On Sequences of Integers of Quadratic Fields and Computations

Nihal Bircan

Berlin University of Technology, Institute for Mathematics, MA 8 − 1, Strasse des 17. Juni 136 D-10623 Berlin, Germany
Çankırı Karatekin University, Department of Mathematics, TR 18100, Çankırı, Turkey
bircan@math.tu-berlin.de

April 5, 2012

In our studies, we investigate the following problems;

- Let $O = \mathbb{Z}[\sqrt{d}]$ be the ring of integers of the real quadratic field $\mathbb{Q}(\sqrt{d})$ and $\varepsilon > 1$ its fundamental unit. Defining $O_f = \mathbb{Z}[f\sqrt{d}]$ for the order of conductor f, what can be said about the smallest positive integer $n(f)$ such that $\varepsilon^{n(f)} \in O_f$?
- What can be said about $n(fp^k)$, where p is an odd prime and k is a positive integer?

Considering the questions above we compute best possible upper bounds for $n(f)$. We consider matrices $A \in \mathrm{GL}(2, \mathbb{Z})$ and we show how the integers α of any quadratic field $\mathbb{Q}(\sqrt{d}\,)$ can be embedded in $\mathrm{GL}(2, \mathbb{Z})$ where $d = 4q + r \in \mathbb{N}$ is square-free. Namely,

$$\alpha = a + b\sqrt{d}, \ \ a, b \in \mathbb{Z} \ \text{ if } r = 2, 3, \ \ \alpha = \tfrac{1}{2}(a + b\sqrt{d}), \ \ a, b \in \mathbb{Z}, \ a + b \in 2\mathbb{Z} \ \text{ if } r = 1.$$

We find the n such that $A^n = I$ or $A^n = cI$ in the residue field $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime and A is defined by

$$A = \begin{pmatrix} a & b \\ bd & a \end{pmatrix} \text{ for } r = 2, 3, \ \ A = \begin{pmatrix} \frac{1}{2}(a + b) & b \\ qb & \frac{1}{2}(a - b) \end{pmatrix} \text{ for } r = 1.$$

Let s =det A and x =tr A, the trace of A. We derive formulas for all $s \neq 0$. As a tool we always use modified Chebyshev polynomials $t_n(x; s)$ and $u_n(x; s)$ which are monic polynomials with integer coefficients. We obtain some results for A^n and formulate these results in terms of $t_n(x; s)$ =tr A^n. The Legendre symbol $\ell := ((x^2 - 4s)/p)$ and the values of n with $A^n \equiv I \pmod p$ are connected with $p - 1$ if $\ell = +1$ and with $p + 1$ if $\ell = -1$. We also prove that if $s = 1$ and $x^2 - 4 \not\equiv 0$ then $t_{\frac{p-\ell}{2}}(x) \equiv 2((x + 2)/p)$ and we generalize this result. We determine the first $n = (p - \ell)/2^m$ with $t_n(x) \equiv 2 \mod p$ in terms of a chain of Legendre symbols. We also consider the more complicated case $s = -1$ and prove similar results.[BiPo]
For the second question we consider the sequence $n(fp^k)$, $k \geq 0$ for a fixed f and any odd prime p. We consider the case $\frac{p\pm1}{2}$ in detail and we always investigate the properties modulo p. We allow any norm $N(\alpha) \neq 0$. We can write the powers as

$$\alpha^n = \begin{cases} \frac{1}{2}t_n(2a) + u_{n-1}(2a)b\sqrt{d} & \text{if } r = 2, 3 \\ \frac{1}{2}t_n(a) + \frac{1}{2}u_{n-1}(a)b\sqrt{d} & \text{if } r = 1. \end{cases}$$

Finally, we compute the frequencies of $k = \frac{p\pm1}{2n(p)}$ for $N(\alpha) = +1$ and $k = \frac{p\pm1}{n(p)}$ for $N(\alpha) = -1$. Our numerical results suggest that the frequencies should have a limit as the ranges of d and p go to infinity.[Bir]

References

[AbSt72] M.Abramowitz and I.A.Stegun, Handbook of mathematical functions, Dover Publications, New York, 1972

[BCP] W. Bosma, J. Cannon, C. Playoust, The Magma Algebra system I. The User Language, J. Symbolic Comput., 1997, 24(3 − 4), 235 − 265

[Bir] N.Bircan, A Conjecture connected with units of quadratic fields, preprint (2011)

[De79] J. Denef, The Diophantine problem for polynomial rings of positive characteristic, Logic Colloquium 78, North-Holland Publishing Company, 1979

[Jar05] J.H.Jaroma, On the rank of apparition of composite N in Lehmer sequences, Nonlinear Analysis, 2005, 63, $e1081 - e1086$

[JLW] M. J. Jacobson, R. F. Lukes, H. Williams, An investigation of bounds for the regulator of quadratic fields, Experiment. Math., 1995, vol. 4, No 3

[JaWi09] M.J.Jacobson jr. and H.C.Williams, Solving the Pell equations, Springer-Verlag, 2009

[Le30] D.H.Lehmer, An extended theory of Lucas functions, Ann. of Math., 1930, 31, 419 − 448

[Ki89] P.Kiss, On rank of apparition of primes in Lucas sequences, Publ.Math. Debrecen, 1989, 36, 147 − 151

[MaRe03] C.Maclachlan and A.W.Reid, The arithmetic of hyperbolic 3-manifolds, Springer-Verlag, New York, 2003

[MOS66] W.Magnus, F.Oberhettinger and R.P.Soni, Formulas and theorems for the special functions of mathematical physics, Springer-Verlag Berlin, 1966 —

[BiPo] N.Bircan, C.Pommerenke, On Chebyshev polynomials and $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$, preprint(2012)

[PoZa] M. Pohst, H. Zassenhaus, Algorithmic algebraic number theory, Cambridge University Press, 1989.

[Wa38] M.Ward, Arithmetical properties of sequences in rings, Ann. of Math., 1938, 39, 210 − 219