divisor greater than 1.

Corollary. *If $a > b$ are relatively prime integers, then 1 can be written as an integer linear combination of a and b in polynomial time, more precisely, in $O(\log^3 a)$ bit operations.*

Definition. Let n be a positive integer. The *Euler phi-function* $\varphi(n)$ is defined to be the number of nonnegative integers b less than n which are prime to n:

$$\varphi(n) \underset{\text{def}}{=} \left|\{0 \le b < n \mid g.c.d.(b, n) = 1\}\right|.$$

It is easy to see that $\varphi(1) = 1$ and that $\varphi(p) = p - 1$ for any prime p. We can also see that for any prime power

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right).$$

To see this, it suffices to note that the numbers from 0 to $p^\alpha - 1$ which are *not* prime to p^α are precisely those that are divisible by p, and there are $p^{\alpha-1}$ of those.

In the next section we shall show that the Euler φ-function has a "multiplicative property" that enables us to evaluate $\varphi(n)$ quickly, provided that we have the prime factorization of n. Namely, if n is written as a product of powers of distinct primes p^α, then it turns out that $\varphi(n)$ is equal to the product of the $\varphi(p^\alpha)$.

Exercises

1. (a) Prove the following properties of the relation $p^\alpha||b$: (i) if $p^\alpha||a$ and $p^\beta||b$, then $p^{\alpha+\beta}||ab$; (ii) if $p^\alpha||a$, $p^\beta||b$ and $\alpha < \beta$, then $p^\alpha||a \pm b$.
   (b) Find a counterexample to the assertion that, if $p^\alpha||a$ and $p^\alpha||b$, then $p^\alpha||a + b$.
2. How many divisors does 945 have? List them all.
3. Let n be a positive odd integer.
   (a) Prove that there is a 1-to-1 correspondence between the divisors of n which are $< \sqrt{n}$ and those that are $> \sqrt{n}$. (This part does not require n to be odd.)
   (b) Prove that there is a 1-to-1 correspondence between all of the divisors of n which are $\ge \sqrt{n}$ and all the ways of writing n as a difference $s^2 - t^2$ of two squares of nonnegative integers. (For example, 15 has two divisors 6, 15 that are $\ge \sqrt{15}$, and $15 = 4^2 - 1^2 = 8^2 - 7^2$.)
   (c) List all of the ways of writing 945 as a difference of two squares of nonnegative integers.
4. (a) Show that the power of a prime p which exactly divides $n!$ is equal to $[n/p] + [n/p^2] + [n/p^3] + \cdots$. (Notice that this is a finite sum.)
   (b) Find the power of each prime 2, 3, 5, 7 that exactly divides 100!, and then write out the entire prime factorization of 100!.