84, 89, 96. [*Hint:* Since $x^2 \equiv (50+x)^2 \pmod{100}$ and $x^2 \equiv (50-x)^2 \pmod{100}$, it suffices to examine the final digits of x^2 for the 26 values $x = 0, 1, 2, \ldots, 25$.]

3. Factor the number $2^{11} - 1$ by Fermat's factorization method.
4. In 1647, Mersenne noted that when a number can be written as a sum of two relatively prime squares in two distinct ways, it is composite and can be factored as follows: if $n = a^2 + b^2 = c^2 + d^2$, then

$$n = (ac + bd)(ac - bd)/(a + d)(a - d).$$

Use this result to factor the numbers

$$493 = 18^2 + 13^2 = 22^2 + 3^2,$$

and

$$38025 = 168^2 + 99^2 = 156^2 + 117^2.$$

5.3 THE LITTLE THEOREM

The most significant of Fermat's correspondents in number theory was Bernhard Frénicle de Bessy (1605–1675), an official at the French mint who was renowned for his gift of manipulating large numbers. (Frénicle's facility in numerical calculation is revealed by the following incident: On hearing that Fermat had proposed the problem of finding cubes which when increased by their proper divisors become squares, as is the case with $7^3 + (1 + 7 + 7^2) = 20^2$, he immediately gave four different solutions; and supplied six more the next day.) Though in no way Fermat's equal as a mathematician, Frénicle alone among his contemporaries could challenge him in number theory and his challenges had the distinction of coaxing out of Fermat some of his carefully guarded secrets. One of the most striking is the theorem which states: If p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$. Fermat communicated the result in a letter to Frénicle dated October 18, 1640, along with the comment, "I would send you the demonstration, if I did not fear its being too long." This theorem has since become known as "Fermat's Little Theorem" to distinguish it from Fermat's "Great" or "Last Theorem," which is the subject of Chapter 11. Almost 100 years were to elapse before Euler published the first proof of the Little Theorem in 1736. Leibniz, however, seems not to have received his share of recognition; for he left an identical argument in an unpublished manuscript sometime before 1683.

We now proceed to a proof of Fermat's Theorem.

THEOREM 5-1 (Fermat's Little Theorem). *If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof: We begin by considering the first $p-1$ positive multiples of a; that is, the integers

$$a, 2a, 3a, \ldots, (p-1)a.$$

None of these numbers is congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that

$$ra \equiv sa \pmod{p}, \qquad 1 \le r < s \le p-1$$

then a could be cancelled to give $r \equiv s \pmod{p}$, which is impossible. Therefore, the above set of integers must be congruent modulo p to 1, 2, 3, ..., $p-1$, taken in some order. Multiplying all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

whence

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

Once $(p-1)!$ is cancelled from both sides of the preceding congruence (this is possible since $p \nmid (p-1)!$), our line of reasoning culminates in $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's Theorem.

This result can be stated in a slightly more general way in which the requirement that $p \nmid a$ is dropped.

COROLLARY. *If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.*

Proof: When $p \mid a$, the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, then in accordance with Fermat's Theorem, $a^{p-1} \equiv 1 \pmod{p}$. When this congruence is multiplied by a, the conclusion $a^p \equiv a \pmod{p}$ follows.

There is a different proof of the fact that $a^p \equiv a \pmod{p}$, involving induction on a. If $a = 1$, the assertion is that $1^p \equiv 1 \pmod{p}$, which is clearly true, as is the case $a = 0$. Assuming that the result holds for a, we must confirm its validity for $a + 1$. In light of the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{k}a^{p-k} + \cdots + \binom{p}{p-1}a + 1,$$

where the coefficient $\binom{p}{k}$ is given by

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k}.$$

Our argument hinges on the observation that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$. To see this, note that

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1) \equiv 0 \pmod{p},$$

by virtue of which $p \mid k!$ or $p \mid \binom{p}{k}$. But $p \mid k!$ implies that $p \mid j$ for some j satisfying $1 \leq j \leq k \leq p-1$, an absurdity. Therefore, $p \mid \binom{p}{k}$ or, converting to a congruence statement,

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

The point which we wish to make is that

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p},$$

where the right-most congruence uses our inductive assumption. Thus, the desired conclusion holds for $a+1$ and, in consequence, for all $a \geq 0$. If a is a negative integer, there is no problem: since $a \equiv r \pmod{p}$ for some r, where $0 \leq r \leq p-1$, we get $a^p \equiv r^p \equiv r \equiv a \pmod{p}$.

Fermat's Theorem has many applications and is central to much of what is done in number theory. On one hand, it can be a labor-saving device in certain calculations. If asked to verify that $5^{38} \equiv 4 \pmod{11}$, for instance, we would take the congruence $5^{10} \equiv 1 \pmod{11}$ as our starting point. Knowing this,

$$\begin{aligned} 5^{38} &= 5^{10\cdot 3+8} = (5^{10})^3(5^2)^4 \\ &\equiv 1^3 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}, \end{aligned}$$

as desired.

Another use of Fermat's Theorem is as a tool in testing the primality of a given integer n. For, if it could be shown that the congruence

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

fails to hold for some choice of a, then n is necessarily composite. As an example of this approach, let us look at $n = 117$. The computation is kept under control by selecting a small integer for a; say, $a = 2$. Since 2^{117} may we written as

$$2^{117} = 2^{7 \cdot 16 + 5} = (2^7)^{16} 2^5$$

and $2^7 = 128 \equiv 11 \pmod{117}$, we have

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8\, 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}.$$

But $2^{21} = (2^7)^3$, which leads to

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}.$$

Combining these congruences, we finally obtain

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117},$$

so that 117 must be composite; actually, $117 = 13 \cdot 9$.

It might be worthwhile to give an example illustrating the failure of the converse of Fermat's Theorem to hold; in other words, to show that if $a^{n-1} \equiv 1 \pmod{n}$ for some integer a, then n need not be prime. As a prelude we require a technical lemma:

LEMMA. *If p and q are distinct primes such that $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.*

Proof: It is known from the last corollary that $(a^q)^p \equiv a^q \pmod{p}$, while $a^q \equiv a \pmod{p}$ by hypothesis. Combining these congruences, we obtain $a^{pq} \equiv a \pmod{p}$ or, in different terms, $p \mid a^{pq} - a$. In an entirely similar manner, $q \mid a^{pq} - a$. The corollary to Theorem 2-4 now yields $pq \mid a^{pq} - a$, which can be recast as $a^{pq} \equiv a \pmod{pq}$.

Our contention is that $2^{340} \equiv 1 \pmod{341}$ where $341 = 11 \cdot 31$. In working towards this end, notice that $2^{10} = 1024 = 31 \cdot 33 + 1$. Thus,

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$$

and

$$2^{31} = 2\,(2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}.$$

Exploiting the lemma,

$$2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$$