1. Suppose that \(a, b, c,\) and \(d\) are integers.

(a) Prove that if \(a\mid b\) and \(b\mid a\), then \(a = \pm b\).

**Proof:** By hypothesis, there exist \(k, l \in \mathbb{Z}\) such that \(b = ka\) and \(a = lb\). Substituting the first equality into the second yields \(a = (kl)a\). This implies that \(kl = 1\). Since \(k, l \in \mathbb{Z}\), \(k = \pm 1 = l\), and thus \(a = \pm b\). ■

(b) Prove that if \(a\mid b\) and \(c\mid d\), then \(ac\mid bd\).

**Proof:** By hypothesis, there exist \(k, l \in \mathbb{Z}\) such that \(b = ka\) and \(d = lc\). Multiplying these equalities together yields \(bd = (kl)ac\). Since \(kl \in \mathbb{Z}\), we see that \(ac\mid bd\). ■

(c) Disprove that if \(a\mid bc\), then \(a\mid b\) or \(a\mid c\).

**Solution:** For example, let \(a = 4\) and \(b = c = 2\).

2. After finding the prime factorisations of 1830 and 1458, find their (a) greatest common factor and (b) least common multiple.

**Solution:** 1830 = \(2 \cdot 3 \cdot 5 \cdot 61\) and 1458 = \(2 \cdot 3^6\).

So, \(\gcd(1830, 1458) = 2 \cdot 3 = 6\) and \(\text{lcm}(1830, 1458) = 2 \cdot 3^6 \cdot 5 \cdot 61\).

3. We call a positive integer **perfect** if it equals the sum of its divisors other than itself.

(a) Show that 6, 28, and 496 are perfect numbers.

**Solution:** \(1 + 2 + 3 = 6, 1 + 2 + 4 + 7 + 14 = 28,\) and \(1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496\)

(b) Show that \(2^{p-1}(2^p - 1)\) is perfect whenever \(2^p - 1\) is prime.

**Proof:** The proper divisors of \(n = 2^{p-1}(2^p - 1)\) are \(1, 2, 2^2, ..., 2^{p-1}, 2^p - 1, 2^1(2^p - 1), 2^2(2^p - 1), ...,\) and \(2^{p-2}(2^p - 1)\). Using the finite geometric series formula, these divisors add up as follows:
\[
(1 + 2 + 2^2 + ... + 2^{p-1}) + ((2^p - 1) + 2^1(2^p - 1) + 2^2(2^p - 1) + ... + 2^{p-2}(2^p - 1)) = (2^p - 1) + (2^p - 1)(2^{p-1} - 1) = (2^p - 1)(1 + (2^{p-1} - 1)) = n. \]

4. With the use of the Fundamental Theorem of Arithmetic, prove that \(\log_2 3\) is irrational.

**Proof:** Suppose to the contrary that \(\log_2 3\) were rational. Then, \(\log_2 3 = \frac{m}{n}\) for some \(m, n \in \mathbb{N}\) (as this quantity is positive). We may rewrite this as \(3^n = 2^m\). This is a contradiction, since this violates the Fundamental Theorem of Arithmetic (unique factorisation into primes). ■

5. Which of the following numbers are congruent to 5 mod 17? (a) 80, (b) 103, (c) \(-29\), (d) \(-122\)

**Solution:** Only \(-29\) is congruent to 5 modulo 17.
6. Use the division algorithm to find the unique integer between 0 and 6 inclusive that is congruent to modulo 7: (a) \(-101 \equiv 4 \mod 7\), (b) \(144 \equiv 4 \mod 7\).

7. Prove that if \(a \equiv b \mod m\) and \(n|m\), then \(a \equiv b \mod n\). Is the converse true?

**Proof:** By hypothesis, \(a - b = km\) and \(m = ln\) for some integers \(k\) and \(l\). Substitution yields \(a - b = (kl)n\). Since \(kl\) is an integer, \(a \equiv b \mod n\). ■

The converse is false; for example, although \(1 \equiv 4 \mod 3\), \(1 \equiv 4 \mod 9\) is false.

8. What is the last digit of \(7^{1021}\)?

**Solution:** Working mod 10, note that \(7^4 \equiv 1 \mod 10\). Thus, \(7^{1021} \equiv (7^4)^{254} \equiv 1 \cdot 7 \equiv 7 \mod 10\). So, the last digit is 7.

9. Establish the following: An integer is divisible by 11 iff the alternating sum of its digits is also divisible by 11.

**Proof:** Let \(n \in \mathbb{Z}\). Writing this in base 10, we see that \(n = a_k10^k + a_{k-1}10^{k-1} + \ldots + a_110 + a_0\) where \(a_0, \ldots, a_k \in \{0, 1, 2, \ldots, 9\}\). Since \(10 \equiv -1 \mod 11\), we see that \(n \equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \ldots + a_1(-1) + a_0 \mod 11\). Since \(n\) is divisible iff \(n \equiv 0 \mod 11\), the assertion now follows. ■

10. Show that for any odd integer \(n\), \(n^2 \equiv 1 \mod 8\).

**Solution:** Since \(n\) is an odd integer \(n \equiv 1, 3, 5,\) or \(7 \mod 8\). Squaring each of these possibilities mod 8 immediately yields the desired result. ■

11. Find two nonzero integers modulo 81 \(a\) and \(b\) such that \(ab \equiv 0 \mod 81\).

**Solution:** For example, let \(a = 9 = b\).

12. By the alternate characterisation of a prime number, we have that if \(p\) is prime and \(a\) and \(k \geq 2\) are positive integers such that \(p|a^k\), then \(p|a\).

Use this fact to prove that \(\sqrt[p]{p}\) is irrational. Can you outline (i.e., not rigorously prove) a generalisation of this?

**Proof:** Suppose to the contrary that \(\sqrt[p]{p}\) were rational. Then, we may write \(\sqrt[p]{p} = m/n\) for some integers \(m\) and \(n\) where \(n \neq 0\) and \(m/n\) is reduced to lowest terms. We may rewrite this equality as \(m^k = pn^k\). So, \(p|m^k\). This implies that \(p|m\) by the above fact (that \(p\) is prime). Now, using the fact that \(m = pl\) for some integer \(l\) yields \((pl)^k = pn^k\) or \(p^{k-1}l^k = n^k\). As before, \(p|n^k\) and thus \(p|n\). This is a contradiction, since then \(m/n\) is not reduced to lowest terms after all. Hence, \(\sqrt[p]{p}\) must be irrational. ■

We may replace \(p\) with any integer that is not a perfect \(k\)th power. The above argument continues to work by examining a prime \(p\) in the integer’s prime factorisation that is not raised to a \(k\)th power (or any power of the \(k\)th power).