On Sequences of Quadratic Fields and Computations

Nihal Bircan {bircan@math.tu-berlin.de}

Berlin University of Technology, Institute for Mathematics, MA 8 – 1, Strasse des 17. Juni 136 D-10623 Berlin, Germany, 2012
Çankırı Karatekin University, Department of Mathematics, TR 18100, Çankırı, Turkey

Motivation

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 the 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?

First, we aim to get numerical information about

$$n(f) = n(p) = min\{\nu \in \mathbb{N} : \varepsilon^{\nu} \in O_p\}.$$

We compute good upper bounds for $n(f)$ for the cases $N(\varepsilon) = \pm 1$. It is known that for $\left(\frac{d}{p}\right) = \mp 1$, $n(f) = n(p)$ is always a divisor of $\frac{p\pm1}{2}$ if $N(\varepsilon) = +1$ and of $p \pm 1$ if $N(\varepsilon) = -1$. Our results become easier to state if we consider the quotients q defined by

$$q = \begin{cases} \frac{p\pm1}{2n(p)} & \text{if } N(\varepsilon) = +1 \quad \text{where } \left(\frac{d}{p}\right) = \mp 1 \\ \frac{p\pm1}{n(p)} & \text{if } N(\varepsilon) = -1 \quad \text{where } \left(\frac{d}{p}\right) = \mp 1. \end{cases} \tag{1}$$

We compute the frequencies of q. 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 consider matrices $A \in \mathrm{GL}(2,\mathbb{Z})$; 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.
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

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

Computations and Conjecture

For $m \in \mathbb{N}$ we define four sequences according to the formula (1);

- $F_1(q;m) = \#\{q = (p-1)/2n(p) : d,\ p \leq m, \left(\frac{d}{p}\right) = +1,\ N(\varepsilon) = +1\}$.
- $F_2(q;m) = \#\{q = (p+1)/2n(p) : d,\ p \leq m, \left(\frac{d}{p}\right) = -1,\ N(\varepsilon) = +1\}$.
- $F_3(q;m) = \#\{q = (p-1)/n(p) : d,\ p \leq m, \left(\frac{d}{p}\right) = +1,\ N(\varepsilon) = -1\}$.
- $F_4(q;m) = \#\{q = (p+1)/n(p) : d,\ p \leq m, \left(\frac{d}{p}\right) = -1,\ N(\varepsilon) = -1\}$.

Let $S_j(m) = \sum_q F_j(q;m)$. In the tables, the line *values* shows the number of total occurencies for the four cases.

The Embedding of the Algebraic Integers of $\mathbb{Q}(\sqrt{d})$ in $\mathrm{GL}(2,\mathbb{Z}/p\mathbb{Z})$ and the Adapted Chebyshev Polynomials

Let $s \neq 0$ be a complex parameter and let T_n and U_n be the classical Chebyshev polynomials. For $n \in \mathbb{N}_0$ we define

- $t_n(x) := t_n(x;s) := 2s^{n/2}T_n(\frac{x}{2\sqrt{s}})$,
- $u_n(x) := u_n(x;s) := s^{n/2}U_n(\frac{x}{2\sqrt{s}})$ and set $u_{-1}(x) = 0$.

We consider the quadratic field $\mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is square-free. We write $d = 4q + r$. The (algebraic) integers α of $\mathbb{Q}(\sqrt{d})$ are given by

$$\alpha = \begin{cases} a + b\sqrt{d}, \quad a,b \in \mathbb{Z} & \text{if } r = 2,3 \\ \frac{1}{2}(a + b\sqrt{d}), \quad a,b \in \mathbb{Z},\ a+b \in 2\mathbb{Z} & \text{if } r = 1. \end{cases}$$

Now we define a homomorphism φ of the multiplicative semi-group of integers $\alpha \neq 0$ into $\mathrm{GL}(2,\mathbb{Z})$. For $r = 2,3$ we set

$$\varphi(\alpha) := A = \begin{pmatrix} a & b \\ bd & a \end{pmatrix}$$

whereas for $r = 1$ we set

$$\varphi(\alpha) := A = \begin{pmatrix} \frac{1}{2}(a+b) & b \\ qb & \frac{1}{2}(a-b) \end{pmatrix}.$$

Numerical Results

$N(\varepsilon) = +1, \left(\frac{d}{p}\right) = +1$

q \ d_{max}	10000	20000	40000	60000	80000	100000
1	57.3	56.9	56.9	56.7	56.7	56.6
2	11.8	12.0	12.0	12.1	12.2	12.2
3	9.91	9.89	9.89	9.88	9.86	9.88
4	4.66	4.72	4.64	4.64	4.65	4.67
5	2.86	2.84	2.84	2.84	2.82	2.82
6	1.98	2.05	2.10	2.13	2.14	2.16
7	1.34	1.35	1.34	1.35	1.34	1.34
8	1.12	1.16	1.16	1.16	1.16	1.16
9	1.09	1.08	1.09	1.08	1.09	1.09
10	0.604	0.610	0.609	0.612	0.618	0.619
11	0.530	0.515	0.521	0.518	0.517	0.510
12	0.817	0.823	0.841	0.854	0.866	0.874
13	0.349	0.365	0.363	0.362	0.363	0.363
14	0.294	0.292	0.289	0.292	0.291	0.295
15	0.497	0.489	0.494	0.492	0.491	0.495
16	0.280	0.306	0.302	0.296	0.293	0.293
17	0.216	0.214	0.210	0.214	0.213	0.210
18	0.221	0.229	0.237	0.239	0.238	0.240
19	0.161	0.164	0.159	0.164	0.163	0.162
20	0.233	0.238	0.239	0.236	0.238	0.240
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Values	2249621	8330759	31140582	67496484	116576513	178609439

$N(\varepsilon) = +1, \left(\frac{d}{p}\right) = -1$

q \ d_{max}	10000	20000	40000	60000	80000	100000
1	56.3	56.2	56.0	56.1	56.1	56.1
2	14.5	14.4	14.4	14.3	14.3	14.4
3	9.94	9.97	9.98	9.97	10.0	9.98
4	3.32	3.31	3.36	3.37	3.37	3.34
5	2.77	2.76	2.80	2.80	2.80	2.81
6	2.45	2.48	2.49	2.49	2.49	2.50
7	1.32	1.36	1.35	1.36	1.36	1.35
8	0.868	0.840	0.849	0.836	0.839	0.837
9	1.07	1.10	1.10	1.11	1.12	1.12
10	0.718	0.728	0.721	0.725	0.736	0.729
11	0.512	0.502	0.518	0.518	0.519	0.514
12	0.561	0.566	0.583	0.581	0.578	0.571
13	0.352	0.363	0.352	0.355	0.351	0.354
14	0.341	0.339	0.328	0.339	0.333	0.332
15	0.480	0.487	0.508	0.507	0.508	0.506
16	0.202	0.200	0.206	0.206	0.210	0.209
17	0.190	0.199	0.201	0.201	0.200	0.204
18	0.274	0.268	0.274	0.274	0.272	0.273
19	0.165	0.168	0.169	0.168	0.168	0.165
20	0.177	0.176	0.175	0.175	0.174	0.171
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Values	2272057	8390244	31303879	67789746	117013651	179198341

$N(\varepsilon) = -1, \left(\frac{d}{p}\right) = +1$

q \ d_{max}	40000	60000	80000	100000	200000	400000
1	37.8	37.6	37.6	37.5	37.4	37.5
2	18.7	18.8	18.8	18.8	18.7	18.7
3	6.58	6.56	6.60	6.62	6.64	6.62
4	14.0	14.0	14.0	14.0	14.0	14.0
5	1.90	1.91	1.89	1.90	1.89	1.90
6	3.28	3.30	3.29	3.29	3.31	3.31
7	0.891	0.897	0.899	0.898	0.894	0.892
8	3.46	3.48	3.49	3.51	3.50	3.49
9	0.724	0.716	0.725	0.728	0.733	0.735
10	0.930	0.928	0.936	0.937	0.943	0.938
11	0.352	0.351	0.348	0.340	0.343	0.339
12	0.249	0.250	0.248	0.248	0.249	0.249
13	0.237	0.239	0.240	0.243	0.239	0.245
14	0.440	0.440	0.438	0.442	0.444	0.447
15	0.329	0.329	0.330	0.333	0.333	0.334
16	0.866	0.868	0.863	0.866	0.872	0.874
17	0.140	0.143	0.143	0.140	0.138	0.140
18	0.371	0.371	0.365	0.366	0.369	0.368
19	0.105	0.109	0.108	0.107	0.109	0.109
20	0.705	0.706	0.705	0.702	0.706	0.703
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Values	2812857	5965306	10163034	15404441	56042335	205444859

$N(\varepsilon) = -1, \left(\frac{d}{p}\right) = -1$

q \ d_{max}	40000	60000	80000	100000	200000	400000
1	37.9	37.6	37.6	37.6	37.6	37.5
2	37.1	37.2	37.2	37.2	37.3	37.3
3	6.66	6.65	6.64	6.62	6.61	6.65
4	0.000	0.000	0.000	0.000	0.000	0.000
5	1.90	1.90	1.92	1.90	1.90	1.89
6	6.59	6.60	6.64	6.63	6.64	6.64
7	0.889	0.910	0.897	0.891	0.891	0.899
8	0.000	0.000	0.000	0.000	0.000	0.000
9	0.727	0.732	0.729	0.723	0.731	0.733
10	1.85	1.85	1.84	1.87	1.87	1.88
11	0.344	0.345	0.347	0.351	0.338	0.343
12	0.000	0.000	0.000	0.000	0.000	0.000
13	0.233	0.236	0.238	0.240	0.241	0.239
14	0.895	0.907	0.907	0.900	0.899	0.895
15	0.342	0.336	0.336	0.332	0.334	0.333
16	0.000	0.000	0.000	0.000	0.000	0.000
17	0.135	0.138	0.139	0.140	0.138	0.138
18	0.734	0.741	0.750	0.754	0.742	0.742
19	0.112	0.112	0.113	0.111	0.110	0.110
20	0.000	0.000	0.000	0.000	0.000	0.000
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Values	2828439	5992331	10206629	15464072	56197833	205855014

The computations were done using Magma and Kash3. For instance, for $N(\varepsilon) = +1, \left(\frac{d}{p}\right) = +1$ and $d_{max} = 100000$ computation time is 14.9 hours.

We have

$$s := \det A = \mathrm{Norm}(\alpha) = \begin{cases} a^2 - b^2 d & \text{if } r = 2,3 \\ \frac{1}{4}(a^2 - b^2 d) & \text{if } r = 1, \end{cases}$$

$$x := \mathrm{tr}\, A = \begin{cases} 2a & \text{if } r = 2,3 \\ a & \text{if } r = 1. \end{cases}$$

Since $A^n = \varphi(\alpha^n)$ and φ is injective, we can write

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

All the following congruences will be modulo the odd prime p.

- $x = \mathrm{tr}\, A \in \mathbb{Z}$, $s = \det A \in \mathbb{Z} \setminus \{0\}$.

The Legendre symbol will be abbreviated

- $\ell := (\frac{x^2-4s}{p})$.

We write $p - \ell$ which is thus $p \mp 1$ for $\ell = \pm 1$. For special cases our first theorem is well-known.

Theorem 1. *Let p be an odd prime and suppose that*

$$s \not\equiv 0,\ x^2 - 4s \not\equiv 0.$$

We set $\sigma = 1$ for $\ell = +1$ and $\sigma = s$ for $\ell = -1$.
If $(\frac{s}{p}) = +1$ then

$$t_{\frac{p-\ell}{2}}(x)^2 \equiv 4\sigma, \quad u_{\frac{p-\ell}{2}-1}(x) \equiv 0.$$

If $(\frac{s}{p}) = -1$ then

$$t_{\frac{p-\ell}{2}}(x) \equiv 0, \quad (x^2 - 4s)u_{\frac{p-\ell}{2}-1}(x) \equiv 4\sigma \not\equiv 0.$$

In the next two theorem we assume

- $s = \det A = +1$. All congruences will be modulo the odd prime p .
- $x = \mathrm{tr}\, A$, $\ell = (\frac{x^2-4}{p})$.

Theorem 2. *Let $k \in \mathbb{N}$ divide $p - \ell$ and let $x^2 - 4 \not\equiv 0$. If $x \equiv t_k(y)$ for some $y \in \mathbb{Z}$ then, with $n = \frac{p-\ell}{k}$,*

$$t_n(x) \equiv 2, \quad u_{n-1}(x) \equiv 0, \quad A^n \equiv I.$$

Theorem 3. *If $s = det\, A = 1$ and $x^2 - 4 \not\equiv 0$ then*

$$t_{\frac{p-\ell}{2}}(x) \equiv 2((x+2)/p).$$

Conjecture. *Let $j = 1,2,3,4$. There is a probability distribution $P_j(q)$ such that, for all q,*

$$F_j(q;m)/S_j(m) \to P_j(q) \text{ as } m \to \infty.$$

More precisely: For $j = 1,\ldots,4$ there is a function

$$P_j : \mathbb{N} \to [0,1] \text{ with } \sum_q P_j(q) = 1$$

such that for every $\delta > 0$ there exists m_0 with the property that

$$|F_j(q;m)/S_j(m) - P_j(q)| < \delta$$

for all q and $m \geq m_0$.

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)

[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, N.3

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

[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)

Acknowledgements

- I would like to thank Prof. Dr. Michael E. Pohst for being my PhD supervisor and for his guidance during this work.
- I would like to thank Prof. Dr. Franz Halter-Koch for suggesting these interesting problems.
- I would like to thank Gerriet Möhlmann very much for helping me to implement and repeatedly improve the algorithm.