NUMBER THEORY

GEORGE E. ANDREWS

Evan Pugh Professor of Mathematics
Pennsylvania State University

DOVER PUBLICATIONS, INC.
NEW YORK

4. Let $w(n)$ denote the number of primes not exceeding n that do not divide n. Is $w(n) < \phi(n)$? Can you find values of n for which $w(n) = \phi(n) - 1$?

4–3 RIFFLING

In this section we shall demonstrate the usefulness of congruences in solving a problem of frequent interest to college students.

Take an ordinary deck of cards arranged in any order. How many shuffles are required before the deck returns to its original order? Of course, to idealize the real life situation, we must stipulate that only the modified perfect faro shuffle is permitted, as follows: Cut the deck into two equal 26-card packs; then proceed by alternating cards from each pack. The cards formerly in positions $1,2,\ldots,26$ are moved to positions $2,4,\ldots,52$; and the cards formerly in positions $27,28,\ldots,52$ are moved to positions $1,3,\ldots,51$. Thus, if a card starts in position x, it will end in position y, where $1 \leq y \leq 52$ and $2x \equiv y \pmod{53}$. After n shuffles, the card will be in position w, where $1 \leq w \leq 52$ and $2^n x \equiv w \pmod{53}$.

To determine the number of necessary shuffles, we must find n such that $2^n x \equiv x \pmod{53}$ for every x such that $1 \leq x \leq 52$. Since 53 is a prime, we may cancel x from both sides of the congruence; thus we must solve the congruence

$$2^n \equiv 1 \pmod{53}. \qquad (4\text{-}3\text{-}1)$$

By Fermat's little theorem, we know that

$$2^{53} \equiv 2 \pmod{53}. \qquad (4\text{-}3\text{-}2)$$

Cancelling 2 from both sides of congruence (4–3–2), we find that

$$2^{52} \equiv 1 \pmod{53}. \qquad (4\text{-}3\text{-}3)$$

Hence, the cards will return to their original order after 52 shuffles. Actually, 52 is the least number of shuffles required, but we shall not prove this here.

In general, if we have a deck of m cards, then n shuffles will return the cards to the original order provided that

$$2^n \equiv 1 \pmod{m+1}. \qquad (4\text{-}3\text{-}4)$$

Thus, if $m = 62$, we need only 6 shuffles, since $2^6 - 1 = 63$.

EXERCISES

1. How many modified perfect faro shuffles are needed to return the cards to their original position in a deck of 6 cards? of 8 cards? of 12 cards?

2. Suppose that instead of performing a modified perfect faro shuffle as described in this section, we shuffle as follows: Take the bottom and top cards of the deck and place them on the table to start a new deck. Then take the remaining bottom and top cards and place them on the newly started pile. Continue this process until all cards are gone from the original pack. For example, if the deck has six cards, then we shuffle as shown in Figure 4–1.

Figure 4–1 Shuffle of a deck of six cards described in Exercise 2 (side view).

Prove that the cards in a deck of 2^n cards will return to their original positions after $n+1$ such shuffles. (Note that the shuffle described in this problem is mechanically somewhat easier to perform than the modified perfect faro shuffle described earlier.)

5. What is the remainder when 41^{75} is divided by 3?

6. What is the remainder when 473^{38} is divided by 5?

7. Prove that if $A = a_0 10^n + a_1 10^{n-1} + \ldots + a_n$ and $S = a_0 + a_1 + \ldots + a_n$, then $A \equiv S \pmod 9$. (This result is the basis for the computational check called "casting out nines".)

8. Suppose that p is a prime, and that $p \nmid a$; use Euler's theorem to prove that $x = a^{p-2}b$ is a solution of

$$ax \equiv b \pmod p.$$

9. Prove that if p is a prime congruent to 1 modulo 4, then

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

[Hint: Prove that $((p-1)/2)!^2 \equiv (p-1)! \pmod p$.]

10. Use Exercise 9 to find a solution of each of the following congruences.

(a) $x^2 \equiv -1 \pmod{13}$

(b) $x^2 \equiv -1 \pmod{17}$.

11. Prove that for each odd prime p and for each a $(0 \le a \le p-1)$,

$$\binom{p-1}{a} \equiv (-1)^a \pmod p.$$

12. Prove that for each prime p $(n < p \le 2n)$,

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

but that

$$\binom{2n}{n} \not\equiv 0 \pmod{p^2}.$$

13. Is $2^{p-1} \equiv 1 \pmod{p^2}$ for $p = 2$? for $p = 3$? for $p = 5$? for $p = 7$? for $p = 11$? (After completing Exercise 13 you may be interested to learn that $2^{1092} \equiv 1 \pmod{1093^2}$.)

14. For each m greater than 1, how many primes are there in the closed interval $[m! + 2, m! + m]$?

15. Suppose p denotes a prime congruent to 3 modulo 4; use Wilson's theorem to prove that

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

[Hint: See the hint for Exercise 9.]

16. Find the *least* positive integer n that satisfies each of the following congruences.

(a) $3^{56} \equiv n \pmod 7$

(b) $7^{38} \equiv n \pmod{11}$

(c) $7^{128} \equiv n \pmod{13}$.

17. Decide whether or not 17 is a prime by determining whether 16! is congruent to -1 modulo 17. Is this an efficient test for determining whether or not 1093 is a prime?

18. Let $\lambda(m)$ be the least positive integer such that for each integer a relatively prime to m,

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

Compute $\lambda(m)$ for each m $(1 \le m \le 10)$. *Is* $\lambda(m) \le \phi(m)$ for each m? Is $\lambda(m) < \phi(m)$ for some m?

19. In 500 B.C. the Chinese seem to have known that $2^p \equiv 2 \pmod p$ for each prime p. They also assumed that if $2^n \equiv 2 \pmod n$, then n is prime.

(a) Show that 341 is not a prime.

(b) Show that $2^{10} \equiv 1 \pmod{341}$.

(c) Show that $2^{341} \equiv 2 \pmod{341}$.

20. Let $\Phi_n = 2^{2^n} + 1$.

(a) Prove that $\Phi_n \mid (2^{2^{n+1}} - 1)$.

(b) Prove that if $a \mid b$, then $(2^a - 1) \mid (2^b - 1)$.

(c) Prove that $(2^{2^{n+1}} - 1) \mid (2^{2^{2^n}} - 1)$.

(d) Prove that $(2^{2^{2^n}} - 1) \mid (2^{2^{2^n+1}} - 2)$.

(e) Prove that $\Phi_n \mid (2^{\Phi_n} - 2)$.

(f) P. Fermat observed that $\Phi_1 = 5$, $\Phi_2 = 17$, $\Phi_3 = 257$, and $\Phi_4 = 65537$ are all primes, and he suggested that Φ_n is prime for each n. Discuss Fermat's suggestion in the light of Exercises 19 and 20(e).

21. Prove that if p denotes an odd prime, then

$$2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

22. Prove that if $p \equiv 3 \pmod 4$, then the product of all the odd integers less than p is congruent either to 1 or to -1 modulo p. [Hint: If $p = 2l + 1$, then $(p-1)! = 2^l l! \cdot 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2l-1)$.]

23. Prove that if $p \equiv 3 \pmod 4$, then the product of all the even integers less than p is congruent either to 1 or to -1 modulo p.

5–3 THE CHINESE REMAINDER THEOREM

Having considered single linear congruences in Section 5–1, we now turn to the problem of finding solutions of systems of linear congruences. A solution of the system of congruences

$$a_1 x \equiv b_1 \pmod{m_1},$$
$$a_2 x \equiv b_2 \pmod{m_2},$$
$$\ldots,$$

and

$$a_s x \equiv b_s \pmod{m_s}$$

is an integer that satisfies each congruence in the system.

The simplest examples of such systems arise in the solution of single linear congruences with large moduli. Let m have the prime factorization

$$m = p_1^{e_1} p_2^{e_2} \ldots p_s^{e_s};$$

then, as a consequence of the fundamental theorem of arithmetic, $m \mid n$ if and only if $p_i^{e_i} \mid n$ for each i. Hence,

$$A \equiv B \pmod{m}$$

if and only if all of the congruences

$$A \equiv B \pmod{p_1^{e_1}},$$
$$A \equiv B \pmod{p_2^{e_2}},$$
$$\ldots,$$

and

$$A \equiv B \pmod{p_s^{e_s}}$$

hold. It follows that the congruence

$$ax \equiv b \pmod{m} \qquad (5\text{-}3\text{-}1)$$

has the same set of solutions as the system of simultaneous congruences

$$ax \equiv b \pmod{p_1^{e_1}},$$
$$ax \equiv b \pmod{p_2^{e_2}},$$
$$\ldots, \qquad (5\text{-}3\text{-}2)$$

and

$$ax \equiv b \pmod{p_s^{e_s}}.$$

Although there are several congruences to solve in (5–3–2), their moduli are generally much smaller than m, and, as we shall see, computations are thus simplified.

Example 5–6: Let us replace the congruence

$$3x \equiv 11 \pmod{2275}$$

by a system of linear congruences with smaller moduli. Since $2275 = 5^2 \cdot 7 \cdot 13$, our congruence may be replaced by the system

$$3x \equiv 11 \pmod{25}, \qquad (5\text{-}3\text{-}3)$$

$$3x \equiv 11 \pmod{7}, \qquad (5\text{-}3\text{-}4)$$

and

$$3x \equiv 11 \pmod{13}, \qquad (5\text{-}3\text{-}5)$$