for a suitable choice of k, where $1 \leq k \leq \phi(n)$. This allows us to frame the following definition.

DEFINITION 8-3. Let r be a primitive root of n. If $\gcd(a, n) = 1$, then the smallest positive integer k such that $a \equiv r^k \pmod{n}$ is called the *index of a relative to r*.

One customarily denotes the index of a relative to r by $\operatorname{ind}_r a$ or, if no confusion is likely to occur, by $\operatorname{ind} a$. Clearly, $1 \leq \operatorname{ind}_r a \leq \phi(n)$ and

$$r^{\operatorname{ind}_r a} \equiv a \pmod{n}.$$

The notation $\operatorname{ind}_r a$ is meaningless unless $\gcd(a, n) = 1$; in the future, this will be tacitly assumed.

For example, the integer 2 is a primitive root of 5 and

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^4 \equiv 1 \pmod{5}.$$

It follows that

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

Observe that indices of integers which are congruent modulo n are equal. Thus, when setting up tables of values for $\operatorname{ind} a$, it suffices to consider only those integers a less than and relatively prime to the modulus n. To see this, suppose that $a \equiv b \pmod{n}$, where a and b are relatively prime to n. Since $r^{\operatorname{ind} a} \equiv a \pmod{n}$ and $r^{\operatorname{ind} b} \equiv b \pmod{n}$, we have

$$r^{\operatorname{ind} a} \equiv r^{\operatorname{ind} b} \pmod{n}.$$

Invoking Theorem 8-1, it may be concluded that $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{\phi(n)}$. But, because of the restrictions on the size of $\operatorname{ind} a$ and $\operatorname{ind} b$, this is only possible if $\operatorname{ind} a = \operatorname{ind} b$.

Indices obey rules which are reminiscent of those for logarithms, with the primitive root playing a role analogous to that of the base for the logarithm.

THEOREM 8-11. *If n has a primitive root r and* ind a *denotes the index of a relative to r, then*

(1) $\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{\phi(n)}$,
(2) $\operatorname{ind} a^k \equiv k \operatorname{ind} a \pmod{\phi(n)}$ for $k > 0$,
(3) $\operatorname{ind} 1 \equiv 0 \pmod{\phi(n)}$, $\operatorname{ind} r \equiv 1 \pmod{\phi(n)}$.

Proof: By the definition of index, $r^{\text{ind } a} \equiv a \pmod{n}$ and $r^{\text{ind } b} \equiv b \pmod{n}$. Multiplying these congruences together, we obtain

$$r^{\text{ind } a + \text{ind } b} \equiv ab \pmod{n}.$$

But $r^{\text{ind } (ab)} \equiv ab \pmod{n}$, so that

$$r^{\text{ind } a + \text{ind } b} \equiv r^{\text{ind } (ab)} \pmod{n}.$$

It may very well happen that ind $a +$ ind b exceeds $\phi(n)$. This presents no problem, for Theorem 8-1 guarantees that the last equation holds if and only if the exponents are congruent modulo $\phi(n)$; that is,

$$\text{ind } a + \text{ind } b \equiv \text{ind } (ab) \pmod{\phi(n)}.$$

The proof of property (2) proceeds along much the same lines. For we have $r^{\text{ind } a^k} \equiv a^k \pmod{n}$ while, by the laws of exponents, $r^{k \text{ ind } a} = (r^{\text{ind } a})^k \equiv a^k \pmod{n}$; hence,

$$r^{\text{ind } a^k} \equiv r^{k \text{ ind } a} \pmod{n}.$$

As above, the implication is that ind $a^k \equiv k$ ind $a \pmod{\phi(n)}$. The two parts of (3) should be fairly apparent.

The theory of indices can be used to solve certain types of congruences. For instance, consider the binomial congruence

$$x^k \equiv a \pmod{n}, \qquad k \geq 2$$

where n is a positive integer having a primitive root and $\gcd(a, n) = 1$. By properties (1) and (2) of Theorem 8-11, this congruence is entirely equivalent to the linear congruence

$$k \text{ ind } x \equiv \text{ind } a \pmod{\phi(n)}$$

in the unknown ind x. If $d = \gcd(k, \phi(n))$ and $d \nmid$ ind a, there is no solution. But, if $d \mid$ ind a, then there are exactly d values of ind x which will satisfy this last congruence, hence d incongruent solutions of $x^k \equiv a \pmod{n}$.

The case in which $k = 2$ and $n = p$, with p an odd prime, is particularly important. Since $\gcd(2, p - 1) = 2$, the foregoing remarks imply that the congruence $x^2 \equiv a \pmod{p}$ has a solution if and only if $2 \mid$ ind a; when this condition is fulfilled, there are exactly two solutions. If r is a primitive root of p, then r^k $(1 \leq k \leq p - 1)$ runs through the integers $1, 2, \ldots, p - 1$, in some order. The even powers of r produce the values of a for which the congruence $x^2 \equiv a \pmod{p}$ is solvable; there are precisely $(p - 1)/2$ such choices for a.

Example 8-4

For an illustration of these ideas, let us solve the congruence

$$4x^9 \equiv 7 \pmod{13}.$$

A table of indices can be constructed once a primitive root of 13 is fixed. Using the primitive root 2, we simply calculate the powers $2, 2^2, \ldots, 2^{12}$ modulo 13. Here,

$$\begin{array}{lll} 2^1 \equiv 2, & 2^5 \equiv 6, & 2^9 \equiv 5 \\ 2^2 \equiv 4, & 2^6 \equiv 12, & 2^{10} \equiv 10 \\ 2^3 \equiv 8, & 2^7 \equiv 11, & 2^{11} \equiv 7 \\ 2^4 \equiv 3, & 2^8 \equiv 9, & 2^{12} \equiv 1 \end{array}$$

all modulo 13, and hence our table is

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	7	6

Taking indices, the congruence $4x^9 \equiv 7 \pmod{13}$ has a solution if and only if

$$\text{ind}_2 4 + 9\, \text{ind}_2 x \equiv \text{ind}_2 7 \pmod{12}.$$

The table gives the values $\text{ind}_2 4 = 2$ and $\text{ind}_2 7 = 11$, so that the last congruence becomes $9\, \text{ind}_2 x \equiv 11 - 2 \equiv 9 \pmod{12}$ which in turn is equivalent to $\text{ind}_2 x \equiv 1 \pmod{4}$. It follows that

$$\text{ind}_2 x = 1, 5, \text{ or } 9.$$

Consulting the table of indices again, we find that the congruence $4x^9 \equiv 7 \pmod{13}$ possesses the three solutions

$$x \equiv 2, 5, \text{ and } 6 \pmod{13}.$$

If a different primitive root is chosen, one obviously obtains a different value for the index of a; but, for purposes of solving the given congruence, it does not really matter which index table is available. The $\phi(\phi(13)) = 4$ primitive roots of 13 are obtained from the powers 2^k $(1 \leq k \leq 12)$, where

$$\gcd(k, \phi(13)) = \gcd(k, 12) = 1.$$

These are

$$2^1 \equiv 2,\ 2^5 \equiv 6,\ 2^7 \equiv 11,\ 2^{11} \equiv 7 \pmod{13}.$$