integers 2, 3, ..., 11 into $(p-3)/2 = 5$ pairs each of whose products is congruent to 1 modulo 13. To write these congruences out explicitly:

$$\begin{aligned} 2 \cdot 7 &\equiv 1 \pmod{13}, \\ 3 \cdot 9 &\equiv 1 \pmod{13}, \\ 4 \cdot 10 &\equiv 1 \pmod{13}, \\ 5 \cdot 8 &\equiv 1 \pmod{13}, \\ 6 \cdot 11 &\equiv 1 \pmod{13}. \end{aligned}$$

Multiplving the above congruences gives the result

$$11! = (2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}$$

and so

$$12! \equiv 12 \equiv -1 \pmod{13}.$$

Thus, $(p-1)! \equiv -1 \pmod{p}$, with $p = 13$.

The converse of Wilson's Theorem is also true: If $(n-1)! \equiv -1 \pmod{n}$, then n must be prime. For, if n is not a prime, then n has a divisor d, with $1 < d < n$. Furthermore, since $d \leq n-1$, d occurs as one of the factors in $(n-1)!$, whence $d \mid (n-1)!$. Now we are assuming that $n \mid (n-1)! + 1$, and so $d \mid (n-1)! + 1$ too. The conclusion is that $d \mid 1$, which is nonsense.

Taken together, Wilson's Theorem and its converse provide a necessary and sufficient condition for determining primality; namely, an integer $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$. Unfortunately, this test is of more theoretical than practical interest since as n increases, $(n-1)!$ rapidly becomes unmanageable in size.

We would like to close this chapter with an application of Wilson's Theorem to the study of quadratic congruences. [It is understood that *quadratic congruence* means a congruence of the form $ax^2 + bx + c \equiv 0 \pmod{n}$, with $a \not\equiv 0 \pmod{n}$.] This is the content of

THEOREM 5-3. *The quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$, where p is an odd prime, has a solution if and only if $p \equiv 1 \pmod{4}$.*

Proof: Let a be any solution of $x^2 + 1 \equiv 0 \pmod{p}$, so that $a^2 \equiv -1 \pmod{p}$. Since $p \nmid a$, the outcome of applying Fermat's Theorem is:

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

The possibility that $p = 4k + 3$ for some k does not arise. If it did, we would have

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1;$$

hence $1 \equiv -1 \pmod{p}$. The net result of this is that $p \mid 2$, which is patently false. Therefore, p must be of the form $4k + 1$.

Now for the opposite direction. In the product

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1),$$

we have the congruences

$$\begin{aligned} p-1 &\equiv -1 \pmod{p}, \\ p-2 &\equiv -2 \pmod{p}, \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p}. \end{aligned}$$

Rearranging the factors produces

$$\begin{aligned} (p-1)! &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p} \\ &\equiv (-1)^{(p-1)/2}\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p}, \end{aligned}$$

since there are $(p-1)/2$ minus signs involved. It is at this point that Wilson's Theorem can be brought to bear; for, $(p-1)! \equiv -1 \pmod{p}$, whence

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

If we assume that p is of the form $4k + 1$, then $(-1)^{(p-1)/2} = 1$, leaving us with the congruence

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

The conclusion: $[(p-1)/2]!$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$.

Let us take a look at an actual example; say, the case $p = 13$, which is a prime of the form $4k + 1$. Here, we have $(p - 1)/2 = 6$ and it is easy to see that

$$6! = 720 \equiv 5 \pmod{13},$$

while

$$5^2 + 1 = 26 \equiv 0 \pmod{13}.$$

Thus the assertion that $[(\frac{1}{2}(p-1))!]^2 + 1 \equiv 0 \pmod{p}$ is correct for $p = 13$.

Wilson's Theorem implies that there exists an infinitude of composite numbers of the form $n! + 1$. On the other hand, it is an open question whether $n! + 1$ is prime for infinitely many values of n. The only values of n in the range $1 \leq n \leq 100$ for which $n! + 1$ is known to be a prime number are $n = 1, 2, 3, 11, 27, 37, 41, 73$, and 77.

PROBLEMS 5.4

1. (a) Find the remainder when $15!$ is divided by 17.
(b) Find the remainder when $2(26!)$ is divided by 29. [*Hint:* By Wilson's Theorem, $2(p-3)! \equiv -1 \pmod{p}$ for any odd prime $p > 3$.]

2. Determine whether 17 is a prime by deciding whether or not $16! \equiv -1 \pmod{17}$.

3. Arrange the integers $2, 3, 4, \ldots, 21$ in pairs a and b with the property that $ab \equiv 1 \pmod{23}$.

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

5. (a) Prove that an integer $n > 1$ is prime if and only if $(n-2)! \equiv 1 \pmod{n}$.
(b) If n is a composite integer, show that $(n-1)! \equiv 0 \pmod{n}$, except when $n = 4$.

6. Given a prime number p, establish the congruence

$$(p-1)! \equiv p - 1 \pmod{1 + 2 + 3 + \cdots + (p-1)}.$$

7. If p is a prime, prove that

$$p \mid a^p + (p-1)!a \quad \text{and} \quad p \mid (p-1)!a^p + a$$

for any integer a. [*Hint:* By Wilson's Theorem, $a^p + (p-1)!a \equiv a^p - a \pmod{p}$.]

8. Find two odd primes $p \leq 13$ for which the congruence $(p-1)! \equiv -1 \pmod{p^2}$ holds.

9. Using Wilson's Theorem, prove that

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

for any odd prime p. [*Hint:* Since $k \equiv -(p-k) \pmod{p}$, it follows that $2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{(p-1)/2} 1 \cdot 3 \cdot 5 \cdots (p-2) \pmod{p}$.]

10. (a) For a prime p of the form $4k+3$, prove that either

$$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \quad \text{or} \quad \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p};$$

hence, $[(p-1)/2]!$ satisfies the quadratic congruence $x^2 \equiv 1 \pmod{p}$.

(b) Use part (a) to show that if $p = 4k+3$ is prime, then the product of all the even integers less than p is congruent modulo p to either 1 or -1. [*Hint:* Fermat's Theorem implies that $2^{(p-1)/2} \equiv \pm 1 \pmod{p}$.]

11. Apply Theorem 5-3 to find two solutions to the quadratic congruences $x^2 \equiv -1 \pmod{29}$ and $x^2 \equiv -1 \pmod{37}$.

12. Show that if $p = 4k+3$ is prime and $a^2 + b^2 \equiv 0 \pmod{p}$, then $a \equiv b \equiv 0 \pmod{p}$. [*Hint:* If $a \not\equiv 0 \pmod{p}$, then there exists an integer c such that $ac \equiv 1 \pmod{p}$; use this fact to contradict Theorem 5-3.]