Suppose that there is a prime q dividing m which is greater than $\left(n^{1/4}+1\right)^2$. If there exists a point P of E such that (i) $mP = O$; *and* (ii) $(m/q)P$ *is defined and not equal to O, then n is prime.*

Proof (compare with the proof of Proposition 6.3.1). If n is not prime, then there is a prime $p \leq \sqrt{n}$ which divides n. Let E' be the elliptic curve given by the same equation as E but considered modulo p, and let m' be the order of the group E'. By Hasse's Theorem, we have $m' \leq p+1+2\sqrt{p} = (\sqrt{p}+1)^2 \leq \left(n^{1/4}+1\right)^2 < q$, and hence $g.c.d.(q, m') = 1$, and there exists an integer u such that $uq \equiv 1 \ (mod\ m')$. Let $P' \in E'$ be the point P considered modulo p. Then in E' we have $(m/q)P' = uq(m/q)P' = umP' = O$, by (i), since mP' is obtained using the same procedure as mP, only working modulo $p|n$ rather than modulo n. But this contradicts (ii), since if $(m/q)P$ is defined and $\neq O$ modulo n, then the same procedure working modulo p rather than modulo n will give $(m/q)P' \neq O$. This completes the proof.

This proposition leads to an algorithm for proving that an integer n (which we may suppose is already known to be a "probable prime") is definitely prime. We proceed as follows. We randomly select three integers a, x, y modulo n and set $b \equiv y^2 - x^3 - ax \ (mod\ n)$. Then $P = (x, y)$ is an element of E, where E is given by $y^2 = x^3 + ax + b$. We use Schoof's algorithm (or another method for counting the number of points on an elliptic curve) to find a number m which, if n is prime, is equal to the number of points on the elliptic curve E over $\mathbf{F}_n$. If we cannot write m in the form $m = kq$, where $k \geq 2$ is a small integer and q is a "probable prime" (i.e., it passes a test as in §V.1), then we choose another random triple a, x, y and start again. Suppose we finally obtain an elliptic curve for which m has the desired form. Then we use the formulas in §VI.1 (working modulo n) to compute mP and kP. If we ever obtain an undefined expression — either in computing a multiple of P or in applying Schoof's algorithm — then we immediately find a nontrivial factor of n. We may assume that this doesn't happen. If $mP \neq O$, then we know that n is composite (because if n were prime, then the group E would have order m, and any element of E would be killed by multiplication by m). If $kP = O$ (which is highly unlikely), we are out of luck, and must start again with another triple. But if $mP = O$ and $kP \neq O$, then by Proposition 6.3.2 we know that n is prime, provided that the large factor q of m is really a prime (we only know it to be a "probable prime"). This reduces the problem to proving primality of q, which has magnitude at most about $n/2$. We then start over with n replaced by q. Thus, we obtain a recursive procedure with t repetitions of the primality test, where t is no more than about $\log_2 n$. When we're done, we have obtained a number q_t which we know to be prime, from which it follows that the previous q_{t-1} was really a prime (not just a "probable prime"), from which it follows that the same is true of q_{t-2}, and so on, until $q_1 = q$, and finally n itself is truly a prime. This concludes the description of the elliptic curve primality test.