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

Greg Kikola

March 19, 2020

This document lives at:

https://www.gregkikola.com/guides/

You can find the LaTeX source code on GitHub at:

https://github.com/gkikola/sol-dudley

Preface

I have written this unofficial solution guide to serve as a companion to the book *Number Theory*, Second Edition, by Underwood Dudley. This manual is intended as an aid for students who are studying number theory using Dudley's text. I strongly encourage students using this guide to first attempt each problem for themselves. If no progress is made after struggling with the problem for a time, or if the student does find a solution and wants to check their work, then this guide may be helpful.

In writing these solutions, I have avoided using any techniques or results before the point at which they are introduced in the text. My solutions should therefore be accessible to students who have read the text up to the appropriate chapter.

This solution manual is lengthy and contains solutions to many problems, so errors are inevitable. If you find an error or have a suggestion, please feel free to email me at gkikola@gmail.com. I appreciate any corrections or feedback.

Please know that this guide is currently unfinished. I am slowly working on adding the remaining chapters, but this will be done at my own pace. If you would like to find a solution to a problem that I have not included, try typing the problem into a web search engine such as Google; it is quite likely that someone somewhere has already solved the problem and published it on the Internet.

I am grateful to Underwood Dudley for authoring such a lovely and concise reference. I also give my thanks to those readers who have taken the time to inform me of errors in my solutions.

Greg Kikola
www.gregkikola.com
gkikola@gmail.com

Contents

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 $k \mid 0$. □

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 $a \mid c$. □

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 $d \mid ca$. □

1.1.4 Exercise 4

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

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

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. □

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. □

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. □

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. □

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 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

$$25, 45, 65, 81, 85.$$ □

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

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

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

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

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

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

and

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

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. □

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. □

(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. □

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. □

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. □

2.2.11 Problem 11

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

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

(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. □

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. □

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. □

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. □

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 $(15, -1)$. □

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 $2 \mid 90$, it follows by Lemma 2 that this equation has at least one solution. □

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

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

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

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

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. □

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 $(6, 1)$. □

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

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

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. □

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 $(3, 1)$, $(7, 4)$, $(11, 7)$, $\ldots$.

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 $(6, 1)$. □

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 $(3, 2)$ which leads to the general solution $(3 + 15t, 2 - 7t)$. However, $t = 0$ is the only value which makes both x and y positive, so $(3, 2)$ is the only valid solution. □

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. □

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. □

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. □

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. □

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 $10 \mid (15-5)$ so $3+5+7 \equiv 5 \pmod{10}$.

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

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

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 $a \equiv b \pmod{m}$. □

4.1.3 Exercise 3

To what least residue (mod 11) is each of 23, 29, 31, 37, and 41 congruent?

Solution. We have

$$\begin{aligned} 23 &\equiv 1 \pmod{11}, \\ 29 &\equiv 7 \pmod{11}, \\ 31 &\equiv 9 \pmod{11}, \\ 37 &\equiv 4 \pmod{11}, \end{aligned}$$

and

$$41 \equiv 8 \pmod{11}.$$ □

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 $n \equiv 1 \pmod 2$, if and only if $n = 2k+1$ for some integer k, if and only if n has remainder 1 when divided by 2. □

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 $p \mid (a - 0)$. □

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 $a \equiv a \pmod m$. □

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 $b \equiv a \pmod m$. □

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 $m \mid (a - c)$. □

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 $a + c \equiv b + d \pmod m$. □

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 $2 \not\equiv 4 \pmod{10}$. □

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 $x \equiv 2 \pmod{7}$. □

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

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

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

$$x \equiv 2 \pmod{3}.$$ □

4.2 Problems

4.2.1 Problem 1

Find the least residue of 1492 (mod 4), (mod 10), and (mod 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 $1492 \equiv 78 \pmod{101}$. □

4.2.2 Problem 2

Find the least residue of 1789 (mod 4), (mod 10), and (mod 101).

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

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. □

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 $2 \not\equiv -4 \equiv 8 \pmod{12}$. □

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. □

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. □

4.2.7 Problem 7

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

Solution. From Lemma 1, we have

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

4.2.8 Problem 8

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

4.2.9 Problem 9

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

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. □

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. □

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:

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

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

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. □

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. □

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. □

4.2.16 Problem 16

Show that

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

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 (mod 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:

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

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

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 $m \geq 1$,

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

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 $m \mid (x^{m-1} + x^{m-2} + \cdots + 1)$ 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. □

Chapter 5

Linear Congruences

5.1 Exercises

5.1.1 Exercise 1

Construct congruences modulo 12 with no solutions, just one solution, and more than one solution.

Solution. The congruence $3x \equiv 4 \pmod{12}$ has no solution since $3x$ is always congruent to 0, 3, 6, or 9 (mod 12) and never 4. The congruence $5x \equiv 2 \pmod{12}$ has one solution, $x = 10$. The congruence $2x \equiv 4 \pmod{12}$ has two solutions, $x = 2$ and $x = 8$. □

5.1.2 Exercise 2

Which congruences have no solutions?

(a) $3x \equiv 1 \pmod{10}$,

(b) $4x \equiv 1 \pmod{10}$,

(c) $5x \equiv 1 \pmod{10}$,

(d) $6x \equiv 1 \pmod{10}$,

(e) $7x \equiv 1 \pmod{10}$.

Solution. Since $3 \cdot 7 = 21 \equiv 1 \pmod{10}$, both of the congruences $3x \equiv 1$ and $7x \equiv 1 \pmod{10}$ have a solution.

The other three congruences do not have solutions. □

5.1.3 Exercise 3

After Exercise 5.1.2, can you guess a criterion for telling when a congruence has no solutions?

Solution. A necessary and sufficient condition that a congruence

$$ax \equiv b \pmod{m}$$

has no solutions is that (a, m) does not divide b. This will be proven in the text. □

5.1.4 Exercise 4

Solve

(a) $8x \equiv 1 \pmod{15}$

Solution. Since $(8, 15) = 1$, there is only one solution (by Lemma 2). We have $8x \equiv 16 \pmod{15}$ so that $x \equiv 2 \pmod{15}$. □

(b) $9x + 10y = 11$

Solution. From the equation we get the congruence $9x \equiv 11 \pmod{10}$. Since $11 \equiv 81 \pmod{10}$, we have $9x \equiv 81 \pmod{10}$ from which we get $x \equiv 9 \pmod{10}$. This is the only solution to the congruence. Thus

$$x = 9 + 10t$$

gives all possible values for x. Substituting this back into the equation, we get

$$9(9 + 10t) + 10y = 11,$$

which gives

$$y = -7 - 9t.$$

So the general solution is $x = 9 + 10t$ and $y = -7 - 9t$. □

5.1.5 Exercise 5

Determine the number of solutions of each of the following congruences:

$$3x \equiv 6 \pmod{15}, \qquad 4x \equiv 8 \pmod{15}, \qquad 5x \equiv 10 \pmod{15},$$
$$6x \equiv 11 \pmod{15}, \qquad 7x \equiv 14 \pmod{15}.$$

Solution. We will use Lemma 3.
$(3, 15) = 3$ and $3 \mid 6$, so $3x \equiv 6 \pmod{15}$ has 3 solutions.
$(4, 15) = 1$, so $4x \equiv 8 \pmod{15}$ has only one solution.
$(5, 15) = 5$ and $5 \mid 10$, so $5x \equiv 10 \pmod{15}$ has 5 solutions.
$(6, 15) = 3$ but $3 \nmid 11$ so the congruence $6x \equiv 11 \pmod{15}$ has no solutions.
Finally, since $(7, 15) = 1$, the congruence $7x \equiv 14 \pmod{15}$ has one solution.
□

5.1.6 Exercise 6

Find all of the solutions of $5x \equiv 10 \pmod{15}$.

Solution. Since $(5, 10) = 5$, we may divide by 5 to get $x \equiv 2 \pmod{3}$. So the solutions modulo 15 are 2, 5, 8, 11, and 14. □

5.1.7 Exercise 7

Solve the rest of the congruences in Exercise 5.1.5.

Solution. From $3x \equiv 6 \pmod{15}$ we get $x \equiv 2 \pmod{5}$, so that the three solutions modulo 15 are 2, 7, and 12.

For $4x \equiv 8 \pmod{15}$ we get the unique solution $x = 2$.

As we saw before, $6x \equiv 11 \pmod{15}$ has no solutions since $(6, 15) \nmid 11$.

Lastly, for $7x \equiv 14 \pmod{15}$ we have the unique solution $x = 2$. □

5.1.8 Exercise 8

Verify that 52 satisfies each of the three congruences, $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, and $x \equiv 3 \pmod{7}$.

Solution. Since

$$52 = 17 \cdot 3 + 1 = 10 \cdot 5 + 2 = 7 \cdot 7 + 3,$$

we see that each congruence is satisfied. □

5.2 Problems

5.2.1 Problem 1

Solve each of the following:

$$2x \equiv 1 \pmod{17}. \qquad 3x \equiv 1 \pmod{17}.$$
$$3x \equiv 6 \pmod{18}. \qquad 40x \equiv 777 \pmod{1777}.$$

Solution. For the first congruence, we have $2x \equiv 1 \equiv 18 \pmod{17}$ so $x \equiv 9 \pmod{17}$. This is the only solution, since $(2, 17) = 1$.

For the second, we have $3x \equiv 1 \equiv 18 \pmod{17}$ so $x \equiv 6 \pmod{17}$ and again, this solution is unique.

For the third congruence, we may divide by the greatest common divisor to get $x \equiv 2 \pmod{6}$. So the 3 solutions modulo 18 are 2, 8, and 14.

Lastly, $(40, 1777) = 1$ so we do have a unique solution. Since

$$40x \equiv 777 \equiv -1000 \pmod{1777},$$

we may divide by 40 to get

$$x \equiv -25 \pmod{1777}.$$

Therefore $x = 1752$ is the only least residue satisfying the congruence. □

5.2.2 Problem 2

Solve each of the following:

$$2x \equiv 1 \pmod{19}. \qquad 3x \equiv 1 \pmod{19}.$$
$$4x \equiv 6 \pmod{18}. \qquad 20x \equiv 984 \pmod{1984}.$$

Solution. For the first congruence, we have $2x \equiv 1 \equiv 20 \pmod{19}$ so that $x \equiv 10 \pmod{19}$, and this is the only solution.

For the second, we have $3x \equiv 1 \equiv 39 \pmod{19}$ so $x \equiv 13 \pmod{19}$, and this is again the only solution.

For the third, we get $2x \equiv 3 \equiv 12 \pmod 9$ so that $x \equiv 6 \pmod 9$. The two solutions (mod 18) are then 6 and 15.

Finally, for the last congruence, we may divide by 4 to get $5x \equiv 246 \pmod{496}$. So $5x \equiv -250 \pmod{496}$ and we get $x \equiv -50 \pmod{496}$. The four solutions modulo 1984 are then $x = 446$, 942, 1438, and 1934. □

5.2.3 Problem 3

Solve the systems

(a) $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$.

Solution. If $x \equiv 1 \pmod 2$, then

$$x = 1 + 2k_1 \quad \text{for some integer } k_1.$$

So if $x \equiv 1 \pmod 3$ then $1 + 2k_1 \equiv 1 \pmod 3$ or $k_1 \equiv 0 \pmod 3$. So $k_1 = 3k_2$ for some k_2. Therefore

$$x = 1 + 6k_2, \quad \text{or} \quad x \equiv 1 \pmod 6.$$

By the Chinese Remainder Theorem, this is the only solution modulo 6. □

(b) $x \equiv 3 \pmod 5$, $x \equiv 5 \pmod 7$, $x \equiv 7 \pmod{11}$.

Solution. From the first congruence we get

$$x = 3 + 5k_1.$$

So by the second congruence we have $3 + 5k_1 \equiv 5 \pmod 7$ and solving this gives $k_1 \equiv 6 \pmod 7$, so that

$$x = 3 + 5(6 + 7k_2) = 33 + 35k_2.$$

Finally, using the last congruence we get $33 + 35k_2 \equiv 7 \pmod{11}$ or $2k_2 \equiv 7 \pmod{11}$. Solving this gives $k_2 \equiv 9 \pmod{11}$, so we get

$$x = 33 + 35(9 + 11k_3) = 348 + 385k_3.$$

So, $x \equiv 348 \pmod{385}$ and this solution is unique modulo 385. □

(c) $2x \equiv 1 \pmod 5$, $3x \equiv 2 \pmod 7$, $4x \equiv 3 \pmod{11}$.

Solution. The first congruence gives $x = 3+5k_1$ for some k_1. Substituting this into the second congruence gives $k_1 = 7k_2$, so that $x = 3+35k_2$. Using the third congruence, we get $k_2 = 3 + 11k_3$. So

$$x = 108 + 385k_3.$$

Therefore $x \equiv 108 \pmod{385}$. □

5.2.4 Problem 4

Solve the systems

(a) $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$.

Solution. By inspection, we see that $x \equiv 5 \pmod{6}$ is a solution, and by the Chinese Remainder Theorem this is the only solution. □

(b) $x \equiv 2 \pmod{5}$, $2x \equiv 3 \pmod{7}$, $3x \equiv 4 \pmod{11}$.

Solution. Using the same technique as in the previous problem, we find that $x \equiv 82 \pmod{385}$. □

(c) $x \equiv 31 \pmod{41}$, $x \equiv 59 \pmod{26}$.

Solution. Again, using the same familiar method as before we get $x \equiv 605 \pmod{1066}$. □

5.2.5 Problem 5

What possibilities are there for the number of solutions of a linear congruence (mod 20)?

Solution. By Theorem 1, the congruence $ax \equiv b \pmod{20}$ has $(20, a)$ solutions, provided that $(20, a) \mid b$. So every divisor of 20, along with 0, is a possibility for the number of solutions: 0, 1, 2, 4, 5, 10, and 20. □

5.2.6 Problem 6

Construct linear congruences modulo 20 with no solutions, just one solution, and more than one solution. Can you find one with 20 solutions?

Solution. The linear congruence $2x \equiv 3 \pmod{20}$ has no solutions since $(2, 20) \nmid 3$. The congruence $3x \equiv 1 \pmod{20}$ has exactly one solution, $x = 7$. The congruence $2x \equiv 8 \pmod{20}$ has more than one solution: $x = 4$ and $x = 14$.

The linear congruence $0x \equiv 0 \pmod{20}$ has 20 solutions. □

5.2.7 Problem 7

Solve $9x \equiv 4 \pmod{1453}$.

Solution. We have $9x \equiv 4 \equiv -1449 \pmod{1453}$ and dividing by 9 gives

$$x \equiv -161 \equiv 1292 \pmod{1453}.$$

This solution is unique, modulo 1453. □

5.2.8 Problem 8

Solve $4x \equiv 9 \pmod{1453}$.

Solution. Since $4x \equiv 9 \equiv -1444 \pmod{1453}$, dividing by 4 gives

$$x \equiv -361 \equiv 1092 \pmod{1453}.$$

This is the only solution. □

5.2.9 Problem 9

Solve for x and y:

(a) $x + 2y \equiv 3 \pmod 7$, $3x + y \equiv 2 \pmod 7$.

Solution. The first congruence gives $x \equiv 3 + 5y \pmod 7$. Substituting into the second congruence, we get

$$3(3 + 5y) + y \equiv 2 \pmod 7,$$

and simplifying gives

$$y \equiv 0 \pmod 7.$$

Therefore the solution to the system is

$$x \equiv 3 \quad \text{and} \quad y \equiv 0 \pmod 7.$$ □

(b) $x + 2y \equiv 3 \pmod 6$, $3x + y \equiv 2 \pmod 6$.

Solution. Solving for x in the first congruence gives $x \equiv 3 + 4y \pmod 6$. Substituting into the second gives

$$3(3 + 4y) + y \equiv 2 \pmod 6,$$

so

$$y \equiv 5 \pmod 6.$$

Therefore

$$x \equiv 5 \quad \text{and} \quad y \equiv 5 \pmod 6.$$ □

5.2.10 Problem 10

Solve for x and y:

(a) $x + 2y \equiv 3 \pmod 9$, $3x + y \equiv 2 \pmod 9$.

Solution. Using the same method as in the previous problem, we get

$$x \equiv 2 \pmod 9 \quad \text{and} \quad y \equiv 5 \pmod 9.$$ □

(b) $x + 2y \equiv 3 \pmod{10}$, $3x + y \equiv 2 \pmod{10}$.

Solution. The first congruence gives $x \equiv 3+8y \pmod{10}$ and substituting into the second produces

$$3(3 + 8y) + y \equiv 2 \pmod{10}$$

which simplifies to

$$5y \equiv 3 \pmod{10}.$$

Since $(5, 10) = 5$ and $5 \nmid 3$, this congruence has no solutions. Therefore the original system of congruences has no solutions. □

5.2.11 Problem 11

When the marchers in the annual Mathematics Department Parade lined up 4 abreast, there was 1 odd person; when they tried 5 in a line, there were 2 left over; and when 7 abreast, there were 3 left over. How large is the Department?

Solution. If x is the size of the department, then we have the following system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod{4}, \\ x &\equiv 2 \pmod{5}, \\ x &\equiv 3 \pmod{7}. \end{aligned}$$

From the first congruence we have $x = 1 + 4k_1$ for some k_1. Then $1 + 4k_1 \equiv 2 \pmod{5}$ which gives $k_1 \equiv 4 \pmod{5}$ or $k_1 = 4 + 5k_2$. Then

$$x = 1 + 4(4 + 5k_2) = 17 + 20k_2.$$

Then $17 + 20k_2 \equiv 3 \pmod{7}$, or $k_2 \equiv 0 \pmod{7}$. Therefore $k_2 = 7k_3$ and we have $x = 17 + 140k_3$. So the general solution is

$$x \equiv 17 \pmod{140}.$$

So the Department could consist of 17 people, or 157 people, or 297 people, or in general, $17 + 140t$ people for some integer $t \geq 0$. □

5.2.12 Problem 12

Find a multiple of 7 that leaves the remainder 1 when divided by 2, 3, 4, 5, or 6.

Solution. We want to find x so that

$$\begin{aligned} x &\equiv 1 \pmod{2}, \\ x &\equiv 1 \pmod{3}, \\ x &\equiv 1 \pmod{4}, \\ x &\equiv 1 \pmod{5}, \\ x &\equiv 1 \pmod{6}, \\ x &\equiv 0 \pmod{7}. \end{aligned}$$

The moduli are not relatively prime, however some of these congruences are redundant. For example, $x \equiv 1 \pmod{2}$ and $x \equiv 1 \pmod{3}$ together imply that $x \equiv 1 \pmod{6}$. And $x \equiv 1 \pmod{4}$ implies $x \equiv 1 \pmod{2}$. So the system reduces to

$$\begin{aligned} x &\equiv 1 \pmod{3}, \\ x &\equiv 1 \pmod{4}, \\ x &\equiv 1 \pmod{5}, \\ x &\equiv 0 \pmod{7}. \end{aligned}$$

Solving this, we find

$$x \equiv 301 \pmod{420},$$

and, by the Chinese Remainder Theorem, this gives all solutions. Therefore any number of the form $x = 301 + 420t$ where t is an integer meets the requirements. □

5.2.13 Problem 13

Find the smallest odd n, $n > 3$, such that $3 \mid n$, $5 \mid n+2$, and $7 \mid n+4$.

Solution. We want $n \equiv 0 \pmod 3$, $n \equiv -2 \pmod 5$, and $n \equiv -4 \pmod 7$. Solving this gives

$$n \equiv 3 \pmod{105}.$$

So the smallest such odd integer, bigger than 3, is $3 + 2 \cdot 105 = 213$. □

5.2.14 Problem 14

Find the smallest integer n, $n > 2$, such that $2 \mid n$, $3 \mid n+1$, $4 \mid n+2$, $5 \mid n+3$, and $6 \mid n+4$.

Solution. We have the following system of linear congruences:

$$\begin{aligned} n &\equiv 0 \pmod 2, \\ n &\equiv -1 \equiv 2 \pmod 3, \\ n &\equiv -2 \equiv 2 \pmod 4, \\ n &\equiv -3 \equiv 2 \pmod 5, \\ n &\equiv -4 \equiv 2 \pmod 6. \end{aligned}$$

The first and last congruence are redundant, since they are implied by the remaining congruences. So we need to solve

$$\begin{aligned} n &\equiv 2 \pmod 3, \\ n &\equiv 2 \pmod 4, \\ n &\equiv 2 \pmod 5. \end{aligned}$$

Applying the Chinese Remainder Theorem, we find

$$n \equiv 2 \pmod{60}.$$

The smallest integer $n > 2$ that works is 62. □

5.2.15 Problem 15

Find a positive integer such that half of it is a square, a third of it is a cube, and a fifth of it is a fifth power.

Solution. Call the integer x. We know that $2 \mid x$, $3 \mid x$, and $5 \mid x$. So we could try an integer of the form $x = 2^i 3^j 5^k$, for some positive integers i, j, and k. Since $x/2$ is a square, we must have $i \equiv 1 \pmod 2$. Since $x/3$ is a cube, $i \equiv 0$

(mod 3). And since $x/5$ is a fifth power, we have $i \equiv 0 \pmod 5$. Taking these three congruences together, we find that $i \equiv 15 \pmod{30}$.

Similarly, for j we must have $j \equiv 0 \pmod 2$, $j \equiv 1 \pmod 3$, and $j \equiv 0 \pmod 5$. This system of congruences admits the solution $j \equiv 10 \pmod{30}$.

Finally, for k we have $k \equiv 0 \pmod 2$, $k \equiv 0 \pmod 3$, and $k \equiv 1 \pmod 5$, which gives $k \equiv 6 \pmod{30}$.

So, one possible value for x is

$$2^{15}3^{10}5^6 = 30{,}233{,}088{,}000{,}000.$$

This is in fact the smallest such number. □

5.2.16 Problem 16

The three consecutive integers 48, 49, and 50 each have a square factor.

(a) Find n such that $3^2 \mid n$, $4^2 \mid n+1$, and $5^2 \mid n+2$.

Solution. We want

$$\begin{aligned} n &\equiv 0 \pmod 9, \\ n &\equiv -1 \equiv 15 \pmod{16}, \\ n &\equiv -2 \equiv 23 \pmod{25}. \end{aligned}$$

Applying the Chinese Remainder Theorem, we find

$$n \equiv 2223 \pmod{3600}.$$ □

(b) Can you find n such that $2^2 \mid n$, $3^2 \mid n+1$, and $4^2 \mid n+2$?

Solution. No. Suppose $4 \mid n$ and $16 \mid n+2$. Then $n = 4k$ and $n+2 = 16\ell$ for some integers k and ℓ. Then

$$4k = 16\ell - 2$$

or

$$2 = 16\ell - 4k = 4(4\ell - k).$$

Therefore $4 \mid 2$, which is absurd. This contradiction shows that there is no such number n. □

5.2.17 Problem 17

If $x \equiv r \pmod m$ and $x \equiv s \pmod{m+1}$, show that

$$x \equiv r(m+1) - sm \pmod{m(m+1)}.$$

Proof. Since $x \equiv r \pmod m$ we have $x = r + km$ for some integer k, and multiplying by $m+1$ on both sides gives

$$x(m+1) = r(m+1) + km(m+1),$$

or

$$x = r(m+1) - xm + km(m+1) \tag{5.1}$$

And since $x \equiv s \pmod{m+1}$ we have $x = s + \ell(m+1)$ for some integer ℓ. Then

$$xm = sm + \ell m(m+1). \tag{5.2}$$

Now substituting (5.2) into (5.1) gives

$$x = r(m+1) - sm + (k-\ell)m(m+1).$$

Since $k-\ell$ is an integer, we have $x \equiv r(m+1) - sm \pmod{m(m+1)}$. □

5.2.18 Problem 18

What three positive integers, upon being multiplied by 3, 5, and 7 respectively and the products divided by 20, have remainders in arithmetic progression with common difference 1 and quotients equal to remainders?

Solution. Let the three positive integers be x, y, and z. Then there is an integer r such that

$$\begin{aligned} 3x &= 20r + r = 21r, \\ 5y &= 20(r+1) + (r+1) = 21(r+1), \\ 7z &= 20(r+2) + (r+2) = 21(r+2), \end{aligned}$$

where $0 \le r < 18$ (since each remainder must be less than 20). Then $x = 7r$, $z = 3(r+2)$, and we know that $5 \mid (r+1)$. So the only possible values for r are 4, 9, or 14. Therefore, we have three sets of solutions:

$$\begin{aligned} &x = 28, \quad y = 21, \quad \text{and} \quad z = 18; \\ &x = 63, \quad y = 42, \quad \text{and} \quad z = 33; \\ &x = 98, \quad y = 63, \quad \text{and} \quad z = 48. \end{aligned}$$

□

5.2.19 Problem 19

Suppose that the moduli in the system

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, k$$

are not relatively prime in pairs. Find a condition that the a_i must satisfy in order that the system have a solution.

Solution. Assume that the system has a solution. Fix i and j with $i \neq j$ and let $d = (m_i, m_j)$. Since $x \equiv a_i \pmod{m_i}$, we have

$$x = a_i + sm_i, \quad \text{for some integer } s, \tag{5.3}$$

and since $x \equiv a_j \pmod{m_j}$, we get

$$x = a_j + tm_j, \quad \text{for some integer } t. \tag{5.4}$$

Combining (5.3) and (5.4) then gives

$$a_i - a_j = tm_j - sm_i.$$

Since d divides the right-hand side of this equation, we also know that d divides $a_i - a_j$. Therefore, the following condition is necessary for the system to have a solution:

$$(m_i, m_j) \mid a_i - a_j \quad \text{for each } i \text{ and } j \text{ with } i \neq j.$$

In fact this condition is also sufficient, but we omit the proof. □

5.2.20 Problem 20

How many multiples of b are there in the sequence

$$a, 2a, 3a, \ldots, ba?$$

Solution. This question is equivalent to asking how many solutions there are to the congruence $ax \equiv 0 \pmod{b}$. Therefore, by Theorem 1, there are exactly (a, b) multiples of b. Note that every integer divides 0 so there is always at least one such multiple, namely ba. □

Chapter 6

Fermat's and Wilson's Theorems

6.1 Exercises

6.1.1 Exercise 1

Verify that Fermat's Theorem is true for $a = 2$ and $p = 5$.

Solution. We have $a^{p-1} = 2^4 = 16 \equiv 1 \pmod{5}$, so the theorem holds. □

6.1.2 Exercise 2

Calculate 2^2 and $20^{10} \pmod{11}$.

Solution. $2^2 \equiv 4 \pmod{11}$. To find 20^{10}, we note that $20^2 = 400 \equiv 4 \pmod{11}$. Squaring gives $20^4 \equiv 16 \equiv 5 \pmod{11}$. Squaring again gives $20^8 \equiv 25 \equiv 3 \pmod{11}$. So

$$20^{10} = 20^8 \cdot 20^2 \equiv 3 \cdot 4 \equiv 1 \pmod{11}.$$

Of course, this result is also guaranteed by Fermat's Theorem. □

6.1.3 Exercise 3

In the proof of Wilson's Theorem, what are the pairs when $p = 11$?

Solution. To find the multiplicative inverse of 2, we look for the least residue satisfying the congruence $2x \equiv 1 \pmod{11}$. Since $1 \equiv 12 \pmod{11}$, we may divide by 2 to get $x \equiv 6 \pmod{11}$. Hence $(2, 6)$ is one such pair. In the same way we can find the remaining pairs. The complete list of pairs follows:

$$(2, 6), (3, 4), (5, 9), (7, 8).$$ □

6.2 Problems

6.2.1 Problem 1

What is the least residue of

$$5^6 \pmod 7 \qquad 5^8 \pmod 7 \qquad 1945^8 \pmod 7?$$

Solution. By Fermat's Theorem, $5^6 \equiv 1 \pmod 7$.

$5^8 = 5^6 \cdot 5^2 \equiv 1 \cdot 4 \equiv 4 \pmod 7$.

Again by Fermat, $1945^6 \equiv 1 \pmod 7$. Therefore

$$1945^8 \equiv 1945^2 = 5^2 \cdot 389^2 \equiv 4 \cdot 4^2 = 64 \equiv 1 \pmod 7. \qquad \square$$

6.2.2 Problem 2

What is the least residue of

$$5^{10} \pmod{11} \qquad 5^{12} \pmod{11} \qquad 1945^{12} \pmod{11}?$$

Solution. $5^{10} \equiv 1 \pmod{11}$ by Fermat's Theorem. So $5^{12} \equiv 5^2 \equiv 3 \pmod{11}$.

By Fermat, $1945^{10} \equiv 1 \pmod{11}$, so $1945^{12} \equiv 1945^2 \equiv 9^2 \equiv 4 \pmod{11}$. □

6.2.3 Problem 3

What is the last digit of 7^{355}?

Solution. We want the least residue of $7^{355} \pmod{10}$. Note that $7^2 = 49 \equiv 9 \pmod{10}$ and $7^4 \equiv 81 \equiv 1 \pmod{10}$. So we have

$$7^{355} = (7^4)^{88} \cdot 7^3 \equiv 7^3 \equiv 3 \pmod{10}.$$

Therefore the last digit of 7^{355} is 3. □

6.2.4 Problem 4

What are the last two digits of 7^{355}?

Solution. This is handled similarly to the previous problem, except now we are working modulo 100. $7^3 = 343 \equiv 43 \pmod{100}$, so $7^4 \equiv 301 \equiv 1 \pmod{100}$. We find

$$7^{355} = (7^4)^{88} \cdot 7^3 \equiv 7^3 \equiv 43 \pmod{100}.$$

The last two digits are therefore 4 and 3. □

6.2.5 Problem 5

What is the remainder when 314^{162} is divided by 163?

Solution. Since 314 is not a multiple of 163, which is prime, we may apply Fermat's Theorem to see that $314^{162} \equiv 1 \pmod{163}$. □

6.2.6 Problem 6

What is the remainder when 314^{162} is divided by 7?

Solution. As in the previous problem, since we know 314 is not a multiple of 7, we have by Fermat that $314^6 \equiv 1 \pmod 7$. Therefore

$$314^{162} = (314^6)^{27} \equiv 1 \pmod 7. \qquad \square$$

6.2.7 Problem 7

What is the remainder when 314^{164} is divided by 165?

Solution. Note that $165 = 3 \cdot 5 \cdot 11$. And, after some brief computation, we find

$$\begin{aligned} 314^{164} &\equiv 1 \pmod 3, \\ 314^{164} &\equiv 1 \pmod 5, \end{aligned}$$

and

$$314^{164} \equiv 9 \pmod{11}.$$

We may now use the Chinese Remainder Theorem to solve the system of congruences given by

$$x \equiv 1 \pmod{15} \qquad \text{and} \qquad x \equiv 9 \pmod{11}.$$

This system admits the unique solution $x \equiv 31 \pmod{165}$. Therefore 31 is the remainder we seek. □

6.2.8 Problem 8

What is the remainder when 2001^{2001} is divided by 26?

Solution. Since $2001 \equiv 25 \equiv -1 \pmod{26}$ we have

$$2001^{2001} \equiv (-1)^{2001} \equiv -1 \equiv 25 \pmod{26}.$$

Therefore the remainder is 25. □

6.2.9 Problem 9

Show that

$$(p-1)(p-2)\cdots(p-r) \equiv (-1)^r r! \pmod p,$$

for $r = 1, 2, \ldots, p-1$.

Proof. Fix an integer $p > 1$. We will prove the statement for all positive r using induction on r. When $r = 1$, we have $p - 1 \equiv -1 \pmod p$, and certainly $-1 = (-1)^1(1!)$, so the statement holds in the base case.

Now, suppose the statement holds for $r = k$ with $k \geq 1$. Then $p - k - 1 \equiv -(k+1) \pmod p$ and we have

$$(p-1)\cdots(p-k)(p-k-1) \equiv -(-1)^k k!(k+1) \equiv (-1)^{k+1}(k+1)! \pmod p.$$

Therefore the statement holds for $r = k + 1$, which completes the proof. □

6.2.10 Problem 10

(a) Calculate $(n-1)! \pmod{n}$ for $n = 10$, 12, 14, and 15.

Solution. Since 9! contains both a factor of 2 and a factor of 5, it follows that $9! \equiv 0 \pmod{10}$. For exactly the same reason, we get

$$\begin{aligned} 11! &\equiv 0 \pmod{12}, \\ 13! &\equiv 0 \pmod{14}, \end{aligned}$$

and

$$14! \equiv 0 \pmod{15}.$$ □

(b) Guess a theorem and prove it.

Solution. The above calculations suggest that $(n-1)! \equiv 0 \pmod{n}$ when n is composite, but we will have to exclude $n = 4$ since it would otherwise be a counterexample.

So, we will show that for all $n > 4$,

$$(n-1)! \equiv 0 \pmod{n} \quad \text{if and only if } n \text{ is composite.}$$

The left-to-right implication is a consequence of Wilson's Theorem, so we will only need to prove the right-to-left direction.

Assume that $n > 4$ and $n = ab$ where $1 < a < n$. There are two cases. First, if a and b are distinct, then $(n-1)!$ must contain both a and b as factors, so that $n \mid (n-1)!$. Therefore $(n-1)! \equiv 0 \pmod{n}$ in this case. The other possibility is that $a = b$, so that $n = a^2$. In this case, since $n > 4$, we know $a > 2$. Both a and $2a$ will occur as separate factors in the expansion of $(n-1)!$, so again we have $n \mid (n-1)!$. In either case, $(n-1)! \equiv 0 \pmod{n}$. □

6.2.11 Problem 11

Show that $2(p-3)! + 1 \equiv 0 \pmod{p}$.

Proof. We will suppose that p is an odd prime. By Wilson's Theorem, we know that $(p-1)! \equiv -1 \pmod{p}$. Therefore

$$(p-1)(p-2)(p-3)! + 1 \equiv 0 \pmod{p}.$$

But $(p-1)(p-2) \equiv (-1)(-2) \equiv 2 \pmod{p}$. This gives the desired result. □

6.2.12 Problem 12

In 1732 Euler wrote: "I derived [certain] results from the elegant theorem, of whose truth I am certain, although I have no proof: $a^n - b^n$ is divisible by the prime $n+1$ if neither a nor b is." Prove this theorem, using Fermat's Theorem.

Proof. If $n+1$ is prime, then Fermat's Theorem says that

$$a^n \equiv b^n \equiv 1 \pmod{n+1},$$

provided that neither a nor b is a multiple of $n+1$. Therefore $a^n - b^n \equiv 1 - 1 \equiv 0 \pmod{n+1}$, which is equivalent to the statement that $n+1$ divides $a^n - b^n$. □

6.2.13 Problem 13

Note that

$$\begin{aligned} 6! &\equiv -1 \pmod 7, \\ 5!1! &\equiv 1 \pmod 7, \\ 4!2! &\equiv -1 \pmod 7, \\ 3!3! &\equiv 1 \pmod 7. \end{aligned}$$

Try the same sort of calculation (mod 11).

Solution. Doing the calculations, we get

$$\begin{aligned} 10! &\equiv -1 \pmod{11}, \\ 9!1! &\equiv 1 \pmod{11}, \\ 8!2! &\equiv -1 \pmod{11}, \\ 7!3! &\equiv 1 \pmod{11}, \\ 6!4! &\equiv -1 \pmod{11}, \\ 5!5! &\equiv 1 \pmod{11}. \end{aligned}$$ □

6.2.14 Problem 14

Guess a theorem from the data of Problem 6.2.13, and prove it.

Solution. The calculations seem to suggest that, for any odd prime p,

$$(p-n)!(n-1)! \equiv (-1)^n \pmod p, \quad \text{for} \quad 1 \le n \le \frac{p+1}{2}.$$

For the proof, we use an inductive argument. The case where $n = 1$ is simply Wilson's Theorem. So assume it holds for $n = k$, where $1 \le k < (p+1)/2$. Then

$$(p-k)!(k-1)! \equiv (-1)^k \pmod p.$$

Rewriting the left-hand side, we get

$$(p-k)(p-k-1)!(k-1)! \equiv (-1)^k \pmod p.$$

Finally, since $p - k \equiv -k \pmod p$, we may multiply both sides by -1 to get

$$(p-k-1)!k! \equiv (-1)^{k+1} \pmod p.$$

This shows that the statement holds for all n with $n = 1, 2, \ldots, (p+1)/2$. □

6.2.15 Problem 15

Suppose that p is an odd prime.

(a) Show that

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p.$$

Proof. By Fermat's Theorem, we have

$$\begin{aligned} 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} &\equiv \overbrace{1 + 1 + \cdots + 1}^{p-1 \text{ terms}} \pmod{p} \\ &\equiv p - 1 \pmod{p} \\ &\equiv -1 \pmod{p}. \end{aligned}$$ □

(b) Show that

$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

Proof. Again, by Fermat we have $a^p \equiv a \pmod{p}$ for all a. So

$$\begin{aligned} 1^p + 2^p + \cdots + (p-1)^p &\equiv 1 + 2 + \cdots + (p-1) \pmod{p} \\ &\equiv \frac{p(p-1)}{2} \pmod{p}. \end{aligned}$$

But $(p-1)/2$ is an integer, so p divides the right-hand side. Hence

$$1^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$ □

6.2.16 Problem 16

Show that the converse of Fermat's Theorem is false.

Solution. We need to show that there exist integers a and n with $(a, n) = 1$ and $a^{n-1} \equiv 1 \pmod{n}$, such that n is composite. Consider $a = 2$ and $n = 341$. Note that $341 = 11 \cdot 31$, and $(2, 341) = 1$. Since $2^{10} = 1024 \equiv 1 \pmod{341}$, we have

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{341}.$$

This gives us a counterexample for the converse of Fermat's Theorem. □

6.2.17 Problem 17

Show that for any two different primes p, q,

(a) $pq \mid (a^{p+q} - a^{p+1} - a^{q+1} + a^2)$ for all a.

Solution. We have

$$\begin{aligned} a^{p+q} - a^{p+1} - a^{q+1} + a^2 &= a^p(a^q - a) - a(a^q - a) \\ &= (a^p - a)(a^q - a). \end{aligned}$$

By Fermat's Theorem, we know $p \mid (a^p - a)$ and $q \mid (a^q - a)$, so pq divides the product. □

(b) $pq \mid (a^{pq} - a^p - a^q + a)$ for all a.

Solution. By Fermat's Theorem, we know $a^p \equiv a \pmod{p}$. Therefore

$$\begin{aligned} a^{pq} - a^p - a^q + a &= (a^p)^q - a^p - a^q + a \\ &\equiv a^q - a - a^q + a \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

So $p \mid (a^{pq} - a^p - a^q + a)$. By the same argument, we also have that $q \mid (a^{pq} - a^p - a^q + a)$. Since p and q are distinct primes, we have $(p, q) = 1$ and we may apply Corollary 3 of Section 1 to establish the result. □

6.2.18 Problem 18

Show that if p is an odd prime, then $2p \mid (2^{2p-1} - 2)$.

Proof. Observe that

$$2^{2p-1} - 2 = 2(2^{2p-2} - 1) = 2(4^{p-1} - 1).$$

Since p is an odd prime, $(p, 4) = 1$ and we may apply Fermat's Theorem to see that $4^{p-1} \equiv 1 \pmod{p}$. This is enough to show that $2p \mid (2^{2p-1} - 2)$. □

6.2.19 Problem 19

For what n is it true that

$$p \mid (1 + n + n^2 + \cdots + n^{p-2})? \tag{6.1}$$

Solution. If $n \equiv 0$ or $n \equiv 1 \pmod{p}$ then (6.1) is certainly false. In every other case, this sum forms a geometric progression:

$$1 + n + n^2 + \cdots + n^{p-2} = \frac{n^{p-1} - 1}{n - 1}.$$

By Fermat's Theorem, we know that if $(n, p) = 1$ then p divides the numerator of this fraction. If we can show that p does not also divide the denominator, then it follows that p must divide the sum. But the only way $p \mid (n - 1)$ is if $n \equiv 1 \pmod{p}$.

Therefore the statement (6.1) is true for all integers n such that $n \not\equiv 0$ and $n \not\equiv 1 \pmod{p}$. □

6.2.20 Problem 20

Show that every odd prime except 5 divides some number of the form $111 \ldots 11$ (k digits, all ones).

Proof. Fix a prime $p > 5$ (the case where $p = 3$ is handled by observing that $3 \mid 111$). Then $(10, p) = 1$ so $10 \not\equiv 0 \pmod{p}$. And certainly $10 \not\equiv 1 \pmod{p}$ since, aside from $p = 7$, we are only considering primes larger than 10. Therefore, we may apply the result from Problem 6.2.19 to establish that

$$p \mid (1 + 10 + 10^2 + 10^3 + \cdots + 10^{p-2}).$$

This completes the proof. □

Chapter 7

The Divisors of an Integer

7.1 Exercises

7.1.1 Exercise 1

Verify that the table of values for $d(n)$ is correct as far as it goes, and complete it.

Solution. For small values of n, we can simply test divisibility by each positive integer up to $n/2$. The completed table follows.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$d(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5

□

7.1.2 Exercise 2

What is $d(p^3)$? Generalize to $d(p^n)$, $n = 4, 5, \ldots$.

Solution. For any prime p, the divisors of p^3 are 1, p, p^2, and p^3. These are the only divisors, so $d(p^3) = 4$.

In general, $d(p^n) = n + 1$. For, if p^n has a divisor a that is not of the form p^i for some nonnegative i, then this divisor a must contain some prime factor q distinct from p. But if $q \mid a$ then $q \mid p^n$. By Lemma 6 of Section 2, it follows that $q \mid p$ as well. Therefore p is a prime which contains a smaller prime as a factor, which is impossible. This contradiction shows that the only divisors of p^n have the form p^i, where $i = 0, 1, \ldots, n$. □

7.1.3 Exercise 3

What is $d(p^3 q)$? What is $d(p^n q)$ for any positive n?

Solution. $p^3 q$ has as its divisors 1, p, p^2, and p^3, and also q, pq, $p^2 q$, and $p^3 q$, for a total of 8 divisors.

In general, every divisor of p^n will be a divisor of $p^n q$, and for each such divisor, multiplying by q will produce a new divisor. So the factor of q effectively doubles the number of divisors. Consequently, we have

$$d(p^n q) = 2(n+1) = 2n+2. \qquad \square$$

7.1.4 Exercise 4

Calculate $d(240)$.

Solution. Using Theorem 1, we have

$$\begin{aligned} d(240) &= d(2^4 \cdot 3 \cdot 5) \\ &= d(2^4)d(3)d(5) \\ &= 5 \cdot 2 \cdot 2 \\ &= 20. \end{aligned} \qquad \square$$

7.1.5 Exercise 5

Verify the table of values for $\sigma(n)$ is correct as far as it goes, and complete it.

Solution. To compute $\sigma(n)$, we can list out the divisors of n and then add them up. For example, for $\sigma(9)$ we compute $1+3+9$ and get a value of 13. The completed table follows.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24

□

7.1.6 Exercise 6

What is $\sigma(p^3)$? $\sigma(pq)$, where p and q are different primes?

Solution. For p^3 we get

$$\sigma(p^3) = 1 + p + p^2 + p^3 = \frac{p^4 - 1}{p - 1}.$$

If p and q are distinct primes, then the divisors are 1, p, q, and pq. So

$$\sigma(pq) = 1 + p + q + pq = (1+p) + q(1+p) = (1+p)(1+q). \qquad \square$$

7.1.7 Exercise 7

Show that $\sigma(2^n) = 2^{n+1} - 1$.

Solution. The divisors of 2^n are 1, 2, 2^2, …, 2^n. The sum of these divisors forms a finite geometric series:

$$\sigma(2^n) = \sum_{k=0}^{n} 2^k = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1. \qquad \square$$

7.1.8 Exercise 8

What is $\sigma(p^n)$, $n = 1, 2, \ldots$?

Solution. Again, we have a geometric series:

$$\sigma(p^n) = \sum_{k=0}^{n} p^k = \frac{p^{n+1} - 1}{p - 1}. \qquad \square$$

7.1.9 Exercise 9

Calculate $\sigma(240)$.

Solution. From Theorem 2, we get

$$\begin{aligned} \sigma(240) &= \sigma(2^4 \cdot 3 \cdot 5) \\ &= \sigma(2^4)\sigma(3)\sigma(5) \\ &= (2^5 - 1) \cdot 4 \cdot 6 \\ &= 31 \cdot 24 \\ &= 744. \end{aligned} \qquad \square$$

7.1.10 Exercise 10

Let f be a multiplicative function defined by $f(p^e) = ep^{e-1}$, where p is prime and $e \geq 1$. Compute $f(n)$ for $n = 13, 14, \ldots, 24$.

Solution. We know that $f(n) = 1$ if n is any square-free integer (that is, if each prime in the factorization of n occurs only to the first power). Other values can be found using multiplicativity together with the defining formula $f(p^e) = ep^{e-1}$. The values are as follows.

n	13	14	15	16	17	18	19	20	21	22	23	24
$f(n)$	1	1	1	32	1	6	1	4	1	1	1	12

□

7.2 Problems

7.2.1 Problem 1

Calculate $d(42)$, $\sigma(42)$, $d(420)$, and $\sigma(420)$.

Solution. Since $42 = 2 \cdot 3 \cdot 7$, we have

$$d(42) = 2 \cdot 2 \cdot 2 = 8 \quad \text{and} \quad \sigma(42) = 3 \cdot 4 \cdot 8 = 96.$$

$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, so

$$d(420) = 3 \cdot 2 \cdot 2 \cdot 2 = 24 \quad \text{and} \quad \sigma(420) = 7 \cdot 4 \cdot 6 \cdot 8 = 1344. \qquad \square$$

7.2.2 Problem 2

Calculate $d(540)$, $\sigma(540)$, $d(5400)$, and $\sigma(5400)$.

Solution. $540 = 2^2 \cdot 3^3 \cdot 5$, so

$$d(540) = 3 \cdot 4 \cdot 2 = 24 \quad \text{and} \quad \sigma(540) = 7 \cdot 40 \cdot 6 = 1680.$$

$5400 = 2^3 \cdot 3^3 \cdot 5^2$, so we get

$$d(5400) = 4 \cdot 4 \cdot 3 = 48 \quad \text{and} \quad \sigma(5400) = 15 \cdot 40 \cdot 31 = 18600.$$ □

7.2.3 Problem 3

Calculate d and σ of $10115 = 5 \cdot 7 \cdot 17^2$ and $100115 = 5 \cdot 20023$.

Solution. We have

$$d(10115) = 2 \cdot 2 \cdot 3 = 12 \quad \text{and} \quad \sigma(10115) = 6 \cdot 8 \cdot 307 = 14736,$$

and

$$d(100115) = 2 \cdot 2 = 4 \quad \text{and} \quad \sigma(100115) = 6 \cdot 20024 = 120144.$$ □

7.2.4 Problem 4

Calculate d and σ of $10116 = 2^2 \cdot 3^2 \cdot 281$ and $100116 = 2^2 \cdot 3^5 \cdot 103$.

Solution. For 10116 we get

$$d(10116) = 3 \cdot 3 \cdot 2 = 18 \quad \text{and} \quad \sigma(10116) = 7 \cdot 13 \cdot 282 = 25662.$$

And for 100116, we have

$$d(100116) = 3 \cdot 6 \cdot 2 = 36$$

and

$$\begin{aligned} \sigma(100116) &= 7 \cdot \frac{3^6 - 1}{3 - 1} \cdot 104 \\ &= 7 \cdot 364 \cdot 104 \\ &= 264992. \end{aligned}$$ □

7.2.5 Problem 5

Show that $\sigma(n)$ is odd if n is a power of two.

Proof. This is immediate from Exercise 7.1.7. □

7.2.6 Problem 6

Prove that if $f(n)$ is multiplicative, then so is $f(n)/n$.

Proof. Let s and t be positive integers with $(s,t)=1$. Since f is multiplicative, we know $f(st)=f(s)f(t)$. Define the function g on the positive integers by

$$g(n)=\frac{f(n)}{n}.$$

Then

$$g(st)=\frac{f(st)}{st}=\frac{f(s)f(t)}{st}=\frac{f(s)}{s}\cdot\frac{f(t)}{t}=g(s)g(t),$$

so g is multiplicative as well. □

7.2.7 Problem 7

What is the smallest integer n such that $d(n)=8$? Such that $d(n)=10$?

Solution. If $d(n)=8$, then n has at most three distinct prime factors. If there are three distinct prime divisors, then the smallest value would be $n=2\cdot3\cdot5=30$. If there are exactly two distinct prime divisors, one would have to have an exponent of 3, making the smallest value $n=2^3\cdot3=24$. Lastly, if n has only a single prime factor, it would have to be raised to the 7th power, giving $n=2^7=128$. From these three possibilities, we see that

$$\text{the smallest } n \text{ such that } d(n)=8 \text{ is } 24.$$

For $d(n)=10$, the reasoning is similar. We either have two distinct prime factors, one raised to the first power and the other raised to the fourth power, or only one prime factor, raised to the 9th power. In the first case, the smallest such n would be $n=2^4\cdot3=48$, and in the second, $n=2^9=512$. Clearly 48 is the smaller of the two, so

$$\text{the smallest } n \text{ such that } d(n)=10 \text{ is } 48.$$ □

7.2.8 Problem 8

Does $d(n)=k$ have a solution n for each k?

Solution. Yes. One possible choice is $n=2^{k-1}$, though this is not necessarily the smallest such n. □

7.2.9 Problem 9

In 1644, Mersenne asked for a number with 60 divisors. Find one smaller than 10,000.

Solution. Our solution to the previous problem isn't quite helpful, since 2^{59} is considerably larger than 10000. But, by using more prime factors, each with smaller exponents, we are likely to make the product much smaller. So let us attempt to find a smaller n with $d(n)=60$.

The prime factorization of 60 is $2^2\cdot3\cdot5$. In order to get a factor of 5 in $d(n)$, we will need an exponent of at least 4. Likewise, to get a factor of 3, we will need an exponent of at least 2. The remaining factors of 2 can be obtained using exponents of 1. This suggests that we choose

$$n = 2^4 \cdot 3^2 \cdot 5 \cdot 7 = 5040,$$

so that

$$d(5040) = 5 \cdot 3 \cdot 2 \cdot 2 = 60.$$

Therefore 5040 fits our criteria. □

7.2.10 Problem 10

Find infinitely many n such that $d(n) = 60$.

Solution. Since there are infinitely many primes, we may simply choose $n = p^{59}$, where p is some prime.

More interesting choices for n can be found by considering more prime factors. For example, we can write $60 = 10 \cdot 3 \cdot 2$, suggesting the choice $n = p^9 q^2 r$ where p, q, and r are distinct primes. Different factorizations of 60 will lead to different choices of n, as will different choices of the primes. □

7.2.11 Problem 11

If p is an odd prime, for which k is $1 + p + \cdots + p^k$ odd?

Solution. Let p be an odd prime. Then $p \equiv 1 \pmod 2$, so

$$1 + p + p^2 + \cdots + p^k \equiv 1 + 1 + 1^2 + \cdots + 1^k \equiv k + 1 \pmod 2.$$

It follows that $1 + p + \cdots + p^k$ is odd if and only if k is even. □

7.2.12 Problem 12

For which n is $\sigma(n)$ odd?

Solution. Take any prime factor p dividing n. First suppose p is an odd prime. If e is the exponent of p in the prime-power decomposition of n ($e \geq 1$), then we know by the previous problem that $\sigma(p^e)$ is odd if and only if e is even. On the other hand, if $p = 2$ then $\sigma(2^e) = 2^{e+1} - 1$ is always odd. So the exponent on 2 makes no difference.

Since σ is multiplicative, we can therefore see that $\sigma(n)$ will be odd if and only if every odd prime factor of n occurs with an even exponent in the prime-power decomposition of n. In other words, if n can be written in the form

$$n = 2^k m^2, \quad \text{where } k \geq 0,\ m \geq 1, \text{ and } m \text{ is odd,}$$

then (and only then) will $\sigma(n)$ be odd. □

7.2.13 Problem 13

If n is a square, show that $d(n)$ is odd.

Proof. Let $n = k^2$ where k is a positive integer. If $k = p_1^{e_1} \cdots p_r^{e_r}$ is the prime-power decomposition of k, then

$$\begin{aligned} d(n) = d(k^2) &= d(p_1^{2e_1}) \cdots d(p_r^{2e_r}) \\ &= (2e_1 + 1) \cdots (2e_r + 1), \end{aligned}$$

and since each factor $2e_i + 1$ is odd, we see that $d(n)$ must be odd. □

7.2.14 Problem 14

If $d(n)$ is odd, show that n is a square.

Proof. If n is not a square, then some exponent e in its prime-power decomposition is odd. Then $e+1$ is even, and therefore $d(n)$ contains an even factor and is thus also even. By the contrapositive, this completes the proof. □

7.2.15 Problem 15

Observe that $1+1/3 = 4/3$; $1+1/2+1/4 = 7/4$; $1+1/5 = 6/5$; $1+1/2+1/3+1/6 = 12/6$; $1+1/7 = 8/7$; and $1+1/2+1/4+1/8 = 15/8$. Guess and prove a theorem.

Solution. Notice that each sum is over the reciprocals of all the divisors of a number n, and the resulting fraction has a numerator equal to $\sigma(n)$ (when left unreduced). This suggests that for each positive integer n,

$$\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}.$$

To prove this, fix a particular n. Let the positive divisors of n be $f_1, \ldots, f_k$, in order from least to greatest. Observe that for each i with $1 \le i \le k$, we have

$$f_i = \frac{n}{f_{k-i}}.$$

This shows that

$$\sum_{d|n} d = \sum_{d|n} \frac{n}{d}.$$

Using this fact, we have

$$\sum_{d|n} \frac{1}{d} = \frac{1}{n} \sum_{d|n} \frac{n}{d} = \frac{1}{n} \sum_{d|n} d = \frac{\sigma(n)}{n}.$$

This completes the proof. □

7.2.16 Problem 16

Find infinitely many n such that $\sigma(n) \leq \sigma(n-1)$.

Solution. Let n be any odd prime except 3. Then $n-1$ is even and must have at least three distinct factors, namely 1, 2, and $n-1$. So

$$\begin{aligned}\sigma(n) = 1 + n &= 2 + (n-1) \\ &< 1 + 2 + (n-1) \\ &\leq \sigma(n-1)\end{aligned}$$

as desired. □

7.2.17 Problem 17

If N is odd, how many solutions does $x^2 - y^2 = N$ have?

Solution. For any odd N, the equation has exactly $2d(N)$ distinct integer solutions, as we will now show.

Suppose (x, y) is a solution. Let $a = x + y$ and $b = x - y$ so that $N = ab$. Solving this system of equations for x and y gives

$$x = \frac{1}{2}(a+b) \quad \text{and} \quad y = \frac{1}{2}(a-b).$$

Since N is odd, both a and b must be odd, so all integer choices of a and b produce integer solutions for x and y. Since a could take positive or negative values, we have $2d(N)$ possible choices for a.

To show that all $2d(N)$ possibilities produce distinct pairs of x and y, assume that a_1 and a_2 both divide N so that $N = a_1 b_1$ and $N = a_2 b_2$. Now if

$$\frac{1}{2}(a_1 + b_1) = \frac{1}{2}(a_2 + b_2) \quad \text{and} \quad \frac{1}{2}(a_1 - b_1) = \frac{1}{2}(a_2 - b_2)$$

then adding these two equations together gives $a_1 = a_2$. □

7.2.18 Problem 18

Develop a formula for $\sigma_2(n)$, the sum of the squares of the positive divisors of n.

Solution. The first ten values of σ_2 are

n	1	2	3	4	5	6	7	8	9	10
$\sigma_2(n)$	1	5	10	21	26	50	50	85	91	130

Certainly if p is prime then $\sigma_2(p) = 1 + p^2$. Since the divisors of p^k are $1, p, \ldots, p^k$, it follows that

$$\sigma_2(p^k) = 1 + p^2 + p^4 + \cdots + p^{2k} = \frac{p^{2(k+1)} - 1}{p^2 - 1}.$$

Assuming σ_2 is multiplicative, this suggests a general formula. We will now prove that for all positive integers n, if the prime-power decomposition of n is $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then

$$\sigma_2(n) = \sigma_2(p_1^{e_1})\sigma_2(p_2^{e_2}) \cdots \sigma_2(p_r^{e_r}).$$

Our proof will mimic the proof of Theorem 2 in the text, using induction on r. For $r = 1$ the statement is trivial, so suppose it is true for $r = k$, $k \geq 1$. Let n be any integer having $k + 1$ distinct prime factors:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} p_{k+1}^{e_{k+1}}.$$

Let $N = p_1^{e_1} \cdots p_k^{e_k}$, let $p = p_{k+1}$ and let $e = e_{k+1}$ so that $n = Np^e$. If $1, d_1, \ldots, d_t$ are the positive divisors of N, then the divisors of n can be arranged

$$\begin{array}{ccccc} 1 & d_1 & d_2 & \cdots & d_t \\ p & d_1 p & d_2 p & \cdots & d_t p \\ p^2 & d_1 p^2 & d_2 p^2 & \cdots & d_t p^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p^e & d_1 p^e & d_2 p^e & \cdots & d_t p^e. \end{array}$$

Summing the squares of these divisors gives

$$\begin{aligned} \sigma_2(n) &= (1 + d_1^2 + d_2^2 + \cdots + d_t^2)(1 + p^2 + p^4 + \cdots + p^{2e}) \\ &= \sigma_2(N)\sigma_2(p^e). \end{aligned}$$

Now, using the inductive hypothesis, the above becomes

$$\sigma_2(n) = \sigma_2(p_1^{e_1})\sigma_2(p_2^{e_2}) \cdots \sigma_2(p_k e^k)\sigma_2(p_{k+1} e^{k+1})$$

as required to complete the proof. □

7.2.19 Problem 19

Guess a formula for

$$\sigma_k(n) = \sum_{d|n} d^k,$$

where k is a positive integer.

Solution. The previous problem suggests (and indeed a similar proof will show) that if n has prime-power decomposition $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$\sigma_k(n) = \sigma_k(p_1^{e_1}) \cdots \sigma_k(p_r^{e_r}),$$

where

$$\sigma_k(p_i^{e_i}) = 1 + p_i^k + p_i^{2k} + \cdots + p_i^{e_i k} = \frac{p_i^{k(e_i+1)} - 1}{p_i^k - 1},$$

for each $i = 1, 2, \ldots, r$. □

7.2.20 Problem 20

Show that the product of the positive divisors of n is $n^{d(n)/2}$.

Solution. Define the arithmetic function f by

$$f(n) = \prod_{d|n} d.$$

For prime powers $n = p^e$, we have

$$\begin{aligned} f(p^e) &= 1(p)(p^2)\cdots(p^e) \\ &= p^{1+2+\cdots+e} \\ &= p^{e(e+1)/2} \\ &= (p^e)^{(e+1)/2} \\ &= n^{d(n)/2}. \end{aligned}$$

Note that $n^{d(n)/2}$ is always an integer, since $d(n)$ is only odd when n is a perfect square (shown in Problem 7.2.14).

Now, let n have r distinct prime factors. We will use induction on r to show that $f(n) = n^{d(n)/2}$. We have already shown (above) that this is true when $r = 1$. Assume that it is true when $r = k$, for some $k \geq 1$. If n has $k+1$ distinct prime factors, then n can be written in prime-power form as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} p_{k+1}^{e_{k+1}}.$$

Now let $N = p_1^{e_1} \cdots p_k^{e_k}$, let $p = p_{k+1}$, and let $e = e_{k+1}$. Then $n = Np^e$. If $1, d_1, d_2, \ldots, d_t$ are the positive divisors of N, then we may list the positive divisors of n as follows.

$$\begin{array}{ccccc} 1 & d_1 & d_2 & \cdots & d_t \\ p & d_1 p & d_2 p & \cdots & d_t p \\ p^2 & d_1 p^2 & d_2 p^2 & \cdots & d_t p^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p^e & d_1 p^e & d_2 p^e & \cdots & d_t p^e \end{array}$$

The product of line i above is

$$\begin{aligned} p^{i-1}(d_1 p^{i-1})(d_2 p^{i-1})\cdots(d_t p^{i-1}) &= (p^{i-1})^{t+1}(d_1 d_2 \cdots d_t) \\ &= (p^{i-1})^{d(N)} f(N). \end{aligned}$$

Taking the product of all $e+1$ lines gives

$$\begin{aligned} f(n) &= \big(1^{d(N)} f(N)\big) \cdot \big(p^{d(N)} f(N)\big) \cdots \big(p^{ed(N)} f(N)\big) \\ &= \big(p \cdot p^2 \cdots p^e\big)^{d(N)} \big(f(N)\big)^{e+1} \\ &= \big(f(p^e)\big)^{d(N)} \big(f(N)\big)^{d(p^e)}. \end{aligned}$$

Applying the inductive hypothesis then gives

$$\begin{aligned} f(n) &= (p^e)^{d(N)d(p^e)/2} N^{d(N)d(p^e)/2} \\ &= (p^e)^{d(n)/2} N^{d(n)/2} \\ &= n^{d(n)/2}. \end{aligned}$$

By induction, the formula works for all positive integers n. □

Chapter 8

Perfect Numbers

8.1 Exercises

8.1.1 Exercise 1

Verify that 1184 and 1210 are amicable.

Solution. $1184 = 2^5 \cdot 37$ and $1210 = 2 \cdot 5 \cdot 11^2$, so

$$\sigma(1184) = \sigma(2^5)\sigma(37) = (2^6 - 1)(38) = 63 \cdot 38 = 2394$$

and

$$\sigma(1210) = \sigma(2)\sigma(5)\sigma(11^2) = 3 \cdot 6 \cdot (1 + 11 + 121) = 18 \cdot 133 = 2394.$$

Since $1184 + 1210 = 2394$, we see that the two numbers form an amicable pair. □

8.2 Problems

8.2.1 Problem 1

Verify that $2620, 2924$ and $17296, 18416$ are amicable pairs.

Solution. $2620 = 2^2 \cdot 5 \cdot 131$ and $2924 = 2^2 \cdot 17 \cdot 43$. We get

$$\sigma(2620) = 7 \cdot 6 \cdot 132 = 5544$$

and

$$\sigma(2924) = 7 \cdot 18 \cdot 44 = 5544,$$

and $2620 + 2924 = 5544$, so the two are amicable.

For 17296 we have

$$\sigma(17296) = \sigma(2^4 \cdot 23 \cdot 47) = 31 \cdot 24 \cdot 48 = 35712$$

and for 18416 we have

$$\sigma(18416) = \sigma(2^4 \cdot 1151) = 31 \cdot 1152 = 35712,$$

and $17296 + 18416 = 35712$, so these two are also amicable. □

8.2.2 Problem 2

It was long thought that even perfect numbers ended alternately in 6 and 8. Show that this is wrong by verifying that the perfect numbers corresponding to the primes $2^{13}-1$ and $2^{17}-1$ both end in 6.

Proof. First note that $2^8 = 256 \equiv 6 \pmod{10}$ so $2^{16} \equiv 6^2 \equiv 6 \pmod{10}$, and $2^{12} = 2^8 \cdot 2^4 \equiv 6 \cdot 6 \equiv 6 \pmod{10}$.

For $p = 13$, we have

$$2^{p-1}(2^p - 1) = 2^{12}(2^{13}-1) \equiv 6 \cdot (6 \cdot 2 - 1) \equiv 6 \pmod{10}$$

and for $p = 17$ we have

$$2^{p-1}(2^p - 1) = 2^{16}(2^{17}-1) \equiv 6 \cdot (6 \cdot 2 - 1) \equiv 6 \pmod{10}.$$

In both cases, we see that the corresponding perfect numbers end in 6. □

8.2.3 Problem 3

Classify the integers $2, 3, \dots, 21$ as abundant, deficient, or perfect.

Solution. The values of $\sigma(n)$ for $n = 1, \dots, 14$ are listed in the table from Exercise 7.1.5. The remaining values are as follows:

$$\begin{aligned}
\sigma(15) &= \sigma(3)\sigma(5) = 4 \cdot 6 = 24,\\
\sigma(16) &= \sigma(2^4) = 2^5 - 1 = 31,\\
\sigma(17) &= 18,\\
\sigma(18) &= \sigma(2)\sigma(3^2) = 3 \cdot (1+3+9) = 39,\\
\sigma(19) &= 20,\\
\sigma(20) &= \sigma(2^2)\sigma(5) = (2^3-1) \cdot 6 = 42,\\
\sigma(21) &= \sigma(3)\sigma(7) = 4 \cdot 8 = 32.
\end{aligned}$$

From these values, we determine that the only perfect number between 2 and 21 is 6. The only abundant numbers between 2 and 21 are 12, 18, and 20. And the remaining values are all deficient. □

8.2.4 Problem 4

Classify the integers $402, 403, \dots, 421$ as abundant, deficient, or perfect.

Solution. The calculations for $\sigma(n)$ are similar to those in the previous problem. We find that, in this range, there are no perfect numbers and the only abundant numbers are 402, 408, 414, 416, and 420. The remaining numbers are deficient. □

8.2.5 Problem 5

If $\sigma(n) = kn$, then n is called a *k-perfect number.* Verify that 672 is 3-perfect, and 2,178,540 $= 2^2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13 \cdot 19$ is 4-perfect.

Solution. We compute

$$\sigma(672) = \sigma(2^5)\sigma(3)\sigma(7) = 63 \cdot 4 \cdot 8 = 2016 = 3 \cdot 672,$$

showing that 672 is 3-perfect. For 2,178,540 we get

$$\begin{aligned}\sigma(2\,178\,540) &= \sigma(2^2)\sigma(3^2)\sigma(5)\sigma(7^2)\sigma(13)\sigma(19)\\ &= 7 \cdot 13 \cdot 6 \cdot 57 \cdot 14 \cdot 20\\ &= 8\,714\,160\\ &= 4 \cdot 2\,178\,540,\end{aligned}$$

showing that it is 4-perfect. □

8.2.6 Problem 6

Show that no number of the form $2^a 3^b$ is 3-perfect.

Proof. Let $n = 2^a 3^b$ for some nonnegative integers a and b. Then

$$\begin{aligned}\sigma(n) = \sigma(2^a)\sigma(3^b) &= (2^{a+1} - 1) \cdot \frac{3^{b+1} - 1}{2}\\ &= \frac{1}{2}(2^{a+1}3^{b+1} - 2^{a+1} - 3^{b+1} + 1)\\ &= \frac{1}{2}(6n - 2^{a+1} - 3^{b+1} + 1)\\ &= 3n - \frac{1}{2}(2^{a+1} + 3^{b+1} - 1).\end{aligned}$$

Now suppose n is 3-perfect. Then $\sigma(n) = 3n$ and we get

$$2^{a+1} + 3^{b+1} - 1 = 0.$$

But $a, b \geq 0$, so the left-hand side of this equation has to be at least $2+3-1 = 4$. This contradiction shows that no such n is 3-perfect. □

8.2.7 Problem 7

Let us say that n is *superperfect* if and only if $\sigma(\sigma(n)) = 2n$. Show that if $n = 2^k$ and $2^{k+1} - 1$ is prime, then n is superperfect.

Proof. Let $n = 2^k$ for some positive integer k and suppose $2^{k+1} - 1$ is prime. Then

$$\sigma(\sigma(n)) = \sigma(2^{k+1} - 1) = (2^{k+1} - 1) + 1 = 2^{k+1} = 2n$$

and n is superperfect. □

8.2.8 Problem 8

It was long thought that every abundant number was even. Show that 945 is abundant, and find another abundant number of the form $3^a \cdot 5 \cdot 7$.

Solution. We have

$$\sigma(945) = \sigma(3^3)\sigma(5)\sigma(7) = (1 + 3 + 9 + 27) \cdot 6 \cdot 8 = 40 \cdot 48 = 1920,$$

and since $1920 > 1890 = 2 \cdot 945$, we see that 945 is indeed abundant.

Another odd abundant number is $2835 = 3^4 \cdot 5 \cdot 7$, since

$$\sigma(2835) = 5808 > 2 \cdot 2835 = 5670. \qquad \square$$

8.2.9 Problem 9

In 1575, it was observed that every even perfect number is a triangular number. Show that this is so.

Proof. Let n be a perfect number, so that $n = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are prime. Then we may write

$$n = \frac{2^p(2^p - 1)}{2} = \frac{k(k + 1)}{2},$$

where $k = 2^p - 1$ is an integer. This shows that n is triangular. □

8.2.10 Problem 10

In 1652, it was observed that

$$\begin{aligned} 6 &= 1 + 2 + 3, \\ 28 &= 1 + 2 + 3 + 4 + 5 + 6 + 7, \\ 496 &= 1 + 2 + 3 + \cdots + 31. \end{aligned}$$

Can this go on?

Solution. Yes, every perfect number n can be written as the sum

$$n = 1 + 2 + 3 + \cdots + k$$

for some positive integer k. The reason for this is because every perfect number is triangular, as was shown in the previous problem, and every triangular number can be written in the form

$$\sum_{k=1}^{n} k = \frac{n(n + 1)}{2}.$$

This is easy to prove by induction. □

8.2.11 Problem 11

Let

$$\begin{aligned} p &= 3 \cdot 2^e - 1, \\ q &= 3 \cdot 2^{e-1} - 1, \\ r &= 3^2 \cdot 2^{2e-1} - 1, \end{aligned}$$

where e is a positive integer. If p, q, and r are all prime, show that $2^e pq$ and $2^e r$ are amicable.

Proof. We will actually need to assume $e \geq 2$ so that p, q, r are odd primes ($e = 1$ produces 20 and 34, which are not amicable). Let $m = 2^e pq$ and $n = 2^e r$.

Note that p, q, and r must be distinct primes, and all are odd, so the four numbers 2^e, p, q, and r are all pairwise coprime. Then we may compute

$$\begin{aligned} \sigma(m) &= \sigma(2^e)\sigma(p)\sigma(q) \\ &= (2^{e+1} - 1)(p + 1)(q + 1) \\ &= (2^{e+1} - 1)(3 \cdot 2^e)(3 \cdot 2^{e-1}) \\ &= 9 \cdot 2^{2e-1}(2^{e+1} - 1), \end{aligned}$$

and

$$\begin{aligned} \sigma(n) &= \sigma(2^e)\sigma(r) \\ &= (2^{e+1} - 1)(r + 1) \\ &= 9 \cdot 2^{2e-1}(2^{e+1} - 1). \end{aligned}$$

Since

$$\begin{aligned} m + n &= 2^e(pq + r) \\ &= 2^e((3 \cdot 2^e - 1)(3 \cdot 2^{e-1} - 1) + (9 \cdot 2^{2e-1} - 1)) \\ &= 2^e(2 \cdot 9 \cdot 2^{2e-1} - 3(2^e + 2^{e-1})) \\ &= 2^e(9 \cdot 2^{2e} - 9 \cdot 2^{e-1}) \\ &= 9 \cdot 2^{2e-1}(2^{e+1} - 1), \end{aligned}$$

we see that $\sigma(m) = \sigma(n) = m + n$ and the two numbers m and n form an amicable pair. □

8.2.12 Problem 12

Show that if $p > 3$ and $2p + 1$ is prime, then $2p(2p + 1)$ is deficient.

Proof. Let $n = 2p(2p+1)$, where p and $2p+1$ are prime, and $p > 3$. We compute

$$\begin{aligned} \sigma(n) &= \sigma(2)\sigma(p)\sigma(2p + 1) \\ &= 3(p + 1)(2p + 2) \\ &= 3p(2p + 2) + 3(2p + 2) \\ &= 3p(2p + 1) + 3p + 3(2p + 2) \\ &= 4p(2p + 1) - p(2p + 1) + 3p + 3(2p + 2) \\ &= 2n - 2(p^2 - 4p - 3). \end{aligned}$$

Now, since $p \geq 5$, it is easy to check that $p^2 - 4p - 3 > 0$. Therefore $\sigma(n) < 2n$ and we conclude that n is deficient. □

8.2.13 Problem 13

Show that all even perfect numbers end in 6 or 8.

Proof. Let n be an even perfect number. We know that

$$n = 2^{p-1}(2^p - 1), \quad \text{where } p \text{ and } 2^p - 1 \text{ are prime.}$$

Note that

$$\begin{aligned} p \equiv 1 \pmod 4 &\quad \Rightarrow \quad 2^{p-1} = 2^{4k} = 16^k \equiv 6 \pmod{10}, \\ p \equiv 2 \pmod 4 &\quad \Rightarrow \quad 2^{p-1} = 2^{4k+1} \equiv 2 \cdot 6 \equiv 2 \pmod{10}, \\ p \equiv 3 \pmod 4 &\quad \Rightarrow \quad 2^{p-1} = 2^{4k+2} \equiv 4 \cdot 6 \equiv 4 \pmod{10}. \end{aligned}$$

We do not need to consider the case where $p \equiv 0 \pmod 4$ since no prime can be divisible by 4.

Let us consider the three cases. First, if $p \equiv 1 \pmod 4$, then we get

$$n \equiv 6(2 \cdot 6 - 1) \equiv 6 \pmod{10}. \tag{8.1}$$

Second, if $p \equiv 2 \pmod 4$ then we get

$$n \equiv 2(2 \cdot 2 - 1) \equiv 6 \pmod{10}. \tag{8.2}$$

Finally, if $p \equiv 3 \pmod 4$ then

$$n \equiv 4(2 \cdot 4 - 1) \equiv 8 \pmod{10}. \tag{8.3}$$

Together, 8.1, 8.2, and 8.3 show that every even perfect number must end in 6 or 8, when written in decimal notation. □

8.2.14 Problem 14

If n is an even perfect number and $n > 6$, show that the sum of its digits is congruent to 1 (mod 9).

Proof. Let $n = 2^{p-1}(2^p - 1)$ be an even perfect number. We proceed in a similar fashion as in the previous problem. Since $n > 6$, we have $p \geq 3$. The case where $p = 3$ is easily handled since $28 \equiv 1 \pmod 9$. So assume $p \geq 5$.

Since the powers of 2 (mod 9) cycle through six different residues, we will consider the congruence class of p modulo 6. There are only two cases: either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$. All other cases require that p be either composite or less than 5.

In the first case, $p \equiv 1 \pmod 6$ so

$$2^{p-1} = 2^{6k} = (2^6)^k \equiv 1 \pmod 9 \quad \text{and} \quad 2^p \equiv 2 \pmod 9.$$

Therefore

$$n = 2^{p-1}(2^p - 1) \equiv 1(2 - 1) \equiv 1 \pmod 9.$$

In the second case, $p \equiv 5 \pmod 6$ which gives

$$2^{p-1} = 2^{6k+4} = (2^6)^k \cdot 2^4 \equiv 1 \cdot 16 \equiv 7 \pmod 9$$

and

$$2^p \equiv 14 \equiv 5 \pmod 9.$$

Therefore

$$n = 2^{p-1}(2^p - 1) \equiv 7(5-1) \equiv 28 \equiv 1 \pmod 9.$$

In both cases, we get $n \equiv 1 \pmod 9$ as required. □

8.2.15 Problem 15

If p is odd, show that $2^{p-1}(2^p - 1) \equiv 1 + 9p(p-1)/2 \pmod{81}$.

Proof. Note that $2^{54} \equiv 1 \pmod{81}$ (this can be determined simply by repeatedly multiplying by 2 and reducing modulo 81). So the left-hand side of the congruence is completely determined by the congruence class of p modulo 54. The right-hand side will depend on the congruence class of p modulo 9. Since $9 \mid 54$, it will suffice to check each odd residue between 1 and 53. This is tedious, but not difficult.

In each case, we see that the congruence holds. In fact, it holds even when p is not prime, so long as p is odd. □

Chapter 9

Euler's Theorem and Function

9.1 Exercises

9.1.1 Exercise 1

Show that $a^6 \equiv 1 \pmod{14}$ for all a relatively prime to 14.

Solution. The least residues that are relatively prime to 14 are 1, 3, 5, 9, 11, and 13. We compute:

$$\begin{aligned} 3^6 &= 27^2 \equiv (-1)^2 \equiv 1 \pmod{14}, \\ 5^6 &= 25^3 \equiv (-3)^3 \equiv 1 \pmod{14}, \\ 9^6 &= (3^6)^2 \equiv 1 \pmod{14}, \\ 11^6 &\equiv (-3)^6 \equiv 1 \pmod{14}, \end{aligned}$$

and

$$13^6 \equiv (-1)^6 \equiv 1 \pmod{14}.$$

In every case, $(a, 14) = 1$ implies $a^6 \equiv 1 \pmod{14}$. □

9.1.2 Exercise 2

Verify that Lemma 1 is true if $m = 14$ and $a = 5$.

Solution. Again, the relatively prime positive integers less than 14 are 1, 3, 5, 9, 11, and 13.

$$\begin{aligned} 5 \cdot 1 = 5 &\equiv 5 \pmod{14}, \\ 5 \cdot 3 = 15 &\equiv 1 \pmod{14}, \\ 5 \cdot 5 = 25 &\equiv 11 \pmod{14}, \\ 5 \cdot 9 = 45 &\equiv 3 \pmod{14}, \\ 5 \cdot 11 = 55 &\equiv 13 \pmod{14}, \end{aligned}$$

and

$$5 \cdot 13 = 65 \equiv 9 \pmod{14}.$$

And, certainly, $(5, 1, 11, 3, 13, 9)$ is a permutation of $\{1, 3, 5, 9, 11, 13\}$. □

9.1.3 Exercise 3

Verify that the entries in the following table are correct.

n	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	2	2	4	2	6	4	6	4

Solution. The verification is straightforward. We simply count the number of positive integers that are relatively prime to n and less than or equal to n. For example, when $n = 8$ the relatively prime residues are 1, 3, 5, and 7, so $\phi(8) = 4$. The other values are checked in the same way. □

9.1.4 Exercise 4

Verify that $3^{\phi(8)} \equiv 1 \pmod{8}$.

Solution. Since $\phi(8) = 4$, we have $3^4 = 9^2 \equiv 1^2 \equiv 1 \pmod{8}$. □

9.1.5 Exercise 5

Which positive integers are less than 4 and relatively prime to it? What is the answer if 4 is replaced by 8? By 16? Can you induce a formula for $\phi(2^n)$, $n = 1, 2, \ldots$?

Solution. For 4 the numbers are 1 and 3. For 8 they are 1, 3, 5, and 7. For 16, they are 1, 3, 5, 7, 9, 11, 13, and 15. So we have $\phi(4) = 2$, $\phi(8) = 4$, and $\phi(16) = 8$.

In general, it looks like $\phi(2^n) = 2^{n-1}$ for each positive n. To prove this, note that there are 2^n positive integers less than or equal to 2^n. Exactly half of these numbers will be even and thus not relatively prime to 2^n. So

$$\phi(2^n) = \frac{1}{2}(2^n) = 2^{n-1}.$$ □

9.1.6 Exercise 6

Verify that the formula of Lemma 2 is correct for $p = 5$ and $n = 2$.

Solution. According to Lemma 2, $\phi(5^2) = 5^1(5 - 1) = 20$. The positive integers less than or equal to 5^2 that are not relatively prime to it are 5, 10, 15, 20, and 25, so $\phi(5^2) = 25 - 5 = 20$ and the formula works in this case. □

9.1.7 Exercise 7

In the proof of Theorem 2, how many rows are there whose first element is relatively prime to m?

Solution. There are exactly $\phi(m)$ such rows. □

9.1.8 Exercise 8

Calculate $\phi(74)$, $\phi(76)$, and $\phi(78)$.

Solution. Using Theorem 3, we get

$$\begin{aligned}\phi(74) &= \phi(2)\phi(37) = (1\cdot 1)(1\cdot 36) = 36,\\ \phi(76) &= \phi(2^2)\phi(19) = (2\cdot 1)(1\cdot 18) = 36,\end{aligned}$$

and

$$\phi(78) = \phi(2)\phi(3)\phi(13) = (1\cdot 1)(1\cdot 2)(1\cdot 12) = 24. \qquad \square$$

9.1.9 Exercise 9

Calculate $\sum_{d|n} \phi(d)$

(a) For $n = 12$, 13, 14, 15, and 16.

Solution. For $n = 12$, we have

$$\begin{aligned}\sum_{d|12} \phi(d) &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12)\\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12.\end{aligned}$$

In the same manner, we can compute the rest of the values. In each case, we find that

$$\sum_{d|n} \phi(d) = n. \qquad \square$$

(b) For $n = 2^k$, $k \geq 1$.

Solution. The positive divisors of 2^k are $1, 2, 4, \ldots, 2^k$. So

$$\begin{aligned}\sum_{d|2^k} \phi(d) &= \sum_{i=0}^{k} \phi(2^i)\\ &= \phi(1) + \sum_{i=1}^{k} 2^{i-1}\\ &= 1 + (2^k - 1) = 2^k\\ &= n. \qquad \square\end{aligned}$$

(c) For $n = p^k$, $k \geq 1$ and p an odd prime.

Solution. The positive divisors of n are $1, p, p^2, \ldots, p^k$, so

$$\begin{aligned}\sum_{d\mid p^k} \phi(d) &= \sum_{i=0}^{k} \phi(p^i)\\ &= 1 + \sum_{i=1}^{k} p^{i-1}(p-1)\\ &= 1 + \sum_{i=1}^{k} p^i - \sum_{i=1}^{k} p^{i-1}\\ &= 1 + \left(p^k + \sum_{i=1}^{k-1} p^i\right) - \left(1 + \sum_{i=1}^{k-1} p^i\right)\\ &= p^k = n.\end{aligned}$$

□

9.1.10 Exercise 10

In the proof of Theorem 4, what are the classes C_d for $n = 14$?

Solution. We have

$$\begin{aligned}C_1 &= \{1, 3, 5, 9, 11, 13\},\\ C_2 &= \{2, 4, 6, 8, 10, 12\},\\ C_7 &= \{7\},\end{aligned}$$

and

$$C_{14} = \{14\}.$$

□

9.1.11 Exercise 11

Check that the number of elements in class C_d is $\phi(n/d)$ for $n = 12$ and $n = 14$.

Solution. For $n = 12$:

$$\begin{aligned}C_1 &= \{1, 5, 7, 11\}, & \phi(12) &= 4,\\ C_2 &= \{2, 10\}, & \phi(6) &= 2,\\ C_3 &= \{3, 9\}, & \phi(4) &= 2,\\ C_4 &= \{4, 8\}, & \phi(3) &= 2,\\ C_6 &= \{6\}, & \phi(2) &= 1,\\ C_{12} &= \{12\}, & \phi(1) &= 1.\end{aligned}$$

In each case, we see that C_d has exactly $\phi(n/d)$ elements.

Similarly, for $n = 14$, $\phi(14) = 6$, $\phi(7) = 6$, $\phi(2) = 1$, and $\phi(1) = 1$, and we see that these numbers match the size of the sets found in the previous exercise. □

9.2 Problems

9.2.1 Problem 1

Calculate $\phi(42)$, $\phi(420)$, and $\phi(4200)$.

Solution. We have

$$\begin{aligned}\phi(42) &= \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = 12\\ \phi(420) &= \phi(2^2)\phi(3)\phi(5)\phi(7) = 2 \cdot 2 \cdot 4 \cdot 6 = 96\end{aligned}$$

and

$$\phi(4200) = \phi(2^3)\phi(3)\phi(5^2)\phi(7) = 4 \cdot 2 \cdot 20 \cdot 6 = 960.$$ □

9.2.2 Problem 2

Calculate $\phi(54)$, $\phi(540)$, and $\phi(5400)$.

Solution.

$$\begin{aligned}\phi(54) &= \phi(2)\phi(3^3) = 1 \cdot 18 = 18,\\ \phi(540) &= \phi(2^2)\phi(3^3)\phi(5) = 2 \cdot 18 \cdot 4 = 144,\end{aligned}$$

and

$$\phi(5400) = \phi(2^3)\phi(3^3)\phi(5^2) = 4 \cdot 18 \cdot 20 = 1440.$$ □

9.2.3 Problem 3

Calculate ϕ of $10115 = 5 \cdot 7 \cdot 17^2$ and $100115 = 5 \cdot 20023$.

Solution.

$$\begin{aligned}\phi(10115) &= \phi(5)\phi(7)\phi(17^2)\\ &= 4 \cdot 6 \cdot 17(17-1)\\ &= 24 \cdot 17 \cdot 16\\ &= 6528\end{aligned}$$

and

$$\begin{aligned}\phi(100115) &= \phi(5)\phi(20023)\\ &= 4 \cdot 20022\\ &= 80088.\end{aligned}$$ □

9.2.4 Problem 4

Calculate ϕ of $10116 = 2^2 \cdot 3^2 \cdot 281$ and $100116 = 2^2 \cdot 3^5 \cdot 103$.

Solution.

$$\begin{aligned}\phi(10116) &= \phi(2^2)\phi(3^2)\phi(281)\\ &= 2 \cdot 6 \cdot 280\\ &= 3360\end{aligned}$$

and

$$\begin{aligned}\phi(100116) &= \phi(2^2)\phi(3^5)\phi(103)\\ &= 2 \cdot 3^4(2) \cdot 102\\ &= 324 \cdot 102\\ &= 33048.\end{aligned}$$ □

9.2.5 Problem 5

Calculate $a^8 \pmod{15}$ for $a = 1, 2, \ldots, 14$.

Solution. Since $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$, we know $a^8 \equiv 1 \pmod{15}$ for each a such that $(a, 15) = 1$. For the remaining values, we have

$$\begin{aligned}3^8 &= (3^4)^2 \equiv 6^2 \equiv 6 \pmod{15},\\ 5^8 &= (5^2)^4 \equiv 10^4 \equiv 10^2 \equiv 10 \pmod{15},\\ 6^8 &= 2^8 3^8 \equiv 6 \cdot 16^4 \equiv 6 \pmod{15},\\ 9^8 &= (3^8)^2 \equiv 36 \equiv 6 \pmod{15},\\ 10^8 &= (10^4)^2 \equiv 10^2 \equiv 10 \pmod{15},\end{aligned}$$

and

$$12^8 = 3^8 4^8 \equiv 6 \cdot (2^4)^4 \equiv 6 \pmod{15}.$$ □

9.2.6 Problem 6

Calculate $a^8 \pmod{16}$ for $a = 1, 2, \ldots, 15$.

Solution. $\phi(16) = 8$, so $a^8 \equiv 1 \pmod{16}$ for all a such that $(a, 16) = 1$. The remaining values are all even, and since 2^8 contains a factor of 16, we will get $a^8 \equiv 0 \pmod{16}$ for each a such that $(a, 16) > 1$. □

9.2.7 Problem 7

Show that if n is odd, then $\phi(4n) = 2\phi(n)$.

Proof. Since n is odd, we know $(4, n) = 1$, so the multiplicativity of ϕ gives

$$\phi(4n) = \phi(4)\phi(n) = 2\phi(n).$$ □

9.2.8 Problem 8

Perfect numbers satisfy $\sigma(n) = 2n$. Which n satisfy $\phi(n) = 2n$?

Solution. There are no positive integers n with $\phi(n) = 2n$, for the simple reason that there are only n positive integers less than or equal to n in the first place. So $\phi(n) \leq n$ for all n. □

9.2.9 Problem 9

$1+2 = (3/2)\phi(3)$, $1+3 = (4/2)\phi(4)$, $1+2+3+4 = (5/2)\phi(5)$, $1+5 = (6/2)\phi(6)$, $1+2+3+4+5+6 = (7/2)\phi(7)$, and $1+3+5+7 = (8/2)\phi(8)$. Guess a theorem.

Solution. For each positive integer $n > 1$, the sum of the positive integers less than or equal to n which are relatively prime to n is $(n/2)\phi(n)$.

To prove this, let T be the set of positive integers less than or equal to n and relatively prime to it, so that $T = \{t_1, t_2, t_3, \ldots, t_{\phi(n)}\}$.

Take the number t_i for some i. Then $(t_i, n) = 1$ and, by Theorem 4 of Section 1, there are integers x and y with

$$t_i x + ny = 1.$$

But by setting $a = -x$ and $b = x + y$, this equation becomes

$$a(n - t_i) + bn = 1,$$

so that $(n - t_i, n) = 1$ and $(n - t_i) \in T$. We see that $t_i \in T$ if and only if $n - t_i \in T$.

Now let S be the sum of the members of T. Then

$$S = t_1 + t_2 + t_3 + \cdots + t_{\phi(n)}. \tag{9.1}$$

On the other hand, we can also write

$$S = (n - t_1) + (n - t_2) + (n - t_3) + \cdots + (n - t_{\phi(n)}). \tag{9.2}$$

Adding equations (9.1) and (9.2) together then gives

$$2S = n\phi(n)$$

and dividing by 2 gives the desired result. □

9.2.10 Problem 10

Show that

$$\sum_{p \leq x} \sigma(p) - \sum_{p \leq x} \phi(p) = \sum_{p \leq x} d(p),$$

where each sum is over the primes less than or equal to x.

Proof. Note that for any prime p, $\sigma(p) = p + 1$, $\phi(p) = p - 1$, and $d(p) = 2$. So we have

$$\begin{aligned}\sum_{p \leq x} \sigma(p) - \sum_{p \leq x} \phi(p) &= \sum_{p \leq x} (p+1) - \sum_{p \leq x} (p-1) \\ &= \sum_{p \leq x} 2 \\ &= \sum_{p \leq x} d(p).\end{aligned}$$

□

9.2.11 Problem 11

Prove Lemma 3 by starting with the fact that there are integers r and s such that $ar + ms = 1$.

Proof. We want to show that if $(a, m) = 1$ and $a \equiv b \pmod{m}$, then $(b, m) = 1$. Since $ar + ms = 1$, we have

$$1 \equiv ar \equiv br \pmod{m},$$

which implies that $br + km = 1$ for some integer k. This is enough to show that $(b, m) = 1$. □

9.2.12 Problem 12

If $(a, m) = 1$, show that any x such that

$$x \equiv ca^{\phi(m)-1} \pmod{m} \tag{9.3}$$

satisfies $ax \equiv c \pmod{m}$.

Proof. Let x satisfy (9.3). Multiplying both sides of this congruence by a gives

$$ax \equiv ca^{\phi(m)} \pmod{m},$$

and since $(a, m) = 1$, we have $ca^{\phi(m)} \equiv c \pmod{m}$ by Euler's Theorem. □

9.2.13 Problem 13

Let $f(n) = (n + \phi(n))/2$. Show that $f(f(n)) = \phi(n)$ if $n = 2^k$, $k = 3, 4, 5, \ldots$.

Proof. We compute

$$\begin{aligned}f(2^k) &= \frac{2^k + \phi(2^k)}{2} \\ &= \frac{2^k + 2^{k-1}}{2} \\ &= 2^{k-1} + 2^{k-2} \\ &= 2^{k-2}(2+1) \\ &= 2^{k-2} \cdot 3.\end{aligned}$$

So,

$$\begin{aligned}
f(f(2^k)) &= f(2^{k-2}\cdot 3)\\
&= \frac{2^{k-2}\cdot 3 + \phi(2^{k-2})\phi(3)}{2}\\
&= \frac{2^{k-2}\cdot 3 + 2^{k-3}\cdot 2}{2}\\
&= 2^{k-3}\cdot 3 + 2^{k-3}\\
&= 2^{k-3}(3+1)\\
&= 2^{k-1}\\
&= \phi(2^k).
\end{aligned}$$

We see that $f(f(2^k)) = \phi(2^k)$ for all $k \geq 3$. □

9.2.14 Problem 14

Find four solutions of $\phi(n) = 16$.

Solution. Since $3-1=2$, $5-1=4$, and $17-1=16$, solutions should have the form $2^a3^b5^c17^d$ for some nonnegative integers a, b, c, d. By inspection, we find

$$\begin{aligned}
&\phi(17) = 16,\\
&\phi(32) = \phi(2^5) = 16,\\
&\phi(34) = \phi(2)\phi(17) = 1\cdot 16 = 16,\\
&\phi(40) = \phi(2^3)\phi(5) = 4\cdot 4 = 16,\\
&\phi(48) = \phi(2^4)\phi(3) = 8\cdot 2 = 16,
\end{aligned}$$

and

$$\phi(60) = \phi(2^2)\phi(3)\phi(5) = 2\cdot 2\cdot 4 = 16.$$ □

9.2.15 Problem 15

Find all solutions of $\phi(n) = 4$ and prove that there are no more.

Solution. Let n be a solution, and let $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ be the prime-power decomposition of n. Then

$$\phi(n) = p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\cdots p_k^{e_k-1}(p_k-1) = 4.$$

Each factor in this expression must be either 1, 2, or 4. If

$$p_i^{e_i-1}(p_i-1) = 1,$$

then $p_i = 2$ and $e_i = 1$. If

$$p_i^{e_i-1}(p_i-1) = 2,$$

then either $p_i = 2$ and $e_i = 2$ or $p_i = 3$ and $e_i = 1$. And if

$$p_i^{e_i-1}(p_i-1) = 4,$$

then either $p_i = 2$ and $e_i = 3$ or $p_i = 5$ and $e_i = 1$. We can see that these are the only possibilities. Thus we have the following solutions.

$$\begin{aligned}\phi(5) &= 4,\\ \phi(8) &= \phi(2^3) = 2^2 = 4,\\ \phi(10) &= \phi(2)\phi(5) = 1 \cdot 4 = 4,\end{aligned}$$

and

$$\phi(12) = \phi(2^2)\phi(3) = 2 \cdot 2 = 4.$$

As we have ruled out all other possibilities, these are the only solutions. □

9.2.16 Problem 16

Show that $\phi(mn) > \phi(m)\phi(n)$ if m and n have a common factor greater than 1.

Proof. Let p be a prime. Then for all positive integers e and f,

$$p^{e+f-1}(p-1) = p^{e+f-2}p(p-1) > p^{e+f-2}(p-1)^2. \tag{9.4}$$

Now suppose $(m, n) = d > 1$ and let k be the number of distinct prime factors of d. We will use induction on k to show that $\phi(mn) > \phi(m)\phi(n)$.

First, if $k = 1$, then we can write $m = ap^e$ and $n = bp^f$ for some positive integers e and f, with $(a, b) = (a, p) = (b, p) = 1$. Then (9.4) implies

$$\begin{aligned}\phi(mn) &= \phi(a)\phi(b)\phi(p^{e+f})\\ &= \phi(a)\phi(b)p^{e+f-1}(p-1)\\ &> \phi(a)\phi(b)p^{e+f-2}(p-1)^2\\ &= \left(\phi(a)p^{e-1}(p-1)\right)\left(\phi(b)p^{f-1}(p-1)\right)\\ &= \phi(a)\phi(p^e)\phi(b)\phi(p^f)\\ &= \phi(m)\phi(n),\end{aligned}$$

so $\phi(mn) > \phi(m)\phi(n)$ in the case where $k = 1$.

Now suppose $\phi(mn) > \phi(m)\phi(n)$ whenever the common factor d has k distinct prime factors for some particular $k \geq 1$. Then suppose d has $k + 1$ distinct prime factors, and let one of the factors be p. Then we can write

$$m = ap^e \quad \text{and} \quad n = bp^f$$

for some positive integers e and f with $(a, p) = (b, p) = 1$. If $(a, b) = c$, then we know that c has at most k distinct prime factors, so the induction hypothesis tells us that $\phi(ab) \geq \phi(a)\phi(b)$ (with equality in the case where $c = 1$). Then, again making use of (9.4), we have

$$\begin{aligned}\phi(mn) &= \phi(ab)\phi(p^{e+f})\\ &= \phi(ab)p^{e+f-1}(p-1)\\ &> \phi(ab)p^{e+f-2}(p-1)^2\\ &\geq \phi(a)p^{e-1}(p-1)\phi(b)p^{f-1}(p-1)\\ &= \phi(m)\phi(n).\end{aligned}$$

By induction, the result holds for all positive integers k. □

9.2.17 Problem 17

Show that $(m, n) = 2$ implies $\phi(mn) = 2\phi(m)\phi(n)$.

Proof. Suppose $(m, n) = 2$. Then both m and n are even, but one of m or n contains only one factor of 2. Without loss of generality, let it be m, so that $m = 2k$ where k is odd. Then $n = 2^e\ell$ for some positive integer e and odd integer ℓ, where $(k, \ell) = 1$. Note that $\phi(m) = \phi(2)\phi(k) = \phi(k)$. So we get

$$\begin{aligned}\phi(mn) &= \phi(2^{e+1}k\ell)\\ &= \phi(2^{e+1})\phi(k)\phi(\ell)\\ &= 2^e\phi(m)\phi(\ell)\\ &= 2\cdot 2^{e-1}\phi(m)\phi(\ell)\\ &= 2\phi(2^e)\phi(m)\phi(\ell)\\ &= 2\phi(m)\phi(n).\end{aligned}$$

□

9.2.18 Problem 18

Show that $\phi(n) = n/2$ if and only if $n = 2^k$ for some positive integer k.

Proof. Suppose $2\phi(n) = n$. Write $n = 2^k m$, where m is odd. Then

$$2^k m = 2\phi(2^k m) = 2\phi(2^k)\phi(m) = 2^k\phi(m).$$

But this can be true if and only if $m = \phi(m)$, which can only be the case when $m = 1$. □

9.2.19 Problem 19

Show that if $n - 1$ and $n + 1$ are both primes and $n > 4$, then $\phi(n) \leq n/3$.

Proof. Since $n-1$ and $n+1$ are prime with $n > 4$, we know that $6 \mid n$. Therefore n has the form $n = 2^a 3^b k$ for some positive integers a, b, and k with $(k, 6) = 1$. Then

$$\begin{aligned}3\phi(n) &= 3\phi(2^a)\phi(3^b)\phi(k)\\ &= 2^{a-1}3^b(3-1)\phi(k)\\ &= 2^a 3^b\phi(k)\\ &\leq 2^a 3^b k = n.\end{aligned}$$

So $\phi(n) \leq n/3$. □

9.2.20 Problem 20

Show that $\phi(n) = 14$ is impossible.

Proof. Suppose $\phi(n) = 14$ for some n. Then

$$\phi(n) = p_1^{e_1-1}(p_1 - 1)\cdots p_k^{e_k-1}(p_k - 1),$$

where $n = p_1^{e_1}\cdots p_k^{e_k}$ is the prime-power decomposition of n.

We know that $7 \mid \phi(n)$, so one of the factors $p_i^{e_i-1}$ or $(p_i - 1)$ must be 7. Since 8 is not a prime, we cannot have $p_i - 1 = 7$, so $p_i^{e_i-1} = 7$ for some i. But then $p_i - 1 = 6$ so that 3 divides $\phi(n)$, which is clearly impossible. Therefore there is no n with $\phi(n) = 14$. □

Chapter 10

Primitive Roots

10.1 Exercises

10.1.1 Exercise 1

What are the orders of 3, 5, and 7, modulo 8?

Solution. Since $3^2 \equiv 1 \pmod 8$, $5^2 \equiv 1 \pmod 8$, and $7^2 \equiv 1 \pmod 8$, we see that each of these residues has order 2. □

10.1.2 Exercise 2

What order can an integer have (mod 9)? Find an example of each.

Solution. Since $\phi(9) = 3 \cdot 2 = 6$, the possible orders are 1, 2, 3, and 6. 1 is the only integer with order 1. 8 has order 2 since $8^2 \equiv 1 \pmod 9$. 4 has order 3 since $4^2 \equiv 7 \pmod 9$ and $4^3 \equiv 1 \pmod 9$. And 2 has order 6, since $2^2 \equiv 4 \pmod 9$ and $2^3 \equiv 8 \pmod 9$. □

10.1.3 Exercise 3

Using the corollary to Theorem 3, what is the smallest possible prime divisor of $2^{19} - 1$?

Solution. By the corollary, any divisor can be written $2 \cdot 19k + 1 = 38k + 1$. The smallest numbers of this form are 1, 39, 77, 115, 153, and 191. The smallest possible prime divisor is therefore 191. (191 is not a divisor, however, as $2^{19} - 1$ happens to be prime). □

10.1.4 Exercise 4

Show that 3 is a primitive root of 7.

Solution. We get

$$\begin{aligned} 3^1 &\equiv 3 \pmod 7, \\ 3^2 &\equiv 2 \pmod 7, \\ 3^3 &\equiv 6 \pmod 7, \\ 3^4 &\equiv 4 \pmod 7, \\ 3^5 &\equiv 5 \pmod 7, \\ 3^6 &\equiv 1 \pmod 7. \end{aligned}$$

Since $\phi(7) = 6$, 3 is a primitive root of 7. □

10.1.5 Exercise 5

Find, by trial, a primitive root of 10.

Solution. $\phi(10) = 4$. The powers of 3 (mod 10) are, respectively, 3, 9, 7, and 1, so 3 is a primitive root of 10. 7 is also a primitive root. □

10.1.6 Exercise 6

Use the table of powers (mod 11) at the beginning of this section to verify that the corollary is true for $p = 11$.

Solution. There is only one least residue with order 2 (namely 10), and $\phi(2) = 1$. There are 4 residues with order 5 (3, 4, 5, and 9), and $\phi(5) = 4$. And there are 4 residues with order 10 (2, 6, 7, and 8), and $\phi(10) = 4$. In each case the corollary holds. □

10.1.7 Exercise 7

Which of the integers $2, 3, \ldots, 25$ do not have primitive roots?

Solution. The only integers with primitive roots are 1, 2, 4, p^e, and $2p^e$ where p is an odd prime. So 8, 12, 15, 16, 20, 21, and 24 do not have primitive roots. □

10.2 Problems

10.2.1 Problem 1

Find the orders of $1, 2, \ldots, 12$ (mod 13).

Solution. 1 has order 1. 12 has order 2. 3 and 9 have order 3. 5 and 8 have order 4. 4 and 10 have order 6. 2, 6, 7, and 11 have order 12. □

10.2.2 Problem 2

Find the orders of $1, 2, \ldots, 16$ (mod 17).

Solution. 1 has order 1. 16 has order 2. 4 and 13 have order 4. 2, 8, 9, and 15 have order 8. 3, 5, 6, 7, 10, 11, 12, and 14 have order 16. □

10.2.3 Problem 3

One of the primitive roots of 19 is 2. Find all of the others.

Solution. According to the corollary to Lemma 1, 2^k will be a primitive root of 19 when $(k, 18) = 1$. So the primitive roots are 2, $2^5 \equiv 13$, $2^7 \equiv 14$, $2^{11} \equiv 15$, $2^{13} \equiv 3$, and $2^{17} \equiv 10 \pmod{19}$. □

10.2.4 Problem 4

One of the primitive roots of 23 is 5. Find all of the others.

Solution. 5^k should be a primitive root when $(k, 22) = 1$. So the primitive roots are 5, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, and 5^{21}. Computing these powers, we find that the primitive roots are 7, 10, 11, 14, 15, 17, 19, 20, and 21. □

10.2.5 Problem 5

What are the orders of 2, 4, 7, 8, 11, 13, and 14 (mod 15)? Does 15 have primitive roots?

Solution. 4, 11, and 14 have order 2. 2, 7, 8, and 13 have order 4. No integer has an order of $\phi(15) = 8$, so 15 does not have primitive roots. □

10.2.6 Problem 6

What are the orders of 3, 7, 9, 11, 13, 17, and 19 (mod 20)? Does 20 have primitive roots?

Solution. 9, 11, and 19 have order 2. 3, 7, 13, and 17 have order 4. No integer has an order of $\phi(20) = 8$, so 20 does not have primitive roots. □

10.2.7 Problem 7

Which integers have order 6 (mod 31)?

Solution. By inspection, 6 has order 6 (mod 31). As in the proof of Theorem 6, we can find the other integers with order 6 by taking 6^k for k such that $(k, 6) = 1$. So the least residues having order 6 are 6 and $6^5 \equiv 26 \pmod{31}$. □

10.2.8 Problem 8

Which integers have order 6 (mod 37)?

Solution. 11 has order 6, so $11^5 \equiv 27 \pmod{37}$ also has order 6. □

10.2.9 Problem 9

If a, $a \neq 1$, has order $t \pmod{p}$, show that

$$a^{t-1} + a^{t-2} + \cdots + 1 \equiv 0 \pmod{p}.$$

Proof. Since a has order t, $a^t - 1 \equiv 0 \pmod{p}$. Then

$$0 \equiv a^t - 1 \equiv (a-1)(a^{t-1} + a^{t-2} + \cdots + 1) \pmod{p}.$$

Since p is prime and $a - 1 \not\equiv 0 \pmod{p}$, we have

$$a^{t-1} + a^{t-2} + \cdots + 1 \equiv 0 \pmod{p}.$$ □

10.2.10 Problem 10

If g and h are primitive roots of an odd prime p, then $g \equiv h^k \pmod{p}$ for some integer k. Show that k is odd.

Proof. This follows from Lemma 1. h has order $p-1$, so h^k has the same order if and only if $(k, p-1) = 1$. But since p is an odd prime, if k is even then $(k, p-1) \geq 2$ and g would not be a primitive root. Therefore k must be odd. □

10.2.11 Problem 11

Show that if g and h are primitive roots of an odd prime p, then the least residue of gh is not a primitive root of p.

Proof. Since g and h are both primitive roots, $h = g^k$ for some integer k. By the previous problem we know that k must be odd. Then $gh = g^{k+1}$ cannot be a primitive root, because $k+1$ is even. □

10.2.12 Problem 12

If g, h, and k are primitive roots of p, is the least residue of ghk always a primitive root of p?

Solution. This is not true in general. For example, for $p = 23$, one can verify that 5, 10, and 17 are primitive roots, but $5 \cdot 10 \cdot 17 \equiv 22 \pmod{23}$ and 22 is not a primitive root of 23. □

10.2.13 Problem 13

Show that if a has order $3 \pmod{p}$, then $a + 1$ has order $6 \pmod{p}$.

Proof. Rewriting $a^3 - 1 \equiv 0 \pmod{p}$, we get $(a-1)(a^2 + a + 1) \equiv 0 \pmod{p}$, and since $a \not\equiv 1 \pmod{p}$, we get $a^2 + a + 1 \equiv 0 \pmod{p}$. Then

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

Since $p > 2$ (because a has order greater than 2), $1 \not\equiv -1 \pmod{p}$ and we see that the order of $a+1$ is not 3. But $(a+1)^6 \equiv 1 \pmod{p}$ so the order of a must divide 6.

The proof will be complete if we can show that $a+1$ does not have order 2. Since

$$\begin{aligned}(a+1)^2 &= a^2 + 2a + 1\\ &= (a^2 + a + 1) + a\\ &\equiv a \pmod{p},\end{aligned}$$

we see that $a+1$ does not have order 2. Therefore $a+1$ has order 6. □

10.2.14 Problem 14

If p and q are odd primes and $q \mid a^p + 1$, show that either $q \mid a+1$ or $q = 2kp+1$ for some integer k.

Proof. We know that $a^p \equiv -1 \pmod{q}$, so the order of $a \pmod{q}$ cannot be 1 or p. And since $a^{2p} \equiv 1 \pmod{q}$, the order of $a \pmod{q}$ is either 2 or $2p$.

If the order of a is 2, then $a \equiv -1 \pmod{q}$ so $q \mid a+1$.

On the other hand, if the order of a is $2p$, then $2p \mid \phi(q) = q-1$ so that $q = 2kp+1$. □

10.2.15 Problem 15

Suppose that a has order 4 (mod p). What is the least residue of $(a+1)^4$ (mod p)?

Solution. Since a has order 4, we know that $a^2 \equiv -1 \pmod{p}$, and $a^3 \equiv -a \pmod{p}$. So

$$\begin{aligned}(a+1)^4 &= a^4 + 4a^3 + 6a^2 + 4a + 1\\ &\equiv 1 - 4a - 6 + 4a + 1 \pmod{p}\\ &\equiv -4 \pmod{p}.\end{aligned}$$

Therefore the least residue of $(a+1)^4$ is $p-4$. □

10.2.16 Problem 16

Show that $131071 = 2^{17} - 1$ is prime.

Solution. Suppose $2^{17}-1$ is not prime, and let q be the smallest positive prime divisor. From Theorem 3, we must have $q = 34k+1$ for some integer k. The only possibilities are $q = 103$, 137, 239, and 307 (since $\sqrt{131071} < 363$). One can easily check that none of these divide 131071. Therefore it is prime. □

10.2.17 Problem 17

Show that $(2^{19}+1)/3$ is prime.

Solution. Let $p = (2^{19}+1)/3 = 174763$. By Problem 10.2.14 we know that any positive prime divisor of p other than 3 must have the form $q = 38k+1$ for some integer k. So the only prime divisors we need to check are 3, 191, and 229. All other possibilities are bigger than $\sqrt{p}$. Since none of these three integers are divisors, p must be prime. □

10.2.18 Problem 18

If g is a primitive root of p, show that two consecutive powers of g have consecutive least residues. That is, show that there exists k such that $g^{k+1} \equiv g^k + 1 \pmod{p}$.

Proof. We want to show that $g^k(g-1) \equiv 1 \pmod{p}$ for some integer k. The linear congruence $x(g-1) \equiv 1 \pmod{p}$ has a solution in x since $(g-1, p) = 1$. But every least residue (mod p) can be written in the form g^k for some k by Theorem 5. Thus a solution exists (and is, in fact, unique modulo p). □

10.2.19 Problem 19

If g is a primitive root of p, show that no three consecutive powers of g have consecutive least residues. That is, show that $g^{k+2} \equiv g^{k+1}+1 \equiv g^k+2 \pmod{p}$ is impossible for any k.

Proof. In order for this to be true, we would need

$$g^k(g-1) \equiv 1 \pmod{p} \quad \text{and} \quad g^{k+1}(g-1) \equiv 1 \pmod{p}.$$

But, as mentioned in the previous problem, $x(g-1) \equiv 1 \pmod{p}$ has exactly one solution since $(g-1, p) = 1$. So we must have $g^k \equiv g^{k+1} \pmod{p}$. But then $g^k(g-1) \equiv 0 \pmod{p}$, which is a contradiction. □

10.2.20 Problem 20

(a) Show that if m is a number having primitive roots, then the product of the positive integers less than or equal to m and relatively prime to it is congruent to $-1 \pmod{m}$.

Proof. The case for $m = 2$ is easy to check, so we will assume that $m > 2$. Let g be a primitive root of m. By Theorem 5, the positive integers less than or equal to m and relatively prime to it are given by the powers of g. That is,

$$g, g^2, g^3, \ldots, g^{\phi(m)}$$

is a permutation of these relatively prime integers. Therefore

$$\begin{aligned}\prod_{\substack{1\le i\le m\\(i,m)=1}} i = \prod_{1\le j\le \phi(m)} g^j\\ &= g\cdot g^2\cdot g^3\cdots g^{\phi(m)}\\ &= g^{1+2+\cdots+\phi(m)}\\ &= g^{\phi(m)(\phi(m)+1)/2}.\end{aligned}$$

Since $\phi(m)$ is even $(m>2)$, we can write

$$\begin{aligned}g^{\phi(m)(\phi(m)+1)/2} &= (g^{\phi(m)+1})^{\phi(m)/2}\\ &\equiv g^{\phi(m)/2} \pmod m\\ &\equiv -1 \pmod m.\end{aligned}$$

Therefore the product of the positive integers less than or equal to m and relatively prime to it is congruent to $-1 \pmod m$. □

(b) Show that the result in (a) is not always true if m does not have primitive roots.

Solution. For example, 8 does not have primitive roots, and

$$1\cdot 3\cdot 5\cdot 7 \equiv 1 \not\equiv -1 \pmod 8. \qquad □$$

Chapter 11

Quadratic Congruences

11.1 Exercises

11.1.1 Exercise 1

Convert $2x^2 + 3x + 1 \equiv 0 \pmod 5$ to a quadratic congruence whose first coefficient is 1.

Solution. Since $3 \cdot 2 = 6 \equiv 1 \pmod 5$, we may multiply the above congruence by 3 to get

$$x^2 + 4x + 3 \equiv 0 \pmod 5. \qquad \square$$

11.1.2 Exercise 2

Change the quadratic in Exercise 11.1.1 to the form (3).

Solution. Completing the square gives

$$x^2 + 4x + 4 \equiv 1 \pmod 5,$$

or

$$(x + 2)^2 \equiv 1 \pmod 5. \qquad \square$$

11.1.3 Exercise 3

By inspection, find all the solutions of the congruence in Exercise 11.1.2.

Solution. The congruence $x^2 \equiv 1 \pmod 5$ has solutions $x \equiv 1$ and $x \equiv 4 \pmod 5$, so

$$(x + 2)^2 \equiv 1 \pmod 5$$

has solutions $x \equiv 2$ and $x \equiv 4 \pmod 5$. □

11.1.4 Exercise 4

If $p > 3$, what are the two solutions of $x^2 \equiv 4 \pmod p$?

Solution. We have $p \mid (x - 2)(x + 2)$ so $p \mid (x - 2)$ or $p \mid (x + 2)$. Then $x \equiv 2$ or $x \equiv p - 2 \pmod p$. By Theorem 1, these are the only solutions. □

11.1.5 Exercise 5

For what values of a does $x^2 \equiv a \pmod 7$ have two solutions?

Solution. We find the values of x^2, reduced modulo 7:

x	1	2	3	4	5	6
$x^2 \pmod 7$	1	4	2	2	4	1

From these values, we see that $x^2 \equiv a \pmod 7$ has two solutions when (and only when) $a \equiv 1$, 2, or 4 (mod 7). □

11.1.6 Exercise 6

Find the solutions of $x^2 \equiv 8 \pmod{31}$.

Solution. One may check that this congruence satisfies Euler's Criterion. We have

$$8 \equiv 39 \equiv 70 \equiv 101 \equiv 132 \equiv 2^2 \cdot 33 \pmod{31},$$

and

$$33 \equiv 64 \equiv 8^2 \pmod{31}.$$

Therefore $8 \equiv 16^2 \pmod{31}$ and we see that the quadratic congruence $x^2 \equiv 8 \pmod{31}$ has the two solutions

$$x \equiv -16 \equiv 15 \pmod{31} \quad \text{and} \quad x \equiv 16 \pmod{31}.$$ □

11.1.7 Exercise 7

What is (1/3)? (1/7)? (1/11)? In general, what is $(1/p)$?

Solution. Since 1 is a quadratic residue mod 3, the Legendre symbol $(1/3) = 1$. Similarly, $(1/7) = (1/11) = 1$. In general, for any odd prime p, 1 satisfies Euler's Criterion so we have $(1/p) = 1$. □

11.1.8 Exercise 8

What is (4/5)? (4/7)? $(4/p)$ for any odd prime p?

Solution. It is easy to see by Euler's Criterion that $(4/5) = (4/7) = 1$. And in fact, 2 and $p - 2$ are always solutions to the quadratic congruence $x^2 \equiv 4 \pmod p$ for any odd prime p. Hence $(4/p) = 1$. □

11.1.9 Exercise 9

Induce a theorem from the two preceding exercises.

Solution. It seems that $(a^2/p) = 1$ for any a, provided $p \nmid a$. Indeed, this is easily seen to be true since a itself is a solution to the congruence $x^2 \equiv a^2 \pmod p$. □

11.1.10 Exercise 10

Verify that

$$\text{if}\quad (a/p) = -1 \quad\text{and}\quad a \equiv b \pmod p, \quad\text{then}\quad (b/p) = -1.$$

Proof. Suppose $(a/p) = -1$ and $a \equiv b \pmod p$, but that $(b/p) = 1$. Then $x^2 \equiv b \pmod p$ has a solution. But now $x^2 \equiv a \pmod p$ must have the same solution, which gives a contradiction. Therefore $(b/p) = -1$. □

11.1.11 Exercise 11

Prove that if $p \nmid a$, then $(a^2/p) = 1$, using the fact that $(a/p) \equiv a^{(p-1)/2} \pmod p$.

Proof. From the above, and by Fermat's Theorem, we have that

$$(a^2/p) \equiv (a^2)^{(p-1)/2} \equiv a^{p-1} \equiv 1 \pmod p.$$

Since the Legendre symbol on the left is either 1 or -1, the congruence implies equality. □

11.1.12 Exercise 12

Prove that $(4a/p) = (a/p)$.

Proof. In Exercise 11.1.8 we saw that $(4/p) = 1$. So, by Theorem 3 (C), we have

$$(4a/p) = (4/p)(a/p) = (a/p).$$ □

11.1.13 Exercise 13

Evaluate $(19/5)$ and $(-9/13)$ by using (A) and (B) of Theorem 3.

Solution. We have

$$(19/5) = (4/5) = (2^2/5) = 1$$

and

$$(-9/13) = (4/13) = (2^2/13) = 1.$$ □

11.1.14 Exercise 14

For which of the primes 3, 5, 7, 11, 13, 17, 19, and 23 is -1 a quadratic residue?

Solution. We can apply Theorem 5. Since $5 \equiv 13 \equiv 17 \equiv 1 \pmod 4$, we see that -1 is a quadratic residue $(\text{mod } p)$ for $p = 5$, 13, and 17. It is not a quadratic residue for the remaining primes. □

11.1.15 Exercise 15

Evaluate (6/7) and (2/23)(11/23).

Solution. Note that $7 \equiv 3 \pmod 4$ and $23 \equiv 3 \pmod 4$. Therefore

$$(6/7) = (-1/7) = -1$$

and

$$(2/23)(11/23) = (22/23) = (-1/23) = -1. \qquad \square$$

11.2 Problems

11.2.1 Problem 1

Which of the following congruences have solutions?

$$\begin{array}{ll} x^2 \equiv 7 \pmod{53} & x^2 \equiv 14 \pmod{31} \\ x^2 \equiv 53 \pmod 7 & x^2 \equiv 25 \pmod{997} \end{array}$$

Solution. By the Quadratic Reciprocity Theorem, we have

$$(7/53) = (53/7) = (4/7) = 1.$$

Therefore $x^2 \equiv 7 \pmod{53}$ and $x^2 \equiv 53 \pmod 7$ both have solutions.

Next,

$$(14/31) = (2/31)(7/31).$$

Since $31 \equiv 7 \pmod 8$, we have by Theorem 6 that $(2/31) = 1$. For $(7/31)$ we get, by Quadratic Reciprocity,

$$(7/31) = -(31/7) = -(3/7) = (7/3) = (1/3) = 1.$$

Therefore $(14/31) = 1 \cdot 1 = 1$ and $x^2 \equiv 14 \pmod{31}$ has a solution.

Lastly, $(25/997) = (5^2/997) = 1$, so $x^2 \equiv 25 \pmod{997}$ also has a solution.

□

11.2.2 Problem 2

Which of the following congruences have solutions?

$$\begin{array}{ll} x^2 \equiv 8 \pmod{53} & x^2 \equiv 15 \pmod{31} \\ x^2 \equiv 54 \pmod 7 & x^2 \equiv 625 \pmod{9973} \end{array}$$

Solution. $53 \equiv 5 \pmod 8$, so

$$(8/53) = (2/53)(4/53) = (2/53) = -1,$$

and therefore the congruence $x^2 \equiv 8 \pmod{53}$ has no solutions.

Next,

$$(15/31) = (3/31)(5/31) = -(31/3)(31/5) = -(1/3)(1/5) = -1,$$

so the congruence $x^2 \equiv 15 \pmod{31}$ has no solutions.

$$(54/7) = (5/7) = (7/5) = (2/5) = -1,$$

so $x^2 \equiv 54 \pmod 7$ has no solutions.

Lastly,

$$(625/9973) = (25^2/9973) = 1,$$

so $x^2 \equiv 625 \pmod{9973}$ does have a solution. □

11.2.3 Problem 3

Find solutions for the congruences in Problem 11.2.1 that have them.

Solution. For $x^2 \equiv 7 \pmod{53}$, we have

$$\begin{gathered} 7 \equiv 60 \equiv 2^2 \cdot 15 \pmod{53}, \\ 15 \equiv 68 \equiv 2^2 \cdot 17 \pmod{53}, \\ 17 \equiv 70 \equiv 123 \equiv 176 \equiv 4^2 \cdot 11 \pmod{53}, \end{gathered}$$

and

$$11 \equiv 64 \equiv 8^2 \pmod{53}.$$

Since $2 \cdot 2 \cdot 4 \cdot 8 = 128 \equiv 22 \pmod{53}$, the congruence $x^2 \equiv 7 \pmod{53}$ has the two solutions

$$x \equiv 22 \pmod{53} \quad \text{and} \quad x \equiv 31 \pmod{53}.$$

Next, $53 \equiv 4 \equiv 2^2 \pmod 7$, so the congruence $x^2 \equiv 53 \pmod 7$ has the two solutions

$$x \equiv 2 \pmod 7 \quad \text{and} \quad x \equiv 5 \pmod 7.$$

Modulo 31, we have

$$14 \equiv 45 \equiv 3^2 \cdot 5 \pmod{31}$$

and

$$5 \equiv 36 \equiv 6^2 \pmod{31}.$$

Since $3 \cdot 6 = 18$, the congruence $x^2 \equiv 14 \pmod{31}$ has the two solutions

$$x \equiv 13 \pmod{31} \quad \text{and} \quad x \equiv 18 \pmod{31}.$$

Finally, the congruence $x^2 \equiv 25 \pmod{997}$ is easily seen to have solutions

$$x \equiv 5 \pmod{997} \quad \text{and} \quad x \equiv 992 \pmod{997}.$$ □

11.2.4 Problem 4

Find solutions for the congruences in Problem 11.2.2 that have them.

Solution. Only $x^2 \equiv 625 \pmod{9973}$ has a solution. Since $625 = 25^2$, we see that the two solutions to the congruence are

$$x \equiv 25 \pmod{9973} \quad \text{and} \quad x \equiv 9948 \pmod{9973}.$$ □

11.2.5 Problem 5

Calculate (33/71), (34/71), (35/71), and (36/71).

Solution. Note that $71 \equiv 3 \pmod 4$ and $71 \equiv 7 \pmod 8$. Therefore

$$\begin{aligned}(33/71) &= (3/71)(11/71) = (71/3)(71/11)\\ &= (2/3)(5/11) = (2/3)(11/5)\\ &= (2/3)(1/5) = -1 \cdot 1 = -1,\\ (34/71) &= (2/71)(17/71) = (71/17)\\ &= (3/17) = (17/3)\\ &= (2/3) = -1,\\ (35/71) &= (5/71)(7/71) = -(71/5)(71/7)\\ &= -(1/5)(1/7) = -1,\end{aligned}$$

and

$$(36/71) = 1.$$ □

11.2.6 Problem 6

Calculate (33/73), (34/73), (35/73), and (36/73).

Solution. Note that $73 \equiv 1 \pmod 4$ and $73 \equiv 1 \pmod 8$. So

$$\begin{aligned}(33/73) &= (3/73)(11/73)\\ &= (73/3)(73/11)\\ &= (1/3)(7/11)\\ &= -(11/7) = -(4/7)\\ &= -1,\\ (34/73) &= (2/73)(17/73)\\ &= (73/17) = (5/17)\\ &= (17/5) = (2/5)\\ &= -1,\\ (35/73) &= (5/73)(7/73)\\ &= (73/5)(73/7)\\ &= (3/5)(3/7)\\ &= -(5/3)(7/3)\\ &= -(2/3)(1/3) = 1,\\ (36/73) &= 1.\end{aligned}$$ □

11.2.7 Problem 7

Solve $2x^2 + 3x + 1 \equiv 0 \pmod 7$ and $2x^2 + 3x + 1 \equiv 0 \pmod{101}$.

Solution. Since $2 \cdot 4 \equiv 1 \pmod 7$ we may multiply the first congruence by 4 to get

$$x^2 + 5x + 4 \equiv 0 \pmod 7.$$

Note that $5 \equiv -2 \pmod 7$, so

$$x^2 - 2x + 4 \equiv 0 \pmod 7.$$

Completing the square now gives

$$(x-1)^2 \equiv -3 \pmod 7.$$

So $(x-1)^2 \equiv 4 \pmod 7$ and we get $x \equiv 3 \pmod 7$ or $x \equiv 6 \pmod 7$.

For the second congruence, we have $2 \cdot 51 \equiv 1 \pmod{101}$, so multiplying by 51 gives

$$x^2 + 52x + 51 \equiv 0 \pmod{101}.$$

Note that $26^2 = 676 \equiv 70 \pmod{101}$, so we can rearrange to get

$$x^2 + 52x + 70 \equiv 19 \pmod{101}$$

or

$$(x+26)^2 \equiv 19 \pmod{101}.$$

Note that $19 \equiv 625 \pmod{101}$, so $x + 26 \equiv \pm 25 \pmod{101}$. The two solutions of the second congruence are therefore

$$x \equiv 50 \pmod{101} \quad \text{and} \quad x \equiv 100 \pmod{101}.$$ □

11.2.8 Problem 8

Solve $3x^2 + x + 8 \equiv 0 \pmod{11}$ and $3x^2 + x + 52 \equiv 0 \pmod{11}$.

Solution. Note that both congruences are the same, since $52 \equiv 8 \pmod{11}$. Now, because 4 is the multiplicative inverse of 3 (mod 11), we have

$$x^2 + 4x + 10 \equiv 0 \pmod{11}.$$

Rearranging, we get

$$x^2 + 4x + 4 \equiv 5 \pmod{11}$$

or

$$(x+2)^2 \equiv 5 \pmod{11}.$$

Since $5 \equiv 16 \pmod{11}$, we get

$$x + 2 \equiv \pm 4 \pmod{11}$$

so that $x \equiv 2$ or $x \equiv 5 \pmod{11}$. □

11.2.9 Problem 9

Calculate (1234/4567) and (4321/4567).

Solution. We have

$$(1234/4567) = (2/4567)(617/4567).$$

Since $4567 \equiv 7 \pmod 8$, we know $(2/4567) = 1$ by Theorem 6. And since $617 \equiv 1 \pmod 4$, we may apply Quadratic Reciprocity to get

$$(617/4567) = (4567/617) = (248/617) = (8/617)(31/617).$$

Now $617 \equiv 1 \pmod 8$, so $(8/617) = (2/617) = 1$. Again, using Quadratic Reciprocity, we get

$$\begin{aligned}(31/617) = (617/31) = (28/31) = (4/31)(7/31)\\ = -(31/7) = -(3/7) = (7/3) = (1/3) = 1.\end{aligned}$$

Therefore

$$(1234/4567) = 1.$$

Next,

$$\begin{aligned}(4321/4567) &= (29/4567)(149/4567)\\ &= (4567/29)(4567/149)\\ &= (14/29)(97/149)\\ &= (2/29)(7/29)(97/149).\end{aligned}$$

Now $(2/29) = -1$ by Theorem 6. For (7/29), we get

$$(7/29) = (29/7) = (1/7) = 1.$$

For (97/149), we get

$$\begin{aligned}(97/149) &= (149/97) = (52/97)\\ &= (4/97)(13/97)\\ &= (97/13) = (6/13)\\ &= (2/13)(3/13).\end{aligned}$$

$(2/13) = -1$ by Theorem 6 and $(3/13) = (13/3) = (1/3) = 1$. Putting everything together, we get

$$(4321/4567) = -1 \cdot 1 \cdot -1 \cdot 1 = 1. \qquad \square$$

11.2.10 Problem 10

Calculate (1356/2467) and (6531/2467).

Solution. In the same fashion as the previous exercise, we may determine that

$$(1356/2467) = 1 \quad \text{and} \quad (6531/2467) = -1. \qquad \square$$

11.2.11 Problem 11

Show that if $p = q + 4a$ (p and q are odd primes), then $(p/q) = (a/q)$.

Proof. Since $p \equiv 4a \pmod{q}$, we have

$$(p/q) = (4a/q) = (4/q)(a/q) = (a/q). \qquad \square$$

11.2.12 Problem 12

Show that if $p = 12k + 1$ for some k, then $(3/p) = 1$.

Proof. $p \equiv 1 \pmod 4$, so we may apply Quadratic Reciprocity to get

$$(3/p) = (p/3) = ((12k + 1)/3) = (1/3) = 1. \qquad \square$$

11.2.13 Problem 13

Show that Theorem 6 could also be written $(2/p) = (-1)^{(p^2-1)/8}$ for odd primes p.

Proof. If $p \equiv 1 \pmod 8$ then $p = 8k + 1$ for some k and we get

$$\frac{p^2 - 1}{8} = \frac{(8k + 1)^2 - 1}{8} = \frac{64k^2 + 16k}{8} = 8k^2 + 2k.$$

If instead $p \equiv 7 \pmod 8$ then $p = 8k + 7$ for some k and

$$\frac{p^2 - 1}{8} = \frac{64k^2 + 112k + 48}{8} = 8k^2 + 14k + 6.$$

In either case, $(p^2 - 1)/8$ is even, so $(-1)^{(p^2-1)/8} = 1 = (2/p)$.

On the other hand, if $p \equiv 3 \pmod 8$ then $p = 8k + 3$ and we have

$$\frac{p^2 - 1}{8} = \frac{64k^2 + 48k + 8}{8} = 8k^2 + 6k + 1,$$

and if $p \equiv 5 \pmod 8$ then $p = 8k + 5$ and

$$\frac{p^2 - 1}{8} = \frac{64k^2 + 80k + 24}{8} = 8k^2 + 10k + 3.$$

In these latter two cases, $(p^2 - 1)/8$ is odd and we get

$$(-1)^{(p^2-1)/8} = -1 = (2/p). \qquad \square$$

11.2.14 Problem 14

Show that the quadratic reciprocity theorem could also be written

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$$

for odd primes p and q.

Proof. If $p \equiv q \equiv 3 \pmod 4$, then $(p/q)(q/p) = -1$. In this case, $p = 4m + 3$ and $q = 4n + 3$ for some m and n, and we get

$$\begin{aligned}\frac{(p-1)(q-1)}{4} &= \frac{(4m+2)(4n+2)}{4}\\ &= \frac{16mn+8m+8n+4}{4}\\ &= 4mn+2m+2n+1.\end{aligned}$$

This number is odd, so

$$(-1)^{(p-1)(q-1)/4} = -1 = (p/q)(q/p).$$

Next, if $p \equiv 1 \pmod 4$ then $p = 4m + 1$ for some m and

$$\frac{(p-1)(q-1)}{4} = \frac{4m(q-1)}{4} = m(q-1).$$

Now, since q is an odd prime, $q - 1$ is even. Therefore

$$(-1)^{(p-1)(q-1)/4} = 1 = (p/q)(q/p).$$

Arguing by symmetry, we see that this is also true when $q \equiv 1 \pmod 4$.

In every case, $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$. □

11.2.15 Problem 15

Student A says, "I've checked all the way up to 100 and I still haven't found n so that n^2+1 is divisible by 7. I'm tired now—I'll find one tomorrow." Student B says, after a few seconds of reflection, "No you won't." How did B know so quickly?

Solution. A is looking for n such that $n^2 \equiv -1 \pmod 7$. But we know from Theorem 5 that $(-1/7) = -1$ (since $7 \equiv 3 \pmod 4$). This shows that -1 is a quadratic nonresidue (mod 7), so what A seeks is impossible to find. □

11.2.16 Problem 16

Show that if a is a quadratic residue (mod p) and $ab \equiv 1 \pmod p$ then b is a quadratic residue (mod p).

Proof. Suppose $(a/p) = 1$ and $ab \equiv 1 \pmod p$. Then

$$(b/p) = (a/p)(b/p) = (ab/p) = (1/p) = 1.$$

Therefore b is a quadratic residue (mod p). □

11.2.17 Problem 17

Does $x^2 \equiv 211 \pmod{159}$ have a solution? Note that 159 is not prime.

Solution. Since $211 \equiv 529 \equiv 23^2 \pmod{159}$, we see that the congruence does have solutions. In particular, $x \equiv 23$ and $x \equiv 136 \pmod{159}$ are solutions.

These are not the only solutions, however. We also have $211 \equiv 5776 \equiv 76^2 \pmod{159}$, giving $x \equiv 76$ and $x \equiv 83 \pmod{159}$ as additional solutions. □

11.2.18 Problem 18

Prove that if $p \equiv 3 \pmod 8$ and $(p-1)/2$ is prime, then $(p-1)/2$ is a quadratic residue $(\text{mod } p)$.

Proof. Let $q = (p-1)/2$ be prime. Since $p \equiv 3 \pmod 8$, we have $p = 8k+3$ for some integer k. Then

$$q = \frac{p-1}{2} = \frac{8k+2}{2} = 4k+1.$$

Hence $q \equiv 1 \pmod 4$ and q is an odd prime. By Quadratic Reciprocity, we have that $(q/p) = (p/q)$.

Now observe that

$$p = 1 + 2 \cdot \frac{p-1}{2} = 1 + 2q,$$

which can be rewritten as $p \equiv 1 \pmod q$. Therefore $(p/q) = (1/q) = 1$. So, by the result in the preceding paragraph, $(q/p) = 1$ and we see that $q = (p-1)/2$ is a quadratic residue $(\text{mod } p)$. □

11.2.19 Problem 19

Generalize Problem 11.2.16 by finding what condition on r will guarantee that if a is a quadratic residue $(\text{mod } p)$ and $ab \equiv r \pmod p$, then b is a quadratic residue $(\text{mod } p)$.

Solution. Since $(a/p) = 1$, we get

$$1 = (b/p) = (a/p)(b/p) = (ab/p) = (r/p).$$

We see that the desired condition on r is that r is itself a quadratic residue $(\text{mod } p)$. □

11.2.20 Problem 20

Suppose that $p = q+4a$, where p and q are odd primes. Show that $(a/p) = (a/q)$.

Proof. Note that $p \equiv q \pmod 4$, $p \equiv 4a \pmod q$, and $q \equiv -4a \pmod p$.

There are two cases. First, if $p \equiv q \equiv 1 \pmod 4$, then

$$(a/p) = (-1/p)(4/p)(a/p) = (-4a/p) = (q/p)$$

and

$$(a/q) = (4/q)(a/q) = (4a/q) = (p/q).$$

The Quadratic Reciprocity Theorem then shows that $(a/p) = (a/q)$.

On the other hand, if $p \equiv q \equiv 3 \pmod 4$, then

$$(a/p) = -(-1/p)(4/p)(a/p) = -(-4a/p) = -(q/p)$$

and

$$(a/q) = (4a/q) = (p/q).$$

Again, Quadratic Reciprocity proves the result. □