Exercise 5

1. Let m, n, and k be positive integers. Prove that

$$v_p(mn) = v_p(m) + v_p(n) \qquad \text{and} \qquad v_p(m^k) = kv_p(m).$$

2. Let d and m be nonzero integers. Prove that d divides m if and only if $v_p(d) \leq v_p(m)$ for all primes p.

3. Let $m = \prod_{i=1}^{k} p_i^{r_i}$, where $p_1, \ldots, p_k$ are distinct primes, $k \geq 2$, and $r_i \geq 1$ for $i = 1, \ldots, k$. Let $m_i = mp_i^{-k_i}$ for $i = 1, \ldots, k$. Prove that $(m_1, \ldots, m_k) = 1$.

4. Let a, b, and c be positive integers. Prove that $(ab, c) = 1$ if and only if $(a, c) = (b, c) = 1$.

5. Prove that if 6 divides m, then there exist integers b and c such that $m = bc$ and 6 divides neither b nor c.

6. Prove that for any positive integers a and b,

$$[a, b] = \frac{ab}{(a, b)}.$$

7. Let a and b be positive integers. Prove that $(a, bc) = (a, b)(a, c)$ for every positive integer c if and only if $(a, b) = 1$.

8. Let $m_1, \ldots, m_k$ be pairwise relatively prime positive integers, and let d divide $m_1 \cdots m_k$. Prove that for each $i = 1, \ldots, k$ there exists a unique divisor d_i of m_i such that $d = d_1 \cdots d_k$.

9. Let $n \geq 2$. Prove that the equation $y^n = 2x^n$ has no solution in positive integers.

10. Let a and b be positive integers with $(a, b) = d$. Prove that

$$\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{[a, b]}{d}.$$

11. Let $a_1, \ldots, a_k$ be positive integers. Prove that $[a_1, \ldots, a_k] = a_1 \cdots a_k$ if and only if the integers $a_1, \ldots, a_k$ are pairwise relatively prime.

12. Let a and b be positive integers and p a prime. Prove that if p divides $[a, b]$ and p divides $a + b$, then p divides (a, b).

13. Let a and b be positive integers such that

$$a + b = 57 \quad \text{and} \quad [a, b] = 680.$$

Find a and b.

Hint: Show that a and b are relatively prime. Then $a(57 - a) = ab = [a, b]$.

14. A positive integer is called *square-free* if it is the product of distinct prime numbers. Prove that every positive integer can be written uniquely as the product of a square and a square-free integer.

15. Prove that the set of all rational numbers of the form a/b, where $a, b \in \mathbf{Z}$ and b is square-free, is an additive subgroup of $\mathbf{Q}$.

16. Let a and n be positive integers. Prove that $a^n - 1$ is prime only if $a = 2$ and $n = p$ is prime. Primes of the form $M_p = 2^p - 1$ are called *Mersenne primes*. Compute the first five Mersenne primes. The largest known primes are Mersenne primes. It is an unsolved problem to determine whether there are infinitely many Mersenne primes. There is a list of all known Mersenne primes in the Notes at the end of this chapter.

17. Let k be a positive integer. Prove that if $2^k + 1$ is prime, then $k = 2^n$. The integer

$$F_n = 2^{2^n} + 1$$

is called the nth *Fermat number*. Primes of the form $2^{2^n} + 1$ are called *Fermat primes*. Show that F_n is prime for $n = 1, 2, 3, 4$.

18. Prove that F_5 is divisible by 641, and so F_5 is composite.

It is an unsolved problem to determine whether there are infinitely many Fermat primes. Indeed, we do not know whether F_n is prime for any $n > 4$.

19. Modify the proof of Theorem 1.14 to prove that there are infinitely many prime numbers whose remainder is 3 when divided by 4.

Hint: Let $p_1, p_2, \ldots, p_n$ be primes of the form $4k + 3$, $p_i \neq 3$. Let $N = 4p_1p_2 \cdots p_n + 3$. Show that N must be divisible by some prime q of the form $4k + 3$.

20. Prove that the equation $3x_1 + 5x_2 = b$ has a solution in integers for every integer b, and a solution in nonnegative integers for $b = 0, 3, 5, 6$ and all $b \geq 8$.

21. Find all solutions in nonnegative integers x_1 and x_2 of the linear diophantine equation

$$2x_1 + 7x_2 = 53.$$