

Exercises Solution for “Elementary Number  
Theory: Second Edition by Underwood Dudley”

Agro Rachmatullah

2018-12-10

# 1 Integers

**Exercise 1.** Which integers divide zero?

For any integer  $a$ ,  $0 \cdot a = 0$ . Therefore all integers divide zero.

**Exercise 2.** Show that if  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .

From the definition, there are integers  $d$  and  $e$  such that  $b = da$  and  $c = eb$ . Therefore,

$$\begin{aligned}c &= eb \\ &= eda \\ &= (ed)a\end{aligned}$$

Which means  $a \mid c$ .

**Exercise 3.** Prove that if  $d \mid a$  then  $d \mid ca$  for any integer  $c$ .

**Method 1** From the definition, there is an integer  $b$  such that  $a = bd$ . Therefore  $ca = cbd = (cb)d$  which means  $d \mid ca$ .

**Method 2** We can use Lemma 2 by setting  $n = 1$ ,  $a_1 = a$ , and  $c_1 = c$ .

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

The positive divisors of 4 are 1, 2, and 4, and the positive divisors of 14 are 1, 2, 7, and 14. Therefore  $(4, 14) = 2$ .

The positive divisors of 5 are 1 and 5. Likewise for 15 they are 1, 3, 5, and 15. Therefore  $(5, 15) = 5$ .

The positive divisors of 6 are 1, 2, 3, and 6. For 16 they are 1, 2, 4, 8, and 16. Therefore  $(6, 16) = 2$ .

**Exercise 5.** What is  $(n, 1)$ , where  $n$  is any positive integer? What is  $(n, 0)$ ?

The only divisor of 1 is 1, and it also divides any positive integer  $n$ , so  $(n, 1) = 1$ .

$n \mid n$  and is the largest divisor of  $n$ . Because  $n \mid 0$ ,  $(n, 0) = n$ .

**Exercise 6.** If  $d$  is a positive integer, what is  $(d, nd)$ ?

The largest divisor of  $d$  is  $d$  itself. Because  $d \mid nd$ ,  $(d, nd) = d$ .

**Exercise 7.** What are  $q$  and  $r$  if  $a = 75$  and  $b = 24$ ? If  $a = 75$  and  $b = 25$ ?

We can create the set

$$\{75, 75 - 24 = 51, 75 - 2 \cdot 24 = 27, 75 - 3 \cdot 24 = 3\}$$

Therefore  $75 = 3 \cdot 24 + 3$  so  $q = 3$  and  $r = 3$ .

Similarly, for the second problem we can create the set

$$\{75, 75 - 25 = 50, 75 - 2 \cdot 25 = 25, 75 - 3 \cdot 25 = 0\}$$

So  $q = 3$  and  $r = 0$ .

**Exercise 8.** Verify that the lemma is true when  $a = 16$ ,  $b = 6$ , and  $q = 2$ .

We have the equation  $16 = 6 \cdot 2 + 4$  so  $r = 4$ .

$(16, 6) = 2$ , and  $(6, 4) = 2$ , which is according to the lemma.

**Exercise 9.** Calculate  $(343, 280)$  and  $(578, 442)$ .

For the first problem,

$$343 = 280 + 63$$

$$280 = 63 \cdot 4 + 28$$

$$63 = 28 \cdot 2 + 7$$

$$28 = 7 \cdot 4$$

$$\text{So } (343, 280) = (280, 63) = (63, 28) = (28, 7) = 7$$

For the second problem,

$$578 = 442 + 136$$

$$442 = 136 \cdot 3 + 34$$

$$136 = 34 \cdot 4$$

$$\text{So } (578, 442) = (442, 136) = (136, 34) = 34$$

**Problem 1.** Calculate  $(314, 159)$  and  $(4144, 7696)$ .

$$314 = 159 \cdot 1 + 155$$

$$159 = 155 \cdot 1 + 4$$

$$155 = 4 \cdot 38 + 3$$

Therefore, using the Euclidian algorithm,

$$(314, 159) = (159, 155)$$

$$= (155, 4)$$

$$= (4, 3)$$

$$= 1$$

$$7696 = 4144 \cdot 1 + 3552$$

$$4144 = 3552 \cdot 1 + 592$$

$$3522 = 592 \cdot 6 + 0$$

Therefore, using the Euclidian algorithm,

$$\begin{aligned}(4144, 7696) &= (7696, 4144) \\ &= (4144, 3552) \\ &= (3522, 592) \\ &= 592\end{aligned}$$

**Problem 2.** Calculate  $(3141, 1592)$  and  $(10001, 100083)$ .

$$3141 = 1592 \cdot 1 + 1549$$

$$1592 = 1549 \cdot 1 + 43$$

$$1549 = 43 \cdot 36 + 1$$

Therefore, using the Euclidian algorithm,

$$\begin{aligned}(3141, 1592) &= (1592, 1549) \\ &= (1549, 43) \\ &= (43, 1) \\ &= 1\end{aligned}$$

$$100083 = 10001 \cdot 10 + 73$$

$$10001 = 73 \cdot 137 + 0$$

Therefore, using the Euclidian algorithm,

$$\begin{aligned}(10001, 100083) &= (100083, 10001) \\ &= (10001, 73) \\ &= 73\end{aligned}$$

**Problem 3.** Find  $x$  and  $y$  such that  $314x + 159y = 1$ .

From problem 1, we know that a solution exists.

$$\begin{aligned}
314 &= 159 \cdot 1 + 155 \text{ implies } 155 = 314 - 159 \\
159 &= 155 \cdot 1 + 4 \quad \text{implies} \quad 4 = -314 + 159 \cdot 2 \\
155 &= 4 \cdot 38 + 3 \quad \text{implies} \quad 3 = 314 \cdot 39 - 159 \cdot 77 \\
4 &= 3 \cdot 1 + 1 \quad \text{implies} \quad 1 = 4 - 3
\end{aligned}$$

Using backsubstitution we get

$$1 = 314(-40) + 159 \cdot 79$$

So  $x = -140$  and  $y = 79$ .

**Problem 4.** Find  $x$  and  $y$  such that  $4144x + 7696y = 592$ .

From problem 1, we know that a solution exists.

$$\begin{aligned}
7696 &= 4144 \cdot 1 + 3552 \text{ implies } 3552 = 7696 - 4144 \\
4144 &= 3552 \cdot 1 + 592 \text{ implies } 592 = 4144 - 3552
\end{aligned}$$

Using backsubstitution we get

$$592 = 7696(-1) + 4144 \cdot 2$$

So  $x = -1$  and  $y = 2$ .

**Problem 5.** If  $N = abc + 1$ , prove that  $(N, a) = (N, b) = (N, c) = 1$ .

Let  $(N, a) = d$ , so  $d \mid N$  and  $d \mid a$ .

Because  $d \mid N$  and  $d \mid abc$ , from  $N = abc + 1$  it must be the case that  $d \mid 1$ .

Since  $d$  is a gcd,  $d \geq 1$ , therefore  $d = 1$ .

The same argument can be said for  $(N, b)$  and  $(N, c)$ .

**Problem 6.** Find two different solutions of  $299x + 247y = 13$ .

Using the Euclidian algorithm, we get  $x_0 = 5$  and  $y_0 = -6$ .

Since the original equation is a linear equation, it can be written as

$$y = -\frac{299}{247}x + c \tag{1}$$

So from any point in the solution, we can go 247 units to the right and 299 units downwards and it will still be a solution. Therefore,

$$\begin{aligned}
x &= 5 + 247n \\
y &= -6 - 299n
\end{aligned}$$

Will be a solution for any integer  $n$ .

**Problem 7.** Prove that if  $a \mid b$  and  $b \mid a$ , then  $a = b$  or  $a = -b$ .

From the proposition,  $b = aq$  for some integer  $q$  and  $a = br$  for some integer  $r$ . Therefore,

$$\begin{aligned} a &= (aq)r \\ &= a(qr) \end{aligned}$$

So  $qr = 1$  which means  $q = r = 1$  or  $q = r = -1$ , and because  $a = br$  either  $a = b$  or  $a = -b$ .

**Problem 8.** Prove that if  $a \mid b$  and  $a > 0$ , then  $(a, b) = a$ .

$a$  is the divisor of both  $a$  and  $b$ . Because  $a > 0$ ,  $a$  is the largest divisor of  $a$ . So for any divisor  $c$  of both  $a$  and  $b$ ,  $c \leq a$ . Thus  $(a, b) = a$ .

**Problem 9.** Prove that  $((a, b), b) = (a, b)$ .

$(a, b) \mid b$  and of course  $(a, b) \mid (a, b)$ , so  $(a, b)$  is a common divisor of both  $(a, b)$  and  $b$ . Furthermore because  $(a, b) > 0$ , no other common divisor can be larger than it (else it won't divide  $(a, b)$ ). Therefore  $((a, b), b) = (a, b)$ .

**Problem 10.**

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

Suppose that  $(n, n + 1) = d$ . It means that  $d \mid n$  and  $d \mid n + 1$ , so it follows that  $d \mid 1$ .

Because  $d > 0$ , then  $d = 1$  (which is actually valid for all  $n$ ).

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

Suppose  $n$  is even, so  $n = 2m$ . Therefore

$$(n, n + 2) = (2m, 2(m + 1))$$

Since  $(m, m + 1) = 1$  as proved before, 2 is the largest common divisor of  $2m$  and  $2(m + 1)$ . Therefore  $(n, n + 2) = 2$ , so if  $n > 0$  then  $(n, n + 2)$  could be 2.

**Problem 11.**

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

If  $d$  is a common divisor of both  $k$  and  $n + k$ ,  $d \mid k$  and  $d \mid n + k$ , so it follows that  $d \mid n$ .

However  $(k, n + k) = 1$  so  $d \leq 1$ . Therefore  $(k, n) = 1$ . The reverse is trivially true.

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

Yes. Replace 1 in the argument above with any other number

**Problem 12.** Prove: If  $a \mid b$  and  $c \mid d$ , then  $ac \mid bd$ .

$a \mid b$  means  $b = aq$  for some  $q$ , and  $c \mid d$  means  $d = cr$  for some  $r$ .  
Therefore

$$\begin{aligned} bd &= aqcr \\ &= (ac)qr \end{aligned}$$

So  $ac \mid bd$ .

**Problem 13.** Prove: If  $d \mid a$  and  $d \mid b$ , then  $d^2 \mid ab$ .

This is just a more specific instance of the previous problem.

**Problem 14.** Prove: If  $c \mid ab$  and  $(c, a) = d$ , then  $c \mid db$ .

$a = dq$  for some  $q$ , and  $c = dr$  for some  $r$ . In other words,  $a/d = q$  and  $c/d = r$ . From Theorem 1.1,  $(a/d, b/d) = 1$ . Therefore  $(q, r) = 1$ .

$$\begin{aligned} a \mid ab &\implies dr \mid dqb \\ &\implies r \mid qb \end{aligned}$$

Because  $(q, r) = 1$ , from Corollary 1.4.1  $r \mid b$ , which means  $dr \mid db$ , or  $c \mid db$ .

**Problem 15.**

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

$$\begin{aligned} x^2 + ax + b &= 0 \\ b &= -x^2 - ax \\ b &= x(-x - a) \end{aligned}$$

Which means that the root divides  $b$ .

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

Suppose that the roots are  $r$  and  $s$ .

$$(x - r)(x - s) = x^2 - (r + s)x + rs$$

Therefore  $a = -(r + s)$  and  $b = rs$ .

Let's say that one of the roots  $r$  can be written as  $m/n$  where  $(m, n) = 1$  (If it is not the case, then the rational number can be simplified so that  $(m, n) = 1$ ). Assume that  $m \neq 0$  because else the proof is done.

Because  $b = rs$ , we have  $s = \frac{bn}{m}$ . Therefore

$$\begin{aligned} a &= -(r + s) \\ &= -\left(\frac{m}{n} + \frac{bn}{m}\right) \\ &= -\left(\frac{m^2 + bn^2}{mn}\right) \\ -mna &= m^2 + bn^2 \\ n(-ma) &= m^2 + n(bn) \end{aligned}$$

Because  $n$  divides the left side and also  $n(bn)$ , we have  $n \mid m^2$ . We use the fact that  $(m, n) = 1$  and Corollary 1.4.1 to conclude that  $n \mid m$ . Therefore  $m/n$  is an integer.