RAFFLES INSTITUTION
H3 Mathematics (9820)

Chapter 4: Modular Arithmetic

SYLLABUS INCLUDES

Students will learn to prove properties and results, and solve non-routine problems involving:

Modulo arithmetic

CONTENT

1 Introduction to Modulo Arithmetic

Another approach to divisibility questions is through the arithmetic of remainders, or the *theory of congruences* or *modular arithmetic* as it is now commonly known. The concept, and the notation that makes it such a powerful tool, was once again introduced by Gauss, in his *Disquisitiones Arithmeticae;* this monumental work, which appeared in 1801 when Gauss was 24 years old, laid the foundations of modern number theory.

In his first chapter, Gauss introduces the concept of congruence and the notation that makes it such a powerful technique (he explains later that he was induced to use the symbol $\equiv$ because of the close analogy with algebraic equality). According to Gauss, "If a number n measures the difference between two numbers a and b, then a and b are said to be congruent to n; if not, incongruent." Putting this into the form of a definition, we have

Definition 1.1 Let n be a fixed positive integer. Two integers a and b are said to be *congruent modulo n*, denoted by

$$a \equiv b \pmod{n}$$

if n divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer k.

Let us have a concrete idea. Consider the case $n = 2$. It is easy to check that

$$17 \equiv 1 \pmod 2, \quad 31 \equiv 1 \pmod 2, \quad 26 \equiv 0 \pmod 2$$

In fact, you should see that what modulo 2 does is to split the integers into 2 sets, the odd integers, which are all congruent to 1 modulo 2, and the even integers, which are all congruent to 0 modulo 2.

To further fix our idea, let us look at modulo 5.

$$17 \equiv 2 \pmod 5, \quad 31 \equiv 1 \pmod 5, \quad -26 \equiv 4 \pmod 5$$

since 17 – 2 = 3(5), 31 – 1 = 6(5) and –26 – 4 = –6(5). When $n \nmid (a-b)$, we say that *a* is *incongruent to b modulo n*, and in this case we write $a \not\equiv b \pmod n$. For example, $26 \not\equiv 7 \pmod 5$.

Recall the Division Algorithm, which states that:

Given integers *a* and *n*, with $n > 0$, there exist unique integers *q* and *r* satisfying

$$a = qn + r, \qquad 0 \le r < b$$

The integers *q* and *r* are called, respectively, the *quotient* and *remainder* in the division of *a* by *n*.

Then, by the definition of congruence, $a \equiv r \pmod n$. Because there are *n* choices for *r*, we see that every integer is congruent modulo *n* to exactly one of the values 0, 1, 2, …, *n* – 1; in particular, $a \equiv 0 \pmod n$ if and only if $n \mid a$.

The set of *n* integers {0, 1, 2, …, *n* – 1} is called the set of least nonnegative **residues modulo *n*.** In general, a collection of *n* integers $a_1, a_2, ..., a_n$, is said to form a **complete set of residues modulo *n*** if every integer is congruent modulo *n* to one and only one of the a_k. To put it in another way, $a_1, a_2, ..., a_n$ are congruent modulo *n* to 0, 1, 2, …, *n* – 1, taken in some order. For instance

$$26, 31, -1, 14, 11, 1, 9$$

constitute a complete set of residues modulo 7.

One first important theorem provides a useful characterization of congruence modulo *n* in terms of remainders upon division by *n*.

Theorem 1.1 For arbitrary integers *a* and *b*, $a \equiv b \pmod n$ if and only if *a* and *b* leave the same nonnegative remainder when divided by *n*.

Proof

Example 1 Since the integers 26 and 31 can be expressed in the form

$$26 = 5(5) + 1 \text{ and } 31 = 6(5) + 1$$

with the same remainder 1, Theorem 1.1 tells us that $26 \equiv 31 \pmod 5$. Conversely, the congruence $11 \equiv -31 \pmod 7$ implies that 11 and –31 have the same remainder when divided by 7.

Congruences may be viewed as a generalised form of equality, in the sense that its behaviour with respect to addition and multiplication is similar to that of ordinary equality. Some of the elementary properties of equality that carry over to congruences are shown in the following theorem.

Theorem 1.2 Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod{n}$.

(b) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

(e) If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$.

(f) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Before we go any further, let us see how the above properties can help us with carrying out certain types of computations.

Example 2 Show that 41 divides $2^{20} - 1$.

Example 3 Find the remainder when $1! + 2! + \ldots + 99! + 100!$ is divided by 12.

In Theorem 1.2, we saw that if $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$. Is the converse true?

Theorem 1.3 If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{\frac{n}{d}}$, where $d = \gcd(c, n)$.

Proof

Theorem 1.3 is especially useful when c and n are coprime. Basically, with this additional condition, we are able to carry out 'cancellation' without a change in modulus:

Corollary 1.1 If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

A special case of the corollary is when n is a prime p. In this case,

Corollary 1.2 If $ac \equiv bc \pmod{p}$ and c is not a multiple of p, then $a \equiv b \pmod{p}$.

Example 4 If $ab \equiv 0 \pmod{n}$, is it true that $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$? What if n is a prime number?

2 The Method of Infinite Descent

Recall in Chapter 1 we have briefly talked about the Method of Infinite Descent introduced by Pierre de Fermat. Armed with tools from number theory (in particular congruences), let us look at a few Diophantine equations, and attempt to solve them.

A **Diophantine equation** is an equation in which only **integer solutions** are allowed. When we tried to show that $\sqrt{2}$ is irrational, the equation we looked at, $2n^2 = m^2$, is a Diophantine equation since we are only interested in integer solutions.

Example 5 Show that the equation

$$x^2 + y^2 + z^2 = 2xyz$$

has no integral solutions except $x = y = z = 0$.

Example 6 Show that the equation

$$x^3 + 2y^3 + 4z^3 = 0$$

has no integral solutions except $x = y = z = 0$.

Perhaps the most renowned Diophantine Equation is that in the statement of Fermat's Last Theorem. The theorem states that no three positive integers a, b and c satisfy the equation

$$a^n + b^n = c^n$$

for any positive integer strictly greater than 2.

This theorem was first conjectured by Pierre de Fermat in 1637 in the margin of a copy of Arithmetica where he claimed he had a proof that was too large to fit in the margin. The first successful proof was released in 1994 by Andrew Wiles, and formally published in 1995, after 358 years of effort by mathematicians. The unsolved problem stimulated the development of algebraic number theory in the 19th century and the proof of the modularity theorem in the 20th century. It is among the most notable theorems in the history of mathematics and prior to its proof, it was in the Guinness Book of World Records as the "most difficult mathematical problem', one of the reasons being that it has the largest number of unsuccessful proofs.

Tutorial

1. Prove each of the following statements:

(a) If $a \equiv b \pmod{n}$ and $m \mid n$, then $a \equiv b \pmod{m}$.

(b) If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$.

(c) If $a \equiv b \pmod{n}$ and the integers a, b and n are all divisible by $d > 0$, then $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

2. (a) Find the remainders when 2^{31} and 31^{26} are divided by 7.

(b) What is the remainder when $\sum_{k=1}^{2019} k^5$ is divided by 4?

3. For $n \geq 1$, use mathematical induction to show that

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}.$$

4. For $n \geq 1$, use modular arithmetic to show that

(a) $7 \mid 5^{2n} + 3(2^{5n-2})$.

(b) $13 \mid 3^{n+2} + 4^{2n+1}$.

(c) $43 \mid 6^{n+2} + 7^{2n+1}$.

5. Prove the following statements:

(a) If a is an odd integer, then $a^2 \equiv 1 \pmod{8}$.

(b) For any integer a, $a^3 \equiv 0, 1 \text{ or } 6 \pmod{7}$.

(c) If the integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

6. If p is a prime satisfying $n < p < 2n$, show that

$$\binom{2n}{n} \equiv 0 \pmod{p}$$

7. The International Standard Book Number (ISBN) used in many libraries consists of nine digits $a_1a_2...a_9$ followed by a check digit a_{10}, which satisfies

$$a_{10} \equiv \sum_{k=1}^{9} ka_k \pmod{11}.$$

Determine whether each of the ISBNs below is correct:
(a) 0-07-232569-0
(b) 91-7643-497-5
(c) 1-56947-303-10

When printing the ISBN $a_1a_2...a_9$, two unequal digits were transposed. Show that the check digits detected this error.

8. **[9225/1982/Dec/2/19]**

Show that every odd number n satisfies $n^2 \equiv 1 \pmod{8}$. Given that r, s and t are numbers such that $r^2 + s^2 = t^2$,

(i) show that at least one of r and s is even,
(ii) deduce that rs is divisible by 4,
(iii) show that rs is also divisible by 3,
(iv) show that rst is divisible by 60.

9. **[9225/1980/June/1/19]**

Let p be a prime number and let r be an integer satisfying $1 \le r \le p - 1$. Show that p divides the binomial coefficient $\binom{p}{r}$.

(i) Deduce that $\frac{r!}{p}\binom{p}{r} \equiv (-1)^{r-1}(r-1)! \pmod{p}$

and hence that $\frac{r}{p}\binom{p}{r} \equiv (-1)^{r-1} \pmod{p}$.

(ii) Show that if p is an odd prime, and a and b are integers, then

$$a^p + b^p \equiv 0 \pmod{p} \Rightarrow (a+b)^p \equiv 0 \pmod{p} \Rightarrow a^p + b^p \equiv 0 \pmod{p^2}.$$

10. **[852/2/1980/Dec/19 (part)]**

Show that if n is a positive integer of the form $8m + 7$, where m is also a positive integer, then there do not exist integers a, b and c such that $n = a^2 + b^2 + c^2$.

Deduce that no integer of the form $4^k(8m + 7)$, where k is a positive integer, can be written as the sum of squares of three integers.

Assignment 4: Modular Arithmetic

1. [9225/1985/June/1/19]

It is given that n is a prime greater than 7.

(i) By considering $n = 3k \pm 1$, or otherwise, show that $n^3 \equiv \pm 1 \pmod 9$.

(ii) By considering $n = 7k \pm t$ for $t = 1, 2, 3$, or otherwise, show that $n^6 \equiv 1 \pmod 7$.

(iii) Show that $n^2 \equiv 1 \pmod 8$.

Deduce that $n^6 - 1$ is divisible by 504.

2. [9225/1983/June/1/19]

(a) Show, by induction or otherwise, that if n is a positive integer then any odd number a satisfies $a^{2^n} \equiv 1 \pmod{2^{n+2}}$.

(b) Show that if a and k are positive integers then $a + 1$ divides $a^{2k+1} + 1$. By considering the case $a = 2^{2^r}$, or otherwise, show that if $2^n + 1$ is prime, then n is a power of 2.

3. [852/1979/June/1/19]

Let a be an integer. Let p and q be distinct prime numbers and α and β positive integers. Show that y is a solution of the congruence

$$y \equiv a \pmod{p^\alpha q^\beta}$$

if and only if y is a solution to both the congruences

$$y \equiv a \pmod{p^\alpha} \quad \text{and} \quad y \equiv a \pmod{q^\beta}$$

Hence or otherwise, find all solutions of the congruence

$$x^3 + 10x + 9 \equiv 0 \pmod{24}.$$

Additional Practice Questions

Refer to the compilation of 2010 to 2019 STEP I and II problems.

1. **2010/STEP I/8**
2. **2011/STEP I/8**
3. **2011/STEP II/2**
4. **2013/STEP II/7**
5. **2014/STEP I/1**
6. **2014/STEP II/8**
7. **2016/STEP I/7**
8. **2018/STEP II/6**
9. **2019/STEP I/7**