(b) Prove that a Mersenne number $n = 2^p - 1$ is a prime if and only if there exists a point $P = (x, y)$ on the curve $E : y^2 \equiv x^3 + x \ mod\ n$ such that (1) $2^{p-1}P$ can be computed without encountering non-invertible denominators mod n, and (2) $2^{p-1}P$ has y-coordinate zero. To do this, first prove that, if $n = 2^p - 1$ is prime, then the group of points on $E \ mod\ n$ is cyclic of order 2^p, and 50% of all $P \in E \ mod\ n$ have the properties (1)–(2) above. Explain how one can generate random points $P \in E \ mod\ n$. You may use any algorithm that assumes that $b^{n-1} \equiv 1 \ mod\ n$ (i.e., that n is a pseudoprime to various bases b), because if you ever encounter a b for which this fails, your test ends with the conclusion that n must be composite.

Note that this is a probabilistic primality test in the sense that, if n is a prime, there is no guarantee of when a suitable P will turn up. However, once such a P is found, then the test ensures that n *must* be prime. In this respect it is different from the pseudoprime tests in § V.1. For a generalization which can test primality of any odd n, see W. Bosma's paper cited below.

References for § VI.3

1. L. Adleman and M. Huang, "Recognizing primes in random polynomial time," *Proc. 19th Annual ACM Symposium on Theory of Computing*, 1987, 462–469.
2. W. Bosma, "Primality testing using elliptic curves," Report 85–12, Mathematisch Instituut, Universiteit van Amsterdam, 1985.
3. S. Goldwasser and J. Kilian, "Almost all primes can be quickly certified," *Proc. 18th Annual ACM Symposium on Theory of Computing*, 1986, 316–329.
4. A. K. Lenstra and H. W. Lenstra, Jr., "Algorithms in number theory," Technical Report 87–008, University of Chicago, 1987.
5. F. Morain, "Implementation of the Goldwasser–Kilian–Atkin primality testing algorithm," INRIA report 911, 1988.
6. H. Pocklington, "The determination of the prime and composite nature of large numbers by Fermat's theorem," *Proc. Cambridge Philos. Soc.*, **18** (1914–16), 29–30.
7. R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," *Math. Comp.* **44** (1985), 483–494.

4 Elliptic curve factorization

A key reason for the increasing interest in elliptic curves on the part of cryptographers is the recent ingenious use of elliptic curves by H. W. Lenstra to