Lenstra, A. K.; **Lenstra, H. W. jun.**; **Lovász, László**
Factoring polynomials with rational coefficients. (English) Zbl 0488.12001
Math. Ann. 261, 515-534 (1982).

For a scan of this review see the web version.

MSC:

11Y16 Number-theoretic algorithms; complexity
11C08 Polynomials in number theory
11R09 Polynomials (irreducibility, etc.)
68W30 Symbolic computation and algebraic computation

Keywords:

polynomial-time algorithm; factorization of primitive polynomials; algorithm for basis reduction; diophantine approximation; operations research; cryptography

Full Text: DOI EuDML

References:

[1] Adleman, L.M., Odlyzko, A.M.: Irreducibility testing and factorization of polynomials, to appear. Extended abstract: Proc. 22nd Annual IEEE Symp. Found. Comp. Sci., pp. 409-418 (1981)

[2] Brentjes, A.J.: Multi-dimensional continued fraction algorithms. Mathematical Centre Tracts 145. Amsterdam: Mathematisch Centrum 1981 · Zbl 0471.10024

[3] Cantor, D.G.: Irreducible polynomials with integral coefficients have succinct certificates. J. Algorithms2, 385-392 (1981) · Zbl 0489.68035 · doi:10.1016/0196-6774(81)90036-5

[4] Cassels, J.W.S.: An introduction to the geometry of numbers. Berlin, Heidelberg, New York: Springer 1971 · Zbl 0209.34401

[5] Ferguson, H.R.P., Forcade, R.W.: Generalization of the Euclidean algorithm for real numbers to all dimensions higher than two. Bull. Am. Math. Soc.1, 912-914 (1979) · Zbl 0424.10021 · doi:10.1090/S0273-0979-1979-14691-3

[6] Hardy, G.H., Wright, E.M.: An introduction to the theory of numbers. Oxford: Oxford University Press 1979 · Zbl 0423.10001

[7] Knuth, D.E.: The art of computer programming, Vol. 2, Seminumerical algorithms. Reading: Addison-Wesley 1981 · Zbl 0477.65002

[8] Lenstra, A.K.: Lattices and factorization of polynomials, Report IW 190/81. Amsterdam: Mathematisch Centrum 1981 · Zbl 0477.12002

[9] Lenstra, H.W., Jr.: Integer programming with a fixed number of variables. Math. Oper. Res. (to appear)

[10] Mignotte, M.: An inequality about factors of polynomials. Math. Comp.28, 1153-1157 (1974) · Zbl 0299.12101 · doi:10.1090/S0025-5718-1974-0354624-3

[11] Pritchard, P.: A sublinear additive sieve for finding prime numbers. Comm. ACM24, 18-23 (1981) · Zbl 0454.68084 · doi:10.1145/358527.358540

[12] Barkley Rosser, J., Schoenfeld, L.: Approximate formulas for some functions of prime numbers. Ill. J. Math.6, 64-94 (1962) · Zbl 0122.05001

[13] Yun, D.Y.Y.: The Hensel lemma in algebraic manipulation. Cambridge: MIT 1974; reprint: New York: Garland 1980

[14] Zassenhaus, H.: On Hensel factorization. I. J. Number. Theory1, 291-311 (1969) · Zbl 0188.33703 · doi:10.1016/0022-314X(69)90047-X

[15] Zassenhaus, H.: A remark on the Hensel factorization method. Math. Comp.32, 287-292 (1978) · Zbl 0383.12003 · doi:10.1090/S0025-5718-1978-0476692-4

[16] Zassenhaus, H.: A new polynomial factorization algorithm (unpublished manuscript, 1981)