or $2^{341} \equiv 2 \pmod{341}$. After cancelling 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 the 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 $n \leq 340$). Needless to say, 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: call a composite integer n *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.

PROBLEMS 5.3

1. Verify that $18^6 \equiv 1 \pmod{7^k}$ for $k = 1, 2, 3$.

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. Prove that there exist infinitely many composite numbers n for which $a^{n-1} \equiv a \pmod{n}$. [*Hint:* Take $n = 2p$, where p is an odd prime.]

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.

5. For any integer a, show that a^5 and a have the same units digit.

6. Find the units digit of 3^{100} by the use of Fermat's Theorem. [*Hint:* Write $3^{100} = 3(3^9)^{11}$.]

7. Prove that for any positive integer n, the following congruences hold:

(a) $2^{2n} \equiv 1 \pmod{3}$.

(b) $2^{3n} \equiv 1 \pmod{7}$.

(c) $2^{4n} \equiv 1 \pmod{15}$.

8. (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 linear congruences $2x \equiv 1 \pmod{31}$, $6x \equiv 5 \pmod{11}$, and $3x \equiv 17 \pmod{29}$.

9. 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.]

10. 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 $1 + 2 + 3 + \cdots + (p-1) = p(p-1)/2$.]

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

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

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

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

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

14. Confirm that the integers $1729 = 7 \cdot 13 \cdot 19$ and $1905 = 3 \cdot 5 \cdot 127$ are both pseudoprimes.

15. 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 $n \mid 3^n - 3$.

5.4 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 (1741–1793) 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, Lagrange soon afterwards (1771) gave a proof of what in the literature is called "Wilson's Theorem" and observed that the converse also holds. It would be perhaps 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 upon the subject.

Now to a proof of Wilson's Theorem.

THEOREM 5-2 (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 $1 \leq a' \leq p - 1$, satisfying $aa' \equiv 1 \pmod{p}$.

Since 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 $a \neq a'$, such that $aa' \equiv 1 \pmod{p}$. 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.

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