Chowla's conjecture

by András BIRÓ

A. Rényi Institute of Mathematics, Hungarian Academy of Sciences

1053 Budapest, Reáltanoda u. 13-15., Hungary; e-mail: biroand@renyi.hu

1. Introduction

The aim of the present paper is to show that the same method which led to the proof of Yokoi's conjecture in our previous paper [B] can be also applied to prove the following conjecture of Chowla.

Let $K = Q(\sqrt{4p^2+1})$, where Q is the rational field and p is a positive integer, $4p^2+1$ is squarefree. S. Chowla conjectured that $h(4p^2+1)$ (i. e. the class number of K) is greater than 1, if $p > 13$. It seems that this conjecture was first mentioned in the literature in the paper [C-F]. Just as in the case of Yokoi's conjecture, Siegel's theorem implies ineffectively that for large p the class number is greater than 1, hence the problem is in fact to find an effective upper bound for p in the class number 1 case.We achieve this goal by proving the following theorem.

THEOREM. *If* $p > 1861$, *then* $h(4p^2+1) > 1$.

What concerns the small solutions, it was proved in [L] that $h(4p^2+1) > 1$ if $13 < p < p_0$, where p_0 is a number much larger than 1861, so we have a full solution (even numerically) of Chowla's conjecture. There are six exceptional fields, belonging to $p = 1, 2, 3, 5, 7, 13$.

We assume throughout the paper that $p > 1861$. Just as in [B], the theorem will follow from two basic facts by elementary number theory and a finite amount of computation. For a real x, denote by $\lceil x \rceil$ the least integer not smaller than x, and let

$$Q(X, Y) = Y^2 - X^2 - 4pXY.$$

FACT A. *If* $4p^2+1$ *is a prime,* $h(4p^2+1) = 1$, q *is an odd integer with* $q > 2$, $(q, 4p^2+1) = 1$, *and* χ *is a primitive character modulo* q *with* $\chi(-1) = -1$, *then*

$$\sum_{a=1}^{q} a\chi(a) \neq 0,$$

and

$$\left(\sum_{(C,D)\in H(q)} \chi(Q(C,D))\lceil(4pC-D)/q\rceil(C-q)\right)\left(\sum_{a=1}^{q} a\chi(a)\right)^{-1}$$

is an algebraic integer, where

$$H(q)=\{(C,D):\ 2C,2D,C-D \text{ are integers, and } 0\le C,D<q\}.$$

FACT B. *If* $h(4p^2+1)=1$, *then* $4p^2+1$ *is a prime, and if* $2<r<p$ *is also a prime, then*

$$\left(\frac{4p^2+1}{r}\right)=-1$$

(Legendre symbol).

The structure of the paper is the same as that of [B]. In each section we show the necessary modifications with respect to the corresponding section of [B], and we omit certain arguments which are explained in detail in [B].

2. Proof of Facts A and B

Let R be the ring of algebraic integers of K, denote by $P(K)$ the set of nonzero principal ideals of R, and let $N(a)$ be the norm of an $a\in P(K)$, i.e. its index in R. Let $q>2$ be an odd integer, χ a character modulo q with $\chi(-1)=-1$. For $\Re s>1$ put

$$\zeta_{P(K)}(s,\chi)=\sum_{a\in P(K)}\frac{\chi(N(a))}{N(a)^s}.$$

Let α be the positive root of the equation $x^2+4px=1$. This time 1, $\frac{1+\alpha^{-1}}{2}$ is an integral basis of R, but it is also true in this case that α^{-1} is the fundamental unit of K; the fundamental totally positive unit of K is α^{-2}. For $\beta\in R$, denote by $\beta^\star$ the algebraic conjugate of β. Any $\beta\in R$ is of the form

$$\beta=C+D\alpha^{-1}$$

with C,D satisfying that $2C,2D$ and $C-D$ are integers; and for this β one has

$$\beta\beta^\star=-Q(C,D).$$

In particular, $Q(C,D)$ is an integer for such numbers C and D (this can be also seen directly).

In order to prove Facts A and B of the paper [B], we needed Lemma 1 and Lemma 2. We prove the analogues of those lemmas for the present case. Then one can derive Facts A and B from Lemmas 1 and 2, respectively, in the same way as in [B]. So we omit those arguments, and we consider Facts A and B as proved once Lemmas 1 and 2 are proved.

In the present case, we have the following expression for the special value at 0.

LEMMA 1. *Using the above notations, $\zeta_{P(K)}(s,\chi)$ extends meromorphically in s for the complex plane and*

$$\zeta_{P(K)}(0,\chi)=\frac{1}{q}\sum_{(C,D)\in H(q)}\chi(Q(C,D))\lceil(4pC-D)/q\rceil(C-q),$$

where $H(q)$ is defined in Fact A.

Proof. The method of Shintani gives again

$$\zeta_{P(K)}(s,\chi)=-q^{-2s}\sum_{0\le C,D\le q-1}\chi(Q(C,D))\sum_{(x,y)\in R(C,D)}\zeta\left(s,\begin{pmatrix}1&\alpha^{-2}\\1&\alpha^{2}\end{pmatrix},(x,y)\right),$$

where the summation is over integers C,D,

$$R(C,D)=\left\{(x,y)\in Q^2:\ 0<x\le 1,\ 0\le y<1,\ x+y\alpha^{-2}-\frac{C+D\alpha^{-1}}{q}\in R\right\},$$

and

$$\zeta\left(s,\begin{pmatrix}a&b\\c&d\end{pmatrix},(x,y)\right)=\sum_{n_1,n_2=0}^{\infty}\left(a(n_1+x)+b(n_2+y)\right)^{-s}\left(c(n_1+x)+d(n_2+y)\right)^{-s}.$$

We can see it in the same way as in [B] (noting that $C+D\alpha^{-1}$ with integers $0\le C,D\le q-1$ form a complete set of representatives of R/qR). Just as in [B] (c_p is a number depending only on p, can be different at different occurrences), we then get

$$\zeta_{P(K)}(0,\chi)=-\sum_{0\le C,D\le q-1}\chi(Q(C,D)\Sigma_{C,D},\tag{1}$$

where

$$\Sigma_{C,D}=\sum_{(x,y)\in R(C,D)}\left(-\frac{(4p)^2}{2}xy-\frac{(4p)^2+4}{4}(x+y)+\frac{(4p)^2+2}{4}(x+y)^2+c_p\right).$$

For any m, n we have

$$\frac{m\alpha^{-1} + n}{q} = \frac{(n - \frac{m}{4p}) + \frac{m}{4p}\alpha^{-2}}{q},$$

and so fixing a pair $0 \leq C, D \leq q-1$, the conditions for (m, n) having $(x, y) \in R(C, D)$ with

$$(x, y) = \left(\frac{1}{q}(n - \frac{m}{4p}), \frac{m}{4qp}\right) \tag{2}$$

(using that q is odd) are that

$$2m, 2n, m - n \text{ are integers,}$$

$$2m \equiv 2D \pmod{q},\ 2n \equiv 2C \pmod{q}$$

and

$$0 \leq 2m < 8qp, \tag{3}$$

$$0 < 2n - \frac{m}{2p} \leq 2q. \tag{4}$$

Then

$$2m = 2D + jq, \tag{5}$$

where

$$j = 0, 1, \ldots, 8p - 1, \text{ if } 0 \leq 2D < q; \tag{6}$$

$$j = -1, 0, \ldots, 8p - 2, \text{ if } q < 2D \leq 2q - 2. \tag{7}$$

If j is fixed, then

$$2n \equiv 2C + jq \pmod{2q},$$

because this is true modulo q, and also modulo 2, since

$$2n \equiv 2m \equiv jq \pmod{2}.$$

Hence

$$2n = 2C + jq + 2Lq \tag{8}$$

with some integer L, and together with (4), this implies

$$L = \left[\frac{m}{4pq} - \frac{2C + jq}{2q} + 1 \right],$$

so

$$L = \left[\frac{m}{4pq} - \frac{C}{q} + 1 \right] - \frac{j}{2}, \text{ if } j \text{ is even,}$$

$$L = \left[\frac{m}{4pq} - \frac{C}{q} + \frac{1}{2} \right] - \frac{j-1}{2}, \text{ if } j \text{ is odd.}$$

Now, by (3) and the conditions for C, we have

$$-1 < \frac{m}{4pq} - \frac{C}{q} < 1,$$

and by (5) we have

$$\frac{m}{4pq} - \frac{C}{q} = \frac{j/2 - (4pC - D)/q}{4p}.$$

It is then clear by (5), (8) and these last conditions that the possibilities for (m, n) having $(x, y) \in R(C, D)$ with (2) are (m_j, n_j), where the conditions for j are (6) and (7), and

$$m_j = D + \frac{j}{2}q;$$

for even j we have

$$n_j = \begin{cases} C \text{ if } j/2 < (4pC - D)/q \\ \\ C + q \text{ if } j/2 \geq (4pC - D)/q \end{cases};$$

for odd j we have

$$n_j = \begin{cases} C - \frac{q}{2} \text{ if } j/2 < ((4pC - D)/q) - 2p \\ \\ C + \frac{q}{2} \text{ if } ((4pC - D)/q) - 2p \leq j/2 < ((4pC - D)/q) + 2p \\ \\ C + \frac{3q}{2} \text{ if } j/2 \geq ((4pC - D)/q) + 2p \end{cases}.$$

This means that

$$\Sigma_{C,D} = \sum_j \left(-\frac{(4p)^2}{2q^2}(n_j - \frac{m_j}{4p})\frac{m_j}{4p} - \frac{(4p)^2 + 4}{4q} n_j + \frac{(4p)^2 + 2}{4q^2} n_j^2 + c_p \right) \tag{9}$$

where the summation is over the integers j satisfying (6) and (7). Let

$$\Sigma_{C,D} = \Sigma_{C,D}^{(e)} + \Sigma_{C,D}^{(o)}, \tag{10}$$

where $\Sigma_{C,D}^{(e)}$ is the sum over the even numbers j in (9), and $\Sigma_{C,D}^{(o)}$ is the sum over the odd numbers. Let us introduce the notation (if $0 \le A \le 4p$ is an integer):

$$F(\delta, \gamma, A) = \sum_{j=0}^{4p-1} \left(-\frac{(4p)^2}{2q^2}(\nu_j - \frac{\mu_j}{4p})\frac{\mu_j}{4p} - \frac{(4p)^2+4}{4q}\nu_j + \frac{(4p)^2+2}{4q^2}\nu_j^2 \right) \tag{11}$$

with

$$\mu_j = \delta + jq,\ \nu_j = \begin{cases} \gamma \text{ if } 0 \le j < A \\ \\ \gamma + q \text{ if } A \le j < 4p \end{cases}.$$

It is then clear that

$$\Sigma_{C,D}^{(e)} = F(D, C, \lceil (4pC - D)/q \rceil) + c_p. \tag{12}$$

For the computation of $\Sigma_{C,D}^{(o)}$, observe that for every fixed C and D in the definition of n_j for odd j we have in fact only two (and not three) cases, because taking into account (6) and (7), we see that if $2C < q$, then

$$j/2 < ((4pC - D)/q) - 2p$$

is impossible, on the other hand, if $2C > q$, then

$$j/2 \ge ((4pC - D)/q) + 2p$$

is impossible. By this remark and (6) and (7), examining a few cases, we see that

$$\Sigma_{C,D}^{(o)} = F(\delta(C,D), \gamma(C,D), A(C,D)) + c_p,$$

where we put

$$\delta(C,D) = \begin{cases} D + \frac{q}{2} \text{ if } 2D < q \\ \\ D - \frac{q}{2} \text{ if } 2D > q \end{cases},$$

similarly

$$\gamma(C,D) = \begin{cases} C + \frac{q}{2} \text{ if } 2C < q \\ \\ C - \frac{q}{2} \text{ if } 2C > q \end{cases},$$

finally

$$A(C,D)=\begin{cases}\lceil((4pC-D)/q)-(1/2)\rceil+2p, & \text{if } 2D<q,\ 2C<q\\ \lceil((4pC-D)/q)+(1/2)\rceil+2p, & \text{if } 2D>q,\ 2C<q\\ \lceil((4pC-D)/q)-(1/2)\rceil-2p, & \text{if } 2D<q,\ 2C>q\\ \lceil((4pC-D)/q)+(1/2)\rceil-2p, & \text{if } 2D>q,\ 2C>q\end{cases}.$$

Observe that writing $\gamma=\gamma(C,D)$, $\delta=\delta(C,D)$, we have

$$A(C,D)=\lceil(4p\gamma-\delta)/q\rceil$$

(this implies in particular $0\le A(C,D)\le 4p$), so

$$\Sigma_{C,D}^{(o)}=F(\delta,\gamma,\lceil(4p\gamma-\delta)/q\rceil)+c_p. \tag{13}$$

(It is not important, but we remark that c_p here is the same as in (12), because in (9) we sum over $4p$ odd and $4p$ even values of j.) Since

$$Q(C,D)\equiv Q(\gamma,\delta)\ (\mathrm{mod}\ q),$$

we get by (1) and formulas (10)-(13) that

$$\zeta_{P(K)}(0,\chi)=-\sum_{(C,D)\in H(q)}\chi(Q(C,D))\left(F(D,C,\lceil(4pC-D)/q\rceil)+c_p\right), \tag{14}$$

since the pairs (C,D) and $(\gamma(C,D),\delta(C,D))$ form the set $H(q)$, if (C,D) runs over the integer pairs with $0\le C,D\le q-1$.

We then proceed just as in [B]. The transformation T is defined on $H(q)$ by the formulas

$$T\left((C,D)\right)=(\hat{C},\hat{D}),$$

$$\hat{C}=D-4pC-q\left[(D-4pC)/q\right],\quad \hat{D}=C.$$

This is a permutation of $H(q)$. As in [B], we put

$$T^2\left((C,D)\right)=(\hat{\hat{C}},\hat{\hat{D}}),$$

($\hat{C}$, $\hat{\hat{C}}$, $\hat{D}$ and $\hat{\hat{D}}$ depend on the pair (C, D)), and using the notation

$$A = \lceil (4pC - D)/q \rceil,$$

we have the relations

$$qA = 4pC - D + \hat{C},\ C = \hat{D},\ \hat{C} = \hat{\hat{D}}.$$

Just as in [B], it is not hard to verify the identity (see (11), and remember that $0 \le A \le 4p$ is an integer)

$$F(D, C, A) = A(1 - \frac{C}{q}) + \Sigma^{(4)}_{C,D} + \Sigma^{(5)}_{C,D} + \Sigma^{(6)}_{C,D} + c_p,$$

where

$$\frac{4q^2}{(4p)}\Sigma^{(4)}_{C,D} = (4p)\left(D\hat{D} + \hat{D}\hat{\hat{D}}\right) + \left(\left(\hat{\hat{D}}\right)^2 - D^2\right),$$

$$-\frac{4q^2}{(4p)^2}\Sigma^{(5)}_{C,D} = D\hat{D} + \hat{D}\hat{\hat{D}},$$

$$4q\Sigma^{(6)}_{C,D} = -2(4p)\left(\hat{D} + D\right) + (4p+2)\left(D - \hat{\hat{D}}\right) + \frac{2(4p)}{q}\left(\left(\hat{D}\right)^2 + D^2\right).$$

Since

$$Q(\hat{C}, \hat{D}) \equiv -Q(C, D) \pmod{q}$$

is also true here, so using (14) and these last identities, the end of the proof is the same as in the case of Lemma 1 of [B]:

$$\Sigma^{(4)}_{C,D},\ \Sigma^{(5)}_{C,D},\ \Sigma^{(6)}_{C,D} \text{ and } c_p$$

give 0 on each orbit of T. So the present lemma is proved.

LEMMA 2. *If $0 \neq \beta \in R$, and $|\beta\beta^\star| < 2p$, then $|\beta\beta^\star|$ is a square, or $|\beta\beta^\star| = p$.*

Proof. Let $\beta = c\alpha - d$, where $2c$, $2d$ and $c - d$ are integers. If one of the coefficients c and d is 0, then the other one is an integer, and we are done. We may assume that $\alpha \le |\beta| \le 1$ and $c > 0$. Then

$$|\beta^\star| = |c\frac{1}{\alpha} + d| = |c(\alpha + \frac{1}{\alpha}) - \beta| \ge c(\alpha + \frac{1}{\alpha}) - 1,$$

hence

$$2p > |\beta\beta^\star| \geq c - \alpha.$$

The right-hand side is greater than $2p-1$ for $2c \geq 4p-1$, so we have $1 \leq 2c \leq 4p-2$. Then $0 < c\alpha < 1/2$, hence $d = \pm 1/2$ or $d = 1$, because $|\beta| \leq 1$, and $d = 0$ is excluded already. We know that

$$8p > 4|\beta\beta^\star| = |(2d)^2 - (2c)^2 + 4p(2c)(2d)|,$$

If $d = \pm 1/2$, then this gives

$$8p > 4|\beta\beta^\star| = |1 + C(4p - C)|$$

with the odd integer $C = \pm 2c$. For $C = \pm 1, 4p \pm 1$ the right-hand side is $4p$, otherwise it is greater than $8p$. So we can assume $d = 1$, then c is an integer and

$$2p > |\beta\beta^\star| = |1 + c(4p - c)|,$$

which implies that the right-hand side is 1. The lemma is proved.

3. The principles of the computation

We will use the same three concrete characters χ_1, χ_2 and χ_3, as in [B], see Section 3 of that paper for their definitions. We also recall some notations and facts from there. The conductors of the characters are

$$q_1 = 175,\ q_2 = q_3 = 61,$$

respectively. Let

$$\psi_t = \sum_{a=1}^{q_t} a\chi_t(a),$$

then, if

$$\mathcal{M} = Q(i, \omega, \xi),\ \mathcal{L} = Q(i, \xi),$$

where ξ is a primitive fifth root of unity, i is the usual primitive fourth root of unity, and ω is a primitive third root of unity, we have $\psi_t \in \mathcal{M}$ for $t = 1, 2$, and $\psi_3 \in \mathcal{L}$. We write

$G_t = G_{\mathcal{M}}$ for $t = 1, 2$ and $G_3 = G_{\mathcal{L}}$, where $G_{\mathcal{M}}$ and $G_{\mathcal{L}}$ are the Galois group of $\mathcal{M}$ and $\mathcal{L}$ (over Q), respectively. We denote by $N(\psi_t)$ the norm:

$$N(\psi_t) = \prod_{g \in G_t} g(\psi_t).$$

Every algebraic integer $a \in \mathcal{M}$ can be uniquely written in the form

$$a = \sum_{0 \le I \le 1,\ 0 \le J \le 1,\ 0 \le K \le 3} \gamma_{I,J,K}(a) i^I \omega^J \xi^K$$

with integers $\gamma_{I,J,K}(a)$. For algebraic numbers a, b and $m \neq 0$ we write

$$a \equiv b \pmod{m},$$

if $(a - b)/m$ is an algebraic integer.

Up to this point, everything in this section was the same as in the corresponding section of [B], since we considered concrete fixed characers, algebraic numbers and cyclotomic fields, which are independent of our class number problem (they are parameters in the proof). We now start to use them in our proof, and there will be some changes with respect to the corresponding places of [B].

Let $p > 1861$, and assume that $h(4p^2 + 1) = 1$. Let

$$4p = P_t q_t + p_{0,t} \text{ with } 0 \le p_{0,t} < q_t$$

for $t = 1, 2, 3$. Observe that P_t and $p_{0,t}$ have the same parity. Then it is easy to see that for $(C, D) \in H(q_t)$ (see Fact A for this notation) we have

$$\lceil (4pC - D)/q_t \rceil = P_t C + f(p_{0,t}, C, D, q_t),$$

where

$$f(p_0, C, D, q) = \begin{cases} \lceil (p_0 C - D)/q \rceil \text{ if } 2Cp_0 \text{ is even} \\ -(1/2) + \lceil (1/2) + ((p_0 C - D)/q) \rceil \text{ if } 2Cp_0 \text{ is odd} \end{cases}.$$

On the other hand, let j_t be an integer such that

$$4j_t \equiv 1 \pmod{q_t}.$$

Then, if we write

$$Q_t(X,Y) = Y^2 - X^2 - 4j_t p_{0,t} XY,$$

we have

$$Q(C,D) \equiv Q_t(C,D) \pmod{q_t}$$

for every $(C,D) \in H(q_t)$.

In the same way as in [B], we can derive the following statement from Fact A. We multiply by 4 in the definition of $\gamma^{(1)}_{I,J,K}$ and $\gamma^{(2)}_{I,J,K}$, in order to have integers everywhere.

FACT C. *Let $1 \le t \le 3$ be fixed, assume that $r > 2$ is a prime satisfying*

$$r | N(\psi_t), \tag{15}$$

and let (I,J,K) be a fixed triple with

$$0 \le I \le 1,\ 0 \le J \le 1,\ 0 \le K \le 3.$$

Introduce the notations

$$\gamma^{(1)}_{I,J,K} = \gamma_{I,J,K} \left(\left(\prod_{1 \ne g \in G_t} g(\psi_t) \right) \left(4 \sum_{(C,D) \in H(q_t)} \chi_t(Q_t(C,D)) C (C - q_t) \right) \right)$$

and

$$\gamma^{(2)}_{I,J,K} = \gamma_{I,J,K} \left(\left(\prod_{1 \ne g \in G_t} g(\psi_t) \right) \left(4 \sum_{(C,D) \in H(q_t)} \chi_t(Q_t(C,D)) (C - q_t) f(p_{0,t}, C, D, q_t) \right) \right)$$

($\gamma^{(1)}_{I,J,K}$ and $\gamma^{(2)}_{I,J,K}$ also depend on t, but we do not denote it), and assume that

$$\gamma^{(1)}_{I,J,K} \not\equiv 0 \pmod{r}.$$

Then

$$4p \equiv -q_t \frac{\gamma^{(2)}_{I,J,K}}{\gamma^{(1)}_{I,J,K}} + p_{0,t} \pmod{r},$$

where dividing means multiplying by the multiplicative inverse modulo r.

This means that (under the above conditions) the residue of $4p$ modulo q_t, i.e. $p_{0,t}$, determines the residue of $4p$ modulo r. We observed in [B] that when we apply Fact C, a residue class $p_{0,t}$ and its negative, $q_t - p_{0.t}$, determine residue classes modulo r which are again negatives of each other, i.e. application of Fact C preserves multiplication by -1. This is also true here, and in order to show this fact it is enough to prove the lemma below, which corresponds to Lemma 3 (i) of [B]. To state and prove the analogue of Lemma 3 (ii) of [B] (which is a formal expression of the fact mentioned above that Fact C preserves multiplication by -1) is starightforward, so we omit it.

LEMMA 3. *Let n, p_0 and q be integers, assume that $0 < p_0 < q$,*

$$(n, q) = (p_0, q) = 1,$$

furthermore, assume that q is odd, and let j be an integer such that

$$4j \equiv 1 \pmod{q}.$$

Let

$$\Sigma_1 = \sum_{(C,D)\in H(q),\ D^2-C^2-4jp_0CD\equiv n \pmod{q}} (C-q)f(p_0, C, D, q),$$

and

$$\Sigma_2 = \sum_{(C,D^\star)\in H(q),\ (D^\star)^2-C^2-4j(q-p_0)CD^\star\equiv n \pmod{q}} (C-q)f(q-p_0, C, D^\star, q).$$

Then

$$\Sigma_1 + \Sigma_2 = \sum_{(C,D)\in H(q),\ D^2-C^2-4jp_0CD\equiv n \pmod{q}} C(C-q).$$

Proof. If we restrict the sums to the integer pairs in $H(q)$, the equality follows from Lemma 3 (i) of [B]. So it is enough to deal with the pairs where C is not an integer. For these pairs the proof is similar (and in fact simpler) to the proof in the integer case. The non-integer solutions (C, D) in Σ_1 are in a one-to-one correspondence with the non-integer solutions $(C, D^\star)$ in Σ_2, the correspondence is given by

$$D + D^\star = q.$$

By symmetry we can assume that p_0 is odd, $q - p_0$ is even, then

$$f(p_0, C, D, q)+f(q-p_0, C, D^\star, q) = -(1/2)+\lceil(1/2)+((p_0C-D)/q)\rceil+\lceil((q-p_0)C-D^\star)/q\rceil,$$

and the right hand side gives C, because

$$\left(\frac{1}{2}+\frac{p_0C-D}{q}\right)+\left(\frac{(q-p_0)C-D^\star}{q}\right)=C-\frac{1}{2},$$

which is an integer, but the two terms of this sum are not integers. The lemma is proved.

4. The computer program

We modify only slightly the program given in [B]. This slight modification is needed only because the sums in Fact C are also modified. We replace the part of the program in [B] between

REM WE COMPUTE THE SUMS (20) AND (21)

and the next REM. We write instead of that part (if $q_t = 175$, then we use $j_t = 44$, if $q_t = 61$, then $j_t = 46$):

```
REM WE COMPUTE THE SUMS (20) AND (21)
FOR c = 0 TO q − 1: FOR d = 0 TO q − 1
I = d ∗ d − c ∗ c − p(a) ∗ c ∗ d
g = 2: Z = 4 ∗ (q − c) ∗ INT((d − p(a) ∗ c) / q)
IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
g = 3: Z = 4 ∗ (c − q) ∗ c
IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
I = (d + 1 / 2) ∗ (d + 1 / 2) − (c + 1 / 2) ∗ (c + 1 / 2) − 44 ∗ p(a) ∗ (2 ∗ c + 1) ∗ (2 ∗
d + 1)
IF q = 175 THEN GOTO 55
I = (d + 1 / 2) ∗ (d + 1 / 2) − (c + 1 / 2) ∗ (c + 1 / 2) − 46 ∗ p(a) ∗ (2 ∗ c + 1) ∗ (2 ∗
d + 1)
55 g = 2: Z = 4 ∗ (q − (c + 1 / 2)) ∗ INT((d + 1 / 2 − p(a) ∗ (c + 1 / 2)) / q)
IF p(a) = 2 ∗ INT(p(a) / 2) THEN GOTO 56
Z = 4 ∗ (q − (c + 1 / 2)) ∗ (1 / 2 + INT((d + 1 / 2 − p(a) ∗ (c + 1 / 2)) / q − 1 / 2))
56 IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
g = 3: Z = 4 ∗ (c + 1 / 2 − q) ∗ (c + 1 / 2)
IF q = 175 THEN GOSUB 20
```

IF q = 61 THEN GOSUB 30
NEXT d: NEXT c

Then

REM ======= WE COMPUTE THE PRODUCT OF (19)
REM ======= WITH ψ_t, (20) AND (21)

follows, and everything else is unchanged.

The data files are also changed (except data0.txt), we now give them. In the first line we write the contents of data0.txt, the second line is data1.txt, the third line is data2.txt, while the fourth one is data3.txt:

175, 3, 8, 13, 17, 18, 22, 27, 32, 38, 43, 48, 52, 53, 57, 62, 67, 73, 78, 83, 87;

175, 3, 8, 22, 32, 38, 43, 52, 62, 67, 73, 78, 0, 0, 0, 0, 0, 0, 0, 0, 0;

61, 18, 24, 30, 59, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0;

61, 52, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.

5. The results

The computations are completely similar to the computations made in [B]. We use our program for the (r, t) pairs (as we saw in [B], (15) is true for all of them)

$$(61, 1),\ (1861, 1),\ (1861, 2),\ (41, 3).$$

Here we always consider the residue of $4p$. Fact C deals with $4p$, and Fact B can be also expressed as a statement about $4p$, because

$$\left(\frac{4p^2+1}{r}\right) = \left(\frac{(4p)^2+4}{r}\right).$$

So we have the same 20 possible values of $p_{0,1}$ (i.e. for the residue of $4p$ modulo 175), as in [B]. We write these values into the first column of Table 1. This table is completely similar

to the corresponding table of [B]. The fourth column gives $4p$ modulo 61, it is computed from the first three columns, using Fact C:

$$4p \equiv -175\frac{\gamma^{(2)}_{0,1,0}}{\gamma^{(1)}_{0,1,0}} + p_{0,1} \pmod{61}.$$

Here we have 11 values of $p_{0,1}$ where the fifth column of Table 1 is empty. We apply Fact C (and our program) with $t = 1$ and $r = 1861$ for these 11 values. The results are in Table 2, which is again similar to Table 2 of [B]; the fourth column is computed as in Table 1, but modulo 1861. Here we have five values where the fifth column is empty.

The remaining possibilities are in Table 3, where we mean that either the plus or the minus sign is valid inside a row, and one of the rows must be valid for $4p$.

For four remaining values modulo 61 we apply Fact C and the program with $t = 2$ and $r = 1861$. The result is Table 4. The fourth column is computed by

$$4p \equiv -61\frac{\gamma^{(2)}_{0,1,0}}{\gamma^{(1)}_{0,1,0}} + p_{0,2} \pmod{1861}.$$

Just as in [B], we see that in these cases the two ways of the determination of $4p$ modulo 1861 give in fact different values, hence a contradiction. So the only possible values for $4p$ modulo 61 are ± 52, i.e. for $p_{0,3}$ the only possibilities are 52 and $61 - 52 = 9$. For $p_{0,3}$= 52 we apply Fact C and the program with $t = 3$ and $r = 41$. We obtain

$$\gamma^{(2)}_{0,0,0} \equiv 0 \pmod{41} \text{ and } \gamma^{(1)}_{0,0,0} \equiv 30 \pmod{41}.$$

Hence Fact C gives

$$4p \equiv 52 \equiv 11 \pmod{41}.$$

By the principle that Fact C preserves multiplication by -1 (which was of course used above several times just as in [B]), we know that then $p_{0,3} = 9$ gives

$$4p \equiv -11 \pmod{41}.$$

In both cases, we have

$$(4p)^2 + 4 \equiv 125 \equiv 17^2 \pmod{41},$$

which is a contradiction by Fact B. The Theorem is proved.

TABLE 1.

Here $r = 61$, and the second and third columns are computed with $t = 1$:

$p_{0,1}$	$\gamma^{(2)}_{0,1,0} \bmod r$	$\gamma^{(1)}_{0,1,0} \bmod r$	$4p \bmod r$	$\sqrt{(4p)^2+4} \bmod r$
3	52	29	51	
8	0	8	8	
13	9	28	33	19
17	21	10	46	30
18	39	31	32	28
22	25	11	18	
27	40	38	29	28
32	36	31	59	
38	33	35	56	
43	6	37	41	
48	16	38	0	2
52	0	17	52	
53	14	29	19	11
57	39	37	44	7
62	26	28	52	
67	53	10	24	
73	23	17	30	
78	28	11	54	
83	28	8	50	8
87	47	35	35	3

TABLE 2.

Here $r = 1861$, and the second and third columns are computed with $t = 1$:

$p_{0,1}$	$\gamma^{(2)}_{0,1,0} \bmod r$	$\gamma^{(1)}_{0,1,0} \bmod r$	$4p \bmod r$	$\sqrt{(4p)^2+4} \bmod r$
3	984	956	913	867
8	0	521	8	505
22	1162	411	1189	
32	267	1165	1166	
38	423	719	388	914
43	704	386	852	751
52	0	1590	52	
62	1277	751	1110	62
67	649	1153	1313	
73	905	1590	1454	
78	1469	411	1635	837

TABLE 3.

$4p \bmod 175$	$4p \bmod 61$	$4p \bmod 1861$
± 22	± 18	± 1189
± 32	± 59	± 1166
± 52	± 52	± 52
± 67	± 24	± 1313
± 73	± 30	± 1454

TABLE 4.

Here $r = 1861$, and the second and third columns are computed with $t = 2$:

$p_{0,2}$	$\gamma^{(2)}_{0,1,0} \bmod r$	$\gamma^{(1)}_{0,1,0} \bmod r$	$4p \bmod r$
18	496	1690	282
24	427	1789	515
30	763	150	1742
59	1209	1209	1859

References

[B] A. Biró, *Yokoi's conjecture,* preprint, 2001, submitted to Acta Arithmetica

[C-F] S. Chowla and J. Friedlander, *Class numbers and quadratic residues,* Glasgow Math. J. 17 (1976), 47-52.

[L] H. Lu, *Gauss's conjectures on the quadratic fields (Chinese),* Shanghai Sci. Tech. Publ., Shanghai, 1994, pp. 379-390.