Chapter 11

Finite Fields and Primitive Roots

11.1 $\mathbb{F}_p[X]$

In this chapter we will construct and study finite fields; an important tool will be the polynomial ring $\mathbb{F}_p[X]$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the finite field with p elements. We know that $\mathbb{F}_p[X]$ is Euclidean, hence a PID and a UFD.

When we regard $\mathbb{Z}/p\mathbb{Z}$ as a finite field $\mathbb{F}_p$, we usually omit the "mod$p$". Thus we simply write $-1 = 2$ in $\mathbb{F}_3$ instead of $-1 \equiv 2 \bmod 3$. This is standard practice – don't let this abuse of language confuse you.

We know that the units in $R = \mathbb{F}_p[X]$ are the nonzero constants: $R^\times = \mathbb{F}_p^\times$. This is because $\deg fg = \deg f + \deg g$, so $fg = 1$ implies $\deg f = \deg g = 0$. In particular, every polynomial $f \in \mathbb{F}_p[X]$ is a unit times a monic polynomial.

Since linear polynomials $X + a$ for every $a \in \mathbb{F}_p$ are irreducible ($X + a = fg$ implies $1 = \deg f + \deg g$, hence f or g is a unit), they are primes. In particular, the polynomials X, $X + 1$, ..., $X + p - 1$ are primes in $\mathbb{F}_p[X]$. Are there more? Of course, if $p \neq 2$, then $2X$, $2X + 1$, ..., $2X + p - 1$ are also prime; but since e.g. $2X + 1 = 2(X + \frac{1}{2}) = 2(X + \frac{p+1}{2})$ differs from $X + \frac{p+1}{2}$ only by the unit 2, we regard them as one and the same prime (just as in $\mathbb{Z}$, the primes 3 and -3 are counted as one).

In order to minimize the confusion, let us agree that a prime is a monic polynomial (just as we can define a prime in $\mathbb{Z}$ to be positive). A more satisfying solution would be to talk about prime ideals instead of primes: in $\mathbb{Z}$ we have $(5) = (-5)$, so 5 and -5 generate the same prime ideal (5), and in $\mathbb{F}_p[X]$ we have $(X + r) = (aX + ar)$ for all nonyero a.

Now we will answer the question whether $\mathbb{F}_p[X]$ contains infinitely many primes:

Proposition 11.1. *There are infinitely many primes in $\mathbb{F}_p[x]$.*

Proof. Assume that there are only finitely many, say $f_1 = X, \ldots, f_r$. Then let

$F = f_1 \cdots f_r + 1$. Since $\deg F \geq 1$, this polynomial must have a prime factor f. Clearly $f \neq f_j$ since $f_j \mid F$ and $f_j \mid F - 1$ would imply that $f_j \mid 1$. Thus f is a prime not on the list. $\square$

In $\mathbb{F}_2[X]$, the primes of degree 1 are X and $X + 1$. In order to find a new one, take $F(X) = X(X + 1) + 1 = X^2 + X + 1$, which is irreducible in $\mathbb{F}_2[X]$ and therefore a prime of degree 2. If you do the same thing in $\mathbb{F}_3[X]$, then $F(X) = X^2 + X + 1$ is not irreducible since $F(X) = (X - 1)^2$. but this gives you a new prime $X - 1 = X + 2$. Repeating Euclid's argument gives $F(X) = X(X + 1)(X - 1) + 1 = X^3 - X + 1$, which is irreducible (since it cannot be divisible by any linear factor) and therefore prime.

Writing down primes explicitly is difficult. For example, $f(X) = X^2 + 1$ is prime in $\mathbb{F}_3[X]$ but not in $\mathbb{F}_5[x]$. In fact:

Proposition 11.2. *Let p be an odd prime. Then $X^2 + 1$ is prime in $\mathbb{F}_p[X]$ if and only if $p \equiv 3 \bmod 4$.*

Proof. If $p \equiv 1 \bmod 4$, then there is some $a \in \mathbb{F}_p$ with $ar2 = -1$. Thus $X^2+1 = X^2 - r^2 = (X - r)(X + r)$ is reducible.

Now assume that $p \equiv 3 \bmod 4$. If $X^2 + 1 = (X - r)(X - s)$, then $r + s = 0$, hence $X^2 + 1 = (X - r)(X + r) = X^2 - r^2$. This implies $r^2 = -1$, which is impossible in $\mathbb{F}_p$ for primes $p \equiv 3 \bmod 4$. $\square$

This result should ring a bell: compare the factorizations of X^2+1 in $\mathbb{F}_p[X]$ with the factorizations of the principal ideal (p) in $\mathbb{Q}(i)$:

p	$\mathbb{F}_p[X]$	$\mathbb{Q}(i)$
2	$X^2 + 1 = (X + 1)^2$	$(2) = (1 + i)^2$
$p \equiv 1 \bmod 4$	$X^2 + 1 = (X - r)(X + r)$	$(p) = (a + bi)(a - bi)$
$p \equiv 3 \bmod 4$	$X^2 + 1 = X^2 + 1$	$(p) = (p)$

This analogy will be explained in algebraic number theory.

Thus it is not obvious that there exist primes of degree 2 in every $\mathbb{F}_p[X]$. In fact, such primes always exist:

Proposition 11.3. *There are exactly $\frac{p(p-1)}{2}$ irreducible quadratic polynomials in $\mathbb{F}_p[X]$.*

Proof. There are exactly p^2 monic polynomials $X^2 + rX + s \in \mathbb{F}_p[X]$. The reducible polynomials among them have the form $(X - a)(X - b)$ for $a, b \in \mathbb{F}_p$. Recalling that $(X - a)(X - b) = (X - b)(X - a)$ we easily see that there are exactly $\binom{p}{2}$ polynomials with $a \neq b$ and p with $a = b$, hence there are $\frac{p(p+1)}{2}$ reducible polynomials. Thus there exist exactly $\frac{p(p-1)}{2}$ irreducible quadratic polynomials in $\mathbb{F}_p[X]$. $\square$

For example, X^2+X+1 is the unique prime of degree 2 in $\mathbb{F}_2[X]$, and the quadratic primes in $\mathbb{F}_3[X]$ are X^2+1, X^2+X-1 and X^2-X-1.

This argument can be generalized to count the number of primes of any given degree. In this way, Gauss proved

Proposition 11.4. *For any prime p and any given $n>0$, there is an irreducible element $f \in \mathbb{F}_p[X]$ of degree n.*

This is proved in abstract algebra.

11.2 Residue Classes modulo Polynomials

Now recall that $g \equiv h \bmod f$ if $f \mid (g-h)$. What can we say about the residue classes modulo f in $\mathbb{F}_p[X]$? Let us look at a few examples.

1. The ring $\mathbb{F}_p[X]/(X)$ has exactly p residue classes $0, 1, \ldots, p-1$: in fact, since $X \equiv 0 \bmod X$ we have $a_nX^n + \ldots + a_1X + a_0 \equiv a_0 \bmod X$. Thus every polynomial is congruent to a constant modulo X. On the other hand, $a \equiv b \bmod X$ implies $a = b$, and the claim follows. The map sending the residue class $a \bmod p$ to $a \bmod X$ is a ring isomorphism: we have $\mathbb{F}_p[X]/(X) \simeq \mathbb{F}_p$.

   More generally, $\mathbb{F}_p[X]/(X-a) \simeq \mathbb{F}_p$ for any $a \in \mathbb{F}_p$. Make sure you understand why $f(X) \equiv f(a) \bmod (X-a)$.

2. The ring $\mathbb{F}_p[X]/(X^2)$ has exactly p^2 residue classes, namely $a+bX$ with $a, b \in \mathbb{F}_p$. Note that this is not a field since $X \cdot X \equiv 0 \bmod X^2$.

3. The ring $\mathbb{F}_2[X]/(f)$ for $f(X) = X^2+X+1)$ has exactly 4 elements, namely the classes represented by 0, 1, X and $X+1$. For example, $X^3 = X \cdot X^2 \equiv X(-X-1) = X(X+1) = X^2+X = X-X-1 = 1 \bmod f$.

   It is straightforward to compute an addition and multiplication table for the residue classes:

$+$	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

In general, there are exactly $N(f) = p^{\deg f}$ residue classes modulo f; they form a ring denoted by $\mathbb{F}_p[X]/(f)$. If you have a polynomial $f(X) = X^n + \ldots + a_1X + a_0 \in \mathbb{F}_p[X]$, then working modulo f works like this: observe that

$$X^n \equiv -a_{n-1}X^{n-1} - \ldots - a_1X - a_0 \bmod f$$

allows you to reduce any polynomial $g \in \mathbb{F}_p[X]$ to some polynomial of degree $< \deg f$ by repeatedly applying this definition. For example, for $f(X) = X^2 + 1$ we get

$$\begin{aligned} X^2 &\equiv -1 \bmod f, \\ X^3 &\equiv -X \bmod f, \\ X^4 &\equiv -X^2 \equiv 1 \bmod f \end{aligned}$$

etc. In particular, every polynomial $g \in \mathbb{F}_p[X]$ is congruent modulo f to one of $S_f = \{b_{n-1}X^{n-1} + \ldots + b_1X + b_0 : b_j \in \mathbb{F}_p\}$. Moreover, none of the polynomials in S_f are congruent modulo f: if $g_i \equiv g_j \bmod f$ for polynomials of degree $< \deg f$, then $f \mid (g_i - g_j)$, and since the polynomial on the right hand side has degree $< \deg f$, it must be 0. This shows that S_f is a complete system of residue classes modulo f, and in particular it shows that there are exactly $p^{\deg f}$ residue classes modulo f.

Proposition 11.5. *The ring $\mathbb{F}_p[X]/(f)$ of residue classes modulo f has exactly $p^{\deg f}$ elements.*

The norm of f is by definition $N(f) = \#\mathbb{F}_p[X]/(f)$ (this is how you define the norm of ideals in algebraic number theory), and we have found that $N(f) = p^{\deg f}$.

11.3 Finite Fields

Now recall that if f is a prime in $\mathbb{F}_p[X]$, then $\mathbb{F}_p[X]/(f)$ is a domain: in fact, if $ab \equiv 0 \bmod f$, then $f \mid ab$, hence $f \mid a$ or $f \mid b$, which in turn implies that $a \equiv 0 \bmod f$ or $b \equiv 0 \bmod f$. Since $\mathbb{F}_p[X]/(f)$ has $p^{\deg f}$ elements, it is a finite field. In abstract algebra you will see a proof that any finite field has p^n elements for some prime p and some integer $n \geq 1$, and that there is exactly one such field for each pair (p, n) up to isomorphism.

Proposition 11.6. *Let K be a field. Then every polynomial $f \in K[X]$ has at most* $\deg f$ *roots.*

Proof. Assume that f has the root $a \in K$. Then $f(a) = 0$. Write $f(X) = (X - a)g(X) + r(X)$ for some polynomial r with $\deg r < \deg(X - a) = 1$. Then $\deg r = 0$, hence $r(X)$ is a constant. Plugging in $X = a$ shows that $r = 0$.

We have seen that if $f(a) = 0$, then $f(X) = (X - a)g(X)$ for some polynomial g of degree $\deg g = \deg f - 1$. If g has a root, we can continue in this way; since after at most $\deg f$ steps we reach a constant polynomial, we see that we can write $f(X) = (X - a_1)\cdots(X - a_r)g(X)$, where g is a polynomial without roots in K. Now $f(a) = (a - a_1)\cdots(a - a_r)g(a)$. If a product in a field is zero, one of the factors is; thus if $f(a) = 0$, then $a = a_i$ for some i, and the claim follows. $\square$

Note that the quadratic polynomial $X^2 - 1$ has four roots in $(\mathbb{Z}/8\mathbb{Z})[X]$, namely $X \equiv 1, 3, 5, 7 \bmod 8$. Although we still can factor $f(X) = X^2 - 1 = (X - 1)(X + 1)$, this does not imply that $X = 1$ and $X = -1$ are the only roots of f: in fact we have $f(3) = 0$ even though none of the factors $3 - 1 = 2$ and $3 + 1 = 4$ are $\equiv 0 \bmod 8$. Also, f has the different factorizations $f(X) = (X - 1)(X + 1) = (X - 3)(X + 3)$.

We now prove a generalization of the Theorem of Euler-Fermat:

Theorem 11.7 (Lagrange's Theorem)**.** *Let G be a finite abelian group of order $\#G = n$ (written multiplicatively). Then $g^n = 1$.*

For the group $G = (\mathbb{Z}/m\mathbb{Z})^\times$ of coprime residue classes modulo m this is just the Theorem of Euler-Fermat. For the multiplicative group $F^\times$ of a finite field with $n = q^m$ elements it means that $a^{n-1} = 1$ for all $a \in F^\times$.

Proof. Write $G = \{g_1 = 1, g_2, \ldots, g_n\}$. Then

$$\begin{aligned} g \cdot g_1 &= h_1, \\ \cdots &\ \cdots \\ g \cdot g_n &= h_n. \end{aligned}$$

We now claim that $G = \{h_1, \ldots, h_n\}$. It is clearly sufficient to show that the h_i are pairwise distinct. But if $h_i = h_j$, then $g \cdot g_i = g \cdot g_j$, and multiplying through by g^{-1} we find $g_i = g_j$.

Multiplying these equations together shows that $g^n \prod g_i = \prod h_i$, and since $\prod g_i = \prod h_i$ we conclude that $g^n = 1$. $\square$

We also can give an abstract version of Wilson's Theorem. In fact, let G be a finite abelian group with n elements, say $G = \{g_1 = 1, \ldots, g_n\}$. In groups, each element has an inverse, and we can form pairs (g, g^{-1}). How often does it happen that $g = g^{-1}$? Elements with this property are solutions of the equation $g^2 = 1$. We claim that the elements with this property form a subgroup H of G. In fact, if $g^2 = 1$ and $h^2 = 1$, then $(gh)^2 = g^2h^2 = 1$ since G is abelian. Moreover, if $g \in H$, then $g^{-1} = g\ inH$.

By multiplying over pairs of inverse elements we see that $\prod_{g \in G \setminus H} = 1$. Thus $\prod_{g \in G} = \prod_{g \in G \setminus H} \prod_{h \in H} = \prod_{h \in H}$.

This is in fact Wilson's theorem: if $G = (\mathbb{Z}/p\mathbb{Z})^\times$, then $H = \{+1, -1\}$, and we find $\prod_{g \in G} g = [-1]$. More generally, we have $H = \{-1, +1\}$ whenever $G = \mathbb{F}_p^\times$ is the multiplicative group of a finite field. In fact, $g^2 = 1$ means $0 = g^2 - 1 = (g - 1)(g + 1)$, and in fields this implies $g = 1$ or $g = -1$.

Note that there are groups in which $g^2 = 1$ has lots of solutions; in $G = (\mathbb{Z}/8\mathbb{Z})^\times$, for example, we have $g^2 = 1$ for each element since $a^2 \equiv 1 \bmod 8$ whenever a is odd.

11.4 Primitive Roots

We now come to an extremely important theorem:

Theorem 11.8. *The multiplicative group of any finite field is cyclic.*

A finite group G is called cyclic if there is an element $g \in G$ such that every $h \in G$ is a power of g, i.e., such that $h = g^n$ for some integer n (if G is written multiplicatively) or $h = ng$ (if G is written additively). In such a case we say that G is generated by g.

Examples:

- A trivial example: The groups $\mathbb{Z}/m\mathbb{Z}$ are generated by the residue class $1 \bmod m$: every element of $\mathbb{Z}/m\mathbb{Z}$ has the form $n \equiv n \cdot 1 \bmod m$.
- The group $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4 \bmod 5\}$ is generated by $2 \bmod 5$ since $2 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$ and $2^4 \equiv 1 \bmod 5$. In our new notation this would read that $\mathbb{F}_5^\times = \{1, 2, 3, 4\}$ is cyclic since $2^1 = 2$, $2^2 = 4$, $2^3 = 3$ and $2^4 = 1$ in $\mathbb{F}_5$.
- The group $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic: each of the residue classes 1, 3, 5, $7 \bmod 8$ does not generate the full group.

Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$, it is cyclic. Generators of $(\mathbb{Z}/p\mathbb{Z})^\times$ are called primitive roots modulo p. For example, 2 is a primitive root modulo 5, and 3 is a primitive root modulo 7.

For the proof we a bit of information on the order of elements a in finite abelian groups G: this is the smallest positive integer r such that $a^r = 1$.

Lemma 11.9. *Let g be an element of order n in some finite abelian group G. If $g^m = 1$, then $n \mid m$.*

Proof. Write $m = qn + r$ with $0 \le r < n$ (Euclidean division); then $1 = g^m = g^{qn+r} = q^{qn} g^r = g^r$. Since n is the minimal positive exponent with this property and $r < n$, we must have $r = 0$. This proves the claim. □

Lemma 11.10. *If G is an abelian group, and if $a, b \in G$ are elements of order m and n respectively such that $\gcd(m, n) = 1$, then ab has order mn.*

Proof. Clearly $(ab)^{mn} = a^{mn} b^{mn} = (a^m)^n (b^m)^n = 1$, so ab has order dividing mn (note that we have used commutativity here).

For the converse, let k denote the order of mn, that is the minimal integer k with $1 \le k \le mn$ such that $(ab)^k = 1$; we have to show that $k = mn$.

From $(ab)^k = 1$ we get $1 = (ab)^{km} = a^{km} b^{km} = b^{km}$; hence $n \mid km$ by Lemma 11.9; since $\gcd(n, m) = 1$, we have $n \mid k$.

Exactly the same reasoning with the roles of a and b interchanged shows that $m \mid k$. But $\gcd(m, n) = 1$, hence $n \mid k$ and $m \mid k$ imply that $mn \mid k$. Since $k \neq 0$, we conclude that $k \ge mn$, and this proves the claim. □

Proof of Theorem 11.8. Let $n = \#\mathbb{F}^\times$ denote the number of elements of the finite abelian group $F^\times$. If $n = 1$, the claim is trivial because $F^\times = \{1\}$ is clearly generated by 1. If $n > 1$, let p be a prime divisor of the order n of $F^\times$. Then there is an element $a \in F$ such that $a^{n/p} \neq 1$. For if not, then every $a \in F$ is a root of the polynomial $f(X) = X^{n/p} - 1$; in particular, f has degree n/p and n roots. But polynomials f over fields can have at most $\deg f$ roots: contradiction.

Now let p^r be the exact power of a prime p that divides $n = \#F^\times$; then we claim that the element $x = a^{n/p^r}$ has order p^r. In fact, $x^{p^r} = a^n = 1$ by Lagrange's Theorem (in the case that we are most interested in, namely $F = \mathbb{Z}/p\mathbb{Z}$, this is just Fermat's Little Theorem), so the order of x divides p^r by Lemma 11.9. If the order were smaller, then we would have $x^{p^{r-1}} = 1$; but $x^{p^{r-1}} = a^{n/p} \neq 1$ by choice of a.

Now write $n = p_1^{r_1} \cdots p_t^{r_t}$. By the above, we can construct an element x_i of order $p_i^{r_i}$ for every $1 \leq i \leq t$. But then $x_1 \cdots x_t$ has order n by Lemma 11.10 (use induction). □

The fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic can be used to give another proof of the fact that the congruence $x^2 \equiv -1 \bmod p$ is solvable if $p \equiv 1 \bmod 4$: since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, there is an element $g \in \mathbb{Z}$ such that $[x]$ has order $p-1$. Thus $g^{p-1} \equiv 1 \bmod p$, hence $p \mid (g^{p-1} - 1) = (g^{(p-1)/2} - 1)(g^{(p-1)/2} + 1)$. If p divided the first factor, then $[g]$ would have order dividing $\frac{p-1}{2}$; thus p divides the second factor, and we find $g^{(p-1)/2} \equiv -1 \bmod p$. Put $x = g^{(p-1)/4}$; then $x^2 \equiv -1 \bmod p$.

Definition. We say that an integer g is a primitive root modulo m if the powers of g generate all residue classes coprime to m. For example, 3 is a primitive root modulo 7, but 2 is not.

Corollary 11.11. *For every prime p there exist primitive roots.*

Proof. Since $\mathbb{Z}/p\mathbb{Z}$ is a finite field, the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, that is, there exists an integer g of order $p-1$; the powers of g generate the whole group $(\mathbb{Z}/p\mathbb{Z})^\times$. □

Proposition 11.12. *Let g be a primitive root modulo some odd prime p. Then $g^{(p-1)/2} \equiv -1 \bmod p$; in particular, $(\frac{g}{p}) = -1$.*

Proof. The square of $g^{(p-1)/2}$ is $\equiv 1 \bmod p$ by Fermat's Little Theorem, hence $g^{(p-1)/2} = \pm 1$. But if $g^{(p-1)/2} = 1$, then the powers of g generate at most $\frac{p-1}{2}$ elements, namely $g^0, g^1, \ldots, g^{(p-3)/2}$, contradicting our assumption that g be a primitive root. □

We also can see why $(\frac{-1}{p}) = +1$ for primes $p \equiv 1 \bmod 4$: in this case, $p-1 = 4m$, and the integer $j \equiv g^m \bmod p$ has the property $j^2 \equiv g^{(p-1)/2} \equiv -1 \bmod p$.

11.5 Gauss and Primitive Roots

Let me also give Gauss's proof of the existence of primitive roots, stated slightly more generally for abelian groups:

Theorem 11.13. *Let G be a finite group. Assume that, for every divisor d of $n = \#G$, the equation $x^d = 1$ has at most d solutions. Then G is cyclic.*

Proof. Assume that $d \mid n$, and let $\psi(d)$ denote the number of elements in G with order d (thus for $G = (\mathbb{Z}/5\mathbb{Z})^\times$, we have $\psi(1) = 1$, $\psi(2) = 1$, and $\psi(4) = 2$). If $\psi(d) \neq 0$, then there is an element $g \in G$ of order d, and then $1, g, g^2, \ldots, g^{d-1}$ are distinct solutions of the equation $x^d = 1$ in G. By assumption, there are at most that many solutions, hence these are all solutions of $x^d = 1$.

Let us now determine the order of g^k for $0 \le k < d$. We claim that g^k has order $d/\gcd(d,k)$. In fact, $(g^k)^{d/\gcd(d,k)} = (g^{k/\gcd(d,k)})^d = 1$, so the order of g^k divides $d/\gcd(d,k)$. On the other hand, from $1 = (g^k)^m = g^{km}$ we deduce that $d \mid km$, since d is the order of g. Dividing through by $\gcd(d,k)$ gives $\frac{d}{\gcd(d,k)} \mid \frac{k}{\gcd(d,k)} m$. But since $\frac{d}{\gcd(d,k)}$ and $\frac{k}{\gcd(d,k)}$ are coprime (we have divided out the common factors), this implies that $\frac{d}{\gcd(d,k)} \mid m$, which proves our claim.

Thus if g has order d, then there are exactly $\phi(d)$ elements of order d in G, namely the g^k with $\gcd(d,k) = 1$. In other words: we have $\psi(d) = 0$ or $\psi(d) = \phi(n)$.

Now clearly every element of g has some order, and this order divides $n = \#G$, hence $n = \sum_{d|n} \psi(d)$. Next $\psi(d) \le \phi(d)$ implies that $n = \sum_{d|n} \psi(d) \le \sum_{d|n} \phi(d) = n$, where we have used that $\sum_{d|n} \phi(d) = n$. Taking this for granted for a moment, we see that we must have equality in $\sum_{d|n} \psi(d) \le \sum_{d|n} \phi(d)$. But this happens if and only if $\psi(d) = \phi(d)$ for every $d \mid n$, and in particular there exists an element of order n since $\psi(n) = \phi(n) \ge 1$. ☐

Note that Gauss's proof shows that there exist $\phi(p-1)$ primitive roots modulo p, since $G = (\mathbb{Z}/p\mathbb{Z})^\times$ has $n = p - 1$ elements.

Corollary 11.14. *The multiplicative group $F^\times$ of a finite field F is cyclic.*

Proof. All we have to do is show that the equation $x^d = 1$ has at most d solutions in $F^\times$, but this is true in any field. ☐

It remains to prove

Lemma 11.15. *For every $n \in \mathbb{N}$ we have $\sum_{d|n} \phi(d) = n$.*

In fact, for $n = 6$ this says $\phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$.

Proof. Consider the fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$. For some $d \mid n$, how many of these fractions have denominator d when written in lowest terms?

Clearly there will be $\phi(n)$ fractions with denominator n since these are exactly the $\frac{k}{n}$ with $\gcd(k,n) = 1$.

Now assume that $n = dm$; the fraction $\frac{k}{n}$ will have denominator d if and only if $k = mt$ and $\gcd(t,d) = 1$. Clearly there are $\phi(d)$ such fractions.

Thus among the n fractions, for each $d \mid n$ there are $\phi(d)$ fractions with denominator d, hence $n = \sum_{d|n} \phi(n)$. $\square$

11.6 Gauss's 6th Proof of Quadratic Reciprocity

I can't bring myself to omit giving a modern version of Gauss's sixth proof of the quadratic reciprocity law in $\mathbb{Z}$ based on the arithmetic of finite fields.

Let p and q be odd primes. By Fermat's Little Theorem, $q^{p-1} \equiv 1 \bmod p$, hence the multiplicative group $\mathbb{F}_n^\times$ of the finite field $\mathbb{F}_n$ with $n = q^{p-1}$ has $n-1$ elements. Since $F_n = \mathbb{F}_q[X]/(f)$ for some irreducible polynomial of degree n, we find that $q = 0$ in $\mathbb{F}_n$; in particular, we have $(a+b)^q = a^q + b^q$ since the binomial coefficients "in the middle" all vanish modulo q.

Let x be a generator of $\mathbb{F}_n^\times$; then x has order $n-1$, hence $\zeta := x^{(n-1)/p}$ has order p, i.e. $\zeta \neq 1$ and $\zeta^p = 1$. Now we form the Gauss sum

$$G = \sum_{a=1}^{p-1} \Big(\frac{a}{p}\Big)\zeta^a.$$

Clearly G is an element of the finite field $\mathbb{F}_n$.

In the special case $p = 3$ we find $G = \zeta - \zeta^2$, where $\zeta^3 = 1$. Since $0 = \zeta^3 - 1 = (\zeta-1)(\zeta^2+\zeta+1)$ and since $\zeta \neq 1$, we conclude that $\zeta^2+\zeta+1 = 0$. Now $G^2 = \zeta^2 - 2\zeta^3 + \zeta^4 = \zeta^2 + \zeta - 2 = \zeta^2 + \zeta + 1 - 3 = -3$.

We now derive the following properties of Gauss sums:

Proposition 11.16. *Let G be the Gauss sum defined above. Then*

1. $G^q = (\frac{q}{p})G$;
2. $G^2 = p^*$, *where* $p^* = (\frac{-1}{p})p$.

This immediately implies the quadratic reciprocity law. In fact we find

$$\Big(\frac{q}{p}\Big) = G^{q-1} = (G^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}} = \Big(\frac{p^*}{q}\Big),$$

which in light of

$$\Big(\frac{p^*}{q}\Big) = \Big(\frac{-1}{p}\Big)^{\frac{q-1}{2}}\Big(\frac{p}{q}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{p}{q}\Big)$$

is the quadratic reciprocity law.

Proof of Prop. 11.16. We see

$$\begin{aligned} G^q &= \Big(\sum_{a=1}^{p-1}\Big(\frac{a}{p}\Big)\zeta^a\Big)^q = \sum_{a=1}^{p-1}\Big(\frac{a}{p}\Big)\zeta^{aq} \\ &= \Big(\frac{q}{p}\Big)\sum_{a=1}^{p-1}\Big(\frac{aq}{p}\Big)\zeta^{aq} = \Big(\frac{q}{p}\Big)\sum_{b=1}^{p-1}\Big(\frac{b}{p}\Big)\zeta^b = \Big(\frac{q}{p}\Big)G \end{aligned}$$

since $(\frac{a}{p})^q = (\frac{a}{p})$, since $(x+y)^q = x^q + y^q$ in any finite field containing $\mathbb{F}_q$, and since $b = aq$ runs through a complete system of coprime residues modulo p if a does.

The proof of the second claim is slightly more technical and requires the following observation:

Lemma 11.17. *For an odd prime p we have* $\quad S = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) = 0.$

Proof. Let a be a quadratic non-residue mod p. Then

$$-S = \left(\frac{a}{p}\right) \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) = \sum_{c=1}^{p-1} \left(\frac{ac}{p}\right) = \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) = S,$$

where we have used that $b = ac$ runs through $(\mathbb{Z}/p\mathbb{Z})^\times$ if c does (this is because different values of a give rise to different values of b: an equation $ac = a'c$ implies $a = a'$). $\square$

Now we find

$$G^2 = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a \cdot \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \zeta^b = \sum_{a,b} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

Now substitute $b = ac$; this yields

$$G^2 = \sum_{a,c} \left(\frac{c}{p}\right) \zeta^{a+ac} = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \sum_{a=1}^{p-1} (\zeta^{1+c})^a.$$

But if $c \neq -1$, then ζ^{1+c} is a primitive p-th root of unity, and $\sum_{a=1}^{p} \zeta^a = 0$ shows $\sum_{a=1}^{p-1} \zeta^a = -1$, thus

$$\begin{aligned} G^2 &= -\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right) \sum_{a=1}^{p-1} 1 = -\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + (p-1)\left(\frac{-1}{p}\right) \\ &= p^* - \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) = p^*. \end{aligned}$$

$\square$

This proof of the quadratic reciprocity law generalizes to cubic and quartic residues; essentially you have to replace the Legendre symbol in the quadratic Gauss sum by the cubic or quartic residue symbol $[\frac{\alpha}{\pi}]$, the summation will be over a complete system of residues modulo π, and the exponent a in ζ^a is replaced by the integer $\alpha + \alpha'$. Then the analog of the first property holds, and the second one is replaced by only slightly more complicated formulas.

Exercises

11.1 Show that 2 is not a primitive root modulo primes $p \equiv \pm 1 \bmod 8$.

11.2 Find a prime $p \equiv 3 \bmod 8$ for which 2 is not a primitive root.

11.3 It is quite easy to state and prove Gauss's Lemma for general finite cyclic groups G of even order $\#G = 2m$. Assume that g generates G.

1. Define $-1 = g^n$. Show that $(-1)^2 = 1$.
2. Show that $a^n \in \{-1, +1\}$.
3. Define a "Legendre symbol" $(\frac{a}{G}) = \pm 1$ via $(\frac{a}{G}) = a^n$. Show that a is a square in G if and only if $(\frac{a}{G}) = 1$. (Hint: write $a = g^m$ for some m.)
4. Show that $A = \{1, g, g^2, \ldots, g^{n-1}\}$ defines a halfsystem, i.e. prove that every $g \in G$ has the property that either $g \in A$ or $-g \in A$.
5. Write $ag^i = (-1)^{s(i)} g^j$ for $0 \le i < n$ and let $\mu = s(0) + s(1) + \ldots + s(n-1)$. Prove Gauss's Lemma $(\frac{a}{G}) = (-1)^{\mu}$.

Applying this abstract result to the cyclic groups $G = (\mathbb{Z}/p\mathbb{Z})^\times$, $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$ and $(\mathbb{F}_p[X]/(P))^\times$ now gives Gauss's Lemma in the rings $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{F}_p[X]$, respectively.