you take a value of k which is not quite a multiple of $p-1$, and try various values of a. Estimate in terms of k and $p-1$ the probability that you obtain the factor $d=p$ in step 4.

3. For the following values of p and B, find (using a computer if necessary) the fraction of the integers between $p+1-2\sqrt{p}$ and $p+1+2\sqrt{p}$ which have no prime divisors greater than B: (a) $p=109$, $B=3$; (b) $p=109$, $B=19$; (c) $p=1009$, $B=19$; (d) $p=1009$, $B=97$; (e) $p=9973$, $B=97$.
4. Each of the values of n in Exercise 5 of § V.4 has a factor $p<100$. In each case (a)–(k) find this factor by Lenstra's elliptic curve method, choosing $B=5$, $C=120$, $P=(1,1)$, and $E: y^2=x^3+ax-a$ with $a=1,2,\ldots$ (taking a's for which the discriminant is prime to n). In each case, what is the first value of a for which you find the factor, and what is the value of k_1 for which the factor appears as $g.c.d.(\text{denominator}, n)$ in your computation of k_1P?
5. With k given by equation (2), suppose that you find a factor of n in the process of computing k_1P modulo n, where k_1 is a partial product in (2). (Recall that we compute kP by successively multiplying by the ℓ's, proceeding in order of increasing ℓ.) Prove that $k_1P \bmod p = O \bmod p$ for some $p|n$, i.e., rule out the possibility that you obtained a denominator not prime to n in the computation of ℓ times $(k_1/\ell)P$ during one of the stages of the repeated doubling method before the last step.
6. (a) Suppose that for any $a \in \mathbf{Z}$ you have an efficient way of generating a point $P=(x,y)$ such that $y^2 \equiv x^3+ax \bmod n$. Explain why it would *not* be a good idea to use the elliptic curves $y^2=x^3+ax$ with various a's to factor n.
   (b) Same question for the family of elliptic curves $y^2=x^3+b$ with various b's.
7. Suppose you want to increase very slightly the probability that the order of $E \bmod p$ for some $p|N$ is a product of small prime factors by ensuring in advance that 4 divides this order. Describe how to do this.

References for § VI.4

1. H. W. Lenstra, Jr., "Factoring integers with elliptic curves," *Annals of Math.* (2) **126** (1987), 649–673.
2. P. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, *Math. Comp.* **48** (1987), 243–264.
3. J. M. Pollard, "Theorems on factorization and primality testing," *Proc. Cambridge Philos. Soc.* **76** (1974), 521–528.