of discriminant 5 to the canonical form *X2 XY Y2*, where s5 is the odd root of *x2* = 5 mod *p*.

This reduction algorithm, outlined by Gauss and cleverly reported in Buell [3], was described in a masterly fashion in Mathews’ book [13], and thus it will be referred to as Mathews’ reduction. It can be applied to any quadratic form of a non-perfect square discriminant. The square root s5 may be computed with deterministic polynomial complexity by distinguishing whether *p* is congruent 3 or 1 modulo 4. In the first case, s5 is one of the two square roots mod *p*, and the computation clearly has deterministic polynomial complexity. In the second case Schoof’s algorithm [18, 21] is applied to compute both and modulo *p*, thus s5 is one of the two values mod *p*. Schoof’s algorithm evaluates a square root modulo p in a number of arithmetical operations of order *O(logt p)* with t 10, that is with deterministic polynomial complexity [18]. A description of Schoof’s algorithm can be found in the original paper [18] or in Washington’s book [21], and is based on properties of elliptic curves that are briefly summarized.

........

1. **Representation of primes in Z()**

........

1. **Computational remarks**

The representations of primes  *Q()* as the sums of two squares, established by Theorems 2 and 3, are computed with deterministic poly-nomial complexity using procedures that will be described separately for the different cases.

1. *Primes* *p* 13, 17 mod 20

The representation p = a2 + b2 does not need any further comment, since p = 1 mod 4 is the sum of two integer squares by Fermat’s theorem, and its computation was shown in Section 2.

1. *Primes p*

*y0F2k+1*)

......

1. **Conclusions**

The representation of primes as sums of two squares in Z() allows us to formulate a theorem concerning the representation of any integer in Z():

**Theorem 4.** *In the field Q(), any totally positive integer*

.....

The computation of the two-square representation of any element in Z() is equivalent to factoring, as in Z, therefore at the present time only the two-square representations of primes can be computed with deterministic polynomial complexity.

**References**

1. B. Berndt and R. Evans, Sums of Gauss, Jacobi and Jacobsthal, *Journal* *of Number Theory*, Vol. 11 (1979), pp. 349–398.
2. J. Brillhart, Note on representing a prime as a sum of two squares, *Mathematics of Computation*, Vol. 26 (1972), pp. 1011–1013.
3. D. A. *Buell, Binary Quadratic Forms*, Springer-Verlag, New York, 1989.
4. D. A. Cox, *Primes of the Form*, Wiley, New York, 1989.
5. F. W. Dodd, *Number Theory in the Quadratic Field with Golden Section Unit*, Polygonal Pub. House, Paissac, 1983.
6. C.F. Gauss, *Disquisitiones Arithmeticae*, Springer-Verlag, New York, 1986.
7. G. H. Hardy and E. M. Wright, An *Introduction to the Theory of Numbers*, Oxford University Press, Oxford, 1971.
8. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1998.
9. D. E. Knuth, *The Art of Computer Programming: Seminumerical Algo-rithms*, Addison-Wesley, Reading, 1970.
10. S. Lang, *Elliptic Functions*, Springer-Verlag, New York, 1987.
11. F. Lemmermeyer, *Reciprocity Laws*, Springer-Verlag, New York, 2000.
12. R. Lidl and H Niederreiter, *Finite Fields*, Addison-Wesley, Reading