{64}$