There are two difficulties with this test, one practical and the other theoretical. In the first place, although Schoof's algorithm takes time polynomial in $log\, n$, in practice it is quite cumbersome. Some progress has been made recently in supplementing and streamlining it, but even so it is rather unpleasant to have to count the number of points on a large number of E until we finally find one for which m has the desired form $m = kq$. In order to deal with this problem, A. O. L. Atkin developed a variant of the elliptic curve primality test using carefully constructed elliptic curves with complex multiplication, for which it is much easier to compute the number of points on their reduction modulo n. For more information on Atkin's method, see the article by Lenstra and Lenstra in the references below.

The second difficulty is theoretical. In order to find an elliptic curve E over $\mathbf{F}_n$ (assuming that n is prime) whose number of points is "almost prime" (i.e., of the form $m = kq$ for k small and q prime), we have to know something about the distribution of primes (rather, of "near primes") in the interval from $p+1-2\sqrt{p}$ to $p+1+2\sqrt{p}$ which, by Hasse's Theorem, is known to contain m. Because the length of this interval is relatively small, there is no theorem which guarantees that we have a high probability of finding such an E after only polynomially many tries (polynomial in $log\, n$). However, there is a very plausible conjecture which would guarantee this, and for practical purposes there should be no problem. But if one wants a provably polynomial time probabilistic algorithm, one has to work much harder: such a primality test was developed by Adleman and Huang using two-dimensional abelian varieties, which are a generalization of elliptic curves to 2 dimensions. However, their algorithm is completely impractical, as well as very complicated.

Exercises

1. (a) In Pocklington's primality test, if n is prime, $n-1$ is divisible by a prime q as in Proposition 6.3.1, and a is chosen at random in $(\mathbf{Z}/n\mathbf{Z})^*$, then what is the probability that a will satisfy the conditions of the proposition?

   (b) In the elliptic curve primality test, if n is prime, one has an elliptic curve of order divisible by a prime q as in Proposition 6.3.2, and P is a random point on it, then what is the probability that P will satisfy the conditions of the proposition?
2. Generalize Pocklington's primality test to the case when one knows an integer s dividing $n-1$ which is greater than $\sqrt{n}-1$ and for which one knows all primes $q|s$. Condition (ii) is required to hold for all $q|s$.
3. (a) (Pépin's primality test for Fermat numbers.) Prove that a Fermat number $n = 2^{2^k} + 1$ is a prime if and only if there exists an integer a such that $a^{2^{2^k-1}} \equiv -1\ mod\ n$. Prove that if n is a prime, then 50% of all $a \in (\mathbf{Z}/n\mathbf{Z})^*$ have this property. Also prove that a can always be chosen to be 3, or 5, or 7, if $k > 1$.