method, which requires approximately the same number of bit operations to find discrete logarithms modulo a prime p as it would to factor a composite number of about the same size as p. To determine how long it takes to solve the discrete logarithm problem modulo a prime p, consult Table 3.2, which shows how long it takes to factor an integer n of the same number of decimal digits as p. For more information about the discrete logarithm problem, and algorithms for solving it, consult [MevaVa97] and the many references cited there.

Power Residues

Indices are also helpful for studying congruences of the form $x^k \equiv a \pmod{m}$, where m is a positive integer with a primitive root and $(a, m) = 1$. Before we study such congruences, we present a definition.

Definition. If m and k are positive integers and a is an integer relatively prime to m, then we say that a is a *kth power residue of* m if the congruence $x^k \equiv a \pmod{m}$ has a solution.

When m is an integer possessing a primitive root, the following theorem gives a useful criterion for an integer a relatively prime to m to be a kth power residue of m.

Theorem 9.17. Let m be a positive integer with a primitive root. If k is a positive integer and a is an integer relatively prime to m, then the congruence $x^k \equiv a \pmod{m}$ has a solution if and only if

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

where $d = (k, \phi(m))$. Furthermore, if there are solutions of $x^k \equiv a \pmod{m}$, then there are exactly d incongruent solutions modulo m.

Proof. Let r be a primitive root modulo the positive integer m. We note that the congruence

$$x^k \equiv a \pmod{m}$$

holds if and only if

$$k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\phi(m)}. \tag{9.4}$$

Now let $d = (k, \phi(m))$ and $y = \operatorname{ind}_r x$, so that $x \equiv r^y \pmod{m}$. By Theorem 4.10, we note that if $d \nmid \operatorname{ind}_r a$, then the linear congruence

$$ky \equiv \operatorname{ind}_r a \pmod{\phi(m)} \tag{9.5}$$

has no solutions and, hence, there are no integers x satisfying (9.4). If $d \mid \operatorname{ind}_r a$, then there are exactly d integers y incongruent modulo $\phi(m)$ such that (9.5) holds and, hence, exactly d integers x incongruent modulo m such that (9.4) holds. Because $d \mid \operatorname{ind}_r a$ if and only if

$$(\phi(m)/d)\operatorname{ind}_r a \equiv 0 \pmod{\phi(m)},$$

and this congruence holds if and only if

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

the theorem is true. ■

We note that Theorem 9.17 tells us that if p is a prime, k is a positive integer, and a is an integer relatively prime to p, then a is a kth power residue of p if and only if

$$a^{(p-1)/d} \equiv 1 \pmod{p},$$

where $d = (k, p-1)$. We illustrate this observation with an example.

Example 9.21. To determine whether 5 is a sixth power residue of 17, that is, whether the congruence

$$x^6 \equiv 5 \pmod{17}$$

has a solution, we determine that

$$5^{16/(6,16)} = 5^8 \equiv -1 \pmod{17}.$$

Hence, 5 is not a sixth power residue of 17. ◀

A table of indices with respect to the least primitive root modulo each prime less than 100 is given in Table 4 of Appendix E.

Proving Theorem 6.10 This proof of Theorem 6.10 is quite long and complicated, but is based only on results already established. We present this proof to give the reader an indication that even elementary proofs can be difficult to create and hard to follow. As you read this proof, follow each part carefully and check each separate case. We restate Theorem 6.10 for convenience.

Theorem 6.10. If n is an odd composite positive integer, then n passes Miller's test for at most $(n-1)/4$ bases b with $1 \leq b < n-1$.

We need the following lemma in the proof.

Lemma 9.2. Let p be an odd prime and let e and q be positive integers. Then the number of incongruent solutions of the congruence $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p-1))$.

Proof. Let r be a primitive root of p^e. By taking indices with respect to r, we see that $x^q \equiv 1 \pmod{p^e}$ if and only if $qy \equiv 0 \pmod{\phi(p^e)}$, where $y = \operatorname{ind}_r x$. Using Theorem 4.10, we see that there are exactly $(q, \phi(p^e))$ incongruent solutions of $qy = 0 \pmod{\phi(p^e)}$. Consequently, there are $(q, \phi(p^e)) = (q, p^{e-1}(p-1))$ incongruent solutions of $x^q \equiv 1 \pmod{p^e}$. ■

We now proceed with a proof of Theorem 6.10.