CONGRUENCES I

Sometimes it takes a great mind to think of a simple idea. An example is the invention of the simple but powerful idea of congruence by the great German mathematician Carl Friedrich Gauss.

DEFINITION. Let a and b be integers and let m be a natural number. We write $a \equiv b \pmod{m}$ if and only if $m|(a-b)$.

The statement $a \equiv b \pmod{m}$ is read *a is congruent to b modulo m*. The number m is called the *modulus* of the congruence.

The following result summarizes the main properties of congruences. These can be easily proved from the definition of congruence and divisibility properties.

FACTS.

1. $a \equiv a \pmod{m}$ for every integer a; congruence is *reflexive*.
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$; congruence is *symmetric*.
3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$; congruence is *transitive*.
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$; congruences may be added.
5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$; congruences may be multiplied. In particular, if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for all $n \in \mathbb{N}$.
6. If $ab \equiv ac \pmod{m}$ and $(a, m) = 1$, then $b \equiv c \pmod{m}$; in other words, we may divide both sides of a congruence by a number that is relatively prime to m.
7. If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, where m and n are relatively prime, then $a \equiv b \pmod{mn}$.

We next state three important theorems in number theory; the exercises will illustrate their usefulness:

FERMAT'S LITTLE THEOREM: If p is a prime number and a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Note that Fermat's Little Theorem implies that if a is not divisible by p, then

$$a^p \equiv a \pmod{p}$$

Fermat's Theorem was generalized by Euler to the case when the modulus isn't necessarily prime. Recall that the *Euler's totient function* ϕ is defined by

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

EULER'S THEOREM: If $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

WILSON'S THEOREM: The natural number n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

In particular, if p is a prime number, then Wilson's Theorem shows that:

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

1. Which of the following congruences are true:

   (a) $57 \equiv 21 \pmod{6}$

   (b) $11 \equiv -14 \pmod{17}$

   (c) $k^2 \equiv k \pmod{k}$, for k a positive integer.

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

3. Find the remainder when $1! + 2! + \cdots + 100!$ is divided by 15.

4. Halley's comet appears in our skies approximately every 76 years. It visited us in 1835, 1910, and most recently in 1986. It will return in 2061. Show that $1835^{1910} + 1986^{2061}$ is divisible by 7.

5. Show that $1941^{1963} + 1963^{1991}$ is divisible by 7.

6. Show that 7 divides $111^{333} + 333^{111}$.

7. *(1987 NEAML)* In decimal notation, what is the sum of the ten's digit and the unit's digit of the following integer:

$$2! + 4! + 6! + 8! + 10! + 12! + 14! + 16!$$

8. *(1986 NEAML)* The number 7^{43} has 37 digits when written in standard form. Find the ten's digit T and the unit's digit U. Express your answer as the ordered pair (T, U).

9. Show that if p is a prime greater than 3, then $p^2 + 2$ is composite.

10. Show that for any positive integer n, $2^{2^n} + 5$ is composite.

11. The number of integers n between 1 and 2000 (inclusive) for which $2^n + 1$ is divisible by 3 is:

    (A) 300 (B) 600 (C) 1000 (D) 100 (E) 500

12. Find the remainder when 2^{4901} is divided by 11.

    (A) 1 (B) 3 (C) 6 (D) 10 (E) 2

13. What are the last two digits in the number 11^{111}?

(A) 01 (B) 11 (C) 21 (D) 31 (E) 41

14. Prove that $36^{36} + 41^{41}$ is divisible by 77.

15. Show that the number $1^{47} + 2^{47} + 3^{47} + 4^{47} + 5^{47} + 6^{47}$ is a multiple of 7.

16. Prove that $20^{15} - 1$ is divisible by 20801.

17. *(AOPS Volume II)* Find the remainder when 4^{87} is divided by 17.

18. *(AOPS Volume II)* Find the remainder when 6^{1000} is divided by 23.

19. Find the last two digits of 3^{1999}.

    (A) 49 (B) 41 (C) 69 (D) 67 (E) 61

20. Find the remainder when 3^{1999} is divided by 47.

(A) 20 (B) 21 (C) 41 (D) 19 (E) 18

21. Find the remainder when 2^{1990} is divided by 1990.

(A) 1024 (B) 1990 (C) 1991 (D) 1023 (E) 1989

22. Find the remainder when $p^6 - 1$ is divided by 504, where $p > 7$ is a prime number.

23. Find the last three digits of 7^{9999}.

24. What are the last two digits of $6^{2007} + 7^{2007}$?

(A) 59 (B) 21 (C) 79 (D) 23 (E) 69

25. What is the smallest prime divisor of $5^{1999} + 6^{1999}$?

(A) 2 (B) 5 (C) 7 (D) 11 (E) 13

26. Determine the last two digits of 9^{9^9}.

27. Find the remainder when $1^5 + 2^5 + \cdots + 100^5$ is divided by 4.

28. Use Wilson's Theorem to show that 17 is prime.

29. Find the remainder when 15! is divided by 17.

30. Show that $18! \equiv -1 \pmod{437}$.

31. For any odd prime p, show that

$$1^2 \cdot 3^2 \ldots (p-2)^2 \equiv 2^2 \cdot 4^2 \ldots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

32. *(J. Wolstenholme 1862)* Prove that if $p > 3$ is a prime, then

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p}$$

33. *(1991 USAMO)* Show that for any fixed integer $n \geq 1$, the sequence

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots \pmod{m}$$

is eventually constant.

34. Let P be a polynomial with integer coefficients, and let a and b be arbitrary integers. Then

$$P(a) \equiv P(b) \pmod{a-b}$$

In other words, $P(a) - P(b)$ is divisible by $a - b$.

35. *(1974 USAMO)* Let a, b, and c denote three distinct integers, and let P denote a polynomial having all integer coefficients. Show that it is impossible that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

36. Let $s(n)$ denote the sum of the digits in the decimal representation of n. Show that

$$n \equiv s(n) \pmod 9$$

37. Prove that there is no integer n such that $n^2 + 3n + 4$ is divisible by 49.

38. By Fermat's Theorem, we know that $n^5 \equiv n \pmod 5$.

(a) Prove that $n^5 \equiv n \pmod{30}$.

(b) Prove that if n is odd, then $n^5 \equiv n \pmod{240}$.

39. Prove that:

(a) $19^{19} + 69^{69}$ is divisible by 44.

(b) $2^{70} + 3^{70}$ is divisible by 13.

40. Prove that $7|(a^2 + b^2)$ if and only if $7|a$ and $7|b$.

41. *(1964 IMO, ♯ 1)*

(a) Find all positive integers n for which $2^n - 1$ is divisible by 7.

(b) Prove that there is no positive integer n for which $2^n + 1$ is divisible by 7.

42. *(1999 Mandelbrot Competition, Round 4 Individual)* Find the sum of all primes less than 20 which are factors of $19^{99} + 99^{19}$.

43. *(2005 USAMO)* Prove that the system

$$\begin{cases} x^6 + x^3 + x^3y + y &= 147^{157} \\ x^3 + x^3y + y^2 + y + z^9 &= 157^{147} \end{cases}$$

has no solutions in integers x, y, and z.

44. *(2000-2001 USAMTS)* Prove that if n is an odd positive integer, then

$$N = 2269^n + 1779^n + 1730^n - 1776^n$$

is an integer multiple of 2001.

45. *(2008 SJSU Problem of the Week Competition)* For any $n \geq 0$ show that

$$157^{2n+1} + 1098^{2n+1} + 46^{2n+1} + 707^{2n+1}$$

is divisible by 2008.

46. *(2000-2001 USAMTS)* It was recently shown that $2^{2^{24}}+1$ is not a prime number. Find the four rightmost digits of this number.

47. *(2000-2001 USAMTS)* Compute the remainder when $1776^{1492!}$ is divided by 2000.