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

Greg Kikola

July 15, 2019

Contents

1 Integers **1**

1.1 Exercises 1

1.2 Problems 2

2 Unique Factorization **7**

2.1 Exercises 7

2.2 Problems 8

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. $\square$

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. $\square$

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. $\square$

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 $(578, 442) = 34$. $\square$

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 $(N, a) = (N, b) = (N, c) = 1$. $\square$

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. $\square$

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 $a = -b$. $\square$

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 $(a, b) = a$. $\square$

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. □

Chapter 2

Unique Factorization

2.1 Exercises

2.1.1 Exercise 1

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

Solution. If a prime p is even then by definition $2 \mid p$. Therefore the only prime that is even is 2 itself. Similarly, any positive integer that ends in a 5 (written in base 10) must be divisible by 5 (this is due to the fact that our base, 10, is itself divisible by 5). And the only prime divisible by 5 is 5 itself. $\square$

2.1.2 Exercise 2

Construct a proof of Lemma 2 using induction.

Solution. Lemma 2 says that every positive integer greater than 1 can be written as a product of primes. 2 is a prime and is a product of itself, so the base case is satisfied. Now suppose there is an integer $n > 1$ such that every integer k with $1 < k \leq n$ can be written as a product of primes. We must show that $n+1$ can be written as such a product.

If $n+1$ is prime, then we are done, it is already a product of primes. If not, then $n+1$ is composite, and we may write $n+1 = st$ where s and t are each integers with $1 < s, t < n+1$. By the inductive hypothesis, s and t can each be written as a product of primes,

$$s = p_1 p_2 \cdots p_i, \quad \text{and} \quad t = q_1 q_2 \cdots q_j,$$

where each p_k and q_k are prime (not necessarily distinct). Then

$$n + 1 = st = p_1 p_2 \cdots p_i q_1 q_2 \cdots q_j,$$

and we have written $n+1$ as a product of primes, completing the inductive step. It follows by induction that all integers $n > 1$ can be written as a product of primes. $\square$

2.1.3 Exercise 3

Write prime decompositions for 72 and 480.

Solution. $72 = 8 \cdot 9 = 2^3 \cdot 3^2$ and $480 = 48 \cdot 10 = 16 \cdot 3 \cdot 10 = 2^5 \cdot 3 \cdot 5$. $\square$

2.1.4 Exercise 4

Which members of the set less than 100 are not prome?

Solution. The set being referenced in the question is the set

$$A = \{4n + 1 \mid n = 0, 1, 2, \dots\},$$

where $k \in A$ is considered "prome" if it has no divisors in A other than 1 and itself.

Since $100^{1/2} = 10$, we only need to look for divisors less than or equal to 10. The only such members of A are 1, 5, and 9. So any nonprome member of A less than 100 must be a multiple of 5 or 9. These numbers are

$$25, 45, 65, 81, 85.$$

$\square$

2.1.5 Exercise 5

What is the prime-power decomposition of 7950?

Solution. 7950 is divisible by $50 = 2 \cdot 5^2$, so dividing by 50 gives 159. 159 is divisible by 3, so divide by 3 to get 53. Since 53 is prime we are done. Therefore

$$7950 = 2 \cdot 3 \cdot 5^2 \cdot 53.$$

$\square$

2.2 Problems

2.2.1 Problem 1

Find the prime-power decompositions of 1234, 34560, and 111111.

Solution. First, 1234 is divisible by 2, so we write $1234 = 2 \cdot 617$. Now 617 is not divisible by 2 or 5. Using the table in Appendix C, we see that 617 is prime. Therefore $1234 = 2 \cdot 617$ is the prime factorization.

For 34560, first we divide by all factors of 2 and 5 to get $34560 = 2^8 \cdot 5 \cdot 27$. Now 27 factors as 3^3 so this gives

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

Finally, 111111 is too big for the table, but by trying small possible divisors we can see that it is divisible by 3, with $111111 = 3 \cdot 37037$. And 37037 is divisible by 7: $37037 = 7 \cdot 5291$. Now we may make use of the table to determine that 5291 is divisible by 11. $5291/11 = 481$, which is divisible by 13. $481/13 = 37$, and 37 is prime. So

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

$\square$

2.2.2 Problem 2

Find the prime-power decompositions of 2345, 45670, and 999999999999.

Solution. Proceeding in the same manner as in the previous problem, we find

$$2345 = 5 \cdot 7 \cdot 67,$$
$$45670 = 2 \cdot 5 \cdot 4567,$$

and

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

2.2.3 Problem 3

Tartaglia (1556) claimed that the sums

$$1+2+4, \quad 1+2+4+8, \quad 1+2+4+8+16, \quad \cdots$$

are alternately prime and composite. Show that he was wrong.

Proof. Looking at the partial sums having an odd number of terms, we find

$$\begin{aligned} 1+2+4 &= 7 \\ 1+2+4+8+16 &= 31 \\ 1+2+4+8+16+32+64 &= 127 \\ 1+2+4+8+16+32+64+128+256 &= 511 = 7 \cdot 73. \end{aligned}$$

Since 511 is not prime, we see that Tartaglia's conjecture was not correct. $\square$

2.2.4 Problem 4

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

Proof. For $n = 20$, we have $6n+1 = 121 = 11^2$ and $6n-1 = 119 = 7 \cdot 17$. Therefore DeBouvelles's claim is not correct. $\square$

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

Proof. Suppose there are finitely many n with both $6n-1$ and $6n+1$ composite. Let them be $n_1, n_2, \ldots, n_k$.

Now let $n = (6n_k + 9)!$, where ! denotes the factorial function (i.e., $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$). Now the integers $n+2, n+3, \ldots, n+9$ are all composite, since for any m with $2 \leq m \leq 9$, we clearly have $m \mid n+m$. So we have found a sequence of 8 consecutive composite numbers. Now these numbers must include a pair of the form $6t-1$ and $6t+1$. But both of these are composite, and $t > n_k$. This is a contradiction, since n_k was supposed to be the largest such value. Therefore there are infinitely many n with both $6n-1$ and $6n+1$ composite. $\square$

2.2.5 Problem 5

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

Proof. Let $n > 1$ be a square and write $n = k^2$ for some integer $k > 1$. Let the prime-power decomposition of k be

$$k = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

Then

$$\begin{aligned} n &= (p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r})^2 \\ &= (p_1^{e_1})^2 (p_2^{e_2})^2 \cdots (p_r^{e_r})^2 \\ &= p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r}. \end{aligned}$$

Since this prime-power decomposition must be unique (up to reordering), we see that every exponent in the prime-power decomposition of n is even. □

2.2.6 Problem 6

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

Proof. Suppose every exponent in the prime-power decomposition of n is even. Then each exponent e_i in the decomposition has the form $e_i = 2f_i$ for some integer f_i. Then n can be written

$$\begin{aligned} n &= p_1^{2f_1} p_2^{2f_2} \cdots p_r^{2f_r} \\ &= (p_1^{f_1})^2 (p_2^{f_2})^2 \cdots (p_r^{f_r})^2 \\ &= (p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r})^2 \\ &= k^2, \end{aligned}$$

where $k = p_1^{f_1} \cdots p_r^{f_r}$, and we see that n is a square. □

2.2.7 Problem 7

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

Solution. Let the smallest such number be n. The least common multiple of 2 and 3 is 6, so $6 \mid n$. n is a square and a fifth power, so n must actually be a tenth power, since 10 is the least common multiple of 2 and 5. The smallest tenth power divisible by 6 is 6^{10}, so we have

$$n = 6^{10} = 60466176.$$ □

2.2.8 Problem 8

If $d \mid ab$, does it follow that $d \mid a$ or $d \mid b$?

Solution. No. For example, $6 \mid 4 \cdot 9$ but $6 \nmid 4$ and $6 \nmid 9$. If, however, we know that d is prime, then the conclusion *does* hold, as proved in Lemma 5. □

2.2.9 Problem 9

Is it possible for a prime p to divide both n and $n+1$ ($n \geq 1$)?

Solution. No. For, if it is possible, suppose the prime p divides both n and $n+1$. Then p also divides their difference, $(n+1)-n=1$. So we would have $p \mid 1$, which is clearly absurd. $\square$

2.2.10 Problem 10

Prove that $n(n+1)$ is never a square for $n>0$.

Proof. Suppose $n(n+1)=k^2$ for some integer $k>0$. Then $n^2+n=k^2$ which gives $k^2-n^2=n$. Factoring the left-hand side then gives

$$(k+n)(k-n)=n.$$

So in particular, $k+n \mid n$. But this is impossible, since $k+n>n>0$. This contradiction shows that $n(n+1)$ is not a square. $\square$

2.2.11 Problem 11

(a) Verify that $2^5 \cdot 9^2 = 2592$.

Solution. Direct computation gives $2^5 \cdot 9^2 = 32 \cdot 81 = 2592$. $\square$

(b) Is $2^5 \cdot a^b = 25ab$ possible for other a, b? (Here $25ab$ denotes the digits of $2^5 \cdot a^b$ and not a product.)

Solution. Suppose it is possible, and let a and b be single-digit integers, $0 \leq a, b \leq 9$, so that

$$2^5 \cdot a^b = 2500 + 10a + b.$$

Note that

$$78 < a^b = \frac{2500+10a+b}{32} < 82.$$

So the only possibilities for a^b are 79, 80, and 81. But 79 is prime, and $80 = 2^4 \cdot 5$, so neither of these are perfect powers. Therefore $a^b = 81$ and we see that either $a=3, b=4$ or $a=9, b=2$. Since $32 \cdot 81 = 2592$, only the second combination works. $\square$

2.2.12 Problem 12

Let p be the least prime factor of n, where n is composite. Prove that if $p > n^{1/3}$, then n/p is prime.

Proof. Let p and n be as stated, and suppose n/p is composite, so that $n/p = ab$, where $a, b > 1$. Then $n = abp$. And since $p > n^{1/3}$, we have

$$n = abp < p^3, \quad \text{which implies} \quad ab < p^2.$$

It follows that one of a, b must be less than p. Since $a, b > 1$ we see that one of a or b must contain a prime factor q smaller than p. But then $q \mid n$, which contradicts the fact that p is the smallest prime divisor. Therefore n/p is prime. $\square$

2.2.13 Problem 13

True or false? If p and q divide n, and each is greater than $n^{1/4}$, then n/pq is prime.

Solution. False. As a counterexample, take $n = 60 = 2^2 \cdot 3 \cdot 5$. Now, we have $60^{1/4} < 81^{1/4} = 3$. So $p = 3$ and $q = 5$ are both greater than $n^{1/4}$, each divide n, but $n/pq = 4$ is not prime. □

2.2.14 Problem 14

Prove that if n is composite, then 2^{n-1} is composite.

Proof. Let n be composite. 2^{n-1} is composite as long as $n > 2$. But the smallest composite number is 4, so we certainly have $n > 2$. Therefore 2^{n-1} is composite for any composite number n. □

2.2.15 Problem 15

Is it true that if $2^n - 1$ is composite, then n is composite?

Solution. No. For example, $2047 = 2^{11} - 1$ is composite since $2047 = 23 \cdot 89$, but 11 is not composite. □