$$b^{p-1} = 1 \in \mathbb{Z}_p.$$

The rings $\mathbb{Z}_p$ and $\mathbb{Z}/p\mathbb{Z}$ are isomorphic where the element $b \in \mathbb{Z}_p$ corresponds to the coset $b + p\mathbb{Z}$. For any integer a that is not a multiple of p, $a + p\mathbb{Z} = b + p\mathbb{Z}$ for some $0 \leq b \leq p - 1$. Thus

$$(a + p\mathbb{Z})^{p-1} = (b + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}.$$

In other words,

$$a^{p-1} \equiv 1 \pmod{p}.$$ ◆

24.2 Corollary If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any prime p.

Proof The corollary follows from Theorem 24.1 if $a \not\equiv 0 \pmod{p}$. If $a \equiv 0 \pmod{p}$, then both sides reduce to 0 modulo p. ◆

24.3 Example Let us compute the remainder of 8^{103} when divided by 13. Using Fermat's theorem, we have

$$\begin{aligned} 8^{103} &\equiv (8^{12})^8(8^7) \equiv (1^8)(8^7) \equiv 8^7 \equiv (-5)^7 \\ &\equiv (25)^3(-5) \equiv (-1)^3(-5) \equiv 5 \pmod{13}. \end{aligned}$$ ▲

■ HISTORICAL NOTE

The statement of Theorem 24.1 occurs in a letter from Pierre de Fermat (1601–1665) to Bernard Frenicle de Bessy, dated 18 October 1640. Fermat's version of the theorem was that for any prime p and any geometric progression $a, a^2, \cdots, a^t, \cdots$, there is a least number a^T of the progression such that p divides $a^T - 1$. Furthermore, T divides $p - 1$ and p also divides all numbers of the form $a^{KT} - 1$. (It is curious that Fermat failed to note the condition that p not divide a; perhaps he felt that it was obvious that the result fails in that case.)

Fermat did not in the letter or elsewhere indicate a proof of the result and, in fact, never mentioned it again. But we can infer from other parts of this correspondence that Fermat's interest in this result came from his study of perfect numbers. (A perfect number is a positive integer m that is the sum of all of its divisors less than m; for example, $6 = 1 + 2 + 3$ is a perfect number.) Euclid had shown that $2^{n-1}(2^n - 1)$ is perfect if $2^n - 1$ is prime. The question then was to find methods for determining whether $2^n - 1$ was prime. Fermat noted that $2^n - 1$ was composite if n is composite, and then derived from his theorem the result that if n is prime, the only possible divisors of $2^n - 1$ are those of the form $2kn + 1$. From this result he was able quickly to show, for example, that $2^{37} - 1$ was divisible by $223 = 2 \cdot 3 \cdot 37 + 1$.

24.4 Example Show that $2^{11,213} - 1$ is not divisible by 11.

Solution By Fermat's theorem, $2^{10} \equiv 1 \pmod{11}$, so

$$\begin{aligned} 2^{11,213} - 1 &\equiv [(2^{10})^{1,121} \cdot 2^3] - 1 \equiv [1^{1,121} \cdot 2^3] - 1 \\ &\equiv 2^3 - 1 \equiv 8 - 1 \equiv 7 \pmod{11}. \end{aligned}$$

Thus the remainder of $2^{11,213} - 1$ when divided by 11 is 7, not 0. (The number 11,213 is prime, and it has been shown that $2^{11,213} - 1$ is a prime number. Primes of the form $2^p - 1$ where p is prime are known as **Mersenne primes.**) ▲

24.5 Example Show that for every integer n, the number $n^{33} - n$ is divisible by 15.

Solution This seems like an incredible result. It means that 15 divides $2^{33} - 2, 3^{33} - 3, 4^{33} - 4$, etc.

Now $15 = 3 \cdot 5$, and we shall use Fermat's theorem to show that $n^{33} - n$ is divisible by both 3 and 5 for every n. Note that $n^{33} - n = n(n^{32} - 1)$.

If 3 divides n, then surely 3 divides $n(n^{32} - 1)$. If 3 does not divide n, then by Fermat's theorem, $n^2 \equiv 1 \pmod 3$ so

$$n^{32} - 1 \equiv (n^2)^{16} - 1 \equiv 1^{16} - 1 \equiv 0 \pmod 3,$$

and hence 3 divides $n^{32} - 1$.

If $n \equiv 0 \pmod 5$, then $n^{33} - n \equiv 0 \pmod 5$. If $n \not\equiv 0 \pmod 5$, then by Fermat's theorem, $n^4 \equiv 1 \pmod 5$, so

$$n^{32} - 1 \equiv (n^4)^8 - 1 \equiv 1^8 - 1 \equiv 0 \pmod 5.$$

Thus $n^{33} - n \equiv 0 \pmod 5$ for every n also. ▲

Euler's Generalization

Theorem 23.3 classifies all the elements in $\mathbb{Z}_n$ into three categories. An element k in $\mathbb{Z}_n$ is either 0, a unit if the $\gcd(n, k) = 1$, or else a divisor of 0 if $\gcd(n, k) > 1$. Exercise 39 in Section 22 shows that the units in a ring form a group under multiplication. Therefore, the set of nonzero elements in $\mathbb{Z}_n$, which are relatively prime to n, form a multiplicative group. Euler's generalization of Fermat's theorem is based on the number of units in $\mathbb{Z}_n$.

Let n be a positive integer. Let $\varphi(n)$ be defined as the number of positive integers less than or equal to n and relatively prime to n. Note that $\varphi(1) = 1$.

24.6 Example Let $n = 12$. The positive integers less than or equal to 12 and relatively prime to 12 are 1, 5, 7, and 11, so $\varphi(12) = 4$. ▲

By Theorem 23.3, $\varphi(n)$ is the number of nonzero elements of $\mathbb{Z}_n$ that are not divisors of 0. This function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is the **Euler phi-function.** We can now describe Euler's generalization of Fermat's theorem.

24.7 Theorem **(Euler's Theorem)** If a is an integer relatively prime to n, then $a^{\varphi(n)} - 1$ is divisible by n, that is, $a^{\varphi(n)} \equiv 1 \pmod n$.

Proof If a is relatively prime to n, then the coset $a + n\mathbb{Z}$ of $n\mathbb{Z}$ containing a contains an integer $b < n$ and relatively prime to n. Using the fact that multiplication of these cosets by multiplication modulo n of representatives is well-defined, we have

$$a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod n.$$

But by Theorem 23.3, b can be viewed as an element of the multiplicative group G_n of order $\varphi(n)$ consisting of the $\varphi(n)$ elements of $\mathbb{Z}_n$ relatively prime to n. Thus

$$b^{\varphi(n)} \equiv 1 \pmod n,$$

and our theorem follows. ◆

24.8 Example Let $n = 12$. We saw in Example 24.6 that $\varphi(12) = 4$. Thus if we take any integer a relatively prime to 12, then $a^4 \equiv 1 \pmod{12}$. For example, with $a = 7$, we have $7^4 = (49)^2 = 2,401 = 12(200) + 1$, so $7^4 \equiv 1 \pmod{12}$. Of course, the easy way to compute $7^4 \pmod{12}$, without using Euler's theorem, is to compute it in $\mathbb{Z}_{12}$. In $\mathbb{Z}_{12}$, we have $7 = -5$ so

$$7^2 = (-5)^2 = (5)^2 = 1 \qquad \text{and} \qquad 7^4 = 1^2 = 1.$$ ▲

Application to $ax \equiv b \pmod{m}$

We can find all solutions of a linear congruence $ax \equiv b \pmod{m}$. We prefer to work with an equation in $\mathbb{Z}_m$ and interpret the results for congruences.

24.9 Theorem Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in $\mathbb{Z}_m$.

Proof By Theorem 23.3, a is a unit in $\mathbb{Z}_m$ and $s = a^{-1}b$ is certainly a solution of the equation. Multiplying both sides of $ax = b$ on the left by a^{-1}, we see this is the only solution. ◆

Interpreting this theorem for congruences, we obtain at once the following corollary.

24.10 Corollary If a and m are relatively prime integers, then for any integer b, the congruence $ax \equiv b \pmod{m}$ has as solutions all integers in precisely one residue class modulo m. ⧫

Theorem 24.9 serves as a lemma for the general case.

24.11 Theorem Let m be a positive integer and let $a, b \in \mathbb{Z}_m$. Let d be the gcd of a and m. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$.

Proof First we show there is no solution of $ax = b$ in $\mathbb{Z}_m$ unless d divides b. Suppose $s \in \mathbb{Z}_m$ is a solution. Then $as - b = qm$ in $\mathbb{Z}$, so $b = as - qm$. Since d divides both a and m, we see that d divides the right-hand side of the equation $b = as - qm$, and hence divides b. Thus a solution s can exist only if d divides b.

Suppose now that d does divide b. Let

$$a = a_1 d, \quad b = b_1 d, \quad \text{and} \quad m = m_1 d.$$

Then the equation $as - b = qm$ in $\mathbb{Z}$ can be rewritten as $d(a_1 s - b_1) = dqm_1$. We see that $as - b$ is a multiple of m if and only if $a_1 s - b_1$ is a multiple of m_1. Thus the solutions s of $ax = b$ in $\mathbb{Z}_m$ are precisely the elements that, read modulo m_1, yield solutions of $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$. Now let $s \in \mathbb{Z}_{m_1}$ be the unique solution of $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$ given by Theorem 24.9. The numbers in $\mathbb{Z}_m$ that reduce to s modulo m_1 are precisely those that can be computed in $\mathbb{Z}_m$ as

$$s, s + m_1, s + 2m_1, s + 3m_1, \cdots, s + (d-1)m_1.$$

Thus there are exactly d solutions of the equation in $\mathbb{Z}_m$. ◆

Theorem 24.11 gives us at once this classical result on the solutions of a linear congruence.

24.12 Corollary Let d be the gcd of positive integers a and m. The congruence $ax \equiv b \pmod{m}$ has a solution if and only if d divides b. When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m. ⧫

Actually, our proof of Theorem 24.11 shows a bit more about the solutions of $ax \equiv b \pmod{m}$ than we stated in this corollary; namely, it shows that if any solution s is found, then the solutions are precisely all elements of the residue classes $(s + km_1) + (m\mathbb{Z})$ where $m_1 = m/d$ and k runs through the integers from 0 to $d - 1$. It also tells us that we can find such an s by finding $a_1 = a/d$ and $b_1 = b/d$, and solving $a_1 x \equiv b_1 \pmod{m_1}$. To solve this congruence, we may consider a_1 and b_1 to be replaced by their remainders modulo m_1 and solve the equation $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$.