Modern Algebra I Section 1 · Assignment 2

JOHN PERRY

Exercise 1. *(pg. 26 Warm Up a) Find the quotient and remainder, as guaranteed by the Division Theorem 2.1, for 13 and -120, -13 and 120, and -13 and -120.*

Solution:

We presume that the first number given is a, and the second b.

For 13 and -120, consider that $120 = 9 \times 13 + 3$, so $-120 = -9 \times 13 - 3$. Since the remainder must be positive, $-120 = -8 \times 13 + 10$.

Use the same reasoning to obtain $120 = 9 \times (-13) + 3$ and $-120 = 8 \times (-13) + 10$. ◊

Exercise 2. *(pg. 26 Warm Up b) What are the possible remainders when you divide by 3, using Division Theorem 2.1? Choose one such remainder, and make a list describing all integers that give this remainder, when divided by 3.*

Solution:

All possible remainders for division by 3 are 0, 1, 2. For 0, we obtain the list

$$\ldots, -6, -3, 0, 3, 6, \ldots$$

◊

Exercise 3. *(pg. 26 Warm Up d) Let m be a fixed integer. Describe succinctly the integers a where*

$$\gcd(a, m) = m.$$

Solution:

The integers are precisely the multiples of m; that is, any integer that m divides with zero remainder. ◊

Exercise 4. *(pg. 27 Exercise 1) (a) Find the greatest common divisor of 34 and 21, using Euclid's Algorithm. Then express this gcd as a linear combination of 34 and 21.*

(b) Now do the same for 2424 and 772.

Solution:

(a) We get:

$$\begin{aligned}
34 &= 21 \times 1 + 13,\\
21 &= 13 \times 1 + 8,\\
13 &= 8 \times 1 + 5,\\
8 &= 5 \times 1 + 3,\\
5 &= 3 \times 1 + 2,\\
3 &= 2 \times 1 + 1,\\
2 &= 1 \times 2 + 0.
\end{aligned}$$

Thus, the greatest common divisor of 34 and 21 is 1.

To obtain the linear combination, reverse the process:

$$\begin{aligned}
1 &= 3 - 2 \times 1 \\
1 &= 3 - (5 - 3 \times 1) \times 1 \\
&= 3 \times 2 - 5 \times 1 \\
1 &= (8 - 5 \times 1) \times 2 - 5 \times 1 \\
&= 8 \times 2 - 5 \times 3 \\
1 &= 8 \times 2 - (13 - 8 \times 1) \times 3 \\
&= 8 \times 5 - 13 \times 3 \\
1 &= (21 - 13 \times 1) \times 5 - 13 \times 3 \\
&= 21 \times 5 - 13 \times 8 \\
1 &= 21 \times 5 - (34 - 21 \times 1) \times 8 \\
&= 21 \times 13 - 34 \times 8.
\end{aligned}$$

(b) For 2424 and 772, Euclid's Algorithm shows the gcd to be 4:

$$\begin{aligned}
2424 &= 3 \times 772 + 108 \\
772 &= 7 \times 108 + 16 \\
108 &= 6 \times 16 + 12 \\
16 &= 1 \times 12 + 4 \\
12 &= 3 \times 4 + 0.
\end{aligned}$$

Reversing the process obtains a linear combination:

$$\begin{aligned}
4 &= 16 - 12 \times 1 \\
4 &= 16 - (108 - 16 \times 6) \times 1 \\
&= 16 \times 7 - 108 \times 1 \\
4 &= (772 - 108 \times 7) \times 7 - 108 \times 1 \\
&= 772 \times 7 - 108 \times 50 \\
4 &= 772 \times 7 - (2424 - 772 \times 3) \times 50 \\
&= 772 \times 157 - 2424 \times 50.
\end{aligned}$$

◊

Exercise 5. *(pg. 27 Exercise 2) Prove that* $\gcd(a,b)$ *divides* $a-b$. *This sometimes provides a short cut in finding gcds. Use this to find* $\gcd(1962,1965)$. *Now find* $\gcd(1961,1965)$.

Solution:

Let $a, b \in \mathbb{Z}$ be arbitrary, but fixed.

Write $d = \gcd(a,b)$.

Since $d \mid a$, there exists $x \in \mathbb{Z}$ such that $dx = a$. Likewise, since $d \mid b$, there exists $y \in \mathbb{Z}$ such that $dy = b$. Then

$$a - b = dx - dy = d(x - y),$$

so d divides $a - b$.

Since $1965 - 1962 = 3$, the gcd of those two numbers is either 1 or 3. Inspection shows that it is 3.

Since $1965-1961=4$, the gcd of those two numbers is 1, 2, or 4. Since both numbers are odd, the gcd cannot be 4 or 2, so it must be 1. ◊

Exercise 6. *(pg. 27 Exercise 4) Two numbers are said to be **relatively prime** if their gcd is 1. Prove that a and b are relatively prime if and only if every integer can be written as a linear combination of a and b.*

Solution:

Let $a,b\in\mathbb{Z}$ be arbitrary. Assume that a and b are relatively prime. Then $\gcd(a,b)=1$. By the gcd identity (Theorem 2.4), $1=ax+by$ for some $x,y\in\mathbb{Z}$. Let n be an arbitrary integer. Then

$$\begin{aligned} n &= n(ax+by)\\ &= a(nx)+n(ny). \end{aligned}$$

So n can be written as a linear combination of a and b. Since n was arbitrary, this holds for all integers.

Conversely, assume that any integer can be written as a linear combination of a and b. Certainly $1\in\mathbb{Z}$ so $1=ax+by$ for some $x,y\in\mathbb{Z}$. Also, 1 is the smallest positive integer possible, so it is the smallest positive integer that can be written as a linear combination of a and b. By Corollary 2.5, 1 is the gcd of a and b.

Another solution: Using the previous exercise in the book, we know that a and b are relatively prime if and only if 1 can be written as a linear combination of a and b. Let n be an arbitrary integer. Using the last fact, a and b are relatively prime if and only if there exist $x,y\in\mathbb{Z}$ such that

$$\begin{aligned} 1 &= ax+by\\ n &= a(nx)+b(ny); \end{aligned}$$

that is, if and only if n can be written as a linear combination of a,b. (You can't really use this one, since I didn't assign the previous exercise in the book.) ◊

Exercise 7. *(pg. 28 Exercise 8) Prove that two consecutive integers of the Fibonacci sequence are relatively prime.*

Solution:

We proceed by induction on n.

For the inductive base, assume $n=1$.

By definition, $a_1=1$ and its successor $a_2=1$ have gcd 1, and so are relatively prime.

Assume $n>2$, and that a_k and a_{k+1} are relatively prime for all $k:1\le k<n$.

By definition, $a_n=a_{n-1}+a_{n-2}$.

Then

$$a_n-a_{n-1}=a_{n-2} \tag{1}$$

Let d be the greatest common divisor of a_n and a_{n-1}.

It is clear that d divides the left hand side of equation (1).

So d also divides the right hand side of equation (1).

So d divides a_{n-2}.

Since d is a common divisor of both a_{n-1} and a_{n-2}, it divides their greatest common divisor, 1.

The only positive integer that divides 1 is 1 itself. Hence $d = 1$.
Hence a_n and a_{n-1} are relatively prime. $\Diamond$