Homework 1
(Euclidean algorithm, Bezout's identity, gcd, lcm, linear Diophantine equations)
Due Wednesday, September 25 at 11:30am.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized.

Part A:

(1) For these problems, you should use a calculator to do the arithmetic.

(a) (3 points) Use the Euclidean algorithm to find $\gcd(12345, 67890)$. Then, find $\text{lcm}(12345, 67890)$.

We have that

$$\begin{aligned} 67890 &= 5 \cdot 12345 + 6165, \\ 12345 &= 2 \cdot 6165 + 15, \\ 6165 &= 411 \cdot 15 + 0. \end{aligned}$$

So $\gcd(12345, 67890) = 15$. Since

$$\gcd(12345, 67890) \cdot \text{lcm}(12345, 67890) = 12345 \cdot 67890,$$

we have that $\text{lcm}(12345, 67890) = 55873470$.

(b) (5 points) Find the general solution of the Diophantine equation $27x + 399y = -12$.

We have that

$$\begin{aligned} 399 &= 14 \cdot 27 + 21, \\ 27 &= 1 \cdot 21 + 6, \\ 21 &= 3 \cdot 6 + 3, \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

So $\gcd(399, 27) = 3$. Using back-substitution, we get

$$\begin{aligned} 3 &= 21 - 3 \cdot 6 \\ &= 21 - 3(27 - 1 \cdot 21) \\ &= 4 \cdot 21 - 3 \cdot 27 \\ &= 4(399 - 14 \cdot 27) - 3 \cdot 27 \\ &= 4 \cdot 399 - 59 \cdot 27. \end{aligned}$$

Note that $-12 = -4 \cdot 3$. So

$$-12 = -16 \cdot 399 + 236 \cdot 27.$$

Thus one solution is $x_0 = 236$ and $y_0 = -16$. The general solution is then

$$x = 236 - \frac{399n}{3} = 236 - 133n$$

and

$$y = -16 + \frac{27n}{3} = -16 + 9n.$$

(2) (2 points each) An example showing that a mathematical statement is false is called a *counterexample*. A counterexample must satisfy the *conditions* of the statement ("if ... "), but not satisfy the *conclusion* ("then ...").

Find counterexamples to each of the following statements and justify that the statement is false for your example.

(a) Let a, b, c, and d be integers. If a divides b, and c divides d, then $a+c$ divides $b+d$.
Let $a = b = c = 1$ and $d = 2$. Then $1 \mid 1$ and $1 \mid 2$, but $2 \nmid 3$.

(b) If a and b are integers, then $\gcd(a, b) = \gcd(a + b, a - b)$.
Let $a = 3$ and $b = 1$, then $\gcd(3, 1) = 1$ while $\gcd(4, 2) = 2$.

(c) Let $a, b, c \in \mathbb{Z}$. If a divides c and b divides c, then ab divides c.
Let $a = 2$, $b = 4$, and $c = 4$. Then $2 \mid 4$ and $4 \mid 4$, but $8 \nmid 4$.

(d) If a and b are integers, then $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.
Let $a = -1$ and $b = 2$. Then $\gcd(-1, 2) = 1$ and $\text{lcm}(-1, 2) = 2$, but $2 \neq -2$.

Part B: (3 points each) Prove each of the following statements.

(1) A positive integer a is divisible by 4 if and only if its last two digits are divisible by 4. (For example, 516 is divisible by 4 because 16 is divisible by 4.)

Proof. Let a be a positive integer. The division algorithm states that we can write $a = q100 + r$ where $0 \leq r < 100$. Note that since a is positive, it must be that $q \geq 0$. Then r is the number formed by the last two digits of a.

$\boxed{\Rightarrow}$ Suppose that a is divisibile by 4. Then $a = 4q'$ for some integer q'. So

$$\begin{aligned} 4q' &= 100q + r, \\ 4q' - 100q &= r, \\ 4(q' - 25q) &= r. \end{aligned}$$

Thus, r is divisible by 4, as desired.

$\boxed{\Leftarrow}$ Suppose that the last two digits of a are divisible by 4. In other words, suppose that $4 \mid r$. Since 4 also divides $100q = 4(25q)$, we have that 4 divides $100q + r$. So 4 divides a, as desired. □

(2) For every integer k, the numbers $2k + 1$ and $9k + 4$ are relatively prime.

Proof. Let k be an integer. We know that two integers a and b are coprime if and only if there exist integers x and y such that $ax + by = 1$. So we need to find x and y such that

$$(2k + 1)x + (9k + 4)y = 1.$$

Consider $x = 9$ and $y = -2$. Then

$$9(2k + 1) - 2(9k + 4) = 1.$$

□

(3) Prove that if you carry out two steps in the Euclidean algorithm for $\gcd(a, b)$ with $a > b > 0$, then the remainder is less than $a/2$.

Proof. Let a and b be integers with $a > b > 0$. The first two steps of the Euclidean algorithm are

$$a = q_1 b + r_1 \text{ with } 0 \leq r_1 < b$$

and

$$b = q_2 r_1 + r_2 \text{ with } 0 \leq r_2 < r_1.$$

We need to show that $r_2 < a/2$, or that $2r_2 < a$. Note that since we have assumed $a > b$, it must be that $q_1 \geq 1$. Thus

$$a \geq b + r_1.$$

Since $r_1 < b$, we have

$$b + r_1 > r_1 + r_1 = 2r_1.$$

Finally, because $r_2 < r_1$, we have

$$2r_1 > 2r_2.$$

Therefore,

$$a \geq b + r_1 > 2r_1 > 2r_2,$$

as desired.

□

Fun problem (will not be graded): The Euclidean algorithm works so well that it is difficult to find pairs of numbers that make it take a long time. Find two numbers whose gcd is 1, for which the Euclidean algorithm takes 10 steps.