7. (a) Prove that: $\log n! - (n \log n - n) = O(\log n)$.
   (b) Derive the more precise estimate: $\log n! - ((n+\frac{1}{2})\log n - n) = O(1)$.
   (c) What is the expected value of $\log j$ for a randomly chosen integer j between 1 and y?
8. (a) What is the probability that a randomly chosen set of k vectors in $\mathbf{F}_2^n$ is linearly independent (where $k \leq n$)?
   (b) What is the probability that 5 randomly chosen vectors in $\mathbf{F}_2^5$ are a basis?
9. Let n be an r-bit integer. By what factor does each of the expressions $\sqrt[4]{n}$ (that appears in the time estimate for the rho method) and $e^{\sqrt{r \log r}}$ (that appears in the estimate for the factor base method) increase if n increases from a 50-decimal-digit to a 100-decimal-digit integer?
10. (a) Suppose that $f(s)$ is a positive monotonically decreasing function and $g(s)$ is a positive monotonically increasing function on an interval, and suppose that $f(s_0) = g(s_0)$. Prove that the function $h(s) = f(s) + g(s)$ "essentially" reaches its minimum at s_0, in the sense that the minimum value of $h(s)$ is between $h(s_0)$ and $\frac{1}{2}\, h(s_0)$.
    (b) Suppose that $f(s) > 1$ is a monotonically decreasing function and $g(s) > 1$ is a monotonically increasing function on an interval, and suppose that $f(s_0) = g(s_0)$. Prove that the function $h(s) = f(s)g(s)$ "essentially" reaches its minimum at s_0, in the sense that the minimum value of $h(s)$ is between $h(s_0)$ and $\sqrt{h(s_0)}$.
    (c) Using part (b), show that the function $h(s) = (r/s)^{r/s}\, e^{ks}$ on the interval $(0, r)$ (here k and r are positive constants) "essentially" reaches its minimum when $(r/s)^{r/s} = e^{ks}$.

References for § V.3

1. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea, 1952, p. 357.
2. M. Kraitchik, *Théorie des Nombres*, Vol. 2, Gauthier–Villars, 1926.
3. R. S. Lehman, "Factoring large integers," *Math. Comp.* **28** (1974), 637-646.
4. C. Pomerance, "Analysis and comparison of some integer factoring algorithms," *Computational Methods in Number Theory, Part I*, Mathematisch Centrum (Amsterdam), 1982.

4 The continued fraction method

In the last section, we saw that the factor-base method of finding a nontrivial factor of a large composite integer n works best if one has a good