Assignment 2, due 9/27, before class

1. (30) Textbook problems 1.11, 1.12, 1.13. For these problems, use the the modular arithmetic rules we learned in class (ref. "algNumbers.pdf ", and Chapter 1 in textbook). You may also find the following fact useful:

   Definition 0.1 *Let $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N | gcd(a, n) = 1\}$ (i.e., set of integers co-prime with N). Let x denote the order of $\mathbb{Z}_N^*$. Then, without loss of generality, if $a \in \mathbb{Z}_N^*$:*

   $$a^y \mod N = a^{y \mod x} \mod N$$

   where $y \geq 0$.

   Example of how to apply the definition: Find $4^{50} \mod 9$.
   Here $N = 9$, So, $\mathbb{Z}_N^* = \mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$, and so, $x = |\mathbb{Z}_9^*| = 6$. $y = 50$.

   $$\begin{aligned} 4^{50} \mod 9 &= 4^{50 \mod 6} \mod 9 \\ &= 4^2 \mod 9 \\ &= 16 \mod 9 \\ &= 7 \end{aligned}$$

   As you can guess, the rule will be useful only when $y \geq x$, which it is, in our 3 problems.[1]

2. (40 points) We had worked out a few examples of Euclid's algorithm and the extended Euclidean algorithm in class. Use that as a reference to solve the following:

   (a) Find $d = gcd(423, 128)$. Are they co-prime? Now find integers x, y, such that $d = x \cdot 423 + y \cdot 128$.

   (b) Find $d = gcd(588, 210)$. Are they co-prime? Now find integers x, y, such that $d = x \cdot 588 + y \cdot 210$.

   (c) Find $d = gcd(420, 96)$. Are they co-prime? Now find integers x, y, such that $d = x \cdot 420 + y \cdot 96$.

   (d) Find $d = gcd(33, 27)$. Are they co-prime? Now find integers x, y, such that $d = x \cdot 33 + y \cdot 27$.

3. (15 points) In class, we had computed multiplicative inverses of elements in $\mathbb{Z}_7$. Find the multiplicative inverses of all elements in $\mathbb{Z}_{23}$.

4. (15 points) Textbook problem 1.17.

How to submit: Upload your **pdf** file on Canvas. You can use my posted template if you wish, for typesetting your assignment, but aren't required to do so.

[1] This rule holds for *any* group G, but we have only considered the special case of the group $\mathbb{Z}_N^*$.