orders N of all elliptic curves modulo p are known to be distributed fairly uniformly in the interval $p+1-2\sqrt{p} \le N \le p+1+2\sqrt{p}$ where Hasse's Theorem tells us they all fall (except that the density of N's drops off near the endpoints of this interval). Thus, the probability is roughly equal to the chance that a randomly chosen integer of size approximately p is not divisible by any prime $> B$. We already saw in our heuristic time estimate in § V.3 that this probability is approximately u^{-u}, where $u = log\,p/log\,B$. This leads to an estimate of the form $O(e^{C\sqrt{r\,log\,r}})$, where r is the number of bits in n. For a detailed derivation of an estimate for the running time, see Lenstra's article.

More precisely, suppose that n is a positive integer which is not a prime power and is not divisible by 2 or 3. Assuming a plausible conjecture about the distribution of integers not divisible by any prime $> B$ in a small interval around p, Lenstra proves the following probabilistic time estimate for the number of bit operations required to produce a nontrivial divisor of n:

$$e^{\sqrt{(2+\epsilon)log\,p\,log\,log\,p}}, \tag{3}$$

where p is the smallest prime factor of n and ϵ approaches zero for large p. Since always $p < \sqrt{n}$, it follows from (3) that we also have the estimate

$$e^{\sqrt{(1+\epsilon)log\,n\,log\,log\,n}}. \tag{4}$$

The estimate (4) has exactly the same form as the (conjectural) time estimates for the best general factoring methods known. However, Lenstra's method has certain advantages over its competitors:

1. It is the only method which is substantially faster if n is divisible by a prime which is much smaller than $\sqrt{n}$.
2. For this reason, it can be used in combination with other factoring methods when the factorization of certain auxiliary numbers is required. (For example, in the continued fraction method in § V.4, we needed the complete factorization of $b_i^2\ mod\ n$ if it is a product of relatively small primes.)
3. It has a very small storage requirement, unlike most of its competitors.

But perhaps the most exciting feature of Lenstra's factorization algorithm is the use for the first time of elliptic curves, which are among the most richly structured and intensively studied objects in modern number theory and algebraic geometry. This shows that new factoring techniques might be found using unexpected constructions from hitherto unrelated branches of mathematics.

Exercises

1. Use Pollard's method with $k = 840$ and $a = 2$ to try to factor $n = 53467$. Then try with $a = 3$.
2. Suppose that only one of the prime divisors p of n has the property that $p-1$ has no large prime factors. Suppose that in Pollard's algorithm