14. For any fixed p, show that there is a sequence $q_j = p^{f_j}$ of powers of p such that the probability that a random element of $\mathbf{F}_{q_j}$ is a generator of $\mathbf{F}_{q_j}^*$ approaches 0 as $j \longrightarrow \infty$.
15. Which polynomials in $\mathbf{F}_p[X]$ have derivative identically zero?
16. Let σ be the automorphism of $\mathbf{F}_q$ in Proposition II.1.5. Prove that the set of elements left fixed by σ^j is the field $\mathbf{F}_{p^d}$, where $d = g.c.d.(j, f)$.
17. Prove that if b is a generator of $\mathbf{F}_{p^n}^*$ and if $d|n$, then $b^{(p^n-1)/(p^d-1)}$ is a generator of $\mathbf{F}_{p^d}^*$.

2 Quadratic residues and reciprocity

Roots of unity. In many situations it is useful to have solutions of the equation $x^n = 1$. Suppose we are working in a finite field $\mathbf{F}_q$. We now answer the question: How many n-th roots of unity are there in $\mathbf{F}_q$?

Proposition II.2.1. *Let g be a generator of $\mathbf{F}_q^*$. Then g^j is an n-th root of unity if and only if $nj \equiv 0 \ mod \ q-1$. The number of n-th roots of unity is $g.c.d.(n, q-1)$. In particular, $\mathbf{F}_q$ has a* **primitive** *n-th root of unity (i.e., an element ξ such that the powers of ξ run through n n-th roots of unity) if and only if $n|\, q-1$. If ξ is a primitive n-th root of unity in $\mathbf{F}_q$, then ξ^j is also a primitive n-th root if and only if $g.c.d.(j, n) = 1$.*

Proof. Any element of $\mathbf{F}_q^*$ can be written as a power g^j of the generator g. A power of g is 1 if and only if the power is divisible by $q-1$. Thus, an element g^j is an n-th root of unity if and only if $nj \equiv 0 \ mod \ q-1$. Next, let $d = g.c.d.(n, q-1)$. According to Corollary 2 of Proposition I.3.1, the equation $nj \equiv 0 \ mod \ q-1$ (with j the unknown) is equivalent to the equation $\frac{n}{d}j \equiv 0 \ mod \ \frac{q-1}{d}$. Since n/d is prime to $(q-1)/d$, the latter congruence is equivalent to requiring j to be a multiple of $(q-1)/d$. In other words, the d distinct powers of $g^{(q-1)/d}$ are precisely the n-th roots of unity. There are n such roots if and only if $d = n$, i.e., $n|\, q-1$. Finally, if n does divide $q-1$, let $\xi = g^{(q-1)/n}$. Then ξ^j equals 1 if and only if $n|j$. The k-th power of ξ^j equals 1 if and only if $kj \equiv 0 \ mod \ n$. It is easy to see that ξ^j has order n (i.e., this equation does not hold for any positive $k < n$) if and only if j is prime to n. Thus, there are $\varphi(n)$ different primitive n-th roots of unity if $n|\, q-1$. This completes the proof.

Corollary 1. *If $g.c.d.(n, q-1) = 1$, then 1 is the only n-th root of unity.*

Corollary 2. *The element $-1 \in \mathbf{F}_q$ has a square root in $\mathbf{F}_q$ if and only if $q \equiv 1 \ mod \ 4$.*

The first corollary is a special case of the proposition. To prove Corollary 2, note that a square root of -1 is the same thing as a primitive 4-th root of 1, and our field has a primitive 4-th root if and only if $4|\, q-1$.

Corollary 2 says that if $q \equiv 3 \ mod \ 4$, we can always get the quadratic extension $\mathbf{F}_{q^2}$ by adjoining a root of X^2+1, i.e., by considering "Gaussian integer" type expressions $a + bi$. We did this for $q = 3$ in the last section.