PODSYPANIN'S PAPER ON THE LENGTH OF THE PERIOD OF A QUADRATIC IRRATIONAL

JOHN ROBERTSON

1. Introduction

The major result in Podsypanin's paper "Length of the period of a quadratic irrational" [11]

$$\ell < O(\Delta^{1/2} \log\log\Delta), \tag{1}$$

where ℓ is the length of the period of the continued fraction expansion of a real quadratic irrational with discriminant Δ (not necessarily a fundamental discriminant), is well known and correct.

But, there are a number of errors in [11], including that the proofs of both lemmas are wrong. Fortunately, all of the errors are easily fixed. I would guess that both lemmas were well-known long before [11] was published.

Here's the list of errors:

(1) His proof of his Lemma 1 is wrong.
(2) His statement of his Lemma 2 is not quite correct, and his proof is wrong.
(3) The misstatement of Lemma 2 carries through to a misstatement of his theorem.
(4) An allusion to a reference for a result is potentially misleading.
(5) There are at least two minor typographical errors.

This note discusses these matters. For Lemma 1 we tell where you can find a proof, and for Lemma 2 we supply a proof along the lines of the proof in [11]. We fill in some other small gaps in the paper. We end with a brief restatement of his main argument in the section titled "Recap."

Date: August 17, 2007.

Really all [11] does is to slightly generalize a result of [15] from the case of a fundamental discriminant to an arbitrary discriminant.

2. The proof of Lemma 1

The first lemma in [11] is

Lemma 1. *We have the inequality*

$$\kappa = \kappa(f) \leq 2f.$$

Here $\kappa(f)$ satisfies $\epsilon_0^{\kappa(f)} = \epsilon$ where ϵ_0 is the fundamental unit of the ring of integers $\mathcal{O}$ of the quadratic field $\mathbf{Q}(\sqrt{d})$ ($d > 1$ squarefree) and ϵ is the fundamental unit of the order of conductor f in $\mathcal{O}$.

A correct proof is easily generated from the results in [9, pp. 94–95] and arguments similar to what is presented there. The result is really about linear recursion equations of the form $a_0 = 0$, $a_1 = 1$,

$$a_{n+1} = u_o a_n - \delta_0 a_{n-1}$$

where u_0 is any positive integer and $\delta_0 = \pm 1$. In addition to the reference just given, this result is easily derived from material in [7, 6], or see [4, Chap. XVII]. For a sketch of a proof, and a lot more information, see [13]. I would very much like to hear of other references, especially for proofs of Lemma 1.

Now we explain why the proof in [11] is not correct. At the bottom of page 921, Podsypanin states

> ... we obtain
>
> $$w_n^2 - u_0 w_n w_{n-1} + \delta_0 w_{n-1}^2 = \delta_0^{n-1}. \ (*)$$
>
> From here it follows that to each value of w_{n-1} there corresponds at most two values of w_n. Together with the relation (12), this shows that there exist at most $2m$ values of the pair (w_{n-1}, w_n) of neighboring values of the sequence $\{w_n\}$, reduced relative to an arbitrary modulus m. From here and from (12) it follows that the sequence $\{w_n\}$ is purely periodic relative to any modulus m, with length of the smallest period $S(m) \leq 2m$.

Relation (12) in [11] is

$$w_0 = 0,\ w_1 = 1,\ w_{n+1} = u_0 w_n - \delta_0 w_{n-1}$$

where $u_0 > 0$ and δ_0 are defined in terms of ϵ_0, the fundamental unit of the field $\mathbb{Q}(\sqrt{D_1})$ with fundamental discriminant D_1:

$$\epsilon_0 = \frac{u_0 + v_0\sqrt{D_1}}{2}$$

and

$$u_0^2 - D_1 v_0^2 = 4\delta_0,\ \delta_0 = \pm 1.$$

Consider $D_1 = 29$, $f = 6$, $m = 6$. The fundamental unit of $\mathbb{Q}(\sqrt{29})$ is

$$\epsilon_0 = \frac{u_0 + v_0\sqrt{29}}{2} = \frac{5 + 1 \cdot \sqrt{29}}{2}$$

and $\delta_0 = -1$. So, the sequence (12) is

$$w_0 = 0,\ w_1 = 1,\ w_{n+1} = 5w_n + w_{n-1}.$$

Then the sequence $\{w_n\}$ modulo 6 is:

$$0, 1, 5, 2, 3, 5, 4, 1, 3, 4, 5, 5, 0, 5, 1, 4, 3, 1, 2, 5, 3, 2, 1, 1, 0, 1, 5, \ldots \tag{2}$$

Clearly this has period 24, which is greater than $12 = 2m$.

Podsypanin's argument goes wrong with the quoted sentence beginning, "Together with relationship (12) ...."

First, a quadratic congruence for a composite modulus can have more than two solutions. Secondly, when $\delta_0 = -1$, the equation (*) is two different equations, depending on whether n is even or odd. Continuing the above example with $m = 6$, $u_0 = 5$, and $\delta_0 = -1$, consider $w_{n-1} = 5$. Then the equation (*) becomes

$$w_n^2 - w_n - 2 \equiv 0 \pmod 6 \tag{3}$$

when n is odd, or

$$w_n^2 - w_n \equiv 0 \pmod 6 \tag{4}$$

when n is even. Equation (3) has two solutions, $w_n = 2, 5$, and equation (4) has four solutions, $w_n = 0, 1, 3, 4$. All six of these solutions occur in the sequence (2).

3. The statement and proof of Lemma 2

In [11], Lemma 2 is stated as

$$\ell < \frac{1}{\log \frac{1+\sqrt{5}}{2}} \log \epsilon$$

where ξ is a reduced quadratic irrational, ℓ is the length of the period of the continued fraction expansion of ξ, and ϵ is the fundamental unit for the quadratic order with discriminant that of ξ.

This should be

$$\ell \leq \frac{1}{\log \frac{1+\sqrt{5}}{2}} \log \epsilon$$

because if $\xi = (1+\sqrt{5})/2$, then equality holds ($\ell = 1$ and $\epsilon = \frac{1+\sqrt{5}}{2}$). For all other reduced quadratic irrationals, the strict inequality is correct.

And, the proof given in [11] is wrong. In particular, the statement in the proof that

$$q_t \geq \alpha_0^{t-1}$$

is wrong. Here $\alpha_0 = \frac{1+\sqrt{5}}{2}$ and q_t is the denominator of the t-th convergent to ξ. The rest of the proof hinges on this incorrect statement. The error seems to be due to a minor confusion over indexing.

As Podsypanin uses indexes in continued fractions (see the display equation just before his equation (4)), a purely periodic continued fraction is

$$< \overline{a_1, a_2, \ldots, a_\ell} >,$$

and $q_1 = 1$ and $q_2 = a_2$. Table 1 compares Podsypanin's indexing to the standard indexing. Clearly it is possible to have $q_t < \alpha_0^{t-1}$ under Podsypanin's indexing.

Also, as a specific example, for $\xi = 28 + \sqrt{819}$,

$$q_t = F_t < \alpha_0^{t-1}$$

for $2 \leq t \leq 10$, where F_t is the t-th Fibonacci number ($F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $\ldots$). This is shown in Table 2.

Essentially, what makes his proof fail is the fact that $F_t < \alpha_0^{t-1}$ for $t \geq 2$.

Standard Indexing			Podsypanin's Indexing		
Index t	Minimum Possible q_t	α_0^t	Index t	Minimum Possible q_t	α_0^t
0	1	1.000	1	1	1.618
1	1	1.618	2	1	2.618
2	2	2.618	3	2	4.236
3	3	4.236	4	3	6.854
4	5	6.854	5	5	11.090
5	8	11.090	6	8	17.944
6	13	17.944	7	13	29.034
7	21	29.034	8	21	46.979

Table 1. Where Podsypanin's proof of Lemma 2 goes wrong

Index t	a_t	q_t	α_0^t
1	56	1	1.618
2	1	1	2.618
3	1	2	4.236
4	1	3	6.854
5	1	5	11.090
6	1	8	17.944
7	1	13	29.034
8	1	21	46.979
9	1	34	76.013
10	1	55	122.992
11	56	3114	199.005
12	1	3169	321.997

Table 2. In the continued fraction expansion of $28 + \sqrt{819}$, $q_t < \alpha_0^{t-1}$ for $2 \le t \le 10$

But, a correct proof is not difficult, as we now show. Actually, Podsypanin's erroneous proof provides the main idea. We just rejigger it to get a 2 (or larger) in the right position in the continued fraction expansion of an appropriate ξ. Similarly, the proof in [15] can be generalized to cover all the cases needed here. In essence, we would need to use G_i in place of A_i where $G_i = Q_0 A_i - P_0 B_i$. Then $G_i^2 - DB_i^2 = (-1)^{i+1} Q_0 Q_{i+1}$ [10, Thm. 5.3.4, p. 246]. Here, either $G_i = A_i$, so the proof is as in [15], or $G_i = 2A_i - B_i \geq A_i$ because $A_i - B_i \geq 0$. See [14] for more information on the relations among G_i, Q_i, and solutions to Pell equations.

I am going to change notation to agree with more common conventions. Let $\phi = (1 + \sqrt{5})/2$. For continued fractions, our indexing will start at zero, so a purely periodic continued fraction with period length ℓ will be

$$< \overline{a_0, a_1, \ldots, a_{\ell-1}} > .$$

We will prove

Lemma 2. *If ξ is a reduced quadratic irrational with discriminant $\Delta > 0$ and continued fraction*

$$< \overline{a_0, a_1, \ldots, a_{\ell-1}} >,$$

and ϵ is the fundamental unit for the quadratic order of discriminant Δ, then

$$\epsilon \geq \phi^{\ell}.$$

Equality holds if and only if $\xi = \phi$, in which case $\Delta = 5$, $\epsilon = \phi$, and $\ell = 1$.

Recall that the discriminant of a quadratic irrational is the discriminant of its minimal polynomial. Also recall that the continued fraction expansion of a reduced quadratic irrational is purely periodic. It will be convenient to index the complete quotients as $\xi_0 = \xi, \xi_1, \xi_2, \ldots, \xi_{\ell-1}$. (See [14] or [12] for any terms that are unfamiliar.)

Proof. First observe that if ϵ is the fundamental unit of a quadratic order, then $\epsilon \geq \phi$. To see this, consider that any fundamental unit can be written as

$$\frac{t + u\sqrt{\Delta}}{2}$$

where $t \geq 1$ and $u \geq 1$ are integers, and $\Delta \geq 5$. Clearly this cannot be less than ϕ.

Now consider the case where $\ell = 1$. Since for any ϵ we have $\epsilon \geq \phi$ for those ϵ associated with ξ for which $\ell = 1$, $\epsilon \geq \phi^\ell$ (and, in fact $\xi = \epsilon$).

Now suppose that $\ell > 1$. Then for at least one of the partial quotients we have $a_n \geq 2$ (if all of the partial quotients were 1, the length of the period of the continued fraction would be 1). Replace ξ with ξ_{n-1} (where if $n = 0$ use $\ell - 1$ for $n - 1$). This new ξ is associated with the same discriminant, and so the same ϵ as the original ξ, and the length of the period of its continued fraction expansion is the same as that for the original ξ. The new ξ_1 is the old ξ_n, so the new a_1 is the old a_n.

Now consider the denominators q_i of the convergents to the continued fraction expansion of ξ. As always, $q_0 = 1$. Because $q_1 = a_1 q_0$ and $a_1 \geq 2$, we have that $q_1 \geq 2$. Finally, because $a_i \geq 1$ for $i \geq 2$, $q_i = a_i q_{i-1} + q_{i-2} \geq q_{i-1} + q_{i-2}$ for $i \geq 2$ (actually for $i \geq 0$). In particular $q_2 \geq 3$, $q_3 \geq 5$, and so on.

Recall that $\phi^2 = \phi + 1$, so $\phi^k = \phi^{k-1} + \phi^{k-2}$ for any integer (or real number) k. Now we have that $q_0 = \phi^0 = 1$ and $q_1 > \phi^1$ (because $q_1 \geq 2$ and $\phi < 2$). By an easy induction $q_i > \phi^i$ for $i \geq 1$ because (for $i \geq 2$)

$$q_i \geq q_{i-1} + q_{i-2} > \phi^{i-1} + \phi^{i-2} = \phi^i.$$

We're practically done, because by [5, Theorem 9.5.2, p. 296]

$$\epsilon = q_{\ell-1}\xi + q_{\ell-2}$$

and the fact that $\xi > 1$, we have

$$\epsilon > q_{\ell-1} + q_{\ell-2} > \phi^{\ell-1} + \phi^{\ell-2} = \phi^\ell.$$

□

Note that when $\ell > 1$, the inequality of the lemma is strict. Also, when $\ell = 1$, $\epsilon = \phi$ only when $\xi = \phi$ (and so $\Delta = 5$).

I am grateful to Keith Matthews for pointing out the reference [5, Theorem 9.5.2, p. 296].

In fact, it is easy to see that we have proved a slightly more general result. Namely, if ξ is any real quadratic irrational (not necessarily reduced) with discriminant Δ, ℓ is the length of the periodic part of the continued fraction expansion of ξ, and ϵ is the fundamental unit of the order with discriminant Δ, then $\epsilon \leq \phi^\ell$.

This lemma is proved in [15, Eqn. 2.1] for the quadratic irrational $\sqrt{D}$, D squarefree, which has discriminant $4D$. If you know a proof in the literature for the more general version of this lemma, I would very much like to hear of it.

4. An allusion to a reference

To quote from [11]

> We shall make use of the terminology and results of [1, Chap. 2, Sec. 7]. Let $M = [1, \xi]$, let $\mathcal{O}_f$ be its ring of coefficients with the fundamental unit

$$\epsilon = q_\ell \xi + q_{\ell-1} > 1. \tag{5}$$

He has previously defined ξ as a reduced quadratic irrational with a purely periodic continued fraction expansion

$$< \overline{a_1, a_2, \ldots, a_\ell} >$$

with convergents p_i/q_i. His reference [1] is the same as our reference [1].

Given the juxtaposition of the two sentences quoted, one might expect that the formula for ϵ would appear in [1, Chap. 2, Sec. 7]. If it does, I have not found it.

The formula for ϵ does appear as [5, Theorem 9.5.2, p. 296], where a proof is also given.

5. The statement of the Theorem

Following from Lemma 2 (see discussion above), the conclusion of the Theorem should be

$$\ell \leq \varkappa \frac{D^{\frac{1}{2}} L(1, \chi)}{h}$$

Equality holds if and only if $D = 5$. Here, I have used "$\varkappa$" in place of a symbol in [11] that I cannot reproduce.

6. Two minor typographical errors

I only have access to the English translation, so these typos might not be in the original Russian language paper.

The display equation in the first paragraph, which is not numbered, is missing a factor of 2 in the denominator on the right hand side of the inequality (and, per the comment on the Theorem, just above, the $<$ should be $\leq$). It should read

$$\ell \leq \frac{\omega}{2\log\frac{1+\sqrt{5}}{2}} \cdot \frac{D^{\frac{1}{2}}L(1,\chi)}{h}$$

It should be clear that this is the formula that is the conclusion of the theorem.

Formula (14) is missing a factor of "f" and should read

$$\ell < \frac{\kappa(f)}{\log\alpha_0}\log\epsilon_0 \leq 2f\varkappa\log\epsilon_0$$

(where I have used "$\varkappa$" for a character in [11] that I cannot reproduce).

7. Other comments

The conclusion that $\ell = O(\sqrt{D}\log\log D)$ on line 5 of page 920 of [11] follows from Littlewood's 1928 paper where he proves, subject to the Riemann hypothesis, that $L(1,\chi) = O(\log\log D)$ [8, Thm. 1, p. 367].

Also [15, Lemma, p. 528] has Podsypanin's main results for squarefree D.

8. Recap

Other than the problems noted above, there is nothing wrong with Podsypanin's main argument. In this section, we walk through his argument.

Here is the notation we will use (which differs slightly from Podsypanin's).

$d > 1$ is a squarefree positive integer.
f will denote the conductor of an order in a quadratic field and is a positive integer.
Δ_0 is the discriminant of the ring of integers of the field $\mathbb{Q}(\sqrt{d})$, and so is a fundamental discriminant.
Δ is the discriminant of the order of conductor f in the ring of integers of the field $\mathbb{Q}(\sqrt{d})$.
$\phi = (1 + \sqrt{5})/2$.
$\varkappa = 1/(2\phi)$ if $f = 1$ and $\varkappa = 1/\phi$ if $f > 1$.
ξ is a reduced quadratic irrational.
ℓ is the length of the period of the quadratic irrational ξ.
ϵ_0 is the fundamental unit of the ring of integers of the field $\mathbb{Q}(\sqrt{d})$.
ϵ is the fundamental unit of the order of conductor f in the ring of integers of the field $\mathbb{Q}(\sqrt{d})$.
$\kappa(f)$ is defined by the equation $\epsilon = \epsilon_0^{\kappa(f)}$ and is a positive integer.
$h = h(\Delta)$ is the class number of the order of conductor f in the field $\mathbb{Q}(\sqrt{d})$.
$\chi = \chi_d(n) = \left(\frac{d}{n}\right)$ where $\left(\frac{d}{n}\right)$ is the Kronecker symbol.
$L(1, \chi) = \sum_{n=1}^{\infty} \chi_d(n)/n = \prod_{p \text{ prime}} (1 - \chi_d(p)/p)^{-1}$.

As usual, $\Delta_0 = d$ if $d \equiv 1 \pmod 4$ and $\Delta_0 = 4d$ otherwise. Also, $\Delta = f^2 d$ if $d \equiv 1 \pmod 4$ and $\Delta = 4f^2 d$ otherwise. Each discriminant Δ is associated with a unique pair $\{d, f\}$.

The discriminant Δ associated with the quadratic irrational ξ is the discriminant of the minimal polynomial for ξ.

With that background, we begin the proof. We will prove

Theorem 1. *Let ξ be a reduced quadratic irrational with discriminant $\Delta > 0$ and for which the length of the period of its continued fraction is ℓ. Then*

$$\ell = O(\sqrt{\Delta} \log \log \Delta).$$

Proof. Lemma 1 says that $\kappa(f) \leq 2f$, and obviously $\kappa(1) = 1$. Using this and Lemma 2, we have

$$\ell \leq \frac{\log \epsilon}{\log \phi} = \frac{\kappa(f) \log \epsilon_0}{\log \phi} \leq 2f\varkappa \log \epsilon_0. \tag{6}$$

Dirichlet's analytic class number formula for a fundamental discriminant is [1, p. 343], [3, pp. 134–135], [2, p. 262], [16, p. 273]

$$h = \frac{\sqrt{\Delta_0}\ L(1,\chi)}{2 \log \epsilon_0}.$$

We can rewrite this as

$$\log \epsilon_0 = \sqrt{\Delta_0}\ L(1,\chi)/2h. \tag{7}$$

Combining (6) and (7) we have

$$\ell \leq 2f\varkappa \log \epsilon_0 = 2f\varkappa\sqrt{\Delta_0}\ L(1,\chi)/2h = \varkappa\sqrt{\Delta}\ L(1,\chi)/h \tag{8}$$

(where $L(1,\chi)$ and h are for the fundamental discriminant Δ_0). This is Podsypanin's theorem. From [8, Thm. 1, p. 367] for fundamental discriminants we have that

$$L(1,\chi) = O(\log\log \Delta_0).$$

Because every discriminant Δ has an associated fundamental discriminant Δ_0, and $\Delta_0 \leq \Delta$, we have that

$$L(1,\chi) = O(\log\log \Delta) \tag{9}$$

where $L(1,\chi)$ is the Dirichlet L-function associated with the fundamental discriminant Δ_0 (i.e., the character χ is $\chi_d(n) = \left(\frac{d}{n}\right)$).

Finally, obviously, $\varkappa$ is bounded by a constant and $h \geq 1$, so combining (8) and (9) we have

$$\ell = O(\sqrt{\Delta} \log\log \Delta).$$

□

Podsypanin's equation (3) is proved in [15] for all nonsquare D. How it follows from his theorem is a mystery to me.

Please direct questions and comments to jpr2718@aol.com.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[2] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[3] Harvey Cohn, *A Classical Introduction to Algebraic Numbers and Class Fields*, Springer–Verlag, 1978.

[4] L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, AMS Chelsea Publishing, Providence, Rhode Island, 1999.

[5] Helmut Koch, *Number Theory–Algebraic Numbers and Functions*, translated by David Kramer, AMS, Providence, RI, 2000, Graduate Studies in Mathematics, Vol. 24.

[6] D. H. Lehmer, On the Multiple Solutions of the Pell Equation, *The Annals of Mathematics*, 2nd Ser., Vol. 30, No. 1/4. (1928 - 1929), pp. 66-72.

[7] D. H. Lehmer, An Extended Theory of Lucas' Functions, *The Annals of Mathematics*, 2nd Ser., Vol. 31, No. 3 (July 1930), 419–448.

[8] J. E. Littlewood, On the Class-Number of the Corpus $P(\sqrt{-k})$, *Proc. London Math. Soc*, 1928; s2-27: 358-372.

[9] G. B. Mathews, *Theory of Numbers*, Chelsea, New York, not dated.

[10] Mollin, R. A., *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, 1998.

[11] E. V. Podsypanin, Length of the period of a quadratic irrational (in Russian), Studies in Number Theory, 5, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI)* 82 (1979) 95-99, 166; Engl. transl. in *J. Soviet Math.* 18 (1982) 919-923; MR0537024 (80h:12002).

[12] J. P. Robertson, Computing in quadratic orders, at http://hometown.aol.com/jpr2718/.

[13] J. P. Robertson, Linear recurrences for Pell equations, at http://hometown.aol.com/jpr2718/.

[14] J. P. Robertson, Solving the generalized Pell equation $x^2 - Dy^2 = N$, at http://hometown.aol.com/jpr2718/.

[15] R. G. Stanton, C. Sudler, and H. C. Williams, An upper bound for the period of the simple continued fraction for $\sqrt{D}$, *Pacific Journal of Mathematics*, 67 (1976), 525–536.

[16] Jeffrey Stopple, *A Primer of Analytic Number Theory*, Cambridge University Press, 2003.