solutions. This last congruence can possess no more than d solutions (Lagrange's Theorem enters again), hence has exactly d solutions.

We take immediate advantage of this corollary to prove Wilson's Theorem in a different way: given a prime p, define the polynomial $f(x)$ by

$$\begin{aligned} f(x) &= (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1) \\ &= a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_1 x + a_0, \end{aligned}$$

which is of degree $p-2$. Fermat's Theorem implies that the $p-1$ integers $1, 2, \ldots, p-1$ are incongruent solutions of the congruence

$$f(x) \equiv 0 \pmod{p}.$$

But this contradicts Lagrange's Theorem, unless

$$a_{p-2} \equiv a_{p-3} \equiv \cdots \equiv a_1 \equiv a_0 \equiv 0 \pmod{p}.$$

It follows that, for any choice of the integer x,

$$(x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod{p}.$$

Now substitute $x = 0$ to obtain

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

or $(-1)^{p-1}(p-1)! + 1 \equiv 0 \pmod{p}$. Either $p-1$ is even or else $p = 2$, in which case $-1 \equiv 1 \pmod{p}$; at any rate, we get

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

Lagrange's Theorem has provided us with the entering wedge. We are now in a position to prove that, for any prime p, there exist integers with order corresponding to each divisor of $p-1$. Stated more precisely:

THEOREM 8-6. *If p is a prime number and $d \mid p-1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p.*

Proof: Let $d \mid p-1$ and let $\psi(d)$ denote the number of integers k, $1 \leq k \leq p-1$, which have order d modulo p. Since each integer between 1 and $p-1$ has order d for some $d \mid p-1$,

$$p - 1 = \sum_{d \mid p-1} \psi(d).$$

At the same time, Gauss' Theorem tells us that

$$p-1=\sum_{d\mid p-1}\phi(d)$$

and so, putting these together,

$$\sum_{d\mid p-1}\psi(d)=\sum_{d\mid p-1}\phi(d). \tag{1}$$

Our aim is to show that $\psi(d)\leq\phi(d)$ for each divisor d of $p-1$, since this, in conjunction with equation (1), would produce the equality $\psi(d)=\phi(d)\neq 0$ (otherwise, the first sum would be strictly smaller than the second).

Given an arbitrary divisor d of $p-1$, there are two possibilities: either $\psi(d)=0$ or $\psi(d)>0$. If $\psi(d)=0$, then certainly $\psi(d)\leq\phi(d)$. Suppose that $\psi(d)>0$, so that there exists an integer a of order d. Then the d integers $a, a^2, \ldots, a^d$ are incongruent modulo p and each of them satisfies the polynomial congruence

$$x^d-1\equiv 0 \pmod{p}; \tag{2}$$

for, $(a^k)^d\equiv(a^d)^k\equiv 1 \pmod{p}$. By the corollary to Lagrange's Theorem, there can be no other solutions of (2). It follows that any integer which has order d modulo p must be congruent to one of $a, a^2, \ldots, a^d$. But only $\phi(d)$ of the just-mentioned powers have order d, namely those a^k for which the exponent k has the property $\gcd(k, d)=1$. Hence, in the present situation, $\psi(d)=\phi(d)$, and the number of integers having order d modulo p is equal to $\phi(d)$. This establishes the result we set out to prove.

Taking $d=p-1$ in Theorem 8-6, we arrive at

COROLLARY. *If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots of p.*

An illustration is afforded by the prime $p=13$. For this modulus, 1 has order 1; 12 has order 2; 3 and 9 have order 3; 5 and 8 have order 4; 4 and 10 have order 6; and four integers, namely 2, 6, 7, 11, have order 12. Thus,

$$\begin{aligned}\sum_{d\mid 12}\psi(d)&=\psi(1)+\psi(2)+\psi(3)+\psi(4)+\psi(6)+\psi(12)\\&=1+1+2+2+2+4=12\end{aligned}$$

as it should. Notice too that

$$\begin{aligned} \psi(1) &= 1 = \phi(1), & \psi(4) &= 2 = \phi(4) \\ \psi(2) &= 1 = \phi(2), & \psi(6) &= 2 = \phi(6) \\ \psi(3) &= 2 = \phi(3), & \psi(12) &= 4 = \phi(12) \end{aligned}$$

Incidentally, there is a shorter and more elegant way of proving that $\psi(d) = \phi(d)$ for each $d \mid p-1$. We simply subject the formula $d = \sum_{c \mid d} \psi(c)$ to Möbius inversion to deduce that

$$\psi(d) = \sum_{c \mid d} \mu(c)(d/c).$$

In light of Theorem 7-8, the right-hand side of the foregoing equation is equal to $\phi(d)$. Of course, the validity of this argument rests upon knowing that ψ is a multiplicative function.

We can use this last theorem to give another proof of the fact that if p is a prime of the form $4k+1$, then the quadratic congruence $x^2 \equiv -1 \pmod{p}$ admits a solution. Since $4 \mid p-1$, Theorem 8-6 tells us that there is an integer a having order 4 modulo p; in other words,

$$a^4 \equiv 1 \pmod{p}$$

or equivalently,

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

Because p is a prime, it follows that either

$$a^2 - 1 \equiv 0 \pmod{p} \quad \text{or} \quad a^2 + 1 \equiv 0 \pmod{p}.$$

If the first congruence held, then a would have order less than or equal to 2, a contradiction. Hence, $a^2 + 1 \equiv 0 \pmod{p}$, making the integer a a solution to the congruence $x^2 \equiv -1 \pmod{p}$.

Theorem 8-6, as proved, has an obvious drawback; while it does indeed imply the existence of primitive roots for a given prime p, the proof is nonconstructive. To find a primitive root, one must usually proceed by brute force or else fall back on the extensive tables that have been constructed. The accompanying table lists the smallest positive primitive root for each prime below 200.

Prime	*Least positive primitive root*	*Prime*	*Least positive primitive root*
2	1	89	3
3	2	97	5
5	2	101	2
7	3	103	5
11	2	107	2
13	2	109	6
17	3	113	3
19	2	127	3
23	5	131	2
29	2	137	3
31	3	139	2
37	2	149	2
41	6	151	6
43	3	157	5
47	5	163	2
53	2	167	5
59	2	173	2
61	2	179	2
67	2	181	2
71	7	191	19
73	5	193	5
79	3	197	2
83	2	199	3

If $\chi(p)$ designates the smallest positive primitive root of the prime p, then the table presented above shows that $\chi(p) \leq 19$ for all $p < 200$. In fact, $\chi(p)$ becomes arbitrarily large as p increases without bound. The table suggests, although the answer is not yet known, that there exist an infinite number of primes p for which $\chi(p) = 2$.

In his *Disquisitiones Arithmeticae*, Gauss conjectured that there are infinitely many primes having 10 as a primitive root. In 1927 Emil Artin generalized this unresolved question as: For a not equal to 1, -1, or a perfect square, do there exist infinitely many primes having a as a primitive root?

The restrictions in Artin's conjecture are justified as follows. Let a be a perfect square, say $a = x^2$, and let p be an odd prime with