Order of an integer.
Primitive roots.

Definition 1. *Let a, n be relatively prime positive integers. The least positive integer x such that*

$$a^x \equiv 1 \mod n$$

is called the order of a modulo n.

Notation. $ord_n a$

Remark. In particular,

$$a^{ord_n a} \equiv 1 \mod n.$$

Theorem 1. *Let a, n be relatively prime integers with $n > 0$. Then the positive integer x is a solution of the congruence*

$$a^x \equiv 1 \mod n$$

if and only if

$$ord_n a | x.$$

Proof. Suppose first that $ord_n a | x$. Then $x = k \cdot ord_n a$ for some $k \in \mathbb{Z}_{>0}$ and

$$a^x = (a^{ord_n a})^k \equiv 1 \mod n.$$

Conversely, if $a^x \equiv 1 \mod n$ and $x = q \cdot ord_n a + r$, with $0 \leq r < ord_n a$, then, by the definition

$$a^x = a^{q \cdot ord_n a + r} = (a^{ord_n a})^q a^r \equiv a^r \mod n.$$

Since $a^x \equiv 1 \mod n$, $a^r \equiv 1 \mod n$. On the other hand, $0 \leq r < ord_n a$. Therefore $r = 0$ because $ord_n a$ is the least positive integer y satisfying $a^y \equiv 1 \mod n$. This implies that $x = q \cdot ord_n a$ and $ord_n a | x$. □

Corollary. *If a, n are relatively prime integers with $n > 0$, then $ord_n a | \phi(n)$.*

Proof. Euler's theorem implies that, since $(a, n) = 1$, $a^{\phi(n)} \equiv 1 \mod n$. Then, by Th. 20.1, $ord_n a | \phi(n)$. □

Theorem 2. *If $ord_n a = t$ and $m \in \mathbb{Z}_{>0}$, then*

$$ord_n(a^m) = \frac{t}{(t,m)}.$$

Proof. Set $s = ord_n(a^m)$, $t_1 = \frac{t}{(t,m)}$ and $m_1 = \frac{m}{(t,m)}$.

Since $ord_n a = t$,

$$(a^m)^{t_1} = (a^{m_1 (t,m)})^{\frac{t}{(t,m)}} = (a^t)^{m_1} \equiv 1 \mod n.$$

Hence, by Th. 20.1., $s | t_1$.

Since, $a^{ms} = (a^m)^s \equiv 1 \mod n$, $t | ms$ (again, by Th. 20.1.). Therefore, $t_1 | m_1 s$ and, since $(t_1, m_1) = 1$, $t_1 | s$.

Since $s | t_1$ and $t_1 | s$, $s = t_1$. □

Definition 2 *Let r, n be relatively prime integers with $n > 0$. If $ord_n r = \phi(n)$, then r is called a* primitive root modulo *n.*

Example. By a direct check, $ord_7 5 = 6$. Since $\phi(7) = 6$, 5 is a primitive root modulo 7.
On the other hand, $ord_7 2 = 3 \neq \phi(7)$, therefore 2 is not a primitive root modulo 7.

Lemma 1 *Let a, n be relatively prime integers with $n > 0$. Then $a^i \equiv a^j \mod n$, $(i, j \in \mathbb{Z}_{\geq 0})$, if and only if $i \equiv j \mod ord_n a$.*

Proof. If $i \equiv j \mod ord_n a$ and $0 \leq j \leq i$, then $i = j + k \cdot ord_n a$ for some $k \in \mathbb{Z}_{\geq 0}$. Therefore,

$$a^i = a^{j+k \cdot ord_n a} = a^j (a^{ord_n a})^k \equiv a^j \mod n$$

since $a^{ord_n a} \equiv 1 \mod n$.
Conversely, if $a^i \equiv a^j \mod m$ with $i \geq j$, then, by the cancelation of a^j in the congruence

$$a^j a^{i-j} \equiv a^j \mod n$$

we obtain $a^{i-j} \equiv 1 \mod n$. Th. 20.1. implies that $ord_n a | (i - j)$, i.e. $i \equiv j \mod ord_n a$. □

Theorem 3. *Let r, n be relatively prime integers with $n > 0$. If r is a primitive root modulo n, then the integers*

$$r, r^2, \ldots, r^{\phi(n)}$$

form a reduced residue system modulo n.

Proof. By the definition of reduced residue systems, it is sufficient to show that all these powers are coprime to n and that no two are congruent modulo n.

- Since $(r, n) = 1$, $(r^j, n) = 1$ $(j = 1, \ldots, \phi(n))$
- If $r^i \equiv r^j \mod n$, for some $i, j \in \{1, \ldots, \phi(n)\}$, then, by Lemma 20.1, $i \equiv j \mod ord_n r$, or, since r is a primitive root modulo n, $i \equiv j \mod \phi(n)$. Since $1 \leq i \leq \phi(n)$ and $1 \leq j \leq \phi(n)$, $i = j$. □

Theorem 4. *Let r be a primitive root modulo n, where n is an integer > 1. Then r^m is a primitive root modulo n if and only if $(m, \phi(n)) = 1$*

Proof. Theorem 2 implies

$$ord_n(r^m) = \frac{ord_n r}{(m, ord_n r)} = \frac{\phi(n)}{(m, \phi(n))}.$$

Therefore, r^m is a primitive root modulo n (i.e. $ord_n(r^m) = \phi(n)$) if and only if $(m, \phi(n)) = 1$. □

Theorem 5. *If $n \in \mathbb{Z}_{>0}$ has a primitive root, then it has exactly $\phi(\phi(n))$ incongruent primitive roots.*

Proof. Let r be a primitive root of n. By Th 20.3, the only integers coprime to n are those congruent to r, r^2, $\ldots$ $r^{\phi(n)}$. On the other hand, by Th. 20.4, r^m is a primitive root modulo n if and only if $(m, \phi(n)) = 1$. Since there are exactly $\phi(\phi(n))$ such integers $m \leq \phi(n)$, we obtain the result. $\square$

Existence of primitive roots.

Theorem 1 (Lagrange) *Let p be a prime and let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial of degree $n \geq 1$ with coefficients in $\mathbb{Z}$ such that $p \nmid a_n$. Then $f(x)$ has at most n incongruent solutions modulo p.*

Proof. D. Burton, *Elementary Number Theory, McGraw Hill, 5th Ed. (2002) (Section 8.2)*

Theorem 2. *If p is a prime and d is a divisor of $p-1$, then $x^d - 1$ has exactly d incongruent roots modulo p.*

Proof. If $p - 1 = dn$, $(n \in \mathbb{Z})$ then $x^{p-1} - 1 = (x^d - 1)h(x)$, where $h(x) = x^{d(n-1)} + \cdots + x^d + 1$. Let R_1, R_2, R_3 be the sets of incongruent solutions $\mod p$ of $x^{p-1} - 1$, $x^d - 1$ and $h(x)$ respectively. Since each solution of $x^{p-1} \equiv 1 \mod p$ is is a solution either of $x^d \equiv 1 \mod p$ or of $g(x) \equiv 0 \mod p$ and vice-versa, $R_1 = R_2 \cup R_3$. Therefore, $|R_1| \leq |R_2| + |R_3|$.

- By Fermat's little theorem, $|R_1| = p - 1$.
- By Lagrange's theorem, $|R_3| \leq d(n-1) = p - d - 1$.

Therefore,

- $|R_2| \geq |R_1| - |R_3| \geq (p-1) - (p-d-1) = d$.

Since, by Lagrange's theorem, $|R_2| \leq d$, $|R_2| = d$. □

Theorem 3. *If p is a prime and d is a divisor of $p-1$, then the number of incongruent integers of order d modulo p is $\phi(d)$.*

Proof. Coursework

Corollary. *Every prime has a primitive root.*

Proof. Let p be a prime. By definition, an integer r is a primitive root modulo p if and only if $ord_p r = \phi(p) = p - 1$. Th. 21.3. implies that there are $\phi(p-1)$ incongruent integers of order $p-1$ modulo p. Therefore, p has $\phi(p-1) > 0$ primitive roots. □

Theorem 4. *The only positive integers having primitive roots are those of the form*

$$2, 4, p^t, 2p^t$$

where p is an odd prime and $t \in \mathbb{Z}_{>0}$.

Proof. D. Burton, *Elementary Number Theory, McGraw Hill, 5th Ed. (2002) (Section 8.3)*

Index arithmetic

Discrete logarithms

Lemma 1. *Suppose that $m \in \mathbb{Z}_{>0}$ has a primitive root r. If a is a positive integer with $(a,m)=1$, then there is a unique integer x with $1 \le x \le \phi(m)$ such that*

$$r^x \equiv a \mod m.$$

Proof. By Th. 20.3., $\{r, r^2, \ldots, r^{\phi(m)}\}$ is a reduced residue system $\mod m$. Therefore, if $(a,m)=1$, then there is a unique element in that set congruent to $a \mod m$. □

Definition 1 *If $m \in \mathbb{Z}_{>0}$ has a primitive root r and a is a positive integer with $(a,m)=1$, then the unique integer x with $1 \le x \le \phi(m)$ and $r^x \equiv a \mod m$ is called the* index *(or* discrete logarithm*) of a to the base r modulo m.*

Notation. $ind_r a$.

Remark. In particular,

$$r^{ind_r a} \equiv a \mod m.$$

Theorem 1. *Let m be a positive integer with primitive root r. If a,b are positive integers coprime to m and k is a positive integer, then*

(i) $ind_r 1 \equiv 0 \mod \phi(m)$

(ii) $ind_r(ab) \equiv ind_r a + ind_r b \mod \phi(m)$

(iii) $ind_r a^k \equiv k \cdot ind_r a \mod \phi(m)$

Proof. (i) Euler's theorem implies that $r^{\phi(m)} \equiv 1 \mod m$. Therefore, $ind_r 1 = \phi(m) \equiv 0 \mod \phi(m)$.

(ii) By definition,

$$r^{ind_r a} \equiv a \mod m$$
$$r^{ind_r b} \equiv b \mod m \text{ and}$$
$$r^{ind_r (ab)} \equiv ab \mod m.$$

Therefore,

$$r^{ind_r(ab)} \equiv ab \equiv r^{ind_r a} r^{ind_r b} = r^{ind_r a + ind_r b} \mod m.$$

Lemma 20.1 then implies that $ind_r(ab) \equiv ind_r a + ind_r b \mod \phi(m)$.

(iii) Since, by (ii), $ind_r(a^{k-1}a) \equiv ind_r a^{k-1} + ind_r a \mod \phi(m)$, the result follows by induction on k.