LECTURE 8: PRIMITIVE ROOTS

1. Orders of residues modulo m

We will be interested in understanding multiplicative structure of the set of reduced residues. Recall that by Euler's Theorem, when $(a, m) = 1$, we have

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

Could we have $a^h \equiv 1 \pmod{m}$ for a smaller exponent h? This leads to the notions of order and of primitive root.

Definition 1.1. Let m be a natural number, and let a be any integer with $(a, m) = 1$. Let h be the least positive integer with $a^h \equiv 1 \pmod{m}$. Then we say that the **order of a modulo m is h** (or that a **belongs to h modulo m**).

We note that if the congruence $a^h \equiv 1 \pmod{m}$ holds with small h, the cryptographic protocols discussed in Lecture 5, (which are based on transmission of residues $a^i \pmod{m}$) become vulnerable.

Lemma 1.2. *Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ satisfy $(a, m) = 1$. Then the order h of a modulo m exists, and $h \mid \phi(m)$. Moreover, whenever $a^k \equiv 1 \pmod{m}$, one has $h \mid k$.*

Proof. By Euler's theorem, one has $a^{\phi(m)} \equiv 1 \pmod{m}$, and so the order of a modulo m clearly exists. Suppose then that h is the order of a modulo m, and further that $a^k \equiv 1 \pmod{m}$. Then it follows from the division algorithm that there exist integers q and r with $k = hq + r$ and $0 \leqslant r < h$. But then we obtain

$$a^k = (a^h)^q a^r \equiv a^r \equiv 1 \pmod{m},$$

whence $r = 0$. Thus we have $h \mid k$, and in particular we deduce that $h \mid \phi(m)$. □

Lemma 1.3. *Suppose that a has order h modulo m. Then a^k has order $h/(h, k)$ modulo m.*

Proof. By Lemma 1.2, one has $(a^k)^j \equiv 1 \pmod{m}$ if and only if $h \mid kj$. But

$$h \mid kj \iff h/(h, k) \mid (k/(h, k))j \iff h/(h, k) \mid j.$$

Thus the least positive integer j such that $(a^k)^j \equiv 1 \pmod{m}$ is $j = h/(h, k)$. □

Lemma 1.4. *Suppose that a has order h modulo m, and b has order k modulo m. Then whenever $(h, k) = 1$, it follows that the product ab has order hk modulo m.*

Proof. Let r denote the order of ab modulo m. Then since

$$(ab)^{hk} = (a^h)^k (b^k)^h \equiv 1 \pmod{m},$$

it follows from Lemma 1.2 that $r \mid hk$. But we also have

$$b^{rh} \equiv (a^h)^r b^{rh} \equiv (ab)^{rh} \equiv 1 \pmod{m},$$

whence $k \mid rh$. Since $(h,k) = 1$, moreover, the latter implies that $k \mid r$. Similarly, on reversing the roles of a and b, we see that $h \mid r$. Then since $(h,k) = 1$, we deduce that $hk \mid r$. We therefore conclude that $hk \mid r \mid hk$, and thus $r = hk$. □

Definition 1.5. If g has order $\phi(m)$ modulo m, then g is called a **primitive root modulo** m.

Note: If g is a primitive root modulo m, then $\{1, g, \ldots, g^{\phi(m)-1}\}$ form a reduced residue system modulo m, and the multiplication table is very simple:

$$g^i \cdot g^j \equiv g^{(i+j) \pmod{\phi(m)}} \pmod{m}.$$

In this case, we say that the set $(\mathbb{Z}/m\mathbb{Z})^\times$ of reduced residues modulo m form a cyclic group $C_{\phi(m)}$ under multiplication:

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{1, g, \ldots, g^{\phi(m)-1}\} \cong C_{\phi(m)}.$$

2. Existence of primitive roots

Now we investigate existence of primitive roots.

Theorem 2.1. *If p is a prime number, then there exists a primitive root modulo p, and in fact there are exactly $\phi(p-1)$ distinct primitive roots modulo p.*

Proof. When $p = 2$, the conclusion of the theorem is immediate, so we suppose henceforth that p is an odd prime. Observe first that each of the residues $1, 2, \ldots, p-1$ have order equal to some divisor d of $p-1$ modulo p. Let $\psi(d)$ denote the number of residues that have order d modulo p. Then plainly,

$$\sum_{d \mid p-1} \psi(d) = p - 1. \tag{2.1}$$

We aim to show that for each divisor d of $p-1$, one has

$$\psi(d) \leqslant \phi(d). \tag{2.2}$$

We recall that we have proved that for every m,

$$\sum_{d \mid n} \phi(d) = m.$$

Hence, given the validity of (2.1)–(2.2), one obtains

$$p - 1 = \sum_{d \mid p-1} \psi(d) \leqslant \sum_{d \mid p-1} \phi(d) = p - 1,$$

and so the central inequality must hold with equality for every d. The desired conclusion then follows from the case $d = p - 1$ of the consequent relation $\psi(d) = \phi(d)$.

In order to verify our claim, suppose that $d \mid p-1$ and $\psi(d) \neq 0$. Let a be any residue that has order d modulo p. It follows that $a, a^2, \ldots, a^d$ are mutually incongruent solutions of the congruence $x^d \equiv 1 \pmod{p}$. For certainly, for each positive integer j one has $(a^j)^d = (a^d)^j \equiv 1 \pmod{p}$. In addition, if it were the case that for two exponents i and j with $1 \leqslant i < j \leqslant d$, one has $a^j \equiv a^i \pmod{p}$, then there would exist a positive integer $h = j - i < d$ with $a^h \equiv 1 \pmod{p}$, contradicting the assumption that a has order d. By Lagrange's theorem, meanwhile, there are at most d solutions modulo p to the congruence $x^d \equiv 1 \pmod{p}$, and thus the above list of residues constitutes the entire solution set modulo p. Next, on making use of Lemma 1.3, we find that whenever $(m, d) > 1$, the residue a^m has order $d/(m, d) < d$, and so the only reduced residues modulo p of order d are congruent to $a^m \pmod{p}$ for some integer m with $1 \leqslant m \leqslant d$ and $(m, d) = 1$. There are consequently precisely $\phi(d)$ such residues.

What we have shown thus far is that for each divisor d of $p - 1$, one has either $\psi(d) = \phi(d)$, or else $\psi(d) = 0$. This is a strong form of the inequality $\psi(d) \leqslant \phi(d)$ that we sought, and so our earlier discussion confirms that the number of distinct primitive roots modulo p is $\phi(p - 1)$. □

Theorem 2.2. *Suppose that g is a primitive root modulo p. Then there exists an integer x such that the residue $g_1 = g + px$ is a primitive root modulo p^2. When p is odd, moreover, this residue g_1 is a primitive root modulo p^k for every natural number k.*

Proof. Let g be a primitive root modulo p. Write $g_1 = g + px$, in which x is interpreted as a variable to be assigned in due course. In view of the expansion

$$(g + px)^{p-1} \equiv g^{p-1} + p(p - 1)xg^{p-2} \pmod{p^2},$$

one may write $g_1^{p-1} = 1 + pz$, in which

$$z \equiv \frac{g^{p-1} - 1}{p} + (p - 1)g^{p-2}x \pmod{p}. \tag{2.3}$$

The coefficient of x in (2.3) is not divisible by p, and so we can find an integer x for which $(z, p) = 1$ (first choose such a z, and then solve for x in (2.3)). We fix such an integer x, and now show that for every prime p this construction ensures that g_1 is a primitive root modulo p^2, and moreover that when p is odd, then the residue g_1 is a primitive root modulo p^k for every natural number k.

Suppose, for some $k \geqslant 2$, that g_1 has order d modulo p^k. Then by Lemma 1.2, it follows that $d \mid p^{k-1}(p-1)$. But g_1 is a primitive root modulo p, and so in particular one has $(p-1) \mid d$. Consequently, one must have $d = p^j(p-1)$ for some integer j with $0 \leqslant j \leqslant k - 1$. But in view of our earlier observation, one has $(z, p) = 1$, and thus $g_1^{p-1} \not\equiv 1 \pmod{p^2}$. Then g_1 is always a primitive root modulo p^2. When p is odd, moreover, we may write $(1 + pz)^{p^j} = 1 + p^{j+1}z_j$, for a suitable integer z_j with $(z_j, p) = 1$. Thus we obtain the relation

$$g_1^d = (g_1^{p-1})^{p^j} = (1 + pz)^{p^j} = 1 + p^{j+1} z_j.$$

Then since g_1 has order d modulo p^k, this last expression must be congruent to 1 modulo p^k, and hence $j + 1 \geqslant k$. Then since $j \leqslant k - 1$, the only possibility is that $j = k - 1$, and we are forced to conclude that $d = \phi(p^k)$. We have shown, therefore, that g_1 is a primitive root modulo p^k, and this completes the proof of the theorem. □

Corollary 2.3. *The number of primitive roots modulo p is $\phi(p-1)$, the number modulo p^2 is $(p-1)\phi(p-1)$, and when p is odd, the number modulo p^j $(j \geqslant 3)$ is $p^{j-2}(p-1)\phi(p-1)$.*

Proof. For each modulus in question, say m, there exists a primitive root g, and moreover g^k is primitive modulo m if and only if $(k, \phi(m)) = 1$. But the $\phi(m)$ residues $g^k \pmod m$ are all distinct for $1 \leqslant k \leqslant \phi(m)$, so every reduced residue has this form. Then the $\phi(\phi(m))$ residues $g^k \pmod m$ with $(k, \phi(m)) = 1$ comprise all of the primitive roots modulo m. The desired conclusion now follows on making use of the multiplicative property of the Euler totient. □

Theorem 2.4. *(i) There exists a primitive root modulo m if and only if $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, in which p is an odd prime number and α is a natural number. (ii) When $j \geqslant 3$, the order of 5 modulo 2^j is 2^{j-2}. Furthermore, every reduced residue class modulo 2^j may be written in the form $(-1)^l 5^m$, where $l = 0$ or 1 and $1 \leqslant m \leqslant 2^{j-2}$, and in which the integers l and m are unique.*

Proof. When $m = 2, 4$, the residues 1, 3, respectively, are primitive roots. When $m = p^\alpha$ the desired conclusion is immediate from Theorem 2.2. Suppose then that $m = 2p^\alpha$. If g is a primitive root modulo p^α (and such exist by Theorem 2.2), then one of g and $g + p^\alpha$ is an odd integer, say g'. The order of g' modulo $2p^\alpha$ must be at least $\phi(p^\alpha)$, since g' is primitive modulo p^α. But $\phi(2p^\alpha) = \phi(2)\phi(p^\alpha) = \phi(p^\alpha)$, so that the latter observation already ensures that g' is primitive modulo $2p^\alpha$.

Suppose next that m is none of 1, 2, 4, p^α or $2p^\alpha$, for any odd prime p. Then provided that m is not a power of 2, there exist integers n_1 and n_2 with $(n_1, n_2) = 1$, $n_1 > n_2 > 2$ and $m = n_1 n_2$. But then $\phi(n_1)$ and $\phi(n_2)$ are both even, whence

$$a^{\phi(m)/2} = (a^{\phi(n_1)})^{\phi(n_2)/2} \equiv 1 \pmod{n_1} \quad \text{whenever } (a, m) = 1,$$

and

$$a^{\phi(m)/2} = (a^{\phi(n_2)})^{\phi(n_1)/2} \equiv 1 \pmod{n_2} \quad \text{whenever } (a, m) = 1.$$

Then since $(n_1, n_2) = 1$ and $m = n_1 n_2$, we find that $a^{\phi(m)/2} \equiv 1 \pmod m$ whenever $(a, m) = 1$. No reduced residue modulo m, therefore, has order exceeding $\phi(m)/2$, and so, in particular, no residue can be a primitive root modulo m.

It remains to consider the situation in which $m = 2^j$ with $j \geqslant 3$. We begin by establishing that for each α with $\alpha \geqslant 2$, one has $2^\alpha \parallel (5^{2^{\alpha-2}} - 1)$. This is clear when $\alpha = 2$. Suppose then that the assertion holds when $\alpha = t$. Then $2^t \parallel (5^{2^{t-2}} - 1)$, whence $2 \parallel (5^{2^{t-2}} + 1)$, and thus $2^{t+1} \parallel (5^{2^{t-2}} - 1)(5^{2^{t-2}} + 1)$, or equivalently, one has $2^{t+1} \parallel (5^{2^{t-1}} - 1)$. Then the assertion that we presently seek to establish holds with $\alpha = t + 1$ whenever it holds with $\alpha = t$, whence by induction it holds for all $\alpha \geqslant 2$.

Since $2^\alpha \parallel (5^{2^{\alpha-2}} - 1)$ for $\alpha \geqslant 2$, it follows that 5 has order precisely $2^{\alpha-2}$ modulo 2^α, and this establishes the first claim of the second part of the theorem. Observe next that there are $2^{\alpha-2}$ distinct reduced residues modulo 2^α of the shape 5^k, all of which are congruent to 1 modulo 4 (why?), and so the remaining reduced residues modulo 2^α must all be congruent to -1 modulo 4, and are hence of the shape -5^k. Thus all reduced residues modulo 2^α may be written in the form $(-1)^l 5^m$, where $l = 0$ or 1 and $1 \leqslant m \leqslant 2^{\alpha-2}$. Furthermore, these choices for l and m are distinct, for the total number of residues represented in this manner is at most $2^{\alpha-1}$, and yet there are precisely $2^{\alpha-1}$ residues to be represented. That there are no primitive roots modulo 2^α when $\alpha > 2$ follows on noting that $(-1)^l 5^m$ has order at most $2^{\alpha-2} < \phi(2^\alpha)$ when $\alpha \geqslant 3$. $\square$

Our main result can be summarised as follows:

$$\begin{aligned} (\mathbb{Z}/p^r\mathbb{Z})^\times &\cong C_{\phi(p^r)}, \quad \text{when } p \text{ is odd}, \\ (\mathbb{Z}/2\mathbb{Z})^\times &\cong C_1, \\ (\mathbb{Z}/4\mathbb{Z})^\times &\cong C_2, \\ (\mathbb{Z}/2^r\mathbb{Z})^\times &\cong C_2 \times C_{2^{r-2}}, \quad \text{when } r \geqslant 3. \end{aligned}$$

Making use of the Chinese Remainder Theorem, we infer that if

$$m = 2^e \prod_{\substack{p^r \parallel m \\ p>2}} p^r,$$

then

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong G_e \times \prod_{\substack{p^r \parallel m \\ p>2}} C_{\phi(p^r)},$$

where

$$G_e \cong \begin{cases} C_1, & \text{when } e = 0, 1, \\ C_2, & \text{when } e = 2, \\ C_2 \times C_{2^{e-2}}, & \text{when } e \geqslant 3. \end{cases}$$

This allows to deduce the following improvement of Euler's theorem. Put

$$e(p^h) = \begin{cases} \phi(p^h), & \text{when } p \text{ is odd, and when } p^h = 2 \text{ or } 4, \\ \frac{1}{2}\phi(p^h), & \text{when } p = 2 \text{ and } h \geqslant 3, \end{cases}$$

and then define the (*Carmichael*) function

$$\lambda(n) = \operatorname*{lcm}_{p^h \| n} e(p^h).$$

It is clear from the above discussion that whenever $(a, n) = 1$, one has

$$a^{\lambda(n)} \equiv 1 \pmod{n},$$

providing a refinement of Euler's theorem. Moreover, for every natural number n, it is apparent also that there exists an integer a with $(a, n) = 1$ having order precisely $\lambda(n)$ modulo n.

Aside: It is an interesting problem what is the least positive integer g_p which gives a primitive root modulo a prime p. Currently, it is known, due to the work of Wang, that assuming the Generalised Riemann Hypothesis (a difficult unsolved problem in Number Theory), we have

$$g_p \leqslant C\,\omega(p-1)^6(\log p)^2,$$

where $\omega(n)$ denotes the number of distinct prime factors of an integer n.

Artin conjectured in 1924 that every positive integer a which is not a square is a primitive root modulo p for infinitely many primes p. This conjecture is still open in general, but Hooley in 1967 proved this conjecture assuming the Generalised Riemann Hypothesis.