Daniel Rosenthal, David Rosenthal, Peter Rosenthal

A Readable Introduction to Real Mathematics

Solutions Manual

Springer

Preface

This manual contains solutions to selected exercises from "A Readable Introduction to Real Mathematics", Springer, 2014. More information about that book, including reviews and how to order hard or electronic copies, can be found at: http://www.springer.com/gp/book/9783319056531

The authors would greatly appreciate being informed of any errors or improvements in the solutions by e-mail to any of the addresses given below.

Daniel Rosenthal: danielkitairosenthal@gmail.com

David Rosenthal: rosenthd@stjohns.edu

Peter Rosenthal: rosent@math.toronto.edu

Toronto, ON, Canada — *Daniel Rosenthal*
Queens, NY, USA — *David Rosenthal*
Toronto, ON, Canada — *Peter Rosenthal*

August 17, 2016

Contents

Chapter 1
Introduction to the Natural Numbers

Solutions to Selected Exercises

1. Show that the following are composite numbers:

(c) 20,101,116

Answer: 20,101,116 is divisible by 2.

2. Which of the following are prime numbers?

(c) 537

Answer: Since 537 is divisible by 3, it is not prime.

6. Find a prime number p such that the number $(2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1$ is not prime.

Answer: The smallest such prime is $p = 13$. Note that $2 \cdot 3 \cdots 13 = 30030$ and $30031 = 59 \cdot 509$.

7. Suppose that p, $p+2$, and $p+4$ are prime numbers. Prove that $p = 3$. [Hint: Why can't p be 5 or 7?]

Answer: If $p = 3$, then p, $p+2 = 5$ and $p+4 = 7$ are all prime. Conversely, suppose $p \neq 3$. Then, since p is prime, p is not divisible by 3. Thus, p leaves a remainder of 1 or 2 when divided by 3. If p leaves a remainder of 1 when divided by 3, then $p = 3m+1$ for some nonnegative integer m, so $p+2 = 3m+3$ is divisible by 3. Since $p+2$ is greater than 3, this contradicts the fact that $p+2$ is prime. If p leaves a remainder of 2 when divided by 3, then $p = 3m+2$ for some nonnegative integer m, and so $p+4 = 3m+6$ is divisible

by 3, which contradicts the fact that $p+4$ is prime. Therefore, for p, $p+2$ and $p+4$ to all be prime, p must equal 3.

8. Prove that, for every natural number $n > 2$, there is a prime number between n and $n!$. (Recall that $n!$ is defined to be $n(n-1)(n-2)\cdots 2\cdot 1$.) [Hint: There is a prime number that divides $n!-1$.]
Note that this gives an alternate proof that there are infinitely many prime numbers.

Answer: Let n be a natural number greater than 2. Let p be any prime number that divides $n!-1$. Since p divides $n!-1$, p does not divide $n!$. It follows that p is not any natural number less than or equal to n, and so p is a natural number greater than n. Also, p is less than or equal to $n!-1$, since p divides $n!-1$. It follows that $n < p < n!$, so there is a prime between n and $n!$.

9. Prove that, for every natural number n, there are n consecutive composite numbers. [Hint: $(n+1)!+2$ is a composite number.]

Answer: Let n be any natural number. For any natural number $k \leq n+1$, $(n+1)!$ is a multiple of k. Then $(n+1)!+k$ is k more than a multiple of k, so $(n+1)!+k$ is a multiple of k as well. Thus $(n+1)!+2$, $(n+1)!+3$, $(n+1)!+4$, $\ldots$, $(n+1)!+n+1$ are n consecutive numbers all of which are composite.

10. Show that a natural number has an odd number of different factors if and only if it is a perfect square (i.e., it is the square of another natural number).

Answer: Let m be a natural number whose distinct factors are $a_1, \ldots, a_n$. For each a_i, there is an a_j such that $a_i \cdot a_j = m$. So each factor can be paired with its complement, and if m is not a perfect square then each a_i is paired with a different a_j, so there are an even number of factors. If m is a perfect square, then there is an a_k such that $a_k^2 = m$. All the other a_i can be paired with their complements, but as a_k only appears once in the list of factors, it follows that there are an odd number of different factors.

Chapter 2
Mathematical Induction

Solutions to Selected Exercises

2. Prove, using induction, that for every natural number n:

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

Answer: This is true when $n=1$, since $\frac{1}{1\cdot 2}=\frac{1}{1+1}$. Suppose it is true for $n=k$, i.e.:

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k\cdot(k+1)}=\frac{k}{k+1}$$

Then:

$$\begin{aligned}\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k\cdot(k+1)}+\frac{1}{(k+1)\cdot(k+2)} &= \frac{k}{k+1}+\frac{1}{(k+1)(k+2)}\\ &= \frac{k(k+2)+1}{(k+1)(k+2)}\\ &= \frac{k^2+2k+1}{(k+1)(k+2)}\\ &= \frac{(k+1)(k+1)}{(k+1)(k+2)}\\ &= \frac{k+1}{k+2}\end{aligned}$$

Therefore, the formula holds for $n=k+1$, and it follows by mathematical induction that the formula is true for all natural numbers n.

7. Prove by mathematical induction that 3 divides n^3+2n, for every natural number n.

Answer: For the case $n = 1$, $n^3 + 2n = 1 + 2 = 3$, so the statement holds in this case. Suppose it holds for the natural number k. Then $(k+1)^3 + 2(k+1) = (k^3 + 3k^2 + 3k + 1) + (2k + 2) = k^3 + 2k + 3k + 3k^2 + 3 = (k^3 + 2k) + 3(k + k^2 + 1)$. Since $k^3 + 2k$ is divisible by 3, by the inductive hypothesis, and $3(k + k^2 + 1)$ is divisible by 3, $(k+1)^3 + 2(k+1)$ is divisible by 3, and the result follows by induction.

8. Show that $3^n > n^2$ for every natural number n.

Answer: For $n = 1$, $3^n = 3$ while $n^2 = 1$, so the inequality holds in this case. For $n = 2$, $3^n = 9 > 4 = n^2$, so it is true in this case as well. Suppose it is true for a natural number $k \geq 2$, that is, $3^k > k^2$. Then $3^{k+1} = 3 \cdot 3^k > 3k^2$, while $(k+1)^2 = k^2 + 2k + 1$. What remains is to show that $3k^2 > k^2 + 2k + 1$ or, equivalently, $2k^2 > 2k + 1$. This is equivalent to $2k^2 - 2k > 1$, but $2k^2 - 2k = 2k(k-1)$, which is clearly greater than 1 for $k \geq 2$.

12. Prove the Well-Ordering Principle using the Principle of Complete Mathematical Induction.

Answer: It must be shown that the only set without a smallest element is the empty set. Let $\mathscr{T}$ be a set of natural numbers without a smallest element. Then 1 is not in $\mathscr{T}$, or else 1 would be the smallest element. Suppose the numbers 1 through k are not in $\mathscr{T}$. Then $k+1$ is also not in $\mathscr{T}$, or else $k+1$ would be the smallest element in $\mathscr{T}$. So if $\mathscr{S}$ is the set of natural numbers that are not in $\mathscr{T}$, then 1 is in $\mathscr{S}$ and $k+1$ is in $\mathscr{S}$ whenever the numbers 1 through k are in $\mathscr{S}$. It follows from the Principle of Complete Mathematical Induction that $\mathscr{S}$ is the set of all natural numbers. Therefore, there are no natural numbers in $\mathscr{T}$; that is, $\mathscr{T}$ is the empty set.

14. Define the nth *Fermat number*, F_n, by $F_n = 2^{2^n} + 1$ for $n = 0, 1, 2, 3, \ldots$. The first few Fermat numbers are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$.

(a) Prove by induction that $F_0 \cdot F_1 \cdots F_{n-1} + 2 = F_n$, for $n \geq 1$.
(b) Use the formula in part (a) to prove that there are an infinite number of primes, by showing that no two Fermat numbers have any prime factors in common. [Hint: For each F_n, let p_n be a prime divisor of F_n and show that $p_{n_1} \neq p_{n_2}$ if $n_1 \neq n_2$.]

Answer: (a) For $n = 1$ the left hand side is $3 + 2$ while the right hand side is 5, so the statement holds. Suppose the statement is true for a natural number m. Then $F_0 \cdot F_1 \cdots F_{m-1} + 2 = F_m$, so:

$$\begin{aligned} F_0 \cdot F_1 \cdots F_{m-1} &= F_m - 2 \\ &= 2^{2^m} + 1 - 2 \\ &= 2^{2^m} - 1 \end{aligned}$$

It follows that:

$$\begin{aligned} F_0 \cdot F_1 \cdots F_{m-1} \cdot F_m &= (2^{2^m} - 1) \cdot F_m \\ &= (2^{2^m} - 1)(2^{2^m} + 1) \\ &= 2^{2^{m+1}} - 1 \\ &= F_{m+1} - 2 \end{aligned}$$

Therefore:

$$F_0 \cdot F_1 \cdots F_{m-1} \cdot F_m + 2 = F_{m+1}$$

and the statement holds for $m+1$.

(b) Let n and m be two different natural numbers, and suppose that F_n and F_m share the prime factor p. One of n and m is greater than the other; assume $n > m$. Then, by the formula from part (a):

$$F_n = F_0 \cdot F_1 \cdots F_{n-1} + 2$$

Since F_m is one of the F_i on the right hand side of this equation, p divides the product on the right hand side. Since p also divides F_n, it follows that p divides 2, and hence $p = 2$. On the other hand, every Fermat number is odd, so 2 is not a factor of any Fermat number. Since no two Fermat numbers have a common prime factor, this provides another proof that there are an infinite number of primes.

15. The sequence of Fibonacci numbers is defined as follows: $x_1 = 1$, $x_2 = 1$, and, for $n > 2$, $x_n = x_{n-1} + x_{n-2}$. Prove that:

$$x_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

for every natural number n. [Hint: Use the fact that $x = \frac{1+\sqrt{5}}{2}$ and $x = \frac{1-\sqrt{5}}{2}$ both satisfy $1 + x = x^2$.]

Answer: To verify the hint, note that $\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2}$, and $\left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{6-2\sqrt{5}}{4} = \frac{3-\sqrt{5}}{2} = 1 + \frac{1-\sqrt{5}}{2}$.

For the base case of the induction, $x_1 = 1$ by definition and:

$$\frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right) - \left(\frac{1-\sqrt{5}}{2} \right) \right] = \frac{1}{\sqrt{5}} \left(\frac{2\sqrt{5}}{2} \right) = 1$$

Suppose the formula holds for all natural numbers less than or equal to k. Then:

$$\begin{aligned} x_{k+1} &= x_k + x_{k-1} \\ &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right] \\ &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(1+\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(1+\frac{1-\sqrt{5}}{2}\right)\right] \end{aligned}$$

and, by the hint, this equals:

$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{1-\sqrt{5}}{2}\right)^2\right]$$

Since this is equal to the right hand side of the formula for $n = k+1$, the result follows by induction.

Chapter 3
Modular Arithmetic

Solutions to Selected Exercises

1. Find a solution x to each of the following congruences. ("Solution" means integer solution.)

(a) $2x \equiv 7 \pmod{11}$

Answer: If there is a solution, there would have to be a solution within the set $\{0, 1, \ldots, 10\}$. Trying each of those numbers gives the solution $x = 9$.

2. For each of the following congruences, either find a solution or prove that no solution exists.

(a) $39x \equiv 13 \pmod{5}$
(b) $95x \equiv 13 \pmod{5}$
(e) $4x^3 + 2x \equiv 7 \pmod{5}$

Answer: (a) Note that if there is a solution to a congruence modulo 5, there would have to be a solution among the set $\{0, 1, 2, 3, 4\}$, since every integer is congruent to one of those numbers modulo 5. Since $39 \equiv 4 \pmod{5}$, and $13 \equiv 3 \pmod{5}$, the equation is equivalent to $4x \equiv 3 \pmod{5}$. Trying each number from $\{0, 1, 2, 3, 4\}$ yields the solution $x = 2$.

(b) No solution exists. None of the numbers from $\{0, 1, 2, 3, 4\}$ satisfy the congruence. Another solution is as follows. For any x, $95x \equiv 0 \pmod{5}$, because $95 \equiv 0 \pmod{5}$. Since $13 \equiv 3 \pmod{5}$, there is no solution.

(e) No solution exists. None of the numbers from $\{0, 1, 2, 3, 4\}$ satisfy the congruence.

3. Find the remainder when:

(c) 243^{101} is divided by 8.
(g) $5! \cdot 181 - 866 \cdot 332$ is divided by 6.

Answer: (c) First note that $243 \equiv 3 \pmod 8$, so $243^2 \equiv 3^2 \equiv 1 \pmod 8$. Then $243^{100} \equiv 1 \pmod 8$, so $243^{101} \equiv 243 \equiv 3 \pmod 8$. Therefore the remainder is 3.

(g) The remainder is 2. To see this, note that $866 \equiv 2 \pmod 6$ and $332 \equiv 2 \pmod 6$, so $-866 \cdot 332 \equiv -4 \equiv 2 \pmod 6$. Since $5! = 20 \cdot 6$, $5! \equiv 0 \pmod 6$, therefore $5! \cdot 181 \equiv 0 \pmod 6$. Then, $5! \cdot 181 - 866 \cdot 332 \equiv 2 \pmod 6$.

7. Suppose that 7^{22} is written out in the ordinary way. What is its last digit?

Answer: Note that the last digit (i.e., the units' digit) of every natural number is the remainder that the natural number leaves upon division by 10. In the present case, since $7^2 \equiv 9 \pmod{10}$, it follows that $7^3 \equiv 63 \equiv 3 \pmod{10}$ and $7^4 \equiv 21 \equiv 1 \pmod{10}$. Then $7^{20} \equiv 1$ and so $7^{22} \equiv 7^2 \equiv 9 \pmod{10}$. Therefore, the remainder upon division by 10 is 9, hence, the last digit is 9.

13. Find the units' digit of 27493^{6782}.

Answer: This is equivalent to finding the remainder that 27493^{6782} leaves upon division by 10. To find this, first note that $27493 \equiv 3 \pmod{10}$, so $27493^2 \equiv 9 \equiv -1 \pmod{10}$, and $27493^4 \equiv 1 \pmod{10}$. It follows that $27493^{6780} \equiv 1 \pmod{10}$, since 6780 is a multiple of 4. Therefore, $27493^{6782} \equiv (27493^{6780})(27493^2) \equiv 9 \cdot 1 \pmod{10}$ and the units' digit is 9.

15. Prove that, for every pair of natural numbers m and n, m^2 is congruent to n^2 modulo $(m+n)$.

Answer: Since $m^2 - n^2 = (m-n)(m+n)$, it follows that $m^2 - n^2$ is divisible by $m+n$. Thus, $m^2 \equiv n^2 \pmod{m+n}$.

17. Prove that 7 divides $8^{2n+1} + 6^{2n+1}$, for every natural number n.

Answer: Note that $8 \equiv 1 \pmod 7$, so $8^{2n+1} \equiv 1 \pmod 7$. Also, $6 \equiv -1 \pmod 7$, so $6^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod 7$. Thus, $8^{2n+1} + 6^{2n+1} \equiv 1 + (-1) \equiv 0 \pmod 7$.
Alternatively, this can be shown by induction. Since $8^3 + 6^3 = 512 + 216 = 728 = 7 \cdot 104$, the formula holds for $n = 1$. Now assume that $8^{2k+1} + 6^{2k+1}$ is

divisible by 7. Then $8^{2(k+1)+1} + 6^{2(k+1)+1} = 8^2(8^{2k+1} + 6^{2k+1}) - 28(6^{2k+1})$, which is congruent to $(0+0)$ modulo 7. Therefore the statement is true for $k+1$.

18. Prove that a natural number that is congruent to 2 modulo 3 has a prime factor that is congruent to 2 modulo 3.

Answer: Let m be an integer greater than 1 such that $m \equiv 2 \pmod 3$. If m is prime, then m itself is the prime factor congruent to 2 modulo 3. If m is not prime, then m can be factored into primes $q_1 \cdot q_2 \cdots q_n$. If all of the prime factors were congruent to 1 mod 3, then m would be congruent to $1^n \equiv 1$ mod 3, and if any prime factor was congruent to 0 mod 3 then m would be congruent to 0 as well. Thus, there must be at least one prime factor of m that is not congruent to 1 mod 3 *and* that prime factor cannot be congruent to 0 mod 3. Since every number is congruent to one of 0, 1, 2 modulo 3, it follows that at least one prime factor must be congruent to 2 mod 3.

22. Show that there do not exist natural numbers x and y such that $x^2 + y^2 = 4003$. [Hint: Begin by determining which of the numbers $\{0,1,2,3\}$ can be congruent to $x^2 \pmod 4$.]

Answer: Suppose there were such x and y. Then $x^2 + y^2 \equiv 4003 \equiv 3 \pmod 4$. However, since $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 0$ and $3^2 \equiv 1$ modulo 4, the only possible numbers in $\{0,1,2,3\}$ that $x^2 + y^2$ could be congruent to modulo 4 are $0,1,2$.

24. Prove that there are an infinite number of primes of the form $4k+3$ with k a natural number. [Hint: If $p_1, p_2, \ldots, p_n$ are n such primes, show that $(4 \cdot p_1 \cdot p_2 \cdots p_n) - 1$ has at least one prime divisor of the given form.]

Answer: We first prove the equivalent statement for primes of the form $4k+3$ where k is any nonnegative integer (thus including the case $k = 0$). Since $4 \cdot 1 + 3 = 7$, and 7 is prime, there is at least one prime of that form. Let $p_1, \ldots, p_n$ be primes of the given form. Factor $4(p_1 \cdots p_n) - 1$ into primes $q_1 \cdots q_j$. For each p_i, $4(p_1 \cdots p_n) - 1$ is one less than a multiple of p_i, so there are no p_i and q_t with $p_i = q_t$. Also $4(p_1 \cdots p_n) - 1 \equiv -1 \equiv 3 \pmod 4$, so $q_1 \cdots q_j \equiv 3 \pmod 4$. If none of the q_t's were congruent to 3 modulo 4, then each would be congruent to 0, 1, or 2 modulo 4, and their product would be congruent to 0, 1, or 2 modulo 4. So one of the q_t's must be congruent to 3 modulo 4, and so $q_t = 4k+3$ for some integer k. Therefore, given any n primes of the given form, it is always possible to find another one. Thus, there are infinitely many of them. In particular, there are infinitely many where k is a natural number (since the case $k = 0$ only gives one prime, 3).

27. Show that, if x, y and z are integers such that $x^2 + y^2 = z^2$, then at least one of $\{x, y, z\}$ is divisible by 2, at least one of $\{x, y, z\}$ is divisible by 3, and at least one of $\{x, y, z\}$ is divisible by 5.

Answer: Suppose that none are divisible by 2. Then each of x, y and z is congruent to 1 modulo 2, so $x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod 2$. However $x^2 + y^2 \equiv z^2 \pmod 2$, giving the equation $1 + 1 \equiv 1 \pmod 2$, a contradiction. Therefore at least one is divisible by 2. Suppose none are divisible by 3. Then each is congruent to 1 or 2 modulo 3. Since $2^2 \equiv 1 \equiv 1^2 \pmod 3$, it follows that each of x^2, y^2 and z^2 is congruent to 1 modulo 3, and the equation $x^2 + y^2 \equiv z^2 \pmod 3$ gives $1 + 1 \equiv 1 \pmod 3$, a contradiction. Finally, suppose none are divisible by 5. Then each is congruent to 1, 2, 3, or 4 modulo 5. Since $1^2 \equiv 1 \pmod 5$, $2^2 \equiv 4 \pmod 5$, $3^2 \equiv 4 \pmod 5$ and $4^2 \equiv 1 \pmod 5$, it follows that each of x^2, y^2 and z^2 is congruent to 1 or 4 modulo 5. Substituting these into the equation $x^2 + y^2 \equiv z^2 \pmod 5$ shows that this is not possible, as $1 + 1 \equiv 2 \pmod 5$, $1 + 4 \equiv 4 + 1 \equiv 0 \pmod 5$, and $4 + 4 \equiv 3 \pmod 5$.

Chapter 4
The Fundamental Theorem of Arithmetic

Solutions to Selected Exercises

1. Find the canonical factorization into primes of each of the following:

(a) 52
(c) 47
(e) $122 \cdot 54$
(h) $112 + 224$

Answer: (a) $52 = 2^2 \cdot 13$.

(c) 47, since 47 is prime.

(e) $122 \cdot 54 = (2 \cdot 61) \cdot (2 \cdot 3^3) = 2^2 \cdot 3^3 \cdot 61$.

(h) $112 + 224 = 112 \cdot (1 + 2) = 2^4 \cdot 3 \cdot 7$.

2. Find natural numbers x, y and z such that

(b) $50 \cdot 2^y \cdot 7^z = 5^x \cdot 2^3 \cdot 14$

Answer: $50 \cdot 2^y \cdot 7^z = (2 \cdot 5^2) \cdot 2^y \cdot 7^z = 2^{y+1} \cdot 5^2 \cdot 7^z$ and $5^x \cdot 2^3 \cdot 14 = 5^x \cdot 2^3 \cdot (2 \cdot 7) = 2^4 \cdot 5^x \cdot 7$. Therefore, by the uniqueness of prime factorization, $x = 2$, $y = 3$, $z = 1$.

5. Find the smallest natural numbers x and y such that

(a) $7^2 x = 5^3 y$

Answer: By the uniqueness of prime factorization (Theorem 4.1.1), x must have 5^3 as a factor and y must have 7^2 as a factor. So the smallest pair (x, y) is $(5^3, 7^2) = (125, 49)$.

6. Find nonnegative integers w, x, y and z such that $17^2 25^2 2^z = 10^x 34^y 7^w$.

Answer: Factoring both sides into primes gives $2^z 5^4 17^2 = 2^{x+y} 5^x 7^w 17^y$. On the left hand side there is no 7, so $w = 0$. Comparing the powers of 5 shows that $x = 4$, and comparing the powers of 17 shows that $y = 2$. Then $z = x + y = 6$.

7. Suppose that p is a prime number and p does not divide a. Prove that the congruence $ax \equiv 1 \pmod{p}$ has a solution. (This proves that a has a *multiplicative inverse modulo p*.)

Answer: This is an immediate consequence of Fermat's Theorem (5.1.2). It can also be proved directly using ideas similar to those used in the proof of Fermat's Theorem. To see this, consider the set of numbers $\{a, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)\}$. We first show that no two of these numbers are congruent to each other. For if $ax_1 \equiv ax_2 \pmod{p}$, then $a(x_1 - x_2) \equiv 0 \pmod{p}$. Since p is prime and p does not divide a, this implies p divides $(x_1 - x_2)$ by Corollary 4.1.3, which is impossible since both x_1 and x_2 are strictly between 0 and p. Similarly, it is impossible that $ax \equiv 0 \pmod{p}$ for any x strictly between 0 and p, since p does not divide a or x. Then, by Theorem 3.1.4, every element of the set $\{a, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)\}$ is congruent to a number in the set $\{1, 2, \ldots, p-1\}$. Since no two of the ax's are congruent to each other, there is some x such that $ax \equiv 1 \pmod{p}$.

9. Prove that $x^2 \equiv 1 \pmod{p}$ implies $x \equiv 1 \pmod{p}$ or $x \equiv (p-1) \pmod{p}$, for every prime p.

Answer: The congruence $x^2 \equiv 1 \pmod{p}$ implies that p divides $x^2 - 1$. Since $x^2 - 1 = (x-1)(x+1)$, this implies that p divides $x-1$ or $x+1$ by Corollary 4.1.3. That is, either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \equiv p-1 \pmod{p}$.

Chapter 5
Fermat's Theorem and Wilson's Theorem

Solutions to Selected Exercises

1. Find the remainder when 24^{103} is divided by 103.

Answer: Since 103 is prime, it follows from the corollary to Fermat's Theorem (5.1.3) that $24^{103} \equiv 24 \pmod{103}$, so the remainder is 24.

2. Find a solution x to each of the following congruences:

(b) $16! \cdot x \equiv 5 \pmod{17}$

Answer: By Wilson's Theorem (5.2.1), $16! + 1 \equiv 0 \pmod{17}$, so $16! \equiv -1 \pmod{17}$. Thus, the congruence is equivalent to $-x \equiv 5 \pmod{17}$, or $x \equiv -5 \pmod{17}$.

4. Suppose that p is a prime greater than 2 and $a \equiv b^2 \pmod{p}$ for some natural number b that is not divisible by p. Prove that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Answer: Since p is a prime greater than 2, p is odd and $p \geq 3$. Thus, $\frac{p-1}{2}$ is a natural number, so $a^{\frac{p-1}{2}}$ is an integer. Since $a \equiv b^2 \pmod{p}$, $a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \pmod{p}$, and since b is not divisible by p, $b^{p-1} \equiv 1 \pmod{p}$, by Fermat's Theorem (5.1.2). So $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

5. Find three different prime factors of $10^{12} - 1$.

Answer: By Fermat's Theorem (5.1.2), $10^{12} - 1$ is divisible by 13. Also $10^{12} - 1 = (10^6 - 1)(10^6 + 1)$, and, using Fermat's Theorem again, $10^6 - 1$ is

divisible by 7. Finally, since $10^6-1=(10^3-1)(10^3+1)$ and $10^3-1=999$ is divisible by 3, $10^{12}-1$ is divisible by 3. Thus, the prime numbers 13, 7, and 3 all divide $10^{12}-1$. Also, since $10\equiv -1 \pmod{11}$, it follows that $10^{12}\equiv 1 \pmod{11}$, i.e., $10^{12}-1\equiv 0 \pmod{11}$. Therefore 11 is another prime factor. Similarly, the prime 101 is a factor, since $10^2\equiv -1 \pmod{101}$ yields $10^{12}\equiv 1 \pmod{101}$. (Although it is not so easy to establish, the other prime factors of $10^{12}-1$ are 37 and 9901.)

8. Find the remainder when:

(a) $(9!\cdot 16+4311)^{8603}$ is divided by 11.

Answer: By Wilson's Theorem (5.2.1), $10!\equiv -1 \pmod{11}$, or equivalently $10\cdot 9!\equiv 10 \pmod{11}$. Thus, $-9!\equiv 10 \pmod{11}$, or $9!\equiv -10\equiv 1 \pmod{11}$. Since $16\equiv 5 \pmod{11}$, it follows that $9!\cdot 16\equiv 5 \pmod{11}$, and, since $4311\equiv 10 \pmod{11}$ (one way to see this is to simply divide by 11), $9!\cdot 16+4311\equiv 5+10\equiv 4 \pmod{11}$. So $(9!\cdot 16+4311)^{8603}\equiv 4^{8603} \pmod{11}$. Note that Fermat's Theorem (5.1.2) yields $4^{10}\equiv 1 \pmod{11}$. Thus, $4^{8600}=(4^{10})^{860}\equiv 1 \pmod{11}$. Therefore, $4^{8603}\equiv 4^{8600}\cdot 4^3\equiv 1\cdot 4^3\equiv 64\equiv 9 \pmod{11}$, so the remainder is 9.

12. Show that if p is a prime number and a and b are natural numbers, then

$$(a+b)^p\equiv a^p+b^p \pmod{p}$$

Answer: By the corollary to Fermat's Theorem (5.1.3), $(a+b)^p\equiv a+b \pmod{p}$. Similarly, $a^p\equiv a \pmod{p}$ and $b^p\equiv b \pmod{p}$, so $(a+b)^p\equiv a^p+b^p \pmod{p}$.

13. For which prime numbers p is $(p-2)!\equiv 1 \pmod{p}$?

Answer: For all primes p, $(p-1)!\equiv -1 \pmod{p}$ by Wilson's Theorem (5.2.1). Therefore, $(p-1)(p-2)!\equiv -1 \pmod{p}$. Since $p-1\equiv -1 \pmod{p}$, it follows that $-1\cdot(p-2)\equiv -1 \pmod{p}$, so $(p-2)!\equiv 1 \pmod{p}$. Thus, the equation holds for all primes.

15. Is there a prime number p such that $(p-1)!+6$ is divisible by p?

Answer: By Wilson's Theorem (5.2.1), $(p-1)!+6 \equiv -1+6 \equiv 5 \pmod{p}$. Thus, p divides $(p-1)!+6$ if and only if p divides 5, and, hence, if and only if $p = 5$.

17. Suppose 2^k+1 is a prime number. Prove that k has no prime divisors other than 2. [Hint: If $k = ab$ with b odd, consider 2^k+1 modulo 2^a+1.]

Answer: Suppose $k = ab$ with b odd and $b > 1$. Modulo 2^a+1, 2^a is congruent to -1. Thus $2^{ab}+1 \equiv (-1)^b+1 \equiv -1+1 \equiv 0 \pmod{2^a+1}$. It follows that $2^{ab}+1$ is divisible by 2^a+1, so $2^{ab}+1$ is not prime, which is a contradiction. Therefore if 2^k+1 is prime, then k has no prime divisors other than 2. Note that this shows that 2^k+1 prime implies that k is a power of 2 (k could be 0). Thus any prime of the form 2^k+1 must be a Fermat Prime (see page 151).

Chapter 6
Sending and Receiving Secret Messages

Solutions to Selected Exercises

1. You are to receive a message using the RSA system. You choose $p = 5$, $q = 7$ and $E = 5$. Verify that $D = 5$ is a decryptor. The encrypted message you receive is 17. What is the actual (decrypted) message?

Answer: Here $\phi(N) = 4 \cdot 6 = 24$, and $ED = 25 = 1 + \phi(N)$, so D is a decryptor. The message is then an M such that $0 \leq M < N = 35$ and $17^5 \equiv M \pmod{35}$. Now $17^2 \equiv 289 \equiv 9 \pmod{35}$, so $17^4 \equiv 81 \equiv 11 \pmod{35}$ and $17^5 \equiv 11 \cdot 17 \equiv 187 \equiv 12 \pmod{35}$. It follows that the message is 12.

Chapter 7
The Euclidean Algorithm and Applications

Solutions to Selected Exercises

1. Find the greatest common divisor of each of the following pairs of integers in two different ways, by using the Euclidean Algorithm and by factoring both numbers into primes:

(a) 252 and 198
(d) 52 and 135

Answer: (a) First by the Euclidean Algorithm,

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2 \end{aligned}$$

so the greatest common divisor is 18. By factoring, $252 = 2^2 \cdot 3^2 \cdot 7$ and $198 = 2 \cdot 3^2 \cdot 11$, so the greatest common divisor is $2 \cdot 3^2 = 18$.

(d) By the Euclidean Algorithm,

$$\begin{aligned} 135 &= 52 \cdot 2 + 31 \\ 52 &= 31 \cdot 1 + 21 \\ 31 &= 21 \cdot 1 + 10 \\ 21 &= 10 \cdot 2 + 1 \\ 10 &= 1 \cdot 10 \end{aligned}$$

so the greatest common divisor is 1.

By factoring, $135 = 3^3 \cdot 5$ and $52 = 2^2 \cdot 13$, so the greatest common divisor is 1.

2. For each of the pairs in Problem 1 above, write the greatest common divisor as a linear combination of the given numbers.

Answer: (a) Working our way backwards from the solution to Problem 1(a),

$$\begin{aligned} 18 &= 54 - 36 \\ &= 54 - (198 - 54 \cdot 3) \\ &= 54 \cdot 4 - 198 \\ &= (252 - 198) \cdot 4 - 198 \\ &= 252 \cdot 4 - 198 \cdot 5 \end{aligned}$$

(d) From the solution to Problem 1(d),

$$\begin{aligned} 1 &= 21 - 10 \cdot 2 \\ &= 21 - (31 - 21) \cdot 2 \\ &= 21 \cdot 3 - 31 \cdot 2 \\ &= (52 - 31) \cdot 3 - 31 \cdot 2 \\ &= 52 \cdot 3 - 31 \cdot 5 \\ &= 52 \cdot 3 - (135 - 52 \cdot 2) \cdot 5 \\ &= 52 \cdot 13 - 135 \cdot 5 \end{aligned}$$

4.(a) Find a formula for all integer solutions of the Diophantine equation $3x + 4y = 14$.

(b) Find all pairs of natural numbers that solve the above equation.

Answer: (a) The greatest common divisor of 3 and 4 is 1, and $1 = 4 - 3$. Thus $14 = 14 \cdot 4 - 14 \cdot 3$, and $x = -14$, $y = 14$ is an integer solution. Then by Theorem 7.2.10, the integral solutions are all pairs x and y of the form $x = -14 + m \cdot 4$, $y = 14 - m \cdot 3$, where m is an integer.

(b) Using the expression from part (a), for x to be a natural number m must satisfy $-14 + m \cdot 4 > 0$, which is equivalent to $m \cdot 4 > 14$, which is equivalent to $m > 3$. Similarly, for y to be a natural number, $14 - m \cdot 3$ must be greater than 0, which requires m to be less than 5. The only m satisfying both of these inequalities is $m = 4$, so the only pair is $(2, 2)$.

5. Let ϕ be Euler's ϕ-function. Find:

(a) $\phi(12)$
(e) $\phi(97)$
(g) $\phi(101 \cdot 37)$

(h) $\phi(3^{100})$

Answer: (a) The only natural numbers less than 12 that are relatively prime to 12 are 1, 5, 7 and 11, so $\phi(12) = 4$.

(e) Since 97 is prime, $\phi(97) = 96$.

(g) Since 101 and 37 are each prime, $\phi(101 \cdot 37) = 100 \cdot 36 = 3600$.

(h) The natural numbers less than 3^{100} that are relatively prime to 3^{100} are those which are not divisible by 3. As two thirds of the natural numbers less than or equal to 3^{100} are not divisible by 3, it follows that $\phi(3^{100}) = \frac{2}{3} \cdot 3^{100} = 2 \cdot 3^{99}$.

6. Use the Euclidean Algorithm to find the decryptors in Problems 1, 2, and 3 in Chapter 6.

Answer: 3. Here $E = 7$ and $N = 15 = 3 \cdot 5$, so $\phi(N) = 2 \cdot 4 = 8$. Then

$$\begin{aligned} 8 &= 7 \cdot 1 + 1 \\ 7 &= 1 \cdot 7 \end{aligned}$$

Thus, $1 = 8 - 7$, and so, $1 + 8(-1) = 7(-1)$. Adding $-8 \cdot 7m$ to both sides gives

$$1 + 8(-1 - 7m) = 7(-1 - 8m).$$

Taking $m = -1$, we get $1 + 8(6) = 7(7)$. Therefore, 7 is a decryptor.

8. Find the smallest natural number x such that $24x$ leaves a remainder of 2 upon division by 59.

Answer: The solution x satisfies the equation $24x - 59y = 2$. Using the Euclidean Algorithm,

$$\begin{aligned} 59 &= 24 \cdot 2 + 11 \\ 24 &= 11 \cdot 2 + 2 \\ 11 &= 2 \cdot 5 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

so $\gcd(24, 59) = 1$. Then

$$\begin{aligned}1 &= 11 - 2\cdot 5\\ &= 11 - (24 - 11\cdot 2)\cdot 5\\ &= 11\cdot 11 - 24\cdot 5\\ &= (59 - 24\cdot 2)\cdot 11 - 24\cdot 5\\ &= 59\cdot 11 - 24\cdot 27\end{aligned}$$

Therefore, $24\cdot(-27) - 59\cdot(-11) = 1$, so $24\cdot(-54) - 59\cdot(-22) = 2$. It follows by Theorem 7.2.10 that the integral solutions of the equation are pairs of numbers of the form

$$(x,y) = (-54 + m\cdot(-59), -22 - m\cdot 24)$$

where m is an integer. For x to be positive, m must be less than 0. If $m = -1$, then $x = 5$, and if m is any smaller integer, then the corresponding x will be greater than 5. Thus, the smallest natural number x is 5.

10. A liquid comes in 17 liter and 13 liter cans. Someone needs exactly 287 liters of the liquid. How many cans of each size should the person buy?

Answer: If x is the number of 17 liter cans and y is the number of 13 liter cans, then x and y satisfy the equation $17x + 13y = 287$. By the Euclidean Algorithm,

$$\begin{aligned}17 &= 13\cdot 1 + 4\\ 13 &= 4\cdot 3 + 1\end{aligned}$$

Thus, $\gcd(17,13) = 1$, and it follows that the equation does have integral solutions (by Theorem 7.2.10). Working our way back up,

$$\begin{aligned}1 &= 13 - 4\cdot 3\\ &= 13 - (17 - 13)\cdot 3\\ &= 13\cdot 4 - 17\cdot 3.\end{aligned}$$

Hence, $17\cdot(-3) + 13\cdot 4 = 1$. Multiplying by 287, we have $17\cdot(-861) + 13\cdot 1148 = 287$. Therefore, the integer solutions are all pairs of the form $(x,y) = (-861 + 13m, 1148 - 17m)$, for integers m (Theorem 7.2.10). However, x and y have to be nonnegative for (x,y) to be a solution of the actual problem. For x to be nonnegative, m has to be greater than 66. For y to be nonnegative, m has to be less than 68. Thus, the only possible choice is $m = 67$, which gives $x = 10$, $y = 9$. Therefore, the person should buy 10 of the 17 liter cans and 9 of the 13 liter cans.

12. Let a, b, m and n be natural numbers with m and n greater than 1. Assume that m and n are relatively prime. Prove that if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{mn}$.

Answer: Since $a \equiv b \pmod{m}$, there is an integer k such that $(a-b) = km$. Since n also divides $(a-b)$, n divides km. Since n is relatively prime to m, it follows from Lemma 7.2.9 that n divides k, so $k = dn$ for some integer d. Therefore, $(a-b) = dnm$, so $a \equiv b \pmod{mn}$.

13. Let a and b be natural numbers.

(a) Suppose there exist integers m and n such that $am + bn = 1$. Prove that a and b are relatively prime.

Answer: If d divides a and d divides b, then d divides $am + bn$, so d divides 1. Hence a and b have no prime factors in common.

14. Let p be a prime number. Prove that $\phi(p^2) = p^2 - p$.

Answer: If m is a natural number less than p^2, then m has a factor in common with p^2 if and only if p is a factor of m. This is the case if and only if m is a multiple of p. There are $p^2 - 1$ many natural numbers less than p^2, and there are $p-1$ multiples of p less than p^2. Therefore, $\phi(p^2) = p^2 - 1 - (p-1) = p^2 - p$.

15. The public key $N = 55$ and $E = 7$ is announced. The encrypted message 5 is received.

(a) Find a decryptor, D, and prove that D is a decryptor.
(b) Decrypt 5 to find the original message.

Answer: (a) Here $N = 11 \cdot 5$, and $\phi(N) = 10 \cdot 4 = 40$. Then

$$\begin{aligned} 40 &= 7\cdot 5+5\\ 7 &= 5\cdot 1+2\\ 5 &= 2\cdot 2+1 \end{aligned}$$

and, working backwards,

$$\begin{aligned} 1 &= 5-2\cdot 2\\ &= 5-2\cdot(7-5)\\ &= 3\cdot 5-2\cdot 7\\ &= 3\cdot(40-7\cdot 5)-2\cdot 7\\ &= 3\cdot 40-17\cdot 7 \end{aligned}$$

Thus, $1-3\cdot 40=-17\cdot 7$, and therefore for any integer m, $1-(3+7m)\cdot 40=(-17-40m)\cdot 7$. Taking $m=-1$ gives $1+4\cdot 40=23\cdot 7$, and so $D=23$ is a decryptor.

(b) The message is the natural number less than 55 that is congruent to 5^{23} modulo 55. First, $5^3\equiv 125\equiv 15 \pmod{55}$, so $5^6\equiv 15^2\equiv 225\equiv 5 \pmod{55}$. Then $5^{18}\equiv 5^3\equiv 15 \pmod{55}$, and $5^{21}\equiv 15\cdot 5^3\equiv 15^2\equiv 5 \pmod{55}$. Thus, $5^{23}\equiv 5\cdot 5^2\equiv 15 \pmod{55}$, and the original message is 15.

19. Show that if m and n are relatively prime and a and b are any integers, then there is an integer x that simultaneously satisfies the two congruences $x\equiv a \pmod{m}$ and $x\equiv b \pmod{n}$.

Answer: Since m and n are relatively prime, there are integers c and d such that $md+nc=1$ (see page 49). Then multiplying both sides by $(b-a)$ gives integers k and j such that $mk+nj=b-a$. Let $x=mk+a=b-nj$. Then $x-a=mk$ and $x-b=-nj$, so $x\equiv a \pmod{m}$ and $x\equiv b \pmod{n}$. This is a special case of the Chinese Remainder Theorem, the general statement of which is Problem 20 in this chapter.

22. Let a and b be relatively prime natural numbers greater than or equal to 2. Prove that $a^{\phi(b)}+b^{\phi(a)}\equiv 1 \pmod{ab}$.

Answer: By Euler's Theorem (7.2.17), there are integers k_1 and k_2 such that $a^{\phi(b)}-1=bk_1$ and $a^{\phi(a)}-1=ak_2$. Then $abk_1k_2=a^{\phi(b)}b^{\phi(a)}-a^{\phi(b)}-b^{\phi(a)}+1$, and so $-abk_1k_2=-a^{\phi(b)}b^{\phi(a)}+a^{\phi(b)}+b^{\phi(a)}-1$. Hence, ab divides

$-a^{\phi(b)}b^{\phi(a)} + a^{\phi(b)} + b^{\phi(a)} - 1$, and, since ab divides $-a^{\phi(b)}b^{\phi(a)}$, it follows that ab divides $a^{\phi(b)} + b^{\phi(a)} - 1$.

25. Suppose that a and m are relatively prime and that k is the smallest natural number such that a^k is congruent to 1 modulo m. Prove that k divides $\phi(m)$.

Answer: Since $a^{\phi(m)} \equiv 1 \pmod{m}$ by Euler's Theorem (7.2.17), it follows that k is less than or equal to $\phi(m)$. Suppose k does not divide $\phi(m)$. Then k is less than $\phi(m)$, and $\phi(m) = kq + r$ for natural numbers q and r, with r less than k. Therefore, $1 \equiv a^{\phi(m)} \equiv a^{kq+r} \equiv a^{kq}a^r \equiv (a^k)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}$. However, r is a natural number less than k, so this contradicts the assumption that k is the smallest natural number such that $a^k \equiv 1 \pmod{m}$. That is, k divides $\phi(m)$.

26. For p a prime and k a natural number, show that $\phi(p^k) = p^k - p^{k-1}$.

Answer: There are $p^k - 1$ natural numbers less than p^k, and a natural number is not relatively prime to p^k if and only if it is a multiple of p. The natural numbers less than p^k which are multiples of p are the numbers of the form $p \cdot m$ where m is a natural number less than p^{k-1}. Since there are $p^{k-1} - 1$ natural numbers less than p^{k-1}, there are $p^{k-1} - 1$ multiples of p which are less than p^k. Thus, $\phi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1}$.

27. If the canonical factorization of the natural number n into primes is $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots p_m^{k_m}$, prove that

$$\phi(n) = \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdot \left(p_2^{k_2} - p_2^{k_2-1}\right) \cdots \left(p_m^{k_m} - p_m^{k_m-1}\right)$$

Answer: We first show that the Euler phi-function is multiplicative on relatively prime natural numbers. That is, if a and b are relatively prime, then $\phi(ab) = \phi(a) \cdot \phi(b)$.

To see this, fix relatively prime natural numbers a and b. Let A be the set of natural numbers less than a that are relatively prime to a, let B be the set of natural numbers less than b that are relatively prime to b, and let S be the set of natural numbers less than ab that are relatively prime to ab. Then the number of elements in A is $\phi(a)$, the number of elements in B is $\phi(b)$, and the number

of elements in S is $\phi(ab)$. Let $A \times B$ be the set of all pairs of natural numbers (c,d) such that c is in A and d is in B. The number of elements in $A \times B$ is $\phi(a) \cdot \phi(b)$, as there are $\phi(a)$ choices for c and $\phi(b)$ choices for d in making a pair (c,d). To show that $\phi(ab) = \phi(a) \cdot \phi(b)$, we show that S has the same number of elements as $A \times B$ does. For each element s of S let $f(s)$ be the pair of nonnegative integers (r_1, r_2) such that $r_1 < a$ and $r_1 \equiv s \pmod{a}$, and $r_2 < b$ and $r_2 \equiv s \pmod{b}$. We prove that the function f pairs the elements of S with those of $A \times B$. That is, we establish that $f(s)$ is in $A \times B$ for every s in S, that distinct elements of S are sent to distinct elements of $A \times B$, and, finally, that every element of $A \times B$ has the form $f(s)$ for some s in S.

We first prove that $f(s)$ is in $A \times B$, for each s in S. To see this, let s in S be given, and let $f(s) = (r_1, r_2)$. We must establish that r_1 and a are relatively prime. Since $r_1 \equiv s \pmod{a}$, a divides $r_1 - s$. Thus, if p is a prime that divides a and r_1, then p divides r_1 and $r_1 - s$, from which it follows that p divides s, contradicting the fact that s is relatively prime to ab. Therefore, we have shown that r_1 and a are relatively prime, so r_1 is in A. The same proof establishes that r_2 and b are relatively prime, so r_2 is in B. It follows that (r_1, r_2) is in $A \times B$. This shows that the function f takes S into $A \times B$.

Suppose $f(s) = f(t)$ for some s and t in S. Then s and t are both simultaneous solutions of the congruences $x \equiv r_1 \pmod{a}$ and $x \equiv r_2 \pmod{b}$, so $s \equiv t \pmod{a}$ and $s \equiv t \pmod{b}$. Since a and b are relatively prime, it follows from Problem 12 above that $s \equiv t \pmod{ab}$. Then, as s and t are both nonnegative integers less than ab, $s = t$. Therefore, f does not send two different elements of S to the same element of $A \times B$.

All that remains to be shown is that for each element of $A \times B$ there is an element of S which is sent onto it by f. Given (r_1, r_2) in $A \times B$, the special case of the Chinese Remainder Theorem (Problem 19) shows that there exists some integer x such that $x \equiv r_1 \pmod{a}$ and $x \equiv r_2 \pmod{b}$. Take the nonnegative integer s less than ab such that $s \equiv x \pmod{ab}$. Since $s - x$ is divisible by ab, $s - x$ is also divisible by a. Thus, $s \equiv x \equiv r_1 \pmod{a}$. Similarly, $s \equiv x \equiv r_2 \pmod{b}$. If s is not relatively prime to ab, then there is some prime p which divides both ab and s. Then p divides a or b (Corollary 4.1.3 or Lemma 7.2.2). Suppose p divides a. Since p divides s and $s - r_1$, p divides r_1. This contradicts the fact that r_1 is relatively prime to a. Similarly, it is not possible that p divides b. Therefore, s must be relatively prime to ab, so s is in S. Since $s \equiv r_1 \pmod{a}$ and $s \equiv r_2 \pmod{b}$, $f(s) = (r_1, r_2)$.

This shows that f gives a pairing of the elements of S with the elements of $A \times B$, so there are the same number of elements in S as are in $A \times B$. Thus, $\phi(ab) = \phi(a) \cdot \phi(b)$ whenever a and b are relatively prime natural numbers.

Repeated application of this result (or, more precisely, induction on m), shows that

$$\phi(p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}) = \phi(p_1^{k_1}) \cdot \phi(p_2^{k_2}) \cdots \phi(p_m^{k_m})$$

It follows from the previous problem (Problem 26) that

$$\phi(p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}) = \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdot \left(p_2^{k_2} - p_2^{k_2-1}\right) \cdots \left(p_m^{k_m} - p_m^{k_m-1}\right).$$

Chapter 8
Rational Numbers and Irrational Numbers

Solutions to Selected Exercises

1. Use the Rational Roots Theorem (8.1.9) to find all rational roots of each of the following polynomials (some may not have any rational roots at all):

(a) x^2+5x+2
(b) $2x^3-5x^2+14x-35$

Answer: (a) By the Rational Roots Theorem, if $\frac{m}{n}$ is a root then m divides 2 and n divides 1. The possible values for m are $2,-2,1,-1$, and the possible values of n are $1,-1$. Therefore, the possible values for $\frac{m}{n}$ are $2,-2,1,-1$. None of these are roots (as can be seen by substituting them into the polynomial), so the polynomial has no rational roots. (Of course, this problem could be solved using the quadratic formula.)

(b) By the Rational Roots Theorem, if $\frac{m}{n}$ is a root then m divides 35 and n divides 2, so m is one of $\pm1,\pm5,\pm7,\pm35$ and n is ±1 or ±2. The possible values of $\frac{m}{n}$ are then $\pm1,\pm5,\pm7,\pm35,\pm\frac{1}{2},\pm\frac{5}{2},\pm\frac{7}{2},\pm\frac{35}{2}$. Trying these possibilities shows that $\frac{5}{2}$ is the only rational root.

4. Must the sum of an irrational number and a rational number be irrational?

Answer: Yes. Let a be rational and c be irrational and let $a+c=b$. Suppose b was rational. Then $b-a$ would be rational since both a and b are, but $b-a=c$, which is irrational. Therefore, b cannot be rational.

6. Must the sum of two irrational numbers be irrational?

Answer: No. For example, $\sqrt{2}$ and $7-\sqrt{2}$ are both irrational but their sum is 7, which is rational.

9. Determine whether each of the following numbers is rational or irrational and prove that your answer is correct:

(e) $\dfrac{\sqrt{63}}{\sqrt{28}}$

(g) $\sqrt[7]{\frac{8}{9}}$

Answer: (e) This is rational, since $\frac{\sqrt{63}}{\sqrt{28}} = \frac{\sqrt{7\cdot 9}}{\sqrt{4\cdot 7}} = \frac{3\sqrt{7}}{2\sqrt{7}} = \frac{3}{2}$.

(g) This is irrational. For suppose that $\sqrt[7]{\frac{8}{9}} = \frac{m}{n}$ for integers m and n with $n \neq 0$. Then $\frac{8}{9} = \frac{m^7}{n^7}$, so $n^7 \cdot 8 = m^7 \cdot 9$. In the prime factorization of the left-hand side 3 occurs to a power which is a multiple of 7, while in the prime factorization of the right-hand side 3 occurs to a power which is 2 more than a multiple of 7. This contradicts the Fundamental Theorem of Arithmetic (4.1.1 or 7.2.4).

10. Prove that $\sqrt[3]{3+\sqrt{11}}$ is irrational.

Answer: Suppose $\sqrt[3]{3+\sqrt{11}} = r$ for some rational number r. Cubing both sides, it follows that $3+\sqrt{11} = r^3$, so $\sqrt{11} = r^3 - 3$. This would imply that $\sqrt{11}$ is rational. However, $\sqrt{11}$ is irrational since 11 is a prime (Theorem 8.2.6).

11. Prove that the following numbers are irrational:

(d) $\sqrt{3}+\sqrt{5}+\sqrt{7}$

Answer: Let $\sqrt{3}+\sqrt{5}+\sqrt{7} = r$, and suppose that r is rational. It follows that $\sqrt{3}+\sqrt{5} = r-\sqrt{7}$, and, squaring both sides,

$$8 + 2\sqrt{3}\sqrt{5} = r^2 - 2r\sqrt{7} + 7$$

so $1 + 2(\sqrt{3}\sqrt{5} + r\sqrt{7}) = r^2$, and $\frac{r^2-1}{2} = \sqrt{3}\sqrt{5} + r\sqrt{7}$. Therefore,

$$\frac{r^2-1}{2} - \sqrt{3}\sqrt{5} = r\sqrt{7}$$

Squaring both sides of this equation yields

$$7r^2 = \left(\frac{r^2-1}{2}\right)^2 - (r^2-1)\sqrt{3}\sqrt{5} + 15$$

Therefore, $7r^2 - (\frac{r^2-1}{2})^2 - 15 = -(r^2-1)\sqrt{3}\sqrt{5}$, so $(r^2-1)\sqrt{3}\sqrt{5}$ is rational. Note that $\sqrt{3}\sqrt{5} = \sqrt{15}$ is irrational (as follows, for example, from Theorem 8.2.8). Thus, by Problem 8 in this chapter, $(r^2-1)\sqrt{3}\sqrt{5}$ is irrational (r is greater than 1, so r^2-1 is not 0). This contradiction establishes that r is irrational.

12. Suppose that a and b are odd natural numbers and $a^2 + b^2 = c^2$. Prove that c is irrational.

Answer: Suppose c is rational. Since c^2 is a natural number, it follows that c is an integer (Theorem 8.2.8). Also, since a and b are odd, a^2 and b^2 are odd and thus c^2 is even. Therefore, the prime factorization of c^2 includes 2, so the prime factorization of c also includes 2. Since a and b are odd natural numbers, there are nonnegative integers k_1 and k_2 such that $a = 2k_1 + 1$ and $b = 2k_2 + 1$. Then $a^2 = 4k_1^2 + 4k_1 + 1$ and $b^2 = 4k_2^2 + 4k_2 + 1$, so $a^2 + b^2 \equiv 4(k_1^2 + k_1 + k_2^2 + k_2) + 2 \equiv 2 \pmod 4$. However, since c is divisible by 2, c^2 is divisible by 4. That is, $c^2 \equiv 0 \pmod 4$, so $a^2 + b^2$ is not congruent to c^2 modulo 4, contradicting $a^2 + b^2 = c^2$.

Chapter 9
The Complex Numbers

Solutions to Selected Exercises

1. Write the following complex numbers in $a+bi$ form, where a and b are real numbers:

(a) $\left(\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right)^{10}$

(f) i^{574}

Answer: (a) The modulus of $\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}$ is $\sqrt{(\frac{1}{\sqrt{2}})^2+(\frac{1}{\sqrt{2}})^2}=\sqrt{\frac{1}{2}+\frac{1}{2}}=1$. An argument is $\frac{\pi}{4}$, since $\cos\frac{\pi}{4}=\frac{1}{\sqrt{2}}=\sin\frac{\pi}{4}$. That is, $\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}=\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}$. Thus, by De Moivre's Theorem (9.2.6), $(\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}})^{10}=\cos\frac{10\pi}{4}+i\sin\frac{10\pi}{4}=\cos(2+\frac{1}{2})\pi+i\sin(2+\frac{1}{2})\pi=\cos\frac{1}{2}\pi+i\sin\frac{1}{2}\pi=0+i(1)=i$. Therefore, $\left(\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right)^{10}=i$.

(f) There are at least two easy approaches to this problem. First, $i^2=-1$ implies that $i^4=1$ and, therefore, that $i^{4k}=1$ for every natural number k. In particular, $i^{572}=1$, so $i^{574}=1\cdot i^2=-1$.

Alternately, note that an argument of i is $\frac{\pi}{2}$, from which it follows by De Moivre's Theorem that an argument of i^{574} is 287π, and as arguments are determined modulo 2π, π is also an argument of i^{574}. Since $|i|=1$, $|i^{574}|=1$, and it follows that $i^{574}=\cos\pi+i\sin\pi=-1$.

4. Find the cube roots of the following numbers:

(b) $8\sqrt{3}+8i$

Answer: First, $|8\sqrt{3}+8i| = \sqrt{(8\sqrt{3})^2+8^2} = \sqrt{4\cdot 64} = \sqrt{4}\sqrt{64} = 16$. Therefore, $8\sqrt{3}+8i = 16(\cos\theta + i\sin\theta)$ for θ satisfying $16\cos\theta = 8\sqrt{3}$ and $16\sin\theta = 8$, so $\cos\theta = \frac{\sqrt{3}}{2}$ and $\sin\theta = \frac{1}{2}$. It follows that $\theta = \frac{\pi}{6}$ is an argument of $8\sqrt{3}+8i$.

Now if $z^3 = 8\sqrt{3}+8i$, then $|z^3| = 16$, so $|z| = \sqrt[3]{16}$ and an argument of z^3 is $\frac{1}{6}\pi$. Therefore, if the argument of z is θ, then $3\theta = (2k+\frac{1}{6})\pi$, for some integer k. If $k = 0$, this gives $3\theta = \frac{1}{6}\pi$ so $\theta = \frac{1}{18}\pi$, and a cube root is $z_1 = \sqrt[3]{16}(\cos\frac{1}{18}\pi + i\sin\frac{1}{18}\pi)$. If $k = 1$, then $\theta = (\frac{2}{3}+\frac{1}{18})\pi = \frac{13}{18}\pi$ and $z_2 = \sqrt[3]{16}(\cos\frac{13}{18}\pi + i\sin\frac{13}{18}\pi)$ is another cube root. If $k = 2$, then $\theta = (\frac{4}{3}+\frac{1}{18})\pi = \frac{25}{18}\pi$ and so a third cube root is $z_3 = \sqrt[3]{16}(\cos\frac{25}{18}\pi + i\sin\frac{25}{18}\pi)$. For any other integer value of k, θ differs from one of the above arguments by a multiple of 2π, and thus no new values of z are obtained. Therefore, z_1, z_2 and z_3 are the cube roots. (Of course, since a polynomial of degree 3 has at most 3 roots (Theorem 9.3.8), every complex number has at most three cube roots.)

9. Find all the complex roots of the polynomial z^6+z^3+1.

Answer: Let $x = z^3$. Then z is a root if and only if $x^2+x+1 = 0$. By the quadratic formula (see Problem 6 in this chapter), x is a root of x^2+x+1 if and only if $x = \frac{-1\pm\sqrt{1-4}}{2} = -\frac{1}{2} \pm \frac{\sqrt{-3}}{2} = -\frac{1}{2} \pm \frac{i\sqrt{3}}{2}$. Then the 6 roots of the original polynomial are the cube roots of $-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ and the cube roots of $-\frac{1}{2}-\frac{\sqrt{3}}{2}i$.

Both $x_1 = -\frac{1}{2}+\frac{\sqrt{3}}{2}i$ and $x_2 = -\frac{1}{2}-\frac{\sqrt{3}}{2}i$ have modulus $\sqrt{\frac{1}{4}+\frac{3}{4}} = 1$. An argument of x_1 is the angle θ with $0 \le \theta < 2\pi$ and $\cos\theta = -\frac{1}{2}$, $\sin\theta = \frac{\sqrt{3}}{2}$, which gives $\theta = \frac{2\pi}{3}$. If z is a cube root of x_1, then $|z| = 1$ and an argument θ of z satisfies $3\theta = (2k+\frac{2}{3})\pi$, where k is an integer. Thus, $\theta = \frac{2}{9}\pi$ or $\frac{8}{9}\pi$ or $\frac{14}{9}\pi$. Therefore, $\cos\frac{2}{9}\pi + i\sin\frac{2}{9}\pi$, $\cos\frac{8}{9}\pi + i\sin\frac{8}{9}\pi$ and $\cos\frac{14}{9}\pi + i\sin\frac{14}{9}\pi$ are three roots of the original polynomial.

An argument of x_2 is an angle θ with $0 \le \theta < 2\pi$ and $\cos\theta = -\frac{1}{2}$ and $\sin\theta = -\frac{\sqrt{3}}{2}$, giving $\theta = \frac{4\pi}{3}$. If z is a cube root of x_2, then $|z| = 1$ and an argument of z is any θ satisfying $3\theta = 2k+\frac{4\pi}{3}$. Possible values for θ are $\frac{4}{9}\pi$, $\frac{10}{9}\pi$, and $\frac{16}{9}\pi$. Therefore, $\cos\frac{4}{9}\pi + i\sin\frac{4}{9}\pi$, $\cos\frac{10}{9}\pi + i\sin\frac{10}{9}\pi$ and $\cos\frac{16}{9}\pi + i\sin\frac{16}{9}\pi$ are the other three roots of the original polynomial. (Note that Theorem 9.3.8 implies that the polynomial has at most six distinct roots.)

13. Let p be a polynomial with real coefficients. Prove that the complex conjugate of each root of p is also a root of p.

Answer: We begin by showing that the conjugate of a sum of two complex numbers is the sum of the conjugates and the conjugate of a product of two complex numbers is the product of the conjugates. This follows from the very straightforward computations below.
For sums:

$$\overline{(a+bi)+(c+di)} = \overline{a+c+(b+d)i} = a+c-(b+d)i,$$

and

$$\overline{a+bi}+\overline{c+di} = (a-bi)+(c-di) = a+c-(b+d)i.$$

For products:

$$\overline{(a+bi)(c+di)} = \overline{ac-bd+(bc+ad)i} = ac-bd-(bc+ad)i,$$

and

$$(\overline{a+bi})(\overline{c+di}) = (a-bi)(c-di) = ac-bd+(-bc-ad)i.$$

Now let $p(z) = a_n z^n + \cdots + a_1 z + a_0$ and suppose that $a+bi$ is a root of p. Then

$$a_n(a+bi)^n + \cdots + a_1(a+bi) + a_0 = 0,$$

so

$$\overline{a_n(a+bi)^n + \cdots + a_1(a+bi) + a_0} = \overline{0} = 0.$$

Repeatedly applying the above computations concerning sums and products yields

$$\overline{a_n(a+bi)^n + \cdots + a_1(a+bi) + a_0} = \overline{a_n}(\overline{a+bi})^n + \cdots + \overline{a_1}(\overline{a+bi}) + \overline{a_0}.$$

Since the a_i are real numbers, $\overline{a_i} = a_i$ for each a_i. Thus,

$$\overline{a_n}(\overline{a+bi})^n + \cdots + \overline{a_1}(\overline{a+bi}) + \overline{a_0} = a_n(\overline{a+bi})^n + \cdots + a_1(\overline{a+bi}) + a_0 = 0.$$

But, $p(\overline{a+bi}) = a_n(\overline{a+bi})^n + \cdots + a_1(\overline{a+bi}) + a_0$, so $p(\overline{a+bi}) = 0$.

Chapter 10
Sizes of Infinite Sets

Solutions to Selected Exercises

1. Show that the set of all polynomials with rational coefficients is countable.

Answer: A polynomial with rational coefficents can be written in the form $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where the a_i are rational numbers and n is a natural number or 0. We use the Enumeration Principle (10.3.16). Let $\mathscr{L} = \mathbb{Q} \cup \{x^n : n \in \mathbb{N}\} \cup \{+\}$. Then $\mathscr{L}$ is a union of a finite number of countable sets and is therefore countable (Theorem 10.2.10). Each polynomial is uniquely labeled by a finite sequence of elements of $\mathscr{L}$ by simply writing it in the usual way. The Enumeration Principle then gives the result.

2. Suppose that the sets $\mathscr{S}$, $\mathscr{T}$ and $\mathscr{U}$ satisfy $\mathscr{S} \subset \mathscr{T} \subset \mathscr{U}$, and that $|\mathscr{S}| = |\mathscr{U}|$. Show that $\mathscr{T}$ has the same cardinality as $\mathscr{S}$.

Answer: Let $f : \mathscr{S} \to \mathscr{T}$ be defined by $f(s) = s$ for all $s \in \mathscr{S}$. Then f is a one-to-one function from $\mathscr{S}$ into $\mathscr{T}$, so $|\mathscr{S}| \leq |\mathscr{T}|$. Similarly if $g : \mathscr{T} \to \mathscr{U}$ is defined by $g(t) = t$, then g is a one-to-one function from $\mathscr{T}$ into $\mathscr{U}$, so $|\mathscr{T}| \leq |\mathscr{U}|$. Therefore, $|\mathscr{S}| \leq |\mathscr{T}| \leq |\mathscr{U}|$. Since $|\mathscr{S}| = |\mathscr{U}|$ this is equivalent to $|\mathscr{S}| \leq |\mathscr{T}| \leq |\mathscr{S}|$. By the Cantor-Bernstein Theorem (10.3.5), this implies that $|\mathscr{S}| = |\mathscr{T}|$.

4. Assume that $|A_1| = |B_1|$ and $|A_2| = |B_2|$. Prove:

a. $|A_1 \times A_2| = |B_1 \times B_2|$.

Answer: (a) By the hypothesis, there exist functions $f : A_1 \to B_1$ and $g : A_2 \to B_2$ that are both one-to-one and onto. Let $h : A_1 \times A_2 \to B_1 \times B_2$ be

defined by $h((a_1,a_2)) = (f(a_1),g(a_2))$. To show that h is one-to-one, suppose that $h((a_1,a_2)) = h((a_3,a_4))$. Then $f(a_1) = f(a_3)$, so $a_1 = a_3$, since f is one-to-one. Similarly, $g(a_2) = g(a_4)$, so $a_2 = a_4$ since g is one-to-one. Thus, $(a_1,a_2) = (a_3,a_4)$, and so h is one-to-one. To show that h is onto, let (b_1,b_2) be any element of $B_1 \times B_2$. Then there exist $a_1 \in A_1$ and $a_2 \in A_2$ such that $f(a_1) = b_1$ and $g(a_2) = b_2$, since f and g are both onto. Therefore $h((a_1,a_2)) = (b_1,b_2)$, which proves that h is onto. Thus, h is one-to-one and onto.

6. What is the cardinality of the set of all functions from $\mathbb{N}$ to $\{1,2\}$?

Answer: We show that the cardinality is c, by observing that this set is essentially the set of characteristic functions. As shown in Theorem 10.3.32, the set of characteristic functions with domain $\mathbb{N}$ has the same cardinality as $\mathscr{P}(\mathbb{N})$. The given set has the same cardinality as the set of characteristic functions on $\mathbb{N}$ since a one-to-one onto function is given by sending a characteristic function f to the function g defined by $g(x) = 1$ if $f(x) = 0$ and $g(x) = 2$ if $f(x) = 1$. The proof is completed by noting that $|\mathscr{P}(\mathbb{N})| = c$ (Theorem 10.3.28).

9. Suppose that $\mathscr{S}$ and $\mathscr{T}$ each have cardinality c. Show that $\mathscr{S} \cup \mathscr{T}$ also has cardinality c.

Answer: We use $\mathscr{T} \setminus \mathscr{S}$ to denote the set of all x in $\mathscr{T}$ such that x is not in $\mathscr{S}$. Note that the set $\mathscr{S} \cup \mathscr{T}$ is equal to the set $\mathscr{S} \cup (\mathscr{T} \setminus \mathscr{S})$. (We use $\mathscr{T} \setminus \mathscr{S}$ rather than $\mathscr{T}$ because $\mathscr{T} \setminus \mathscr{S}$ is always disjoint from $\mathscr{S}$.) Since $\mathscr{S}$ has cardinality c, there is a one-to-one function f mapping $\mathscr{S}$ onto $[0,1]$ (Theorem 10.3.8). As $\mathscr{T} \setminus \mathscr{S}$ is a subset of $\mathscr{T}$, it has cardinality at most c. Thus, there is a one-to-one function g mapping $\mathscr{T} \setminus \mathscr{S}$ into $[2,3]$.

Since $[0,1] \cup [2,3] \subset \mathbb{R}$, $\big|[0,1] \cup [2,3]\big| \leq c$. A one-to-one function from $\mathscr{S} \cup (\mathscr{T} \setminus \mathscr{S})$ into $[0,1] \cup [2,3]$ is given by sending x to $f(x)$ if x is in $\mathscr{S}$ and x to $g(x)$ if x is in $\mathscr{T} \setminus \mathscr{S}$. (This is where we use the fact that $\mathscr{S}$ and $\mathscr{T} \setminus \mathscr{S}$ are disjoint; otherwise, the new function would not be well-defined.) Thus, $\big|\mathscr{S} \cup (\mathscr{T} \setminus \mathscr{S})\big| \leq c$. Since $\mathscr{S}$ is a subset of $\mathscr{S} \cup (\mathscr{T} \setminus \mathscr{S})$, $\big|\mathscr{S} \cup (\mathscr{T} \setminus \mathscr{S})\big| \geq c$. Therefore, by the Cantor-Bernstein Theorem (10.3.5), $\big|\mathscr{S} \cup (\mathscr{T} \setminus \mathscr{S})\big| = c$.

10. What is the cardinality of $\mathbb{R}^2 = \big\{(x,y) : x,y \in \mathbb{R}\big\}$ (the *Euclidean plane*)?

Answer: We have already seen that the cardinality of the unit square, $[0,1] \times [0,1]$, is c (Theorem 10.3.30) and that $|\mathbb{R}| = \big|[0,1]\big|$ (Theorem 10.3.8). It follows from Problem 4(a) that $\big|\mathbb{R}^2\big| = |\mathbb{R} \times \mathbb{R}| = \big|[0,1] \times [0,1]\big| = c$.

11. What is the cardinality of the set of all complex numbers?

Answer: A one-to-one function mapping $\mathbb{R}^2$ onto $\mathbb{C}$ is given by $f(a,b) = a + bi$. Thus, $\big|\mathbb{R}^2\big| = |\mathbb{C}|$, and it follows from Problem 10 that $|\mathbb{C}| = c$.

14. What is the cardinality of the unit cube, where the unit cube is $\big\{(x,y,z) : x,y,z \in [0,1]\big\}$?

Answer: We have seen that the cardinality of the unit square, $[0,1] \times [0,1]$, is c (Theorem 10.3.30), which is also the cardinality of $[0,1]$ (Theorem 10.3.8). The unit cube can be regarded as $\big([0,1] \times [0,1]\big) \times [0,1]$. Therefore, it follows from Problem 4(a) that the cardinality of the unit cube is c.

15. What is the cardinality of $\mathbb{R}^3 = \big\{(x,y,z) : x,y,z \in \mathbb{R}\big\}$?

Answer: The cardinality of $\mathbb{R}^3$ is c. By Problem 10, the cardinality of $\mathbb{R}^2$ is c. Since $\mathbb{R}^3 = \mathbb{R}^2 \times \mathbb{R}$, it follows from Problem 4(a) that $\big|\mathbb{R}^3\big| = \big|\mathbb{R}^2 \times \mathbb{R}\big| = \big|\mathbb{R} \times \mathbb{R}\big| = c$.

19. Find the cardinality of the set $\big\{(x,y) : x \in \mathbb{R},\ y \in \mathbb{Q}\big\}$.

Answer: The cardinality is c. To see this, let $S = \{(x,y) : x \in \mathbb{R},\ y \in \mathbb{Q}\}$. Since $S \subset \mathbb{R}^2$, $|S| \leq c$. However, $\{(x,0) : x \in \mathbb{R}\}$ is a subset of S and it has cardinality c (since the mapping f that sends $(x,0)$ to x is clearly a one-to-one mapping of this set onto $\mathbb{R}$). Therefore, $c \leq |S| \leq c$ and it follows by the Cantor-Bernstein Theorem (10.3.5) that $|S| = c$.

20. What is the cardinality of the set of all numbers in the interval $[0,1]$ that have decimal expansions that end with an infinite sequence of 7's?

Answer: There are two easy natural proofs of the fact that the cardinality of this set is $\aleph_0$. For the first proof, simply note that every element of the set is rational, so the set is a subset of the set of rational numbers, which finishes the proof. Alternately, the result is a very straightforward application of the Enumeration Principle (10.3.16), since each element x in the set can be labeled $.a_1a_2a_3\ldots a_n$, where a_n is the last digit in the decimal expansion of x before the infinite sequence of 7's, and each a_i is in $\{0,1,2,3,4,5,6,7,8,9\}$.

22. Suppose that $\mathscr{T}$ is an infinite set and $\mathscr{S}$ is a countable set. Show that $\mathscr{S}\cup\mathscr{T}$ has the same cardinality as $\mathscr{T}$.

Answer: Since $\mathscr{T}$ is infinite, it has a countably infinite subset (Theorem 10.3.24). Denote one such by $\mathscr{A}=\{a_1,a_2,\ldots\}$. Since $\mathscr{S}$ is countable, it can be enumerated $\mathscr{S}=\{b_1,b_2,\ldots\}$. Assume first that $\mathscr{S}$ and $\mathscr{T}$ are disjoint. A one-to-one onto function $f:\mathscr{T}\to\mathscr{T}\cup\mathscr{S}$ can then be defined by $f(x)=x$ if $x\notin\mathscr{A}$, $f(a_i)=a_{\frac{i}{2}}$ if i is even, and $f(a_i)=b_{\frac{i+1}{2}}$ if i is odd. To show that f is onto, first note that if x is in $\mathscr{T}$ but is not in $\mathscr{A}$, then $f(x)=x$. If x is an element a_i of A, then $f(a_{2i})=x$. If x is an element b_i of S, then $f(a_{2i-1})=x$. Thus f is onto. To see that f is also one-to-one, suppose $f(x)=f(y)$. If $f(x)$ and $f(y)$ are both in $\mathscr{T}\setminus\mathscr{A}$, then $f(x)=x$ and $f(y)=y$, so $x=y$. If $f(x)$ and $f(y)$ are both in $\mathscr{A}$, then $f(x)=a_i$ for some a_i, in which case $x=y=a_{2i}$. If $f(x)$ and $f(y)$ are both in $\mathscr{S}$, then $f(x)=b_i$ for some b_i, and $x=y=a_{2i-1}$. This proves the result in the case that $\mathscr{S}$ and $\mathscr{T}$ are disjoint.
If $\mathscr{S}$ and $\mathscr{T}$ are not disjoint, then $\mathscr{S}\cup\mathscr{T}=\mathscr{T}\cup(\mathscr{S}\setminus\mathscr{T})$, and the result follows from the disjoint case. (The set $\mathscr{S}\setminus\mathscr{T}$ is disjoint from $\mathscr{T}$, and it is countable since it is a subset of the countable set $\mathscr{S}$.)

23. Let $\mathscr{S}$ be the set of real numbers t such that $\cos t$ is algebraic. Prove that $\mathscr{S}$ is countably infinite.

Answer: Since cosine is one-to-one on $[0,\pi]$, the set of all $t\in[0,\pi]$ such that $\cos t$ is algebraic is in one-to-one correspondence with a subset of the set of all algebraic numbers, and is therefore countable (Theorem 10.3.20). Similarly, for each integer m, the set of all $t\in\big[(m-1)\pi,m\pi\big]$ such that $\cos t$ is algebraic is countable. Therefore, $\mathscr{S}$ is a countable union of countable sets, and thus $\mathscr{S}$ is countable (Theorem 10.2.10). Moreover, $\mathscr{S}$ is not finite since for any integer k, $\cos 2\pi k=\cos 0=1$, and so there are infinitely many t with $\cos t$ algebraic.

26. Prove that there does not exist a set with a countably infinite power set.

Answer: Let $\mathscr{S}$ be any set. If $\mathscr{S}$ is finite, then $|\mathscr{P}(\mathscr{S})| = 2^{|\mathscr{S}|}$ (Theorem 10.3.26), which is finite. If $\mathscr{S}$ is infinite, then $|\mathscr{S}| \geq \aleph_0$ (Theorem 10.3.24). Thus, $|\mathscr{P}(\mathscr{S})| \geq |\mathscr{P}(\mathbb{N})|$. Since $|\mathscr{P}(\mathbb{N})| = c$ (Theorem 10.3.28), it follows that $\mathscr{P}(\mathscr{S})$ is not countable. Therefore it is not possible for a set to have a power set with cardinality $\aleph_0$.

27. Find a one-to-one function mapping the interval $(-\frac{\pi}{2}, \frac{\pi}{2})$ onto $\mathbb{R}$.

Answer: The trigonometric function tan is a one-to-one mapping of $(-\frac{\pi}{2}, \frac{\pi}{2})$ onto $\mathbb{R}$.

28. (a) Prove directly that the cardinality of the closed interval $[0,1]$ is equal to the cardinality of the open interval $(0,1)$ by constructing a function $f : [0,1] \to (0,1)$ that is one-to-one and onto.

Answer: A suitable function f can be defined as follows. Let $f(x) = x$ for all x which are not equal to 0 or $\frac{1}{n}$ for any natural number n, and for each natural number n, let $f(\frac{1}{n}) = \frac{1}{n+2}$. Then, $f(1) = \frac{1}{3}$, and there is not yet any element which is sent to $\frac{1}{2}$. We can therefore define $f(0) = \frac{1}{2}$. It is clear that f is a one-to-one function mapping $[0,1]$ onto $(0,1)$.

29. Prove that a set is infinite if and only if it has the same cardinality as a proper subset of itself.

Answer: If $\mathscr{S}$ is a finite set, then its cardinality is n for some natural number n. Every proper subset of $\mathscr{S}$ has cardinality strictly less than n, so $\mathscr{S}$ does not have the same cardinality as any proper subset of itself. Now assume that $\mathscr{S}$ is infinite; we must prove that $\mathscr{S}$ has the same cardinality as a proper subset of itself. By Theorem 10.3.24, $\mathscr{S}$ has a countably infinite subset. Call such a subset $\mathscr{A} = \{a_1, a_2, \dots\}$. We show that $\mathscr{S}$ has the same cardinality as its proper subset $\mathscr{S} \setminus \{a_1\}$. A one-to-one onto function f from $\mathscr{S}$ to $\mathscr{S} \setminus \{a_1\}$ can be defined by letting $f(x) = x$ if $x \notin \mathscr{A}$ and $f(a_i) = a_{i+1}$ for every a_i in $\mathscr{A}$.

32. What is the cardinality of the set of all countable sets of real numbers?

Answer: We show that the cardinality is c. We begin by proving that the set of all countable subsets of $[0,1]$ has cardinality c. For this, we show that each countable subset can be specified by one real number.

For each countable subset $\mathscr{S}$ of $[0,1]$, there is a one-to-one function $f_{\mathscr{S}}$ from $\mathbb{N}$ onto $\mathscr{S}$. Thus, $\mathscr{S}$ can be written $\{f_{\mathscr{S}}(1), f_{\mathscr{S}}(2), \dots\}$. Writing each $f_{\mathscr{S}}(n)$ as an infinite decimal, we can list the elements of $\mathscr{S}$, as follows:

$$f_{\mathscr{S}}(1) = .a_{11}a_{12}a_{13}\cdots$$

$$f_{\mathscr{S}}(2) = .a_{21}a_{22}a_{23}\cdots$$

$$f_{\mathscr{S}}(3) = .a_{31}a_{32}a_{33}\cdots$$

$$\vdots$$

Let F be the function which sends each such set $\mathscr{S}$ to $.a_{11}a_{12}a_{21}a_{31}a_{22}a_{13}a_{14}\dots$. That is, each $\mathscr{S}$ is assigned to an infinite decimal created by zigzagging through the array given by $f_{\mathscr{S}}$, where the decimal is extended by an infinite number of 0's if the set $\mathscr{S}$ is finite. (This is similar to the proof that $\mathbb{Q}$ is countable (Theorem 10.1.14).) Now F is a one-to-one mapping of the collection of all countable subsets of $[0,1]$ into $[0,1]$. Therefore, the set of all countable subsets of $[0,1]$ has cardinality less than or equal to $\left|[0,1]\right| = c$. Conversely, the set of all countable subsets of $[0,1]$ contains the set of all singleton sets. Thus, the set of all countable subsets of $[0,1]$ has a subset with cardinality c. Therefore, the cardinality of the set of all countable subsets of $[0,1]$ is at least c. By the Cantor-Bernstein Theorem (10.3.5), the cardinality is equal to c.

We must extend the above to countable subsets of $\mathbb{R}$. Let g be any one-to-one mapping of $\mathbb{R}$ onto $[0,1]$. Then g induces a mapping of subsets of $\mathbb{R}$ to subsets of $[0,1]$, sending each subset $\mathscr{S}$ of $\mathbb{R}$ to $\{g(s) : s \in \mathscr{S}\}$. That induced mapping sends countable subsets to countable subsets. Therefore, it is a one-to-one mapping that sends the collection of countable subsets of $\mathbb{R}$ onto the collection of countable subsets of $[0,1]$.

33. Find the cardinality of the set of all lines in the plane.

Answer: The cardinality is c. First note that the set $\mathscr{S}$ of vertical lines (that is, the lines parallel to the y-axis) has cardinality c, since there is an obvious one-to-one correspondence between those lines and the x-axis, where each line corresponds to its point of intersection with the x-axis.

We now consider the set of all lines in the plane that are not vertical. Each such line has some real number, say m, as its slope. Moreover, each such line meets the y-axis in some point $(0,b)$. Thus if $\mathscr{T}$ denotes the set of all

non-vertical lines in the plane, then $\mathscr{T}$ is in one-to-one correspondence with $\{(b,m) : b,m \in \mathbb{R}\}$. Therefore, $\mathscr{T}$ has the same cardinality as $\mathbb{R}^2$, and this cardinality is c (by Problem 10). It now follows that the set of all lines in the plane, equal to $\mathscr{S} \cup \mathscr{T}$, has cardinality c, by Problem 9.

34. Show that the set of all functions mapping $\mathbb{R} \times \mathbb{R}$ into $\mathbb{Q}$ has cardinality 2^c.

Answer: Let $\mathscr{F}$ denote the set of functions mapping $\mathbb{R} \times \mathbb{R}$ into $\mathbb{Q}$. Since $|\mathbb{R} \times \mathbb{R}| = c$ (by Problem 10), the set of characteristic functions of $\mathbb{R} \times \mathbb{R}$ has cardinality 2^c (by Theorem 10.3.32 it is the same as the cardinality of the set of subsets of $\mathbb{R} \times \mathbb{R}$, and a one-to-one function mapping $\mathbb{R} \times \mathbb{R}$ onto $\mathbb{R}$ induces a one-to-one function mapping $\mathscr{P}(\mathbb{R} \times \mathbb{R})$ onto $\mathscr{P}(\mathbb{R})$). Since the set of characteristic functions is a subset of $\mathscr{F}$, $|\mathscr{F}| \geq 2^c$.

To show that $|\mathscr{F}| \leq 2^c$, note that each function f from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{Q}$ defines a subset $\mathscr{H}_f$ of $\mathbb{R}^3$ by $\mathscr{H}_f = \{(a,b,c) : a,b \in \mathbb{R} \text{ and } f(a,b) = c\}$. The mapping from f to $\mathscr{H}_f$ is one-to-one since if $\mathscr{H}_{f_1} = \mathscr{H}_{f_2}$, then $f_1(a,b) = f_2(a,b)$ for every $(a,b) \in \mathbb{R} \times \mathbb{R}$, and so $f_1 = f_2$. Thus, there is a one-to-one function mapping $\mathscr{F}$ into the power set of $\mathbb{R}^3$, from which it follows that $|\mathscr{F}| \leq \left|\mathscr{P}(\mathbb{R}^3)\right|$. Since $\left|\mathbb{R}^3\right| = c$ (by Problem 15), $\left|\mathscr{P}(\mathbb{R}^3)\right| = 2^c$. Therefore, $|\mathscr{F}| \leq 2^c$, and so, by the Cantor-Bernstein Theorem (10.3.5), $|\mathscr{F}| = 2^c$.

35. Prove the following: If n is the smallest natural number such that a polynomial of degree n with integer coefficients has x_0 as a root, and if p and q are polynomials of degree n with integer coefficients that have the same leading coefficients (i.e., coefficients of x^n) and each have x_0 as a root, then $p = q$.

Answer: Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $q(x) = a_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Since $p(x_0) = 0 = q(x_0)$:

$$\begin{aligned} 0 &= p(x_0) - q(x_0) \\ &= (a_n x_0^n + a_{n-1}x_0^{n-1} + \cdots + a_0) - (a_n x_0^n + b_{n-1}x_0^{n-1} + \cdots + b_0) \\ &= (a_{n-1} - b_{n-1})x_0^{n-1} + \cdots + (a_0 - b_0) \end{aligned}$$

Therefore, x_0 is a root of the polynomial $(a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_0 - b_0)$. This latter polynomial has integer coefficients and has degree smaller than n. Moreover, it has x_0 as a root. Since n is the smallest natural number such that a polynomial of degree n with integer coefficients has x_0 as a root, it follows that all of the coefficients of this latter polynomial are 0. Thus, $a_i = b_i$ for all i, and so $p = q$.

40. Prove that the union of c sets that each have cardinality c has cardinality c.

Answer: The union clearly has a subset of cardinality c (any one of the original c sets), so the union has cardinality greater than or equal to c. We will show that the union also has cardinality less than or equal to c.

The idea is to show that there is a one-to-one mapping of the union into $\mathbb{R}^2$. Let $\mathscr{U}$ be the union, and let $\mathscr{C}$ be the collection of sets (so the elements of $\mathscr{C}$ are the original c sets). Since the cardinality of $\mathscr{C}$ is c, there is a one-to-one onto mapping $F : \mathscr{C} \to \mathbb{R}$. This gives a labeling of each element of $\mathscr{C}$ by an element of $\mathbb{R}$, by labeling each set $\mathscr{S}$ in $\mathscr{C}$ by $F(\mathscr{S})$. Thus, $\mathscr{C} = \{\mathscr{S}_r : r \in \mathbb{R}\}$ (where $r = F(\mathscr{S})$).

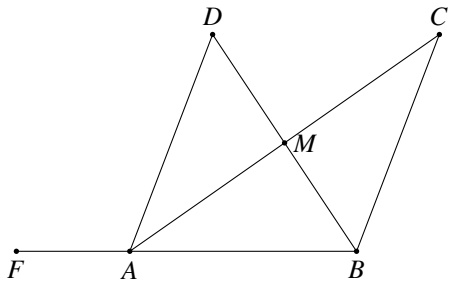
Each set $\mathscr{S}_r$ has cardinality c, so for each r there is a one-to-one mapping f_r taking $\mathscr{S}_r$ onto $\mathbb{R}$. Each $x \in \mathscr{U}$ is in some $\mathscr{S}_r$, and we would like to send each such x to $(r, f_r(x))$. This would send $\mathscr{U}$ onto $\mathbb{R}^2$. However, since the sets $\mathscr{S}_r$ may not be disjoint, this mapping may not be well-defined. To deal with this issue, let $\mathscr{C}'$ be the collection of all sets of the form $\{(r,s) : s \in \mathscr{S}_r\}$. That is, $\mathscr{C}'$ is the collection of all $\{r\} \times \mathscr{S}_r$ for $\mathscr{S}_r$ in $\mathscr{C}$. Let $\mathscr{U}'$ be the union of all the sets in $\mathscr{C}'$. A one-to-one onto (and well-defined) mapping from $\mathscr{U}'$ to $\mathbb{R}^2$ is given by sending each (r,x) to $(r, f_r(x))$. Since $\mathbb{R}^2$ has cardinality c (by Problem 10), $\mathscr{U}'$ has cardinality c. Next we show that $|\mathscr{U}| \leq |\mathscr{U}'|$. For each $x \in \mathscr{U}$, let $h(x)$ be some r such that $x \in \mathscr{S}_r$, and let $H : \mathscr{U} \to \mathscr{U}'$ be defined by $H(x) = (h(x), x)$. Since H is one-to-one, $|\mathscr{U}| \leq |\mathscr{U}'| = c$. Since we also have $|\mathscr{U}| \geq c$, the Cantor-Bernstein Theorem (10.3.5) implies that $|\mathscr{U}| = c$.

Chapter 11
Fundamentals of Euclidean Plane Geometry

Solutions to Selected Exercises

3. In the given diagram, the line segment BD is perpendicular to the line segment AC, the length of AM is equal to the length of MC, the measure of $\angle C$ is 35° and the measure of $\angle FAD$ is 111°.

(a) Prove that triangle ABM is congruent to triangle CBM.



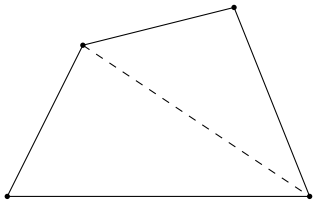
Answer: (a) It is given that $CM = MA$, and the triangles ABM and CBM have the side MB in common. Since DB is perpendicular to CA, $\angle CMB = 90^\circ = \angle AMB$. Therefore, by side-angle-side (11.1.2), $\triangle ABM$ is congruent to $\triangle CBM$.

4. Prove that two right triangles are congruent if they have equal hypotenuses and a pair of equal legs.

Answer: If h is the length of the hypotenuses and a is the length of the equal legs, then, by the Pythagorean Theorem (11.3.7), the lengths of the other legs are both equal to the square root of $h^2 - a^2$. Thus, by side-side-side (Theorem 11.1.8), the triangles are congruent.

5. A *quadrilateral* is a four-sided figure in the plane. Prove that the sum of the angles of a quadrilateral is 360 degrees.

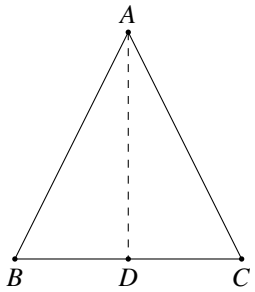
Answer: Connect two opposite vertices of the quadrilateral by a line segment, dividing the quadrilateral into two triangles.



It is apparent that the sum of the angles of the quadrilateral is equal to the sum of the angles of the two triangles. Since the sum of the angles of each of the triangles is 180 degrees (Theorem 11.2.5), the sum of the angles of the quadrilateral is 360 degrees.

7. Prove that if two angles of a triangle are equal, then the sides opposite those angles are equal.

Answer: Let ABC be a triangle with $\angle ABC = \angle ACB$. Draw the bisector of $\angle BAC$ and let its point of intersection with BC be D.

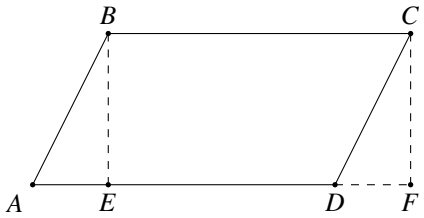


Then triangles BAD and CAD have two pairs of equal angles and also have a side in common, AD. It follows that these triangles are congruent by angle-angle-side (Corollary 11.2.7) and, thus, that the corresponding sides AB and AC are equal.

9. A *parallelogram* is a four-sided figure in the plane whose opposite sides are parallel to each other. Prove the following:

(b) The area of a parallelogram is the product of the length of any side and the length of a perpendicular to that side from a vertex not on that side.

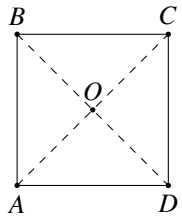
Answer: (b) Let the parallelogram be $ABCD$, as pictured below. Drop a perpendicular from B to the side AD and call E the point of intersection with the side. Drop a perpendicular from C to the extension of the side AD and call the point of intersection F.



Since AD is parallel to BC, the length BE is equal to the length CF (Lemma 11.3.9). Also, since AB is parallel to DC, the corresponding angles BAE and CDF are equal to each other (Theorem 11.2.3). Thus, triangles ABE and CDF are right triangles that are congruent to each other by angle-angle-side (Corollary 11.2.7). It follows that the area of triangle ABE is equal to the area of triangle CDF, and therefore that the area of the original parallelogram $ABCD$ is equal to the area of the rectangle $BCFE$, and this is the product of the length of BC and the length of CF.

11. A *square* is a four-sided figure in the plane all of whose sides are equal to each other and all of whose angles are right angles. The *diagonals* of the square are the lines joining opposite vertices. Prove that the diagonals of a square are perpendicular to each other.

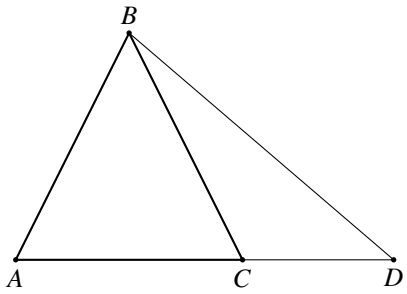
Answer: Let the vertices of the square be A, B, C, D. Draw the diagonals, which are line segments AC and BD, and label their intersection by O, as shown in the diagram below.



Then $\triangle ABD$ is isosceles, so $\angle ABD = \angle ADB$ (Theorem 11.1.4), and, since $\angle BAD = 90^\circ$, $\angle ABD = 45^\circ$ (since the sum of the angles of triangle ABD is 180°). The same argument applied to the isosceles triangles ACB, CDA and BDC shows that the triangles BCO, BAO, CDO, and DAO, all have both of their "base angles" (those angles for which one side is a side of the square) equal to 45°. Therefore, the remaining angle in each triangle is 90°, from which it follows that each of the angles BOC, BOA, DOC, and DOA is 90 degrees.

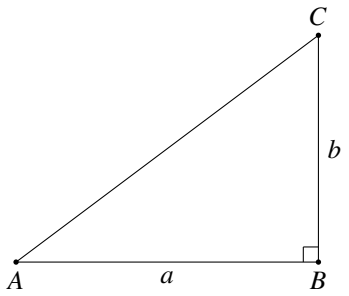
13. Give an example of two triangles that agree in "angle-side-side" but are not congruent to each other.

Answer: Start with an isosceles triangle, ABC, where $AB = BC$. Extend AC past C to a point D. Connect D and B.



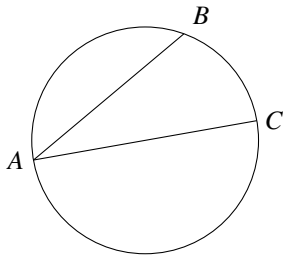
Then triangles ABD and CBD share the angle ADB and the side BD. Since $BA = BC$, the triangles ABD and CBD agree in angle-side-side. However, they are obviously not congruent.

15. Prove the converse of the Pythagorean Theorem; i.e., show that if the lengths of the sides of a triangle satisfy the equation $a^2 + b^2 = c^2$, then the triangle is a right triangle.

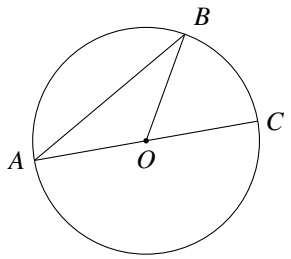


Answer: Let a triangle be given with sides a, b, and c satisfying the equation. Take a line segment AB such that the length of AB is a. Then draw a line segment perpendicular to AB at the point B and extend it to a point C such that the length of BC is b. Connecting C to A by a line segment creates a right triangle ABC (since $\angle ABC$ is 90° by construction). By the Pythagorean Theorem (11.3.7), the square of the length of the side of CA is c^2, so the length of CA is c. Thus, $\triangle ABC$ agrees with the originally given triangle in side-side-side, so those two triangles are congruent (Theorem 11.1.8). Therefore the angles of the two triangles are equal to each other and, in particular, one of the angles of the original triangle is 90 degrees.

17 . (This problem generalizes the result of Theorem 11.3.12.) Prove that the measure of an angle inscribed in a circle is one half the measure of the arc cut off by the angle. That is, in the diagram below, the number of degrees of $\angle BAC$ is half the number of degrees in the arc BC. (The number of degrees in a full circle is 360, and the number of degrees in any arc of a circle is the product of 360 and the length of that arc divided by the circumference of the circle.)

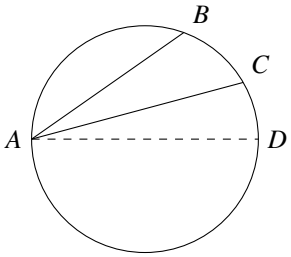


Answer: First consider the special case where AC is a diameter of the circle. Let O be the midpoint of AC, which is the center of the circle. Draw a line segment connecting O to B. Then $\angle BOC + \angle BOA = \angle BAO + \angle BOA + \angle ABO$ (since the sums are both 180°). It follows that $\angle BOC = \angle BAO + \angle ABO$. Since AC is a diameter, $BO = AO$, as they are both radii of the circle. Thus, $\triangle ABO$ is isosceles, from which it follows that $\angle BAO = \angle ABO$ (Theorem 11.1.14). Therefore $\angle BOC$ is twice $\angle BAO$.



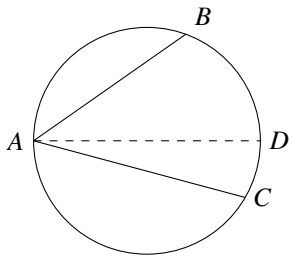
Thus we have shown that $\angle BAC$ is half of $\angle BOC$. The proof of this special case, where one side is a diameter, will be complete if we show that the measure of $\angle BOC$ is the same as the measure of the arc BC. But this follows immediately from the fact that the measure of the central angle BOC is the same fraction of a full rotation of 360 degrees as the fraction that the measure of the arc BC is of the full circle of 360 degrees. This establishes the special case where one side of the angle is a diameter of the circle.

We now consider the case where AC is not a diameter of the circle, which we divide into several sub-cases. Draw a diameter of the circle from A. Suppose that this diameter is below AC, so that it intersects the circle across from A at a point D below C and below B (that is, outside of the angle BAC).



By the previous case, the number of degrees of $\angle BAD$ is half the number of degrees in the arc BD, and the number of degrees of $\angle CAD$ is half the number of degrees in the arc CD. Since $\angle BAC = \angle BAD - \angle CAD$, the number of degrees in $\angle BAC$ is half the number of degrees in the arc BD minus half the number of degrees in the arc CD, which is half the number of degrees in $BD - CD$, which is half the number of degrees in BC. Since rotating, flipping, and interchanging B and C does not change the angle, this proof also applies to the case where D is above both C and B.

The remaining case to consider is the one in which the diameter is above AC but below AB, intersecting the circle at a point D between B and C.



Then the measure of the angle BAC is the measure of $\angle BAD$ plus the measure of $\angle DAC$, which is one half of the number of degrees in the arc BD plus one half the number of degrees in the arc DC, which is one half of the number of degrees in the arc BC. Thus, in all cases, the measure of an angle inscribed in a circle is one half of the measure of the arc cut off by the angle.

Chapter 12
Constructability

Solutions to Selected Exercises

1. Determine which of the following numbers are constructible.

(a) $\frac{1}{\sqrt{3+\sqrt{2}}}$ (d) $\sqrt[16]{79}$ (l) $\cos 10^\circ$

(b) $\sqrt[6]{79}$ (j) $\cos 51^\circ$ (n) $11^{\frac{3}{2}}$

Answer:
(a) First, $3+\sqrt{2}$ is constructible since it is in $\mathbb{Q}(\sqrt{2})$. Since square roots and quotients of constructible numbers are constructible (Theorem 12.2.15 and Corollary 12.2.7), $\frac{1}{\sqrt{3+\sqrt{2}}}$ is constructible.

(b) It is not constructible. Suppose it was. Then $79^{\frac{1}{6}} \cdot 79^{\frac{1}{6}} = 79^{\frac{1}{3}}$ would be constructible (since the constructible numbers are a field (Theorem 12.2.10)), which would imply that the cubic polynomial $x^3 - 79$ has a constructible root. But then $x^3 - 79$ would have a rational root (Theorem 12.3.22) and, using the Rational Roots Theorem (8.19), any rational root would have to be an integer. However, this is impossible since 3^3 is less than 79 and 4^3 is greater than 79, so $x^3 - 79$ has no integer roots.

(d) This is constructible. Since 79 is constructible, repeatedly applying the fact that the square root of a constructible number is constructible (see Theorem 12.2.15) shows that $\sqrt[16]{79}$ is constructible.

(j) This is constructible, since $\cos 51^\circ$ is constructible if 51° is a constructible angle (Theorem 12.3.13), and 51° is a constructible angle since 51 is a multiple of 3 (Theorem 12.4.13).

(l) This is not constructible, since, if it was, then 10° would be a constructible angle (Theorem 12.3.13), but 10° is not a constructible angle since 10 is not a multiple of 3.

(n) This is constructible. Since 11^3 is an integer, it is constructible, and then, since the square root of a constructible number is constructible (Theorem 12.2.15), $11^{\frac{3}{2}}$ is constructible.

2. Determine which of the following angles are constructible.

(a) 6° (i) 92.5° (j) 37.5°

Answer:
(a) This is constructible, since 6 is a multiple of 3 (Theorem 12.4.13)

(i) This angle is not constructible. Suppose it was. Then doubling this would produce a constructible angle (Corollary 12.1.7), but an angle of 185° is not constructible, since 185 is not a multiple of 3 (Theorem 12.4.13).

(j) This angle is constructible. A 75° angle is constructible because it is a multiple of 3 (Theorem 12.4.13). Since 37.5° is half of 75°, it is also constructible (Theorem 12.1.4).

3. Determine which of the following angles can be trisected.

(a) 12°

Answer: (a) This angle cannot be trisected. Suppose it could. Then, since an angle of 12° is constructible, trisecting it would show that an angle of 4° is constructible. However, 4 is not a multiple of 3, so it is not possible to construct an angle of 4° (Theorem 12.4.13).

4. Determine which of the following polynomials have at least one constructible root.

(a) $x^4 - 3$ (f) $x^3 - 2x - 1$
(c) $x^4 + \sqrt{7}x^2 - \sqrt{3} - 1$ (j) $2x^3 - 4x^2 + 1$

Answer:
(a) This polynomial has a constructible root. Since 3 is constructible and the square root of a constructible number is constructible (Theorem 12.2.15), it follows that $\sqrt{3}$ is constructible and $x = \sqrt{\sqrt{3}} = \sqrt[4]{3}$ is constructible, which satisfies $x^4 - 3 = 0$.

(c) This polynomial has a constructible root. To see this, note that x is a root of this polynomial if $y = x^2$ and y is a root of the polynomial $y^2 + \sqrt{7}y - \sqrt{3} - 1$. By the Quadratic Formula (Problem 6 in Chapter 9), $y_0 = \frac{-\sqrt{7}+\sqrt{11+4\sqrt{3}}}{2}$ is a root of this new polynomial. Since the square root of a constructible number is constructible (Theorem 12.2.15) and the constructible numbers form a field (Theorem 12.2.10), y_0 is constructible. Also, y_0 is positive. The positive square root of y_0 is then a constructible root of the original polynomial.

(f) Clearly, -1 is a constructible root of this polynomial. (If it has a constructible root, it must have a rational root (Theorem 12.3.22). By the Rational Roots Theorem (8.1.9), such a root would have to be ± 1.)

(j) If it had a constructible root, then it would have a rational root (Theorem 12.3.22). By the Rational Roots Theorem (8.1.9), such a root would have to be ± 1 or $\pm\frac{1}{2}$. Substituting these numbers into the polynomial shows that none of them are roots. Therefore the polynomial does not have a constructible root.

5. Determine which of of the following regular polygons can be constructed with straightedge and compass.

(a) A regular polygon with 14 sides.
(d) A regular polygon with 240 sides.

Answer:
(a) Such a polygon cannot be constructed. If it could, then a regular polygon with 7 sides would be constructible (Theorem 12.4.7)). However, a regular polygon with 7 sides is not constructible (Theorem 12.4.12).

(d) Such a regular polygon can be constructed. First note that a regular polygon with 120 sides can be constructed, since its central angle is $\frac{360}{120} = 3$ degrees, and so it is constructible (the central angle is constructible by Theorem 12.4.13, and this implies that the polygon is constructible, by Theorem 12.4.5). Thus, a regular polygon with $2(120) = 240$ sides is constructible (Theorem 12.4.7).

7. True or False:

(a) If the angle of θ degrees is constructible and the number x is constructible, then the angle of $x \cdot \theta$ degrees is constructible.

(d) There is an angle θ such that $\cos\theta$ is constructible, but $\sin\theta$ is not constructible.

Answer:
(a) False. For example, an angle of 30 degrees is constructible, and the number $\frac{2}{3}$ is constructible, but an angle of 20 degrees is not constructible (Theorem 12.3.23).

(d) This is false. Suppose $\cos\theta$ is constructible. Then, since the constructible numbers are a field, $1-\cos^2\theta$ is also constructible. Since $\sin^2\theta = 1-\cos^2\theta$, it follows that $\sin^2\theta$ is constructible. Since the square root of a constructible number is constructible, $\sin\theta$ is constructible (both $\sqrt{\sin^2\theta}$ and $-\sqrt{\sin^2\theta}$ are constructible).

9. Determine which of the following numbers are constructible.

(b) $\sin 75^\circ$

Answer:
(b) This is constructible. Since 75 is a multiple of 3, 75° is a constructible angle (Theorem 12.4.13), and therefore $\cos(75^\circ)$ is a constructible number (Theorem 12.3.13). Since $\sin^2(75^\circ) = 1-\cos^2(75^\circ)$, it follows that $\sin^2(75^\circ)$ is constructible, and so $\sin(75^\circ)$ is constructible as well.

10. Determine which of the following numbers are constructible. (The angles below are in radians.)

(b) $\cos\pi$

Answer:
(b) Since $\cos\pi = -1$, it is a constructible number.

11.(b) Prove that the side of a cube with volume a natural number n is constructible if and only if $n^{\frac{1}{3}}$ is a natural number.

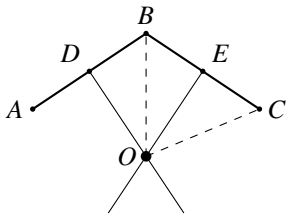
Answer:
(b) If the side of a cube with volume n is constructible, then $n^{\frac{1}{3}}$ is a constructible number, so $x^{\frac{1}{3}} - n$ has a constructible root, and therefore it has a rational root (Theorem 12.3.22). By the Rational Roots Theorem (8.1.9), such a root must have denominator 1 (if it is in lowest terms), so it has to be an integer. It also has to be positive, since n is positive. Therefore, if $x^{\frac{1}{3}} - n$ has a constructible root, then it has a root which is a natural number, so $n^{\frac{1}{3}}$ (the real cube root of n) is a natural number.

12. Using mathematical induction, prove that, for every integer $n \geq 1$, a regular polygon with $3 \cdot 2^n$ sides can be constructed with straightedge and compass.

Answer: For the case $n = 1$, the central angle of a regular polygon with 6 sides is $\frac{360}{6} = 60$ degrees which is constructible (Theorem 12.3.14). Therefore a regular polygon with 6 sides is constructible (Theorem 12.4.5). Now let k be any natural number and assume that a regular polygon of $3 \cdot 2^k$ sides is constructible. Then, by Theorem 12.4.7, a regular polygon of $2 \cdot (3 \cdot 2^k) = 3 \cdot 2^{k+1}$ sides is constructible, and the result follows by induction.

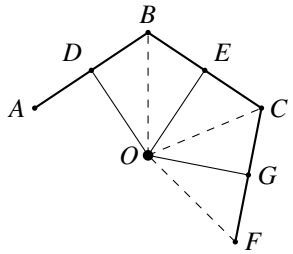
13. Prove that, given a regular polygon, its center can be constructed using only a straightedge and compass.

Answer:
Let two adjacent sides of the polygon be labelled AB and BC. As shown in the diagram below, construct perpendicular bisectors of the two sides. Let D denote the midpoint between A and B, and let E denote the midpoint between between B and C. Let O be the point of intersection of the two perpendicular bisectors.



We will show that O is the center of the polygon (i.e., it has the same distance from each vertex). Join O to B by a line segment. This creates tri-

angles DOB and EOB as shown in the diagram. Each of these triangles is a right triangle. They share the side BO, and the length of BE is the same as the length of BD (each is half of a side of the given regular polygon). By the Pythagorean Theorem (11.3.7), their third sides have equal length. Thus these two triangles are congruent (by side-side-side, Theorem 11.1.8). Join O to C by a line segment. This creates a right triangle EOC which is congruent to the triangle EOB since they share the side EO and have second sides BE and EC of equal length. Thus $OC = OB$.



Let the other vertex of the regular polygon which is adjacent to C be F, and let G be the midpoint of CF. We must show that OF is equal to OC. From the congruence of triangles DOB and EOB, we have $\angle OBD = \angle OBE$. Thus $\angle OBE$ is one half of the angle between adjacent sides of the original polygon. Moreover, from the congruence of triangles EOC and EOB, it follows that $\angle OCE$ is also half of the angle of the regular polygon. Therefore, $\angle OCG$ is equal to $\angle OCE$. Then by side-angle-side (11.1.2), $\triangle EOC$ is congruent to $\triangle GOC$. It follows that $\angle OGC = 90^\circ$, and since $\angle OGF$ sums with $\angle OGC$ to a straight angle, it is also 90°. Since the right triangles GOC and GOF share the side OG, and have second sides CG and GF of equal length, they are congruent to each other. Thus, $OF = OC$, and all the right triangles DOB, EOB, EOC, GOC, and GOF are congruent to each other. This process can then be continued by letting H be the other vertex adjacent to F, and repeating the above.

14. Prove that an acute angle cannot be trisected with straightedge and compass if its cosine is:

(a) $\frac{3}{7}$

Answer:
(a) Since the cosine of the given angle is a constructible number, it follows that the angle itself is constructible (Theorem 12.3.13). If the angle could

be trisected, then there would be a constructible acute angle θ such that $\cos 3\theta = \frac{3}{7}$. We use the trigonometric identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ (Theorem 12.3.16). If θ were constructible, then $\cos\theta$ would be a constructible root of $4x^3 - 3x - \frac{3}{7}$. Then $4x^3 - 3x - \frac{3}{7}$ would have a rational root (by Theorem 12.3.22). Multiplying the polynomial by 7, it follows that the polynomial $28x^3 - 21x - 3$ would have a rational root. By the Rational Roots Theorem (8.1.9), such a root (in lowest terms) would have to have numerator ± 1 or ± 3 and denominator ± 1, ± 2, ± 4, ± 7, ± 14, or ± 28. Checking all the possibilities individually shows that none of them are roots.

15. Can a polynomial of degree 4 with rational coefficients have a constructible root without having a rational root?

Answer: Yes. An example is the polynomial $x^4 - 2$. Since square roots of constructible numbers are constructible, $2^{\frac{1}{2}}$ is constructible, and then $(2^{\frac{1}{2}})^{\frac{1}{2}} = 2^{\frac{1}{4}}$ is constructible. Thus, the polynomial $x^4 - 2$ has a constructible root. By the Rational Roots Theorem (8.1.9), if $x^4 - 2$ has a rational root it must be ± 1 or ± 2, but none of these are roots, so it has no rational roots.

16. Prove that the following equation has no constructible solutions:

$$x^3 - 6x + 2\sqrt{2} = 0.$$

[Hint: You can use Theorem 12.3.22 if you make an appropriate substitution.]

Answer:
Suppose r is a constructible solution. Since $\sqrt{2}$ is constructible and the constructible numbers form a field, $\frac{r}{\sqrt{2}}$ would then be constructible. Let $t = \frac{r}{\sqrt{2}}$. Then $r = t\sqrt{2}$, and so there is a constructible number t such that $(t\sqrt{2})^3 - 6t\sqrt{2} + 2\sqrt{2} = 0$. It follows that $t^3 2\sqrt{2} - 6t\sqrt{2} + 2\sqrt{2} = 0$, so $\sqrt{2}(2t^3 - 6t + 2) = 0$, and thus $2t^3 - 6t + 2 = 0$. Therefore the polynomial $2x^3 - 6x + 2$ has a constructible root, and so it has a rational root (Theorem 12.3.22). The Rational Roots Theorem (8.1.9) implies that such a root has to be ± 1, ± 2, or $\pm\frac{1}{2}$. Substituting these numbers into the equation shows that none of them are roots. It follows that there can be no such r.

17. Let t be a transcendental number. Prove that $\{(a+bt) : a,b \in \mathbb{Q}\}$ is not a subfield of $\mathbb{R}$.

Answer:
Suppose it was a subfield of $\mathbb{R}$. The set contains $t = 0+1\cdot t$, so if it was a field, it would also contain t^2. Then $t^2 = a+bt$ for some $a,b \in \mathbb{Q}$. This implies that $t^2 - bt - a = 0$, so t is a root of the polynomial $x^2 - bx - a$. Since this polynomial has rational coefficients, this contradicts the fact that t is transcendental (multiplying through by the product of the denominators of b and a gives a polynomial with integer coefficients which has t as a root).

20. Is $\left\{a\sqrt{2} : a \in \mathbb{Q}\right\}$ a subfield of $\mathbb{R}$?

Answer: No. For example, it does not contain 1. For if $1 = a\sqrt{2}$ with a rational, then $a \neq 0$ and $\frac{1}{a} = \sqrt{2}$, which contradicts the fact that $\sqrt{2}$ is not rational (Theorem 8.2.2).

21. Is the set of all towers countable? (Recall that a *tower* is a finite sequence of subfields of $\mathbb{R}$, the first of which is $\mathbb{Q}$, such that the other subfields are obtained from their predecessors by adjoining square roots.)

Answer: Yes, by the Enumeration Principle (10.3.16). Each tower can be labelled by a finite sequence from the set $\{0,1,2,\ldots,9,\sqrt{\ },/,-,+,,\}$. Begin by putting the first square root adjoined, then a comma, then the second square root adjoined (which may be a square root of any positive number already in the tower), then a comma, and then the third and so on.

22. Prove the following.

(a) If x_0 is a root of a polynomial with coefficients in $\mathscr{F}(\sqrt{r})$, then x_0 is a root of a polynomial with coefficients in $\mathscr{F}$.
(b) Every constructible number is algebraic.

Answer:

(a) Let x_0 be a root of a polynomial with coefficients in $\mathscr{F}(\sqrt{r})$. Then there are a_i and b_i in $\mathscr{F}$ and a natural number n such that

$$(a_n + b_n\sqrt{r})x_0^n + \cdots + (a_1 + b_1\sqrt{r})x_0 + (a_0 + b_0\sqrt{r}) = 0.$$

Then

$$\begin{aligned} a_n x_0^n + \cdots + a_1 x_0 + a_0 &= -(b_n\sqrt{r}x_0^n + \cdots + b_1\sqrt{r}x_1 + b_0\sqrt{r}) \\ &= -\sqrt{r}(b_n x_0^n + \cdots + b_1 + b_0) \end{aligned}$$

so

$$(a_n x_0^n + \cdots + a_1 x_0 + a_0)^2 = r(b_n x_0^n + \cdots + b_1 x + b_0)^2.$$

Since r is in $\mathscr{F}$ and all the a_i and b_i are in $\mathscr{F}$, then squaring both sides, bringing everything over to one side, collecting terms, and replacing x_0 by a variable x gives a polynomial with coefficients in $\mathscr{F}$ which has x_0 as a root.

(b) If x_0 is a constructible number, then either it is rational (in which case we are done) or it is in some field $\mathscr{F}(\sqrt{r})$ which is at the end of a tower (Theorem 12.3.12). Then x_0 is a root of the polynomial $x - x_0$, which has coefficients in that $\mathscr{F}(\sqrt{r})$. Applying part (a) of this problem shows that x_0 is also a root of a polynomial that has coefficients in $\mathscr{F}$. If $\mathscr{F}$ is not $\mathbb{Q}$, then we can apply part (a) again to show that x_0 is a root of a polynomial with coefficients in the predecessor of $\mathscr{F}$ in the tower. Continuing this process a finite number of times shows that x_0 is a root of a polynomial with coefficients in $\mathbb{Q}$, and hence x_0 is algebraic. (A more formal proof would use induction on the length of the tower.)

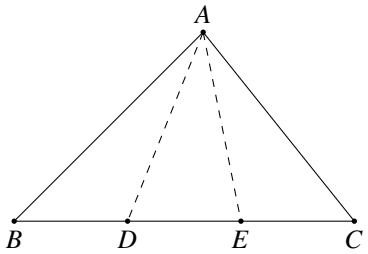
27. Suppose that regular polygons with m sides and n sides can be constructed, and m and n are relatively prime. Prove that a regular polygon of mn sides can be constructed.
[Hint: Use central angles and use the fact that a linear combination of m and n is 1.]

Answer: By Theorem 12.4.5, the central angles of the two given regular polygons are constructible. That is, angles of $\frac{360}{m}$ and $\frac{360}{n}$ degrees are constructible. Since m and n are relatively prime, there are integers s and t such that $sm + tn = 1$ (see page 50 of Chapter 7). Then one of s and t is positive and the other is negative. Assume that s is positive (if not, simply interchange the roles of s and t, and m and n, in the proof below). By placing s angles of size $\frac{360}{n}$ appropriately adjacent to each other, it is possible to construct an angle of $\frac{360}{n} \cdot s$ degrees. Similarly, it is possible to construct an angle of $\frac{360}{m} \cdot |t|$ degrees.

Since $\frac{360}{mn} = \frac{360(sm+tn)}{mn} = \frac{360sm+360tn}{mn} = \frac{360}{n}s + \frac{360}{m}t = \frac{360}{n} \cdot s - \frac{360}{m} \cdot |t|$, it follows that it is possible to construct an angle of $\frac{360}{mn}$ degrees (by "subtracting" an angle of $\frac{360}{m} \cdot |t|$ degrees from one of $\frac{360}{n} \cdot s$ degrees). Therefore, the central angle of a regular polygon with mn sides is constructible, and thus, a regular polygon of mn sides is constructible (Theorem 12.4.5).

29. (Very challenging) Prove that you cannot trisect an angle by trisecting the side opposite the angle in a triangle containing it. That is, prove that, if ABC is any triangle, there do not exist two lines through A such that those lines trisect both the side BC of the triangle and the angle BAC of the triangle.
[Hint: Suppose that there do exist two such lines. The lines then divide the triangle into three sub-triangles. One approach uses the easily established fact that all three sub-triangles have the same area.]

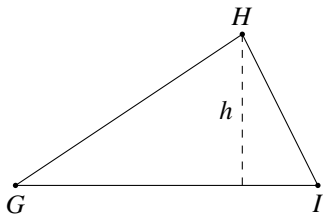
Answer: Let an arbitrary triangle ABC be given. Suppose there exist lines AD and AE, as pictured in the diagram, so that $\angle BAD$ is equal to $\angle DAE$ and $\angle EAC$. Also suppose that the line segment BD is equal to the line segments DE and EC.



We want to show that this is impossible. To establish that, we will show that the above would imply that the three triangles ABD, ADE, and AEC are all congruent to each other, after which we will demonstrate that that is not possible.

Take the base of each sub-triangle to be its side along BC so that its height is the height of triangle ABC. Then the length of the base of each sub-triangle is $\frac{1}{3}$ of BC, and the heights are the same, so the sub-triangles all have the same area.

We now want to show that if two triangles agree in angle-side and have equal areas, then they are congruent. Suppose we are given fixed points G and H, and an angle at G, as pictured below.



Each point I on the other side of G determines a unique triangle GHI. Let h denote the height of the triangle to the base GI. The height h is the same regardless of the position of I on the line. Since the area of the triangle GHI is $\frac{1}{2}$ of the product of h and the length of GI, the length GI is uniquely determined by the area of the triangle. Thus, any two triangles that agree in angle-side and area also have the same second side, GI, and therefore are congruent by side-angle-side (11.1.2).

The triangles ABD and AEC both agree in angle-side with the triangle ADE, so it follows from what we have shown so far that all three triangles are congruent. Therefore, $\angle ADE$ is equal to either $\angle ABD$ or $\angle ADB$. It is not possible that $\angle ADE = \angle ABD$, since $\angle ADE$ sums with $\angle ADB$ to a straight angle, while $\angle ABD$ sums with $\angle ADB$ and $\angle DAB$ to a straight angle. Thus, $\angle ADE = \angle ADB$. Similarly, $\angle AED = \angle AEC$. Since $\angle ADE + \angle ADB = 180^\circ = \angle AED + \angle AEC$, it follows that $\angle ADE = \angle ADB = \angle AED = \angle AEC = 90^\circ$. However, $\angle ADE$ and $\angle AED$ are two angles in the triangle AED, so their sum plus $\angle DAE$ is a straight angle. This contradicts the fact that their sum was already 180°.