The index table for, say, the primitive root 6 is displayed below:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_6 a$	12	5	8	10	9	1	7	3	4	2	11	6

Employing this table, the congruence $4x^9 \equiv 7 \pmod{13}$ is replaced by

$$\text{ind}_6 4 + 9 \text{ ind}_6 x \equiv \text{ind}_6 7 \pmod{12}$$

or rather,

$$9 \text{ ind}_6 x \equiv 7 - 10 \equiv -3 \equiv 9 \pmod{12}.$$

Thus, $\text{ind}_6 x = 1$, 5, or 9, leading to the solutions

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

as before.

The following criterion for solvability is often useful.

THEOREM 8-12. *Let n be an integer possessing a primitive root and let* $\gcd(a, n) = 1$. *Then the congruence* $x^k \equiv a \pmod{n}$ *has a solution if and only if*

$$a^{\phi(n)/d} \equiv 1 \pmod{n},$$

where $d = \gcd(k, \phi(n))$; *if it has a solution, there are exactly d solutions modulo n.*

Proof: Taking indices, the congruence $a^{\phi(n)/d} \equiv 1 \pmod{n}$ is equivalent to

$$\frac{\phi(n)}{d} \text{ ind } a \equiv 0 \pmod{\phi(n)}$$

which in its turn holds if and only if $d \mid \text{ind } a$. But we have just seen that the latter is a necessary and sufficient condition for the congruence $x^k \equiv a \pmod{n}$ to be solvable.

COROLLARY (Euler). *Let p be a prime and* $\gcd(a, p) = 1$. *Then the congruence* $x^k \equiv a \pmod{p}$ *has a solution if and only if* $a^{(p-1)/d} \equiv 1 \pmod{p}$, *where* $d = \gcd(k, p - 1)$.

Example 8-5

Let us consider the congruence

$$x^3 \equiv 4 \pmod{13}.$$

Here, $d = \gcd(3, \phi(13)) = \gcd(3, 12) = 3$ and so $\phi(13)/d = 4$. Since $4^4 \equiv 9 \not\equiv 1 \pmod{13}$, Theorem 8-12 asserts that the given congruence is not solvable.

On the other hand, the same theorem guarantees that

$$3x^4 \equiv 5 \pmod{11}$$

will possess a solution (in fact, there are three incongruent solutions modulo 13); for, in this case, $5^4 \equiv 625 \equiv 1 \pmod{13}$. These solutions can be found by means of the index calculus as follows: The congruence $x^3 \equiv 5 \pmod{13}$ is equivalent to

$$3 \operatorname{ind}_2 x \equiv 9 \pmod{12},$$

which becomes

$$\operatorname{ind}_2 x \equiv 3 \pmod{4}.$$

This last equation admits three incongruent solutions modulo 12, namely

$$\operatorname{ind}_2 x = 3, 7, \text{ or } 11.$$

The integers corresponding to these indices are, respectively, 7, 8, and 11, so that the solutions of the congruence $x^3 \equiv 5 \pmod{13}$ are

$$x \equiv 7, 8, \text{ and } 11 \pmod{13}.$$

PROBLEMS 8.4

1. Find the index of 5 relative to each of the primitive roots of 13.
2. Using a table of indices for a primitive root of 11, solve the congruences (a) $7x^3 \equiv 3 \pmod{11}$ (b) $3x^4 \equiv 8 \pmod{11}$ (c) $x^8 \equiv 10 \pmod{11}$
3. The following is a table of indices for the prime 17 relative to the primitive root 3:

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

With the aid of this table, solve the congruences

(a) $x^{12} \equiv 13 \pmod{17}$ (b) $8x^5 \equiv 10 \pmod{17}$
(c) $9x^8 \equiv 8 \pmod{17}$ (d) $7^x \equiv 7 \pmod{17}$

4. Find the remainder when 3^{3^3} is divided by 17. [*Hint:* Use the theory of indices.]

5. If r and r' are both primitive roots of the odd prime p, show that for $\gcd(a, p) = 1$

$$\operatorname{ind}_{r'} a \equiv (\operatorname{ind}_r a)(\operatorname{ind}_{r'} r) \pmod{p-1}.$$

This corresponds to the rule for changing the base of logarithms.

6. (a) Construct a table of indices for the prime 17 with respect to the primitive root 5. [*Hint:* By the previous problem, $\operatorname{ind}_5 a \equiv 13 \operatorname{ind}_3 a \pmod{16}$.]
(b) Using the table in part (a), solve the congruences in Problem 3.

7. If r is a primitive root of the odd prime p, verify that

$$\operatorname{ind}_r(-1) = \operatorname{ind}_r(p-1) = \tfrac{1}{2}(p-1).$$

8. (a) Determine the integers a $(1 \leq a \leq 12)$ such that the congruence $ax^4 \equiv b \pmod{13}$ has a solution for $b = 2$, 5, and 6.
(b) Determine the integers a $(1 \leq a \leq p-1)$ such that the congruence $x^4 \equiv a \pmod{p}$ has a solution for $p = 7$, 11, and 13.

9. Employ the corollary to Theorem 8-12 to establish that if p is an odd prime, then
(a) $x^2 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{4}$;
(b) $x^4 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{8}$.

10. Given the congruence $x^3 \equiv a \pmod{p}$, where $p \geq 5$ is a prime number and $\gcd(a, p) = 1$, prove that
(a) if $p \equiv 1 \pmod{6}$, then the congruence has either no solutions or three incongruent solutions modulo p;
(b) if $p \equiv 5 \pmod{6}$, then the congruence has a unique solution modulo p.

11. Show that $x^3 \equiv 3 \pmod{19}$ has no solutions, while $x^3 \equiv 11 \pmod{19}$ has three incongruent solutions.

12. Determine whether the two congruences $x^5 \equiv 13 \pmod{23}$ and $x^7 \equiv 15 \pmod{29}$ are solvable.

13. If p is a prime and $\gcd(k, p-1) = 1$, prove that the integers

$$1^k, 2^k, 3^k, \ldots, (p-1)^k$$

form a reduced set of residues modulo p.

14. Let r be a primitive root of the odd prime p and $d = \gcd(k, p-1)$. Prove that the values of a for which the congruence $x^k \equiv a \pmod{p}$ is solvable are $r^d, r^{2d}, \ldots, r^{[(p-1)/d]d}$.