8. Primitive elements and Euler's φ-function

Let $n \in \mathbb{N}$ and $\mathbb{Z}_n = \{0, 1, \cdots, n-1\} \subseteq \mathbb{Z}$. Then,

- given any integer a, there is a unique integer $a_1 \in \mathbb{Z}_n$ such that $a \equiv a_1 \pmod{n}$. In particular, no two elements of $\mathbb{Z}_n$ are congruent mod n.
- Addition (modulo n) and multiplication (modulo n) are commutative and associative binary operations on $\mathbb{Z}_n$. We saw earlier, the following:

(1) $(\mathbb{Z}_n, +)$ is an abelian group. Any subgroup A of it consists of the multiples in $\mathbb{Z}_n$ of the elements of $\mathbb{Z}_n$ which are multiples of a fixed element d of $\mathbb{Z}_n$; i.e.,

$$A = \langle d \rangle_{\mathbb{Z}_n} = \{ dm : m \in \mathbb{Z}_n \}.$$

We say that d generates A, ~~and that A is~~

~~cyclic group~~. Further, $d\mathbb{Z}_n = \mathbb{Z}_n$ if, and only if $\gcd(d,n)=1$. Thus, $\mathbb{Z}_n$ is a cyclic group generated by any element of $\mathbb{Z}_n$ coprime to n. Note that, for $d, m \in \mathbb{Z}_n$, dm is d added to itself m times. So, dm as an element of the additive group makes sense.

DEF: $\varphi(n) := |\{d \in \mathbb{Z}_n : \gcd(d,n)=1\}|$

$\varphi : \mathbb{N} \to \mathbb{N}$ is called the Euler's φ-function. Thus, $\varphi(n)$ is the number of generators of the abelian group $\mathbb{Z}_n$.

$\varphi(1) = \varphi(2) = 1$, $\varphi(3) = 2 = \varphi(4) = \varphi(6)$

For a prime p, $\varphi(p) = p-1$, $\varphi(p^n) = p^{n-1}(p-1)$.

$n=2$

$\{1, 2, \cdots, p-1, \boxed{p}$

$p+1, \cdots p+(p-1), \boxed{2p}$

$2p+1, \cdots 2p+(p-1), \boxed{3p}$

$(p-1)p+1, \cdots (p-1)p+(p-1), \boxed{p^2}\}$

$\varphi(p^2)$

2) $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with identity.

(i) Each ideal in it is of the form $d\mathbb{Z}_n$ for some $d \in \mathbb{Z}_n$. (Recall: A subset I of a commutative ring R is called an ideal if it is a subgroup with respect to addition and $ra \in I$ for each $r \in R$ and $a \in I$). $\mathbb{Z}[x]$ is not an ideal in $R[x]$, but for any element a of a commutative ring R, the set $\langle a \rangle = Ra = \{ra : r \in R\}$ is an ideal of R. If each ideal of R is equal to Ra for some $a \in R$, we say that R is a principal ideal ring.)

i.e., $\mathbb{Z}_n$ is a principal ideal ring.

(ii) $(\mathbb{Z}_n, +, \cdot)$ is an integral domain if, and only if, n is a prime. If n is a prime, then $\mathbb{Z}_n$ is a field.

(iii) Let $\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n : \gcd(a, n) = 1 \}$.

Prop: Then, $\mathbb{Z}_n^*$ is a group of order $\varphi(n)$ with respect to multiplication.

Proof: If $(a, n) = 1 = (b, n)$, then $(ab, n) = 1$. So, $\mathbb{Z}_n^*$ is closed under multiplication.

Recall that, if $r, s \in \mathbb{Z}$ and $\gcd(r, s) = d$, then there exist $x, y \in \mathbb{Z}$ such that $rx + sy = d$.

Now, if $(a, n) = 1$, then $al + nl' = 1$ for $l, l' \in \mathbb{Z}$. We have $al \equiv 1 \pmod{n}$. If $a \in \mathbb{Z}_n$ and $c \in \mathbb{Z}_n$ with $c \equiv l \pmod{n}$, then $ac \equiv 1 \pmod{n}$; i.e., c is the multiplicative inverse of a in $\mathbb{Z}_n^*$.

Clearly, associativity and the existence of the identity hold. So, $\mathbb{Z}_n^*$ is a group. □

Observe: $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ if p is a prime.

Two arithmetic functions

A real or a complex valued function defined on $\mathbb{N}$ is called an arithmetic function. They play an important role in Number theory. We discuss the properties of two such functions: the Möbius function and the Euler's φ-function.

($p_i \neq p_j$ for $i \neq j$, p_i are prime)

DEF: The Möbius function μ is defined as follows:

$\mu(1) = 1$; if $n > 1$ and $n = p_1^{a_1} \cdots p_t^{a_t}$, then $\mu(n) = (-1)^t$ if $a_1, \cdots, a_t$ are all equal to 1; and zero otherwise.

Thus, $\mu(n) = 0$ if, and only if, $p^2 \mid n$ for some prime p.

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

Theorem. If $n \geq 1$, $\sum_{d \mid n, d \geq 1} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$

Proof. (If $n > 1$,) the only nonzero contribution to the LHS comes from 1 and products of elements

of subsets of the set of all prime divisors of n. So,

$$\sum_{d|n,\, d\geq 0} \mu(d) = \mu(1) + \mu(p_1) + \cdots + \mu(p_t) + \mu(p_1p_2) + \cdots$$
$$\mu(p_{t-1}p_t) + \cdots + \mu(p_1 \cdots p_t)$$
$$= 1 + \binom{t}{1}(-1) + \binom{t}{2}(-1)^2 + \cdots + \binom{t}{t}(-1)^t = (1-1)^t = 0. \quad \square$$

Euler's φ-function (also called **Euler's totient function**)

For $n \geq 1$, $\varphi(n) \overset{\text{def}}{=} |\{d \in \mathbb{N} : d \leq n \text{ and } \gcd(d,n) = 1\}|$.

Theorem. For $n \geq 1$, $\sum_{d|n,\, d\geq 1} \varphi(d) = n$.

Proof. Let $S = \{1, \cdots, n\}$. For each divisor d of n, let $A(d) := \{s \in S : \gcd(s,n) = d\}$. Then, S is a disjoint union of the sets $\{A(d) : d|n,\ d \geq 1\}$.

observe that, for $t \in S$, $(t,n) = d$ iff $\left(\frac{t}{d}, \frac{n}{d}\right) = 1$ and $0 < \frac{t}{d} \leq \frac{n}{d}$.

Thus, $t \to t/d$ is a bijection from $A(d)$ to the set $\{l \in \mathbb{N} : 0 < l \leq \frac{n}{d} \text{ and } (l, \frac{n}{d}) = 1\}$ and the latter set has $\varphi(n/d)$ number of elements. So, $n = \sum_{d|n} \varphi(n/d)$. As d runs over all divisors of n, so does n/d. So, the theorem follows. □

Lemma. Given integers a, b, c, ~~$(a, bc) = 1 = (a, 1$~~
$\gcd(a, bc) = 1$ if, and only if, $\gcd(a, b) = 1 = \gcd(a, c)$.

Proof. (i) Let $(a, bc) = 1$ and $(a, b) = d$. Then, $d|a$, $d|b$ and so, $d|a$ and $d|bc$. Thus, $d|(a, bc) = 1$ and $d = 1$. Similarly, $d|(a, c)$.

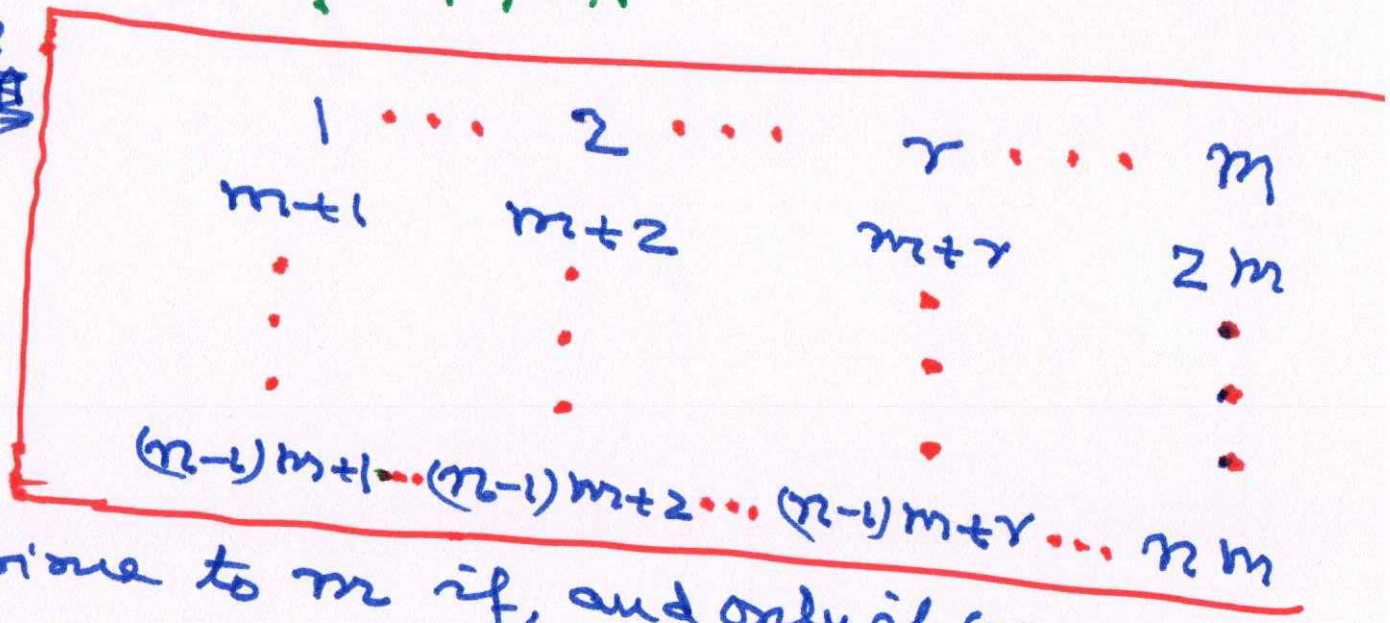
(ii) Now, let $(a, b) = 1 = (a, c)$ and $(a, bc) = d$. If $d > 1$, then there is a prime p dividing a as well as bc. So, $d|a$, $d|b$ or $d|c$. If $d|b$, then $d|(a, b) = 1$, so $d = 1$. Similarly, if $d|c$. So, the proof of the lemma is complete. □

Theorem: If $m, n \in \mathbb{Z}$ and $(m,n)=1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. For $s = 1, \cdots, n-1$

$(sm+r, m) = (r, m)$.

So, members of the r^{th} column are relatively prime to m if, and only if $(r,m)=1$.



- For $1 \le r \le m$, and $1 \le t, 1 \le n-1$, $tm+r \not\equiv lm+r \pmod{n}$.
- Thus, elements of the r^{th} colum is a complete set of representatives for the congruence modulo n.
- So, the number of elements of the r^{th} column which are relatively prime to n is equal to the number of elements in $\{0, 1, \cdots, n-1\}$ which are relatively prime to n, which is $\varphi(n)$.

Thus, the integers relatively prime to m appear in only $\varphi(m)$ of the rows $\{tm+r\}_{t=0}^{n-1}$, $1 \le r \le m$ such that $(r, m) = 1$ and in each row, it occurs $\varphi(n)$ times. So, the theorem follows. □

Cor 1: If $n \ge 1$ and $n = p_1^{t_1} \cdots p_s^{t_s}$, $t_i \ge 1$, p_i - primes, is the prime decomposition of n, then

$$\varphi(n) = \prod_{i=1}^{s} p_i^{(t_i-1)}(p_i - 1) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).$$

Proof. For $i = 1, \ldots, s$ $\varphi(p_i^{t_i})$ is the number of integers in $\{1, \ldots, p_i - 1, p_i, p_i + 1, \ldots, p_i^{r} - 1, p_i^{r}, p_i^{r} + 1, \ldots, p_i^{t_i} - 1, p_i^{t_i}\}$ which are not multiples of p_i which is $p_i^{t_i} - p_i^{t_i - 1}$. Since $p_i \ne p_j$ for $i \ne j$, the result follows from previous theorem and induction on s. □

Cor 2: If $n \geq 3$, $\varphi(n)$ is an even integer.

Proof. If $2^t \mid n$, $2^{t+1} \nmid n$, $\varphi(2^t) = 2^t(1-\frac{1}{2}) = 2^{t-1}$ and $\varphi(2^t) \mid \varphi(n)$. So, if $t \geq 2$, $\varphi(2^t)$, and so, $\varphi(n)$ is even. If $t = 1$, $n = p^s m$ for a prime $p \neq 2$, $s \geq 1$ and $(p, m) = 1$. Now, $\varphi(n) = \varphi(p^s)\varphi(m) = (p^s - p^{s-1})\varphi(m)$ which is even because $s \geq 1$. □

Cor 3: (Euclid) There are infinite number of prime integers.

Proof. Deny. Let $p_1, \cdots, p_r$ are the only prime numbers. Let $N = p_1 \cdots p_r$. Take $a \in \mathbb{Z}$ with $1 < a \leq N$. Then, by the Fundamental Theorem of Arithmetic, there is a prime $q = p_i$ which divides a. So, $\gcd(a, N) > 1$ and $\varphi(N) = 1$, contradicting Cor. 2. So, the number of primes is infinite. □

Remark: For any mathematical insight (Theorem, Principal), mathematicians look for various contexts from which it can be ~~solved~~ understood; not because one (correct) proof is not enough, but because different proofs throw light on different interconnections And mathematics is not about objects but interconnections between various mathematical concepts. The most illustrious examples in the history of mathematics are:

- Quadratic reciprocity law (more than 150 proofs)
- Fundamental theorem of Algebra
- Infinity of primes
- Prime number theorem. □

We now return to the Möbius function μ and relate it to the Euler function φ.

Theorem. μ is a multiplicative function.

Def: An arithmetic function $f: \mathbb{N} \to \mathbb{C}$ is said to be *multiplicative* if $f(mn) = f(m)f(n)$ when $(m,n)=1$.

Proof of the theorem.

We need to show that $\mu(mn) = \mu(m)\mu(n)$ if $(m,n)=1$.

Since $\mu(1)=1$, we may assume $m \geq 2$, $n \geq 2$.

Since $\mu(a)=0$ if $p^2 | a$ for some prime, we need to deal only with the case

$m = p_1 \cdots p_r$, $n = p_{r+1} \cdots p_k$, $p_i \neq p_j$ for $i \neq j$, p_i are primes, $i = 1, \cdots, k$.

Then, $\mu(mn) = (-1)^k = (-1)^r \cdot (-1)^{k-r}$

$= \mu(m) \cdot \mu(n)$. □

Theorem (*Möbius inversion formula*). Let F and f be multiplicative function and $F(n) = \sum_{d|n} f(d)$.

Then, $$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

Proof. $$\sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{c|\frac{n}{d}} f(c)\right) = \sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d) f(c)\right)$$

Note that: $d|n$ and $c|\frac{n}{d} \iff c|n$ and $d|\frac{n}{c}$. So,

$$\sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d) f(c)\right) = \sum_{c|n} \left(\sum_{d|\frac{n}{c}} f(c)\mu(d)\right) = \sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d)\right)$$

$$\overset{(*)}{=} \sum_{c=n} f(c) \cdot 1 = f(n).$$

The equality (*) follows because $\left(\sum_{d|\frac{n}{c}} \mu(d)\right)$ vanishes except when $\frac{n}{c} = 1$; i.e., $n = c$, in which case it is one. □

Illustrations

(1) For $n \in \mathbb{N}$, let $\tau(n)$ denote the number positive divisors of n and $\sigma(n)$ the sum of these divisors:

$$\tau(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d$$

• Then, τ and σ are multiplicative functions. This is easily seen by observing that, if $n = p_1^{t_1} \cdots p_r^{t_r}$ is the prime decomposition of n, $n \in \mathbb{N}$, then

$$\tau(n) = (t_1+1)(t_2+1)\cdots(t_r+1), \text{ and}$$

$$\sigma(n) = \frac{p_1^{t_1+1}-1}{p_1-1} \cdot \frac{p_2^{t_2+1}-1}{p_2-1} \cdots \frac{p_r^{t_r+1}-1}{p_r-1}.$$

By Möbius inversion formula, ~~they are related~~

$$1 = \sum \mu\left(\frac{n}{d}\right)\tau(d) \quad \text{and} \quad n = \sum \mu\left(\frac{n}{d}\right)\sigma(d) \quad (n \geq 1).$$

[2] For $n \in \mathbb{N}$, $\varphi(n) = n \sum \frac{\mu(d)}{d}$. □

Proof. Apply the inversion formula with $F(n) = n = \sum_{d|n} \varphi(d)$ and $f(n) = \varphi(n)$:

$$\varphi(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\frac{n}{d}. \quad \square$$

Example:

$$10\left(\sum_{d\mid 10}\frac{\mu(d)}{d}\right)=10\left[\mu(1)+\frac{\mu(2)}{2}+\frac{\mu(5)}{5}+\frac{\mu(10)}{10}\right]$$

$$=10\left[1-\frac{1}{2}-\frac{1}{5}+\frac{1}{10}\right]=10\times\frac{2}{5}=4=\varphi(10).\ \square$$

Prop: For $n\in\mathbb{N}$, $n>1$, the sum of integers less than n and relatively prime to n is $\frac{1}{2}n\varphi(n)$.

Proof. For $a\in\mathbb{N}$, $1\le a\le n$, $\gcd(a,n)=1$ iff $\gcd(n-a,n)=1$. So, the set $\{a_1,\dots,a_{\varphi(n)}\}$ of integers a_i such that $1\le a_i\le n$ and $(a_i,n)=1$ is the same as the set $\{n-a_1,\dots,n-a_{\varphi(n)}\}$. So,

$$a_1+\cdots+a_{\varphi(n)}=(n-a_1)+\cdots+(n-a_{\varphi(n)})$$

$$=n\varphi(n)-(a_1+\cdots+a_{\varphi(n)}).\ \square$$

Mertens conjecture:

For $n \geq 1$, Let $M(n) := \sum_{t=1}^{n} \mu(t)$. This is the difference between the number of square free integers $t \leq n$ with an even number of prime factors and those with an odd number of prime factors. For example, $M(9) = 2 - 4 = -2$.

- Franz Mertens (1897) calculated this up to 10,000 and speculated that $|M(n)| < \sqrt{n}$ for $n > 1$.
- This was verified up to 10 billion by a computer search in 1963.
- Andrew Odlyzko and Herman te Riele showed that there exists an integer n such that $\sqrt{n} < |M(n)|$. No such number was produced.
- It has been proved that there exists a number with $\sqrt{n} < |M(n)|$ for $n \leq (3.21)10^{64}$. No such number is known!

$\mathbb{Z}_n^*$ and primitive roots mod n.

$\mathbb{Z}_n^* := \{a \in \mathbb{Z} : 1 \leq a \leq n, (a,n) = 1\}$ is a (abelian) group of order $\varphi(n)$ w.r.t. multiplication (modulo n) as group operation.

DEF: If $a \in \mathbb{Z}_n^*$ and t is the smallest (positive) integer such that $a^t \equiv 1 \pmod n$, we say that t is the order of a in $\mathbb{Z}_n^*$ and write $t = \mathrm{Ord}_n(a)$ or $|a|_n$ or $|a|$.

We say that $a \in \mathbb{Z}_n^*$ is a primitive root mod n if $\mathrm{Ord}_n(a) = \varphi(n)$. In this case, $\mathbb{Z}_n^*$ is a cyclic group generated by a.

Remarks: (1) $\mathbb{Z}_n^*$ need not be cyclic group for all n; i.e., there need not exist primitive roots mod n for all $n \in \mathbb{N}$. In fact, they exist only for $n = 1, 2, 4, p^t$ and $2p^t$, p any odd prime, $t \geq 1$.

2) If $a \in \mathbb{Z}_n^*$ is a primitive root (mod n), then $\mathbb{Z}_n^* = \langle a \rangle$ is a cyclic group of order $\varphi(n)$ and $\mathbb{Z}_n^*$ has $\varphi(\varphi(n))$ number of primitive roots (mod n).

This follows because, for $r \in \mathbb{Z}_n^*$, $r \neq 1$ and $r = a^s$ for some s, $1 \leq s \leq \varphi(n)$, $|r| = \varphi(n)$ if, and only if $(s, \varphi(n)) = 1$. More explicitly, the smallest integer t such that $(a^s)^t \equiv 1 \pmod{n}$ is $\varphi(n)$ if, and only if, $(s, \varphi(n)) = 1$.

Thus, $\{a^t : 1 \leq t \leq \varphi(n), (t, \varphi(n)) = 1\}$ are all the primitive roots (mod n).

There is no general method known for calculating a primitive root mod n.

3) Gauss conjectured that there exist an infinite number of primes with 10 as a primitive root, mod p. In 1927, Emil Artin extended this question

if a is not equal to 1, -1 or a perfect square, do there exist an infinite number of primes p for which a is a primitive root mod p.

It is known to hold for an infinite number of elements a and for all but two primes. □

Theory of indices

This was introduced by Gauss. Let $n \in \mathbb{N}$ admit a primitive root r mod n. If $a \in \mathbb{Z}_n^*$ (i.e., $(a, n) = 1$), then $a \equiv r^t \pmod{n}$. The smallest such positive integer t is called the index of a relative to r. We write it as $\operatorname{ind}_r a$ or just ind a, if there is no ambiguity about r.

Ex. Let $n = 5$. Then, $r = 2$ is a primitive root mod 5. Since $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$, $2^4 \equiv 1 \pmod{5}$,

$\operatorname{ind}_2 1 = 4$, $\operatorname{ind}_2 2 = 1$, $\operatorname{ind}_2 3 = 3$, $\operatorname{ind}_2 4 = 2$

Indices obey laws very similar to logarithms:

Prop: If n has a primitive root r and $a, b \in \mathbb{Z}_n^*$,

(i) $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(n)}$;

(ii) $\text{ind}_r a^t \equiv t \,\text{ind}_r a \pmod{\varphi(n)}$;

(iii) $\text{ind}_r 1 \equiv 0 \pmod{\varphi(n)}$; $\text{ind}_r r = 1 \pmod{\varphi(n)}$.

Proof. Direct application of definition. □

This can be used to solve certain congruence relations.

Ex: i) Assume that $n \in \mathbb{Z}$, $n > 0$, has a primitive root and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Consider the equation $x^k \equiv a \pmod{n}$. (1) This has a solution in x if and only if $k \,\text{ind}_r x \equiv \text{Ind}_r a \pmod{\varphi(n)}$ (2) has a solution. If $d = \gcd(k, \varphi(n))$ and $d \nmid \text{ind}_r a$, (2) does not have a solution.

If $d \mid \operatorname{ind}_r a$, then there are exactly d values of $\operatorname{ind}_r a$ which satisfy (2) and so there are d incongruent solutions of (1).

For ex. Let $k=2$ and $n=p$ an odd prime. Now $d=(2,\varphi(p))=(2,p-1)=2$. So, $x^2 \equiv a \pmod p$ has 2 solutions or no solutions according as $2 \mid \operatorname{ind}_r a$ or $2 \nmid \operatorname{ind}_r a$. If r is a primitive roots $(\bmod p)$, then $\{r, \cdots, r^{p-1}\} = \{1, 2, \cdots, (p-1)\} = \mathbb{Z}_p^*$. The even powers of r produce the elements $a \in \mathbb{Z}_p^*$ for which $x^2 \equiv a \pmod p$ has two solutions $(\bmod p)$ in x and no solutions if a is an odd power of r. □

Ex. 2. Solve $4x^9 \equiv 7 \pmod{13}$ for x.

Solⁿ. We see that 2 is a primitive root mod 13:

$2^6 = 64 \equiv -1$, $2^{12} \equiv 1 \pmod{13}$; $2^t \not\equiv 1 \ (13)$ for $t < 12$.

$\mathbb{Z}_{13}^* = \{1, 2, \cdots, 12\}$ $\varphi(13) = 13-1 = 12$

Mod 13, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 3$; $2^5 \equiv 6$, $2^6 \equiv 12$

$2^7 \equiv 11$, $2^8 \equiv 9$, $2^9 \equiv 5$, $2^{10} \equiv 10$, $2^{11} = 7$; $2^{12} \equiv 1$

So,

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	2	6

The congruence $4x^9 \equiv 7 \pmod{13}$ has a solution if, and only if $\text{ind}_2 4 + 9\,\text{ind}_2 x \equiv \text{ind}_2 7 \pmod{\varphi(13)}$ has a solution; i.e., if and only if, $\exists\, x \pmod{12}$ such that $9\,\text{ind}_2 x \equiv \text{ind}_2 7 - \text{ind}_2 4 \equiv 11 - 2 \pmod{12}$

This has $(9, 12) = 3$ solns because $\text{ind}_2 x \equiv 1 \pmod 3$ has a solution; namely $3\,\text{ind}_2 x \equiv 1 \pmod 3$.

So, $9\,\text{ind}_2 x \equiv 9 \pmod{12}$ has 3 solutions:

$\text{ind}_2 x = 1, 5$ or 9. Now, by table, $x \equiv 2, 6, 5 \pmod{13}$. □

Here is a criteria for solvability.

Prop: Let n be an integer possessing a primitive root and $a \in \mathbb{N}$ such that $\gcd(a,n)=1$; i.e., $\mathbb{Z}_n^* = \langle r \rangle$ cyclic and $a \in \mathbb{Z}_n^*$. Then, $x^t \equiv a \pmod n$ has a solution if, and only if, $a^{\varphi(n)/d} \equiv 1 \pmod n$, where $d = \gcd(t, \varphi(n))$, in which case, there are exactly d solutions mod n to $x^t \equiv a \pmod n$.

Proof. Taking indices, $a^{\varphi(n)/d} \equiv 1 \pmod n$ is equivalent to $\frac{\varphi(n)}{d} \operatorname{ind}_r a \equiv 0 \pmod{\varphi(n)}$, which in turn is equivalent to $d \mid \varphi(n)$. Further, this is equivalent to the solvability of $x^t \equiv a \pmod n$. □

Ex 3: (Linear congruence) Let $\mathbb{Z}_n^* = \langle r \rangle$ and $(a,b) \in \mathbb{Z}_n^*$. Then, the linear congruence $ax \equiv b \pmod{n}$ (1) is equivalent to $\text{ind}_r a + \text{ind}_r x = \text{ind}_r b \pmod{\varphi(n)}$. Taking $\text{ind}_r x$ as the variable y, (1) has a solution if and only if $y = \text{ind}_r b - \text{ind}_r a \pmod{\varphi(n)}$ has a solution.

For illustration, consider $9x \equiv 13 \pmod{47}$. —(1)

By calculation $r = 5$ is a (infact, smallest ~~prime~~ primitive root of 47).

(1) has a solution iff $\text{ind}_5 x \equiv \text{ind}_5 13 - \text{ind}_5 9 \pmod{46}$ has a solution. By calculation, $\text{ind}_5 13 = 11$ and $\text{ind}_5 9 = 40$. If $\text{ind}_5 x = 11 - 40 = -29 \equiv 17 \pmod{46}$ again by calculation, $x \equiv 38 \pmod{47}$. □

Ex 2: (Binomial congruence) $x^t \equiv a \pmod n$ —(1) has a solution if, and if, $t \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\varphi(n)}$ —(2) has a solution for $y = \operatorname{ind}_r x$. Of course, here, $\mathbb{Z}_n^* = \langle r \rangle$ and $a \in \mathbb{Z}_n^*$.

(2) has a solution **iff** $\operatorname{ind}_r a$ is divisible by $d = (t, \varphi(n))$ **and** in this case, it has d solutions.

Illustration: Consider $x^8 \equiv a \pmod{17}$ — (1)

Then, $d = (8, \varphi(17)) = (8, 16) = 8$. $r \equiv 3 \pmod{17}$ is a primitive root $\pmod{17}$; i.e., $\mathbb{Z}_{17}^* = \langle 3 \rangle$.

By calculation, 1 and 16 are the only integers in $\mathbb{Z}_{17}^*$ whose index is divisible by 8. In fact, $\operatorname{ind}_3 1 = 0$ and $\operatorname{ind}_3 16 = 8$. So, (1) has NO solutions if $a \neq 1, a \neq 8$.

If $a = 1$, (1) is equivalent to $8 \operatorname{ind}_3 x \equiv 0 \pmod{16}$ —(2)

If $a = 16$, (1) — " — $8 \operatorname{ind}_3 x \equiv 1 \pmod{16}$ —(3)

The solutions of (2) are those integers $x \in \mathbb{Z}_{17}^*$ which have even index 2 (relative to 3); i.e., quadratic residues:

$$x = 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$$

The solutions of (3) are those integers $x \in \mathbb{Z}_{17}^*$ such that $\text{ind}_3 x$ is odd. By looking at the $\text{ind}_3 x$ tables for $\mathbb{Z}_{17}^*$, we see that

$$x = 3, 5, 6, 7, 10, 11, 12, 14 \pmod{17}. \quad \square$$

$n = 17, r = 3.$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Example 5: (Exponential congruence) Let $\mathbb{Z}_n^* = \langle r \rangle$, $a, b \in \mathbb{Z}_n^*$. The congruence

$$a^x \equiv b \pmod{n} \quad \text{— (1)}$$

has a solution for $x \bmod \varphi(n)$ if, and only if,

$$x \, \text{ind}_r a \equiv \text{ind}_r b \pmod{\varphi(n)} \quad \text{— (2)}$$

has a solution $\pmod{\varphi(n)}$

Let $d = (\text{ind}_r a, \varphi(m))$. Then, the linear congruence (2) has a solution iff $d \mid \text{ind}_r b$ in which case there are exactly d solutions.

Illustration: Consider $25^x \equiv 17 \pmod{47}$. —(1)

- $\mathbb{Z}_{47}^* = \langle 5 \rangle$, $\text{ind}_5 25 = 2$, $\text{ind}_5 17 = 16$, $d = (2, 46) = 2$.
- (1) has a solution (mod 47) iff $2x \equiv 16 \pmod{46}$ —(2) has a solution. (2) has 2 solutions $x \equiv 8$ and $31 \pmod{46}$. These are also solutions of (1) (mod 47). □