International Mathematical Olympiad
2006-07 Training Phase 1 Level 1
(Session 5, 27 July 2006)
Topic: Number Theory 1

1. Elementary Number Theory

1.1 The Ring of Congruence Classes

Let m be a positive integer. If a and b are integers such that a-b is divisible by m, then we say that a and b are **congruent modulo m,** and write

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

Integers a and b are called **incongruent modulo m** if they are not congruent modulo m.

Exercises:

1. Prove that $a^3 \equiv a \pmod 6$ for every integer a.
2. Prove that $a^4 \equiv 1 \pmod 5$ for every integer a that is not divisible by 5.
3. Prove that if a is an odd integer, then $a^2 \equiv 1 \pmod 8$.
4. Let d be a positive integer that is a common divisor of a,b and m. Prove that

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

   if and only if

   $$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

1.2 Linear Congruences

The following theorem is one the most useful and important tools in elementary number theory.

Theorem 1.1

Let m,a,b be integers with $m \geq 1$. Let $d = (a,m)$ be the greatest common divisor of a and m. The congruence

$$ax \equiv b \pmod{m} \quad (1.1)$$

has a solution if and only if

$$b \equiv 0 \pmod{d}$$

If $b \equiv 0 \pmod{d}$, then the congruence (1.1) has exactly d solutions in integers that are pairwise incongruent modulo m. In particular, if (a,m) = 1, then for every integer b the congruence (1.1) has a unique solution modulo m.

Proof (Exercise)

Lemma 1.2

Let p be a prime number. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

Proof (Exercise)

Theorem 1.3 (Wilson) If p is prime, then

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

Proof (Demonstration)

1.2 Euler-phi Function

Definition

Congruence Class:

a and b belongs to the same congruence class modulo m if $a \equiv b \pmod{m}$.

We denote by $\varphi(m)$ the number of congruence classes that are relatively prime to m. Or simply, the function $\varphi(m)$ is the number of integers in the set 1,2,…,m that are relatively prime to m, which is called **Euler Phi Function**.

A set of integers $\{r_1, r_2, ..., r_{\varphi(m)}\}$ is called **a reduced set of residues modulo m** if every integer x such that (x,m) = 1 is congruent modulo m to some integer r_i.

For example: the set {1,2,3,4,5,6} and {2,4,6,8,10,12} are reduced sets of residues modulo 7. The sets {1,3,5,7} and {3,9,15,21} are reduced sets of residues modulo 8.

An integer a is called **invertible modulo m or a unit modulo m** if there exists an integer x such that

$$ax \equiv 1 \pmod{m}.$$

Hint: An effective way to find inverse is to use ***Euclidean Algorithm***

Exercise

5. Find all solutions of the congruence $4x \equiv 9 \pmod{11}$.
6. Find all solutions of the congruence $12x \equiv 3 \pmod{45}$.
7. Find all solutions of the congruence $28x \equiv 35 \pmod{42}$.
8. Find all solutions of the system of congruences

$$5x + 7y \equiv 3 \pmod{17}$$
$$2x + 3y \equiv -2 \pmod{17}$$

9. Find all solutions of the system of congruences

$$8x + 5y \equiv 1 \pmod{13}$$
$$4x + 3y \equiv 3 \pmod{13}$$

10. Prove that if $p \geq 5$ is an odd prime, then

$$6(p-4)! \equiv 1 \pmod{p}.$$

11. Let m and a be integers such that $m \geq 1$ and (a,m)=1. prove that if $\{r_1, ..., r_{\varphi(m)}\}$ is a reduced set of residues modulo m, then $\{ar_1, ..., ar_{\varphi(m)}\}$ is also a reduced set of residues modulo m.
12. For $n \geq 1$, consider the rational number

$$h_n = \sum_{k=1}^{n} \frac{1}{k} = \frac{u_n}{v_n},$$

where u_n and v_n are positive integers. Prove that if p is an odd prime, then the numerator u_{p-1} of h_{p-1} is divisible by p. (Hint : By Wilson's Theorem)

1.3 Some Important Properties of Euler Phi Function.

Lemma 1.4

Let m and n be relatively prime positive integers. For every integer c, there exist unique integers a and b such that

$$\begin{matrix} 0 \le a \le n-1 \\ 0 \le b \le m-1 \end{matrix},$$

and

$$c \equiv ma + nb \pmod{mn}\ldots\ldots.(1.3)$$

Moreover (c,mn) =1 if and only if (a,n)=(b,m)=1.

Theorem 1.5

The Euler Phi Function is multiplicative, i.e. $\varphi(mn) = \varphi(m)\varphi(n)$ if $(m,n) = 1$.

Moreover,

$$\varphi(m) = m\prod_{p|m}\left(1 - \frac{1}{p}\right)$$

Example: Find $\varphi(7875)$

Theorem 1.6

For every positive integer m,

$$\sum_{d|m}\varphi(d) = m$$

Exercises

13. Compute $\varphi(6993)$.
14. Represent the congruence classes modulo 12 in the form $3a + 4b$ with $0 \le a \le 3$ and $0 \le b \le 2$.
15. Let m=15. Compute $\varphi(d)$ for every divisor d of m, and check $\sum_{d|m}\varphi(d) = m$.

    Repeat the exercise for 16,17 and 18.
16. Prove that $\varphi(m)$ is even for all $m \ge 3$.
17. Prove that $\varphi(m^k) = m^{k-1}\varphi(m)$ for all positive integers m and k.
18. Prove that m is prime if and only if $\varphi(m) = m - 1$.
19. Prove that $\varphi(m) = \varphi(2m)$ if and only if m is odd.
20. Prove that if m divides n, then $\varphi(m)$ divides $\varphi(n)$.

21. Find all positive integers n such that $\varphi(n)$ is not divisible by 4.
22. Find all positive integers n such that $\varphi(5n) = 5\varphi(n)$.
23. Let $f(n) = \varphi(n)/n$. Prove that $f(p^k) = f(p)$ for all primes p and all positive integers k.

1.4 Chinese Remainder Theorem

Theorem 1.7

Let m and n be positive integers. For any integers a and b, there exists an integer x such that

$$x \equiv a \pmod{m} \text{ ....(1)}$$

and

$$x \equiv b \pmod{n} \text{ ...... (2)}$$

if and only if

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

If x is a solution of congruences (1) and (2), then the integer y is also a solution if and only if

$$x \equiv y \pmod{[m,n]}.$$

Theorem 1.8 *(Generalized version of Theorem 1.8 --- Chinese Remainder Theorem)*

Let $k \ge 2$. If $a_1, \dots, a_k$ are integers and $m_1, \dots, m_k$ are pairwise relatively prime positive integers, then there exists an integer x such that

$$x \equiv a_i \pmod{m_i} \quad \text{for all } i=1,2,\dots,k.$$

If x is any solution of this set of congruences, then the integer y is also a solution if and only if

$$x \equiv y \pmod{m_1, \dots m_k}$$

Theorem 1.9

Let

$$m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

be the standard factorization of the positive integer m. Let $f(x)$ be a polynomial with integral coefficients. The congruence

$$f(x) \equiv 0 \pmod{m}$$

is solvable if and only if the congruences

$$f(x) \equiv 0 \pmod{p_i^{r_i}}$$

are solvable for all i=1,2,…,k.

Exercises

24. Find all solutions of the system of congruences
$$x \equiv 4 \pmod 5$$
$$x \equiv 5 \pmod 6 .$$
25. Find all solutions of the system of congruences
$$x \equiv 5 \pmod{12}$$
$$x \equiv 8 \pmod 9 .$$
26. Find all solutions of the system of congruences
$$x \equiv 5 \pmod{12}$$
$$x \equiv 8 \pmod{10} .$$
27. Find all solutions of the system of congruences
$$2x \equiv 1 \pmod 5$$
$$3x \equiv 4 \pmod 7 .$$
28. Find all solutions of the congruence
$$f(x) = 5x^3 - 93 \equiv 0 \pmod{231}.$$
29. Find all integers that have remainder of 1 when divided by 3,5,and 7.
30. Find all integers that have a remainder of 2 when divided by 4 and that have a remainder of 3 when divided by 5.
31. A basket contains n eggs. If the eggs are removed 2,3,4,5, or 6 at a time, then the number of eggs that remain in the basket is 1,2,3,4 or 5 respectively. If the eggs are removed 7 at a time, then no eggs remain. What is the smallest number n eggs that could have been in the basket at the start of this procedure?

--- End of Session 5---

Reference:

1. **Elementary Methods in Number Theory; Melvyn B.Nathanson, Springer-Verlag.**
2. **A course in Number Theory and Cryptography(2nd Edition); Neal Koblitz, Springer-Verlag.**
3. **An Introduction to the Theory of Numbers(5th Edition); Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, John Wiley & Son inc.**
4. **Elementary Number Theory; Edmund Landau, Chelsea Publishing Company**
5. **數論講義 上冊 第二版; 柯召 孫琦 編著, 高等教育出版社**
6. **競賽數學解題研究 張同君 陳傳理 主編, 高等教育出版社**