3.9 Modular arithmetic (part 2)

1. Find the least positive integer n satisfying the following.
   (a) $5^n \equiv 1 \pmod{16}$ (b) $7^n \equiv 1 \pmod{36}$

2. Let $a_1 \leq a_2 \leq \cdots \leq a_5$ be integers. Prove that it is always possible to find three of them with their sum divisible by 3.

3. Compute the remainder when 3^{40} is divided by 100 by at two ways – first using the fact of $9 = 10 - 1$, then using the proceeding problem.

4. What is the sum of all primes p such that $7^p - 6^p + 2$ is divisible by 43?

5. Let n be an integer greater than 3. Prove that $1! + 2! + \cdots + n!$ cannot be a perfect power.

3.10 Establishing the Frobenius Coin theorem (part 2)

1. For given integers (a, b, n), consider all pairs (x, y) of integers such that $ax + by = n$.
   (a) If $(a, b, n) = (5, 9, 59)$, find a pair (x, y) with $0 \le x \le 8$. Is such pair unique?
   (b) If $(a, b, n) = (5, 9, -59)$, find a pair (x, y) with $0 \le y \le 4$. Is such pair unique?
   (c) If $(a, b, n) = (5, 9, 2014)$, find a pair (x, y) with $0 \le y \le 4$. Is such pair unique?
   (d) If $(a, b, n) = (5, 9, -2014)$, find a pair (x, y) with $0 \le x \le 8$. Is such pair unique?
2. If (x_0, y_0) is a pair of integers with $5x_0 + 9y_0 = n$ for some given integer n, express all pairs (x, y) (with $5x + 9y = n$) in terms of (x_0, y_0). In particular, how many pairs of (x, y) further satisfies the condition $0 \le x \le 8$? What if $0 \le y \le 4$?
3. Let a and b be two relative prime positive integers. We say a number n is *representable* by a and b if $n = ax + by$ for some nonnegative integers x and y. Determine if each of the following statements is true.
   - If integers m is not representable by a and b and $m = ax + by$ for some integers a and b, then $ab \le 0$.
   - If integers m is representable by a and b and $m = ax + by$ for some integers a and b, then $ab \ge 0$.
4. Let m and n be integers. Show that
   (a) if $m + n = 31$, then one of m and n is not representable by 5 and 9;
   (b) if $m + n = 31$, then exactly one of m and n is not representable by 5 and 9.
5. Let a and b be relatively prime positive integers. The equation
   $$ax + by = n$$
   has nonnegative integer solutions (x, y) for integers $n > ab - a - b$ and has no nonnegative integer solutions (x, y) for $n = ab - a - b$.

   Is the above result equivalent to the following statement?

   > Let a and b be relatively prime positive integers. The equation
   > $$ax + by = n$$
   > has nonnegative integer solutions (x, y) if and only if n is a integer greater than $ab - a - b$.

3.24 A direct proof of the Fundamental Theorem of Arithmetic

1. A positive integer p is prime if it has exactly two positive integer divisors, namely, 1 and p. This is called the irreducible property of a number.

   Another fundamental property of primes is the following:

   > If p divides ab for some integers a and b, then p divides a or p divides b.

   The difference between this property and the irreducible property leads to the study of algebraic number fields. Throughout this section assume that primes possess only the irreducible property, that is, you cannot use the other property in any of your arguments.

   Show that any given integer $n \geq 2$ can be written as a product of primes.

2. Consider the set S consisting of positive integer n that has two distinct prime factorizations; that is,

   $$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_h$$

   where $p_1, p_2, \ldots, p_k$, $q_1, q_2, \ldots, q_h$ are primes with $p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \cdots \leq q_h$ such that the k-tuple $(p_1, p_2, \ldots, p_k)$ is not the same as the h-tuple $(q_1, q_2, \ldots, q_h)$. Explain why it is necessary that $k \geq 2$ and $h \geq 2$.

   Assume that S is nonempty, and further assume that n be the minimal such integer; that is, n is the smallest element in S. Prove that $p_i \neq q_j$ for any i and j.

3. (Continuation) Assume without loss of generality that $p_1 < q_1$; that is, p_1 is the least prime factor of n in the above representations. By applying the division algorithm it follows that

   $$\begin{aligned} q_1 &= p_1 c_1 + r_1, \\ q_2 &= p_1 c_2 + r_2, \\ &\vdots \\ q_h &= p_1 c_h + r_h, \end{aligned}$$

   where $1 \leq r_i < p_1$, $i = 1, \ldots, h$. Prove that $n' = r_1 r_2 \cdots r_h$ is also in S.

4. (The Fundamental Theorem of Arithmetic) Prove that any integer n greater than 1 has a unique representation (up to a permutation) as a product of primes.

5. Many people think the fundamental property of primes:

   > If p divides ab for some integers a and b, then p divides a or p divides b.

   is part of the definition of primes, and use it without proof to establish (trivially but wrongly) the Fundamental Theorem of Arithmetic. Use Fundamental Theorem of Arithmetic to prove this property.

3.27 Number theory practice set 10

1. Prove that, for integers x and y, $2x + 3y$ is divisible by 17 if and only if $9x + 5y$ is.

2. Let p be a prime, and let k be an integer with $1 \leqslant k < p$. Then $p \mid \binom{p}{k}$.

3. Assume that $(w, x, y, z) = (w_0, x_0, y_0, z_0)$ is a quadruple of integers that satisfies the following equation.
$$x^2 + y^2 = 3(z^2 + w^2)$$
Show that one can find a *smaller* quadruple of integers satisfies the same equation. What conclusion can you draw from this fact? (Note that there are different ways to interpret the term *smaller*.)

   This process is called *finite/infinite descent*. We will discuss this method in detail in our future series.

4. Mr. Fat wants to find the smallest positive integer k which is representable in the form $k = 19^n - 5^m$ for some positive integers m and n. An obvious choice for k is 14. But to prove that positive integers less than 14 is not representable in the form of $19^n - 5^m$ is a bit more difficult.

   (a) Prove that we only need to consider two possible candidates 4 and 6.

   (b) Assume that $19^n - 5^m = 6$ for some positive integers n and m. First prove that both n and m are even. And then prove that there are no such n and m.

   (c) Prove that 4 is not representable in the form of $19^n - 5^m$.

5. Find the largest integer divisible by all integers less than or equal to its square root.