CHAPTER 5

FERMAT'S THEOREM

And perhaps posterity will thank me for having shown it that the ancients did not know everything.
P. DE FERMAT

5.1 PIERRE DE FERMAT

What the ancient world had known was largely forgotten during the intellectual torpor of the Dark Ages, and it was only after the 12th century that Western Europe again became conscious of mathematics. The revival of classical scholarship was stimulated by Latin translations from the Greek and, more especially, from the Arabic. The Latinization of Arabic versions of Euclid's great treatise, the *Elements*, first appeared in 1120. The translation was not a faithful rendering of the *Elements*, having suffered successive, inaccurate translations from the Greek—first into Arabic, then into Castilian, and finally into Latin—done by copyists not versed in the content of the work. Nevertheless, this much-used copy, with its accumulation of errors, served as the foundation of all editions known in Europe until 1505, when the Greek text was recovered.

With the fall of Constantinople to the Turks in 1453, the Byzantine scholars who had served as the major custodians of mathematics brought the ancient masterpieces of Greek learning to the West. It is reported that a copy of what survived of Diophantus's *Arithmetica* was found in the Vatican library around 1462 by Johannes Müller (better known as Regiomontanus from the Latin name of his native town, Königsberg). Presumably, it had been brought to Rome by the refugees from Byzantium. Regiomontanus observed, "In these books the very flower of the whole

Pierre de Fermat
(1601–1665)

(*David Eugene Smith Collection, Rare Book and Manuscript Library, Columbia University*)

of arithmetic lies hid," and tried to interest others in translating it. Notwithstanding the attention that was called to the work, it remained practically a closed book until 1572 when the first translation and printed edition was brought out by the German professor Wilhelm Holzmann, who wrote under the Grecian form of his name, Xylander. The *Arithmetica* became fully accessible to European mathematicians when Claude Bachet—borrowing liberally from Xylander—published (1621) the original Greek text, along with a Latin translation containing notes and comments. The Bachet edition probably has the distinction of being the work that first directed the attention of Fermat to the problems of number theory.

Few if any periods were so fruitful for mathematics as was the 17th century; Northern Europe alone produced as many men of outstanding ability as had appeared during the preceding millennium. At a time when such names as Desargues, Descartes, Pascal, Wallis, Bernoulli, Leibniz, and Newton were becoming famous, a certain French civil servant, Pierre de Fermat (1601–1665), stood as an equal among these brilliant scholars. Fermat, the "Prince of Amateurs," was the last great mathematician to pursue the subject as a sideline to a nonscientific career. By profession a lawyer and magistrate attached to the provincial parliament at Toulouse, he sought refuge from controversy in the abstraction of mathematics. Fermat evidently had no particular mathematical training and he evidenced no interest in its study until he was past 30; to him, it was merely a hobby to be cultivated in leisure time. Yet no practitioner of his day made greater discoveries or contributed more to the advancement of the discipline: one of the inventors of analytic geometry (the actual term was coined in the early 19th century), he laid the technical foundations of differential and integral calculus and, with Pascal, established the conceptual guidelines of the theory of probability. Fermat's real love in mathematics was undoubtedly number theory, which he rescued from the realm of superstition and occultism where it had long been imprisoned. His contributions here overshadow all else; it may well be said that the revival of interest in the abstract side of number theory began with Fermat.

Fermat preferred the pleasure he derived from mathematical research itself to any reputation that it might bring him; indeed, he published only one major manuscript during his lifetime and that just 5 years before his death, using the concealing initials M.P.E.A.S. Adamantly refusing to put his work in finished form, he thwarted several efforts by others to make the results available in print under his name. In partial compensation for his lack of interest in publication, Fermat carried on a voluminous correspondence with contemporary mathematicians. Most of what little we know about his investigations is found in the letters to friends with whom he exchanged problems and to whom he reported his successes. They did their best to publicize Fermat's talents by passing these letters from hand to hand or by making copies, which were dispatched over the Continent.

As his parliamentary duties demanded an ever greater portion of his time, Fermat was given to inserting notes in the margin of whatever book he happened to be using. Fermat's personal copy of the Bachet edition of Diophantus held in its margin many of his famous theorems in number theory. These were discovered by his son Samuel 5 years after Fermat's death. His son brought out a new edition of the *Arithmetica* incorporating Fermat's celebrated marginalia. Because there was little space available, Fermat's habit had been to jot down some result and omit all steps leading to the conclusion. Posterity has wished many times that the margins of the *Arithmetica* had been wider or that Fermat had been a little less secretive about his methods.

5.2 FERMAT'S LITTLE THEOREM AND PSEUDOPRIMES

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 that 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 Fermat in number theory and Frénicle's challenges had the distinction of coaxing out of Fermat some of his carefully guarded secrets. One of the most striking is the theorem that 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," or just "Fermat's Theorem," to distinguish it from Fermat's "Great" or "Last Theorem," which is the subject of Chapter 12. 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 theorem. Let p be a prime and suppose that $p \nmid a$. 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

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

then a could be canceled to give $r \equiv s \pmod{p}$, which is impossible. Therefore, the previous set of integers must be congruent modulo p to $1, 2, 3, \ldots, p-1$, 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 canceled from both sides of the preceding congruence (this is possible because since $p \nmid (p-1)!$), our line of reasoning culminates in the statement that $a^{p-1} \equiv 1 \pmod{p}$, 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 according to Fermat's theorem, we have $a^{p-1} \equiv 1 \pmod{p}$. 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 clearly is 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 we wish to make is that

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

where the rightmost congruence uses our inductive assumption. Thus, the desired conclusion holds for $a+1$ and, in consequence, for all $a \geq 0$. If a happens to be a negative integer, there is no problem: because $a \equiv r \pmod{p}$ 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. In the least, it can be a labor-saving device in certain calculations. If asked to verify that $5^{38} \equiv 4 \pmod{11}$, for instance, we 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. 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, $a = 2$. Because 2^{117} may be 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 with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.

Proof. The last corollary tells us that $(a^q)^p \equiv a^q \pmod{p}$, whereas $a^q \equiv a \pmod{p}$ holds 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, $q \mid a^{pq} - a$. Corollary 2 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 toward 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,

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

or $2^{341} \equiv 2 \pmod{341}$. After canceling a factor of 2, we pass to

$$2^{340} \equiv 1 \pmod{341}$$

so that the converse to Fermat's theorem is false.

The historical interest in numbers of the form $2^n - 2$ resides in the claim made by Chinese mathematicians over 25 centuries ago that n is prime if and only if $n \mid 2^n - 2$ (in point of fact, this criterion is reliable for all integers $n \leq 340$). Our example, where $341 \mid 2^{341} - 2$, although $341 = 11 \cdot 31$, lays the conjecture to rest; this was discovered in the year 1819. The situation in which $n \mid 2^n - 2$ occurs often enough to merit a name, though: a composite integer n is called *pseudoprime* whenever $n \mid 2^n - 2$. It can be shown that there are infinitely many pseudoprimes, the smallest four being 341, 561, 645, and 1105.

Theorem 5.2 allows us to construct an increasing sequence of pseudoprimes.

Theorem 5.2. If n is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof. Because n is a composite number, we can write $n = rs$, with $1 < r \leq s < n$. Then, according to Problem 21, Section 2.3, $2^r - 1 \mid 2^n - 1$, or equivalently $2^r - 1 \mid M_n$, making M_n composite. By our hypotheses, $2^n \equiv 2 \pmod{n}$; hence $2^n - 2 = kn$ for some integer k. It follows that

$$2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}$$

This yields

$$\begin{aligned} 2^{M_n - 1} - 1 &= 2^{kn} - 1 \\ &= (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &= M_n(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &\equiv 0 \pmod{M_n} \end{aligned}$$

We see immediately that $2^{M_n} - 2 \equiv 0 \pmod{M_n}$, in light of which M_n is a pseudoprime.

More generally, a composite integer n for which $a^n \equiv a \pmod{n}$ is called a *pseudoprime to the base a*. (When $a = 2$, n is simply said to be a pseudoprime.) For instance, 91 is the smallest pseudoprime to base 3, whereas 217 is the smallest such to base 5. It has been proved (1903) that there are infinitely many pseudoprimes to any given base.

These "prime imposters" are much rarer than are actual primes. Indeed, there are only 247 pseudoprimes smaller than one million, in comparison with 78498 primes. The first example of an even pseudoprime, namely, the number

$$161038 = 2 \cdot 73 \cdot 1103$$

was found in 1950.

There exist composite numbers n that are pseudoprimes to every base a; that is, $a^{n-1} = 1 \pmod{n}$ for all integers a with $\gcd(a, n) = 1$. The least such is 561. These exceptional numbers are called *absolute pseudoprimes* or *Carmichael numbers*, for R. D. Carmichael, who was the first to notice their existence. In his first paper on the subject, published in 1910, Carmichael indicated four absolute pseudoprimes including the well-known $561 = 3 \cdot 11 \cdot 17$. The others are $1105 = 5 \cdot 13 \cdot 17$, $2821 = 7 \cdot 13 \cdot 31$, and $15841 = 7 \cdot 31 \cdot 73$. Two years later he presented 11 more having three prime factors and discovered one absolute pseudoprime with four factors, specifically, $16046641 = 13 \cdot 37 \cdot 73 \cdot 457$.

To see that $561 = 3 \cdot 11 \cdot 17$ must be an absolute pseudoprime, notice that $\gcd(a, 561) = 1$ gives

$$\gcd(a, 3) = \gcd(a, 11) = \gcd(a, 17) = 1$$

An application of Fermat's theorem leads to the congruences

$$a^2 \equiv 1 \pmod{3} \qquad a^{10} \equiv 1 \pmod{11} \qquad a^{16} \equiv 1 \pmod{17}$$

and, in turn, to

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv (a^{16})^{35} \equiv 1 \pmod{17} \end{aligned}$$

These give rise to the single congruence $a^{560} \equiv 1 \pmod{561}$, where $\gcd(a, 561) = 1$. But then $a^{561} \equiv a \pmod{561}$ for all a, showing 561 to be an absolute pseudoprime.

Any absolute pseudoprime is square-free. This is easy to prove. Suppose that $a^n \equiv a \pmod{n}$ for every integer a, but $k^2 \mid n$ for some $k > 1$. If we let $a = k$, then $k^n \equiv k \pmod{n}$. Because $k^2 \mid n$, this last congruence holds modulo k^2; that is, $k \equiv k^n \equiv 0 \pmod{k^2}$, whence $k^2 \mid k$, which is impossible. Thus, n must be square-free.

Next we present a theorem that furnishes a means for producing absolute pseudoprimes.

Theorem 5.3. Let n be a composite square-free integer, say, $n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes. If $p_i - 1 \mid n - 1$ for $i = 1, 2, \ldots, r$, then n is an absolute pseudoprime.

Proof. Suppose that a is an integer satisfying $\gcd(a, n) = 1$, so that $\gcd(a, p_i) = 1$ for each i. Then Fermat's theorem yields $p_i \mid a^{p_i - 1} - 1$. From the divisibility hypothesis $p_i - 1 \mid n - 1$, we have $p_i \mid a^{n-1} - 1$, and therefore $p_i \mid a^n - a$ for all a and $i = 1, 2, \ldots, r$. As a result of Corollary 2 to Theorem 2.4, we end up with $n \mid a^n - a$, which makes n an absolute pseudoprime.

Examples of integers that satisfy the conditions of Theorem 5.3 are

$$1729 = 7 \cdot 13 \cdot 19 \qquad 6601 = 7 \cdot 23 \cdot 41 \qquad 10585 = 5 \cdot 29 \cdot 73$$

It was proven in 1994 that infinitely many absolute pseudoprimes exist, but that they are fairly rare. There are just 43 of them less than one million, and 105212 less than 10^{15}.

PROBLEMS 5.2

1. Use Fermat's theorem to verify that 17 divides $11^{104} + 1$.

2. (a) If $\gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$.
[*Hint:* From Fermat's theorem $a^6 \equiv 1 \pmod 7$ and $a^4 \equiv 1 \pmod 5$.]
(b) If $\gcd(a, 42) = 1$, show that $168 = 3 \cdot 7 \cdot 8$ divides $a^6 - 1$.
(c) If $\gcd(a, 133) = \gcd(b, 133) = 1$, show that $133 \mid a^{18} - b^{18}$.

3. From Fermat's theorem deduce that, for any integer $n \geq 0$, $13 \mid 11^{12n+6} + 1$.

4. Derive each of the following congruences:
(a) $a^{21} \equiv a \pmod{15}$ for all a.
[*Hint:* By Fermat's theorem, $a^5 \equiv a \pmod 5$.]
(b) $a^7 \equiv a \pmod{42}$ for all a.
(c) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ for all a.
(d) $a^9 \equiv a \pmod{30}$ for all a.

5. If $\gcd(a, 30) = 1$, show that 60 divides $a^4 + 59$.

6. (a) Find the units digit of 3^{100} by the use of Fermat's theorem.
(b) For any integer a, verify that a^5 and a have the same units digit.

7. If $7 \nmid a$, prove that either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

8. The three most recent appearances of Halley's comet were in the years 1835, 1910, and 1986; the next occurrence will be in 2061. Prove that

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod 7$$

9. (a) Let p be a prime and $\gcd(a, p) = 1$. Use Fermat's theorem to verify that $x \equiv a^{p-2}b \pmod p$ is a solution of the linear congruence $ax \equiv b \pmod p$.
(b) By applying part (a), solve the congruences $2x \equiv 1 \pmod{31}$, $6x \equiv 5 \pmod{11}$, and $3x \equiv 17 \pmod{29}$.

10. Assuming that a and b are integers not divisible by the prime p, establish the following:
(a) If $a^p \equiv b^p \pmod p$, then $a \equiv b \pmod p$.
(b) If $a^p \equiv b^p \pmod p$, then $a^p \equiv b^p \pmod{p^2}$.
[*Hint:* By (a), $a = b + pk$ for some k, so that $a^p - b^p = (b + pk)^p - b^p$; now show that p^2 divides the latter expression.]

11. Employ Fermat's theorem to prove that, if p is an odd prime, then
(a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p$.
(b) $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod p$.
[*Hint:* Recall the identity $1 + 2 + 3 + \cdots + (p - 1) = p(p - 1)/2$.]

12. Prove that if p is an odd prime and k is an integer satisfying $1 \leq k \leq p-1$, then the binomial coefficient

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

13. Assume that p and q are distinct odd primes such that $p - 1 \mid q - 1$. If $\gcd(a, pq) = 1$, show that $a^{q-1} \equiv 1 \pmod{pq}$.

14. If p and q are distinct primes, prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

15. Establish the statements below:

(a) If the number $M_p = 2^p - 1$ is composite, where p is a prime, then M_p is a pseudoprime.

(b) Every composite number $F_n = 2^{2^n} + 1$ is a pseudoprime ($n = 0, 1, 2, \ldots$).
[*Hint:* By Problem 21, Section 2.3, $2^{n+1} \mid 2^{2^n}$ implies that $2^{2^{n+1}} - 1 \mid 2^{F_n - 1} - 1$; but $F_n \mid 2^{2^{n+1}} - 1$.]

16. Confirm that the following integers are absolute pseudoprimes:

(a) $1105 = 5 \cdot 13 \cdot 17$.

(b) $2821 = 7 \cdot 13 \cdot 31$.

(c) $2465 = 5 \cdot 17 \cdot 29$.

17. Show that the smallest pseudoprime 341 is not an absolute pseudoprime by showing that $11^{341} \not\equiv 11 \pmod{341}$.
[*Hint:* $31 \nmid 11^{341} - 11$.]

18. (a) When $n = 2p$, where p is an odd prime, prove that $a^{n-1} \equiv a \pmod{n}$ for any integer a.

(b) For $n = 195 = 3 \cdot 5 \cdot 13$, verify that $a^{n-2} \equiv a \pmod{n}$ for any integer a.

19. Prove that any integer of the form

$$n = (6k+1)(12k+1)(18k+1)$$

is an absolute pseudoprime if all three factors are prime; hence, $1729 = 7 \cdot 13 \cdot 19$ is an absolute pseudoprime.

20. Show that $561 \mid 2^{561} - 2$ and $561 \mid 3^{561} - 3$. It is an unanswered question whether there exist infinitely many composite numbers n with the property that $n \mid 2^n - 2$ and $n \mid 3^n - 3$.

21. Establish the congruence

$$2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$$

[*Hint:* First evaluate 1111 modulo 7.]

5.3 WILSON'S THEOREM

We now turn to another milestone in the development of number theory. In his *Meditationes Algebraicae* of 1770, the English mathematician Edward Waring (1734–1798) announced several new theorems. Foremost among these is an interesting property of primes reported to him by one of his former students, a certain John Wilson. The property is the following: If p is a prime number, then p divides $(p-1)! + 1$. Wilson appears to have guessed this on the basis of numerical computations; at any rate, neither he nor Waring knew how to prove it. Confessing his inability to supply a demonstration, Waring added, "Theorems of this kind will be very hard to prove, because of the absence of a notation to express prime numbers." (Reading the passage, Gauss uttered his telling comment on "notationes versus notiones," implying that in questions of this nature it was the notion that really mattered, not the notation.) Despite Waring's pessimistic forecast, soon afterward Lagrange (1771) gave a proof of what in literature is called "Wilson's theorem" and observed that the converse also holds. Perhaps it would be more just to name the theorem after Leibniz, for there is evidence that he was aware of the result almost a century earlier, but published nothing on the subject.

Now we give a proof of Wilson's theorem.

Theorem 5.4 **Wilson.** If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Dismissing the cases $p = 2$ and $p = 3$ as being evident, let us take $p > 3$. Suppose that a is any one of the $p - 1$ positive integers

$$1, 2, 3, \ldots, p-1$$

and consider the linear congruence $ax \equiv 1 \pmod{p}$. Then $\gcd(a, p) = 1$. By Theorem 4.7, this congruence admits a unique solution modulo p; hence, there is a unique integer a', with $1 \le a' \le p - 1$, satisfying $aa' \equiv 1 \pmod{p}$.

Because p is prime, $a = a'$ if and only if $a = 1$ or $a = p - 1$. Indeed, the congruence $a^2 \equiv 1 \pmod{p}$ is equivalent to $(a-1)\cdot(a+1) \equiv 0 \pmod{p}$. Therefore, either $a - 1 \equiv 0 \pmod{p}$, in which case $a = 1$, or $a + 1 \equiv 0 \pmod{p}$, in which case $a = p - 1$.

If we omit the numbers 1 and $p - 1$, the effect is to group the remaining integers $2, 3, \ldots, p-2$ into pairs a, a', where $a \ne a'$, such that their product $aa' \equiv 1 \pmod{p}$. When these $(p-3)/2$ congruences are multiplied together and the factors rearranged, we get

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

or rather

$$(p-2)! \equiv 1 \pmod{p}$$

Now multiply by $p - 1$ to obtain the congruence

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

as was to be proved.

Example 5.1. A concrete example should help to clarify the proof of Wilson's theorem. Specifically, let us take $p = 13$. It is possible to divide the integers $2, 3, \ldots, 11$ into $(p-3)/2 = 5$ pairs, each product of which is congruent to 1 modulo 13. To write these congruences out explicitly:

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

Multiplying these 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, because $d \leq n-1$, 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 because 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 5.5.

Theorem 5.5. 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 $a^2 \equiv -1 \pmod{p}$. Because $p \nmid a$, 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

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

because 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 is that the integer $[(p-1)/2]!$ 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

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

and

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

Thus, the assertion that $[((p-1)/2)!]^2 + 1 \equiv 0 \pmod{p}$ 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. Currently, the largest prime of the form $n! + 1$ is $6380! + 1$, discovered in 2000.

PROBLEMS 5.3

1. (a) Find the remainder when 15! is divided by 17.
   (b) Find the remainder when 2(26!) is divided by 29.
2. Determine whether 17 is a prime by deciding whether $16! \equiv -1 \pmod{17}$.
3. Arrange the integers $2, 3, 4, \ldots, 21$ in pairs a and b that satisfy $ab \equiv 1 \pmod{23}$.
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 for any integer a,

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

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

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

9. Using Wilson's theorem, prove that for any odd prime p,

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

[*Hint:* Because $k \equiv -(p-k) \pmod{p}$, 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

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

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 5.5 to obtain two solutions to each of 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 5.5.]

13. Supply any missing details in the following proof of the irrationality of $\sqrt{2}$: Suppose $\sqrt{2} = a/b$, with $\gcd(a,b) = 1$. Then $a^2 = 2b^2$, so that $a^2 + b^2 = 3b^2$. But $3 \mid (a^2 + b^2)$ implies that $3 \mid a$ and $3 \mid b$, a contradiction.

14. Prove that the odd prime divisors of the integer $n^2 + 1$ are of the form $4k+1$.
[*Hint:* Theorem 5.5.]

15. Verify that $4(29!) + 5!$ is divisible by 31.

16. For a prime p and $0 \le k \le p-1$, show that $k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}$.

17. If p and q are distinct primes, prove that for any integer a,

$$pq \mid a^{pq} - a^p - a^q + a$$

18. Prove that if p and $p+2$ are a pair of twin primes, then

$$4((p-1)! + 1) + p \equiv 0 \pmod{p(p+2)}$$

5.4 THE FERMAT-KRAITCHIK FACTORIZATION METHOD

In a fragment of a letter, written in all probability to Father Marin Mersenne in 1643, Fermat described a technique of his for factoring large numbers. This represented the first real improvement over the classical method of attempting to find a factor of n by dividing by all primes not exceeding $\sqrt{n}$. Fermat's factorization scheme has at its heart the observation that the search for factors of an odd integer n (because powers of 2 are easily recognizable and may be removed at the outset, there is no loss in assuming that n is odd) is equivalent to obtaining integral solutions x and y of the equation

$$n = x^2 - y^2$$

If n is the difference of two squares, then it is apparent that n can be factored as

$$n = x^2 - y^2 = (x + y)(x - y)$$

Conversely, when n has the factorization $n = ab$, with $a \geq b \geq 1$, then we may write

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Moreover, because n is taken to be an odd integer, a and b are themselves odd; hence $(a + b)/2$ and $(a - b)/2$ will be nonnegative integers.

One begins the search for possible x and y satisfying the equation $n = x^2 - y^2$, or what is the same thing, the equation

$$x^2 - n = y^2$$

by first determining the smallest integer k for which $k^2 \geq n$. Now look successively at the numbers

$$k^2 - n, (k + 1)^2 - n, (k + 2)^2 - n, (k + 3)^2 - n, \ldots$$

until a value of $m \geq \sqrt{n}$ is found making $m^2 - n$ a square. The process cannot go on indefinitely, because we eventually arrive at

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

the representation of n corresponding to the trivial factorization $n = n \cdot 1$. If this point is reached without a square difference having been discovered earlier, then n has no factors other than n and 1, in which case it is a prime.

Fermat used the procedure just described to factor

$$2027651281 = 44021 \cdot 46061$$

in only 11 steps, as compared with making 4580 divisions by the odd primes up to 44021. This was probably a favorable case devised on purpose to show the chief virtue of his method: It does not require one to know all the primes less than $\sqrt{n}$ to find factors of n.

Example 5.2. To illustrate the application of Fermat's method, let us factor the integer $n = 119143$. From a table of squares, we find that $345^2 < 119143 < 346^2$; thus it suffices to consider values of $k^2 - 119143$ for those k that satisfy the inequality $346 \leq k < (119143 + 1)/2 = 59572$. The calculations begin as follows:

$$346^2 - 119143 = 119716 - 119143 = 573$$
$$347^2 - 119143 = 120409 - 119143 = 1266$$
$$348^2 - 119143 = 121104 - 119143 = 1961$$
$$349^2 - 119143 = 121801 - 119143 = 2658$$
$$350^2 - 119143 = 122500 - 119143 = 3357$$
$$351^2 - 119143 = 123201 - 119143 = 4058$$
$$352^2 - 119143 = 123904 - 119143 = 4761 = 69^2$$

This last line exhibits the factorization

$$119143 = 352^2 - 69^2 = (352 + 69)(352 - 69) = 421 \cdot 283$$

the two factors themselves being prime. In only seven trials, we have obtained the prime factorization of the number 119143. Of course, one does not always fare so luckily; it may take many steps before a difference turns out to be a square.

Fermat's method is most effective when the two factors of n are of nearly the same magnitude, for in this case a suitable square will appear quickly. To illustrate, let us suppose that $n = 23449$ is to be factored. The smallest square exceeding n is 154^2, so that the sequence $k^2 - n$ starts with

$$154^2 - 23449 = 23716 - 23449 = 267$$
$$155^2 - 23449 = 24025 - 23449 = 576 = 24^2$$

Hence, factors of 23449 are

$$23449 = (155 + 24)(155 - 24) = 179 \cdot 131$$

When examining the differences $k^2 - n$ as possible squares, many values can be immediately excluded by inspection of the final digits. We know, for instance, that a square must end in one of the six digits 0, 1, 4, 5, 6, 9 (Problem 2(a), Section 4.3). This allows us to exclude all values in Example 5.2, save for 1266, 1961, and 4761. By calculating the squares of the integers from 0 to 99 modulo 100, we see further that, for a square, the last two digits are limited to the following 22 possibilities:

00
01
04
09
16
21
24
25
29
36
41
44
49
56
61
64
69
76
81
84
89
96

The integer 1266 can be eliminated from consideration in this way. Because 61 is among the last two digits allowable in a square, it is only necessary to look at the numbers 1961 and 4761; the former is not a square, but $4761 = 69^2$.

There is a generalization of Fermat's factorization method that has been used with some success. Here, we look for distinct integers x and y such that $x^2 - y^2$ is a multiple of n rather than n itself; that is,

$$x^2 \equiv y^2 \pmod{n}$$

Having obtained such integers, $d = \gcd(x - y, n)$ (or $d = \gcd(x + y, n)$) can be calculated by means of the Euclidean Algorithm. Clearly, d is a divisor of n, but is it a nontrivial divisor? In other words, do we have $1 < d < n$?

In practice, n is usually the product of two primes p and q, with $p < q$, so that d is equal to 1, p, q, or pq. Now the congruence $x^2 \equiv y^2 \pmod{n}$ translates into $pq \mid (x - y)(x + y)$. Euclid's lemma tells us that p and q must divide one of the factors. If it happened that $p \mid x - y$ and $q \mid x - y$, then $pq \mid x - y$, or expressed as a congruence $x \equiv y \pmod{n}$. Also, $p \mid x + y$ and $q \mid x + y$ yield $x \equiv -y \pmod{n}$. By seeking integers x and y satisfying $x^2 \equiv y^2 \pmod{n}$, where $x \not\equiv \pm y \pmod{n}$, these two situations are ruled out. The result of all this is that d is either p or q, giving us a nontrivial divisor of n.

Example 5.3. Suppose we wish to factor the positive integer $n = 2189$ and happen to notice that $579^2 \equiv 18^2 \pmod{2189}$. Then we compute

$$\gcd(579 - 18, 2189) = \gcd(561, 2189) = 11$$

using the Euclidean Algorithm:

$$\begin{aligned} 2189 &= 3 \cdot 561 + 506 \\ 561 &= 1 \cdot 506 + 55 \\ 506 &= 9 \cdot 55 + 11 \\ 55 &= 5 \cdot 11 \end{aligned}$$

This leads to the prime divisor 11 of 2189. The other factor, namely 199, can be obtained by observing that

$$\gcd(579 + 18, 2189) = \gcd(597, 2189) = 199$$

The reader might wonder how we ever arrived at a number, such as 579, whose square modulo 2189 also turns out to be a perfect square. In looking for squares close to multiples of 2189, it was observed that

$$81^2 - 3 \cdot 2189 = -6 \qquad \text{and} \qquad 155^2 - 11 \cdot 2189 = -54$$

which translates into

$$81^2 \equiv -2 \cdot 3 \pmod{2189} \qquad \text{and} \qquad 155^2 \equiv -2 \cdot 3^3 \pmod{2189}$$

When these congruences are multiplied, they produce

$$(81 \cdot 155)^2 \equiv (2 \cdot 3^2)^2 \pmod{2189}$$

Because the product $81 \cdot 155 = 12555 \equiv -579 \pmod{2189}$, we ended up with the congruence $579^2 \equiv 18^2 \pmod{2189}$.

The basis of our approach is to find several x_i having the property that each x_i^2 is, modulo n, the product of small prime powers, and such that their product's square is congruent to a perfect square.

When n has more than two prime factors, our factorization algorithm may still be applied; however, there is no guarantee that a particular solution of the congruence $x^2 \equiv y^2 \pmod{n}$, with $x \not\equiv \pm y \pmod{n}$, will result in a nontrivial divisor of n. Of course the more solutions of this congruence that are available, the better the chance of finding the desired factors of n.

Our next example provides a considerably more efficient variant of this last factorization method. It was introduced by Maurice Kraitchik in the 1920s and became the basis of such modern methods as the quadratic sieve algorithm.

Example 5.4. Let $n = 12499$ be the integer to be factored. The first square just larger than n is $112^2 = 12544$. So we begin by considering the sequence of numbers $x^2 - n$

for $x = 112, 113, \ldots$. As before, our interest is in obtaining a set of values x_1, $x_2, \ldots, x_k$ for which the product $(x_i - n)\cdots(x_k - n)$ is a square, say y^2. Then $(x_1 \cdots x_k)^2 \equiv y^2 \pmod{n}$, which might lead to a nontrivial factor of n.

A short search reveals that

$$112^2 - 12499 = 45$$

$$117^2 - 12499 = 1190$$

$$121^2 - 12499 = 2142$$

or, written as congruences,

$$112^2 \equiv 3^2 \cdot 5 \pmod{12499}$$

$$117^2 \equiv 2 \cdot 5 \cdot 7 \cdot 17 \pmod{12499}$$

$$121^2 \equiv 2 \cdot 3^2 \cdot 7 \cdot 17 \pmod{12499}$$

Multiplying these together results in the congruence

$$(112 \cdot 117 \cdot 121)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17)^2 \pmod{12499}$$

that is,

$$1585584^2 \equiv 10710^2 \pmod{12499}$$

But we are unlucky with this square combination. Because

$$1585584 \equiv 10710 \pmod{12499}$$

only a trivial divisor of 12499 will be found. To be specific,

$$\gcd(1585584 + 10710, 12499) = 1$$

$$\gcd(1585584 - 10710, 12499) = 12499$$

After further calculation, we notice that

$$113^2 \equiv 2 \cdot 5 \cdot 3^3 \pmod{12499}$$

$$127^2 \equiv 2 \cdot 3 \cdot 5 \cdot 11^2 \pmod{12499}$$

which gives rise to the congruence

$$(113 \cdot 127)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 11)^2 \pmod{12499}$$

This reduces modulo 12499 to

$$1852^2 \equiv 990^2 \pmod{12499}$$

and fortunately $1852 \not\equiv \pm\, 990 \pmod{12499}$. Calculating

$$\gcd(1852 - 990, 12499) = \gcd(862, 12499) = 431$$

produces the factorization $12499 = 29 \cdot 431$.

PROBLEMS 5.4

1. Use Fermat's method to factor each of the following numbers:
(a) 2279.
(b) 10541.
(c) 340663 [*Hint:* The smallest square just exceeding 340663 is 584^2.]

2. Prove that a perfect square must end in one of the following pairs of digits: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96.
[*Hint:* Because $x^2 \equiv (50 + x)^2 \pmod{100}$ 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

$$n = \frac{(ac + bd)(ac - bd)}{(a + d)(a - d)}$$

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. Employ the generalized Fermat method to factor each of the following numbers:
(a) 2911 [*Hint:* $138^2 \equiv 67^2 \pmod{2911}$.]
(b) 4573 [*Hint:* $177^2 \equiv 92^2 \pmod{4573}$.]
(c) 6923 [*Hint:* $208^2 \equiv 93^2 \pmod{6923}$.]

6. Factor 13561 with the help of the congruences

$$233^2 \equiv 3^2 \cdot 5 \pmod{13561} \qquad \text{and} \qquad 1281^2 \equiv 2^4 \cdot 5 \pmod{13561}$$

7. (a) Factor the number 4537 by searching for x such that

$$x^2 - k \cdot 4537$$

is the product of small prime powers.
(b) Use the procedure indicated in part (a) to factor 14429.
[*Hint:* $120^2 - 14429 = -29$ and $3003^2 - 625 \cdot 14429 = -116$.]

8. Use Kraitchik's method to factor the number 20437.