NUMBER THEORY

UNIT 2 CONGRUENCES

1. Basic Properties

Recall that in Unit 0, we came across the problem of finding the odd one out among the following group of numbers:

13, 17, 25, 39, 45

We remarked that 39 is the odd one out, for it leaves a remainder of 3 when divided by 4, while the others leave a remainder of 1 when divided by 4. In view of this, integers can be classified into four types, according to whether they leave a remainder of 0, 1, 2 or 3 when divided by 4.

Of course, there is no need to restrict ourselves to dividing by 4. The division algorithm (Lemma 2.2 in Unit 1) asserts that given any integers a, b with $a \neq 0$, there exist unique integers q, r, $0 \leq r < |a|$, such that

$$b = aq + r .$$

The number r is called the **remainder** when b is divided by a. It may take one of the values 0, 1, …, $a-1$. Hence we may classify the integers into a types according to their remainders upon division by a. This leads us to the following definition.

Definition 1.1.

Let $m \neq 0$ be an integer. We say that x is **congruent** to y modulo m, denoted as $x \equiv y \pmod{m}$, if $m \mid x - y$.

Illustrations. $38 \equiv 74 \pmod 4$, $6 \equiv -1 \pmod 7$, $83 \equiv 123 \pmod{10}$.

Note that $x \equiv y \pmod m$ means that x and y leave the same remainder when divided by m.

As for divisibility, we have the following basic properties about congruences which are easy to verify.

Theorem 1.1.

Let a, b, c, d, m, n be integers, $m \neq 0$, $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$. Then

(1) $a \pm c \equiv b \pm d \pmod{m}$

(2) $ac \equiv bd \pmod{m}$

(3) $a^n \equiv b^n \pmod{m}$

(4) if $n \mid a$, $n \mid b$ and $(m, n) = 1$, we have $\frac{a}{n} \equiv \frac{b}{n} \pmod{m}$.

Example 1.1.

Find the remainder when

(a) 8^{2002} is divided by 7

(b) 3^{2003} is divided by 26

(c) 1978^{20} is divided by 125

Solution.

(a) $8^{2002} \equiv 1^{2002} = 1 \pmod{7}$.

$\therefore$ The remainder is 1.

(b) $3^{2003} = (3^3)^{667}(3^2) = 27^{667}3^2 \equiv 1^{667}3^2 = 9 \pmod{26}$

$\therefore$ The remainder is 26.

(c) $1978^{20} \equiv (-22)^{20} = 484^{10} \equiv (-16)^{10} \equiv 256^5 \equiv 6^5 = 2^5 3^5 = 32(243) \equiv 32(-7) \equiv 26 \pmod{125}$

$\therefore$ The remainder is 26.

Example 1.2.

Show that a natural number N is divisible by 3 if and only if its sum of digits is divisible by 3.

Solution.

Write $N = \overline{a_k a_{k-1} \cdots a_2 a_1 a_0}$ in its decimal notation.

Then $N = a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0 \times 1$

$\equiv a_k \times 1^k + a_{k-1} \times 1^{k-1} + \cdots + a_2 \times 1^2 + a_1 \times 1 + a_0 \times 1$

$= a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \pmod{3}$

Hence $3 | N$ if and only if 3 | sum of digits of *N*.

Remark. Compare this proof with the one given in Unit 1. In this proof, we showed that *N* is congruent to its sum of digits modulo 3. Hence we can easily find the remainder of a number upon division by 3 by considering its sum of digits.

Example 1.3.

Show that the sequence 11, 111, 1111, … contains no perfect squares.

Solution.

For all integers *n*, $n \equiv 0, 1, 2$ or 3 (mod 4). If $n \equiv 0$ or 2 (mod 4), then $n^2 \equiv 0 \pmod 4$. If $n \equiv 1$ or 3 (mod 4), then $n^2 \equiv 1 \pmod 4$.

Note that in the sequence 11, 111, 1111, …, all terms leave a remainder of 3 when divided by 4. Thus there is no perfect square in the sequence.

Example 1.4.

Find the largest even number which cannot be expressed as the sum of two odd composite numbers.

Solution.

Let *n* be an even number.

If $n \equiv 0 \pmod 3$, then we have $n = 9 + (n - 9)$. Since $n - 9$ is divisible by 3, it is an odd composite number whenever $n > 12$.

If $n \equiv 1 \pmod 3$, then we have $n = 25 + (n - 25)$. Since $n - 25$ is divisible by 3, it is an odd composite number whenever $n > 28$.

If $n \equiv 2 \pmod 3$, then we have $n = 35 + (n - 35)$. Since $n - 35$ is divisible by 3, it is an odd composite number whenever $n > 38$.

It follows that all even numbers greater than 38 can be expressed as the sum of two odd composite numbers. However, there is no way of writing 38 as the sum of two odd composite numbers (this can be seen by listing all odd composite numbers less than 38: 9, 15, 21, 25, 27, 35). Therefore, the answer is 38.

2. The Euler ϕ-function

In Example 1.1, part (b), we found that our calculation is very much simplified by expressing the number as a power of 3^3, because $3^3 \equiv 1 \pmod{26}$. Therefore, in attempting to find the remainder when a certain power of *a* is divided by *n*, where *a* and *n* are given, we probably want to find an exponent *k* for which $a^k \equiv 1 \pmod{n}$. In the next section we will come across a theorem which enables us to find such an exponent efficiently. In order to understand the theorem, we first go over the **Euler ϕ-function** in this section.

Definition 2.1.

For positive integer *n*, we define

$\phi(n)$ = number of positive integers not exceeding *n* that are relatively prime to *n*.

Illustrations. $\phi(12) = 4$ since 1, 5, 7, 11 are relatively prime to 12. $\phi(16) = 8$ since 1, 3, 5, 7, 9, 11, 13, 15 are relatively prime to 16.

The Euler ϕ-function turns out to be an important function in number theory on which many theorems are built. Before we proceed, let's study some nice properties of the function which facilitate easy computation of $\phi(n)$ for a given *n*.

Theorem 2.1.

Let *a*, *b* be relatively prime natural numbers, *p* be a prime number and *m* be a positive integer. Then

(a) $\phi(ab) = \phi(a)\phi(b)$

(b) $\phi(p^m) = p^m - p^{m-1}$

Illustrations. (a) $\phi(3) = 2$, $\phi(4) = 2$, $\phi(12) = 4$; (b) $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$.

Remark. Because of the property in (a), the function ϕ is said to be **multiplicative**. This is a very nice property because, if a function $f : \mathbb{N} \to \mathbb{R}$ is multiplicative, we need only know the value of *f* at prime powers. The other values can be computed via the prime factorization of a natural number. With the formula in (b), therefore, we can compute $\phi(n)$ easily for all *n*.

Example 2.1.

Find $\phi(360)$.

Solution.

$\phi(360) = \phi(2^3 \times 3^2 \times 5) = \phi(2^3) \times \phi(3^2) \times \phi(5) = (2^3 - 2^2)(3^2 - 3^1)(5^1 - 5^0) = 96$.

Example 2.2.

Find all natural numbers *n* for which $\phi(n)$ is odd.

Solution.

Clearly, $\phi(1) = 1$ is odd. Now suppose $n > 1$.

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where p_i is prime and e_i is a positive integer for *i* = 1, 2, …, *k*. Then

$$\phi(n) = \prod_{i=1}^{k} \left(p_i^{e_i} - p_i^{e_i - 1} \right).$$

For $\phi(n)$ to be odd, $p_i^{e_i} - p_i^{e_i - 1}$ is odd for all *i*. If p_i is odd, then $p_i^{e_i} - p_i^{e_i - 1}$ is even since both $p_i^{e_i}$ and $p_i^{e_i - 1}$ are odd. So p_i must be even, i.e. $n = 2^e$ for some $e > 0$.

Consequently, $\phi(n) = 2^e - 2^{e-1}$. This cannot be odd unless $e = 1$, i.e. $n = 2$. Indeed, we check that $\phi(2) = 1$ is odd.

Consequently, we see that $\phi(n)$ is odd only if *n* = 1 or 2.

3. Euler's and Fermat's Theorems

With the concept of the Euler ϕ-function in mind, we can now go into Euler's Theorem, which helps us find an exponent *k* for which $a^k \equiv 1 \pmod{n}$ given integers *a* and *n* under certain conditions.

Theorem 3.1. (Euler's Theorem)

Let *a* and *n* be relatively prime natural numbers. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Illustration. (3, 100) = 1, $\phi(100) = \phi(2^2)\phi(5^2) = (2^2 - 2^1)(5^2 - 5^1) = 40$. Thus $3^{40} \equiv 1 \pmod{100}$.

Remark. Given natural numbers *a* and *n*, we say that *b* is an **inverse** of *a* modulo *n* if $ab \equiv 1 \pmod{n}$. For example, 7 is an inverse of 4 (mod 9) since $4 \times 7 \equiv 1 \pmod{9}$. Inverses are useful in simplifying computations and solving congruence equations such as $4x \equiv 3 \pmod{7}$, but in general finding an inverse is not easy. Nevertheless, Euler's Theorem tells us that when (*a*, *n*) = 1, $a^{\phi(n)-1}$ is an inverse of *a* (mod *n*).

Example 3.1.

Find the last two digits of 17^{2002}.

Solution.

As we have seen, $\phi(100) = 40$.

Since (17, 100) = 1, Euler's theorem asserts that $17^{40} \equiv 1 \pmod{100}$.

$\therefore\ 17^{2002} \equiv \left(17^{40}\right)^{50} 17^2 \equiv 1^{50} \cdot 289 \equiv 89 \pmod{100}$.

Hence the last two digits are 89.

When *p* is prime, then $\phi(p) = p - 1$. As a particular case of the Euler's theorem, we have

Theorem 3.2. (Fermat Little Theorem)

Let *p* be a prime and (*a*, *p*) = 1. Then $a^{p-1} \equiv 1 \pmod{p}$.

Illustration. 2003 is prime. (1234, 2003) = 1. Thus $1234^{2002} \equiv 1 \pmod{2003}$.

Example 3.2.

Let *p* be a prime number, $p \equiv 3 \pmod{4}$ and $p \mid a^2 + b^2$ for some integers *a* and *b*. Prove that $p \mid a$ and $p \mid b$.

Solution.

Suppose $p \nmid a$. Then we must have $p \nmid b$ as well.

Consequently, we have $(p, a) = (p, b) = 1$ and so Fermat Little Theorem applies.

Since $b^2 \equiv -a^2 \pmod{p}$, by Fermat Little Theorem, we have, on one hand,

$$\left(a^{p-2}b\right)^2 \equiv \left(a^{p-2}\right)^2\left(-a^2\right) \equiv -\left(a^{p-1}\right)^2 \equiv -1^2 = -1 \pmod{p},$$

so that

$$\left(a^{p-2}b\right)^{p-1} = \left[\left(a^{p-2}b\right)^2\right]^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

where we made use of the fact that $p \equiv 3 \pmod 4$ which implies $\dfrac{p-1}{2}$ is odd.

On the other hand, $a^{p-2}b$ is also relatively prime to p, so Fermat Little Theorem asserts that

$$\left(a^{p-2}b\right)^{p-1} \equiv 1 \pmod{p}.$$

Since $p \neq 2$, this is a contradiction. So we must have $p \mid a$ and hence $p \mid b$.

4. The Chinese Remainder Theorem

To motivate our discussion, let's consider the following example:

> A positive integer n leaves a remainder of 3 when divided by 5 and a remainder of 4 when divided by 7. What is the smallest possible value of n?

Solving the question is not hard: we first note that the unit digit of n must be 3 or 8, and so n is among 3, 8, 13, 18, 23, 28, … We then find the smallest one among these integers which leaves a remainder of 4 upon division by 7. It is easy to see that the smallest n is 18.

Note that the conditions imposed on n can be rephrased into t e system of congruences:

$$\begin{cases} n \equiv 3 \pmod 5 \\ n \equiv 4 \pmod 7 \end{cases}$$

and we have shown that the smallest positive n satisfying the system is 18. If we repeat the above process, it is not hard to see that n = 53, 88, 123, 158, … all satisfy the system and they occur at intervals of 35. Indeed, any integer n with $n \equiv 18 \pmod{35}$ satisfies the system.

A natural question to ask is whether all such systems are solvable. A little thought would tell us that the answer is negative, for the system

$$\begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 2 \pmod 4 \end{cases}$$

is clearly not solvable (as the first constraint requires *n* to be odd and the second constraint requires *n* to be even).

Despite this negative result, an extra constraint would give us something encouraging, as given in the next theorem.

Theorem 4.1. (Chinese remainder theorem)

If b_1, b_2, …, b_k are integers and m_1, m_2, …, m_k are pairwise relatively prime integers, then the system

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

is solvable and the solution is unique modulo $m_1 m_2 \cdots m_k$.

Proof. We first prove the uniqueness, and then prove the existence.

(Uniqueness)

Suppose *x* and *x*' both satisfy the system.

Then $x \equiv x' \pmod{m_i}$ for *i* = 1, 2, …, *k*, i.e. $m_i \mid x - x'$ for *i* = 1, 2, …, *k*.

Since m_1, m_2, …, m_k are pairwisely relatively prime, we have $m_1 m_2 \cdots m_k \mid x - x'$, i.e.

$$x \equiv x' \pmod{m_1 m_2 \cdots m_k}.$$

(Existence)

Define $M_j = \dfrac{m_1 m_2 \cdots m_k}{m_j}$ for *j* = 1, 2, …, *k*. Set

$$x = M_1^{\phi(m_1)} b_1 + M_2^{\phi(m_2)} b_2 + \cdots + M_k^{\phi(m_k)} b_k .$$

Then for *j* = 1, 2, …, *k*, $x \equiv M_j^{\phi(m_j)} b_j \equiv (1) b_j = b_j \pmod{m_j}$ where we made use of the fact that $m_j \mid M_r$ for $r \neq j$ and the Euler's theorem (noting that m_j is relatively prime to M_j for all *j*).

Q.E.D.

In the above proof we gave an explicit formula to find *x*, but in practice this is rarely used as the number gets too large when we take powers. There is another formula which overcomes this difficulty but which is not as simple as the preceding one.

Recall that *b* is said to be an **inverse** of *a* modulo *n* if $ab \equiv 1 \pmod{n}$. It can be shown that such *b* exists if and only if (*a*, *n*) = 1 (see exercise 8). Now, $(m_j, M_j) = 1$ for all *j*, where M_j is defined as above, since the m_i's are pairwise relatively prime. Hence M_j has an inverse modulo m_j, which we denote by $\overline{M_j}$. Then a solution for the system in Theorem 4.1 can be written as

$$x = b_1 M_1 \overline{M_1} + b_2 M_2 \overline{M_2} + \cdots + b_k M_k \overline{M_k}.$$

We leave it to the reader to verify that such *x* indeed satisfies the system.

Example 4.1.

Find all integers *x* for which $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ and $x \equiv 4 \pmod{7}$.

Solution.

Since 3, 5, 7 are pairwise relatively prime, the Chinese remainder theorem asserts that there is a unique solution modulo $3 \times 5 \times 7 = 105$.

Now $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$, $\overline{M_1} = 2$, $\overline{M_2} = 1$, $\overline{M_3} = 1$, so one solution for *x* is given by

$$x = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 4 \times 15 \times 1 = 263.$$

Note that $263 \equiv 53 \pmod{105}$, so the general solution is $x = 53 + 105t$ for any integer *t*.

5. Exercises

1. Prove or disprove each of the following statements. All variables denote natural numbers.

   (a) If $a \equiv b \pmod{m}$, then $a^2 \equiv b^2 \pmod{m}$.

   (b) If $a \equiv b \pmod{m}$, then $a^2 \equiv b^2 \pmod{m^2}$.

   (c) If $a^2 \equiv b^2 \pmod{m^2}$, then $a \equiv b \pmod{m}$.

(d) If $ax \equiv bx \pmod{mx}$, then $a \equiv b \pmod{m}$.

(e) If $m > n$, then $\phi(m) > \phi(n)$.

(f) If $p > q$ and $m > 1$, then $\phi(m^p) > \phi(m^q)$.

2. Find the remainder when 1234^{5678} is divided by 13.

3. Show that a natural number N is divisible by 9 if and only if its sum of digits is divisible by 9.

4. In Unit 1 and its exercises, we came across various divisibility tests and proved their validity using divisibility arguments. Try to rephrase the proofs in the language of congruences that we have been using throughout this unit.

5. Find all prime numbers p for which $2^p + p^2$ is prime.

6. Prove that there are infinitely many prime numbers p satisfying $p \equiv 3 \pmod{4}$.

7. Suppose n has k distinct prime factors $p_1, p_2, \ldots, p_k$. Show that

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

8. (a) Let a, n be integers, $n \neq 0$. Show that a has an inverse modulo n if and only if a and n are relatively prime.

(Hint: Recall that there exist integers u, v such that $cu + dv = \gcd(c, d)$.)

(b) In the condition of (a), show that the inverse is unique modulo n.

9. Show that

$$x = b_1 M_1 \overline{M_1} + b_2 M_2 \overline{M_2} + \cdots + b_k M_k \overline{M_k}$$

satisfies the system of congruences in the statement of Theorem 4.1.

9. (a) Let p_1, p_2, …, p_{2n} be distinct prime numbers. Show that there is an integer x such that $p_{2i-1}p_{2i}$ divides $x + i$ for $i = 1, 2, \ldots, n$.

   (b) We say that a positive integer k is 'good' if it is not the power of a prime number. Using (a), show that for every natural number n we can find n consecutive 'good' integers.

   (Remark: Part (b) is essentially the same as a problem in IMO 1989.)

10. (a) **Wilson's Theorem** asserts that

$$(p-1)! \equiv -1 \pmod{p}$$

   for all prime numbers p. Give a proof of this fact.

   (Hint: Group the terms of $(p-1)!$ into pairs.)

   (b) Show that the converse of Wilson's Theorem is also true.

   (c) In view of (a) and (b), we see that

$$(n-1)! \equiv -1 \pmod{n}$$

   if and only if n is prime. This gives a test of whether a given natural number n is prime. But in practice such a test is rarely used. Suggest a reason for this.

11. (IMO 2002 Hong Kong Team Selection Test 1) Considering (mod 4) or otherwise, prove that if a, b, c, d are integers satisfying

$$(3a+5b)(7b+11c)(13c+17d)(19d+23a) = 2001^{2001}$$

   then a must be even.

12. (IMO 2001) Let n be an odd integer greater than 1, and let k_1, k_2, …, k_n be given integers. For each of the $n!$ permutations $a = (a_1, a_2, \ldots, a_n)$ of 1, 2, …, n, let

$$S(a) = \sum_{i=1}^{n} k_i a_i \ .$$

   Prove that there are two permutations b and c, $b \neq c$, such that $n!$ is a divisor of $S(b) - S(c)$.