Modern Algebra I Section 1 · Assignment 3

JOHN PERRY

Exercise 1. *(pg. 27 Warm Up e) Give the prime factorizations of 92, 100, 101, 502, and 1002.*

Solution:
$92 = 4 \times 23 = 2^2 \times 23$
$100 = 4 \times 25 = 2^2 \times 5^2$
101 is prime.
$502 = 2 \times 251$
$1002 = 2 \times 501 = 2 \times 3 \times 167$ ◊

Exercise 2. *(pg. 27 Exercise 6) Suppose that a and b are positive integers. If $a + b$ is prime, prove that* $\gcd(a, b) = 1$.

Solution:
Assume that $a + b$ is prime.
Let $d = \gcd(a, b)$.
By the definition of the gcd, d divides a and d divides b.
Using the definition of divisibility, let $x, y \in \mathbb{Z}$ such that $dx = a$ and $dy = b$.
Then

$$a + b = dx + dy = d(x + y) \quad (1)$$

So d divides $a + b$.
Recall that $a + b$ is prime; by Theorem 2.7, it is irreducible.
Since $a + b$ is irreducible and $a + b = d(x + y)$, by definition $d = 1$ or $x + y = 1$.
If $d = 1$, then $\gcd(a, b) = 1$, and we are done.
Otherwise, $x + y = 1$. We show that this assumption gives a contradiction.
Substituting into (1), we see that $a + b = d$.
Recall that $d = \gcd(a, b)$. Since a and b are positive, $d \leq a$ and $d \leq b$.
By substitution, $d = a + b \geq d + d = 2d$. So $d \geq 2d$.
But d is a gcd, hence a positive integer, so $d < 2d$. We have a contradiction.
The assumption that $x + y = 1$ produced a contradiction, so $x + y \neq 1$.
Thus $d = 1$, so $\gcd(a, b) = 1$. ◊

Exercise 3. *(pg. 27 Exercise 7) (a) A natural number greater than 1 that is not prime is called* ***composite****. Show that for any n, there is a run of n consecutive composite numbers.* Hint: *think factorial.*
(b) Therefore, there is a string of 5 consecutive composite numbers starting where?

Solution:
(a) Let $n \in \mathbb{N}$ be arbitrary, but fixed.
Consider $c_2 = (n + 1)! + 2$, $c_3 = (n + 1)! + 3$, …, $c_{n+1} = (n + 1)! + (n + 1)$.
Let i be arbitrary, but fixed. Assume $2 \leq i \leq n + 1$.
By definition of factorial, $i \mid (n + 1)!$.

By definition of divisibility, $(n+1)! = id$ for some $d \in \mathbb{Z}$.
Thus $c_i = (n+1)! + i = i(d+1)$.
By definition of divisibility, $i \mid c_i$.
Since $i > 1$ and $d+1 > 1$, c_i is not irreducible by definition.
By Theorem 2.7, c_i is not prime.
Since i was arbitrary, none of $c_2, c_3, \ldots, c_{n+1}$ is prime, so they are all composite.
We have found $(n+1) - 2 + 1 = n$ consecutive composite numbers.
(b) A string of 5 consecutive composite numbers starts with $6! + 2 = 722$. ◊

Exercise 4. *Show that if a, d, x are integers such that dx divides ad, then x divides a.*

Solution:
Assume that a, d, x are integers such that dx divides ad.
By definition, there exists $y \in \mathbb{Z}$ such that $(dx)y = ad$.
Thus $xy = a$.
By definition, x divides a. ◊

Exercise 5. *Show* $\gcd(ad, bd) = d\gcd(a, b)$.

Solution:
By Theorem 2.4, there exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by. \tag{2}$$

By Corollary 2.5, equation (2) gives the smallest positive linear combination of a and b.
Multiply both sides of equation (2) by d to obtain

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

Distribute the d and regroup to obtain

$$d\gcd(a, b) = x(ad) + y(bd). \tag{3}$$

Equation (3) is a linear combination of ad and bd.
By Theorem 2.4, we know that there exist $u, v \in \mathbb{Z}$ such that

$$\gcd(ad, bd) = u(ad) + v(bd). \tag{4}$$

By Corollary 2.5, equation (4) gives the smallest positive linear combination of ad and bd. Since equation (3) gives another linear combination of ad and bd, it must be that

$$u(ad) + v(bd) \le x(ad) + y(bd).$$

Divide by d and we have

$$au + bv \le ax + by. \tag{5}$$

Recall equation (2) gives the smallest linear combination of a and b. Since $au + bv$ is another linear combination of a and b, it must be that

$$au + bv \ge ax + by. \tag{6}$$

Equations (5) and (6) imply that $au + bv = ax + by$.
Multiply by d to get $u(ad) + v(bd) = x(ad) + y(bd)$.
Substituting from equations (4) and (3), we have

$$\gcd(ad, bd) = d\gcd(a, b).$$

◊

Exercise 6. *(pg. 28 Exercise 10) Suppose that two integers a and b have been factored into primes as follows:*

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

and

$$b = p_1^{m_1} p_2^{m_2} \cdots p_r^{n_r},$$

where the p_i's are primes, and the exponents m_i and n_i are nonnegative integers. It is the case that

$$\gcd(a,b) = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r},$$

where s_i is the smaller of n_i and m_i. Show this with $a = 360 = 2^3 3^2 5$ and $b = 900 = 2^2 3^2 5^2$. Now prove this fact in general.

Solution:

We can use the Euclidean algorithm to find $\gcd(360,900)$:

$$900 = 2 \times 360 + 180$$
$$360 = 2 \times 180 + 0.$$

So $\gcd(360,900) = 180$. Observe that

$$900 = 2^2 3^2 5^2$$
$$360 = 2^3 3^2 5$$
$$180 = 2^2 3^2 5 = 2^{\min(2,3)} 3^{\min(2,2)} 5^{\min(1,2)}.$$

To prove this fact in general, let $d = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$ where $s_i = \min(m_i, n_i)$.

It is clear that d is a divisor of a and d is a divisor of b, since

$$a = dx \quad \text{and} \quad b = dy$$

where

$$x = p_1^{n_1 - s_1} p_2^{n_2 - s_2} \cdots p_r^{n_r - s_r} \quad \text{and} \quad y = p_1^{m_1 - s_1} p_2^{m_2 - s_2} \cdots p_r^{m_r - s_r}.$$

It remains to show that d is the *greatest* common divisor.

Applying the previous exercise, $\gcd(a,b) = \gcd(dx, dy) = d\gcd(x,y)$.

If $d = \gcd(a,b)$, then $\gcd(x,y) = 1$. So by way of contradiction, assume that $\gcd(x,y) \neq 1$.

Let p be one of the prime divisors of $\gcd(x,y)$. Then p divides x and p divides y.

By unique factorization, $p = p_i$ for some $i : 1 \leq i \leq r$.

Either $\min(m_i, n_i) = m_i$ or $\min(m_i, n_i) = n_i$.

If $\min(m_i, n_i) = m_i$, then $s_i = m_i$, so $m_i - s_i = 0$. So $p_i \nmid y$.

If $\min(m_i, n_i) = n_i$, then $s_i = n_i$, so $n_i - s_i = 0$. So $p_i \nmid x$.

So $p \nmid x$ or $p \nmid y$. Thus $p \nmid \gcd(x,y)$. This contradicts the assumption that p was a divisor of $\gcd(x,y)$.

The assumption that $\gcd(x,y) \neq 1$ leads to a contradiction. Hence $\gcd(x,y) = 1$.

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

By definition of d,

$$\gcd(a,b) = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}.$$

◊