

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

Greg Kikola

July 28, 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
3	Linear Diophantine Equations	13
3.1	Exercises	13
3.2	Problems	14
4	Congruences	19
4.1	Exercises	19
4.2	Problems	21

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

$$343 = 280 \cdot 1 + 63$$

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

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

$$28 = 7 \cdot 4.$$

Therefore $(343, 280) = 7$.

For the second pair,

$$578 = 442 \cdot 1 + 136$$

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

$$136 = 34 \cdot 4,$$

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

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 $d = 1$. \square

(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 $(4, 6) = 2$. \square

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 $d = 1$. \square

(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 $(k, n + k) = (k, n)$. \square

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 $ac \mid bd$. \square

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. \square

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 $c \mid db$. \square

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. \square

- (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 . \square

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 $480 = 48 \cdot 10 = 16 \cdot 3 \cdot 10 = 2^5 \cdot 3 \cdot 5$. □

2.1.4 Exercise 4

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

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 “prime” 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 nonprime member of A less than 100 must be a multiple of 5 or 9. These numbers are

$$25, 45, 65, 81, 85. \quad \square$$

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

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

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

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

2.2.2 Problem 2

Find the prime-power decompositions of 2345, 45670, and 99999999999.

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

$$\begin{aligned} 2345 &= 5 \cdot 7 \cdot 67, \\ 45670 &= 2 \cdot 5 \cdot 4567, \end{aligned}$$

and

$$99999999999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901. \quad \square$$

2.2.3 Problem 3

Tartaglia (1556) claimed that the sums

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

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, \dots, 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 $n + 2, n + 3, \dots, n + 9$ 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. \square

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. \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

$$n = 6^{10} = 60466176. \quad \square$$

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. \square

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. \square

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 . \square

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. \square

Chapter 3

Linear Diophantine Equations

3.1 Exercises

3.1.1 Exercise 1

The equation $2x + 4y = 5$ has no solutions in integers. Why not?

Solution. If x and y are integers such that $2x + 4y = 5$, then $2(x + 2y) = 5$ and we see that $2 \mid 5$, which is clearly absurd. \square

3.1.2 Exercise 2

Find by inspection a solution of $x + 5y = 10$ and use it to write five other solutions.

Solution. Certainly $x = 0$ and $y = 2$ works, so by Lemma 1 we also have the solutions

$$x = 5t \quad \text{and} \quad y = 2 - t$$

for any integer t . Five such solutions, written as ordered pairs, are $(-10, 4)$, $(-5, 3)$, $(5, 1)$, $(10, 0)$, and $(15, -1)$. \square

3.1.3 Exercise 3

Which of the following linear diophantine equations is impossible? (We will say that a diophantine equation is *impossible* if it has no solutions).

(a) $14x + 34y = 90$.

Solution. Since $(14, 34) = 2$ and $2 \nmid 90$, it follows by Lemma 2 that this equation has at least one solution. \square

(b) $14x + 35y = 91$.

Solution. $(14, 35) = 7$ and $7 \mid 91$, so this equation has a solution. \square

(c) $14x + 36y = 93$.

Solution. This time, $(14, 36) = 2$ but $2 \nmid 93$, so this equation is impossible. \square

3.1.4 Exercise 4

Find all solutions of $2x + 6y = 20$.

Solution. Dividing by 2 gives $x + 3y = 10$. A particular solution is given by $(x_0, y_0) = (10, 0)$, so by Lemma 3 all solutions have the form

$$x = 10 + 3t \quad \text{and} \quad y = -t$$

where t is an integer. \square

3.1.5 Exercise 5

Find all the solutions of $2x + 6y = 18$ in *positive* integers.

Solution. In the text, the general solution was found to be

$$x = 9 + 3t \quad \text{and} \quad y = -t,$$

for t an integer. If x is to be positive, then $9 + 3t > 0$ and, solving for t , we get $t > -3$. On the other hand, if $y > 0$ then $t < 0$. So we have $-3 < t < 0$ and we see that the only solutions are given by $t = -2$ and $t = -1$. These solutions are, respectively, $(3, 2)$ and $(6, 1)$. \square

3.2 Problems

3.2.1 Problem 1

Find all the integer solutions of $x + y = 2$, $3x - 4y = 5$, and $15x + 16y = 17$.

Solution. For $x + y = 2$, a particular solution is $(1, 1)$, so the general solution is

$$x = 1 + t \quad \text{and} \quad y = 1 - t,$$

where t is an integer.

For $3x - 4y = 5$ we find by inspection the particular solution $(3, 1)$ which gives the general solution of

$$x = 3 - 4t \quad \text{and} \quad y = 1 - 3t.$$

Lastly, for $15x + 16y = 17$, one solution is $(-1, 2)$. Then the general solution is

$$x = -1 + 16t \quad \text{and} \quad y = 2 - 15t. \quad \square$$

3.2.2 Problem 2

Find all the integer solutions of $2x + y = 2$, $3x - 4y = 0$, and $15x + 18y = 17$.

Solution. For $2x + y = 2$, one solution is $(1, 0)$, so the general solution is

$$x = 1 + t \quad \text{and} \quad y = -2t$$

for an integer t .

For $3x - 4y = 0$, a particular solution is $(4, 3)$, producing the general solution

$$x = 4 - 4t \quad \text{and} \quad y = 3 - 3t.$$

Lastly, the equation $15x + 18y = 17$ has no solutions since $(15, 18) = 3$ but 3 does not divide 17. \square

3.2.3 Problem 3

Find the solutions in positive integers of $x + y = 2$, $3x - 4y = 5$, and $6x + 15y = 51$.

Solution. In Problem 3.2.1 we found the general solution of $x + y = 2$ to be $(1 + t, 1 - t)$. If $x > 0$ then $t > -1$ and if $y > 0$ then $t < 1$. So the only solution in positive integers is given by $t = 0$, which corresponds to the solution $(1, 1)$.

For $3x - 4y = 5$ we found the general solution to be $(3 - 4t, 1 - 3t)$. Setting $y > 0$ gives

$$t < \frac{1}{3},$$

and we see that x and y are positive integers if and only if t is an integer with $t \leq 0$. So the solutions are $(3, 1)$, $(7, 4)$, $(11, 7)$, \dots .

To solve $6x + 15y = 51$, we divide by 3 to get $2x + 5y = 17$. A particular solution is $(1, 3)$, leading to the general solution of $(1 + 5t, 3 - 2t)$. By setting x and y greater than 0, we determine that

$$-\frac{1}{5} < t < \frac{3}{2}.$$

So $t = 0$ or 1 , making the only positive solutions $(1, 3)$ and $(6, 1)$. \square

3.2.4 Problem 4

Find all the solutions in positive integers of $2x + y = 2$, $3x - 4y = 0$, and $7x + 15y = 51$.

Solution. Using the results from Problem 3.2.2, the general solution for $2x + y = 2$ was $(1 + t, -2t)$. Both variables are positive when $-1 < t < 0$, but there are no integers strictly between -1 and 0 , so there are no positive solutions.

For $3x - 4y = 0$ we found the general solution $(4 - 4t, 3 - 3t)$. All of these solutions are positive integers so long as $t \leq 0$. Particular solutions are $(4, 3)$, $(8, 6)$, $(12, 9)$, and so on.

For $7x + 15y = 51$, we find the particular solution $(0, 1)$ which leads to the general solution $(15t, 1 - 7t)$. However, there is no integer value of t which makes both x and y positive. \square

3.2.5 Problem 5

Find all the positive solutions in integers of

$$\begin{aligned}x + y + z &= 31, \\x + 2y + 3z &= 41.\end{aligned}$$

Solution. Subtracting the first equation from the second gives

$$y + 2z = 10.$$

This equation has the particular solution $(y, z) = (0, 5)$ which leads to the general solution $(2t, 5 - t)$. Taking $y, z > 0$ we find that the only relevant solutions are $(2, 4)$, $(4, 3)$, $(6, 2)$, and $(8, 1)$. Substituting these into either of the original equations allows us to find the corresponding values for x . The four solutions are

$$\begin{aligned}x = 25, \quad y = 2, \quad \text{and} \quad z = 4; \\x = 24, \quad y = 4, \quad \text{and} \quad z = 3; \\x = 23, \quad y = 6, \quad \text{and} \quad z = 2; \\x = 22, \quad y = 8, \quad \text{and} \quad z = 1.\end{aligned}$$

□

3.2.6 Problem 6

Find the five different ways a collection of 100 coins—pennies, dimes, and quarters—can be worth exactly \$4.99.

Solution. Let x be the number of pennies, y the number of dimes, and z the number of quarters. Since there are 100 coins, whose total value is \$4.99, we have the two equations

$$\begin{aligned}x + y + z &= 100 \\x + 10y + 25z &= 499.\end{aligned}$$

Subtracting the first equation from the second gives $9y + 24z = 399$. Dividing this equation by 3 then gives $3y + 8z = 133$. By inspection, a particular solution is $y = 7$ and $z = 14$. This gives the general solution $y = 7 + 8t$ and $z = 14 - 3t$. We find the positive solutions to be

$$\begin{aligned}t = 0: \quad x = 79, \quad y = 7, \quad \text{and} \quad z = 14; \\t = 1: \quad x = 74, \quad y = 15, \quad \text{and} \quad z = 11; \\t = 2: \quad x = 69, \quad y = 23, \quad \text{and} \quad z = 8; \\t = 3: \quad x = 64, \quad y = 31, \quad \text{and} \quad z = 5; \\t = 4: \quad x = 59, \quad y = 39, \quad \text{and} \quad z = 2.\end{aligned}$$

These are the only five solutions in the positive integers.

□

3.2.7 Problem 7

A man bought a dozen pieces of fruit—apples and oranges—for 99 cents. If an apple costs 3 cents more than an orange, and he bought more apples than oranges, how many of each did he buy?

Solution. Let x be the number of apples that the man bought, and let y be the number of oranges. The equation $x + y = 12$ has only five solutions in the positive integers with $x > y$, namely $(7, 5)$, $(8, 4)$, $(9, 3)$, $(10, 2)$, and $(11, 1)$.

Now, if a is the price of an apple, then the solution for x and y must also satisfy the equation $ax + (a - 3)y = 99$. If we substitute the solution $(7, 5)$ into this equation and simplify, we get $12a - 15 = 99$ or $a = 19/2$, which is not an integer. Similarly, the solutions $(8, 4)$, $(10, 2)$, and $(11, 1)$ also lead to non-integer values of a . The only solution that works is

$$x = 9 \quad \text{and} \quad y = 3,$$

with $a = 9$. Therefore, the man bought 9 apples at 9 cents each, and 3 oranges at 6 cents each. \square

3.2.8 Problem 8

The enrollment in a number theory class consists of sophomores, juniors, and backward seniors. If each sophomore contributes \$1.25, each junior \$.90, and each senior \$.50, the instructor will have a fund of \$25. There are 26 students; how many of each?

Solution. Let x be the number of sophomores, y the number of juniors, and z the number of seniors. Then we have the following system of equations:

$$x + y + z = 26, \tag{3.1}$$

$$125x + 90y + 50z = 2500. \tag{3.2}$$

Multiplying (3.1) by 50 and subtracting from (3.2) gives the equation

$$75x + 40y = 1200.$$

Dividing by 5 gives $15x + 8y = 240$. A particular solution is $(0, 30)$, so we have the general solution

$$x = 8t \quad \text{and} \quad y = 30 - 15t.$$

If x and y are to be positive, we see that $0 < t < 2$, so that $t = 1$. Therefore, there are 8 sophomores, 15 juniors, and 3 seniors. \square

3.2.9 Problem 9

The following problem first appeared in an Indian book written around 850 AD. Three merchants found a purse along the way. One of them said, “If I secure this purse, I shall become twice as rich as both of you with your money on hand.” Then the second said, “I shall become thrice as rich as both of you.” The third man said, “I shall become five times as rich as both of you.” How much did each merchant have, and how much was in the purse?

Solution. Let the three merchants each have x , y , and z units of currency, respectively, and let w be the amount of money in the purse. We have the following system of equations.

$$\begin{aligned}x + w &= 2(y + z), \\y + w &= 3(x + z), \\z + w &= 5(x + y).\end{aligned}$$

Rearranging and simplifying then gives

$$\begin{aligned}x - 2y - 2z + w &= 0, \\-3x + y - 3z + w &= 0, \\-5x - 5y + z + w &= 0.\end{aligned}$$

Solving these simultaneously, we find that the system reduces to

$$\begin{aligned}15x - w &= 0, \\5y - w &= 0, \\3z - w &= 0.\end{aligned}$$

So the purse has 15 times as much money as the first merchant, the second merchant has 3 times as much money as the first merchant, and the third merchant has 5 times as much money as the first merchant. So the three merchants and the purse have, respectively, x , $3x$, $5x$, and $15x$ units of currency, for an integer x . Any positive value for x will produce a valid solution. \square

3.2.10 Problem 10

A man cashes a check for d dollars and c cents at a bank. Assume that the teller by mistake gives the man c dollars and d cents. Assume that the man does not notice the error until he has spent 23 cents. Assume further that he then notices that he has $2d$ dollars and $2c$ cents. Assume still further that he asks you what amount the check was for. Assuming that you can accept all the assumptions, what is the answer?

Solution. Let the check be for T cents. The man starts with c dollars and d cents. After spending 23 cents, he has $2d$ dollars and $2c$ cents. This gives

$$\begin{aligned}100d + c &= T, \\100c + d - 23 &= 100(2d) + 2c,\end{aligned}$$

or, rearranging,

$$\begin{aligned}c + 100d &= T, \\98c - 199d &= 23.\end{aligned}$$

By inspection, a particular solution to $98c - 199d = 23$ is $c = 51$ and $d = 25$. The general solution is then

$$c = 51 + 199t \quad \text{and} \quad d = 25 + 98t.$$

We know $0 \leq c < 100$ so the only possible value for t is $t = 0$. Therefore the check was written for $T = 25 \cdot 100 + 51 = 2551$ cents or \$25.51. \square

Chapter 4

Congruences

4.1 Exercises

4.1.1 Exercise 1

True or false? $91 \equiv 0 \pmod{7}$. $3 + 5 + 7 \equiv 5 \pmod{10}$. $-2 \equiv 2 \pmod{8}$. $11^2 \equiv 1 \pmod{3}$.

Solution. Only the third congruence is false.

Since $91 = 7 \cdot 13$ we have $7 \mid (91 - 0)$ so that $91 \equiv 0 \pmod{7}$.

$3 + 5 + 7 = 15$ and $10 \nmid (15 - 5)$ so $3 + 5 + 7 \not\equiv 5 \pmod{10}$.

It is not true that $-2 \equiv 2 \pmod{8}$, since $8 \nmid -4$.

And since $3 \mid (121 - 1)$, we indeed have $11^2 \equiv 1 \pmod{3}$. \square

4.1.2 Exercise 2

Complete the proof that $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.

Solution. In the text, Dudley proves the left-to-right implication. So we need to show the converse. Suppose that $a = b + km$ for some integer k . Then $a - b = km$ and we have by the definition of divisibility that $m \mid (a - b)$. Therefore $a \equiv b \pmod{m}$. \square

4.1.3 Exercise 3

To what least residue $\pmod{11}$ is each of 23, 29, 31, 37, and 41 congruent?

Solution. We have

$$23 \equiv 1 \pmod{11},$$

$$29 \equiv 7 \pmod{11},$$

$$31 \equiv 9 \pmod{11},$$

$$37 \equiv 4 \pmod{11},$$

and

$$41 \equiv 8 \pmod{11}. \quad \square$$

4.1.4 Exercise 4

Say “ n is odd” in three other ways.

Solution. From the theorems in the text, n is odd if and only if $n \equiv 1 \pmod{2}$, if and only if $n = 2k + 1$ for some integer k , if and only if n has remainder 1 when divided by 2. \square

4.1.5 Exercise 5

Prove that $p \mid a$ if and only if $a \equiv 0 \pmod{p}$.

Proof. This is immediate from the definition of congruence, since $p \mid a$ if and only if $p \mid (a - 0)$. \square

4.1.6 Exercise 6

Prove that $a \equiv a \pmod{m}$ for all integers a .

Proof. Since any positive integer m must divide 0, we have $m \mid (a - a)$ so that $a \equiv a \pmod{m}$. \square

4.1.7 Exercise 7

Prove that for all integers a and b , if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

Proof. If $a \equiv b \pmod{m}$ then $a - b = km$ for some integer k . Then we also have $b - a = (-k)m$ so that $b \equiv a \pmod{m}$. \square

4.1.8 Exercise 8

Prove that for integers a , b , and c , if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof. By definition, there are integers s and t with $a - b = sm$ and $b - c = tm$. So

$$a - c = (a - b) + (b - c) = sm + tm = (s + t)m,$$

hence $m \mid (a - c)$. \square

4.1.9 Exercise 9

Prove that for integers a , b , c , and d , if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Proof. We have $a = b + sm$ and $c = d + tm$ for integers s and t . So

$$a + c = (b + sm) + (d + tm) = (b + d) + (s + t)m,$$

and we see that $a + c \equiv b + d \pmod{m}$. \square

4.1.10 Exercise 10

Construct a like example for modulus 10 to show that $ab \equiv ac \pmod{m}$ and $a \not\equiv 0 \pmod{m}$ do not together imply $b \equiv c \pmod{m}$.

Solution. We have $5 \cdot 2 \equiv 5 \cdot 4 \pmod{10}$ and $5 \not\equiv 0 \pmod{10}$, but $2 \not\equiv 4 \pmod{10}$. \square

4.1.11 Exercise 11

What values of x satisfy

(a) $2x \equiv 4 \pmod{7}$?

Solution. Since $(2, 7) = 1$, we are allowed (by Theorem 4) to cancel a factor of 2 on each side to get $x \equiv 2 \pmod{7}$. \square

(b) $2x \equiv 1 \pmod{7}$?

Solution. Since $1 \equiv 8 \pmod{7}$, we can again cancel a factor of 2 to get $x \equiv 4 \pmod{7}$. \square

4.1.12 Exercise 12

Which x will satisfy $2x \equiv 4 \pmod{6}$?

Solution. We have $(2, 6) = 2$. Applying Theorem 5, we get

$$x \equiv 2 \pmod{3}. \quad \square$$

4.2 Problems**4.2.1 Problem 1**

Find the least residue of $1492 \pmod{4}$, $\pmod{10}$, and $\pmod{101}$.

Solution. Since $1492 = 4 \cdot 373$ we have $1492 \equiv 0 \pmod{4}$. Since its last decimal digit is 2, we know that $1492 \equiv 2 \pmod{10}$. Finally, since $1492 = 14 \cdot 101 + 78$, we have $1492 \equiv 78 \pmod{101}$. \square

4.2.2 Problem 2

Find the least residue of $1789 \pmod{4}$, $\pmod{10}$, and $\pmod{101}$.

Solution. We have $1789 \equiv 1 \pmod{4}$, $1789 \equiv 9 \pmod{10}$, and $1789 \equiv 72 \pmod{101}$. \square

4.2.3 Problem 3

Prove or disprove that if $a \equiv b \pmod{m}$, then $a^2 \equiv b^2 \pmod{m}$.

Solution. This is true. The proof is immediate from part (e) of Lemma 1. \square

4.2.4 Problem 4

Prove or disprove that if $a^2 \equiv b^2 \pmod{m}$, then $a \equiv b$ or $-b \pmod{m}$.

Solution. This is not true in general. For a counterexample, take $m = 12$. We have $2^2 \equiv 4^2 \pmod{12}$ but $2 \not\equiv 4 \pmod{12}$ and $2 \not\equiv -4 \equiv 8 \pmod{12}$. \square

4.2.5 Problem 5

Find all m such that $1066 \equiv 1776 \pmod{m}$.

Solution. We need m to divide $1776 - 1066 = 710$. Since $710 = 2 \cdot 5 \cdot 71$, the possible values of m are 1, 2, 5, 10, 71, 142, 355, and 710. \square

4.2.6 Problem 6

Find all m such that $1848 \equiv 1914 \pmod{m}$.

Solution. $1914 - 1848 = 66$ which factors as $66 = 2 \cdot 3 \cdot 11$, so the possible values for m are 1, 2, 3, 6, 11, 22, 33, or 66. \square

4.2.7 Problem 7

If $k \equiv 1 \pmod{4}$, then what is $6k + 5$ congruent to $\pmod{4}$?

Solution. From Lemma 1, we have

$$6k + 5 \equiv 6 \cdot 1 + 5 \equiv 11 \equiv 3 \pmod{4}. \quad \square$$

4.2.8 Problem 8

Show that every prime (except 2) is congruent to 1 or 3 $\pmod{4}$.

Solution. Let p be a prime bigger than 2. Since no prime (other than 2) is divisible by 2, we cannot have $p = 4k$ or $p = 4k + 2$ for an integer k . So $4 \nmid p$ and $4 \nmid (p - 2)$. Therefore $p \not\equiv 0 \pmod{4}$ and $p \not\equiv 2 \pmod{4}$. The only remaining possibilities are $p \equiv 1$ or $3 \pmod{4}$. \square

4.2.9 Problem 9

Show that every prime (except 2 or 3) is congruent to 1 or 5 $\pmod{6}$.

Solution. Let p be a prime larger than 3. If $p \equiv 0 \pmod{6}$, then $6 \mid p$ which is impossible. If $p \equiv 2 \pmod{6}$ then $p = 6k + 2 = 2(3k + 1)$ for an integer k , which is impossible. If $p \equiv 3 \pmod{6}$ then $p = 6k + 3 = 3(2k + 1)$, which is impossible. And if $p \equiv 4 \pmod{6}$ then $p = 6k + 4 = 2(3k + 2)$, which is again impossible. The only possibilities are $p \equiv 1$ or $5 \pmod{6}$. \square

4.2.10 Problem 10

What can primes (except 2, 3, or 5) be congruent to (mod 30)?

Solution. Let p be a prime greater than 5 and let k be a nonnegative integer less than 30. If $p \equiv k \pmod{30}$ then $p = 30n + k$ for some integer n . From this we see that p cannot be prime (larger than 5) unless $(30, k) = 1$ (since the factors of 30 are 2, 3, and 5, and primes larger than 5 cannot be divisible by these numbers). So the possible values for k are those that are relatively prime to 30, namely 1, 7, 11, 13, 17, 19, 23, or 29. \square

4.2.11 Problem 11

In the multiplication $31415 \cdot 92653 = 2910\ 93995$, one digit in the product is missing and all the others are correct. Find the missing digit without doing the multiplication.

Solution. By repeatedly summing the digits, we see that

$$31415 \cdot 92653 \equiv 14 \cdot 25 \equiv 5 \cdot 7 \equiv 35 \equiv 8 \pmod{9}.$$

Using k in place of the missing digit in the product, we have

$$2910k93995 \equiv 47 + k \equiv 11 + k \equiv 2 + k \pmod{9}.$$

So $2 + k \equiv 8 \pmod{9}$ and we see that k must be 6. \square

4.2.12 Problem 12

Show that no square has as its last digit, 2, 3, 7, or 8.

Proof. Let n be any nonnegative integer. Modulo 10, there are only 10 possible least residues for n , so we may simply square each of them and reduce:

$$\begin{array}{llll} n \equiv 0 \pmod{10} & \Rightarrow & n^2 \equiv 0 \pmod{10}, \\ n \equiv 1 \pmod{10} & \Rightarrow & n^2 \equiv 1 \pmod{10}, \\ n \equiv 2 \pmod{10} & \Rightarrow & n^2 \equiv 4 \pmod{10}, \\ n \equiv 3 \pmod{10} & \Rightarrow & n^2 \equiv 9 \pmod{10}, \\ n \equiv 4 \pmod{10} & \Rightarrow & n^2 \equiv 6 \pmod{10}, \\ n \equiv 5 \pmod{10} & \Rightarrow & n^2 \equiv 5 \pmod{10}, \\ n \equiv 6 \pmod{10} & \Rightarrow & n^2 \equiv 6 \pmod{10}, \\ n \equiv 7 \pmod{10} & \Rightarrow & n^2 \equiv 9 \pmod{10}, \\ n \equiv 8 \pmod{10} & \Rightarrow & n^2 \equiv 4 \pmod{10}, \\ n \equiv 9 \pmod{10} & \Rightarrow & n^2 \equiv 1 \pmod{10}. \end{array}$$

We see in each case that n^2 can only have 0, 1, 4, 5, 6, or 9 as its last digit. \square

4.2.13 Problem 13

What can the last digit of a fourth power be?

Solution. We simply raise each least residue (mod 10) to the fourth power, similar to what we did in the previous problem. Modulo 10, we have $0^4 = 0$, $1^4 = 1$, $2^4 = 16 \equiv 6$, $3^4 = 81 \equiv 1$, and so on. After going through all the digits, we can see that the only possibilities for the last digit of a fourth power are 0, 1, 5, or 6. \square

4.2.14 Problem 14

Show that the difference of two consecutive cubes is never divisible by 3.

Proof. Let n be an integer. We have

$$\begin{aligned}(n+1)^3 - n^3 &= n^3 + 3n^2 + 3n + 1 - n^3 \\ &= 3n^2 + 3n + 1 \\ &\equiv 1 \pmod{3}.\end{aligned}$$

Since $(n+1)^3 - n^3$ always has a remainder of 1 when divided by 3, it cannot be divisible by 3. \square

4.2.15 Problem 15

Show that the difference of two consecutive cubes is never divisible by 5.

Proof. Let n be an integer. As in the previous problem,

$$(n+1)^3 - n^3 = 3n^2 + 3n + 1.$$

We find that

$$\begin{aligned}3(0)^2 + 3(0) + 1 &= 1 \equiv 1 \pmod{5}, \\ 3(1)^2 + 3(1) + 1 &= 7 \equiv 2 \pmod{5}, \\ 3(2)^2 + 3(2) + 1 &= 19 \equiv 4 \pmod{5}, \\ 3(3)^2 + 3(3) + 1 &= 37 \equiv 2 \pmod{5},\end{aligned}$$

and

$$3(4)^2 + 3(4) + 1 = 61 \equiv 1 \pmod{5}.$$

So, if n is congruent (mod 5) to 0, 1, 2, 3, or 4, then $(n+1)^3 - n^3$ is not divisible by 5. But n must be congruent to one of these, so we have checked every case. \square

4.2.16 Problem 16

Show that

$$\begin{aligned} d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0 \\ \equiv d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k \pmod{11} \end{aligned} \quad (4.1)$$

and deduce a test for divisibility by 11.

Solution. Since $10 \equiv -1 \pmod{11}$, it follows that $10^n \equiv 1 \pmod{11}$ when n is even and $10^n \equiv -1 \pmod{11}$ when n is odd. So any positive integer is congruent $\pmod{11}$ to the sum of its digits but with alternating signs. Therefore (4.1) holds.

To test for divisibility by 11, simply find the sum of every other digit, and subtract the sum of the remaining digits. Then this difference is divisible by 11 if and only if the original number is as well.

For example, 37,536,760,679 is divisible by 11 since

$$3 + 5 + 6 + 6 + 6 + 9 = 35,$$

$$7 + 3 + 7 + 0 + 7 = 24,$$

and $35 - 24 = 11$ is divisible by 11. □

4.2.17 Problem 17

A says, “27,182,818,284,590,452 is divisible by 11.” B says, “No, it isn’t.” Who is right?

Solution. We may simply use the divisibility rule found in the previous problem. The cross-digit sums are

$$2 + 1 + 2 + 1 + 2 + 4 + 9 + 4 + 2 = 27$$

and

$$7 + 8 + 8 + 8 + 8 + 5 + 0 + 5 = 49.$$

Since $49 - 27 = 22$ and $11 \mid 22$, we see that the original number is divisible by 11. Therefore A’s assertion is correct. □

4.2.18 Problem 18

A *palindrome* is a number that reads the same backward as forward. Examples are 22, 1331, and 935686539.

- (a) Prove that every four-digit palindrome is divisible by 11.

Proof. Let n be a four-digit palindrome having decimal representation $abba$, where a and b represent digits. By the divisibility test established in Problem 4.2.16, n must be congruent to $a - b + b - a = 0 \pmod{11}$. Therefore $11 \mid n$. □

- (b) What about six-digit palindromes?

Solution. The previous proof is easily adapted to this case. In fact, any palindrome with an even number of digits will be divisible by 11. □

4.2.19 Problem 19

Show that if $n \equiv 4 \pmod{9}$, then n cannot be written as the sum of three cubes.

Proof. By cubing each integer from 0 to 8, we see that the only possible least residues for cubes are 0, 1, or 8. Suppose we can select three numbers from 0, 1, and 8 such that their sum is congruent to 4 (mod 9). $1 + 1 + 1$ is too small, so at least one of the numbers has to be 8. We check the possibilities:

$$\begin{aligned} 0 + 1 + 8 &= 9 \equiv 0 \pmod{9}, \\ 1 + 1 + 8 &= 10 \equiv 1 \pmod{9}, \\ 0 + 8 + 8 &= 16 \equiv 7 \pmod{9}, \\ 1 + 8 + 8 &= 17 \equiv 8 \pmod{9}, \\ 8 + 8 + 8 &= 24 \equiv 6 \pmod{9}. \end{aligned}$$

So, there is no such sum congruent to 4. This shows that n cannot be written as the sum of three cubes. \square

4.2.20 Problem 20

Show that for $k > 0$ and $m \geq 1$, $x \equiv 1 \pmod{m^k}$ implies $x^m \equiv 1 \pmod{m^{k+1}}$.

Proof. Note that for each $m \geq 1$,

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + x + 1). \quad (4.2)$$

Also note that, since $m^k \mid (x - 1)$, we also have $m \mid (x - 1)$ so that

$$x^{m-1} + x^{m-2} + \cdots + x + 1 \equiv \overbrace{1 + 1 + \cdots + 1 + 1}^{m \text{ terms}} \equiv m \equiv 0 \pmod{m}.$$

Therefore $m \mid (x^{m-1} + x^{m-2} + \cdots + x + 1)$ and we can write

$$x^{m-1} + x^{m-2} + \cdots + x + 1 = ms$$

for some integer s . And $m^k \mid (x - 1)$ so $x - 1 = m^k t$ for an integer t . By (4.2), we therefore have

$$x^m - 1 = (m^k t)(ms) = m^{k+1} st.$$

Hence $m^{k+1} \mid (x^m - 1)$ as required to complete the proof. \square