Section 10

Primitive roots

Week 7

Warning: The work is getting harder all the time. Don't fall behind.

10.1 The Order of a modulo m

By now we know that

$$\phi(12) = \phi(2^2)\phi(3) = 2^1(3-1) = 4,$$

and indeed, 1, 5, 7 and 11 are the only least residues (mod 12) relatively prime to 12. Hence by Euler's Theorem (Theorem 9.1), whenever $(a, 12) = 1$, that is, the least residue of a is one of the numbers $1, 5, 7, 11$, we have $a^4 \equiv 1 \pmod{12}$. However, we also have

$$\begin{aligned} 1^2 &\equiv 1 \pmod{12} \\ 5^2 &\equiv 25 \equiv 1 \pmod{12} \\ 7^2 &\equiv 49 \equiv 1 \pmod{12} \\ 11^2 &\equiv 121 \equiv 1 \pmod{12}. \end{aligned}$$

Thus, although it is true that $a^{\phi(12)} \equiv 1 \pmod{12}$ if $(a, 12) = 1$, it is not true that $\phi(12)$ is the *smallest* positive integer t such that $a^t \equiv 1 \pmod{12}$.

Definition

If $(a, m) = 1$, then the smallest positive integer t such that $a^t \equiv 1 \pmod{m}$ is called the **order** of a modulo m, written $\operatorname{ord}_m a$.

Example: Since $\phi(9) = 6$, we know that $4^6 \equiv 1 \pmod{9}$, but what is the order of 4 modulo 9? We know that it is at most 6, but is there a smaller integer t such that $4^t \equiv 1 \pmod{9}$?

Yes, $\text{ord}_9\, 4 = 3$ because

$$4^2 \equiv 16 \equiv 7 \pmod{9},$$
$$4^3 \equiv 28 \equiv 1 \pmod{9}.$$

Recall that $\phi(13) = 12$ and consider the least residues of $a^n \pmod{13}$ for $a, n \in \{1, 2, ..., 12\}$.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	**1**
3	9	**1**	3	9	1	3	9	1	3	9	1
4	3	12	9	10	**1**	4	3	12	9	10	1
5	12	8	**1**	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	**1**
7	10	5	9	11	12	6	3	8	4	2	**1**
8	12	5	**1**	8	12	5	1	8	12	5	1
9	3	**1**	9	3	1	9	3	1	9	3	1
10	9	12	3	4	**1**	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	**1**
12	**1**	12	1	12	1	12	1	12	1	12	1

Table 10.1: Least residues of $a^n \pmod{13}$ for $a, n \in \{1, 2, ..., 12\}$

There are two questions to be considered:

?1 Which powers of a are congruent to 1 (mod 13)? Compare them with the order (the powers of a in the columns with boldfaced 1s) of $a \pmod{13}$.

?2 Which numbers occur as orders of $a \pmod{13}$? Compare them with $\phi(13)$.

These questions are answered in the next two theorems.

Theorem 10.1 *If* $(a, m) = 1$ *and* $\text{ord}_m\, a = t$, *then* $a^n \equiv 1 \pmod{m}$ *if and only if* $t|n$.

Proof.
If $n = tq$ for some $q \in \mathbb{Z}$, then

$$a^n \equiv a^{tq} \equiv (a^t)^q \equiv 1^q \equiv 1 \pmod{m}.$$

Conversely, suppose $a^n \equiv 1 \pmod{m}$. Since t is the smallest positive integer such that $a^t \equiv 1 \pmod{m}$, we have $n \geq t$. Dividing n by t we get

$$n = tq + r \text{ for some } q \geq 1 \text{ and } 0 \leq r < t.$$

Thus

$$1 \equiv a^n \equiv a^{tq+r} \equiv (a^t)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}.$$

Since t is the smallest positive integer such that $a^t \equiv 1 \pmod{m}$, $a^r \equiv 1 \pmod{m}$ with $0 \leq r < t$ is only possible if $r = 0$. Thus $n = tq$ and the result follows. ■

Theorem 10.2 *If* $(a, m) = 1$ *and* $\operatorname{ord}_m a = t$, *then* $t | \phi(m)$.

Proof.
By Euler's Theorem (Theorem 9.1), $a^{\phi(m)} \equiv 1 \pmod{m}$ and so by Theorem 10.1, $t | \phi(m)$. ■

Example: Determine $\operatorname{ord}_{18} 5$ and $\operatorname{ord}_{13} 2$.

Solution

First determine $\phi(18)$: Since $18 = 2 \cdot 3^2$, $\phi(18) = 18(\frac{1}{2})(\frac{2}{3}) = 6$. By Theorem 10.2, the only possible orders of $5 \pmod{18}$ are 1, 2, 3 or 6.

Obviously $\operatorname{ord}_{18} 5 \neq 1$. Since $5^2 \equiv 7 \pmod{18}$, $5^3 \equiv 7 \times 5 \equiv 17 \equiv -1 \pmod{18}$, and $5^6 \equiv 17^2 \equiv (-1)^2 \equiv 1 \pmod{18}$, $\operatorname{ord}_{18} 5 = 6$.

Determine $\phi(13)$: Since 13 is prime, $\phi(13) = 12$. By Theorem 10.2, the only possible orders of $2 \pmod{13}$ are 1, 2, 3, 4, 6 or 12. Since $2^2 \equiv 4 \pmod{13}$, $2^3 \equiv 8 \pmod{13}$, $2^4 \equiv 3 \pmod{13}$, $2^6 \equiv 3 \times 2^2 \equiv 12 \equiv -1 \pmod{13}$, $\operatorname{ord}_{13} 2 = 12 = \phi(13)$.

(**Note:** This shows that $(\mathbb{Z}_{13} - \{[0]\}, \cdot)$ is a cyclic group with generator $[2]$.)

The previous two theorems have a very useful application:

Theorem 10.3 *If* p *and* q *are odd primes and* $q | (a^p - 1)$, *then either* $q | (a - 1)$ *or* $q = 2kp + 1$ *for some integer* k.

Proof.
Since $q|(a^p - 1)$, we have $a^p \equiv 1 \pmod{q}$. By Theorem 10.1, $\text{ord}_q\, a|p$. This means that a has order 1 or $p \pmod{q}$.

- If the order is 1, then $a \equiv 1 \pmod{q}$ and so $q|(a-1)$.
- If the order of $a \pmod{q}$ is p, then by Theorem 10.2, $p|\phi(q)$. But $\phi(q) = q - 1$ since q is prime, hence $p|(q-1)$. Then $q - 1 = rp$ for some integer r. Since $q - 1$ is even, it follows that $r = 2k$ for some integer k and we therefore have shown that $q = 2kp + 1$.

■

Corollary 10.1 *Any prime divisor of $2^p - 1$ is of the form $2kp + 1$.*

This means that to test whether a number $2^p - 1$ is a Mersenne prime, we only have to consider as possible divisors of $2^p - 1$ the prime numbers of the form $2kp + 1$.

Example: Suppose we want to factor $2^{19} - 1$. What is the smallest possible prime number that we need to consider?

Solution
Any positive divisor (prime or otherwise) of $2^{19} - 1$ is of the form $38k + 1$, $k \in \mathbb{N}$.

k	1	2	3	4	5
$38k+1$	39	77	115	153	191

Of these, only 191 is prime, so the smallest possible prime divisor (hence the smallest possible proper divisor) of $2^{19} - 1$ is 191. (Continuing in this way, and only calculating $2^{19} \pmod{p}$ if p is a prime of the form $38k + 1 < \sqrt{2^{19} - 1}$, we soon show that $2^{19} - 1 = 524\,287$ is prime.)

Another application of Theorems 10.1 and 10.2 gives the following criterion for an integer to be prime.

Theorem 10.4 *Let $m > 1$ and suppose that for every prime factor p of $m - 1$ there is an integer a such that*

(*i*) $a^{m-1} \equiv 1 \pmod{m}$ *and*

(*ii*) $a^{(m-1)/p} \not\equiv 1 \pmod{m}$.

Then m is prime.

Proof.
To show m is prime we need only show that $\phi(m) = m - 1$, which would follow if we can prove that $(m-1)|\phi(m)$.
Suppose this is not the case. Then there is a prime p and an exponent $r > 0$ such that $p^r|(m-1)$, but $p^r \nmid \phi(m)$. Since $p^r|(m-1)$, $m - 1 = p^r k$ for some integer k. By the hypothesis, for this prime p there exists an integer a that satisfies conditions (i) and (ii) above.

Note that (i) is only possible if $(a, m) = 1$, otherwise $(a, m) \nmid 1$. Therefore $\text{ord}_m a$ is defined. Let $t = \text{ord}_m a$. By Theorem 10.2, $t|\phi(m)$. From Theorem 10.1 and (i), $t|(m-1)$, that is, $t|p^r k$. This means that t is of the form $t = p^s d$, where $s \leq r$ and $d|k$. But from Theorem 10.1 and (ii), $t \nmid (m-1)/p$, that is, $p^s d \nmid p^{r-1}k$. Since $d|k$, it follows that $p^s \nmid p^{r-1}$. But this implies that $s \geq r$, that is, $p^r|t$. But $t|\phi(m)$ and so $p^r|\phi(m)$, a contradiction.

■

Even though this test itself is impractical if m is large (because one has to find an a for *every* prime factor p of $m-1$), Theorem 10.4 is the basis of all modern primality tests whether they are as simple as the test above or something as elaborate such as the methods using elliptic curves or number fields.

Note that if m is prime, then (i) in the statement of Theorem 10.4 holds – it is Fermat's Theorem. After studying the next section we will also know that (ii) holds if m is prime, hence Theorem 10.4 gives a necessary and sufficient condition for a number to be prime.

Theorem 10.5 *If* $\text{ord}_m a = t$, *then*

$$a^r \equiv a^s \pmod{m} \text{ if and only if } r \equiv s \pmod{t}.$$

Proof.
Suppose $a^r \equiv a^s \pmod{m}$. We may assume that $r \geq s$ (for otherwise we just switch r and s). Also, $(a, m) = 1$ (otherwise $\text{ord}_m a$ is not defined) and so we may divide both sides of the congruence by a^s to get $a^{r-s} \equiv 1 \pmod{m}$. By Theorem 10.1, $t|(r-s)$ and thus $r \equiv s \pmod{t}$.

Conversely, suppose $r \equiv s \pmod{t}$. Then $r = kt + s$ for some integer k, and

$$a^r \equiv a^{kt+s} \equiv (a^t)^k a^s \equiv a^s \pmod{m}$$

because $a^t \equiv 1 \pmod{m}$. ■

10.2 Primitive Roots

Let $\Phi(m)$ denote the set of least residues of m that are relatively prime to m. Then $|\Phi(m)| = \phi(m)$.

If $a \in \Phi(m)$ and $\text{ord}_m a = \phi(m)$, then a is called a **primitive root** of m.

Example: Recall that $\phi(9) = \phi(3^2) = 3(3-1) = 6$. Also, checking only the powers of 2 that are divisors of 6 (WHY?), we see that

$$2^2 \equiv 4 \pmod 9, \quad 2^3 \equiv -1 \pmod 9, \quad 2^6 \equiv (-1)^2 \equiv 1 \pmod 9,$$

thus 2 is a primitive root of 9.

Theorem 10.6 *If g is a primitive root of m, then the least residues, modulo m, of*

$$g, \ g^2, ..., \ g^{\phi(m)} \tag{10.1}$$

are a permutation of the elements of $\Phi(m)$.

Proof.
Since $(g, m) = 1$, $(g^k, m) = 1$ for each $k = 1, 2, ..., \phi(m)$. Thus the least residues of the numbers in (10.1) are all relatively prime to m, hence they are elements of $\Phi(m)$. There are $\phi(m)$ numbers in (10.1), so we only have to show that no two of them have the same least residues (mod m).
Suppose

$$g^k \equiv g^j \pmod m$$

for some integers $1 \le k \le \phi(m)$ and $1 \le j \le \phi(m)$. We want to prove that $k = j$.

Since g is a primitive root of m, $\text{ord}_m g = \phi(m)$. By Theorem 10.5, $k \equiv j \pmod{\phi(m)}$.

If $k, j < \phi(m)$, then they are least residues (mod $\phi(m)$) and so they are equal. If one of them, say k, is equal to $\phi(m)$, then the only number in $\{1, 2, ..., \phi(m)\}$ congruent to k is $\phi(m)$, and so $j = \phi(m)$ also. ■

★ We say that the primitive root g of m **generates** $\Phi(m)$.

★ It was proved in Lemma 9(b) that $\Phi(m)$ is closed under multiplication modulo m. From this (and other properties) it follows that $\Phi(m)$ is a group under this operation. Theorem 10.6 now shows that if m has a primitive root, then this group is cyclic, i.e. generated by a single element.

Example: Once again, $\phi(9) = 6$; indeed, $\Phi(9) = \{1, 2, 4, 5, 7, 8\}$. We've seen before that 2 is a primitive root of 9 and that

$$2^1 \equiv 2 \pmod 9, \quad 2^2 \equiv 4 \pmod 9, \quad 2^3 \equiv 8 \pmod 9,$$
$$2^4 \equiv 7 \pmod 9, \quad 2^5 \equiv 5 \pmod 9, \quad 2^6 \equiv 1 \pmod 9,$$

so 2 generates all the least residues (mod 9) relatively prime to 9.

10.3 Finding Primitive Roots

? If g is a primitive root of m, which of the $\phi(m)$ numbers g, g^2, ..., $g^{\phi(m)}$ are also primitive roots of m?

To answer this question, we first prove a lemma.

Lemma 10.1 *Suppose* $\operatorname{ord}_m a = t$. *Then* $\operatorname{ord}_m a^k = t$ *if and only if* $(k,t) = 1$.

Proof. Suppose $(k,t) = 1$ and let $s = \operatorname{ord}_m a^k$. We want to prove that $s = t$. We have $a^t \equiv 1 \pmod{m}$, hence

$$1 \equiv (a^t)^k \equiv (a^k)^t \pmod{m}.$$

By Theorem 10.1 applied to a^k, $s|t$. Also, since $s = \operatorname{ord}_m a^k$,

$$1 \equiv (a^k)^s \equiv a^{ks} \pmod{m}.$$

By Theorem 10.1 applied to a, $t|ks$. Since $(k,t) = 1$, it follows that $t|s$ and so $t = s$.

Conversely, suppose $\operatorname{ord}_m a = \operatorname{ord}_m a^k = t$ and $(k,t) = d$. Then $a^t \equiv 1 \pmod{m}$, and k/d and t/d are integers, hence

$$1 \equiv a^t \equiv (a^t)^{k/d} \equiv (a^k)^{t/d} \pmod{m}.$$

But $t = \operatorname{ord}_m a^k$, thus by Theorem 10.1 applied to a^k, t/d is a multiple of t. This is only possible if $d = 1$ and it follows that $(k,t) = 1$. ■

Corollary 10.2 *If* g *is a primitive root of* m, *then the least residue of* $g^k \pmod{m}$ *is a primitive root of* m *if and only if* $(k, \phi(m)) = 1$.

Proof.
If g is a primitive root of m, then by definition g has order $\phi(m) \pmod{m}$. By Lemma 10.1, g^k has order $\phi(m) \pmod{m}$ (thus its least residue is a primitive root of m) if and only if $(k, \phi(m)) = 1$. ■

▼ This shows that if we can find **one** primitive root g of m, then we can find **all of them**, because

(*i*) g generates $\Phi(m)$ (as g^k for some $k = \{1, 2, ..., \phi(m)\}$),

(*ii*) the primitive roots of m are contained in $\Phi(m)$ (by definition), and

(*iii*) we know that the least residue of g^k is a primitive root of m if and only if $(k, \phi(m)) = 1$.

(*iv*) Moreover, there are $\phi(\phi(m))$ integers in $\{1, 2, ..., \phi(m)\}$ relatively prime to $\phi(m)$, so if m has primitive roots, then it has $\phi(\phi(m))$ primitive roots.

Example: We know from before that 2 is a primitive root of 9 and that $\phi(9) = 6$. So, by the corollary, the following numbers should be the only primitive roots of 9: the least residues of 2^k for $k \in \{1, 2, ..., 6\}$ and $(k, 6) = 1$, i.e.

$$2^1 \equiv 2 \pmod{9} \quad \text{and} \quad 2^5 \equiv 5 \pmod{9}.$$

Indeed (checking only the exponents that are divisors of 6),

$$5^2 \equiv 7 \pmod{9}, \quad 5^3 \equiv 5 \cdot 7 \equiv -1 \pmod{9}, \quad 5^6 \equiv (5^3)^2 \equiv (-1)^2 \equiv 1 \pmod{9},$$

while

$$\begin{aligned}
&(2^2)^2 \equiv 7 \pmod{9}; \quad (2^2)^3 \equiv 2^6 \equiv 1 \pmod{9}, \quad \text{i.e. } \operatorname{ord}_9 2^2 = 3,\\
&(2^3)^2 \equiv 2^6 \equiv 1 \pmod{9}, \quad \text{i.e. } \operatorname{ord}_9 2^3 = 2,\\
&(2^4)^2 \equiv 4 \pmod{9}; \quad (2^4)^3 \equiv 2^{12} \equiv (2^6)^2 \equiv 1 \pmod{9}, \quad \text{i.e. } \operatorname{ord}_9 2^4 = 3,\\
&(2^6)^1 \equiv 1 \pmod{9}, \text{ i.e. } \operatorname{ord}_9 2^6 = 1.
\end{aligned}$$

Corollary 10.3 *If g is a primitive root of the prime p, then the least residue of g^k is a primitive root of p if and only if $(k, p-1) = 1$.*

? So here is the million dollar question: How do we find one primitive root of m in the first place, and in particular, the smallest one?

This, in general, is an unsolved problem, but we shall show later that 2 is always a primitive root of certain primes.

10.4 Integers with Primitive Roots

? But which integers have primitive roots?

Example: Note that $\phi(12) = 4$ and $\Phi(12) = \{1, 5, 7, 11\}$, and

$$\begin{aligned}
1 &\equiv 1 \pmod{12}\\
5^2 &\equiv 25 \equiv 1 \pmod{12}\\
7^2 &\equiv 49 \equiv 1 \pmod{12}\\
11^2 &\equiv 121 \equiv 1 \pmod{12}.
\end{aligned}$$

So the order of each of these numbers (mod 12) is less than $\phi(12)$ and we see that 12 has no primitive roots. It can be proved (but we won't) that the following result is true.

Theorem 10.7 *The integer m has primitive roots if and only if*

$$m \in \{1, 2, 4, p^e, 2p^e\},$$

where p is an odd prime and e is a positive integer. If m has primitive roots, then (by previous results) it has $\phi(\phi(m))$ primitive roots. In particular, the prime p has $\phi(p-1)$ primitive roots.

Now we see that the converse of Theorem 10.4 holds: if m is prime, then by Theorem 10.7, m has a primitive root a, and so $\mathrm{ord}_n\, a = m - 1$, which means that the smallest integer k such that $a^k \equiv 1 \pmod{m}$ is $m - 1$. Hence *for each prime divisor p* of $m - 1$, (i) and (ii) in the hypothesis of Theorem 10.4 both hold for a.