Steven Rosendahl
Homework 6

1. For each of the following linear congruences of the form $ax \equiv c \mod n$, determine whether a solution exists. If so, find a formula for all solutions and determine how many solutions there are in $\mathbb{Z}_n$.

   (a) $3x \equiv 5 \mod 7$

   The *gcd* of a and n is 1, so there is a solution since $1 \mid 5$, and there is only one solution. If we solve the Diophantine equation $3x + 7y = 5$, we get a general solution for x as $x = -3 + 7n$. The solution we want is 4, since all other n give a solution equal to 4 in $\mathbb{Z}_7$.

   (b) $4x \equiv 9 \mod 12$

   This congruence has no solution since $gcd(4, 12) = 4$, but $4 \nmid 9$.

   (c) $18x \equiv 27 \mod 45$

   The $gcd(18, 45) = 9$, and $9 \mid 27$, so there is a solution, and in fact there are 9 solutions. If we solve the Diophantine equation $18x_0 + 45y_0 = 27$, we get that $x_0 = -1 + 5n$. The nine solutions can be found by starting with $n = 1$ to $n = 9$, and are $4, 9, 14, 19, 24, 29, 34, 39, 44$.

2. Let S denote the number of solution to the linear congruence $ax \equiv c \mod 20$. Prove that $S \in \{0, 1, 2, 4, 5, 10, 20\}$.

   We know that there are either 0 or $gcd(a, 20)$ solutions to the congruence $ax \equiv c \mod 20$. Suppose we have the set $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}$. We know that for these numbers, we will have a unique *gcd* with 20, and in fact all possible $gcd's$ will be represented in this set. If we find the *gcd* of a relatively prime number r and 20, then $gcd(r, 20) = 1$, so it is possible to have only one solution. In addition, $gcd(1, 20) = 1$, so we can eliminate this number as well. Now we can consider the set $B = A\backslash\{3, 7, 9, 11, 13, 17, 19\} = \{0, 2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18, 20\}$. For both 0 and 20, $gcd(0, 20) = gcd(20, 20) = 20$, so it is possible to have 20 solutions. Now consider the set $C = B\backslash\{0, 20\} = \{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18\}$. We can find all the elements of C such that $gcd(20, c) = 2$, which are $\{2, 6, 14, 18\}$, which leaves us with the set $D = \{4, 5, 8, 10, 12, 15, 16\}$. Now we can consider all the elements with which give us a *gcd* of 4, which are $\{4, 8, 12, 16\}$. This leaves us with the set $E = \{5, 15\}$. If we take any element of E and find $gcd(e, 20)$, we will get 5. Now we are only left with $gcd(10, 20) = 10$, which provides us with 10.

3. Suppose that $a, n \in \mathbb{Z}$ with $n \geq 3$ and $gcd(a, n) > 1$. Prove that there exist at least two non-zero points $c \in \mathbb{Z}_n$ such that $ax \equiv c \mod n$ has no solutions.

   Suppose $ax \equiv c \mod n$. Then there are either $gcd(a, n)$ solutions, or 0 solutions. If there are 0 solutions, then there are n number of non-solutions $c \in \mathbb{Z}_n$. Now suppose we have $gcd(a, n)$ solutions. We know that $gcd(a, n) > 1$, so we can let $c_1 = 1$. In this case, the only thing that divides c_1 is 1, but $gcd(a, n) > 1$, so there is no solution. We can also choose $c_2 = n - 1$. In this case, $n - 1 \equiv -1 \mod n$, and the only thing that divides -1 is 1. Since $gcd(a, n) > 1$, it does not divide -1, and therefore there are no solutions.

4. Determine whether each given point is a unit in the given $\mathbb{Z}_n$. If so, find its multiplicative inverse. If not, explain why it fails to be a unit.

   (a) $3 \in \mathbb{Z}_6$

   $3 \equiv 1 \mod 6$ implies that $3x + 6y = 1$. However, $gcd(3, 6) = 3$, which does not divide 1. Therefore, 3 is not a unit.

   (b) $7 \in \mathbb{Z}_{12}$

   The greatest common divisor of 7 and 12 is 1, so 7 is a unit in $\mathbb{Z}_{12}$. We have the relationship that $7x \equiv 1 \mod 12$, so $7x + 12y = 1$. One solution to this Diophantine equation is $x_0 = -5$, so all solutions can be expressed as $x = -5 + 12n,\ n \in \mathbb{Z}$. When $n = 1$, $x = 7$, which means that 7 is its own inverse.

(c) $13 \in \mathbb{Z}_{18}$

$gcd(13, 18) = 1$, so 13 is a unit in $\mathbb{Z}_{18}$. We can form the relationship $13 \equiv 1 \mod 18$, so we have that $13x + 18y = 1$. We have one solution, $x_0 = 7$, so all solutions x can be expressed as $x = 7 + 18n,\ n \in \mathbb{Z}$. If we choose $n = 0$, then we have $x = 7$, so 7 is the inverse of 13.

5. Suppose that p is prime.

(a) Prove that the set $\{0, 1, 2, \ldots, p^2 - 2, p^2 - 1\}$ contains exactly $p(p-1)$ elements which are relatively prime to p. Conclude that $\mathbb{Z}_{p^2}$ contains exactly $p(p-1)$ units.

Suppose we consider the set containing all non-units of $\mathbb{Z}_{p^2}$. This set contains elements of the form $\{0, p, 2p, 3p, \ldots, p(p-1)\}$. We know this set contains p elements, since it contains $p - 1$ multiples of p, and 0. If we subtract the number of elements in the $\mathbb{Z}_{p^2}$ from the number of non-units, we get $p^2 - p$, or $p(p-1)$.

(b) How many units does $\mathbb{Z}_{p^n}$ have? Prove your answer.

We can consider the set of non-units in $\mathbb{Z}_{p^n}$. This yields the set

$$\{0, p, 2p, \ldots, p^2, 2p^2, \ldots, p^3, \ldots, p^{n-1}(p-1)\}.$$

We know this set has size p^{n-1}, since it contains all multiples of powers of p up to the $n-1$ power. Again, we can subtract the sizes of the entire set and the set of non-units, and we get $p^n - p^{n-1} = p^{n-1}(p-1)$.

6. Suppose p and q are distinct primes. Prove that $\mathbb{Z}_{pq}$ contains exactly $(p-1)(q-1)$ units.

We can consider the set of non-units of $\mathbb{Z}_{pq}$, which takes the form

$$\{0, p, q, \ldots, np, mq\},\ n < p,\ m < q.$$

If we can determine the size of the set of non-units, then we can find the size of the units. We know that the non-units contain all multiples of p, np for some $n \in \mathbb{Z}$, and the set also contains all multiples of q, mq for some $m \in \mathbb{Z}$. We know we have up to p multiples of p, and q multiples of q, so there are $q+p$ multiples in total. However, when $n = m$, we have a duplicate multiple, so the set of non-units contains $q + p - 1$ elements. If we subtract the total size of the set from the size of the set of non-units, we have $pq - p - q + 1 = (p-1)(q-1)$.