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

Agro Rachmatullah

2018-12-10

1 Integers

Exercise 1.1. Which integers divide zero?

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

Exercise 1.2. 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 1.3. 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 1.4. 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 1.5. 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 1.6. 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 1.7. 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 1.8. 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 1.9. Calculate $(343, 280)$ and $(578, 442)$.

For the first problem,

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

So $(343, 280) = (280, 63) = (63, 28) = (28, 7) = 7$
For the second problem,

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

So $(578, 442) = (442, 136) = (136, 34) = 34$

Problem 1.1. Calculate $(314, 159)$ and $(4144, 7696)$.

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

Therefore, using the Eucledian algorithm,

$$\begin{aligned} (314, 159) &= (159, 155) \\ &= (155, 4) \\ &= (4, 3) \\ &= 1 \end{aligned}$$

$$\begin{aligned}
7696 &= 4144 \cdot 1 + 3552 \\
4144 &= 3552 \cdot 1 + 592 \\
3522 &= 592 \cdot 6 + 0
\end{aligned}$$

Therefore, using the Eucledian algorithm,

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

Problem 1.2. Calculate $(3141, 1592)$ and $(10001, 100083)$.

$$\begin{aligned}
3141 &= 1592 \cdot 1 + 1549 \\
1592 &= 1549 \cdot 1 + 43 \\
1549 &= 43 \cdot 36 + 1
\end{aligned}$$

Therefore, using the Eucledian algorithm,

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

$$\begin{aligned}
100083 &= 10001 \cdot 10 + 73 \\
10001 &= 73 \cdot 137 + 0
\end{aligned}$$

Therefore, using the Eucledian algorithm,

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

Problem 1.3. 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 1.4. Find x and y such that $4144x + 7696y = 592$.

From problem 1, we know that a solution exists.

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

Using backsubstitution we get

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

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

Problem 1.5. 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, $d \geqslant 1$, therefore $d = 1$.
The same argument can be said for (N, b) and (N, c).

Problem 1.6. Find two different solutions of $299x + 247y = 13$.

Using the Eucledian 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 1.7. 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 1.8. 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, $c \leqslant a$. Thus $(a, b) = a$.

Problem 1.9. 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 1.10.

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

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

   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 1.11.

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 $d \leqslant 1$. 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 1.12. 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 1.13. 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 1.14. 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 1.15.

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.

2 Unique Factorization

Exercise 2.1. How many even primes are there? How many whose last digit is 5?

2 is a prime. But for other positive even numbers, by definition they are divisible by 2. So there is only one even prime.

5 is a prime. But for other positive numbers that has 5 as their last digit, the number can be written as

$$10^n d_n ... + 100 d_2 + 10 d_1 + 5$$

Where $d_1, d_2, ..., d_n$ are the digits of that number. All the terms are divisible by 5, so the number itself is divisible by 5 which means that it is not a prime. Therefore the only prime number whose last digit is 5 is 5 itself.

Exercise 2.2. Using induction, show that every integer n where $n > 1$ can be written as a product of primes.

It is true for $n = 2$, because 2 itself is a prime. Suppose it is true for $n \leqslant k$. If $k+1$ is a prime, then we are done. If not, then it is divisible by a prime p_1 by Lemma 1. So $k+1 = p_1 q$ where $1 < q \leqslant k$, But from the induction assumption, q can be written as a product of primes $p_2 p_3 \cdots p_i$, so $k+1$ can be written as $p_1 p_2 p_3 \cdots p_i$ which is a product as primes.

Exercise 2.3. Write prime decompositions for 72 and 480.

Just repeatedly do divisions using the first divisor that comes into mind.

$$\begin{aligned}72 &= 2 \cdot 36\\ &= 2 \cdot 2 \cdot 18\\ &= 2 \cdot 2 \cdot 2 \cdot 9\\ &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3\end{aligned}$$

$$\begin{aligned}480 &= 2 \cdot 240\\ &= 2 \cdot 2 \cdot 120\\ &= 2 \cdot 2 \cdot 2 \cdot 60\\ &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 30\\ &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 15\\ &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5\end{aligned}$$

Exercise 2.4. Which members of the set $4n + 1, n \geqslant 0$ less than 100 are not prome (like prime, but based on this set)?

- $25 = 5 \cdot 5$
- $45 = 5 \cdot 9$
- $65 = 5 \cdot 13$
- $85 = 5 \cdot 17$

Exercise 2.5. What is the prime-power decomposition of 7950?

We see that it is divisible by 2 and 5, so we get $7950 = 2 \cdot 5 \cdot 795$. We divide it again by 5 to get $7950 = 2 \cdot 5 \cdot 5 \cdot 159$. Then consulting the factor table, we see that 159 is divisible by 3, so we get $7950 = 2 \cdot 3 \cdot 5 \cdot 5 \cdot 53$. Finally we see from the table that 53 is a prime so we are done.

Problem 2.1. Find the prime-prower decompositions of 1234, 34560, and 111111.

We can try repeatedly dividing it by 2, and if that fails 3, then 5, while checking whether the quotient is a prime using the factor table.

$$1234 = 2 \cdot 617$$

$$34560 = 2^8 \cdot 3^3 \cdot 5$$

111111 can be seen at a glance as three 11s, so they are just the sum of 11 times a multiple of 10 which changes their decimal place.

$$\begin{aligned}111111 &= 110000 + 1100 + 11\\ &= 11(10000 + 100 + 1)\\ &= 11 \cdot 10101\end{aligned}$$

Now note that shifting 111 around, we get 11100 + 111 = 11211 which is not quite 10101, but 11211 - 1110 = 10101. Therefore

$$\begin{aligned}10101 &= 11100 - 1110 + 111\\ &= 111(100 - 10 + 1)\\ &= 111 \cdot 91\end{aligned}$$

Therefore

$$\begin{aligned}111111 &= 11 \cdot 10101\\ &= 11 \cdot 111 \cdot 91\end{aligned}$$

111 and 91 are both composite, and it is quite easy to check their factorization which gives

$$111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$$

Problem 2.2. Find the prime-power decompositions of 2345, 45670, and 999999999999. (Note that $101 \mid 1000001$.)

With the help of the factor table, we can see that

$$2345 = 5 \cdot 7 \cdot 67$$

and

$$45670 = 2 \cdot 5 \cdot 4567$$

For 999999999999, first note that the number is divisible by $9 = 3 \cdot 3$, so

$$999999999999/(3 \cdot 3) = 111111111111$$

In addition, 111111111111/11 = 10101010101

The digits of 10101010101 is just 101 shifted several times, and indeed

$$\begin{aligned}10101010101 &= 10100000000 + 1010000 + 101\\ &= 101(100000000 + 10000 + 1)\\ &= 101 \cdot 100010001\end{aligned}$$

After that we can repeatedly divide by small primes, which gives

$$100010001 = 3 \cdot 7 \cdot 13 \cdot 366337$$

Note that $3663 = 3330 + 333 = 333 \cdot 11$, and $333 = 37 \cdot 9$. Indeed $366337 = 37 \cdot 9901$. We can check from the factor table that 9901 is a prime, so by gathering all of the factors above we get

$$999999999999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$$

Problem 2.3. Tartaglia (1556) claimed that the sums $1+2+4$, $1+2+4+8$, $1+2+4+8+16$, ... are alternately prime and composite. Show that he was wrong.

Written in binary, the sequence is 111, 1111, 11111, ... so their values are $2^n - 1$ where $n \geqslant 3$. The values are then $\mathbf{7}, 15, \mathbf{31}, 63, \mathbf{127}, 255, \mathbf{511}, \dots$ where the numbers in bold are supposed to be prime.

However we can confirm that $511 = 7 \cdot 73$, so Tartaglia's claim is false.

Problem 2.4.

a) DeBouvelles (1509) claimed that one or both of $6n+1$ and $6n-1$ are primes for all $n \geqslant 1$. Show that he was wrong.

b) Show that there are infinitely many n such that both $6n-1$ and $6n+1$ are composite.

By trial for $n = 1, 2, 3, \dots$ we find that for $n = 20$, $6 \cdot 20 - 1 = 119 = 7 \cdot 17$ and $6 \cdot 20 + 1 = 121 = 11^2$ so the statement doesn't hold. It doesn't only show that he was wrong, but also lazy (presumably checking only up to $n = 19$) or couldn't factorize.

For the proof that there are infinitely many such n, we will use the Chinese Remainder Theorem so understanding material from chapter 5 is recommended. The method could perhaps be used without the language of congruence, but it will be wordy.

Note that for $n = 36$, $6 \cdot 36 - 1 = 215 = 5 \cdot 43$ and $6 \cdot 36 + 1 = 217 = 7 \cdot 31$. In that instance $5 \mid 6n-1$ and $7 \mid 6n+1$, and it suffices to show that we can find infinitely many other n where it holds. In other words,

$$6n - 1 \equiv 0 \pmod 5$$

and

$$6n + 1 \equiv 0 \pmod 7$$

Or simplifying

$$n \equiv 1 \pmod 5$$

and

$$n \equiv 1 \pmod 7$$

By using Chinese Remainder Theorem, we know that a solution exists (mod 35) and it is

$$n \equiv 1 \pmod{35}$$

So there are infinite numbers of n where the equation holds.

(Note that the divisors 5 and 7 is not special, we can use the method for other n and divisors but 5 and 7 are small numbers so we chose it.)

Reference: `https://math.stackexchange.com/questions/102493/infinite-number-of-composite-pa`

Problem 2.5. Prove that if n is a square, then each exponent in its prime-power decomposition is even.

Suppose that $n = a^2$ and $a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ is the prime-power decomposition of a. Then it follows that

$$\begin{aligned} n &= \left(p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}\right)^2 \\ &= p_1^{2e_1} p_2^{2e_2} \cdots p_m^{2e_m} \end{aligned}$$

Problem 2.6. Prove that if each exponent in the prime-power decomposition of n is even, then n is a square.

$$\begin{aligned} n &= p_1^{2e_1} p_2^{2e_2} \cdots p_m^{2e_m} \\ &= \left(p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}\right)^2 \\ &= m^2 \end{aligned}$$

where m is an integer. Therefore n is a square.

Problem 2.7. Find the smallest integer divisible by 2 and 3 which is simultaneously a square and a fifth power.

If it is a square, its prime-power decomposition must have the form of

$$p_1^{2e_1} p_2^{2e_2} \cdots p_m^{2e_m}$$

And if it is a fifth power, it must have the form

$$p_1^{5f_1} p_2^{5f_2} \cdots p_m^{5f_m}$$

To satisfy both, the form must then be

$$p_1^{2\cdot 5g_1} p_2^{2\cdot 5g_2} \cdots p_m^{2\cdot 5g_m} = p_1^{10g_1} p_2^{10g_2} \cdots p_m^{10g_m}$$

Since we want to find the smallest such number, we have to set $g_k = 1$ for all k, so the number is

$$p_1^{10} p_2^{10} \cdots p_m^{10}$$

Furthermore, because the number is both divisible by 2 and 3, it must be

$$2^{10} 3^{10} p_3^{10} \cdots p_m^{10}$$

But again, we want the smallest such number so $m = 2$, which means the number is

$$2^{10} 3^{10} = 60466176$$