Math 422 HMWK 4 Selected Solutions

Savage

Exercise 1

Silverman 5.4, Part A, with GCD

$$\begin{aligned} \operatorname{lcm}(8,12) &= 24 & \gcd(8,12) &= 4 \\ \operatorname{lcm}(20,30) &= 60 & \gcd(20,30) &= 10 \\ \operatorname{lcm}(51,68) &= 204 & \gcd(51,168) &= 17 \\ \operatorname{lcm}(23,18) &= 414 & \gcd(23,18) &= 1 \end{aligned}$$

Silverman 5.4, Part B

The idea here is to think about how you would compute the lcm by hand and relate that fact with the examples. Observe that the lcm is the gcd times the "union" of the factors of m, n that didn't occur in the gcd. For example, $24 = 6 \cdot 4$ which involves the gcd, but also, $6 = 2 \cdot 3$ and 2 and 3 are the remaining factors after removing the gcd from 8 and 12, respectively. Also note that "remove" means divide in this case. This idea leads to the more general formula:

$$\operatorname{lcm}(m,n) = \gcd(m,n) \cdot \frac{m}{\gcd(m,n)} \cdot \frac{n}{\gcd(m,n)} = \frac{mn}{\gcd(m,n)}.$$

Silverman 5.4, Part C

For this exercise, we will use a fact from the following chapter that there exist $x, y \in \mathbb{Z}$ such that

$$xm + yn = \gcd(m,n).$$

Lets define $g = \gcd(m,n)$, $L = \operatorname{lcm}(m,n)$, and assume we have the $x, y \in \mathbb{Z}$ satisfing the equation above. Next, let $T = \frac{mn}{g}$. Observe that if we write T as $(m/g)n$ and as $(n/g)m$, then we can easily see that T is a common multiple of both n and m. We also know L divides any common multiple of m and n, so $L|T$. Now let S be any common multiple of m and n. Observe that

$$\frac{S}{T} = \frac{S}{(mn/g)} = \frac{Sg}{mn} = \frac{S(xm+yn)}{mn}.$$

From here we can write

$$\frac{S(xm+yn)}{mn} = \frac{S}{n} \cdot x + \frac{S}{m} \cdot y.$$

One should note that S/n and S/m are integers since S was a common multiple of both m and n. This last equation illustrates that $T|S$. In particular, since S was any common multiple, we can choose $S = L$ and so $T|L$. The result follows if we require both T and L to be positive.

Silverman 5.4, Part D

$$\operatorname{lcm}(301337, 307829) = \frac{301337 \cdot 307829}{\gcd(301337, 307829)}.$$

Using the Euclidean Algorithm for the denominator we find

$$\gcd(301337, 307829) = 541$$

and to help save memory in our calculator, we write

$$\frac{301337 \cdot 307829}{541} = \frac{307829}{541} \cdot 301337 = 171460753.$$

Silverman 5.4, Part E

From the relation

$$720 = \frac{mn}{18},$$

it follows $720 \cdot 18 = mn$. Clearly, setting $m = 18, n = 720$ will not affect our parameters. Lets write

$$m = 18 \text{ and,}$$
$$n = 720 = 18 \cdot 2^3 \cdot 5.$$

Let m' and n' be another pair of integers satisfying $m'n' = mn$, but $\gcd(m', n')$ is 18 and $\operatorname{lcm}(m', n')$ is 720. Clearly this means $m|m'$ and $n'|n$. This means we can find $x, y \in \mathbb{Z}$ such that

$$m' = xm \text{ and } n = yn'.$$

Multiplying the first equation by n, we have $mxn = m'n = ym'n'$. Since we require $m'n' = mn$, this means $x = y$. One can check the only possible choices for x are $x \in \{1, 5, 8, 40\}$ (whatever we multiply m by we have to divide n by the same number, but retain a gcd of 18). This gives us the following (distinct) pairs:

$$(m, n) = (18, 720), (144, 90).$$

Exercise 3

We just give part B and a proof it works.

Silverman 6.3, Part B

```
def egcd(a,b):
        """Computes the gcd=g of a and b and returns g as well as
        integers x,y such that ax+by=g"""

        x,g,v,w=1,a,0,b
        t,s=0,0
        while w>0:
                t=g%w; s=x-(g//w)*v
                x,g,v,w=v,w,s,t
        y=(g-a*x)/b
        return g,x,y
```

0.1 Proof

First note that if we eliminate all mention of the variables x, y, v, s (so the while loop reduces to t, g, w on the left hand side for example), we actually get the old gcd algorithm back. The old algorithm has already been shown to terminate when $w = 0$ and output the correct gcd. To now show that x, y are correctly ouput, let N be the last iteration of the while loop. Then

$$y := (g_N - ax)/b.$$

We provide a lemma showing y is an integer after each iteration of the while loop.

Lemma 0.1. *In the above program, if $b > 0$, then after each iteration of the WHILE loop, $b|g - ax$ and $b|w - av$.*

Proof. (Proof by induction). Since $b > 0$, the WHILE loop will run at least once. Observe after the first iteration:

$$t = \text{rem}(a, b), s = 1 - (a//b) \cdot 0 = 1,$$
$$x = 0, g = b, v = 1, w = t.$$

Observe $g - ax = b - a \cdot 0 = b$ and $b|b$. Also, $w - av = \text{rem}(a, b) - a \cdot 1 = bq$ where q is the quotient $a = bq + r$ from the quotient remainder theorem. Clearly $b|bq$, so the claim is proven for the first iteration. Now suppose it holds for the $n^{\underline{th}}$ iteration. On the $n + 1$ iteration:

$$t_{n+1} = \text{rem}(g_n, w_n), s_{n+1} = x_n - \text{quotient}(g_n, w_n) \cdot v_n,$$
$$x_{n+1} = v_n, g_{n+1} = w_n, v_{n+1} = s_{n+1}, w_{n+1} = t_{n+1}.$$

Observe $g_{n+1} - ax_{n+1} = w_n - av_n$ and $b|(w_n - av_n)$ by inductive hypothesis. Next, $w_{n+1} - av_{n+1}$

$$= \text{rem}(g_n, w_n) - as_{n+1} \quad (1)$$
$$= \text{rem}(g_n, w_n) - ax_n + a \cdot \text{quotient}(g_n, w_n)v_n. \quad (2)$$

The trick here is to re-write $\text{rem}(g_n, w_n) = g_n - \text{quotient}(g_n, w_n) \cdot w_n$. This means

$$\begin{aligned} &\text{rem}(g_n, w_n) - ax_n + a \cdot \text{quotient}(g_n, w_n)v_n && (3)\\ &= g_n - \text{quotient}(g_n, w_n) \cdot w_n - ax_n + a \cdot \text{quotient}(g_n, w_n) \cdot v_n && (4)\\ &= (g_n - ax_n) + \text{quotient}(g_n, w_n)(w_n - av_n). && (5)\end{aligned}$$

By the inductive hypothesis, b divides this last equation because it divides each term in the difference. □

This shows on the last iteration y is actually an integer. Finally, by multiplying both sides by b and solving for g where $g = \gcd(a, b)$ at this point in the algorithm, we see that

$$ax + by = g.$$

So the correct x and y are output as well and in the desired order (and as integers).

1 Exercise 4

Silverman 6.4, Part A

The tuple $(x, y, z) = (1, 1, -1)$ satisfies

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

Silverman 6.4, Part B

For three numbers, $\gcd(a, b, c) = g$ means g is the largest positive integer that divides a, b, and c at the same time. We fire give a small lemma before proving the main result.

Lemma 1.1. *Let* $a, b, c \in \mathbb{Z}$. *If* $\gcd(a, b, c) = 1$, *then* $\gcd(\gcd(a, b), c) = 1$.

Proof. Let $d = \gcd(\gcd(a, b), c)$. This means $d|c$ and $d|\gcd(a, b)$, but by transitivity of divisibility, this means $d|a$ and $d|b$. Therefore d divides a, b, and c. Since $\gcd(a, b, c) = 1$, $d = 1$. □

Theorem 1.2. *Let* $a, b, c \in \mathbb{Z}$. *The equation*

$$ax + by + cz = 1$$

has solutions $(x, y, z) \in \mathbb{Z}^3$ *if and only if* $\gcd(a, b, c) = 1$.

Proof. If $\gcd(a, b, c) = g > 1$, then

$$ax + by + cz = g(a'x + b'y + c'z).$$

Regardless of the tuple (x, y, z) chosen, the result must be a multiple of g and since $g > 1$, the result cannot be 1. Now suppose $g = 1$ and let $t = \gcd(a, b)$. We know there exist integers $x, y \in \mathbb{Z}$ such that $ax + by = t$. Now consider the expression

$$ts + cz.$$

By Lemma 1.1, $\gcd(t, c) = 1$, so there exists integers $s, z \in \mathbb{Z}$ such that $tz + cz = 1$. Observe

$$a(xs) + b(ys) + cz = 1.$$

□

The idea is to compute the $g = \gcd(x, y)$ first then use that information along with the fact $\gcd(g, c) \overset{\text{known}}{=} 1$ to find a solution.

Silverman 6.4, Part C

Consider the expression

$$155x + 341y + 385z$$

where $x, y, z \in \mathbb{Z}$. By the above lemma, since $\gcd(155, 341, 385) = 1$ (easy to check), there exists $a, b, c \in \mathbb{Z}$ such that

$$155a + 341b + 385c = 1.$$

To find (a, b, c), we first compute $\text{egcd}(155, 341) = (31, -2, 1)$ which means

$$155s + 341t = 31$$

When $s = -2$ and $t = 1$. Next, by using $\text{egcd}(31, 385)$, we find

$$31m + 385z = 1$$

when $(m, z) = (-149, 12)$. So if we set $x = -149 \cdot -2$, $y = -149 \cdot 1$, and $z = 12$, then

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