# Selected Solutions to Underwood Dudley's Elementary Number Theory Second Edition

Greg Kikola

July 13, 2019

# Contents

**1 Integers** **1**
1.1 Exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
1.2 Problems . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2

# Chapter 1

# Integers

## 1.1 Exercises

### 1.1.1 Exercise 1

Which integers divide zero?

*Solution.* Every integer divides 0. For, if $k$ is any integer, then $0k = 0$ so that $k \mid 0$. $\square$

### 1.1.2 Exercise 2

Show that if $a \mid b$ and $b \mid c$ then, $a \mid c$.

*Proof.* Let $a \mid b$ and $b \mid c$. Then there are integers $m$ and $n$ such that $am = b$ and $bn = c$. But then $a(mn) = (am)n = bn = c$. Since $mn$ is an integer, we have $a \mid c$. $\square$

### 1.1.3 Exercise 3

Prove that if $d \mid a$ then $d \mid ca$ for any integer $c$.

*Proof.* Again, by definition we can find an integer $n$ such that $dn = a$. But then $cdn = ca$. Since $cn$ is an integer, it follows that $d \mid ca$. $\square$

### 1.1.4 Exercise 4

What are $(4, 14)$, $(5, 15)$, and $(6, 16)$?

*Solution.* By inspection, $(4, 14) = 2$, $(5, 15) = 5$, and $(6, 16) = 2$. $\square$

### 1.1.5 Exercise 5

What is $(n, 1)$, where $n$ is any positive integer? What is $(n, 0)$?

*Solution.* We have $(n, 1) = 1$ since there is no integer greater than 1 which divides 1. We also have $(n, 0) = n$ since no integer larger than $n$ can divide $n$, and $n$ certainly divides itself and 0. $\square$

### 1.1.6 Exercise 6

If $d$ is a positive integer, what is $(d, nd)$?

*Solution.* $(d, nd) = d$ since $d$ is a common divisor ($d \mid nd$ by Lemma 2) and there can be no greater divisor of $d$. □

### 1.1.7 Exercise 7

What are $q$ and $r$ if $a = 75$ and $b = 24$? If $a = 75$ and $b = 25$?

*Solution.* We have

$$75 = 3(24) + 3 \quad \text{and} \quad 75 = 3(25) + 0.$$

So $q = 3$ and $r = 3$ in the first case, and $q = 3$ and $r = 0$ in the second. □

### 1.1.8 Exercise 8

Verify that Lemma 3 is true when $a = 16$, $b = 6$, and $q = 2$.

*Solution.* Since $16 = 6 \cdot 2 + 4$, we have $r = 4$. And since $(16, 6) = 2 = (6, 4)$, the lemma is true for this case. □

### 1.1.9 Exercise 9

Calculate $(343, 280)$ and $(578, 442)$.

*Solution.* Following the Euclidean Algorithm, we have

$$\begin{aligned} 343 &= 280 \cdot 1 + 63 \\ 280 &= 63 \cdot 4 + 28 \\ 63 &= 28 \cdot 2 + 7 \\ 28 &= 7 \cdot 4. \end{aligned}$$

Therefore $(343, 280) = 7$.

For the second pair,

$$\begin{aligned} 578 &= 442 \cdot 1 + 136 \\ 442 &= 136 \cdot 3 + 34 \\ 136 &= 34 \cdot 4, \end{aligned}$$

so $(578, 442) = 34$. □

## 1.2 Problems

### 1.2.1 Problem 1

Calculate $(314, 159)$ and $(4144, 7696)$.

*Solution.* For the first pair, we have

$$\begin{aligned}
314 &= 159 \cdot 1 + 155 \\
159 &= 155 \cdot 1 + 4 \\
155 &= 4 \cdot 38 + 3 \\
4 &= 3 \cdot 1 + 1 \\
3 &= 1 \cdot 3,
\end{aligned}$$

so $(314, 159) = 1$ and the two numbers are relatively prime.

For the second pair, we have

$$\begin{aligned}
4144 &= 7696 \cdot 0 + 4144 \\
7696 &= 4144 \cdot 1 + 3552 \\
4144 &= 3552 \cdot 1 + 592 \\
3552 &= 592 \cdot 6,
\end{aligned}$$

so $(4144, 7696) = 592$. □

### 1.2.2 Problem 2

Calculate $(3141, 1592)$ and $(10001, 100083)$.

*Solution.* The procedure is the same as before, so we omit the details. We have $(3141, 1592) = 1$ and $(10001, 100083) = 73$. □

### 1.2.3 Problem 3

Find $x$ and $y$ such that $314x + 159y = 1$.

*Solution.* We applied the Euclidean algorithm to 314 and 159 in the first problem. Working through those equations in reverse order, we find

$$\begin{aligned}
1 &= 4 - 3 = 4 - (155 - 4 \cdot 38) \\
&= -1 \cdot 155 + 39 \cdot 4 = -1 \cdot 155 + 39(159 - 155) \\
&= -40 \cdot 155 + 39 \cdot 159 = -40(314 - 159) + 39 \cdot 159 \\
&= -40 \cdot 314 + 79 \cdot 159.
\end{aligned}$$

So $x = -40$ and $y = 79$ is one solution. □

### 1.2.4 Problem 4

Find $x$ and $y$ such that $4144x + 7696y = 592$.

*Solution.* We proceed as in the previous problem.

$$\begin{aligned}
592 &= 4144 - 3552 = 4144 - (7696 - 4144) \\
&= 2 \cdot 4144 - 7696,
\end{aligned}$$

so $x = 2$ and $y = -1$ is one possibility. □

### 1.2.5 Problem 5

If $N = abc + 1$, prove that $(N, a) = (N, b) = (N, c) = 1$.

*Proof.* Let $d = (N, a)$. Since $1 = N - abc$, it follows that $d \mid 1$, and therefore $d = 1$. Using the same reasoning for $b$ and $c$, we see that $(N, a) = (N, b) = (N, c) = 1$. □

### 1.2.6 Problem 6

Find two different solutions of $299x + 247y = 13$.

*Solution.* The Euclidean Algorithm produces

$$\begin{aligned} 299 &= 247 \cdot 1 + 52 \\ 247 &= 52 \cdot 4 + 39 \\ 52 &= 39 \cdot 1 + 13 \\ 39 &= 13 \cdot 3. \end{aligned}$$

Now, working backwards using substitution gives

$$\begin{aligned} 13 &= 52 - 39 = 52 - (247 - 4 \cdot 52) \\ &= 5 \cdot 52 - 247 = 5(299 - 247) - 247 \\ &= 5 \cdot 299 - 6 \cdot 247. \end{aligned}$$

This gives one solution.

Since $299 = 23 \cdot 13$ and $247 = 19 \cdot 13$, subtracting 19 from $x$ and adding 23 to $y$ will keep the equation balanced. The reason this works is because

$$\begin{aligned} 299(x - 19) + 247(y + 23) &= 299x + 247y - 19 \cdot 299 + 23 \cdot 247 \\ &= 299x + 247y - 19 \cdot 23 \cdot 13 + 23 \cdot 19 \cdot 13 \\ &= 299x + 247y = 13. \end{aligned}$$

Therefore a second solution is given by $x = -14$ and $y = 17$.

Note that we can continue this indefinitely (in both directions) to find infinitely many solutions. For example, $x = -33$ and $y = 40$ is a third solution. □

### 1.2.7 Problem 7

Prove that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

*Proof.* There are integers $x$ and $y$ such that $ax = b$ and $by = a$. Substituting $ax$ for $b$ in the second equation gives $axy = a$ or $xy = 1$. But the only integers having a multiplicative inverse are 1 and $-1$. So either $x = y = 1$ in which case $a = b$, or else $x = y = -1$ in which case $a = -b$. □

### 1.2.8 Problem 8

Prove that if $a \mid b$ and $a > 0$, then $(a, b) = a$.

*Proof.* Since $a$ divides itself and $b$, we must have $a \mid (a, b)$ by Corollary 2. But we also know that $(a, b) \mid a$ by definition. By the previous problem, it follows that either $(a, b) = a$ or $(a, b) = -a$. But $a > 0$, so we must have $(a, b) = a$. □

### 1.2.9 Problem 9

Prove that $((a, b), b) = (a, b)$.

*Proof.* Let $d = (a, b)$. Then $d \mid b$ by definition, and $d > 0$. So we may apply the previous problem to establish that $(d, b) = d$. □

### 1.2.10 Problem 10

(a) Prove that $(n, n + 1) = 1$ for all $n > 0$.

*Proof.* Fix an $n > 0$ and put $d = (n, n + 1)$. Then $d$ divides both $n + 1$ and $n$, so by Lemma 2, $d$ also divides their difference $(n + 1) - n = 1$. Since $d \mid 1$ and $d > 0$, we must have $d = 1$. □

(b) If $n > 0$, what can $(n, n + 2)$ be?

*Solution.* Again, if $d = (n, n + 2)$, then $d$ must divide $(n + 2) - n = 2$. Thus $d$ must be either 1 or 2. For example, $(3, 5) = 1$ and $(4, 6) = 2$. □

### 1.2.11 Problem 11

(a) Prove that $(k, n + k) = 1$ if and only if $(k, n) = 1$.

*Proof.* Suppose $(k, n + k) = 1$ and set $d = (k, n)$. Since $d$ divides $k$ and $n$, $d$ also divides their sum $n + k$. Hence $d$ is a common divisor of $k$ and $n + k$, so $d = 1$.

Conversely, suppose $(k, n) = 1$ and put $d = (k, n + k)$. Again, $d \mid k$ and $d \mid n + k$, so $d$ divides their difference $n$. Therefore $d$ is a common divisor of $k$ and $n$, so $d = 1$. □

(b) Is it true that $(k, n + k) = d$ if and only if $(k, n) = d$?

*Solution.* Yes. Using the same reasoning as above, we can see that $c$ is a common divisor of $k$ and $n + k$ if and only if it is a common divisor of $k$ and $n$. It follows that $(k, n + k) = (k, n)$. □

### 1.2.12 Problem 12

Prove: If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

*Proof.* There are integers $m$ and $n$ such that $am = b$ and $cn = d$. Therefore $bd = (am)(cn) = mn(ac)$, so $ac \mid bd$. □

### 1.2.13 Problem 13

Prove: If $d \mid a$ and $d \mid b$, then $d^2 \mid ab$.

*Proof.* This is a special case of the previous problem. □

### 1.2.14 Problem 14

Prove: If $c \mid ab$ and $(c, a) = d$, then $c \mid db$.

*Proof.* Find integers $x$ and $y$ with $cx + ay = d$. Multiplying by $b$ then gives

$$cxb + ayb = db.$$

Since $c$ divides the left-hand side, it must divide the right-hand side. Therefore $c \mid db$. □

### 1.2.15 Problem 15

(a) If $x^2 + ax + b = 0$ has an integer root, show that it divides $b$.

*Proof.* We are assuming that $a$ and $b$ are integers. Let the polynomial have the integer root $c$. Then

$$b = -c^2 - ac = c(-c - a),$$

and we see that $c \mid b$ since $-c - a$ is an integer. □

(b) If $x^2 + ax + b = 0$ has a rational root, show that it is in fact an integer.

*Proof.* Let the root be $c/d$ where $c$ and $d$ are relatively prime integers with $d$ nonzero. Then

$$\frac{c^2}{d^2} + \frac{ac}{d} + b = 0.$$

Multiplying through by $d^2$ then gives

$$c^2 + acd + bd^2 = 0$$

or $c^2 = -d(ac + bd)$. We see that $d \mid c^2$. Since $(c, d) = 1$, we have by Corollary 1 that $d \mid c$ as well. But then $(c, d) = d$, so we must have $d = 1$. Therefore the rational number $c/d$ is actually just the integer $c$. □