HOMEWORK 3

CHRIS POWELL

STARDATE 2019.44

1. Silverman 5.4. A number L is called a common multiple of m and n if both m and n divide L. The smallest such L is called the *least common multiple* of m and n and is denoted by $\text{LCM}(m, n)$.

   (a) Find the following lease common multiples.

   (i) $\text{LCM}(8, 2) = 24$
   (ii) $\text{LCM}(20, 30) = 60$
   (iii) $\text{LCM}(51, 68) = 204$
   (iv) $\text{LCM}(23, 18) = 414$

   (b) For each of the following LCMs that you computed in (a), compare the value of $\text{LCM}(m, n)$ to the values of m, n and $\gcd(m, n)$ Try to find a relationship.

   (i) $\text{LCM}(8, 12) = 3 \cdot 8 = 2 \cdot 12 = (3 \cdot 2) \cdot \gcd(8, 12) = (3 \cdot 2) \cdot 4$
   $\text{LCM}(8, 12) \cdot \gcd(8, 12) = 24 \cdot 4 = (8 \cdot 3) \cdot 4 = 8 \cdot (3 \cdot 4) = 8 \cdot 12$

   (ii) $\text{LCM}(20, 30) = 3 \cdot 20 = 2 \cdot 30 = (3 \cdot 2) \cdot \gcd(20, 30) = (3 \cdot 2) \cdot 10$
   $\text{LCM}(20, 30) \cdot \gcd(20, 30) = 60 \cdot 10 = (20 \cdot 3) \cdot 10 = 20 \cdot (3 \cdot 10) = 20 \cdot 30$

   (iii) $\text{LCM}(51, 68) = 4 \cdot 51 = 3 \cdot 68 = (4 \cdot 3) \cdot \gcd(51, 68) = (4 \cdot 3) \cdot 17$
   $\text{LCM}(51, 68) \cdot \gcd(51, 68) = 204 \cdot 17 = (51 \cdot 4) \cdot 17 = 51 \cdot (4 \cdot 17) = 51 \cdot 68$

   (iv) $\text{LCM}(23, 18) = 18 \cdot 23 = 23 \cdot 18 = 23 \cdot 18 \cdot \gcd(23, 18) = (23 \cdot 18) \cdot 1$
   $\text{LCM}(23, 18) \cdot \gcd(23, 18) = 414 \cdot 1 = (23 \cdot 18) \cdot 1 = 23 \cdot (18 \cdot 1) = 23 \cdot 18$

   (c) Give an argument proving that the relationship you found is correct for all m and n.

   Proposition. For all integers m and n,

   $$\text{LCM}(m, n) \cdot \gcd(m, n) = mn.$$

   Proof. Let $m, n \in \mathbb{Z}$. Assume $d = \gcd(m, n)$. Then $m = xd$ and $n = yd$ for some relatively prime integers x and y. But $\ell = \text{LCM}(m, n)$ is divisible by $m = xd$ and $n = yd$. So $\ell = dxy$ since $\gcd(x, y) = 1$. Therefore,

   $$\text{LCM}(m, n) \cdot \gcd(m, n) = d(dxy) = (dx)(dy) = mn.$$

   □

   (d) Use your result in (b) to compute $\text{LCM}(301337, 307829)$.

$$\begin{aligned}\gcd(301337, 307829) &= \gcd() \\ &= 541\end{aligned}$$

Therefore, by the above result,

$$\begin{aligned}\text{LCM}(301337, 307829) &= \frac{301337 \cdot 307829}{\gcd(301337, 307289)} \\ &= \frac{301337 \cdot 307829}{541} \\ &= \frac{92760267373}{541} \\ &= 1714607573\end{aligned}$$

(e) Suppose that $\gcd(m, n) = 18$ and $\text{LCM}(m, n) = 720$. Find m and n. Is there more than one possibility? Is so, find them all.

2. Silverman 6.1.

(a) Find a solution in integers to the equation

$$12345x + 67890y = \gcd(12345, 67890).$$

To evaluate the $\gcd(12345, 67890)$, we apply the euclidean algorithm:

$$\begin{aligned} 67890 &= q_1(12345) + r_1 && (q_1, r_1) = (5, 6165) \\ 12345 &= q_2(6165) + r_2 && (q_2, r_2) = (2, 15) \\ 6165 &= q_3(15) + r_3 && (q_3, r_3) = (411, 0)\end{aligned}$$

Since $r_3 = 0$, we have $\gcd(12345, 67890) = r_2 = 15$. Write $a = 67890$ and $b = 12345$. Then

$$\begin{aligned} r_1 &= a - q_1 b \\ &= a - 5b \\ r_2 &= b - r_1 q_2 \\ &= b - (a - 5b)(2) \\ &= -2a + 11b\end{aligned}$$

So $(x, y) = (11, -2)$ is a solution. The set of all integer solutions is given by

$$\left\{ (x, y) \in \mathbb{Z}^2 \mid x = 11 + k\left(\tfrac{12345}{15}\right), y = -2 - k\left(\tfrac{67890}{15}\right), k \in \mathbb{Z} \right\}.$$

(b) Find a solution in integers to the equation

$$54321x + 9876y = \gcd(54321, 9876).$$

To evaluate the $\gcd(54321, 9876)$, we apply the euclidean algorithm:

$$\begin{aligned} 54321 &= 9876(5) + 4941 && (q_1, r_1) = (5, 4941) \\ 9876 &= 4941(1) + 4935 && (q_2, r_2) = (1, 4935) \\ 4941 &= 4935(1) + 6 && (q_3, r_3) = (1, 6) \\ 4935 &= 6(822) + 3 && (q_4, r_4) = (822, 3) \\ 822 &= 3(274) + 0 && (q_5, r_5) = (284, 0) \end{aligned}$$

Since $r_5 = 0$, we have $\gcd(54321, 9876) = r_4 = 3$. Write $a = 54321$ and $b = 9876$. Then

$$\begin{aligned} r_1 &= a - q_1 b \\ &= a - 5b \\ r_2 &= b - r_1 q_2 \\ &= b - (a - 5b)(1) \\ &= -a + 6b \\ r_3 &= r_1 - r_2 q_3 \\ &= (a - 5b) - (-a + 6b)(1) \\ &= 2a + 11b \\ r_4 &= r_2 - r_3 q_4 \\ &= (-a + 6b) - (2a + 11b)(822) \\ &= -1645a + 9048b \end{aligned}$$

Thus $(x, y) = (-1645, 9048)$ is a solution to the given equation. Furthermore, the set of all integer solutions is given by

$$\left\{ (x, y) \in \mathbb{Z}^2 \mid x = -1645 + k\left(\tfrac{9876}{3}\right), y = 9048 - k\left(\tfrac{54321}{3}\right), k \in \mathbb{Z} \right\}.$$

3. Silverman 6.4.

   (a) Find integers x, y, and z that satisfy the equation

   $$6x + 15y + 20z = 1.$$

Observe that

$$\begin{aligned} 20 &= 6(0) + 15(0) + 20(1) \\ 15 &= 6(0) + 15(1) + 20(0) \\ 6 &= 6(1) + 15(0) + 20(0) \\ 5 &= 6(0) + 15(-1) + 20(1) \\ 1 &= 6(1) + 15(1) + 20(-1) \end{aligned}$$

Therefore, $(x, y, z) = (1, 1, -1)$ is a solution.

   (b) Under what conditions on a, b, and c is it true that the equation

   $$ax + by + cz = 1$$

   has a solution? Describe a general method of finding a solution when one exists.

The equation $ax+by+cz = 1$ has integer solutions when $\gcd(\gcd(a,b),c) = 1$. So first find a solution to

$$ax + by = \gcd(a, b).$$

Then find a solution to

$$\gcd(a, b)k + cz = 1.$$

(c) Use your method from (b) to find a solution in integers to the equation

$$155x + 341y + 385z = 1.$$

4. Silverman 7.1. Suppose that $\gcd(a, b) = 1$, and suppose further a divides the product bc. Show that a must divide c.

Proof. As $\gcd(a, b) = 1$, we know $ax + by = 1$ for some $x, y \in \mathbb{Z}$. So $c(ax + by) = c(1)$. But $c = c(1)$ and

$$c(ax + by) = c(ax) + c(by) = (ca)x + (cb)y = (ac)x + (bc)y$$

since $\mathbb{Z}$ is a commutative ring with unity. But $a \mid bc$ by hypothesis, so $bc = ak$ for some $k \in \mathbb{Z}$. Thus

$$c = (ac)x + (ak)y = a(cx) + a(ky) = a(cx + ky).$$

Therefore, $a \mid c$. □

5. Silverman 7.2. Suppose that $\gcd(a, b) = 1$, and suppose further that a divides c and that b divides c. Show that the product ab must divide c.

Proof. As $\gcd(a, b) = 1$, we can find $x, y \in \mathbb{Z}$ such that $ax+by = 1$. So $c(ax+by) = c(1)$. But $c = c(1)$ and $c(ax + by) = c(ax) + c(by)$ since $\mathbb{Z}$ is a ring. By hypothesis, $a, b \mid c$. So $c = ka$ and $c = \ell b$ for some $k, \ell \in \mathbb{Z}$. Thus

$$c = (b\ell)(ax) + (ak)(by) = (ab)(\ell x) + (ab)(ky) = ab(\ell x + ky).$$

Hence, $c \mid ab$. □

6. Two players play the following game: The numbers 25 and 36 are written on a board. On each player's turn, they select any two numbers currently up and write on the board the positive difference of those two numbers, provided the difference is not already written on the board. The game continues until a player cannot write anything down. The last player to write down a number wins. Does the game always end? If so, assuming perfect play, who wins?

Let t be the total number of plays. Then $t \leq \max\{36, 25\} - 2 = 34$ since all plays are positive and the game begins with the numbers 36 and 25 already written. Since $\gcd(36, 25) = 1$, we can find some numbers which differ by 1. So every $x \in S' = S \setminus \{36, 25\}$ is a possible play. Thus $t \geq |S'| = 34$. Hence $t = 34$. Now since the last player to write down a number wins, and t is even, we know that the player who takes the second turn will win.

E-mail address: powel054@cougars.csusm.edu