La relation $D < (N'')^5$ entraîne que deux D_i, au plus, sont supérieurs à N''. On a aussi $D_1 \leqslant D^{1/3}$, on applique le lemme 4 avec

$$M = D^{\varepsilon}(D_2 \ldots D_r)^{1+\varepsilon^9} \leqslant D^{\varepsilon}(D^{1/3}N')^{1+\varepsilon^9} \quad \text{et} \quad N = D_1^{1+\varepsilon^9} \leqslant D^{(1+\varepsilon^9)/3}$$

pour obtenir la relation (4). Il suffit de regrouper les relations (1), (3) et (4) et de remplacer par la valeur de D, pour obtenir le théorème.

Bibliographie

[1] J.-M. Deshouillers and H. Iwaniec, *Kloosterman sums and the Fourier coefficients of cusp forms*, Invent. Math. 70 (1982), p. 219–288.

[2] — — *On the Brun–Titchmarsh theorem on average*, Proc. János Bolyai Soc. Conf. (à paraître).

[3] E. Fouvry, *Repartition des suites dans les progressions arithmétiques*, Acta Arith. 41 (1982), p. 359–382.

[4] — *Autour du théorème de Bombieri–Vinogradov*, Acta Math. (à paraître).

[5] — *Répartition des suites dans les progressions arithmétiques*, Thèse de Doctorat d'état, Université de Bordeaux I, 1981.

[6] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London –New York 1974.

[7] D. R. Heath-Brown and H. Iwaniec, *On the difference between consecutive primes*, Inv. Math. 55 (1979), p. 44–69.

[8] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith. 37 (1980), p. 307–320.

[9] — *On the Brun–Titchmarsh theorem and related questions*, Proc. of the Queen's Number Theory Conference, 1979, p. 67–78.

[10] — *On the Brun–Titchmarsh theorem*, J. Math. Soc. Japan 34 (1982), p. 95–123.

U.E.R. DE MATHÉMATIQUES ET D'INFORMATIQUE
UNIVERSITÉ DE BORDEAUX I
351 cours de la Libération
33405 Talence Cedex, France

Reçu le 3.12.1982 (1331)

ACTA ARITHMETICA
XLIII (1984)

Reducibility of lacunary polynomials, V

by

A. Schinzel (Warszawa)

To Professor Paul Erdős on his 70-th birthday

The main subject of this paper are reciprocal factors of quadrinomials over $\boldsymbol{Q}$. For a quadrinomial

$$(1) \qquad q(x) = a_0 + \sum_{i=1}^{3} a_i x^{n_i}, \quad 0 < n_1 < n_2 < n_3, \; a_0a_1a_2a_3 \neq 0$$

with given coefficients a_i the question of non-reciprocal factors has been completely settled in [1] and the cyclotomic factors are easily determined by means of a theorem of Mann (cf. [5], Corollary 4). Some partial results about non-cyclotomic reciprocal factors have been obtained in [5]. In particular it has been proved there that if either $|a_0|+|a_3| \geqslant |a_1|+|a_2|$ or for some g, h: $0 \leqslant g, h \leqslant 3$

$$(2) \qquad a_g^2 \not\equiv a_h^2 \bmod \underset{0\leqslant j\leqslant 3}{\text{g.c.d.}}\, a_j \cdot \underset{j\neq g,h}{\text{g.c.d.}}\, a_j \quad \text{or} \quad |a_0| = |a_3|, \quad |a_1| = |a_2|$$

then either all reciprocal factors of $q(x)$ are cyclotomic or else there is a relation $\sum_{j=1}^{3} \gamma_j n_j = 0$ with γ_j integers satisfying

$$0 < \max_{1\leqslant j\leqslant 3} |\gamma_j| \leqslant \max_{0\leqslant j\leqslant 3} \frac{\log |a_j|^2}{\log 2}.$$

The condition (2) is fulfilled by about 82 % of all quadruples $\langle a_0, a_1, a_2, a_3\rangle$ with $|a_i| \leqslant a$ $(a \to \infty)$.

Now we shall show that for almost all quadruples $\langle a_0, a_1, a_2, a_3\rangle$ in the sense of density reciprocal factors do not exist. More exactly we shall prove

Theorem 1. *The number of integer quadruples* $\langle a_0, a_1, a_2, a_3\rangle$ *with* $0 < |a_i| \leqslant a$ $(0 \leqslant i \leqslant 3)$ *for which* $q(x) = a_0 + \sum_{i=1}^{3} a_i x^{n_i}$ *has a reciprocal factor at least one triple* $\langle n_1, n_2, n_3\rangle$ *is* $O\left(a^4/(\log a)^{3/4}\right)$.

The proof of Theorem 1 is based on several lemmata. The first of them is of independent interest, since it gives a necessary condition for a quadrinomial to have a reciprocal factor.

The estimate $O\big(a^4/(\log a)^{3/4}\big)$ can probably be replaced by $O(a^3)$. In order to justify this conjecture we shall show

THEOREM 2. *The number of integer triples* $\langle a_0, a_1, a_2\rangle$ *with* $0 < |a_i| \leqslant a$ $(0 \leqslant i \leqslant 2)$ *for which the trinomial* $a_0 + \sum_{i=1}^{3} a_i x^{n_i}$ *has a reciprocal factor for at least one pair* $\langle n_1, n_2\rangle$ *is* $O(a^2)$.

I thank Dr. J. Browkin and Dr. M. Ram Murty for their valuable suggestions used in the proof of Theorem 1.

DEFINITION 1. If $\{i, j, k\} = \{1, 2, 3\}$ let in the notation of Theorem 2 a_i^* be the greatest factor of a_i prime to $a_0a_ja_k$,

$$d_i = (n_j, n_k),$$
$$\Delta_i = a_0^4+a_j^4+a_k^4-2a_0^2a_j^2-2a_0^2a_k^2-2a_j^2a_k^2,$$
$$a_{ij} = \frac{-(a_0^2+a_j^2-a_k^2)+\sqrt{\Delta_i}}{2a_0a_j}.$$

LEMMA 1. *If* $q(x)$ *given by* (1) *has a reciprocal factor and* $\{i, j, k\} = \{1, 2, 3\}$ *then*

$$a_{ij}^{n_k/d_i}a_{ik}^{n_j/d_i}+a_{ij}^{-n_k/d_i}a_{ik}^{-n_j/d_i} \equiv 2 \bmod a_i^*. \tag{3}$$

(Note that the number on the left hand side is rational.)

Proof. Suppose that λ is a zero of the reciprocal factor in question. It follows that

$$q(\lambda) = q(\lambda^{-1}) = 0,$$

hence $(a_i^*, \lambda)|(a_i^*, a_0) = 1$ and $(a_i^*, \lambda^{-1})|(a_i^*, a_0) = 1$. From the above equations we get the congruences

$$-a_k\lambda^{n_k} \equiv a_j\lambda^{n_j}+a_0 \pmod{a_i^*},$$
$$-a_k\lambda^{-n_k} \equiv a_j\lambda^{-n_j}+a_0 \pmod{a_i^*},$$

which imply

$$a_0a_j\lambda^{2n_j}+(a_0^2+a_j^2-a_k^2)\lambda^{n_j}+a_0a_j \equiv 0 \bmod a_i^*,$$
$$a_0a_j(\lambda^{n_j}-a_{ij})(\lambda^{n_j}-a_{ij}^{-1}) \equiv 0 \bmod a_i^*$$

and by symmetry between j and k

$$a_0a_k(\lambda^{n_k}-a_{ik})(\lambda^{n_k}-a_{ik}^{-1}) \equiv 0 \bmod a_i^*.$$

Since $(a_0a_ja_k, a_i^*) = 1$ it follows that $a_i^*|(A^*B^*, C^*D^*)$, where A^*, B^*, C^*, D^* are numerators of the fractional ideals generated by

$$A = \lambda^{n_j}-a_{ij},\quad B = \lambda^{n_j}-a_{ij}^{-1},\quad C = \lambda^{n_k}-a_{ik},\quad D = \lambda^{n_k}-a_{ik}^{-1},$$

respectively. However

$$a_i\lambda^{n_i}+a_jA+a_kC = -\frac{\sqrt{\Delta_i}}{a_0} = a_j(B-A) = a_k(D-C),$$
$$a_i\lambda^{n_i}+a_jB+a_kD = \frac{\sqrt{\Delta_i}}{a_0} = a_j(A-B) = a_k(C-D).$$

Hence

$$(a_i^*, A^*, C^*)|(a_i^*, A^*, B^*, C^*, D^*),$$
$$(a_i^*, B^*, D^*)|(a_i^*, A^*, B^*, C^*, D^*)$$

and it follows that

$$a_i^*|(a_i^*, A^*B^*, C^*D^*)|(a_i^*, A^*, D^*)(a_i^*, B^*, C^*).$$

Now

$$\lambda^{n_jn_k/d_i} \equiv a_{ij}^{n_k/d_i} \bmod (a_i^*, A^*),$$
$$\lambda^{n_jn_k/d_i} \equiv a_{ik}^{-n_j/d_i} \bmod (a_i^*, D^*),$$

hence

$$a_{ij}^{n_k/d_i}-a_{ik}^{-n_j/d_i} \equiv 0 \bmod (a_i^*, A^*, D^*).$$

Similarly

$$a_{ij}^{-n_k/d_i}-a_{ik}^{n_j/d_i} \equiv 0 \bmod (a_i^*, B^*, C^*)$$

and it follows that

$$(a_{ij}^{n_k/d_i}-a_{ik}^{-n_j/d_i})(a_{ij}^{-n_k/d_i}-a_{ik}^{n_j/d_i}) \equiv 2-a_{ij}^{n_k/d_i}a_{ik}^{n_j/d_i}-a_{ij}^{-n_k/d_i}a_{ik}^{-n_j/d_i} \equiv 0 \bmod a_i^*.$$

Remark 1. Applying Lemma 1 to the quadrinomial $x^{n_3}q(x^{-1})$ one obtains under the same assumption the congruence

$$a_{01}^{(n_3-n_2)/d_0}a_{02}^{(n_3-n_1)/d_0}+a_{01}^{(n_2-n_3)/d_0}a_{02}^{(n_1-n_3)/d_0} \equiv 2 \bmod a_0^*,$$

where $d_0 = (n_3-n_1, n_3-n_2)$, a_0^* is the greatest factor of a_0 prime to $a_1a_2a_3$ and

$$a_{0j} = \frac{-(a_3^2+a_j^2-a_{3-j}^2)+\sqrt{a_0^4+a_1^4+a_2^4-2a_0^2a_1^2-2a_0^2a_2^2-2a_1^2a_2^2}}{2a_3a_j}.$$

I was unable to use this congruence to improve Theorem 2, but it may be useful in dealing with specific quadrinomials.

DEFINITION 2. Let for a prime $p|a_i^*$, $j\neq i$ $(1\leqslant i,j\leqslant 3)$

$$\varepsilon_{ij}(p)=\begin{cases}\left(a_{ij}-\dfrac{\sqrt{\Delta_i}-\delta_i}{2a_0a_j}\Big|p\right) & \text{if}\quad \left(\dfrac{\Delta_i}{p}\right)=0 \text{ or } 1,\quad \Delta_i\equiv\delta_i^2 \bmod p,\\[2ex] (a_{ij}+a_{ij}^{-1}+2|p) & \text{if}\quad \left(\dfrac{\Delta_i}{p}\right)=-1\end{cases}$$

and let for $\varepsilon=\pm1$

$$\mathscr{S}_{ij}^{\varepsilon}(p)=\{\langle a_0,a_1,a_2,a_3\rangle\colon p|a_i^*,\ \varepsilon_{ij}(p)=\varepsilon\}.$$

Remark 2. The definition of $\varepsilon_{ij}(p)$ is correct in spite of the ambiguity in the choice of δ_i. Indeed

$$\left(a_{ij}-\frac{\sqrt{\Delta_i}-\delta_i}{2a_0a_j}\right)\left(a_{ij}-\frac{\sqrt{\Delta_i}+\delta_i}{2a_0a_j}\right)=\left(a_{ij}-\frac{\sqrt{\Delta_i}}{2a_0a_j}\right)^2-\left(\frac{\delta_i}{2a_0a_j}\right)^2\equiv 1 \bmod p.$$

LEMMA 2. *If $\{i,j,k\}=\{1,2,3\}$, p is an odd prime and*[1]

$$\langle a_0,a_1,a_2,a_3\rangle\in\mathscr{S}_{ij}^{-}(p) \tag{4}$$

or

$$\langle a_0,a_1,a_2,a_3\rangle\in\mathscr{S}_{ij}^{-}(p)\cap\mathscr{S}_{ik}^{+}(p) \tag{5}$$

the condition (3) *implies*

$$\operatorname{ord}_2 n_k\geqslant\operatorname{ord}_2 n_j \tag{6}$$

or

$$\operatorname{ord}_2 n_k>\operatorname{ord}_2 n_j, \tag{7}$$

respectively.

Proof. Take a prime ideal factor $\mathfrak{p}$ of p in $Q(\sqrt{\Delta_i})$ and let γ be a primitive root mod $\mathfrak{p}$. The congruence (3) implies

$$\frac{(a_{ij}^{n_k/d_i}a_{ik}^{n_j/d_i}-1)^2}{a_{ij}^{n_k/d_i}a_{ik}^{n_j/d_i}}\equiv 0 \bmod \mathfrak{p}$$

and since a_{ij}, a_{ik} are $\mathfrak{p}$-adic units

$$a_{ij}^{n_k/d_i}a_{ik}^{n_j/d_i}\equiv 1 \bmod \mathfrak{p}.$$

Hence

$$\frac{n_k}{d_i}\operatorname{ind}_\gamma a_{ij}+\frac{n_j}{d_i}\operatorname{ind}_\gamma a_{ik}\equiv 0 \bmod N\mathfrak{p}-1. \tag{8}$$

Now we distinguish two cases

$$\left(\frac{\Delta_i}{p}\right)=0 \text{ or } 1 \tag{9}$$

and

$$\left(\frac{\Delta_i}{p}\right)=-1. \tag{10}$$

In the case (9) the conditions (4) and (5) take the form

$$\left(\frac{a_{ij}}{\mathfrak{p}}\right)=-1 \tag{11}$$

and

$$\left(\frac{a_{ij}}{\mathfrak{p}}\right)=-1,\quad \left(\frac{a_{ik}}{\mathfrak{p}}\right)=1 \tag{12}$$

respectively.

Now (11) implies $\operatorname{ind}a_{ij}\equiv 1 \bmod 2$ and since $N\mathfrak{p}-1$ is even we infer from (8) that

$$\text{either}\quad n_k/d_i\equiv n_j/d_i\equiv 1 \bmod 2\quad\text{or}\quad n_k/d_i\equiv 0 \bmod 2.$$

Since $(n_j/d_i, n_k/d_i)=1$, (6) follows.

Similarly (12) implies $\operatorname{ind}_\gamma a_{ij}\equiv 1 \bmod 2$, $\operatorname{ind}_\gamma a_{ik}\equiv 0 \bmod 2$, we infer from (8) that $n_k/d_i\equiv 0 \bmod 2$ and (7) follows. In the case (10) we have $N\mathfrak{p}=p^2$,

$$a_{ij}^{-1}+1\equiv(a_{ij}+1)^p \bmod \mathfrak{p} \tag{13}$$

and since

$$a_{ij}=(a_{ij}+1)/(a_{ij}^{-1}+1)$$

we get

$$\operatorname{ind}_\gamma a_{ij}\equiv(1-p)\operatorname{ind}_\gamma(a_{ij}+1) \bmod p^2-1.$$

Similarly

$$\operatorname{ind}_\gamma a_{ik}\equiv(1-p)\operatorname{ind}_\gamma(a_{ik}+1) \bmod p^2-1$$

and the congruence (8) takes the form

$$\frac{n_k}{d_i}\operatorname{ind}_\gamma(a_{ij}+1)+\frac{n_j}{d_i}\operatorname{ind}_\gamma(a_{ik}+1)\equiv 0 \bmod p+1. \tag{14}$$

On the other hand,

$$\varepsilon_{ij}(p)=\left(\frac{(a_{ij}+1)(a_{ij}^{-1}+1)}{p}\right)$$

and in view of (13) the conditions (4) and (5) imply

$$(p+1)\operatorname{ind}_\gamma(a_{ij}+1)\not\equiv 0 \bmod 2(p+1),\quad\text{i.e.}\quad \operatorname{ind}_\gamma(a_{ij}+1)\equiv 1 \bmod 2$$

[1] $\mathscr{S}_{ij}^{\pm}(p)$ stands for $\mathscr{S}_{ij}^{\pm1}(p)$.

and

$$\operatorname{ind}_\gamma(a_{ij}+1) \equiv 1 \bmod 2, \qquad \operatorname{ind}_\gamma(a_{ik}+1) \equiv 0 \bmod 2,$$

respectively. Now (6) and (7) follow from (14) in the same way as they followed from (8) in the case (9).

DEFINITION 3. Let for $i > 0$, $j > 0$, $i \not\equiv j \bmod 3$, $\varepsilon = \pm 1$,

$$n_i = n_{i'}, \qquad \mathscr{S}^{\varepsilon}_{ij}(p) = \mathscr{S}^{\varepsilon}_{i'j'}(p),$$

where i', j' are the least positive residues mod 3 of i, j respectively.

LEMMA 3. *If*

$$\langle a_0, a_1, a_2, a_3\rangle \in \bigcup_{\substack{p_0,p_1,p_2,p_3\\ \text{odd primes}}} \Big(\Big(\bigcup_{i=1}^{3} \mathscr{S}^{+}_{i,i+1}(p_0) \cap \mathscr{S}^{-}_{i,i+2}(p_0)\Big) \cap$$
$$\cap \bigcap_{j=1}^{3} \big(\mathscr{S}^{+}_{j,j+1}(p_j) \cap \mathscr{S}^{-}_{j,j+2}(p_j) \cup \mathscr{S}^{-}_{j+1,j+2}(p_j)\big)\Big)$$

then $q(x)$ given by (1) *has no reciprocal factor for any choice of n_1, n_2, n_3.*

Proof. If for an odd prime p_0

$$\langle a_0, a_1, a_2, a_3\rangle \in \bigcup_{i=1}^{3} \big(\mathscr{S}^{+}_{i,i+1}(p_0) \cap \mathscr{S}^{-}_{i,i+2}(p_0)\big)$$

we have by Lemma 2 and Definition 3 for a suitable $i \leqslant 3$

$$\operatorname{ord}_2 n_{i+2} < \operatorname{ord}_2 n_{i+1}. \tag{15}$$

On the other hand from

$$\langle a_0, a_1, a_2, a_3\rangle \in \bigcap_{j=1}^{3} \big(\mathscr{S}^{+}_{j,j+1}(p_j) \cap \mathscr{S}^{-}_{j,j+2}(p_j) \cup \mathscr{S}^{-}_{j+1,j+2}(p_j)\big)$$

we infer by Lemma 2 and Definition 3 that for every positive j

$$\operatorname{ord}_2 n_{j+2} < \operatorname{ord}_2 n_{j+1} \quad \text{or} \quad \operatorname{ord}_2 n_{j+2} \leqslant \operatorname{ord}_2 n_j. \tag{16}$$

Substituting in (16) $j = i+2$ we get

$$\operatorname{ord}_2 n_{i+1} < \operatorname{ord}_2 n_i \quad \text{or} \quad \operatorname{ord}_2 n_{i+1} \leqslant \operatorname{ord}_2 n_{i+2},$$

which together with (15) gives

$$\operatorname{ord}_2 n_{i+2} < \operatorname{ord}_2 n_{i+1} < \operatorname{ord}_2 n_i. \tag{17}$$

Substituting in (16) $j = i+1$ we get

$$\operatorname{ord}_2 n_i < \operatorname{ord}_2 n_{i+2} \quad \text{or} \quad \operatorname{ord}_2 n_i \leqslant \operatorname{ord}_2 n_{i+1}$$

which contradicts (17).

LEMMA 4. *For an odd prime p and $a, b \in \boldsymbol{F}_p^*$ let*

$$\Delta(c) = a^4+b^4+c^4-2a^2b^2-2a^2c^2-2b^2c^2$$

and let $\mathscr{Q}(p, a, b)$ be the set of all $c \in \boldsymbol{F}_p^*$ such that

$$\text{either } \sqrt{\Delta(c)} \in \boldsymbol{F}_p \text{ and } \sqrt{\frac{-(c^2+b^2-a^2)+\sqrt{\Delta(c)}}{2bc}} \notin \boldsymbol{F}_p$$

$$\text{or } \sqrt{\Delta(c)} \notin \boldsymbol{F}_p \text{ and } \sqrt{\frac{-(c^2+b^2-a^2)}{bc}+2} \notin \boldsymbol{F}_p.$$

Then

$$|\mathscr{Q}(p, a, b)| = p/2 + O(\sqrt{p})$$

where the constant in the O-symbol is absolute.

Remark 3. $\mathscr{Q}(p, a, b)$ is independent of the choice of $\sqrt{\Delta(c)}$ since

$$\frac{-(c^2+b^2-a^2)+\sqrt{\Delta(c)}}{2bc} \cdot \frac{-(c^2+b^2-a^2)-\sqrt{\Delta(c)}}{2bc} = 1.$$

Proof. We choose an element $e \in \boldsymbol{F}_p$ such that $\sqrt{e} \notin \boldsymbol{F}_p$ and consider two function fields

$$\boldsymbol{K}_1 = \boldsymbol{F}_p\left(t, \sqrt{e\,\frac{-(t^2+b^2-a^2)+\sqrt{\Delta(t)}}{2bt}}\right),$$

$$\boldsymbol{K}_2 = \boldsymbol{F}_p\left(t, \sqrt{e\Delta(t)}, \sqrt{e\,\frac{a^2-(t-b)^2}{bt}}\right).$$

Note that

$$\frac{a^2-(t-b)^2}{bt} = \frac{-(t^2+b^2-a^2)}{bt}+2.$$

For every finite extension $\boldsymbol{F}_q$ of $\boldsymbol{F}_p$ the composite fields $\boldsymbol{K}_1\boldsymbol{F}_q$ and $\boldsymbol{K}_2\boldsymbol{F}_q$ are each of degree 4 over $\boldsymbol{F}_q(t)$. To prove this it is enough to show that

$$\Delta(t),\ e\Delta(t),\ e\,\frac{a^2-(t-b)^2}{bt},\ \Delta(t)\,\frac{a^2-(t-b)^2}{bt} \tag{18}$$

are not squares in $\boldsymbol{F}_q(t)$

and that

$$e\,\frac{-(t^2+b^2-a^2)+\sqrt{\Delta(t)}}{2bt} \text{ is not a square in } \boldsymbol{F}_q(t, \sqrt{\Delta(t)}). \tag{19}$$

Now

$$\varDelta(t) = \big(a^2-(t-b)^2\big)\big(a^2-(t+b)^2\big) = (a-t+b)(a+t-b)(a-t-b)(a+t+b)$$

and (18) follows by considering the factorization of all four functions in question into factors linear with respect to t.

If $a \neq \pm b$ $\varDelta(t)$ is squarefree in $\boldsymbol{F}_q[t]$ hence $1, \sqrt{\varDelta(t)}$ forms a basis of the ring $\boldsymbol{F}_q[t, \sqrt{\varDelta(t)}]$ over $\boldsymbol{F}_q[t]$ and the ring itself is integrally closed. Hence in order to prove (19) it is enough to show that

$$2ebt\big(-(t^2+b^2-a^2)+\sqrt{\varDelta(t)}\big) \neq \big(\alpha+\beta\sqrt{\varDelta(t)}\big)^2, \quad \alpha, \beta \in \boldsymbol{F}_q[t].$$

Assuming the contrary we get

$$-2ebt(t^2+b^2-a^2) = \alpha^2+\beta^2\varDelta(t), \quad 2ebt = 2\alpha\beta,$$

$\deg\alpha \leqslant 1$, $\deg\beta^2\varDelta \geqslant 4$, hence

$$\deg(\alpha^2+\beta^2\varDelta) \geqslant 4 > \deg t(t^2+b^2-a^2),$$

a contradiction.

If $a = \pm b$ then $\sqrt{\varDelta(t)} = t\sqrt{t^2-4a^2}$ and (19) can be proved by an argument similar to the above but with $\sqrt{\varDelta(t)}$ replaced by $\sqrt{t^2-4a^2}$. Hence $\boldsymbol{F}_p$ is the exact constant field of $\boldsymbol{K}_i$ $(i = 1, 2)$.

By Weil's theorem the number of divisors of degree one over $\boldsymbol{F}_p(t)$ of the field $\boldsymbol{K}_i$ is $p+1+2g_i\theta_{ip}\sqrt{p}$, where $|\theta_{ip}| \leqslant 1$ and g_i is the genus of $\bar{\boldsymbol{K}}_i$. Over each $c \in \boldsymbol{F}_p \cup \{\infty\}$ which is not ramified lie 0 or 4 such divisors and since c corresponding to 4 divisors in $\boldsymbol{K}_1$ (resp. $\boldsymbol{K}_2$) gives raise to 0 divisors of degree one in $\boldsymbol{K}_2$ (resp. $\boldsymbol{K}_1$) we get

$$|\mathscr{Q}(p, a, b)| = \sum_{i=1}^{2} \frac{p+1+2g_i\theta_{ip}\sqrt{p}}{4} + O(1) = \frac{p}{2} + O(\sqrt{p}).$$

The constant in the O-symbol is absolute since the number of ramification points of $\boldsymbol{K}_1, \boldsymbol{K}_2$ is bounded by a number independent of a, b. Indeed, if $a \neq \pm b$ there are 6 ramification points $(\pm a, \pm b, 0, \infty)$ and if $a = \pm b$ there are 3 $(\pm 2a, \infty)$. Incidentally $g_1 = g_2 = 3$ in the former case and $g_1 = g_2 = 0$ in the latter. This proves the lemma.

LEMMA 5. *In the notation of Lemma 4 let $\mathscr{R}(p, a, b)$ be the set of $c \in \boldsymbol{F}_p^*$ such that*

$$\textit{either } \sqrt{\varDelta(c)} \in \boldsymbol{F}_p \textit{ and } \sqrt{\frac{-(c^2+b^2-a^2)+\sqrt{\varDelta(c)}}{2bc}} \notin \boldsymbol{F}_p \textit{ and } \sqrt{\frac{-(c^2+a^2-b^2)+\sqrt{\varDelta(c)}}{2ac}} \in \boldsymbol{F}_p$$

$$\textit{or } \sqrt{\varDelta(c)} \notin \boldsymbol{F}_p \textit{ and } \sqrt{\frac{-(c^2+b^2-a^2)}{bc}+2} \notin \boldsymbol{F}_p \textit{ and } \sqrt{\frac{-(c^2+a^2-b^2)}{ac}+2} \in \boldsymbol{F}_p.$$

If $a \neq \pm b$ then

$$|\mathscr{R}(p, a, b)| = p/4+O(\sqrt{p}),$$

where the constant in the O-symbol is absolute.

Proof. Using the notation introduced in the proof of Lemma 4 we consider the function fields

$$\boldsymbol{K}_3 = \boldsymbol{K}_1\left(\sqrt{\frac{-(t^2+a^2-b^2)+\sqrt{\varDelta(t)}}{2at}}\right), \quad \boldsymbol{K}_4 = \boldsymbol{K}_2\left(\sqrt{\frac{b^2-(t-a)^2}{at}}\right).$$

For every finite extension $\boldsymbol{F}_q$ of $\boldsymbol{F}_p$ the composite fields $\boldsymbol{K}_3\boldsymbol{F}_q$ and $\boldsymbol{K}_4\boldsymbol{F}_q$ are each of degree 8 over $\boldsymbol{F}_q(t)$. Indeed, since for $i = 1, 2$, $[\boldsymbol{K}_i\boldsymbol{F}_q : \boldsymbol{F}_q(t)] = 4$ it is enough to show that

$$(20) \qquad \frac{b^2-(t-a)^2}{at}, \quad e\varDelta(t)\frac{b^2-(t-a)^2}{at}, \quad e\,\frac{a^2-(t-b)^2}{bt}\cdot\frac{b^2-(t-a)^2}{at},$$
$$\varDelta(t)\frac{a^2-(t-b)^2}{bt}\cdot\frac{b^2-(t-a)^2}{at} \text{ are not squares in } \boldsymbol{F}_q(t)$$

and

$$(21) \qquad \frac{-(t^2+a^2-b^2)+\sqrt{\varDelta(t)}}{2at}, \quad \frac{-(t^2+b^2-a^2)+\sqrt{\varDelta(t)}}{2bt}\times$$
$$\times\frac{-(t^2+a^2-b^2)+\sqrt{\varDelta(t)}}{2at} \text{ are not squares in } \boldsymbol{F}_q\big(t, \sqrt{\varDelta(t)}\big).$$

The assertion (20) is easily verified by factorization of the four elements in question into linear factors. The first part of the (21) is proved similarly to (19). To prove the second part of (21) we notice that

$$\frac{-(t^2+b^2-a^2)+\sqrt{\varDelta(t)}}{2bt}\cdot\frac{-(t^2+a^2-b^2)+\sqrt{\varDelta(t)}}{2at} = \frac{t^2-a^2-b^2-\sqrt{\varDelta(t)}}{2ab}.$$

Since $1, \sqrt{\varDelta}$ is a basis of the ring $\boldsymbol{F}_q[t, \sqrt{\varDelta(t)}]$ over $\boldsymbol{F}_q[t]$ and the ring itself is integrally closed it is enough to show that

$$\frac{t^2-a^2-b^2-\sqrt{\varDelta(t)}}{2ab} \neq \big(\alpha+\beta\sqrt{\varDelta(t)}\big)^2, \quad \alpha, \beta \in \boldsymbol{F}_q[t].$$

Assuming the contrary we get $2\alpha\beta \in \boldsymbol{F}_q^*$ hence $\alpha, \beta \in \boldsymbol{F}_q^*$ and

$$\deg(\alpha^2+\beta^2\Delta) = 4 > \deg(t^2-a^2-b^2),$$

a contradiction. Hence $\boldsymbol{F}_p$ is the exact constant field of $\boldsymbol{K}_i$ $(i = 3, 4)$.

By Weil's theorem the number of divisors of degree one over $\boldsymbol{F}_p(t)$ of the field $\boldsymbol{K}_i$ $(i = 3, 4)$ is $p+1+2g_i\theta_{ip}\sqrt{p}$, where $|\theta_{ip}| \leqslant 1$ and g_i is the genus of $\boldsymbol{K}_i$. Over each $c \in \boldsymbol{F}_p \cup \{\infty\}$ which is not ramified lie 0 or 8 such divisors and since c corresponding to 8 divisors in $\boldsymbol{K}_3$ (resp. $\boldsymbol{K}_4$) gives raise to 0 divisors of degree one in $\boldsymbol{K}_4$ (resp. $\boldsymbol{K}_3$) we get

$$|\mathscr{R}(p, a, b)| = \sum_{i=3}^{4} \frac{p+1+2g_i\theta_{ip}\sqrt{p}}{8} + O(1) = \frac{p}{4} + O(\sqrt{p}).$$

The constant in the O-symbol is absolute since the number of ramification points of $\boldsymbol{K}_3$, $\boldsymbol{K}_4$ is always six. Indeed $\boldsymbol{K}_3$, $\boldsymbol{K}_4$ have the same ramification points as $\boldsymbol{K}_1$, $\boldsymbol{K}_2$ and $g_3 = g_4 = 5$.

Lemma 6. *For each $i > 0$ and for every odd prime p we have*

$$(p-1)^3 \geqslant |\mathscr{S}_{i+1,i+2}^{-}(p) \cap [1, p]^4| = p^3/2+O(p^{5/2}),$$

$$(p-1)^3 \geqslant |\mathscr{S}_{i,i+1}^{+}(p) \cap \mathscr{S}_{i,i+2}^{-}(p) \cap [1, p]^4| = p^3/4+O(p^{5/2}).$$

Proof. Denoting the residue mod p by a bar we have

$$\mathscr{S}_{i+1,i+2}^{-}(p) = \{\langle a_0, a_1, a_2, a_3\rangle \in \boldsymbol{Z}^4\colon\ p|a_{i+1},\ p\nmid a_i a_{i+2},$$
$$\bar{a}_0 \in \mathscr{Q}(p, \bar{a}_i, \bar{a}_{i+2})\},$$

$$\mathscr{S}_{i,i+1}^{+}(p) \cap \mathscr{S}_{i,i+2}^{-}(p) = \{\langle a_0, a_1, a_2, a_3\rangle \in \boldsymbol{Z}^4\colon\ p|a_i,\ p\nmid a_{i+1}a_{i+2},$$
$$\bar{a}_0 \in \mathscr{R}(p, \bar{a}_{i+1}, \bar{a}_{i+2})\}.$$

In virtue of Lemmata 4 and 5 it follows that

$$|\mathscr{S}_{i+1,i+2}^{-}(p) \cap [1, p]^4| = \sum_{a=1}^{p-1}\sum_{b=1}^{p-1} |\mathscr{Q}(p, a, b)| = (p-1)^2\frac{p}{2} + O\big((p-1)^2\sqrt{p}\big)$$
$$= p^3/2+O(p^{5/2})$$

and since $\mathscr{R}(p, a, b) \neq \emptyset$

$$|\mathscr{S}_{i,i+1}^{+}(p) \cap \mathscr{S}_{i,i+2}^{-}(p) \cap [1, p]^4| = \sum_{\substack{a=1\\ a\neq b}}^{p-1}\sum_{b=1}^{p-1} |\mathscr{R}(p, a, b)|$$
$$= \sum_{a=1}^{p-1} |\mathscr{R}(p, a, p-a)| + \sum_{\substack{a=1\\ a\neq b,\, p-b}}^{p-1}\sum_{b=1}^{p-1} |\mathscr{R}(p, a, b)|$$
$$= (p-1)(p-3)\frac{p}{4} + O\big((p-1)(p-3)\sqrt{p}\big) = \frac{p^3}{4} + O(p^{5/2}).$$

Since

$$|\mathscr{Q}(p, a, b)| \leqslant |\boldsymbol{F}_p^*| = p-1, \qquad |\mathscr{R}(p, a, b)| \leqslant |\boldsymbol{F}_p^*| = p-1$$

we get similarly the desired estimates from above.

Remark 4. In the above proof Lemmata 4 and 5 could be replaced by the theorem of Lang and Weil [4] applied to suitable varieties. This would result in a slight shortening of the proof at the cost of conceptual complication.

Lemma 7 (Gallagher). *For each prime p let $\Omega(p)$ be a subset of the group $\boldsymbol{Z}^n/p\boldsymbol{Z}^n$ of cardinality $\omega(p)p^{n-1}$. If $E(N)$ is the number of integral vectors $[a_0, \ldots, a_{n-1}]$ with $\max\limits_{0\leqslant i<n} |a_i| \leqslant N$ then for every real $x > 0$ and $N \geqslant x^2$ we have*

$$E(N) \ll N^n/S(\omega; x),$$

where

$$S(\omega; x) = \sum_{q\leqslant x} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p-\omega(p)}$$

and the constant in the Vinogradov symbol depends at most on n.

Proof, see [2], p. 92 with a slightly different notation.

Lemma 8 (Halberstam–Richert). *If for some real numbers $\varkappa$, $A_1 > 1$, $A_2 > 1$ a function $\omega(p)$ defined on primes satisfies the conditions*

$$0 \leqslant \frac{\omega(p)}{p} < 1 - \frac{1}{A_1}, \qquad 0 \leqslant \sum_{w<p\leqslant z} \frac{\omega(p)\log p}{p} \leqslant \varkappa \log\frac{z}{w} + A_2$$

then for a certain $B = B(A_2, \varkappa)$

$$S(\omega; x)^{-1} \leqslant B \prod_{p\leqslant x}\left(1 - \frac{\omega(p)}{p}\right).$$

Proof. Put $x = z$, $\lambda = 1$ in Lemma 4.1 of [3].

Proof of Theorem 1. Let us take in Lemma 7 $n = 4$, $\Omega(2) = \emptyset$ and $\Omega(p) = \Omega_j(p)$ $(j = 0, 1, 2, 3)$ the set of residue classes mod p represented in

$$\mathscr{T}_p^j = \begin{cases} \bigcup\limits_{i=1}^{3} \mathscr{S}_{i,i+1}^{+}(p) \cap \mathscr{S}_{i,i+2}^{-}(p) & \text{for} \quad j = 0, \\ \mathscr{S}_{j,j+1}^{+}(p) \cap \mathscr{S}_{j,j+2}^{-}(p) \cup \mathscr{S}_{j+1,j+2}^{-}(p) & \text{for} \quad j = 1, 2, 3. \end{cases}$$

The sets $\mathscr{T}_p^j$ are unions of cosets mod p thus we have

$$\omega(p) = \omega_j(p) = \begin{cases} 0 & \text{if} \quad p = 2, \\ p^{-3}|\mathscr{T}_p^j \cap [1, p]^4| & \text{if} \quad p > 2. \end{cases}$$

In virtue of Lemma 6 we have

$$|\mathscr{T}_p^j \cap [1, p]^4| \leqslant \begin{cases} 3(p-1)^3 & \text{if} \quad j = 0, \\ 2(p-1)^3 & \text{if} \quad j > 0 \end{cases}$$

and since the sets $\bigcup\limits_{\varepsilon=\pm 1} \mathscr{S}^{\varepsilon}_{j,j+1}$ $(j = 1, 2, 3)$ are disjoint

$$|\mathscr{T}_p^j \cap [1, p]^4| = \tfrac{3}{4}p^3 + O(p^{5/2}) \qquad (0 \leqslant j \leqslant 3).$$

It follows that for $j = 0, 1, 2, 3$

$$\omega_j(p) < 3,$$

$$\frac{1}{2} > \frac{\omega_j(p)}{4p} + O\left(\frac{1}{p^{3/2}}\right) \tag{22}$$

hence (see [3], Chapter 2, formula (3.2))

$$\sum_{w \leqslant p \leqslant z} \frac{\omega_j(p) \log p}{p} < 3 \sum_{w \leqslant p \leqslant z} \frac{\log p}{p} \leqslant 3 \log \frac{z}{w} + 3.$$

Thus the conditions of Lemma 8 are fulfilled with $A_1 = 2$, $A_2 = 3$, $\varkappa = 3$. In virtue of that lemma

$$S_j(\omega; \sqrt{a})^{-1} \ll \prod_{p < \sqrt{a}} \left(1 - \frac{\omega_j(p)}{p}\right),$$

hence by Lemma 7 with $N = a$, $x = \sqrt{a}$

$$E_j(a) = |[-a, a]^4 \setminus \bigcup_p \mathscr{T}_p^j| \ll a^4 \prod_{p < \sqrt{a}} \left(1 - \frac{\omega_j(p)}{p}\right).$$

By (22)

$$\log \prod_{p < \sqrt{a}} \left(1 - \frac{\omega_j(p)}{p}\right) \leqslant -\sum_{p < \sqrt{a}} \frac{\omega_j(p)}{p} = -\frac{3}{4} \sum_{p < \sqrt{a}} \frac{1}{p} + O\Big(\sum_{p < \sqrt{a}} \frac{1}{p^{1/3}}\Big)$$
$$= -\tfrac{3}{4} \log\log a + O(1)$$

and it follows that

$$E_j(a) = O\left(\frac{a^4}{(\log a)^{3/4}}\right).$$

Hence

$$|[-a, a]^4 \setminus \bigcap_{j=0}^{3} \bigcup_p \mathscr{T}_p^j| = |\bigcup_{j=0}^{3} ([-a, a]^4 \setminus \bigcup_p \mathscr{T}_p^j)| \leqslant \sum_{j=0}^{3} E_j(a)$$
$$= O\left(\frac{a^4}{(\log a)^{3/4}}\right).$$

However

$$\bigcap_{j=0}^{3} \bigcup_p \mathscr{T}_p^j = \bigcup_{p_0, p_1, p_2, p_3} \bigcap_{j=0}^{3} \mathscr{T}_{p_j}^j$$

and by the definition of $\mathscr{T}_p^j$ and Lemma 3 if

$$\langle a_0, a_1, a_2, a_3 \rangle \in \bigcup_{p_0, p_1, p_2, p_3 \in \mathscr{P}} \bigcap_{j=0}^{3} \mathscr{T}_{p_j}^j$$

then $q(x)$ given by (1) has no reciprocal factor. The proof is complete.

Lemma 9. *If a trinomial*

$$a_0 + a_1 x^{n_1} + a_2 x^{n_2}, \qquad a_0 a_1 a_2 \neq 0, \qquad 0 < n_1 < n_2$$

has a reciprocal factor then either for suitable $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$

$$a_0 + a_1 \varepsilon_1 + a_2 \varepsilon_2 = 0 \tag{23}$$

or for suitable integers k, m, n, p, q

(24)

$$a_0 = k \frac{\alpha^{n-m} - \beta^{n-m}}{\alpha - \beta} q^m, \qquad a_1 = -k \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad a_2 = k \frac{\alpha^m - \beta^m}{\alpha - \beta} q^{n-m},$$

where $n > m > 0$, $p \neq 0$, $q > 0$, $(n, m) = (p, q) = 1$ *and* α, β *are zeros of the trinomial* $z^2 - pz + q^2$.

Proof. It follows from the equations

$$a_0 + a_2 \xi^{n_1} + a_2 \xi^{n_2} = 0 = a_0 + a_1 \xi^{-n_1} + a_2 \xi^{-n_2}$$

that

$$\xi^{n_1}, \xi^{n_2} \in Q(\sqrt{\Delta}), \qquad \Delta = \sum_{i=0}^{2} a_i^4 - 2 \sum_{\substack{i,j=0 \\ j > i}}^{2} a_i^2 a_j^2.$$

Hence

$$\theta = \xi^{(n_1, n_2)} \in Q(\sqrt{\Delta})$$

and putting

$$m = \frac{n_1}{(n_1, n_2)}, \qquad n = \frac{n_2}{(n_1, n_2)}$$

we get

$$a_0 + a_1 \theta^m + a_2 \theta^n = 0 = a_0 + a_1 \theta^{-m} + a_2 \theta^{-n}.$$

It follows that

$$a_1(\theta^m - \theta^{-m}) + a_2(\theta^n - \theta^{-n}) = 0$$

and either $\theta^m - \theta^{-m} = \theta^n - \theta^{-n} = 0$ or for a suitable $\varrho \in Q(\sqrt{\Delta})$

$$a_1 = -\varrho(\theta^n - \theta^{-n}), \qquad a_2 = \varrho(\theta^m - \theta^{-m}).$$

In the former case since $(m, n) = 1$ we get from $\theta^{2m} = \theta^{2n} = 1$ that $\theta^2 = 1$, $\theta = \pm 1$, thus (23) holds. In the latter case assume first that θ is rational, $\theta = r/s$, $(r, s) = 1$. We get that

$$\varrho\frac{r^{2m}-s^{2m}}{r^m s^m} \in \boldsymbol{Z}, \quad \varrho\frac{r^{2n}-s^{2n}}{r^n s^n} \in \boldsymbol{Z},$$

hence $\varrho\dfrac{r^2-s^2}{r^n s^n} = k \in \boldsymbol{Z}$ and (24) is satisfied with $p = r^2+s^2$, $q = rs$.

Assume now that θ is a quadratic irrational and let q be the least positive integer such that $q\theta$ is an algebraic integer. Since θ^m is conjugate to θ^{-m} and θ^n is conjugate to θ^{-n} we infer from $(m, n) = 1$ that θ is conjugate to θ^{-1}. Hence (θ) factorizes into prime ideal factors of degree one unramified in $\boldsymbol{Q}(\sqrt{\Delta})$ and q equals the norm of the denominator of (θ). It follows that q^n is the least positive integer t such that $t\theta^n$ is an algebraic integer and q^{n-1} is the least positive integer u such that $u\dfrac{\theta^n-\theta^{-n}}{\theta-\theta^{-1}}$ is an algebraic integer. On the other hand from $(\theta^n-\theta^{-n})/(\theta-\theta^{-1}) \in \boldsymbol{Q}$ we infer that $\varkappa = \varrho(\theta-\theta^{-1}) \in \boldsymbol{Q}$ and $\varkappa\dfrac{\theta^n-\theta^{-n}}{\theta-\theta^{-1}} \in \boldsymbol{Z}$ implies that $\varkappa = q^{n-1}k/l$, $(qk, l) = 1$. Putting

$$\alpha = q\theta, \quad \beta = q\theta^{-1}, \quad p = q(\theta+\theta^{-1})$$

we get (24) with a_i replaced by la_i $(i = 0, 1, 2)$. However since $(\alpha, \beta) = 1$ we have $\left(\dfrac{\alpha^n-\beta^n}{\alpha-\beta}, \dfrac{\alpha^m-\beta^m}{\alpha-\beta}q^{n-m}\right) = 1$, thus $l = 1$. From $p = 0$ we infer $\theta^2 = -1$, $a_0a_1a_2 = 0$ contrary to the assumption. Hence $p \neq 0$ and the proof is complete.

Proof of Theorem 2. Estimating the number of triples $\langle a_0, a_1, a_2\rangle$ such that for at least one pair $\langle n_1, n_2\rangle$ the trinomial $a_0+\sum_{i=1}^{2} a_i x^{n_i}$ has a reciprocal factor we may assume in view of symmetry that $n_1 < n_2$. This enables us to use Lemma 9. The number of triples $\langle a_0, a_1, a_2\rangle$ satisfying

$$0 \leqslant |a_i| \leqslant a \quad (i = 0, 1, 2) \tag{25}$$

and (23) is clearly $O(a^2)$. Let $N_k(a)$ be the number of triples $\langle a_0, a_1, a_2\rangle$ satisfying (25) and (24) for a fixed k and suitable m, n, p, q. Since

$$N_k(a) = N_1(a/k) \quad \text{and} \quad \sum 1/k^2 < \infty$$

it is enough to show that $N_1(a) = O(a^2)$. Now

$$N_1(a) \leqslant N^0(a) + \sum_{n=1}^{\infty}\sum_{m=1}^{n-1} N^{+}_{m,n}(a) + \sum_{n=1}^{\infty}\sum_{m=1}^{n-1} N^{-}_{m,n}(a), \tag{26}$$

where $N^0(a)$ is the number of triples $\langle a_0, a_1, a_2\rangle$ satisfying (25) and (24) with $k = 1$,

$$q = 1, \quad |p|-2q \leqslant 0; \tag{27}$$

$N^{-}_{m,n}(a)$ is the number of triples satisfying (25) and (24) with $k = 1$,

$$|p|-2q < 0, \quad q > 1; \tag{28}$$

$N^{+}_{m,n}(a)$ is the number of triples satisfying (25) and (24) with $k = 1$,

$$|p|-2q > 0. \tag{29}$$

The conditions (24) and (27) imply that $|a_0| = |a_1| = |a_2|$. Hence

$$N^0(a) = O(a). \tag{30}$$

The conditions (24), (25) and (28) imply that

$$\max\{m, n-m\} \leqslant \frac{\log a}{\log q} \leqslant \frac{\log a}{\log 2}$$

and

$$q \leqslant a, \quad |p| \leqslant 2a \quad \text{if} \quad m = n-m = 1,$$

$$q \leqslant \sqrt{a}, \quad |p| < 2\sqrt{a} \quad \text{otherwise.}$$

Hence

$$\sum_{n=1}^{\infty}\sum_{m=1}^{n-1} N^{-}_{m,n}(a) < 4a^2+4a\left(\frac{\log a}{\log 2}\right)^2. \tag{31}$$

The condition (29) implies that α, β are real hence for ζ_n being a primitive nth root of unity

$$4\left|\frac{\alpha-\zeta_n^r\beta}{1-\zeta_n^r}\right|^2 = (\alpha+\beta)^2+(\alpha-\beta)^2\cot^2\frac{\pi r}{n} \quad (0 < r < n).$$

It follows that

$$\left|\frac{\alpha^n-\beta^n}{\alpha-\beta}\right| = \prod_{r=1}^{n-1}|\alpha-\zeta_n^r\beta| \geqslant \left|\frac{\alpha+\beta}{2}\right|^{n-1}\prod_{r=1}^{n-1}(1-\zeta_n^r) = \left|\frac{p}{2}\right|^{n-1} n > \left(\frac{3}{2}\right)^{n-1}$$

and the conditions (24) and (25) imply

$$n < \frac{\log\frac{3}{2}a}{\log\frac{3}{2}},$$

$$|p| \leqslant a \quad \text{if} \quad n = 2, \quad p \leqslant 2\sqrt{a/3} \quad \text{otherwise.}$$

Hence

$$\sum_{n=1}^{\infty}\sum_{m=1}^{n-1} N^{+}_{m,n}(a) < a^2+\frac{4}{3}a\left(\frac{\log\frac{3}{2}a}{\log\frac{3}{2}}\right)^2, \tag{32}$$

and $N_1(a) = O(a^2)$ follows from (26), (30), (31) and (32).

Remark 5. By a modification of the above argument one could get an asymptotic formula for the number of triples in question.

References

[1] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith. 21 (1972), pp. 153–171.

[2] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Proc. Symp. Pure Math. 24 (1973), pp. 91–101.

[3] H. Halberstam and H.-E. Richert, *Sieve methods*, New York–London 1974.

[4] S. Lang and A. Weil, *Varieties over finite fields*, Amer. J. Math. 76 (1954), pp. 819–827.

[5] A. Schinzel, *Reducibility of lacunary polynomials III*, Acta Arith. 34 (1977), pp. 225–266.

Received on 1.2.1983

and in revised form on 30.6.1983 (1337)

ACTA ARITHMETICA
XLIII (1984)

An application of the Fouvry–Iwaniec theorem

by

Martin Huxley (Cardiff)

The celebrated prime number theorem of Bombieri [1] and A. I. Vinogradov [7] states that for any $A > 0$ there is a constant B for which

$$Q \leqslant x^{1/2}(\log x)^{-B}$$

implies

$$\sum_{q\leqslant Q}\max_{(a,q)=1}\sup_{y\leqslant x}\left|\pi(y;q,a)-\frac{1}{\varphi(q)}\operatorname{li}y\right| \ll \frac{x}{(\log x)^A}.$$

It would be of great interest to extend the range for Q, even at the cost of the maxima over a and y. The first step in this direction has been taken by Fouvry and Iwaniec [4],

$$\sum_{\substack{q\leqslant Q\\(a,q)=1}}\lambda(q)\left\{\pi(x;q,a)-\frac{1}{\varphi(q)}\operatorname{li}x\right\} \ll \frac{x}{(\log x)^A}, \tag{1}$$

for

$$Q \leqslant x^{9/17-\varepsilon},$$

where $\lambda(q)$ satisfies extremely technical conditions, and the implied constant depends on a as well as on A and ε. A study of their paper indicates that we may replace the bound on the right hand side of (1) by

$$\ll \frac{|a|^{1/2}x}{(\log x)^A},$$

the implied constant now being independent of a. The Corollary in [4] stated only for $a = 2$, can now be extended as follows.

Let $\pi_2(x, a)$ denote the number of pairs of primes p, $p+a$ such that $p \leqslant x$. We then have with $B = 34/9$

$$\pi_2(x,a) \leqslant (B+\varepsilon)H(a)\frac{x}{(\log x)^2} \tag{2}$$