This proof can best be illustrated by carrying it out with some specific numbers. Let $n = 9$, for instance. The positive integers less than and relatively prime to 9 are

$$1, 2, 4, 5, 7, 8.$$

These play the role of the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in the proof of Theorem 7-5. If $a = -4$, then the integers aa_i are

$$-4, -8, -16, -20, -28, -32,$$

where, modulo 9,

$$-4 \equiv 5, \ -8 \equiv 1, \ -16 \equiv 2, \ -20 \equiv 7, \ -28 \equiv 8, \ -32 \equiv 4.$$

When the above congruences are all multiplied together, we obtain

$$(-4)(-8)(-16)(-20)(-28)(-32) \equiv 5 \cdot 1 \cdot 2 \cdot 7 \cdot 8 \cdot 4 \pmod 9,$$

which becomes

$$(1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8)(-4)^6 \equiv (1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8) \pmod 9.$$

Being relatively prime to 9, the six integers 1, 2, 4, 5, 7, 8 may be successively cancelled to give

$$(-4)^6 \equiv 1 \pmod 9.$$

The validity of this last congruence is confirmed by the calculation

$$(-4)^6 \equiv 4^6 \equiv (64)^2 \equiv 1^2 \equiv 1 \pmod 9.$$

Note that Theorem 7-5 does indeed generalize the one due to Fermat, which we proved earlier. For if p is a prime, then $\phi(p) = p - 1$; hence, whenever $\gcd(a, p) = 1$, we get

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

and so:

Corollary (Fermat). *If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$.*

Example 7-2

Euler's Theorem is helpful in reducing large powers modulo n. To cite a typical example, let us find the last two digits in the decimal representation of 3^{256}; this is equivalent to obtaining the smallest nonnegative integer to which 3^{256} is congruent modulo 100. Since $\gcd(3,100) = 1$ and

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100(1 - \tfrac{1}{2})(1 - \tfrac{1}{5}) = 40,$$

Euler's Theorem yields

$$3^{40} \equiv 1 \pmod{100}.$$

By the Division Algorithm, $256 = 6 \cdot 40 + 16$; whence

$$3^{256} \equiv 3^{6 \cdot 40 + 16} \equiv (3^{40})^6 3^{16} \equiv 3^{16} \pmod{100}$$

and our problem reduces to one of evaluating 3^{16}, modulo 100. The calculations are as follows, with reasons omitted:

$$3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2 \equiv 61^2 \equiv 21 \pmod{100}.$$

There is another path to Euler's Theorem, one which requires the use of Fermat's Theorem.

Second Proof of Euler's Theorem: To start, we argue by induction that if $p \nmid a$ (p a prime), then

(1) $$a^{\phi(p^k)} \equiv 1 \pmod{p^k}, \qquad k > 0.$$

When $k = 1$, this assertion reduces to the statement of Fermat's Theorem. Assuming the truth of (1) for a fixed value of k, we wish to show that it is true with k replaced by $k + 1$.

Since (1) is assumed to hold, we may write

$$a^{\phi(p^k)} = 1 + qp^k$$

for some integer q. Notice too that

$$\phi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p\phi(p^k).$$

Using these facts, along with the Binomial Theorem, we obtain

$$\begin{aligned} a^{\phi(p^{k+1})} &= a^{p\phi(p^k)} \\ &= (1 + qp^k)^p \\ &= 1 + \binom{p}{1}(qp^k) + \binom{p}{2}(qp^k)^2 + \cdots + \binom{p}{p-1}(qp^k)^{p-1} + (qp^k)^p \\ &\equiv 1 + \binom{p}{1}(qp^k) \pmod{p^{k+1}}. \end{aligned}$$

But $p \mid \binom{p}{1}$ and so $p^{k+1} \mid \binom{p}{1}(qp^k)$. Thus, the last-written congruence becomes

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

completing the induction step.

Now let $\gcd(a, n) = 1$ and n have the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. In view of what has already been proved, each of the congruences

$$a^{\phi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}, \qquad i = 1, 2, \ldots, r \tag{2}$$

holds. Noting that $\phi(n)$ is divisible by $\phi(p_i^{k_i})$, we may raise both sides of (2) to the power $\phi(n)/\phi(p_i^{k_i})$ and arrive at

$$a^{\phi(n)} \equiv 1 \pmod{p_i^{k_i}}, \qquad i = 1, 2, \ldots, r.$$

Inasmuch as the moduli are relatively prime, this leads us to the relation

$$a^{\phi(n)} \equiv 1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}$$

or $a^{\phi(n)} \equiv 1 \pmod{n}$.

The usefulness of Euler's Theorem in number theory would be hard to exaggerate. It leads, for instance, to a different proof of the Chinese Remainder Theorem. In other words, we seek to establish that if $\gcd(n_i, n_j) = 1$ for $i \neq j$, then the system of linear congruences

$$x \equiv a_i \pmod{n_i}, \qquad i = 1, 2, \ldots, r$$

admits a simultaneous solution. Let $n = n_1 n_2 \cdots n_r$ and put $N_i = n/n_i$ for $i = 1, 2, \ldots, r$. Then the integer

$$x = a_1 N_1^{\phi(n_1)} + a_2 N_2^{\phi(n_2)} + \cdots + a_r N_r^{\phi(n_r)}$$

fulfills our requirements. To see this, first note that $N_j \equiv 0 \pmod{n_i}$ whenever $i \neq j$; whence,

$$x \equiv a_i N_i^{\phi(n_i)} \pmod{n_i}.$$

But, since $\gcd(N_i, n_i) = 1$, we have

$$N_i^{\phi(n_i)} \equiv 1 \pmod{n_i}$$

and so $x \equiv a_i \pmod{n_i}$ for each i.

As a second application of Euler's Theorem, let us show that if n is an odd integer which is not a multiple of 5, then n divides an integer all of whose digits are equal to 1. (For example: $7 \mid 111111$.) Since $\gcd(n, 10) = 1$ and $\gcd(9, 10) = 1$, we have $\gcd(9n, 10) = 1$ Quoting Theorem 7-5 again,

$$10^{\phi(9n)} \equiv 1 \pmod{9n}.$$

This says that $10^{\phi(9n)} - 1 = 9nk$ for some integer k or, what amounts to the same thing,

$$kn = \frac{10^{\phi(9n)} - 1}{9}.$$

The right-hand side of the above expression is an integer whose digits are all equal to 1, each digit of the numerator being clearly equal to 9.

PROBLEMS 7.3

1. Use Euler's Theorem to establish the following:
   (a) For any integer a, $a^{37} \equiv a \pmod{1729}$. [*Hint:* $1729 = 7 \cdot 13 \cdot 19$.]
   (b) For any integer a, $a^{13} \equiv a \pmod{2730}$. [*Hint:* $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.]
   (c) For any odd integer a, $a^{33} \equiv a \pmod{4080}$. [*Hint:* $4080 = 15 \cdot 16 \cdot 17$.]
2. Show that if $\gcd(a, n) = \gcd(a - 1, n) = 1$, then

$$1 + a + a^2 + \cdots + a^{\phi(n) - 1} \equiv 0 \pmod{n}.$$

   [*Hint:* Recall that $a^{\phi(n)} - 1 = (a - 1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1)$.]
3. If m and n are relatively prime positive integers, prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

4. Fill in any missing details in the following proof of Euler's Theorem: Let p be a prime divisor of n and $\gcd(a, p) = 1$. By Fermat's Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so that $a^{p-1} = 1 + tp$ for some t. Then $a^{p(p-1)} = (1 + tp)^p = 1 + \binom{p}{1}(tp) + \cdots + (tp)^p \equiv 1 \pmod{p^2}$ and, by induction, $a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$ where $k = 1, 2, \ldots$. Raise both sides of this congruence to the $\phi(n)/p^{k-1}(p - 1)$ power to get $a^{\phi(n)} \equiv 1 \pmod{p^k}$. Thus $a^{\phi(n)} \equiv 1 \pmod{n}$.
5. Find the units digit of 3^{100} by means of Euler's Theorem.
6. (a) If $\gcd(a, n) = 1$, show that the linear congruence $ax \equiv b \pmod{n}$ has the solution $x \equiv ba^{\phi(n)-1} \pmod{n}$.
   (b) Use part (a) to solve the congruences $3x \equiv 5 \pmod{26}$, $13x \equiv 2 \pmod{40}$ and $10x \equiv 21 \pmod{49}$.
7. Prove that every prime other than 2 or 5 divides infinitely many of the integers, 1, 11, 111, 1111, ...