possibilities: *no* element has order d, or exactly $\varphi(d)$ elements have order d.

Now every element has some order $d|(q-1)$. And there are either 0 or $\varphi(d)$ elements of order d. But, by Proposition I.3.7, $\sum_{d|(q-1)} \varphi(d) = q-1$, which is the number of elements in $\mathbf{F}_q^*$. Thus, the only way that every element can have some order $d|(q-1)$ is if there are always $\varphi(d)$ (and never 0) elements of order d. In particular, there are $\varphi(q-1)$ elements of order $q-1$; and, as we saw in the previous paragraph, if g is any element of order $q-1$, then the other elements of order $q-1$ are precisely the powers g^j for which $g.c.d.(j,\ q-1) = 1$. This completes the proof.

Corollary. *For every prime p, there exists an integer g such that the powers of g exhaust all nonzero residue classes modulo p.*

Example 1. We can get all residues *mod* 19 from 1 to 18 by taking powers of 2. Namely, the successive powers of 2 reduced *mod* 19 are: 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1.

In many situations when working with finite fields, such as $\mathbf{F}_p$ for some prime p, it is useful to find a generator. What if a number $g \in \mathbf{F}_p^*$ is chosen at random? What is the probability that it will be a generator? In other words, what proportion of all of the nonzero elements consists of generators? According to Proposition II.1.2, the proportion is $\varphi(p-1)/(p-1)$. But by our formula for $\varphi(n)$ following the corollary of Proposition I.3.3, this fraction is equal to the $\prod(1-\frac{1}{\ell})$, where the product is over all primes ℓ dividing $p-1$. Thus, the odds of getting a generator by a random guess depend heavily on the factorization of $p-1$. For example, we can prove:

Proposition II.1.3. *There exists a sequence of primes p such that the probability that a random $g \in \mathbf{F}_p^*$ is a generator approaches zero.*

Proof. Let $\{n_j\}$ be any sequence of positive integers which is divisible by more and more of the successive primes 2, 3, 5, 7,... as $j \longrightarrow \infty$. For example, we could take $n_j = j!$. Choose p_j to be any prime such that $p_j \equiv 1 \bmod n_j$. How do we know that such a prime exists? That follows from *Dirichlet's theorem on primes in an arithmetic progression*, which states: *If n and k are relatively prime, then there are infinitely many primes which are $\equiv k \bmod n$.* (In fact, more is true: the primes are "evenly distributed" among the different possible $k \bmod n$, i.e., the proportion of primes $\equiv k \bmod n$ is $1/\varphi(n)$; but we don't need that fact here.) Then the primes dividing $p_j - 1$ include all of the primes dividing n_j, and so $\frac{\varphi(p_j-1)}{p_j-1} \leq \prod_{\text{primes } \ell|n_j}(1-\frac{1}{\ell})$. But as $j \longrightarrow \infty$ this product approaches $\prod_{\text{all primes } \ell}(1-\frac{1}{\ell})$, which is zero (see Exercise 23 of § I.3). This proves the proposition.

Existence and uniqueness of finite fields with prime power number of elements. We prove both existence and uniqueness by showing that a finite field of $q = p^f$ elements is the splitting field of the polynomial $X^q - X$. The following proposition shows that for every prime power q there is one and (up to isomorphism) only one finite field with q elements.

Proposition II.1.4. *If $\mathbf{F}_q$ is a field of $q = p^f$ elements, then every element satisfies the equation $X^q - X = 0$, and $\mathbf{F}_q$ is precisely the set*