Note that this primality test is probabilistic only in the sense that a randomly chosen a may or may not satisfy condition (ii) (of course, if it fails to satisfy (i), then n is not prime). But once such an a is found (and $a = 2$ will usually work), then the test shows that n is definitely a prime. Unlike the primality tests in §V.1 (the Solovay–Strassen and Miller–Rabin tests), the conclusion of Pocklington's test is a certainty: n is a prime, not a "probable prime."

The elliptic curve primality test is based on an analogous proposition, where we suppose that we have an equation $y^2 = x^3 + ax + b$ considered modulo n. That is, a and b are integers modulo n, and we let E denote the set of all integers $x, y \in \mathbf{Z}/n\mathbf{Z}$ which satisfy the equation, along with a symbol O, which we call the "point at infinity." If n is prime (as is almost certainly the case — since in practice we are only considering numbers n which have already passed some of the probable prime tests in §V.1), then E is an elliptic curve with identity element O.

Before stating the analog of Proposition 6.3.1 for E, we note that, even without knowing that n is prime, we can apply the formulas in §1 to add elements of E. One of three things happens when we add two points (or double a point): (1) we get a well-defined point, (2) if the points are of the form (x, y) and $(x, -y)$ modulo n, then we get the point at infinity, (3) the formulas are undefined, because we have a denominator which is not invertible modulo n. But case (3) means that n is composite, and we can find a nontrivial divisor by taking the *g.c.d.* of n with the denominator. So without loss of generality in what follows we may assume that case (3) never occurs.

It can be shown that for P an element of E modulo n, even if n is composite the answer our algorithm gives for mP does not depend on the particular manner in which we successively add and double points. (This is not *a priori* obvious.) However, this fact will not be needed below. It suffices to let mP denote *any* point which is obtained working modulo n with the formulas in §1.

Just as we can add points modulo n without knowing that n is prime, similarly, given an algorithm for computing the number of points on an elliptic curve (such as Schoof's method), we can apply it to our set E modulo n. We will either obtain some number m — which if n is prime is guaranteed to be the number of points on the *elliptic curve* E — or else encounter an undefined expression whose denominator has a nontrivial common factor with n. As in the case of the addition of points, without loss of generality we may assume that the latter never happens.

Such an m will play the role of $n - 1$ in Proposition 6.3.1 — notice that $n - 1$ is the order of $(\mathbf{Z}/n\mathbf{Z})^*$ if n is prime.

We are now ready to state the elliptic curve analog of Pocklington's criterion.

Proposition 6.3.2. *Let n be a positive integer. Let E be the set given by an equation $y^2 = x^3 + ax + b$ modulo n, as above. Let m be an integer.*