MODERN ALGEBRA I FALL 2018:
SEVENTH PROBLEM SET

1. Let \( n \in \mathbb{N} \), and let \( d \) be a divisor of \( n \). Suppose that \( a, a' \in \mathbb{Z} \) and that \( a \equiv a' \mod n \). Show that \( d \mid a \iff d \mid a' \). Conclude that \( \gcd(a, n) = \gcd(a', n) \), i.e. that the function \( f(a) = \gcd(a, n) \) is a well-defined function from \( \mathbb{Z}/n\mathbb{Z} \) to \( \mathbb{Z} \).

2. By factorization, the gcd of 9 and 16 is 1. Via trial and error (or something more systematic if you have seen the Euclidean algorithm before), find integers \( n \) and \( m \) such that \( 9n + 16m = 1 \).

3. Do there exist integers \( x \) and \( y \) such that \( 57x + 93y = 2 \)? Why or why not? Do there exist integers \( x \) and \( y \) such that \( 57x + 93y = -6 \), and why or why not?

4. For each of the following \( a \mod n \), find \( a^{-1} \mod n \), i.e. find an integer \( x \) with \( ax \equiv 1 \mod n \), or explain why such an integer does not exist:

\[
5^{-1} \mod 11; \quad (21)^{-1} \mod 28; \quad 2^{-1} \mod 101; \quad 4^{-1} \mod 101.
\]

5. Let \( n = 2k+1 \) be an odd number. What is \( 2^{-1} \mod n \)? What happens when \( n = 2k \) is even?

6. (i) Show that, for \( a, b \in \mathbb{Z} \), if \( a \) is relatively prime to \( b \), then every divisor \( d \) of \( a \) is relatively prime to \( b \). (You can begin by writing \( 1 = ax + by \).)

(ii) Show that, \( a, n, m \in \mathbb{Z} \), if \( a \) is relatively prime to \( n \) and to \( m \), then \( a \) is relatively prime to \( nm \). (Again, you can start by writing \( 1 = ax + ny, 1 = aw + mz \) for some integers \( x, y, z, w \).) Conversely, if \( a \) is relatively prime to \( nm \), show that \( a \) is relatively prime to \( n \) and to \( m \). (In fact, this is a special case of (i).)

7. If \( d = \gcd(a, b) \), then, using the definition of a gcd, show that \( a/d \) and \( b/d \) are relatively prime.

8. For the group \( \mathbb{Z}/18\mathbb{Z} \), list all of the possible subgroups of \( \mathbb{Z}/18\mathbb{Z} \) together with all of their generators, and verify that \( \sum_{d \mid 18} \varphi(d) = 18 \).

9. (i) What is the order of the element 21 in the group \( \mathbb{Z}/36\mathbb{Z} \)? What is the smallest positive integer \( a \) such that, viewing \( a \) as an element of \( \mathbb{Z}/36\mathbb{Z} \), \( (21) = \langle a \rangle \)?
(ii) What is the order of the element 30 in the group $\mathbb{Z}/45\mathbb{Z}$? What is the smallest positive integer $a$ such that, viewing $a$ as an element of $\mathbb{Z}/45\mathbb{Z}$, $\langle 30 \rangle = \langle a \rangle$?

(iii) What is the order of $(21, 30)$ in the group $(\mathbb{Z}/36\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$?

10. Consider the group $(\mathbb{Z}/7\mathbb{Z})^*$ (under multiplication, of course). What is the order of $(\mathbb{Z}/7\mathbb{Z})^*$? Show that $(\mathbb{Z}/7\mathbb{Z})^*$ is cyclic by finding a generator. Then list all of the possible subgroups of $(\mathbb{Z}/7\mathbb{Z})^*$ together with all of their generators. (Be systematic, and use the theory we have developed in class. You already know what all the possible orders of the subgroups are and that there is exactly one of each order, and how to write it in terms of a generator of $(\mathbb{Z}/7\mathbb{Z})^*$.)