Example 6.6. To find $2^{9!} \pmod{5,157,437}$, we perform the following sequence of computations:

$$r_2 \equiv r_1^2 = 2^2 \equiv 4 \pmod{5,157,437}$$
$$r_3 \equiv r_2^3 = 4^3 \equiv 64 \pmod{5,157,437}$$
$$r_4 \equiv r_3^4 = 64^4 \equiv 1,304,905 \pmod{5,157,437}$$
$$r_5 \equiv r_4^5 = 1,304,905^5 \equiv 404,913 \pmod{5,157,437}$$
$$r_6 \equiv r_5^6 = 404,913^6 \equiv 2,157,880 \pmod{5,157,437}$$
$$r_7 \equiv r_6^7 = 2,157,880^7 \equiv 4,879,227 \pmod{5,157,437}$$
$$r_8 \equiv r_7^8 = 4,879,227^8 \equiv 4,379,778 \pmod{5,157,437}$$
$$r_9 \equiv r_8^9 = 4,379,778^9 \equiv 4,381,440 \pmod{5,157,437}.$$

It follows that $2^{9!} \equiv 4,381,440 \pmod{5,157,437}$. ◀

The following example illustrates the use of the Pollard $p-1$ method to find a factor of the integer 5,157,437.

Example 6.7. To factor 5,157,437 using the Pollard $p-1$ method, we successively find r_k, the least positive residue of $2^{k!}$ modulo 5,157,437, for $k = 1, 2, 3, \ldots$, as was done in Example 6.6. We compute $(r_k - 1, 5,157,437)$ at each step. To find a factor of 5,157,437 requires nine steps, because $(r_k - 1, 5,157,437) = 1$ for $k = 1, 2, 3, 4, 5, 6, 7, 8$ (as the reader can verify), but $(r_9 - 1, 5,157,437) = (4,381,439, 5,157,437) = 2269$. It follows that 2269 is a divisor of 5,157,437. ◀

The Pollard $p-1$ method does not always work. However, because nothing in the method depends on the choice of 2 as the base, we can extend the method and find a factor for more integers by using integers other than 2 as the base. In practice, the Pollard $p-1$ method is used after trial divisions by small primes, but before the heavy artillery of such methods as the quadratic sieve and the elliptic curve method.

6.1 Exercises

1. Show that $10! + 1$ is divisible by 11, by grouping together pairs of inverses modulo 11 that occur in 10!.
2. Show that $12! + 1$ is divisible by 13, by grouping together pairs of inverses modulo 13 that occur in 12!.
3. What is the remainder when 16! is divided by 19?
4. What is the remainder when 5!25! is divided by 31?
5. Using Wilson's theorem, find the least positive residue of $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ modulo 7.
6. What is the remainder when $7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43$ is divided by 11?

7. What is the remainder when 18! is divided by 437?
8. What is the remainder when 40! is divided by 1763?
9. What is the remainder when 5^{100} is divided by 7?
10. What is the remainder when 6^{2000} is divided by 11?
11. Using Fermat's little theorem, find the least positive residue of $3^{999,999,999}$ modulo 7.
12. Using Fermat's little theorem, find the least positive residue of $2^{1000000}$ modulo 17.
13. Show that $3^{10} \equiv 1 \pmod{11^2}$.
14. Using Fermat's little theorem, find the last digit of the base 7 expansion of 3^{100}.
15. Using Fermat's little theorem, find the solutions of the following linear congruences.
    a) $7x \equiv 12 \pmod{17}$ b) $4x \equiv 11 \pmod{19}$
16. Show that if n is a composite integer with $n \neq 4$, then $(n-1)! \equiv 0 \pmod{n}$.
17. Show that if p is an odd prime, then $2(p-3)! \equiv -1 \pmod{p}$.
18. Show that if n is odd and $3 \nmid n$, then $n^2 \equiv 1 \pmod{24}$.
19. Show that $a^{12} - 1$ is divisible by 35 whenever $(a, 35) = 1$.
20. Show that $a^6 - 1$ is divisible by 168 whenever $(a, 42) = 1$.
21. Show that $42 \mid (n^7 - n)$ for all positive integers n.
22. Show that $30 \mid (n^9 - n)$ for all positive integers n.
23. Show that $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{(p-1)} \equiv -1 \pmod{p}$ whenever p is prime. (It has been conjectured that the converse of this is also true.)
24. Show that $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$ when p is an odd prime.
25. Show that if p is prime and a and b are integers not divisible by p, with $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.
26. Use the Pollard $p-1$ method to find a divisor of 689.
27. Use the Pollard $p-1$ method to find a divisor of 7,331,117. (For this exercise, you will need to use either a calculator or computational software.)
28. Show that if p and q are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
29. Show that if p is prime and a is an integer, then $p \mid (a^p + (p-1)!\,a)$.
30. Show that if p is an odd prime, then $1^2 3^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.
31. Show that if p is prime and $p \equiv 3 \pmod{4}$, then $((p-1)/2)! \equiv \pm 1 \pmod{p}$.
32. a) Let p be prime, and suppose that r is a positive integer less than p such that $(-1)^r r! \equiv -1 \pmod{p}$. Show that $(p-r+1)! \equiv -1 \pmod{p}$.
    b) Using part (a), show that $61! \equiv 63! \equiv -1 \pmod{71}$.
33. Using Wilson's theorem, show that if p is a prime and $p \equiv 1 \pmod{4}$, then the congruence $x^2 \equiv -1 \pmod{p}$ has two incongruent solutions given by $x \equiv \pm((p-1)/2)! \pmod{p}$.

34. Show that if p is a prime and $0 < k < p$, then $(p-k)!(k-1)! \equiv (-1)^k \pmod{p}$.

35. Show that if n is an integer, then

$$\pi(n) = \sum_{j=2}^{n} \left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j} \right] \right].$$

* **36.** For which positive integers n is $n^4 + 4^n$ prime?

37. Show that the pair of positive integers n and $n+2$ are twin primes if and only if $4((n-1)!+1)+n \equiv 0 \pmod{n(n+2)}$, where $n \neq 1$.

38. Show that if the positive integers n and $n+k$, where $n > k$ and k is an even positive integer, are both prime, then $(k!)^2((n-1)!+1)+n(k!-1)(k-1)! \equiv 0 \pmod{n(n+k)}$.

39. Show that if p is prime, then $\binom{2p}{p} \equiv 2 \pmod{p}$.

40. Exercise 74 of Section 3.5 shows that if p is prime and k is a positive integer less than p, then the binomial coefficient $\binom{p}{k}$ is divisible by p. Use this fact and the binomial theorem to show that if a and b are integers, then $(a+b)^p \equiv a^p + b^p \pmod{p}$.

41. Prove Fermat's little theorem by mathematical induction. (*Hint:* In the induction step, use Exercise 40 to obtain a congruence for $(a+1)^p$.)

* **42.** Using Exercise 30 of Section 4.3, prove *Gauss's generalization of Wilson's theorem*, namely that the product of all the positive integers less than m that are relatively prime to m is congruent to 1 (mod m), unless $m = 4$, p^t, or $2p^t$, where p is an odd prime and t is a positive integer, in which case it is congruent to -1 (mod m).

43. A deck of cards is shuffled by cutting the deck into two piles of 26 cards. Then, the new deck is formed by alternating cards from the two piles, starting with the bottom pile.

a) Show that if a card begins in the cth position in the deck, it will be in the bth position in the new deck, where $b \equiv 2c \pmod{53}$ and $1 \leq b \leq 52$.

b) Determine the number of shuffles of the type described above that are needed to return the deck of cards to its original order.

44. Let p be prime and let a be a positive integer not divisible by p. We define the *Fermat quotient* $q_p(a)$ by $q_p(a) = (a^{p-1} - 1)/p$. Show that if a and b are positive integers not divisible by the prime p, then $q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}$.

45. Let p be prime and let $a_1, a_2, \ldots, a_p$ and $b_1, b_2, \ldots, b_p$ be complete systems of residues modulo p. Show that $a_1b_1, a_2b_2, \ldots, a_pb_p$ is not a complete system of residues modulo p.

* **46.** Show that if n is a positive integer with $n \geq 2$, then n does not divide $2^n - 1$.

* **47.** Let p be an odd prime. Show that $(p-1)!^{p^{n-1}} \equiv -1 \pmod{p^n}$.

48. Show that if p is a prime with $p > 5$, then $(p-1)!+1$ has at least two different prime divisors.

49. Show that if a and n are relatively prime integers with $n > 1$, then n is prime if and only if $(x-a)^n$ and $x^n - a$ are congruent modulo n as polynomials. (Recall from the preamble to Exercise 40 in Section 4.1 that two polynomials are congruent modulo n as