$a^{j-i} = 1$.) Let $S = \{1, a, a^2, \ldots, a^{d-1}\}$ denote the set of all powers of a, and for any $b \in \mathbf{F}_q^*$ let bS denote the "coset" consisting of all elements of the form ba^j (for example, $1S = S$). It is easy to see that any two cosets are either identical or distinct (namely: if some b_1a^i in b_1S is also in b_2S, i.e., if it is of the form b_2a^j, then *any* element $b_1a^{i'}$ in b_1S is of the form to be in b_2S, because $b_1a^{i'} = b_1a^ia^{i'-i} = b_2a^{j+i'-i}$). And each coset contains exactly d elements. Since the union of all the cosets exhausts $\mathbf{F}_q^*$, this means that $\mathbf{F}_q^*$ is a disjoint union of d-element sets; hence $d|(q-1)$.

Second proof. First we show that $a^{q-1} = 1$. To see this, write the product of all nonzero elements in $\mathbf{F}_q$. There are $q-1$ of them. If we multiply each of them by a, we get a rearrangement of the same elements (since any two distinct elements remain distinct after multiplication by a). Thus, the product is not affected. But we have multiplied this product by a^{q-1}. Hence $a^{q-1} = 1$. (Compare with the proof of Proposition I.3.2.) Now let d be the order of a, i.e., the smallest positive power which gives 1. If d did not divide $q-1$, we could find a smaller positive number r — namely, the remainder when $q-1 = bd + r$ is divided by d — such that $a^r = a^{q-1-bd} = 1$. But this contradicts the minimality of d. This concludes the proof.

Definition. A *generator* g of a finite field $\mathbf{F}_q$ is an element of order $q-1$; equivalently, the powers of g run through all of the elements of $\mathbf{F}_q^*$.

The next proposition is one of the very basic facts about finite fields. It says that the nonzero elements of any finite field form a *cyclic group*, i.e., they are all powers of a single element.

Proposition II.1.2. *Every finite field has a generator. If g is a generator of $\mathbf{F}_q^*$, then g^j is also a generator if and only if g.c.d.$(j, q-1) = 1$. In particular, there are a total of $\varphi(q-1)$ different generators of $\mathbf{F}_q^*$.*

Proof. Suppose that $a \in \mathbf{F}_q^*$ has order d, i.e., $a^d = 1$ and no lower power of a gives 1. By Proposition II.1.1, d divides $q-1$. Since a^d is the smallest power which equals 1, it follows that the elements $a, a^2, \ldots, a^d = 1$ are distinct. We claim that the elements of order d are precisely the $\varphi(d)$ values a^j for which $g.c.d.(j, d) = 1$. First, since the d distinct powers of a all satisfy the equation $x^d = 1$, these are all of the roots of the equation (see paragraph 5 in the list of facts about fields). Any element of order d must thus be among the powers of a. However, not all powers of a have order d, since if $g.c.d.(j, d) = d' > 1$, then a^j has lower order: because d/d' and j/d' are integers, we can write $(a^j)^{(d/d')} = (a^d)^{j/d'} = 1$. Conversely, we now show that a^j does have order d whenever $g.c.d.(j, d) = 1$. If j is prime to d, and if a^j had a smaller order d'', then $a^{d''}$ raised to either the j−th or the d−th power would give 1, and hence $a^{d''}$ raised to the power $g.c.d.(j, d) = 1$ would give 1 (this is proved in exactly the same way as Proposition I.4.2). But this contradicts the fact that a is of order d and so $a^{d''} \neq 1$. Thus, a^j has order d if and only if $g.c.d.(j, d) = 1$.

This means that, if there is any element a of order d, then there are exactly $\varphi(d)$ elements of order d. So for every $d|(q-1)$ there are only two