PRIMALITY AND FACTORIZATION

H.W. Lenstra, Jr.*

This is a brief summary of two lectures on primality testing and factorization methods, with an annotated bibliography.

1. INTRODUCTION

Two fundamental problems from algorithmic number theory are the following:

A. given an integer $n > 1$, how to determine whether n is a prime number or not?

B. if n is not prime, how to find integers $a, b > 1$ such that $n = ab$?

The interest of these problems for cryptography stems from a scheme introduced by Rivest, Shamir and Adleman. For this scheme it is essential that problem A is *easy* and that B is *hard*. In these lectures we shall see to which extent this is actually the case.

2. PRIMALITY

All modern primality testing methods depend on generalizations of *Fermat's theorem*, which asserts that

$$n \text{ prime} \Rightarrow a^n \equiv a \bmod n \quad \text{for all} \quad a \in \mathbb{Z}.$$

The converse of this theorem is wrong; but even if one uses a version that does admit a converse the problem presents itself that not all integers $a \pmod n$ can be tried. In *probabilistic* primality tests this problem is overcome by trying a random sample of values of a. Such tests are practically feasible for numbers n of thousands of decimal digits, and they suffice for cryptographic purposes; on the other hand, they yield no mathematical certainty. Mathematically *rigorous* tests depend on generalizations of Fermat's theorem to algebraic number fields. They can be used to provide rigorous primality proofs for arbitrary prime numbers of up to

* Mathematisch Instituut, Universiteit van Amsterdam,
Roetersstraat 15, 1018 WB Amsterdam, The Netherlands.

several hundreds of decimal digits.

3. *FACTORIZATION*

If n fails to pass a primality test, e.g. because an integer a is found for which $a^n \not\equiv a \bmod n$, then n is certainly not prime, but we do not know a factorization $n = ab$ of n. The best known practical methods to factor n are of a probabilistic nature, but in a way that is different from the probabilistic primality tests: the lack of certainty concerns the running time of the algorithm, not the final result.

At the moment the best performing factorization algorithms are the *continued fraction method* of Morrison and Brillhart and the *quadratic sieve method* of Pomerance. These methods can factor numbers of up to 50 decimal digits approximately. Theoretically the *class group method* of Shanks, in the version of Schnorr and Lenstra, is better, but its practical merits are still unclear. The latter method has several special features that may be relevant for cryptography.

4. REFERENCES

4.1. *General*

[K] KNUTH, D.E., *The art of computer programming*, vol. 2, Seminumerical algorithms, Chapter 4, Addison-Wesley Publ. Comp., Reading, Mass., second edition, 1981.
A standard reference on algorithmic number theory.

[LT] LENSTRA, JR., H.W. & TIJDEMAN, R., *Computational methods in number theory*, Mathematical Centre Tracts 154/155, Mathematisch Centrum, Amsterdam, 1982.
A collection of lectures on several subjects in algorithmic number theory.

[D] DIXON, J.D., Factorization and primality tests, *Amer. Math. Monthly*, to appear.
A survey article that includes recent work.

4.2. *Cryptography*

RIVEST, R.L., SHAMIR, A. & ADLEMAN, L., A method for obtaining digital signatures and public-key cryptosystems, *Comm. of the ACM*, 1978, 21, 120-126.
The original paper about the RSA-scheme. See also [K], pp. 386

-389, and the contribution of P.J. HOOGENDOORN to [LT].

4.3. *Primality tests*

WILLIAMS, H.C., Primality testing on a computer, *Ars Combinatoria*, 1978, 5, 127-185.
An excellent survey of the older methods. See also [K], pp. 374-380.

ADLEMAN, L.M., POMERANCE, C. & RUMELY, R.S., On distinguishing prime numbers from composite numbers, *Ann. Math.*, 1983, 117, 173-206.
This paper presents a new rigorous primality test.

LENSTRA, JR., H.W., Primality testing algorithms, *Séminaire Bourbaki* 1980/81, exposé 576, Lecture Notes in Mathematics 901, 243-257, Springer-Verlag, Berlin, 1981.

COHEN, H. & LENSTRA, JR., H.W., Primality testing and Jacobi sums, *Math. Comp.* , to appear.
These two papers contain theoretical and practical simplifications of the test of Adleman, Pomerance and Rumely. A forthcoming publication of H. COHEN and A.K. LENSTRA will discuss the implementation of the new test.

POMERANCE, C., The search for prime numbers, *Scientific American*, 1982, 247, 6, 122-130.

POMERANCE, C., Recent developments in primality testing, *The Mathematical Intelligencer*, 1981, 3, 97-105.
Two more or less popular accounts. See also my paper in [LT].

4.4. *Factorization methods*

GUY, R.K., How to factor a number, *Proc. Fifth Manitoba Conf. Numer. Math.*, Utilitas, Winnipeg, 1975, 49-89.

MONIER, L., *Algorithmes de factorisation d'entiers*, Thèse de 3^{me} cycle, Orsay, 1980.
These are surveys of older factoring methods; see also [K], section 4.5.4, and the contribution of M. VOORHOEVE to [LT]. Precise analyses of many methods, as well as new techniques, are presented in C. POMERANCE's contribution to [LT]. A discussion of class group methods can be found in R.J. SCHOOF's contribution to [LT], and a new variant in a forthcoming paper by C.P. SCHNORR and myself; extended abstracts of the latter paper are:

SCHNORR, C.P., Monte-Carlo factoring algorithm with finite storage, in: CREMERS, A.B. & KRIEGEL, H.P. (eds), *Theoretical computer science, 6th GI-conference, Dortmund* 1983, Lecture Notes in Computer Science 145, 19-33, Springer-Verlag, Berlin, 1982.

SCHNORR, C.P., A Monte Carlo factoring algorithm with finite storage, *Séminaire de Théorie des Nombres* 1981-1982, exposé 40, Université de Bordeaux I, Bordeaux, 1982.

Note. This bibliography is by no means complete. Further references, in particular to the older literature, can be found in the papers mentioned above.