Math 445 — Problem Set #2
Due: Friday, September 8 by 7 pm, on Canvas

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand.

If you do work with others, I ask that you write something along the top like "I collaborated with Steven Smale on problems 1 and 3". If you use a reference, indicate so clearly in your solutions. In short, be intellectually honest at all times.

Please write neatly, using complete sentences and correct punctuation. Label the problems clearly.

(1) Let a, b, c be integers. Show that if a and b are coprime, a divides c, and b divides c, then ab divides c.

> We can write $am + bn = 1$ for some $m, n \in \mathbb{Z}$ by the coprime hypothesis. Write $c = ak = b\ell$ for some $k, \ell \in \mathbb{Z}$. Then $k = k(am + bn) = (am)k + bkn = b\ell m + bkn = bt$ for $t = \ell m + kn$ so $c = abt$. (You can also argue using prime factorization.)

(2) Find all solutions to the equation $x^2 + [4]x = [5]$ in $\mathbb{Z}_8$ by trial and error (plugging in all possible values). Use this to find all integer solutions to $x^2 + 4x \equiv 5 \pmod 8$.

> Plugging in $x = [0], [1], \ldots, [7]$ into the left hand side, we get $[5]$ for $x = [1], [3], [5], [7]$.

(3) Given integers $a_1, \ldots, a_m$, the **greatest common divisor** of $a_1, \ldots, a_m$ is the largest integer that divides all of them.
(a) Compute $\gcd(12, 18, 42)$.
(b) Prove or disprove: If $\gcd(a, b, c) = 1$, then some pair of the numbers a, b, c is coprime.

> (a) Taking prime factorizations, $12 = 2^2 \cdot 3$, $18 = 2 \cdot 3^2$, $42 = 2 \cdot 3 \cdot 7$. Thus $2 \cdot 3 = 6$ is a common divisor, and no larger number can be, so it is the GCD.
> (b) This is false: for example, we can take $a = 6$, $b = 10$, $c = 15$.

(4) *Use the methods we have developed in class* to solve the following:
(a) Find all integer pairs (x, y) such that $275x - 126y = 9$.
(b) Find the inverse of $[126]$ in $\mathbb{Z}_{275}$.
(c) Find the smallest positive integer x such that

$$x \equiv 7 \pmod{126} \quad \text{and} \quad x \equiv 8 \pmod{275}.$$

> (a) To see if there is a solution, and to find a particular solution if so, we start by using the Euclidean algorithm to find the GCD of 275 and 126.
>
> $$275 = 2 \cdot 126 + 23$$
> $$126 = 5 \cdot 23 + 11$$
> $$23 = 2 \cdot 11 + 1$$

so the GCD is one, and

$$\begin{aligned} 23 &= 1 \cdot 275 - 2 \cdot 126 \\ 11 &= 1 \cdot 126 - 5 \cdot 23 = -5 \cdot 275 + 11 \cdot 126 \\ 1 &= 1 \cdot 23 - 2 \cdot 11 = 11 \cdot 275 - 24 \cdot 126 \end{aligned}$$

so

$$9 = (9 \cdot 11) \cdot 275 - (9 \cdot 24) \cdot 126$$

yielding particular solution $(x, y) = (99, 216)$. Then the general solution is of the form

$$(x, y) = (99 - 126n, 216 + 275n) \quad n \in \mathbb{Z}.$$

(b) From the equation $1 = 11 \cdot 275 - 24 \cdot 126$, an evident inverse is $[-24]$. While we're at it, an inverse for 275 modulo 126 is 11.

(c) For a particular solution, we use the formula $x = 7*126*(-24)+8*275*11 = 3032$. Every solution is of the form $3032+126*275n$ for $n \in \mathbb{Z}$. Since $0 \leq 3032 < 34650 = 126 * 275$, we must have the smallest positive solution.

(5) Solving linear equations in $\mathbb{Z}_n$: Let a, b, n be integers, with $n > 0$.

(a) Show that $[a]x = [b]$ has a solution x in $\mathbb{Z}_n$ if and only if $\gcd(a, n)$ divides b.

(b) Show that if $[a]x = [b]$ has a solution x in $\mathbb{Z}_n$, then there are exactly $\gcd(a, n)$ distinct solutions.

(c) Solve the equation $[20][x] + [17] = [29]$ in $\mathbb{Z}_{36}$.

(a) We have that $x = [k]$ is a solution to $[a]x = [b]$ if and only if $ak \equiv b \pmod{n}$. This is equivalent to $ak - b = n\ell$ for some $\ell \in \mathbb{Z}$, which we can rewrite as $ak + (-n)\ell = b$. From our theorem on linear diophantine equations, there exist k, ℓ that solve this if and only if $\gcd(a, n)$ divides b.

(b) Set $d = \gcd(a, n)$. Suppose that $ak \equiv b \pmod{n}$ has a solution. As above, k is a solution if and only there is some $\ell \in \mathbb{Z}$ such that $ak + (-n)\ell = b$. The general solution is of the form $(k, \ell) = (k_0 + n/dw, \ell_0 - a/dw)$ for some particular solution (k_0, ℓ_0) and $w \in \mathbb{Z}$. We claim that the integers of the form $k_0 + n/dw$ for $w \in \mathbb{Z}$ form exactly d congruence classes modulo n, namely $[k_0], [k_0 + n/d], \ldots, [k_0 + (d-1)\frac{n}{d}]$. Indeed, we can write $w = vd + u$ with $0 \leq u < d$, and so

$$k_0 + wn/d = k_0 + (vd + u)n/d = k_0 + un/d + vn \equiv k_0 + un/d \pmod{n},$$

showing that each such integer is in one of these congruence classes. A similar argument shows that these classes are distinct. Thus, there are exactly d solutions.

(c) First, rewrite as $[20][x] = [12]$. As above, we rewrite as $20x + 36y = 12$. We use the Euclidean algorithm to find the GCD of 20 and 36 and linear combination

$$2 \cdot 20 - 1 \cdot 36 = 4.$$

Multiplying by 3 gives a particular solution:

$$6 \cdot 20 - 3 \cdot 36 = 12,$$

and for the general solution we have

$$(x, y) = (6 + 9n, -3 - 5n), \quad n \in \mathbb{Z}.$$

Then, following the proof above, we get the four solutions

$$[6], [6+9] = [15], [6+18] = [24], [6+27] = [33].$$

The remaining problems are only required for Math 845 students, though all are encouraged to think about them.

(6) Solve the equation $8x + 25y + 15z = 19$ over $\mathbb{Z}$.

First, take the change of variables $x = u - 3y$, so $u = x - 3y$:

$$8(u - 3y) + 25y + 15z = 19$$
$$8u + y + 15z = 19.$$

Then we can express y in terms of u, z:

$$y = 19 - 8u - 15z$$
$$(u, y, z) = (u, 19 - 8u - 15z, z).$$

Then we rewrite in x, y, z-coordinates:

$$(x, y, z) = (u - 3y, 19 - 8u - 15z, z) = (-57 + 23u + 45z, 19 - 8u - 15z, z), \quad u, z \in \mathbb{Z}.$$