6
The Group of Units

We saw in Chapter 5 that for each n, the set U_n of units in $\mathbb{Z}_n$ forms a group under multiplication. Our aim in this chapter is to understand more about multiplication and division in $\mathbb{Z}_n$ by studying the structure of this group. An important result is that if $n = p^e$, where p is an odd prime, then U_n is cyclic; following a commonly-used strategy, we shall prove this first for $n = p$, and then deduce it for $n = p^e$. As often happens in number theory, the prime 2 is exceptional: although U_2 and U_4 are cyclic, we shall see that the group U_{2^e} is not cyclic for $e \geq 3$, although in a certain sense it is nearly cyclic. Using the Chinese Remainder Theorem, we can use our knowledge of the prime-power case to deduce the structure of U_n for arbitrary n. As an application, we will continue the study of Carmichael numbers, begun in Chapter 4.

From now on, for notational simplicity we will often omit the square brackets when using congruence classes. Thus we will sometimes regard an integer a as an element of $\mathbb{Z}_n$ or of U_n, when we should really write $[a]$. The context should make our meaning clear.

6.1 The group U_n

We say that a group G is *abelian* if its elements commute, that is, $gh = hg$ for all $g, h \in G$.

Lemma 6.1

U_n is an abelian group under multiplication mod (n).

Proof

Theorem 5.2 shows that U_n is a group, and Exercise 5.2 shows that it is abelian. □

If G is a finite group with an identity element e, the *order* of an element $g \in G$ is the least integer $k > 0$ such that $g^k = e$; then the integers l such that $g^l = e$ are the multiples of k.

Example 6.1

In U_5 the element 2 has order 4: its powers are $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$ and $2^4 \equiv 1 \bmod (5)$, so $k = 4$ is the least positive exponent such that $2^k = 1$ (the identity element) in U_5. Similarly, the element 1 has order 1, while the elements 3 and 4 have orders 4 and 2 respectively.

Example 6.2

In U_8, the elements $1, 3, 5, 7$ have orders $1, 2, 2, 2$ respectively.

Exercise 6.1

Find the orders of the elements of U_9 and of U_{10}.

In Lemma 2.12 we showed that distinct Fermat numbers are coprime; as an application of the group structure of U_n we can now prove the corresponding result for the Mersenne numbers. First we need:

Lemma 6.2

If l and m are coprime positive integers, then $2^l - 1$ and $2^m - 1$ are coprime.

Proof

Let n be the highest common factor of $2^l - 1$ and $2^m - 1$. Clearly n is odd, so 2 is a unit mod (n). Let k be the order of the element 2 in the group U_n. Since n divides $2^l - 1$ we have $2^l = 1$ in U_n, so k divides l. Similarly k divides m, so

k divides $\gcd(l, m) = 1$. Thus $k = 1$, so the element 2 has order 1 in U_n. This means that $2^1 \equiv 1 \bmod (n)$, so $n = 1$, as required. □

Exercise 6.2

Show that if l and m are positive integers with highest common factor h, then $\gcd(2^l - 1, 2^m - 1)$ divides $2^h - 1$.

Corollary 6.3

Distinct Mersenne numbers are coprime.

Proof

In Lemma 6.2, if we take l and m to be distinct primes we see that $M_l = 2^l - 1$ and $M_m = 2^m - 1$ are coprime. □

6.2 Primitive roots

Our aim is to describe the structure of the group U_n for all n. To do this, it is not sufficient simply to know its order $\phi(n)$. For example, since $\phi(5) = 4 = \phi(8)$, the groups U_5 and U_8 both have order 4. However, these two groups are not isomorphic, since U_5 has elements of order 4, namely 2 and 3, whereas U_8 has none (see Examples 6.1 and 6.2). In group-theoretic terminology and notation, U_5 is a cyclic group of order 4 ($U_5 \cong C_4$), generated by 2 or by 3, whereas U_8 is a Klein four-group ($U_8 \cong V_4 = C_2 \times C_2$).

Exercise 6.3

The groups U_{10} and U_{12} both have order 4; show that exactly one of them is cyclic.

Definition

If U_n is cyclic then any generator g for U_n is called a *primitive root* mod (n). This means that g has order equal to the order $\phi(n)$ of U_n, so that the powers of g yield all the elements of U_n. For instance, 2 and 3 are primitive roots mod (5), but there are no primitive roots mod (8) since U_8 is not cyclic.

Finding primitive roots in U_n (if they exist) is a non-trivial problem, and there is no simple solution. One obvious but tedious method is to try each of the $\phi(n)$ units $a \in U_n$ in turn, each time computing powers a^i mod (n) to find the order of a in U_n; if we find an element a of order $\phi(n)$ then we know that this must be a primitive root. The following result is a rather more efficient test for primitive roots:

Lemma 6.4

An element $a \in U_n$ is a primitive root if and only if $a^{\phi(n)/q} \neq 1$ in U_n for each prime q dividing $\phi(n)$.

Proof

($\Rightarrow$) If a is a primitive root, then it has order $|U_n| = \phi(n)$, so $a^i \neq 1$ for all i such that $1 \leq i < \phi(n)$; in particular, this applies to $i = \phi(n)/q$ for each prime q dividing $\phi(n)$.

($\Leftarrow$) If a is not a primitive root, then its order k must be a proper factor of $\phi(n)$, so $\phi(n)/k > 1$. If q is any prime factor of $\phi(n)/k$, then k divides $\phi(n)/q$, so that $a^{\phi(n)/q} = 1$ in U_n, against our hypothesis. Thus a must be a primitive root. □

Example 6.3

Let $n = 11$, and let us see whether $a = 2$ is a primitive root mod (11). Lemma 5.4 gives $\phi(11) = 11 - 1 = 10$, which is divisible by the primes $q = 2$ and $q = 5$, so we take $\phi(n)/q$ to be 5 and 2 respectively. Now $2^5, 2^2 \not\equiv 1$ mod (11), so Lemma 6.4 implies that 2 is a primitive root mod (11). To verify this, note that in U_{11} we have

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10,$$
$$2^6 = 9,\ 2^7 = 7,\ 2^8 = 3,\ 2^9 = 6,\ 2^{10} = 1;$$

thus 2 has order 10, and its powers give all the elements of U_{11}. If we apply Lemma 6.4 with $a = 3$, however, we find that $3^5 = 243 \equiv 1$ mod (11), so 3 is not a primitive root mod (11): its powers are $3, 9, 5, 4$ and 1.

Example 6.4

Let us find a primitive root mod (17). We have $\phi(17) = 16$, which has only $q = 2$ as a prime factor. Lemma 6.4 therefore implies that an element $a \in U_{17}$ is a primitive root if and only if $a^8 \neq 1$ in U_{17}. Trying $a = 2$ first, we have

$2^8 = 256 \equiv 1 \bmod (17)$, so 2 is not a primitive root. However, $3^8 = (3^4)^2 \equiv (-4)^2 = 16 \not\equiv 1 \bmod (17)$, so 3 is a primitive root.

Example 6.5

To demonstrate that Lemma 6.4 also applies when n is composite, let us take $n = 9$. We have $\phi(9) = 6$, which is divisible by the primes $q = 2$ and $q = 3$, so that $\phi(n)/q$ is 3 and 2 respectively. Thus an element $a \in U_9$ is a primitive root if and only if $a^2, a^3 \neq 1$ in U_9. Since $2^2, 2^3 \not\equiv 1 \bmod (9)$, we see that 2 is a primitive root.

Exercise 6.4

Find primitive roots in U_n for $n = 18, 23, 27$ and 31.

Exercise 6.5

Show that if U_n has a primitive root then it has $\phi(\phi(n))$ of them.

We will show that U_n contains primitive roots if n is prime. This follows from the next theorem.

Theorem 6.5

If p is prime, then the group U_p has $\phi(d)$ elements of order d for each d dividing $p - 1$.

Before proving this, we deduce:

Corollary 6.6

If p is prime then the group U_p is cyclic.

Proof

Putting $d = p - 1$ in Theorem 6.5, we see that there are $\phi(p - 1)$ elements of order $p - 1$ in U_p. Since $\phi(p - 1) \geq 1$, the group contains at least one element of this order. Now U_p has order $\phi(p) = p - 1$, so such an element is a generator for U_p, and hence this group is cyclic. □

Example 6.6

Let $p = 7$, so $U_p = U_7 = \{1, 2, 3, 4, 5, 6\}$. The divisors of $p-1 = 6$ are $d = 1, 2, 3$ and 6, and the sets of elements of order d in U_7 are respectively $\{1\}$, $\{6\}$, $\{2, 4\}$ and $\{3, 5\}$; thus the numbers of elements of order d are $1, 1, 2$ and 2 respectively, agreeing with the values of $\phi(d)$. To verify that 3 is a generator, note that

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1$$

in U_7, so every element of U_7 is a power of 3.

Exercise 6.6

Verify that the element 5 is a generator of U_7.

Exercise 6.7

Find the elements of order d in U_{11}, for each d dividing 10; which elements are generators?

Proof (Proof of Theorem 6.5.)

(In reading this proof, it may help to check each of its steps in a specific example, for instance by taking $p = 7$ or $p = 11$ throughout.) For each d dividing $p - 1$ let us define

$$\Omega_d = \{a \in U_p \mid a \text{ has order } d\} \quad \text{and} \quad \omega(d) = |\Omega_d|,$$

the number of elements of order d in U_p. Our aim is to prove that $\omega(d) = \phi(d)$ for all such d. Theorem 4.3 implies that the order of each element of U_p divides $p - 1$, so the sets Ω_d form a partition of U_p and hence

$$\sum_{d|p-1} \omega(d) = p - 1\,.$$

If we put $n = p - 1$ in Theorem 5.8 we get

$$\sum_{d|p-1} \phi(d) = p - 1\,,$$

so

$$\sum_{d|p-1} \big(\phi(d) - \omega(d)\big) = 0\,.$$

If we can show that $\omega(d) \leq \phi(d)$ for all d dividing $p - 1$, then each summand in this expression is non-negative; since their sum is 0, the summands must all be 0, so $\omega(d) = \phi(d)$, as required.

The inequality $\omega(d) \leq \phi(d)$ is obvious if Ω_d is empty, so assume that Ω_d contains an element a. By the definition of Ω_d, the powers $a^i = a, a^2, \ldots, a^d$ (= 1) are all distinct, and they satisfy $(a^i)^d = 1$, so they are d distinct roots of the polynomial $f(x) = x^d - 1$ in $\mathbb{Z}_p$; by Theorem 4.1, $f(x)$ has at most $\deg(f) = d$ roots in $\mathbb{Z}_p$, so these are a complete set of roots of $f(x)$. We shall show that Ω_d consists of those roots a^i with $\gcd(i, d) = 1$. If $b \in \Omega_d$ then b is a root of $f(x)$, so $b = a^i$ for some $i = 1, 2, \ldots, d$. If we let j denote $\gcd(i, d)$, then

$$b^{d/j} = a^{id/j} = (a^d)^{i/j} = 1^{i/j} = 1$$

in U_p; but d is the order of b, so no lower positive power of b than b^d can be equal to 1, and hence $j = 1$. Thus every element b of order d has the form a^i where $1 \leq i \leq d$ and i is coprime to d. The number of such integers i is $\phi(d)$, so the number $\omega(d)$ of such elements b is at most $\phi(d)$, and the proof is complete. □

Comments

1 The method of proof of Theorem 6.5 and Corollary 6.6 can be adapted slightly to prove a much stronger result, that if F is any field, so that $F^* = F \setminus \{0\}$ is a group under multiplication, then every finite subgroup G of F^* is cyclic. The idea is to let $|G| = n$, and to replace $p - 1$ with n in the above proof. Thus we use Theorem 5.8, that $\sum_{d|n} \phi(d) = n$, to show that for each d dividing n, G has $\phi(d)$ elements of order d; taking $d = n$ we see that G is cyclic. In number theory, the main interest is in the present case, where $F = \mathbb{Z}_p$ for some prime p and $G = \mathbb{Z}_p^* = U_p$, but the general result is also particularly useful in algebra, for instance when F is the field $\mathbb{C}$ of complex numbers.

2 The converse of Corollary 6.6 is false: for example the group U_4 is cyclic (generated by 3). We aim eventually to determine all the values of n for which U_n is cyclic, since cyclic groups are the easiest to work with. Having dealt with prime values of n, we next consider prime-powers, treating the odd case first.

6.3 The group U_{p^e}, where p is an odd prime

Theorem 6.7

If p is an odd prime, then U_{p^e} is cyclic for all $e \geq 1$.

Proof

Corollary 6.6 deals with the case $e = 1$, so we may assume that $e \geq 2$. We use the following strategy to find a primitive root mod p^e:

(a) first we pick a primitive root g mod (p) (possible by Corollary 6.6);

(b) next we show that either g or $g + p$ is a primitive root mod (p^2);

(c) finally we show that if h is any primitive root mod p^2, then h is a primitive root mod p^e for all $e \geq 2$.

Corollary 6.6 covers step (a), giving us a primitive root g mod (p). Thus $g^{p-1} \equiv 1 \bmod (p)$, but $g^i \not\equiv 1 \bmod (p)$ for $1 \leq i < p-1$. We now proceed to step (b).

Since $\gcd(g, p) = 1$ we have $\gcd(g, p^2) = 1$, so we can consider g as an element of U_{p^2}. If d denotes the order of g mod (p^2), then Euler's Theorem implies that d divides $\phi(p^2) = p(p-1)$. By definition of d, we have $g^d \equiv 1$ mod (p^2), so $g^d \equiv 1 \bmod (p)$; but g has order $p-1$ mod (p), so $p-1$ divides d. Since p is prime, these two facts imply that either $d = p(p-1)$ or $d = p-1$. If $d = p(p-1)$ then g is a primitive root mod (p^2), as required, so assume that $d = p-1$. Let $h = g + p$. Since $h \equiv g \bmod (p)$, h is a primitive root mod (p), so arguing as before we see that h has order $p(p-1)$ or $p-1$ in U_{p^2}. Since $g^{p-1} \equiv 1$ mod (p^2), the Binomial Theorem gives

$$h^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \cdots \equiv 1 - pg^{p-2} \bmod (p^2),$$

where the dots represent terms divisible by p^2. Since g is coprime to p, we have $pg^{p-2} \not\equiv 0$ mod (p^2) and hence $h^{p-1} \not\equiv 1$ mod (p^2). Thus h does not have order $p-1$ in U_{p^2}, so it must have order $p(p-1)$ and is therefore a primitive root. This completes step (b), but before proceeding to step (c), we look at an example of step (b).

Example 6.7

Let $p = 5$. We have seen that $g = 2$ is a primitive root mod (5), since it has order $\phi(5) = 4$ as an element of U_5. If we regard $g = 2$ as an element of $U_{p^2} = U_{25}$, then by the above argument its order d in U_{25} must be either $p(p-1) = 20$ or $p - 1 = 4$. Now $2^4 = 16 \not\equiv 1 \bmod (25)$, so $d \neq 4$ and hence $d = 20$. Thus $g = 2$ is a primitive root mod (25). (One can check this directly by computing the powers $2, 2^2, \ldots, 2^{20}$ mod (25), using $2^{10} = 1024 \equiv -1$ mod(25) to simplify the calculations.) Suppose instead that we had chosen $g = 7$; this is also a primitive root mod (5), since $7 \equiv 2 \bmod (5)$, but it is *not* a primitive root mod (25): we have $7^2 = 49 \equiv -1 \bmod (25)$, so $7^4 \equiv 1$ and hence 7 has order 4 in U_{25}. Step (b) guarantees that in this case, $g + p = 12$ must be a primitive root.

Exercise 6.8

Verify that 2 is a primitive root mod (25) by calculating its powers.

Proof (Continued.)

Now we consider step (c). Let h be any primitive root mod (p^2). We will show, by induction on e, that h is a primitive root mod (p^e) for all $e \geq 2$. Suppose, then, that h is a primitive root mod (p^e) for some $e \geq 2$, and let d be the order of h mod (p^{e+1}). An argument similar to that at the beginning of step (b) shows that d divides $\phi(p^{e+1}) = p^e(p-1)$ and is divisible by $\phi(p^e) = p^{e-1}(p-1)$, so $d = p^e(p-1)$ or $d = p^{e-1}(p-1)$. In the first case, h is a primitive root mod (p^{e+1}), as required, so it is sufficient to eliminate the second case by showing that $h^{p^{e-1}(p-1)} \not\equiv 1 \bmod (p^{e+1})$.

Since h is a primitive root mod (p^e), it has order $\phi(p^e) = p^{e-1}(p-1)$ in U_{p^e}, so $h^{p^{e-2}(p-1)} \not\equiv 1 \bmod (p^e)$. However $p^{e-2}(p-1) = \phi(p^{e-1})$, so $h^{p^{e-2}(p-1)} \equiv 1 \bmod (p^{e-1})$ by Euler's Theorem. Combining these two results, we see that $h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$ where k is coprime to p, so the Binomial Theorem gives

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

The dots here represent terms divisible by $(p^{e-1})^3$ and hence by p^{e+1}, since $3(e-1) \geq e+1$ for $e \geq 2$, so

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e + \frac{1}{2}k^2 p^{2e-1}(p-1) \bmod (p^{e+1}).$$

Now p is odd, so the third term $k^2 p^{2e-1}(p-1)/2$ is also divisible by p^{e+1}, since $2e-1 \geq e+1$ for $e \geq 2$. Thus

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e \bmod (p^{e+1}).$$

Since p does not divide k, we therefore have $h^{p^{e-1}(p-1)} \not\equiv 1 \bmod (p^{e+1})$, so step (c) is complete. (Notice where we need p to be odd: if $p = 2$ then the third term $k^2 p^{2e-1}(p-1)/2 = k^2 2^{2e-2}$ is not divisible by 2^{e+1} when $e = 2$, so the first step of the induction argument fails.) □

Comment

If g is a primitive root mod (p), where p is an odd prime, then g is *usually* a primitive root mod (p^2), in which case g is *always* a primitive root mod (p^e) for all e. For instance, $g = 2$ is a primitive root mod (5^e) for $e = 2$, and hence for all e.

Exercise 6.9

Show that 2 is a primitive root mod (3^e) for all $e \geq 1$.

Exercise 6.10

Find an integer which is a primitive root mod (7^e) for all $e \geq 1$.

6.4 The group U_{2^e}

We now deal with the powers of 2: in contrast with Theorem 6.7, we find that U_{2^e} is cyclic only for $e \leq 2$; in this sense, at least, the prime 2 is very odd!

Theorem 6.8

The group U_{2^e} is cyclic if and only if $e = 1$ or $e = 2$.

Proof

The groups $U_2 = \{1\}$ and $U_4 = \{1, 3\}$ are cyclic, generated by 1 and by 3, so it is sufficient to show that U_{2^e} is not cyclic for $e \geq 3$. We show that U_{2^e} has no elements of order $\phi(2^e) = 2^{e-1}$ by showing that

$$a^{2^{e-2}} \equiv 1 \bmod (2^e) \tag{6.1}$$

for all odd a. We prove this by induction on e. For the lowest value $e = 3$, (6.1) says that $a^2 \equiv 1 \bmod (8)$ for all odd a, and this is true since if $a = 2b + 1$ then $a^2 = 4b(b + 1) + 1 \equiv 1 \bmod (8)$. If we assume (6.1) for some exponent $e \geq 3$, then for each odd a we have

$$a^{2^{e-2}} = 1 + 2^e k$$

for some integer k. Squaring, we get

$$a^{2^{(e+1)-2}} = (1+2^e k)^2 = 1+2^{e+1}k+2^{2e}k^2 = 1+2^{e+1}(k+2^{e-1}k^2) \equiv 1 \bmod (2^{e+1}),$$

which is the required form of (6.1) for exponent $e+1$. Thus (6.1) is true for all integers $e \geq 3$, and the proof is complete. □

Exercise 6.11

Find the order of each element of U_{16}.

Exercise 6.12

Show that in U_{2^e} $(e \geq 3)$, the elements of order 2 are $2^{e-1} \pm 1$ and -1.

Despite Theorem 6.8, we will show that U_{2^e} is nearly cyclic for $e \geq 3$ in the sense that the element 5 is almost a primitive root. First we need some notation and a lemma.

Notation. Recall that if p is prime, then $p^e \parallel n$ means that n is divisible by p^e but not by p^{e+1}. Thus $2^2 \parallel 20$, $5 \parallel 20$, and so on.

Lemma 6.9

$2^{n+2} \parallel 5^{2^n} - 1$ for all $n \geq 0$.

Proof

We use induction on n. The result is trivial for $n = 0$. Suppose it is true for some $n \geq 0$. Now

$$5^{2^{n+1}} - 1 = \left(5^{2^n}\right)^2 - 1 = \left(5^{2^n} - 1\right)\left(5^{2^n} + 1\right),$$

with $2^{n+2} \parallel 5^{2^n} - 1$ by the induction hypothesis, and with $2 \parallel 5^{2^n} + 1$ since $5^{2^n} \equiv 1 \bmod (4)$. Combining the powers of 2 we get $2^{n+3} \parallel 5^{2^{n+1}} - 1$ as required. □

Theorem 6.10

If $e \geq 3$ then $U_{2^e} = \{\pm 5^i \mid 0 \leq i < 2^{e-2}\}$.

Proof

Let m be the order of the element 5 in U_{2^e}. By Euler's Theorem, m divides $\phi(2^e) = 2^{e-1}$, so $m = 2^k$ for some $k \leq e - 1$. Theorem 6.8 implies that U_{2^e} has no elements of order 2^{e-1}, so $k \leq e - 2$. By putting $n = e - 3$ in Lemma 6.9 we see that $2^{e-1} \parallel 5^{2^{e-3}} - 1$, so $5^{2^{e-3}} \not\equiv 1 \bmod (2^e)$ and hence $k > e - 3$. Thus $k = e - 2$, so $m = 2^{e-2}$. This means that 5 has 2^{e-2} distinct powers 5^i $(0 \leq i < 2^{e-2})$ in U_{2^e}. Since $5 \equiv 1 \bmod (4)$, these are all represented by

integers congruent to 1 mod (4). This accounts for exactly half of the 2^{e-1} elements $1, 3, 5, \ldots, 2^e - 1$ of U_{2^e}, and the other half, represented by integers congruent to -1 mod (4), must be the elements of the form -5^i. This shows that every element has the form $\pm 5^i$ for some $i = 0, 1, \ldots, 2^{e-2} - 1$, as required. □

Comment

The proof shows that the group U_{2^e} is generated by its elements -1 and 5, which individually generate cyclic subgroups of orders 2 and $m = 2^{e-2}$. These subgroups commute, and intersect in the identity subgroup, so they generate their direct product. Thus $U_{2^e} \cong C_2 \times C_{2^{e-2}}$ for $e \geq 3$, with the factors C_2 and $C_{2^{e-2}}$ generated by -1 and by 5 respectively. In terms of elements, this means that each $a \in U_{2^e}$ can be written uniquely in the form $a = (-1)^j 5^i$, where $j = 0, 1$ and $i = 0, 1, \ldots, 2^{e-2} - 1$.

Example 6.8

U_{16} consists of $1 = 5^4$, $3 = -5^3$, $5 = 5^1$, $7 = -5^2$, $9 = 5^2$, $11 = -5^1$, $13 = 5^3$, $15 = -5^4$.

Exercise 6.13

Show that if $e \geq 3$ then $U_{2^e} = \{\pm 3^i \mid 0 \leq i < 2^{e-2}\}$.

6.5 The existence of primitive roots

Having dealt with prime powers, we can now determine all the integers n for which there exist primitive roots mod (n).

Theorem 6.11

The group U_n is cyclic if and only if

$$n = 1,\ 2,\ 4,\ p^e \text{ or } 2p^e,$$

where p is an odd prime.

Proof

($\Leftarrow$) The cases $n = 1, 2$ and 4 are trivial, and Theorem 6.7 deals with the odd prime-powers, so we may assume that $n = 2p^e$ where p is an odd prime. Then Corollary 5.7 gives $\phi(n) = \phi(2)\phi(p^e) = \phi(p^e)$. By Theorem 6.7 there is a primitive root g mod (p^e). Then $g + p^e$ is also a primitive root mod (p^e), and one of g and $g+p^e$ is odd, so there is an odd primitive root h mod (p^e). We will show that h is a primitive root mod $(2p^e)$. By its construction, h is coprime to both 2 and p^e, so h is a unit mod $(2p^e)$. If $h^i \equiv 1$ mod $(2p^e)$, then certainly $h^i \equiv 1$ mod (p^e); since h is a primitive root mod (p^e), this implies that $\phi(p^e)$ divides i. Since $\phi(p^e) = \phi(2p^e)$, this shows that $\phi(2p^e)$ divides i, so h has order $\phi(2p^e)$ in U_{2p^e} and is therefore a primitive root. Before proving the converse part of the theorem, let us consider an example.

Example 6.9

We know that $g = 2$ is a primitive root mod (5^e) for all $e \geq 1$ (this follows from Example 6.7 and step (c) of the proof of Theorem 6.7). Now g is even, so $h = 2 + 5^e$ is an odd primitive root mod (5^e). The above argument then shows that h is also a primitive root mod (2.5^e). For instance, 7 is a primitive root mod (10), and 27 is a primitive root mod (50).

Proof (Continued.)

($\Rightarrow$) If $n \neq 1, 2, 4, p^e$ or $2p^e$, then either

(a) $n = 2^e$ where $e \geq 3$, or

(b) $n = 2^e p^f$ where $e \geq 2$, $f \geq 1$ and p is an odd prime, or

(c) n is divisible by at least two odd primes.

Theorem 6.8 shows that in case (a), U_n is not cyclic. Cases (b) and (c) are covered by the following result:

Lemma 6.12

If $n = rs$ where r and s are coprime and are both greater than 2, then U_n is not cyclic.

Proof

Since $\gcd(r,s) = 1$ we have $\phi(n) = \phi(r)\phi(s)$ by Theorem 5.6. Since $r, s > 2$, both $\phi(r)$ and $\phi(s)$ are even (see Exercise 5.7), so $\phi(n)$ is divisible by 4. It follows that the integer $e = \phi(n)/2$ is divisible by both $\phi(r)$ and $\phi(s)$. If a is a unit mod (n), then a is a unit mod (r) and also a unit mod (s), so $a^{\phi(r)} \equiv 1$ mod (r) and $a^{\phi(s)} \equiv 1$ mod (s) by Euler's Theorem. Since $\phi(r)$ and $\phi(s)$ divide e, we therefore have $a^e \equiv 1$ mod (r) and $a^e \equiv 1$ mod (s). Since r and s are coprime, this implies that $a^e \equiv 1$ mod (rs), that is, $a^e \equiv 1$ mod (n). Thus every element of U_n has order dividing e, and since $e < \phi(n)$, this means that there is no primitive root mod (n). □

Proof (Proof of Theorem 6.11, concluded.)

In case (b) we can take $r = 2^e$ and $s = p^f$, while in case (c) we can take $r = p^e \| n$ for some odd prime p dividing n, and $s = n/r$. In either case, $n = rs$ where r and s are coprime and greater than 2, so Lemma 6.12 shows that U_n is not cyclic. □

Exercise 6.14

Find an integer which is a primitive root mod (2.3^e) for all $e \geq 1$. Find an integer which is a primitive root mod (2.7^e) for all $e \geq 1$.

Theorem 6.11 tells us when U_n has a primitive root, and its proof, together with the proof of Theorem 6.7, shows us how to find one, provided we can first find a primitive root in U_p where p is an odd prime. Unfortunately, although Corollary 6.6 proves that U_p has a primitive root, it does not give us a specific example of one; the best we can do is to keep applying Lemma 6.4 to elements $a \in U_p$ until we find a primitive root.

6.6 Applications of primitive roots

In this chapter, we have determined when there is a primitive root mod (n), and in those cases where one does exist, we have shown how to find one. We will now consider some applications of primitive roots, specifically to solving congruences of the form $x^m \equiv c$ mod (n), where m, c and n are given, and x has to be found. We will do this by considering some typical examples, and then explaining how our methods extend to more general situations.

Example 6.10

Consider the congruence $x^4 \equiv 13 \bmod (17)$. First note that any solution x must be a unit mod (17), so x, like 13, is an element of U_{17}. By Corollary 6.6, this group is cyclic, so both x and 13 can be expressed as powers of a primitive root g mod (17). We saw earlier that 3 is a primitive root mod (17), so we will take $g = 3$. In general, there is no efficient way of expressing an arbitrary element, like 13, as a power of a primitive element g: we simply have to compute powers of g until the required element appears. In this case, $3^2 = 9, 3^3 = 27 \equiv 10$ and $3^4 = 81 \equiv 13 \bmod (17)$, so we have $13 = 3^4$ in U_{17}. We now write $x = 3^i$, where the exponent i is unknown. Then $x^4 = 3^{4i}$, so our congruence becomes $3^{4i} = 3^4$ in U_{17}. Now 3, being a primitive root, has order $\phi(17) = 16$, so $3^{4i} = 3^4$ if and only if $4i \equiv 4 \bmod (16)$, or equivalently $i \equiv 1 \bmod (4)$. The relevant values of i (between 0 and 15) are therefore $1, 5, 9$ and 13, so the solutions of the original congruence are $x \equiv 3, 3^5, 3^9$ and $3^{13} \bmod (17)$. We have seen that $3^4 \equiv 13$, so $3^5 \equiv 39 \equiv 5$. Instead of computing 3^9 and 3^{13}, we can take a short cut, and notice that if x is a solution then so is $-x$, so the remaining two classes of solutions must be $x \equiv -3 \equiv 14$ and $x \equiv -5 \equiv 12$. To summarise, there are four congruence classes of solutions, namely $x \equiv 3, 5, 12$ and 14 mod (17).

This example is typical of cases where there is a primitive root g mod (n): by writing $x = g^i$ and $c = g^b$, we convert the original non-linear congruence $x^m \equiv c \bmod (n)$ into a linear congruence $mi \equiv b \bmod \phi(n)$ of the type considered in Chapter 3. The techniques described there allow us to find all the relevant values of i, and hence to find all the solutions x of the original congruence. The only difficulties tend to be the rather tedious problems of finding a primitive root g, and then expressing c as a power of g.

Exercise 6.15

Solve the congruence $x^6 \equiv 4 \bmod (23)$.

The next example illustrates the methods available when there is not a primitive root mod (n).

Example 6.11

Consider the congruence $x^3 \equiv 1 \bmod (63)$. Since 63 factorises as $3^2 \times 7$, Theorem 6.11 shows that there is no primitive root mod (63), so the method of the previous example does not work here. Instead, we note that this congruence is equivalent to the pair of simultaneous congruences $x^3 \equiv 1 \bmod (9)$ and $x^3 \equiv 1 \bmod (7)$; we find the solutions of each of these congruences, using primitive roots

mod (9) and mod (7), and then we use Theorem 3.10 (the Chinese Remainder Theorem) to combine these solutions to get solutions of the original congruence.

We have seen that 2 is a primitive root mod (9). Writing $x = 2^i$ we see that $x^3 \equiv 1 \bmod (9)$ is equivalent to $2^{3i} \equiv 1 \bmod (9)$, and thus to $3i \equiv 0 \bmod (6)$, since 2 has order $\phi(9) = 6$ in U_9. The general solution of this is $i \equiv 0 \bmod (2)$, so $x^3 \equiv 1 \bmod (9)$ has general solution $x \equiv 2^0, 2^2, 2^4 \equiv 1, 4, 7 \bmod (9)$.

We have also seen that 3 is a primitive root mod (7), so by putting $x = 3^i$ we can rewrite $x^3 \equiv 1 \bmod (7)$ as $3^{3i} \equiv 1 \bmod (7)$; since 3 has order $\phi(7) = 6$ in U_7, this is equivalent to $3i \equiv 0 \bmod (6)$, so again $i \equiv 0 \bmod (2)$. Thus $x^3 \equiv 1 \bmod (7)$ has general solution $x \equiv 3^0, 3^2, 3^4 \equiv 1, 2, 4 \bmod (7)$.

We thus have three classes of solutions mod (9), and three classes mod (7). Since these moduli are coprime, the Chinese Remainder Theorem implies that each of these nine pairs of solutions gives rise to a single class of solutions mod (63): for instance, the pair of solutions $x \equiv 1 \bmod (9)$ and $x \equiv 1 \bmod (7)$ clearly correspond to the solution $x \equiv 1 \bmod (63)$ of the original congruence. By using the method of Chapter 3, we can solve the other eight pairs of simultaneous congruences (try this as an exercise!), and we find that the general solution is $x \equiv 1, 4, 16, 22, 25, 37, 43, 46, 58 \bmod (63)$. This gives another illustration of how Lagrange's Theorem (Theorem 4.1) on polynomials does not extend to composite moduli: the cubic polynomial $f(x) = x^3 - 1$ has nine roots in $\mathbb{Z}_{63}$.

Exercise 6.16

Solve the congruence $x^4 \equiv 4 \bmod (99)$.

Example 6.11 is typical of those cases where there is no primitive root: we factorise the modulus n, giving a set of simultaneous congruences modulo various prime-powers p^e; we solve these individually, and then combine their solutions by means of the Chinese Remainder Theorem. We have seen how to use primitive roots to solve congruences of the form $x^m \equiv c \bmod (p^e)$ when p is an odd prime; however, Theorem 6.8 shows that if $p = 2$ and $e \geq 3$ then there is no primitive root, so in this case we need another method. Again, we will illustrate this with a typical example.

Example 6.12

Consider the congruence $x^3 \equiv 3 \bmod (16)$. Since $16 = 2^4$, Theorem 6.8 implies that there is no primitive root mod (16); however, we know from Theorem 6.10 that every element of U_{16} has a unique expression of the form $\pm 5^i$ where $0 \leq i \leq 3$. By trial and error, we find that $5^3 = 125 \equiv -3 \bmod (16)$, so $3 = -5^3$ in U_{16}. If we write $x = \pm 5^i$ then the congruence becomes $(\pm 5^i)^3 \equiv -5^3$, that is,

$\pm 5^{3i} \equiv -5^3$. If we take the plus sign (so that $x = 5^i$), then we have $5^{3i} = -5^3$ in U_{16}; this is impossible, since the powers of 5 are all congruent to 1 mod (4). If we take the minus sign (so that $x = -5^i$), then $5^{3i} = 5^3$ in U_{16}; since 5 has order $\phi(16)/2 = 4$ in U_{16}, this is equivalent to $3i \equiv 3$ mod (4), that is, $i \equiv 1$ mod (4), so $x \equiv -5^1 \equiv 11$ mod (16). Thus there is a unique class of solutions, namely $x \equiv 11$ mod (16).

Exercise 6.17

Solve the congruence $x^{11} \equiv 7$ mod (32).

When solving congruences $x^m \equiv c$ mod (2^e), it is sometimes more convenient to write each element in the form $\pm 3^i$ (see Exercise 6.13), rather than $\pm 5^i$: for instance, in Example 6.12 it is a little easier to express $c = 3$ in the form $\pm 3^i$ than in the form $\pm 5^i$!

6.7 The algebraic structure of U_n

Theorem 6.11 tells us the integers n for which U_n is cyclic. For most values of n, this group is not cyclic, and it is also useful to determine its structure in these cases; indeed, we have already done this for $n = 2^e$ in Theorem 6.10 and the subsequent comment. We will show that the ring $\mathbb{Z}_n$ and the group U_n each have a factorisation as a direct product, which imitates the prime-power factorisation of the integer n (see Appendix B for rings and direct products). This reduces the study of U_n to the prime-power case, which we have already considered.

First we need to understand the relationship between the rings $\mathbb{Z}_l$ and $\mathbb{Z}_n$ when l divides n. If $l|n$ then $a \equiv a'$ mod (n) implies $a \equiv a'$ mod (l), so $[a]_n \subseteq [a]_l$. In fact, it is easy to verify that if $n = lm$ then

$$[a]_l = [a]_n \cup [a+l]_n \cup [a+2l]_n \cup \cdots \cup [a+(m-1)l]_n ,$$

so each class of $\mathbb{Z}_l$ is the disjoint union of m classes of $\mathbb{Z}_n$. For instance, if $l = 2$ and $n = 6$ (so $m = 3$) then

$$[0]_2 = [0]_6 \cup [2]_6 \cup [4]_6 \qquad \text{and} \qquad [1]_2 = [1]_6 \cup [3]_6 \cup [5]_6 .$$

We can therefore define an m-to-1 function $\phi = \phi_{n,l} : \mathbb{Z}_n \to \mathbb{Z}_l$ by sending each class of $\mathbb{Z}_n$ to the unique class of $\mathbb{Z}_l$ which contains it, that is, $\phi([a]_n) = [a]_l$. Now

$$\phi([a]_n \pm [b]_n) = \phi([a]_n) \pm \phi([b]_n) \quad \text{and} \quad \phi([a]_n.[b]_n) = \phi([a]_n).\phi([b]_n)$$

for all $[a]_n, [b]_n \in \mathbb{Z}_n$; for instance, $[a]_n + [b]_n = [a+b]_n$, so $\phi([a]_n + [b]_n) = \phi([a+b]_n) = [a+b]_l$, while $\phi([a]_n)+\phi([b]_n) = [a]_l+[b]_l = [a+b]_l$ also, with similar proofs for subtraction and multiplication. Thus ϕ takes sums, differences and products in $\mathbb{Z}_n$ to the corresponding operations in $\mathbb{Z}_l$; in algebra, one says that ϕ is a *homomorphism* between these two rings. If a is coprime to n then it is also coprime to l, so $\phi(U_n) \subseteq U_l$; the restriction of ϕ to U_n takes products in U_n to products in U_l, so it is a homomorphism $U_n \to U_l$ of groups. This situation is symmetric with respect to l and m, so we also obtain a ring-homomorphism $\phi' = \phi_{n,m} : \mathbb{Z}_n \to \mathbb{Z}_m$, $[a]_n \mapsto [a]_m$, which restricts to a group-homomorphism $U_n \to U_m$.

The direct product $\mathbb{Z}_l \times \mathbb{Z}_m$ is the set of all ordered pairs $([a]_l, [b]_m)$ where $[a]_l \in \mathbb{Z}_l$ and $[b]_m \in \mathbb{Z}_m$. We define addition, subtraction and multiplication of such ordered pairs by performing these operations on their components:

$$([a]_l, [b]_m) + ([a']_l, [b']_m) = ([a+a']_l, [b+b']_m)\,,$$

and so on. This makes $\mathbb{Z}_l \times \mathbb{Z}_m$ into a ring, and its subset $U_l \times U_m$ into a group. There is a ring-homomorphism $\theta : \mathbb{Z}_n \to \mathbb{Z}_l \times \mathbb{Z}_m$ given by $\theta([a]_n) = ([a]_l, [a]_m)$, which restricts to a group-homomorphism $U_n \to U_l \times U_m$.

We now show if that l and m are coprime (with $n = lm$ as before), then θ is an isomorphism, that is, in addition to being a homomorphism, it is a bijection. We have $n = \mathrm{lcm}(l, m)$, so the Chinese Remainder Theorem (Theorem 3.10) implies that, for each pair $([a]_l, [b]_m) \in \mathbb{Z}_l \times \mathbb{Z}_m$, there is a single congruence class x mod (n) of solutions of the simultaneous congruences $x \equiv a$ mod (l) and $x \equiv b$ mod (m). This means that there is exactly one class $[x]_n \in \mathbb{Z}_n$ such that $\theta([x]_n) = ([a]_l, [b]_m)$, so θ is a bijection. Thus θ is an ring-isomorphism

$$\mathbb{Z}_n \cong \mathbb{Z}_l \times \mathbb{Z}_m\,,$$

and it restricts to a group-isomorphism

$$U_n \cong U_l \times U_m\,.$$

An obvious extension of this argument, either by induction on k or using the full strength of the Chinese Remainder Theorem, proves the following theorem:

Theorem 6.13

If $n = n_1 \ldots n_k$ where $n_1, \ldots, n_k$ are mutually coprime, then there is a ring-isomorphism $\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ given by $\theta([a]_n) = ([a]_{n_1}, \ldots, [a]_{n_k})$, which restricts to a group-isomorphism $U_n \to U_{n_1} \times \cdots \times U_{n_k}$. In particular, if $n = p_1^{e_1} \ldots p_k^{e_k}$ where $p_1, \ldots, p_k$ are distinct primes, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}} \quad \text{and} \quad U_n \cong U_{p_1^{e_1}} \times \cdots \times U_{p_k^{e_k}}\,.$$

For instance, in solving the congruence $x^3 \equiv 1 \bmod (63)$ in Example 6.11, we used a pair of simultaneous congruences mod (9) and mod (7). In effect, we were using the isomorphism $U_{63} \cong U_9 \times U_7$, and working simultaneously in the two direct factors U_9 and U_7.

Theorem 6.13 describes the structure of U_n in terms of that of U_{p^e} for various prime-powers p^e. We know from Lemma 5.4 that U_{p^e} has order $\phi(p^e) = p^{e-1}(p-1)$ for all $e \geq 1$; if p is odd then U_{p^e} is cyclic, by Theorem 6.7, while Theorem 6.10 implies that $U_{2^f} \cong C_2 \times C_{2^{f-2}}$ for all $f \geq 2$, and U_2 is the identity group. Putting all this information together, we get the following description of U_n as a direct product of cyclic groups:

Corollary 6.14

If $2^f \| n$ then

$$U_n \cong \begin{cases} C_2 \times C_{2^{f-2}} \times \prod_{p^e \| n} C_{p^{e-1}(p-1)} & \text{if } f \geq 2, \text{ and} \\ \prod_{p^e \| n} C_{p^{e-1}(p-1)} & \text{if } f \leq 1, \end{cases}$$

where $\prod_{p^e \| n}$ denotes the direct product as p^e ranges over the odd prime-powers appearing in the prime-power factorisation of n.

Example 6.13

If $n = 784 = 2^4.7^2$, then $f = 4$ and there is a unique odd prime-power $p^e = 7^2$ in the factorisation of n, so $U_{784} \cong C_2 \times C_4 \times C_{42}$.

In general, one can further factorise the cyclic groups $C_{p^{e-1}(p-1)}$ appearing in Corollary 6.14 into direct products of cyclic groups of prime-power order, using the factorisation of $p^{e-1}(p-1)$: this depends on the group-theoretic result that $C_m \cong \prod_q C_q$, where q ranges over all the prime-powers in the factorisation of m (this follows by applying the isomorphism $\mathbb{Z}_m \cong \prod_q \mathbb{Z}_q$, given by Theorem 6.13, to the additive groups of these rings). For instance, $C_{42} \cong C_2 \times C_3 \times C_7$, so in Example 6.13 we have $U_{784} \cong C_2 \times C_4 \times C_2 \times C_3 \times C_7$. Note, however, that a cyclic group C_q of prime-power order cannot be factorised further as a direct product: for instance $C_4 \ncong C_2 \times C_2$, since C_4 has elements of order 4 whereas $C_2 \times C_2$ has none.

6.8 The universal exponent

The factorisation of U_n can be used to simplify large powers, in the same way as we used Euler's Theorem for this in Chapter 5. The *exponent* $e(G)$ of a finite group G is the least integer $e > 0$ satisfying $a^e = 1$ for all $a \in G$; the other integers with this property are the multiples of $e(G)$. Lagrange's Theorem implies that $a^{|G|} = 1$ for all $a \in G$, so $e(G)$ divides $|G|$. If we put $G = U_n$, of order $|U_n| = \phi(n)$, we get Euler's Theorem, that $a^{\phi(n)} = 1$ for all $a \in U_n$. The exponent $e(U_n)$ of U_n is called the *universal exponent* $e(n)$ of n; it divides $\phi(n)$, and it is the least positive integer e such that $a^e = 1$ for all $a \in U_n$. (Some authors use the notation $\lambda(n)$ for the universal exponent, but we will need the symbol λ for a different function in Chapter 9, Section 7.) If $e(n) < \phi(n)$ then the identity $a^{e(n)} = 1$ for all $a \in U_n$ is stronger, and often more useful than Euler's Theorem. Fortunately, it is easy to compute the exponent of U_n, or indeed of any finite abelian group G: simply express G as a direct product of cyclic groups, and take the least common multiple of their orders. In the case of U_n, Corollary 6.14 shows that $e(n)$ is the least common multiple of the numbers $e(2^f)$ and $e(p^e)$, where $2^f \| n$ and p^e ranges over the odd prime-powers in the factorisation of n; here $e(p^e) = \phi(p^e) = p^{e-1}(p-1)$ by Theorem 6.7, and $e(2^f) = 1, 2$ or 2^{f-2} as $f \leq 1, f = 2$ or $f \geq 3$ by Theorem 6.10.

Example 6.14

In Example 6.13 we saw that $U_{784} \cong C_2 \times C_4 \times C_{42}$; this group has order $\phi(784) = 2 \times 4 \times 42 = 336$, and exponent $e(784) = \text{lcm}(2, 4, 42) = 84$. In place of Euler's Theorem $a^{336} = 1$ we therefore have the stronger result $a^{84} = 1$ for all $a \in U_{784}$. For instance, if we want to calculate 3^{256} mod (784), then Euler's Theorem cannot be used directly, since $1 \leq 256 < 336$; however, $256 \equiv 4$ mod (84), so putting $a = 3$ we get $3^{256} \equiv 3^4 \equiv 81$ mod (784).

Exercise 6.18

Express U_{520} as a direct product of cyclic groups of prime-power order. Find $e(520)$, and hence calculate 11^{123} mod (520).

Exercise 6.19

Show that a finite abelian group G satisfies $e(G) = |G|$ if and only if G is cyclic. For which integers n is $e(n) = \phi(n)$?

Recall that a Carmichael number is a composite integer n such that $a^{n-1} \equiv 1 \bmod (n)$ for every $a \in U_n$. Lemma 4.8 states that if n is square-free, and if $p-1$ divides $n-1$ for each prime p dividing n, then n is either a prime or a Carmichael number. We can now use $e(n)$ to prove the converse of this, as promised in Chapter 4. Clearly any prime number has the stated properties, so we need to prove that Carmichael numbers also have them.

Theorem 6.15

If n is a Carmichael number then n is square-free, and $p-1$ divides $n-1$ for each prime p dividing n.

Proof

By the definition of a Carmichael number, $a^{n-1} \equiv 1 \bmod (n)$ for all $a \in U_n$, so $n-1$ is a multiple of $e(n)$. If $p^f \| n$ for some prime p and $f \geq 1$, then $e(n)$ is divisible by $e(p^f) = \phi(p^f) = p^{f-1}(p-1)$, so $p-1$ divides $n-1$. If $f > 1$, then this argument also shows that p divides $n-1$, which is impossible since p divides n; thus n must be square-free. □

Comment

This proof also shows that a Carmichael number n must be odd: since n is composite, we have $n > 2$, so $e(n)$ is even; since $e(n)$ divides $n-1$, this shows that n is odd.

Exercise 6.20

Show that a Carmichael number must be a product of at least three distinct primes.

6.9 Supplementary exercises

Exercise 6.21

Show that if there exists $a \in \mathbb{Z}$ such that $a^{p-1} \equiv 1 \bmod (p)$, whereas $a^{(p-1)/q} \not\equiv 1 \bmod (p)$ for each prime q dividing $p-1$, then p is prime and a is a primitive root mod (p). Hence show that the Fermat number $F_4 = 2^{2^4} + 1 = 65537$ is prime.

Exercise 6.22

Show that if p is prime, then $(p-2)! \equiv 1 \bmod (p)$. Show that if p is an odd prime, then $(p-3)! \equiv (p-1)/2 \bmod (p)$.

Exercise 6.23

Use Corollary 6.3 to show that there are infinitely many primes. (Take care to avoid a circular argument!)

Exercise 6.24

For which Fermat primes and Mersenne primes is 2 a primitive root?

Exercise 6.25

Find all the primitive roots for the integers $n = 18$ and 27. (Hint: see Exercises 6.4 and 6.5.)

Exercise 6.26

(a) Show that if p is an odd prime, and g is a primitive root mod (p) but not mod (p^2), then $g + rp$ is a primitive root mod (p^2) for $r = 1, 2, \ldots, p-1$. By counting primitive roots, deduce that if g is a primitive root mod (p) then exactly one of $g, g+p, g+2p, \ldots, g+(p-1)p$ is not a primitive root mod (p^2).

(b) Find elements of U_{25} congruent to $2, 3 \bmod (5)$ respectively, which are not primitive roots mod (25).