2.3 Modular inverse

1. Let m be a positive integer. Let a be an integer relatively prime to m, and let b be an integer. Prove that there exist integers x such that $ax \equiv b \pmod{m}$, and all these integers form exactly one residue class modulo m.

2. (Continuation) In particular, setting $b = 1$ in the last problem shows that if $\gcd(a, m) = 1$, then there is x such that $ax \equiv 1 \pmod{m}$. We call such x the *inverse of a modulo m*, denoted by a^{-1} or $\frac{1}{a} \pmod{m}$. Because all such numbers form exactly one residue class modulo m, the inverse of a is uniquely determined (or well defined) modulo m for all integers relatively prime to m.

   Compute the inverse of 5 modulo n for each of the following.

   (a) $n = 3$ (b) $n = 4$ (c) $n = 7$
   (d) $n = 12$ (e) $n = 21$ (f) $n = 28$

3. Compute the inverse of each of $1, 2, \ldots, n-1$ modulo n for each of the following.

   (a) $n = 11$ (b) $n = 12$ (c) $n = 13$

4. We want to find the inverse of 11 modulo 37. We could do the following: $11 \cdot 3 \equiv -4 \pmod{37}$, $11 \cdot 27 \equiv 1 \pmod{37}$. Explain the reasons behind this approach.

   The above method has a lot of hit-and-miss flavor. We introduce a more systematic approach. Note that

   $$37 = 11 \cdot 3 + \underline{4}, \quad 11 = 4 \cdot 2 + \underline{3}, \quad 4 = 3 \cdot 1 + \underline{1}.$$

   Therefore,

   $$\underline{1} = 4 - \underline{3} \cdot 1 = 4 - (11 - 4 \cdot 2) \cdot 1 = \underline{4} \cdot 3 - 11 = (37 - 11 \cdot 3) \cdot 3 - 11 = 37 \cdot 3 - 11 \cdot 10,$$

   and hence -10 or 27 is the inverse of 11 modulo 37. (This is the *Euclidean algorithm*, the most effective way to find the great common divisor of two numbers. We will discuss this method in detail in the future.)

   Use Euclidean algorithm to compute the following inverses.

   (a) $7x \equiv 1 \pmod{25}$ (b) $32y \equiv 1 \pmod{75}$ (c) $37z \equiv 1 \pmod{374}$

5. Compute each of the following.

   (a) $10! \pmod{11}$ (b) $11! \pmod{12}$ (c) $12! \pmod{13}$

   Can you make a conjecture on $(n-1)! \pmod{n}$ for positive integer n? Can you explain the reason behind your observation?

2.4 Wilson's theorem

1. (Wilson's theorem) Wilson's theorem states that for any prime p, $(p-1)! \equiv -1 \pmod{p}$. Prove this Wilson's theorem.

2. (Continuation) What is the converse of the Wilson's theorem? Is the converse true?

3. Show that if p is a prime, then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$. Does the statement hold if p is not a prime?

4. Show that $61! + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$.

5. Given a positive integer n, evaluate $\gcd(n! + 1, (n+1)!)$.

2.19 Proofs in modular arithmetic (part 4)

1. Determine whether there exist an infinite set of even positive integers k such that for every prime p the number $p^2 + k$ is composite. If the answer is *no*, explain why; if the answer is *yes*, find such a set.

2. Let p be a prime of the form $3k+2$ that divides a^2+ab+b^2 for some integers a and b. Prove that a and b are both divisible by p.

3. For a positive integer n, we consider all its divisors (including 1 and itself). Suppose that $p\%$ of these divisors have their unit digit equal to 3 (For example $n = 1001$, has eight divisors, namely 1, 7, 11, 13, 77, 91, 143, 1001. Two of these divisors, namely 13 and 143, have unit digits equal to 3. Hence for $n = 1001$, $p = 25$). Find, when n is any positive integer, the maximum possible value of p.

4. Let a and b be two relatively prime positive integers. Determine with proof the least integer m, in terms of a and b, such that every positive integer n, with $n > m$, can be written in the form $ax + by$ for some nonnegative integers x and y? What if x and y are both positive? What if one of x and y is positive and the other is nonnegative?

5. Prove that for each positive integer n, there are pairwise relatively prime integers k_0, k_1, $\ldots k_n$, all strictly greater than 1, such that $k_0k_1 \ldots k_n - 1$ is the product of two consecutive integers.

2.20 Diophantine equations

1. Determine all integers n such that $n^4 + 6n^3 + 11n^2 + 3n + 31$ is a perfect square.

2. Determine the number of ordered pairs of integers (m, n) for which $mn \geq 0$ and

$$m^3 + n^3 + 99mn = 33^3.$$

3. Find all integers (a, b, c, x, y, z) such that

$$a + b + c = xyz,$$
$$x + y + z = abc,$$

and $a \geq b \geq c \geq 1$, $x \geq y \geq z \geq 1$.

4. Let $P_1P_2 \dots P_{101}$ be a regular 101-gon. We associate 1 to vertex P_1. From P_1, count 2 points in the clockwise direction, we reach P_3 and associate it with 2. From the point labeled 2, count 3 points in the clockwise direction and associate this vertex with 3. Continue this process until each of $1, 2, 3, \dots, 101$ is associated with a vertex. A vertex is called *lonely* if it is not associated with any numbers. A vertex is called *social* if it is associate with more than one numbers. How many lonely vertices are there? How many social vertices are there?

5. Let p be a prime and n a positive integer. Determine all pairs of positive integers (x, y) such that

$$x(x + 1) = p^{2n}y(y + 1).$$