5. N. Koblitz, Constructing elliptic curve cryptosystems in characteristic 2, *Advances in Cryptology — Crypto '90*, Springer-Verlag, 1991, 156–167.
6. N. Koblitz, Elliptic curve implementation of zero-knowledge blobs, *J. Cryptology* **4** (1991), 207–213.
7. N. Koblitz, CM-curves with good cryptographic properties, *Advances in Cryptology — Crypto '91*, Springer-Verlag, 1992, 279–287.
8. H. W. Lenstra, Jr., "Elliptic curves and number-theoretic algorithms," Report 86–19, Mathematisch Instituut, Universiteit van Amsterdam, 1986.
9. A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Acad. Publ., 1993.
10. A. Menezes, T. Okamoto, and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions on Information Theory IT-39* (1993), 1639–1646.
11. A. Menezes, S. Vanstone, and R. Zuccherato, Counting points on elliptic curves over $\mathbf{F}_{2^m}$, *Math. Comp.* **60** (1993), 407–420.
12. V. Miller, "Use of elliptic curves in cryptography," *Abstracts for Crypto 85*, 1985.
13. A. M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance," *Advances in Cryptology, Proc. Eurocrypt 84*, Springer-Verlag, 1985, 224–314.
14. R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," *Math. Comp.* **44** (1985), 483–494.

3 Elliptic curve primality test

The elliptic curve primality test, due to S. Goldwasser, J. Kilian and (in another variant) A. O. L. Atkin, is an analog of the following primality test of Pocklington based on the group $(\mathbf{Z}/n\mathbf{Z})^*$:

Proposition 6.3.1. *Let n be a positive integer. Suppose that there is a prime q dividing $n-1$ which is greater than $\sqrt{n}-1$. If there exists an integer a such that* (i) $a^{n-1} \equiv 1 \ (mod\ n)$*; and* (ii) $g.c.d.(a^{(n-1)/q}-1, n) = 1$*, then n is prime.*

Proof. If n is not prime, then there is a prime $p \le \sqrt{n}$ which divides n. Since $q > p-1$, it follows that $g.c.d.(q, p-1) = 1$, and hence there exists an integer u such that $uq \equiv 1 \ (mod\ p-1)$. Then $a^{(n-1)/q} \equiv a^{uq(n-1)/q} = a^{u(n-1)} \equiv 1 \ (mod\ p)$ by condition (i), and this contradicts condition (ii).

Remarks. This is an excellent test provided that $n-1$ is divisible by a prime $q > \sqrt{n}-1$, and we have been able to find q (and prove that it's prime). Otherwise, we're out of luck. (This is not quite true — there's a more general version which can be used whenever we have a large divisor of $n-1$ in fully factored form, see Exercise 2 below.)