M 2 4 6

Number Theory

Workbook 3 (without solutions)

Primitive Roots and Discrete Logarithms

Summer 2013

(originally written and devised by
Trevor Hawkes and Alyson Stibbard;
revised in 2010 by John Cremona)

Aims of these workbooks:

(a) To encourage you to teach yourself mathematics from written material,

(b) To help you develop the art of independent study — working either alone, or co-operatively with other students,

(c) To help you learn a mathematical topic, in this case Number Theory, through calculation and problem-solving.

Copies of this workbook, both with and without solutions, can be found on Mathstuff.

Icons in this Workbook

The 'Section Targets' box contains an idea of what you should aim to get out of the current section. Perhaps you might return to this at the end to evaluate your progress.

Reaching this icon in your journey through the workbook is an indication that an idea should be starting to emerge from the various examples you have seen.

Material here includes reference either to earlier workbooks, or to previous courses such as foundations/Sets and Groups.

A caution. Watch your step over issues involved here.

Are You Ready?

To understand the material and do the problems in each section of this workbook, you will need to be on good terms with:

Section 1: • The Remainder theorem (for polynomials)
Section 3: • orders of elements in groups
• binomial expansions and induction

Note: You will need a pocket calculator for some of the questions in the workbooks, and are encouraged to use one for this purpose and to experiment with results and ideas in the course. Calculators are NOT needed and are NOT allowed in tests or in the examination.

These workbooks were orginally written and devised by *Trevor Hawkes and and Alyson Stibbard*. *Ben Carr* designed the LaTeX template and *Rob Reid* converted their drafts into elegant print. Over the years, other lecturers and students have corrected a number of typos, mistakes and other infelicities. In 2010 *John Cremona* made some substantial revisions.

Send corrections, ask questions or make comments at the module forum. You can join the MA246 forum by going to `http://forums.warwick.ac.uk/wf/misc/welcome.jsp` and signing in, clicking the *browse* tab, and then following the path: Departments > Maths > Modules > MA2xx modules > MA246 Number Theory.

1 Primitive Roots & Finite Logarithms

Motivation — a Worked Example

(a) Find a unit g in $\mathbb{Z}/11\mathbb{Z}$ whose powers generate the group of units $\mathbb{U}_{11}$, in other words, such that

$$\mathbb{U}_{11} = \{1, g, g^2, g^3, g^4, \ldots, g^9\}$$

(b) For each $u \in \mathbb{U}_{11}$, define $\ell(u)$ to be the smallest non-negative integer such that $g^{\ell(u)} = u$. Complete the following "log table":

u	1	2	3	4	5	6	7	8	9	10
$\ell(u)$										

Solution

(a) Since 11 is prime, $\mathbb{U}_{11}$ consists of all non-zero elements of $\mathbb{Z}/11\mathbb{Z}$; thus

$$\mathbb{U}_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

We now look at the set of powers $\{g^i : i \in \mathbb{N}\}$ for various choices of $g \in \mathbb{U}_{11}$. If $g = 1$, then $\{g, g^2, g^3, \ldots\} = \{1\}$, so 1 generates the identity subgroup of $\mathbb{U}_{11}$. We are looking for an element g which generates the whole group $\mathbb{U}_{11}$. Try $g = 2$; then $g^2 = 4, g^3 = 8, g^4 = 5$ (because $2^4 = 16 \equiv 5 \pmod{11}$), $g^5 = 10$ (because $2^5 = 2^4 \times 2 = 5 \times 2 = 10 \pmod{11}$), $g^6 = 9, g^7 = 7, g^8 = 3, g^9 = 6, g^{10} = 1 = g^0$. Thus, at our second attempt we have found a generator for $\mathbb{U}_{11}$, namely $g = 2$. If we tried $g = 3$, we would have found

$$\{3^i : i \in \mathbb{N}\} = \{3, 9, 5, 4, 1\}$$

which is a subgroup of $\mathbb{U}_{11}$ of order 5 (recall that $\mathbb{U}_{11}$ has order 10) and had we chosen $g = 10 (\equiv -1 \pmod{11})$, then we would have found

$$\{10^i : i \in \mathbb{N}\} = \{10, 1\}$$

a subgroup of $\mathbb{U}_{11}$ of order 2.

(b) We can now use the above calculation to complete the log table to the base 2, recalling that $\ell(u)$ is the smallest non-negative power of 2 congruent to u mod 11.

u	1	2	3	4	5	6	7	8	9	10
$\ell(u)$	0	1	8	2	4	9	7	3	6	5

Remark Recall that $\mathbb{U}_{11}$ has order $\phi(11) = 10$, and so an element g that generates $\mathbb{U}_{11}$ is simply an element of order 10 in the group $\mathbb{U}_{11}$. Observe that we have defined $\ell(1)$ to be zero rather than 11 to ensure that the "log" function ℓ takes values in the group $(\mathbb{Z}/10\mathbb{Z}, +)$, whose underlying set is $\{0, 1, \ldots, 9\}$.

(1.1) Definition An element g that generates the group $\mathbb{U}_n$ of units in $\mathbb{Z}/n\mathbb{Z}$ is called *a primitive root modulo n*.

(1.2) Remarks

(a) In the language of group theory, a primitive root is simply a generator for the multiplicative group of units $\mathbb{U}_n$ of $\mathbb{Z}/n\mathbb{Z}$. We have **not** yet proved that such a generator ever exists (except in the case $n = 11$, in the example above)! One of the goals of this workbook is to see which $n \in \mathbb{N}$ have primitive roots; in other words, to determine for which n the group $\mathbb{U}_n$ is cyclic.

(b) In general, cyclic groups have many generators; so when there exists a primitive root modulo n there will (in general) be many of them. We will count how many there are later.

(c) In the language of congruences a primitive root is viewed as an integer (not an element of $\mathbb{Z}/n\mathbb{Z}$) with the property that the set of its positive powers contains a complete set of residues for $\mathbb{U}_n$. Many authors of books on Number Theory use this definition.

How do we know that

$$0 \leq \ell(u) < \phi(n)?$$

(1.3) Definition Let g be a primitive root of $\mathbb{Z}/n\mathbb{Z}$. For all $u \in \mathbb{U}_n$, we define $\ell(u)$, the *logarithm* of u (to the base g) to be the smallest non-negative integer such that $g^{\ell(u)} = u$. We refer to the function

$$\ell : \mathbb{U}_n \to \mathbb{Z}/\phi(n)\mathbb{Z}$$

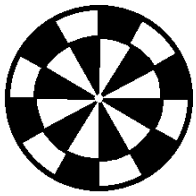
given by $u \mapsto \ell(u)$ as a *finite logarithm* or *discrete logarithm*. As we shall see, such functions share many properties with the standard logarithms.

Section Targets

(a) to investigate the question, 'for which values of n does $\mathbb{Z}/n\mathbb{Z}$ have a primitive root?'

(b) to study

- properties of the finite logarithm
- an interesting fact about Euler's phi-function
- the generators of cyclic groups
- the number of primitive roots
- some unsolved problems



Interesting Point

In those cases when $\mathbb{Z}/n\mathbb{Z}$ has a primitive root, it turns out that it has precisely $\phi(\phi(n))$ of them. You might like to think about why this is so.

(1.4) Questions about primitive roots

For the values,

(i) $n = 7$,

(ii) $n = 10$,

(iii) $n = 12$,

(a) list the elements of $\mathbb{U}_n$,

(b) work out the orders of each of these elements,

(c) use (b) to write down the primitive roots modulo n, if any exist,

(d) where appropriate, compare the number of primitive roots modulo n with the value $\phi(\phi(n))$.

(e) Calculate the log table to the base g, where g is the smallest primitive root in each case where a primitive root exists.

Answers to (1.4)

(a)(i)

(ii)

(iii)

(b)

(i)

(ii)

(iii)

(c)

(d)(i)

(ii)

(e)(i)

(ii)

(iii)

Good old Days

When the authors started school, pocket calculators had not been invented. In those days, school children used log tables for the real numbers to convert a multiplication task to one of addition. Here the log table modulo n (to a given base) allows us to carry out multiplication in $\mathbb{U}_n$ by adding in $\mathbb{Z}/\phi(n)\mathbb{Z}$. Finite log tables also play an important part in modern cryptography.

(1.5) Question about using log tables It is a fact that 197 is a prime and that 2 is a primitive root modulo 197. Write out the log table to the base 2 just for the values of $\ell(u) = 0, 1, 2, \ldots, 15$, and use it to work out the product 64×118 in $\mathbb{U}_{197}$ without carrying out the multiplication. Check your answer with your calculator.

Answer to (1.5)

(1.6) Theorem *Let g be a primitive root modulo n. Then the finite logarithm map (base g) defined in (1.3) is an isomorphism from the group $(\mathbb{U}_n, \times)$ to the group $(\mathbb{Z}/\phi(n)\mathbb{Z}, +)$.*

Let $(G, \bullet)$ and $(H, *)$ be two groups with binary operations $\bullet$ and $*$ respectively. A map $f : G \to H$ is called a *(group) homomorphism* if

$$f(g_1 \bullet g_2) = f(g_1) * f(g_2)$$

for all $g_1, g_2 \in G$. In words: "the image of a product is the product of the images".

If additionally f is a bijection, it is called an *isomorphism*.

Proof It is a general fact in group theory that any two *cyclic* groups of the same order m are isomorphic. Now $\mathbb{U}_n$ is a cyclic multiplicative group of order $m = \phi(n)$, with multiplicative generator g (by definition of primitive root); and $\mathbb{Z}/m\mathbb{Z}$ is a cyclic additive group with additive generator 1, so our Theorem is a special case of the general result.
To prove it directly, it is more convenient to work with the map $e : \mathbb{Z}/\phi(n)\mathbb{Z} \to \mathbb{U}_n$ defined by $l \mapsto e(l) = g^l$. This map is well-defined, since

$$\begin{aligned} l_1 \equiv l_2 \pmod{\phi(n)} &\implies l_2 = l_1 + k\phi(n) \\ &\implies g^{l_2} \equiv g^{l_1 + k\phi(n)} \\ &\equiv g^{l_1}(g^{\phi(n)})^k \equiv g^{l_1} \pmod{n} \end{aligned}$$

since $g^{\phi(n)} = 1$ by Euler's theorem.
It is a group homomorphism, since

$$e(l + l') = g^{l+l'} = g^l g^{l'} = e(l)e(l').$$

It is surjective, since by definition of primitive root every $a \in \mathbb{U}_n$ has the form $a = g^l = e(l)$ for some l. It must therefore also be injective, since $|\mathbb{Z}/\phi(n)\mathbb{Z}| = \phi(n) = |\mathbb{U}_n|$. One could also check directly that

$$g^{l_1} = g^{l_2} \implies l_1 \equiv l_2 \pmod{\phi(n)}.$$

Finally, the inverse of the map $e : l \mapsto g^l$ is just the discrete logarithm $\ell : g^l \mapsto l$. □

Note that it follows from the proof that

$$\ell(xy) = \ell(x) + \ell(y),$$

since if $x = g^{l_1}$ and $y = g^{l_2}$ then $xy = g^{l_1+l_2}$. It does not matter that $0 \le l_1 < \phi(n)$ and $0 \le l_2 < \phi(n)$ do not imply $0 \le l_1 + l_2 < \phi(n)$, since the values of ℓ lie in $\mathbb{Z}/\phi(n)\mathbb{Z}$ so only matter modulo $\phi(n)$.

We now prepare the way to proving the existence of primitive roots modulo *primes*.

(1.7) Question on divisors of n

For the values, (i) $n = 6$, (ii) $n = 8$, (iii) $n = 12$,

(a) write down all the divisors of n in increasing order, $d_1 = 1, d_2, \ldots, d_k = n$.

(b) write down the set

$$\left\{ \frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_k} \right\}$$

and compare it with the set $\{d_1, d_2, \ldots, d_k\}$

(c) work out the following sum,

$$\sum_{d|n} \phi(d) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_k) \qquad (1.a)$$

(d) work out the following sum

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) \qquad (1.b)$$

(e) make a conjecture (for general n) for the values of the sums labelled (1.a) and (1.b).

Answers to (1.7)

(a)

(b)

(c)(i)

(ii)

(iii)

(d)

(e)

(1.8) Question about HCFs Let s and n be integers. Prove that $\text{hcf}\{s, n\} = d$ if and only if $\text{hcf}\{\frac{s}{d}, \frac{n}{d}\} = 1$.

Answer to (1.8)

Notation Let n be a natural number and let $S = \{1, 2, \ldots, n\}$. Define

$$S_d = \{s \in S : \text{hcf}\{s, n\} = d\}$$

(1.9) Question on the meaning of this notation If $d \not| n$, then $S_d = \emptyset$. Therefore we are only interested in the sets S_d for divisors d of n.

(a) For (i) $n = 8$ and (ii) $n = 12$, write down the sets S_d for all d dividing n.

(b) Observe that the sets S_d form a partition of S (that is to say, a division of S into pairwise-disjoint subsets)

(c) In each case, compare $|S_d|$ with $\phi\left(\frac{n}{d}\right)$.

Answers to (1.9)

(a)(i)

(ii)

(b)

(c)(i)

(ii)

(1.10) Lemma *Let $n \in \mathbb{N}$ and let S_d denote the set*

$$S_d = \{s : 1 \leq s \leq n, \text{hcf}\{s, n\} = d\}$$

(a) *the sets S_d, such that $d|n$, partition the set $\{1, 2, \ldots, n\}$.*

(b) $|S_d| = \phi\left(\frac{n}{d}\right)$.

Proof

(a) Each element $s \in \{1, \ldots, n\}$ has a unique highest common factor with n and therefore belongs to one and only one of the sets S_d. This is precisely what we mean by saying that the subsets S_d form a partition of $\{1, \ldots, n\}$.

(b) By definition $s \in S_d$ if and only if $\text{hcf}\{s, n\} = d$ if and only if $\text{hcf}\{s/d, n/d\} = 1$ by (1.8). Therefore the number of elements in S_d is equal to the number of elements s_1 $(= s/d)$ which are relatively prime to n/d and this is equal to $\phi(n/d)$ by definition of the Euler phi-function.

Gauss was the first to discover and prove the following interesting property of the Euler phi-function.

(1.11) Proposition *If $n \in \mathbb{N}$ and $d_1, d_2, \ldots, d_k$ are the distinct divisors of n, then*

$$\begin{aligned} n &= \phi(d_1) + \phi(d_2) + \cdots + \phi(d_k) \\ &= \sum_{d|n} \phi(d) \end{aligned}$$

(1.12) Example
$9 = 1 + 2 + 6 = \phi(1) + \phi(3) + \phi(9) = \sum_{d|9} \phi(d)$.

Alternative proof
Consider the n fractions

$$\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}.$$

Reduce each to lowest terms: $\frac{i}{n}$ with $0 \le i < n$ reduces to $\frac{a}{d}$ with $0 \le a < d$ and $\mathrm{hcf}(a, d) = 1$.

Which integers d appear as denominators in the list? The divisors of n.

How many numerators a appear on top of each denominator d? $\phi(d)$.

How many fractions are there in the list? n.

Proof of (1.11) Since the sets S_d where $d|n$ partition the set $S = \{1, \ldots, n\}$, we have

$$\begin{aligned} n &= |S_{d_1}| + \cdots + |S_{d_k}| \qquad (1.c) \\ &= \sum_{d|n} |S_d| \\ &= \sum_{d|n} \phi\left(\frac{n}{d}\right) \end{aligned}$$

by (1.10)(b). As d runs through the divisors of n, so does $\frac{n}{d}$ (see (1.7)(b)), and therefore we can rearrange the sum as follows

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d) \qquad (1.d)$$

Equations (1.c) and (1.d) together yield the desired conclusion of Proposition 1.11 □

The next result, when expressed in the language of congruences, is due to Lagrange. It is simply a statement, for the field $\mathbb{Z}/p\mathbb{Z}$, of the well-known result that a polynomial of degree n has at most n distinct roots. This is true for polynomials over any **field**, but fails for polynomials over rings with zero-divisors. For example, the polynomial $x^2 - 1$ has 4 roots in $\mathbb{Z}/8\mathbb{Z}$ (count them!).

(1.13) Theorem *Let p be a prime and let*

$$q(x) = x^d + a_1x^{d-1} + \ldots + a_{d-1}x + a_d$$

be a polynomial of degree $d \geq 0$ with coefficients a_i in $\mathbb{Z}/p\mathbb{Z}$. Then $q(\alpha) = 0$ for at most d distinct values of α in $\mathbb{Z}/p\mathbb{Z}$.

Proof Since p is a prime, $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors; in other words, if $a, b \in \mathbb{Z}/p\mathbb{Z}$ with $a \neq 0$, and if $ab = 0$, then $b = 0$.
We use induction on the degree d. If $d = 0$ then $q(x)$ is the constant polynomial 1 which has no roots. Suppose that $d \geq 1$ and that the result holds for polynomials of degree $d - 1$.
If $q(x)$ has no roots in $\mathbb{Z}/p\mathbb{Z}$ that is fine since $0 \leq d$.
If $q(x)$ has a root a, then by the Remainder Theorem,

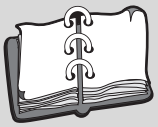
$$q(x) = (x - a)q_1(x)$$

for some polynomial $q_1(x)$ of degree $d-1$. Now $q_1(x)$ has at most $d - 1$ roots by induction, and every root b of $q(x)$ is either a root of $q_1(x)$ or is equal to a (or both), since

$$q(b) = (b - a)q_1(b) = 0 \iff b = a \text{ or } q_1(b) = 0.$$

(This is where we use the fact that $\mathbb{Z}/p\mathbb{Z}$ has no zero-divisors.) So the number of roots of $q(x)$ is at most $(d - 1) + 1 = d$ as required.

□



Recall that a *zero-divisor* a is a *non-zero* element (in some set with multiplication) for which there is a second non-zero element b such that $ab = 0$.
Dividing the polynomial $(x - a)$ into the polynomial $q(x)$ gives

$$q(x) = (x - a)q_1(x) + r,$$

where $q_1(x)$ is a polynomial of degree $d-1$ and $r \in \mathbb{Z}/p\mathbb{Z}$. Substituting $x = a$ gives $r = q(a)$. This is the *Remainder Theorem*. In particular, if a is a root of $q(x)$, then $r = 0$ and $q(x) = (x - a)q_1(x)$.

(1.14) Questions on generators for cyclic groups

(a) Let $G = \{g, g^2, g^3, g^4, g^5, g^6 = 1\}$ be a cyclic group of order 6, generated by g. Which elements of G are also generators of G (in other words, which elements of G have order 6)?

(b) Let $(\mathbb{Z}/8\mathbb{Z}, +)$ be the additive group of integers modulo 8. Which elements (if any) are generators?

(c) Make a conjecture about the number of generators in a cyclic group of order n.

Answers to (1.14)

(a)

(b)

(c)

The next result is a group-theoretical version of the frisbee question answered in Section 2 of Workbook 1.

(1.15) Lemma *Let g be a generator of a cyclic group G of order n. Then g^a is a generator of G if and only if* $\mathrm{hcf}\{a, n\} = 1$. *In particular, G has $\phi(n)$ generators.*

Proof If $\mathrm{hcf}\{a, n\} = d > 1$, then $(g^a)^{n/d} = (g^n)^{a/d} = (1)^{a/d} = 1$, and so the order of g^a is at most $n/d < n$, whence g^a is not a generator. Conversely, suppose that $\mathrm{hcf}\{a, n\} = 1$ and let $0 \leq b \leq n-1$. By Theorem 2.9 of Workbook 1, there exists an x such that $ax = b + kn$, and we get

$$(g^a)^x = g^{b+kn} = g^b g^{kn} = g^b (g^n)^k = g^b.$$

Hence every element g^b of G can be expressed as a power of g^a, and therefore g^a is a generator of G. □

We now have all the machinery in place to prove the main result in this section. In the language of group theory, it states that when p is a prime, the group of units $\mathbb{U}_p = \{1, 2, \ldots, p-1\}$ of $\mathbb{Z}/p\mathbb{Z}$ is cyclic.

(1.16) Euler-Lagrange-Legendre Theorem *For every prime p, there exist primitive roots modulo p. The number of primitive roots modulo p is $\phi(p-1)$.*

A generalization
Exactly the same proof shows that for every field F, every finite subgroup of the multiplicative group F^* of F is cyclic. [Just replace $p-1$ by the order of the group.]
For example, taking $F = \mathbb{C}$, we see that the only finite subgroups of $\mathbb{C}^*$ are the cyclic groups $\mu_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$, where $\zeta = e^{2\pi i/n}$, containing all nth roots of unity, for each $n \geq 1$.

Proof Let $f(d)$ denote the number of elements in $\mathbb{U}_p$ of order d. Since the order of each element in $\mathbb{U}_p = \{1, 2, \ldots, p-1\}$ is a natural number dividing $p-1$, it follows that

$$p - 1 = \sum_{d|p-1} f(d) \tag{1.e}$$

It therefore follows from Proposition 1.11 that

$$\sum_{d|p-1} f(d) = \sum_{d|p-1} \phi(d) \tag{1.f}$$

We will now show that

$$f(d) = \phi(d) \tag{1.g}$$

for each and every divisor d of $p-1$.

Case 1: $f(d) > 0$. Let a be an element of order d. Then a generates a cyclic subgroup $\{a, a^2, \ldots, a^d = 1\}$ of $\mathbb{U}_p$ and these d distinct elements are all roots of the equation $x^d - 1 = 0$. By Theorem 1.13, these are the *only* roots of this equation: so the elements of order d in $\mathbb{U}_p$ are all among these elements $\{a, a^2, \ldots, a^d\}$. But by Lemma 1.15 only $\phi(d)$ of these have order d, and so $f(d) = \phi(d)$ in this case, as required.

Case 2: $f(d) = 0$. Since $\phi(d) \geq 1$, we see that $f(d) < \phi(d)$. But this is impossible given equation 1.f and the result in Case 1.
Thus we can conclude that $f(d) = \phi(d)$ for *all* divisors d of $p-1$. In particular, $f(p-1) = \phi(p-1) \geq 1$ as claimed. □

Taking it further

(a) We saw in Question 1.4 that there is no primitive root modulo 12. In fact, it is easy to check that this is the second smallest value of n for which no primitive roots exist. In his *Disquisitiones Arithmeticae*, Gauss gave a complete description of which values of n have primitive roots. We will give this description, and prove it, later in this Workbook.

(b) For many primes, 2 is a primitive root (for the primes $3, 5, 11, 13, 29, 37, 53, 59, 61, 67$ and so on.) It is conjectured that, but not known whether 2 is a primitive root for infinitely many primes. We will see later in this Workbook how to test efficiently if a given integer a is a primitive root modulo a prime p.

(c) For a given n, let $\chi(n)$ denote the smallest (positive) primitive root modulo n. You might like to work out $\chi(23)$. For primes $p \leq 181$ it is known that $\chi(p) \leq 7$.

However $\chi(191) = 19$ and it is known that for any $M \in \mathbb{N}$, there exists a prime p with $\chi(p) > M$.

(d) In conclusion, you might like to try the following exercise: Let p be an odd prime, and let a be an integer satisfying

(a) $1 \leq a \leq p-1$, and

(b) $a \equiv b^2 \pmod{p}$ for some $b \in \mathbb{Z}$.

Show that a is not a primitive root modulo p. Artin has conjectured that all integers apart from ± 1 and perfect squares are primitive roots for infinitely many primes.

Summary of Section 1

Our main efforts have been directed towards proving the existence of primitive roots in a prime modulus. En route we looked at finite log tables for the units $\mathbb{U}_n$ of $\mathbb{Z}/n\mathbb{Z}$ and highlighted the fact that the two groups $(\mathbb{U}_n, \times)$ and $(\mathbb{Z}/\phi(n)\mathbb{Z}, +)$ are isomorphic when a primitive root exists. We showed that

- $\sum_{d|n} \phi(d) = n$,
- polynomials with coefficients in $\mathbb{Z}/p\mathbb{Z}$ can have no more distinct roots than their degree, and
- a cyclic group of order n has $\phi(n)$ distinct generators.

We then put these facts together to prove Theorem 1.16, sometimes called the 'theorem of the primitive root'.
In the next section we'll see how to actually find primitive roots modulo primes in practice.

2 Primitive Roots modulo primes

Given a prime p, Theorem 1.16 shows us that there exist primitive roots modulo p, but the proof of that theorem was not *constructive*: it does not tell us how to actually find a primitive root. So, how do we find one? We may assume that p is odd since $p = 2$ has $g = 1$ as primitive root (trivially, since $\mathbb{U}_1 = \{1\}$ is the trivial group).

Question
Why does it not make sense to test $a = 4$? Or any square?

(2.1) If we have a way of *testing* whether a given integer a is or is not a primitive root, then we can apply this test to $a = 2, 3, 5, 6, \ldots$ until we find one that works.
So, how do we test a candidate a for being a primitive root modulo p? the obvious thing to do is to list the powers

$$a, a^2, a^3, \ldots \pmod{p}$$

where each successive power is obtained by multiplying the previous one by a and then reducing modulo p, and making sure that the first time you get $a^k \equiv 1$ is for $k = p - 1$.

Question
Can you see how to halve the amount of work here? Why can you stop when $a^k \equiv -1 \pmod{p}$?

(2.2) Example: $p = 17$. the powers of 2 modulo 17 are, in order and reduced to lie between -8 and $+8$:

$$2, 4, 8, -1, -2, -4, -8, 1$$

so $2^8 \equiv 1 \pmod{17}$ and so $a = 2$ is *not* a primitive root modulo 17.
Taking $a = 3$ instead, we find the powers to be

$$3, -8, -7, -4, 5, -2, -6, -1, \ldots$$

which shows that the first power congruent to 1 is 3^{16}, so that 3 is a primitive root modulo 17.

(2.3) Find a primitive root modulo $p = 19$.

Answer to (2.3)

Using this method is time-consuming, and not very efficient: it takes about $p/2$ steps (assuming that you stop when you reach -1), so will be prohibitive when p is large. Also, we are not using to full advantage the strength of Lagrange's theorem, which says that the order of $a \pmod{p}$ must be a *divisor* of $p - 1$ (since $p - 1$ is the order of the

group $\mathbb{U}_p$). So we do not need to look at $a^k \pmod p$ for all exponents k, only for some of them.

(2.4) Let $p = 31$. List the divisors of $p - 1 = 30$. Suppose that $d \mid 30$ but $d \nmid 6$, $d \nmid 10$, $d \nmid 15$. What is d? Hence show that if $a \in \mathbb{U}_{31}$ and $a^6 \not\equiv 1$, $a^{10} \not\equiv 1$, $a^{15} \not\equiv 1 \pmod{31}$, then a is a primitive root modulo 31.

Answer to (2.4)

The point about the numbers $6, 10, 15$ in the previous example is that $6 = 30/5$, $10 = 30/3$, $15 = 30/2$, so these are the numbers $30/q$ where q is a *prime* factor of $30 = p - 1$.

This example generalizes to give a useful theorem:

(2.5) Theorem Let p be an odd prime, and let $q_1, q_2, \ldots, q_k$ be the prime divisors of $p - 1$. Suppose that a is coprime to p and satisfies

$$a^{(p-1)/q_i} \not\equiv 1 \pmod p \qquad \text{for } i = 1, 2, \ldots, k.$$

Then a is a primitive root modulo p.

This is a contrapositive proof. Make sure you understand its logic!

(2.6) Proof of Theorem 2.5: Justify the steps in the following argument, which proves the Theorem:

(a) If a is *not* a primitive root, then its order modulo p is $d = (p-1)/m$ for some $m > 1$.

(b) m is divisible by at least one of the q_i.

(c) So $\frac{p-1}{m} \mid \frac{p-1}{q_i}$ for at least one i.

(d) So $a^{(p-1)/q_i} \equiv 1$ for at least one i.

Answer to (2.6)

(a)

(b)

(c)

(d)

(2.7) Example: $p = 37$: $p-1 = 36 = 2^2 \cdot 3^2$ so $q_1 = 2$ and $q_2 = 3$. To test whether a is a primitive root modulo 37 we thus only need to check that $a^{12} \not\equiv 1$ and $a^{18} \not\equiv 1$. These can be computed in the order

$$a^2, a^3 = a \cdot a^2, a^6 = (a^3)^2, a^{12} = (a^6)^2, a^{18} = a^6 \cdot a^{12}.$$

Testing $a = 2$: $a^2 \equiv 4$, $a^3 \equiv 8$, $a^6 \equiv 8^2 = 64 \equiv -10$, $a^{12} \equiv (-10)^2 = 100 \equiv -11 \not\equiv 1$, $a^{18} \equiv (-10)(-11) = 110 \equiv -1 \not\equiv 1 \pmod{37}$. So 2 is a primitive root modulo 37.

(2.8) Example: $p = 257$: $p - 1 = 256 = 2^8$ so $q_1 = 2$ is the only relevant prime, and to test whether a is a primitive root modulo 257 we thus only need to check that $a^{128} \not\equiv 1$. We can compute a^{128} by repeated squaring.
Testing $a = 2$: note that $p = 2^8 + 1$, so $2^8 \equiv -1 \pmod{p}$ and $2^{16} \equiv 1$. So 2 is not a primitive root modulo 257.
Testing $a = 3$: we find $3^2 \equiv 9$, $3^4 \equiv 81$, $3^8 \equiv 81^2 \equiv 136$, $3^{16} \equiv (136)^2 = -8 = (-2)^3$, $a^{32} \equiv (-2)^6 = 2^6$, $a^{64} \equiv 2^{12} \equiv -2^4$ (since $2^8 \equiv -1$), $a^{128} \equiv 2^8 \equiv -1 \not\equiv 1 \pmod{257}$. So 3 is a primitive root modulo 257.

There are other tricks one can play to find primitive roots modulo primes. It is also possible to use the theory of primitive roots to prove that large primes really are primes!

Do not assume that p is prime just because it is called "p"!

(2.9) Let $p = 65537 = 2^{16} + 1$. Given that $3^{2^{15}} \equiv -1 \pmod{p}$ (which you do not need to check unless you really want to), show that p is prime.

Answer to (2.9)

Using this method, and a slightly more sophisticated version of it called the Pocklington Primality Test, it is quite easy to prove that enormous primes p actually are prime, provided that $p-1$ can be factorised. Try looking it up online if you are interested (there's a reasonably good article on Wikipedia.)

(2.10) More examples of primitive roots. Find the smallest primitive root for (a) $p = 29$; (b) $p = 31$; (c) $p = 41$.

Answer to (2.10)

(a)

(b)

(c)

Summary of Section 2

In this section we saw how to test efficiently whether or not a given integer a is or is not a primitive root modulo a given prime p, based on the factorization of $p-1$.
As an application, we saw how the same technique can be used to prove that primes are prime, without actually having to try to find factors.
In the next section we'll move on to considering primitive roots modulo composite numbers (numbers which are not prime).

3 Primitive Roots for other moduli

We have seen that every *prime* modulus has a primitive root, or in other words that $\mathbb{U}_p$ is cyclic for prime p. What about $\mathbb{U}_n$ for composite n? In this section we will prove that the only numbers n which have primitive roots are $n = p^e$ and $n = 2p^e$ where p is an odd prime and $e \geq 1$, as well as (trivially) $n = 1, 2$ and 4. This was proved by Gauss in his *Disquisitiones Arithmeticae*.

We will reach this goal by proving some *negative* statements, of the form

"if $n = \ldots$ then n does *not* have a primitive root",

and some *positive* statements of the form

"if $n = \ldots$ then n *does* have a primitive root".

The negative statements are easier, so we will do those first.

Powers of 2

Check these statements.

$\mathbb{U}_2 = \{1\}$ and $\mathbb{U}_4 = \{1, 3\}$ are cyclic, while $\mathbb{U}_8 = \{1, 3, 5, 7\}$ is not.
What about larger powers of 2?

(3.1) Multiple square roots

(a) Show that ± 1 and ± 9 are all solutions to $x^2 \equiv 1 \pmod{16}$.

(b) Show that ± 1 and ± 17 are all solutions to $x^2 \equiv 1 \pmod{32}$.

(c) Can you generalise?

Answer to (3.1)

Reminder
In a cyclic group of order N, for every $d \mid N$ the number of elements of order d is $\phi(d)$. We proved this in the first section of this Workbook (where?).

(3.2) The last question shows that when $m \geq 3$ we have (at least) four distinct solutions to the congruence $x^2 \equiv 1 \pmod{2^m}$, namely $x \equiv \pm 1$ and $x \equiv \pm(1 + 2^{m-1})$. This is enough to show that there cannot be a primitive root modulo $n = 2^m$! The reason is that if $\mathbb{U}_n$ were a cyclic group it could have only 1 element of order 2 in it, while we have found three (-1 and $\pm(1 + 2^{m-1})$). Hence the following result:

(3.3) Theorem For $m \geq 3$, the group $\mathbb{U}_{2^m}$ is not cyclic, and $n = 2^m$ has no primitive roots.

Taking it further The group $\mathbb{U}_{2^m}$, which has order 2^{m-1} is not cyclic; no element of the group has order as big as 2^{m-1}. But it is *almost* cyclic! It has elements of half the order, namely 2^{m-2}. And in fact 5 always has order 2^{m-2} modulo 2^m (for all $m \geq 2$). This is not too hard to prove: see if you can show, by induction on $k \geq 0$, that

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}$$

and take it from there.

Numbers with at least two prime factors

Leaving odd prime powers to one side for the moment, we now turn our attention to numbers which are not prime powers, i.e. numbers with two or more (distinct) prime factors. We will see that (with one type of exception) these never have primitive roots.

One way to see this is to use the "Chinese Remainder theorem Mark V" from Workbook 2 (see Corollary (3.4) there) and a fact from group theory that the direct product of two finite groups whose orders are not coprime is never cyclic. But we will work more directly with congruences instead.

Check that you understand this (see the following question). It follows from the Fundamental Theorem of Arithmetic.

(3.4) Let $n \in \mathbb{N}$. If n is not a prime power then there is a factorization $n = n_1 n_2$ where $n_1, n_2 > 1$ and the factors n_1, n_2 are *coprime*.

(3.5) Find such a factorization for $n = 6$, $n = 100$, $n = 250$ and $n = 2310$.

Answer to (3.5)

Properties of ϕ
Recall (from Workbook 2) what it means for ϕ to be multiplicative. We need $\text{hcf}(n_1, n_2) = 1$ here.

Can you remember why $\phi(m)$ is even for all $m \geq 3$?

(3.6) By the multiplicativity of ϕ we then have $\phi(n) = \phi(n_1)\phi(n_2)$. If we further assume that both $n_1, n_2 \geq 3$ then both $\phi(n_1)$ and $\phi(n_2)$ are *even*. So we can write

$$\frac{1}{2}\phi(n) = \left(\frac{1}{2}\phi(n_1)\right)\phi(n_2) = \phi(n_1)\left(\frac{1}{2}\phi(n_2)\right).$$

From this it will follow that

$$a^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{n} \qquad (*)$$

for all a coprime to n (improving on Euler's theorem for these n) so that n cannot have a primitive root: no a has order as large as $\phi(n)$.
It remains to justify the preceding claim, and to check exactly which integers n this all applies to.

(3.7) Example Let $n = 55 = 5 \cdot 11$, so that $\phi(n) = \phi(5)\phi(11) = 4 \cdot 10 = 40$. Show that, for all a coprime to 55,

(a) $a^4 \equiv 1 \pmod{5}$ and hence $a^{20} \equiv 1 \pmod{5}$;

(b) $a^{10} \equiv 1 \pmod{11}$ and hence $a^{20} \equiv 1 \pmod{11}$;

(c) $a^{20} \equiv 1 \pmod{55}$;

(d) a is not a primitive root modulo 55.

Answers to (3.7)

(3.8) Theorem Let $n = n_1 n_2$ where $n_1, n_2 \geq 3$ and $\text{hcf}(n_1, n_2) = 1$. Then n has no primitive roots.

(3.9) Proof of Theorem 3.8 As noted above, $\phi(n) = \phi(n_1)\phi(n_2)$, and both $\phi(n_1)$, $\phi(n_2)$ are even. Let $a \in \mathbb{N}$ be coprime to n; then a is also coprime to each of n_1, n_2. Now Euler's Theorem modulo n_1 gives

$$a^{\phi(n_1)} \equiv 1 \pmod{n_1}.$$

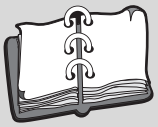
Raising to the integral power $\frac{1}{2}\phi(n_2)$ gives

$$a^{\frac{1}{2}\phi(n)} = \left(a^{\phi(n_1)}\right)^{\frac{1}{2}\phi(n_2)} \equiv 1 \pmod{n_1}.$$

Similarly, $a^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{n_2}$. Since $\text{hcf}(n_1, n_2) = 1$ the two congruences together imply that $a^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{n}$. So a has order at most $\frac{1}{2}\phi(n)$ and is therefore not a primitive root modulo n.

(3.10) Applying the Theorem Which numbers n does Theorem 3.8 apply to?

Answer to (3.10)



Recall the Chinese Remainder Theorem from Workbook 2.

As an alternative method of proof of Theorem 3.8 you can also use the same method as we used for powers of 2: if there is any solution to $x^2 \equiv 1 \pmod{n}$ other than ± 1, then n cannot have a primitive root. To find such an x when $n = n_1 n_2$ with n_1, n_2 coprime and ≥ 3, use the Chinese Remainder Theorem to find x such that both $x \equiv 1 \pmod{n_1}$ and also $x \equiv -1 \pmod{n_2}$. Details left to the reader!

Summary of "negative" results

The following numbers do *not* have primitive roots:

- powers of 2 (apart from 2 and 4);
- all numbers which are not of the form p^e or $2p^e$ where p is an odd prime and $e \geq 1$.

Odd prime powers

We now turn to proving some positive results. We will show that all the numbers not excluded in the previous subsection actually do have primitive roots.

Let p be an odd prime. We know by Theorem 1.16 that p has a primitive root, say g. Miraculously, it turns out that this same integer g is (almost) always a primitive root modulo *every* power of p, and also (almost) of $2p^e$.

We deal with the prime powers first, and start with $n = p^2$.

(3.11) Let p be an odd prime with primitive root g, and let $n = p^2$. What can we say about the order of g modulo p^2?

(3.12) Show that the order of g modulo p^2:

(a) is a divisor of $p(p-1)$;

(b) is a multiple of $p-1$;

(c) is either $p-1$ or $p(p-1)$.

Answers to (3.12)

(a)

(b)

(c)

Orders
If g is an element of some group and has order d, then g^e is the identity if and only $d \mid e$. Look this up if you need to.

So all we need to check to see if g is also a primitive root modulo p^2 is whether $g^{p-1} \equiv 1 \pmod{p^2}$. Even if this is the case, it is easy to fix:

(3.13) Theorem Let p be an odd prime and g a primitive root modulo p.
If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a primitive root modulo p^2.
Otherwise, if $g^{p-1} \equiv 1 \pmod{p^2}$, then $g+p$ is a primitive root modulo p^2.

(3.14) Proof of Theorem 3.13 The first part was proved above, so suppose that $g^{p-1} \equiv 1 \pmod{p^2}$. Set $g_1 = g + p$; since $g_1 \equiv g \pmod{p}$, g_1 is also a primitive root modulo p. So we just have to check that $g_1^{p-1} \not\equiv 1 \pmod{p^2}$. Using the binomial expansion,

$$\begin{aligned} g_1^{p-1} = (g+p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}p \\ &\equiv 1 - pg^{p-2} \pmod{p^2}, \end{aligned}$$

which is not 1 since $p \nmid g$.

(3.15) Examples modulo prime squares

(a) Show that 2 is a primitive root modulo 9, and also modulo 25.

(b) Find a primitive root modulo 49.

Answers to (3.15)

(a)

(b)

Once we have a primitive root modulo p^2, we are home and dry, since (as we will see) the same number is then automatically also a primitive root modulo *every* power of p.

We start with a primitive root g modulo p satisfying $g^{p-1} \not\equiv 1 \pmod{p^2}$. As we proved above, if the first primitive root modulo p fails the second condition, we just add p to it to get one which passes.

This is the key to the induction argument:

(3.16) Lemma. Let p be an odd prime and g a primitive root modulo p satisfying $g^{p-1} \not\equiv 1 \pmod{p^2}$. Show by induction that for all $e \geq 2$,

$$g^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}.$$

Answer to (3.16)

(3.17) Theorem Let g be a primitive root modulo the prime p, such that $g^{p-1} \not\equiv 1 \pmod{p^2}$. Then g is a primitive root modulo p^e for all $e \geq 1$.

(3.18) Proof of Theorem 3.17 Induction on e: true for $e = 1$ by hypothesis. Suppose true for $e-1$, i.e. that g is a primitive root modulo p^{e-1}. Let d be the order of g modulo p^e. As in an earlier proof, we have that d is a multiple of $\phi(p^{e-1}) = p^{e-2}(p-1)$ and a divisor of $\phi(p^e) = p^{e-1}(p-1)$, hence either $d = p^{e-2}(p-1)$ or $d = p^{e-1}(p-1)$. The first case is ruled out by the Lemma, so the second case holds, and this says that g has order $\phi(p^e)$ modulo p^e, so g is a primitive root modulo p^e.

(3.19) Examples modulo prime powers

(a) Show that 2 is a primitive root modulo 3^e and modulo 5^e for all $e \geq 1$.

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

Answers to (3.19)

(a)

(b)

(3.20) And finally... The only moduli n for which we have neither proved the existence of primitive roots nor shown that they do not exist are $n = 2p^e$ where p is an odd prime and $e \geq 1$. Since $\phi(2p^e) = \phi(2)\phi(p^e) = \phi(p^e)$, the groups $\mathbb{U}_{p^e}$ and $\mathbb{U}_{2p^e}$ have the same order, and it is almost true to say that any g which generates the first (i.e., which is a primitive root modulo p^e) also generates the second. The only problem is that g may be even and so not even in $\mathbb{U}_{2p^e}$!

(3.21)

(a) We know that 3 is a primitive root modulo 5. What is the order of 3 modulo 10?

(b) We know that 3 is a primitive root modulo 7. What is the order of 3 modulo 14?

(c) Given that 6 is a primitive root modulo 41, can you find a primitive root modulo 82?

(d) Find primitive root modulo 250.

Answer to (3.21)

(3.22) Theorem Let g be a primitive root modulo the prime p, such that g is odd and $g^{p-1} \not\equiv 1 \pmod{p^2}$. Then g is a primitive root modulo $2p^e$ for all $e \geq 1$.

(3.23) Proof of Theorem 3.22 By Theorem 3.17 we know that g has order $\phi(p^e)$ modulo p^e, so the smallest positive exponent k such that $g^k \equiv 1 \pmod{p^e}$ is $k = \phi(p^e)$. But since $g^k - 1$ is even for all $k > 0$,

$$g^k \equiv 1 \pmod{p^e} \iff g^k \equiv 1 \pmod{2p^e},$$

so the smallest k such that that $g^k \equiv 1 \pmod{2p^e}$ is also $k = \phi(p^e) = \phi(2p^e)$. So g is a primitive root modulo $2p^e$.

(3.24) To summarise this subsection: for any odd prime p, take any primitive root g modulo p. If $g^{p-1} \equiv 1 \pmod{p^2}$, replace g by $g+p$. Then g is a primitive root modulo p^e for all $e \geq 1$; if g is odd then g is also a primitive root modulo $2p^e$ for all $e \geq 1$, while if g is even then $g + p^e$ is a primitive root modulo $2p^e$ for all $e \geq 1$.

Taking it further

- Just as 5 has almost, but not quite, large enough order to be a primitive root modulo powers of 2, it is possible to show that for every odd prime p, the number $1+p$ has exact order p^{e-1} modulo p^e, for every $e \geq 1$. That is not enough for it to be a primitive root, since a primitive root has to have order $p^{e-1}(p-1)$. In fact, $p+1$ generates the subgroup of $\mathbb{U}_{p^e}$ consisting of the residues congruent to 1 (mod p), which has order p^{e-1} (just as 5 generates the subgroup of $\mathbb{U}_{2^e}$ consisting of the residues which are congruent to 1 (mod 4)).

  You can try to prove this, by first proving by induction on $e \geq 2$ that

  $$(1+p)^{p^{e-2}} \equiv 1 + p^{e-1} \pmod{p^e}.$$

- It is actually quite hard to find primes p whose smallest primitive root g satisfies $g^{p-1} \equiv 1 \pmod{p^2}$. One example is $p = 40487$, for which $g = 5$ is the smallest primitive root and $5^{40486} \equiv 1 \pmod{40487}$.

  In the case $g = 2$, primes p such that $2^{p-1} \equiv 1 \pmod{p^2}$ are very special and also rare: they are called Wieferich primes, after Arthur Wieferich (1909) who encountered them in trying to prove Fermat's Last Theorem with exponent p. Only two are known, but it is an unsolved problem to decide whether or not there are infinitely many of them! The smallest is $p = 1093$. Can you find the only other known example?

Summary of Section 3

In this section we have given a complete answer to the question

which $n \in \mathbb{N}$ have primitive roots?

The answer is:

$$n = 1, 2, 4,\ n = p^e \text{ and } n = 2p^e \text{ for } p \text{ any odd prime.}$$

We also saw that (almost) every primitive root modulo p is also a primitive root modulo p^e and $2p^e$.