Chapter 9

Primitive Roots

9.1 The multiplicative group of a finite field

Theorem 9.1. *The multiplicative group $F^\times$ of a finite field is cyclic.*

Remark: In particular, if p is a prime then $(\mathbb{Z}/p)^\times$ is cyclic.

In fact, this is the only case we are interested in. But since the proof works equally well for any finite field we prove the more general result.

Proof. The *exponent* of a finite group G is the smallest number $e > 0$ such that

$$g^e = e$$

for all $g \in G$.

By Lagrange's Theorem, if G is of order n

$$g^n = e$$

for all $g \in G$. Hence $e \le n$.

In fact it is easy to see that $e \mid n$. For suppose $d = \gcd(e, n)$. Then

$$d = er + ns.$$

It follows that

$$g^d = (g^e)^r (g^n)^s = e.$$

We assume in the rest of the proof that F is a finite field, containing q elements.

Lemma 9.1. *The exponent of $F^\times$ is $q - 1$.*

Proof. Each of the $q-1$ elements $x \in F^\times$ (ie all the elements of F except 0) satisfies the equation

$$x^e - 1 = 0$$

over the field F.

But this equation has at most e roots. It follows that

$$q - 1 \leq e.$$

Since $e \mid q-1$ it follows that

$$e = q - 1.$$

□

Lemma 9.2. *If A is a finite abelian group, and $a, b \in A$ have coprime orders r, s then*

$$\text{order}(ab) = rs.$$

Proof. Suppose $\text{order}(ab) = n$. Then

$$(ab)^{rs} = 1 \implies n \mid rs.$$

On the other hand, since r, s are coprime we can find $x, y \in \mathbb{Z}$ such that

$$rx + sy = 1.$$

But then

$$(ab)^{sy} = a^{sy} = a^{1-rx} = a.$$

It follows that $r \mid n$. Similarly $s \mid n$. Since $\gcd(r, s) = 1$ this implies that

$$rs \mid n.$$

Hence

$$n = rs.$$

□

Lemma 9.3. *Suppose A is a finite abelian group of exponent e. Then A has an element of order e.*

Proof. Let
$$e = p_1^{e_1} \cdots p_r^{e_r},$$
where $p_1, \dots, p_r$ are distinct primes.

Suppose $i \in [1, r]$. There must be an element a_i whose order is divisible by $p_i^{e_i}$; for otherwise we could take e/p_i as exponent in place of e. Let
$$\text{order}(a_i) = p_i^{e_i} q_i.$$
Then
$$b_i = a_i^{q_i}$$
has order $p_i^{e_i}$.

Let
$$a = b_1 \cdots b_r.$$
Since the orders $p_1^{e_1}, \dots, p_r^{e_r}$ of $b_1, \dots, b_r$ are mutually coprime it follows from the last Lemma that that the order of a is
$$p_1^{e_1} \cdots p_r^{e_r} = e.$$
□

It follows from the first and last of these 3 Lemmas that we can find an element $a \in F^\times$ of order $q - 1$. In other words, $F^\times$ is cyclic. □

9.2 Primitive roots

Definition 9.1. *A generator of* $(\mathbb{Z}/p)^\times$ *is called a* primitive root mod p.

Example: Take $p = 7$. Then
$$2^3 \equiv 1 \bmod 7;$$
so 2 has order 3 mod 7, and is not a primitive root.

However,
$$3^2 \equiv 2 \bmod 7,\ 3^3 \equiv 6 \equiv -1 \bmod 7.$$
Since the order of an element divides the order of the group, which is 6 in this case, it follows that 3 has order 6 mod 7, and so is a primitive root.

If g generates the cyclic group G then so does g^{-1}. Hence
$$3^{-1} \equiv 5 \bmod 7$$
is also a primitive root mod 7.

Proposition 9.1. *If a is a primitive root* mod p *then a^r is a primitive root if and only if* $\gcd(r, p-1) = 1$.

Proof. This is really a result from elementary group theory: If G is a cyclic group of order n generated by g, then g^r is also a generator if and only if $\gcd(r, n) = 1$.

For suppose $\gcd(r, n) = 1$. If g^r has order d then

$$(g^r)^d = e,$$

ie

$$g^{rd} = e.$$

But since $\gcd(r, n) = 1$

$$rd = n \implies d = n.$$

Conversely, suppose g^r generates the group. Then g is a power of g^r, say

$$g = (g^r)^s = g^{rs}.$$

Hence

$$rs \equiv 1 \bmod n,$$

and in particular $\gcd(r, n) = 1$. □

Corollary 9.1. *There are $\phi(p-1)$ primitive roots* mod p.

Example: Suppose $p = 11$. Then $(\mathbb{Z}/11)^\times$ has order 10, so its elements have orders 1,2,5 or 10. Now

$$2^5 = 32 \equiv -1 \bmod 11.$$

So 2 must be a primitive root mod 11.

There are

$$\phi(10) = 4$$

primitive roots mod 11, namely

$$2, 2^3, 2^7, 2^9 \bmod 11,$$

ie

$$2, 8, 7, 6.$$

9.3 Prime power moduli

Suppose
$$n = p_1^{e_1} \dots p_r^{e_r}.$$
Then
$$(\mathbb{Z}/n)^\times = (\mathbb{Z}/p_1^{e_1})^\times \times \cdots \times (\mathbb{Z}/p_1^{e_1})^\times.$$

Thus the structure of the multiplicative groups $(\mathbb{Z}/n)^\times$ will be completely determined once we know the structure of $(\mathbb{Z}/p^e)^\times$ for each prime power p^e. It turns out that we have already done most of the work in determining the structure of $(\mathbb{Z}/p)^\times$.

Proposition 9.2. *If p is an odd prime number then the multiplicative group*
$$(\mathbb{Z}/p^e)^\times$$
is cyclic for all $e \geq 1$.

Proof. We have proved the result for $e = 1$. We derive the result for $e > 1$ in the following way.

The group $(\mathbb{Z}/p^e)^\times$ has order
$$\phi(p^e) = p^{e-1}(p-1).$$

By the Theorem, there exists an element a with
$$\text{order}(a \bmod p) = p - 1.$$
Evidently
$$\text{order}(a \bmod p) \mid \text{order}(a \bmod p^e).$$
Thus the order of a mod p^e is divisible by $p - 1$, say
$$\text{order}(a \bmod p^e) = (p-1)r.$$
Then
$$\text{order}(a^r \bmod p^e) = p - 1.$$

It is therefore sufficient by Lemma 9.2 to show that there exists an element of order p^{e-1} in the group.

The elements in $(\mathbb{Z}/p^e)^\times$ of the form $x = 1 + py$ form a subgroup
$$S = \{x \in (\mathbb{Z}/p^e)^\times : x \equiv 1 \bmod p\}$$
of order p^{e-1}. It suffices to show that this subgroup is cyclic.

That is relatively straightforward. Each element of the group has order p^j for some j. We have to show that some element $x = 1+py$ has order p^{e-1}, ie

$$(1+py)^{p^{e-2}} \not\equiv 1 \bmod p^e.$$

By the binomial theorem,

$$(1+py)^{p^{e-2}} = 1 + p^{e-2}py + \binom{p^{e-2}}{2}p^2y^2 + \binom{p^{e-2}}{3}p^3y^3 + \cdots .$$

We claim that all the terms after the first two are divisible by p^e, ie

$$p^e \mid \binom{p^{e-2}}{r}p^r y^r$$

for $r \geq 2$.

For

$$\begin{aligned}\binom{p^{e-2}}{r} &= \frac{p^{e-2}(p^{e-2}-1)\cdots(p^{e-2}-r+1)}{1\cdot 2\cdots r}\\ &= \frac{p^{e-2}}{r}\cdot\frac{(p^{e-2}-1)\cdots(p^{e-2}-r+1)}{1\cdot 2\cdots(r-1)}\\ &= \frac{p^{e-2}}{r}\cdot\binom{p^{e-2}-1}{r-1}.\end{aligned}$$

Thus if

$$p^f \parallel r$$

(ie $p^f \mid r$ but $p^{f+1} \nmid r$) then

$$p^{e-2-f} \mid \binom{p^{e-2}}{r}.$$

Hence

$$p^{e-2-f+r} \mid \binom{p^{e-2}}{r}p^r y^r.$$

We must show that

$$e-2-f+r \geq e,$$

ie

$$r \geq f+2.$$

Now $r \geq p^f$ (since $p^f \mid r$), so it is sufficient to show that

$$p^f \geq f + 2,$$

which is more or less obvious. (If $f = 1$ then $p \geq 3$ since p is an odd prime, and each time we increase f we multiply the left by p and add 1 to the right.)

It follows that

$$(1 + py)^{p^{e-2}} \equiv 1 + p^{e-1}y \bmod p^e.$$

Thus any element of the form $1 + py$ where y is not divisible by p (for example, $1 + p$) must have multiplicative order p^{e-1}, and so must generate S. In particular the subgroup S is cyclic, and so $(\mathbb{Z}/p^e)^\times$ is cyclic. □

Turning to $p = 2$, it is evident that $(\mathbb{Z}/2)^\times$ is trivial, while $(\mathbb{Z}/4)^\times = C_2$.

Proposition 9.3. *If* $e \geq 3$ *then*

$$(\mathbb{Z}/2^e)^\times \cong C_2 \times C_{2^{e-2}}.$$

Proof. Since

$$\phi(2^e) = 2^{e-1},$$

$(\mathbb{Z}/2^e)^\times$ contains 2^{e-1} elements.

We argue as we did for odd p, except that now we take the elements in $(\mathbb{Z}/2^e)^\times$ of the form $x = 1 + 2^2y$, forming the subgroup

$$S = \{x \in (\mathbb{Z}/2^e)^\times : x \equiv 1 \bmod 4\}$$

or order 2^{e-2}.

By the binomial theorem,

$$(1 + 2^2y)^{2^{e-3}} = 1 + 2^{e-3}2^2y + \binom{2^{e-3}}{2}2^4y^2 + \binom{2^{e-3}}{3}2^6y^3 + \cdots.$$

As before, all the terms after the first two are divisible by 2^e, ie

$$2^e \mid \binom{p^{e-3}}{r}2^{2r}y^r$$

for $r \geq 2$. For

$$\binom{2^{e-3}}{r} = \frac{2^{e-3}}{r} \cdot \binom{2^{e-3} - 1}{r - 1}.$$

Thus if $2^f \parallel r$ it is sufficient to show that

$$e - 3 - f + 2r \geq e,$$

ie

$$2r \geq f + 3,$$

which follows easily from the fact that

$$r \geq 2^f.$$

Thus any element of the form $1 + 2^2 y$ with y odd (for example, 5) must have multiplicative order 2^{e-2}. So the subgroup S is cyclic of this order.

Now let

$$C = \{\pm 1 \bmod 2^e\}.$$

This is a subgroup of order 2. Also it is clear that

$$C \cap S = \{1\}.$$

It follows that

$$(\mathbb{Z}/2^e)^\times = C \times S \cong C_2 \times C_{2^{e-2}},$$

as required. □

Example: Consider

$$(\mathbb{Z}/8)^\times = \{1, 3, 5, 7\}.$$

All the elements except 1 have order 2, so

$$(\mathbb{Z}/8)^\times = C_2 \times C_2.$$

Concretely,

$$(\mathbb{Z}/8)^\times = \{\pm 1\} \times \{1, 5\}.$$

As we said, this allows us to determine the structure of any $(\mathbb{Z}/n)^\times$.

Example: Suppose $n = 48$. Then

$$\begin{aligned}(\mathbb{Z}/48)^\times &= (\mathbb{Z}/16)^\times \times (\mathbb{Z}/3)^\times \\ &= (C_2 \times C_8) \times C_2 \\ &= C_2 \times C_2 \times C_8.\end{aligned}$$

9.4 Carmichael numbers, again

We can now complete the proof of our Proposition on Carmichael numbers in the last Chapter:

Proposition 9.4. *The number n is a Carmichael number if and only if it is square-free, and*

$$n = p_1 p_2 \cdots p_r$$

where $r \geq 2$ and

$$p_i - 1 \mid n - 1$$

for $i = 1, 2, \ldots, r$.

Proof. Suppose

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

is a Carmichael number, ie

$$x^n \equiv x \bmod n$$

for all x.

Note first that n must be odd; for otherwise

$$(-1)^n \equiv 1 \not\equiv -1 \bmod n.$$

First we show that n is square-free. For suppose

$$p^e \parallel n,$$

where $e > 1$. Then $(\mathbb{Z}/p^e)^\times$, and so $(Z/n)^\times$, contains an element x of order p. But $p \mid n$. Hence

$$x^n \equiv 1 \not\equiv x \bmod n.$$

Now suppose $p \mid n$.

Then $(\mathbb{Z}/p)^\times$, and so $(Z/n)^\times$, contains an element x of order $p - 1$. This element must be coprime to n, so

$$\begin{aligned} x^n \equiv x \bmod n &\implies x^{n-1} \equiv 1 \bmod n \\ &\implies p - 1 \mid n - 1. \end{aligned}$$

□