where $\varrho(s, 2v+2, -1)$ *is given by* (4.10), $\varrho(s, 2v, 1)$ *is given by* (4.11), *and* $g(s)$ *is given by* (4.9).

Hence, we have proved the following

THEOREM 4.2. *The number of* $s \times n$ *matrices* X *over* F_q *such that* $XX^T = 0$ *is*

$$N_s(I, 0) = \frac{1}{q^{s(s+1)/2}} \left\{ \sum_{\substack{r=0 \\ r \text{ even}}}^{s} \frac{g(s)}{\varrho(s, r, 1)} (q^{(2s-r)/2})^n + \sum_{\substack{r=1 \\ r \text{ odd}}}^{s} \frac{g(s)}{\varrho(s, r, -1)} (q^{(2s-r)/2})^n \right\}.$$

References

[1] A. A. Albert, *Symmetric and alternate matrices in an arbitrary field, I*, AMS Trans. 43 (1938), pp. 386–436.

[2] L. Carlitz, *Representations by quadratic forms in a finite field*, Duke Math. J. 21 (1954), pp. 123–137.

[3] — *Gauss sums over finite fields of order* 2^n, Acta Arith. 15 (1969), pp. 247–267.

[4] C. Chevalley, *The Algebraic Theory of Spinors*, New York 1954.

[5] L. E. Dickson, *Linear Groups With an Exposition of the Galois Theory*, Leipzig: Reprinted by Dover, 1958.

[6] Xu-ning Feng (Hsii-ning Feng) and Zong-duo Dai (Tsung-tuo Tai), *Studies in finite geometries and the construction of incomplete block designs V, Some Anzahl theorems in orthogonal geometry over finite fields of characteristic* 2, Chinese Math. Acta. 15 (1965), pp. 392–410.

[7] John H. Hodges, *A symmetric matrix equation over a finite field*, Math. Nachr. 30 (1965), pp. 221–228.

[8] John C. Perkins, *Rank r solutions to the matrix equation* $XX^T = 0$ *over a field of characteristic* 2, Math. Nachr. (to appear).

Received on 8. 3. 1970 56

ACTA ARITHMETICA
XIX (1971)

On a problem of Schinzel concerning principal divisors in arithmetic progressions

by

CHARLES J. PARRY (East Lansing, Mich.)

The following problem was proposed by A. Schinzel at the A. M. S. Number Theory Institute held at Stony Brook, New York in July of 1969.

QUESTION I. *Let* $f(x)$ *be a primitive polynomial and* k *an algebraic number field. Do there exist infinitely many integers* x *such that* $f(x)$ *factors into principal ideals in* k? (*unknown even for* f *linear*).

For the case that f is linear, I prove here that the answer is yes. It has been noted [2] for polynomials of higher degree that the following additional assumptions are necessary:

(i) the content of any factor of $f(x)$ in k is principal (MacCluer);
(ii) each fixed divisor of $f(x)$ is principal (Schinzel).

Introduction. In the linear case, that is, when $f(x) = mx+b$ with $(m, b) = 1$, it seems reasonable to ask the slightly stronger:

QUESTION II. *Do there exist infinitely many primes of the form* $mx+b$ *which split into principal prime ideals in* k?

The following example (MacCluer) shows that the answer to Question II is no. (Schinzel has informed me that a similar counterexample was found earlier by J. Tate.)

The number field $Q(\sqrt{10})$ has class number $h = 2$ and Hilbert class field $\mathrm{CF}(Q(\sqrt{10})) = Q(\sqrt{2}, \sqrt{5})$. According to Artin reciprocity, a rational prime $p \neq 2, 5$ has non-principal divisors in $Q(\sqrt{10})$ when and only when p splits in $Q(\sqrt{10})$ into two distinct prime divisors, each of which remains prime in $Q(\sqrt{2}, \sqrt{5})$, in Legendre symbols this is equivalent to

$$\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = -1$$

which obtains when and only when $p \equiv \pm 3, \pm 13 \pmod{40}$. Thus for instance, no prime of the form $p = 40x+3$ has principal divisors in $Q(\sqrt{10})$.

However, Question II is worthy of closer examination as it suggests an approach to the first question. Specifically I shall prove the following:

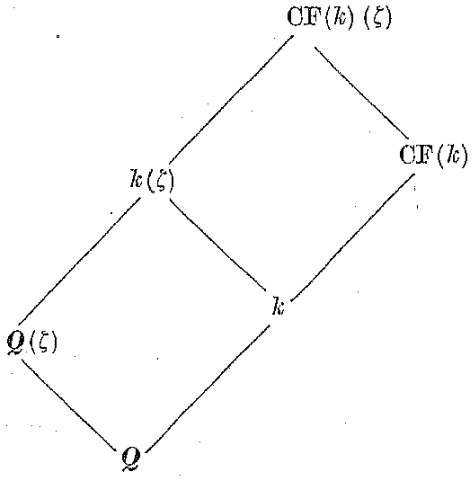
THEOREM I. *Let k be a number field galois over $\boldsymbol{Q}$, $\mathrm{CF}(k)$ the class field of k and ζ a primitive m-th root of unity. If $\mathrm{CF}(k) \cap k(\zeta) = k$ and if $k \cap \boldsymbol{Q}(\zeta) = \boldsymbol{Q}$, then for each $(a, m) = 1$ there are infinitely many primes $p \equiv a \pmod m$ which split principally and completely in k.* (I will say a rational p prime *splits principally* in k if each prime factor of p in k is principal in k.)

Recall the following result [1] which I shall prove for completeness.

LEMMA I. *If K/k is galois, then so is $\mathrm{CF}(K)/k$.*

Proof. Let σ be an isomorphism of $\mathrm{CF}(K)/k$. Then $\sigma\big(\mathrm{CF}(K)\big)$ is an unramified abelian extension of $\sigma(K) = K$. Hence $\sigma\big(\mathrm{CF}(K)\big) \subset \mathrm{CF}(K)$ and by a degree argument $\sigma\big(\mathrm{CF}(K)\big) = \mathrm{CF}(K)$.

Proof of Theorem I. We have the following Artin diagram.



A prime $\mathfrak{p}$ with Artin symbol, $\left(\frac{k(\zeta)/k}{\mathfrak{p}}\right) = \sigma_a$, where $\sigma_a(\zeta) = \zeta^a$, has absolute norm $\|\mathfrak{p}\| \equiv a \bmod m$. Thus if in addition $\mathfrak{p}$ in linear over $\boldsymbol{Q}$, then $\|\mathfrak{p}\| = p \equiv a \bmod m$. It remains then only to produce infinitely many such principal primes $\mathfrak{p}$, i.e., with Artin symbol $\left(\frac{\mathrm{CF}(k)/k}{\mathfrak{p}}\right) = 1$.

But by hypothesis the galois group

$$G\big(\mathrm{CF}(k)\,(\zeta)/k\big) \cong G\big(\mathrm{CF}(k)/k\big) \times G\big(k(\zeta)/k\big).$$

Thus by the Čebotarev density theorem $1/h\varphi(m)$ of the primes of k have $\left(\frac{\mathrm{CF}(k)\,(\zeta)/k}{\mathfrak{p}}\right) = 1 \times \sigma_a$ and thus at least $1/h\varphi(m)\,(k : \boldsymbol{Q})$ of the rational primes p split principally in k and satisfy

$$p \equiv a \bmod m.$$

COROLLARY I. *Let k be a number field (not necessarily galois over $\boldsymbol{Q}$) and Δ be the discriminant of k. Suppose $(m, \Delta) = 1$; then there are infinitely many primes $p \equiv a \bmod m$ which split principally and completely in k.*

Proof. Since $(\Delta, m) = 1$ we have that every prime divisor of m is unramified in k and hence unramified in the galois closure $\bar{k}$ of k. However, the only primes ramified in $\boldsymbol{Q}(\zeta)$ are the divisors of m. Hence $\boldsymbol{Q}(\zeta) \cap \bar{k} = \boldsymbol{Q}$. From this it follows that

$$[\mathrm{CF}(\bar{k}) \cap \bar{k}(\zeta) : \bar{k}] = \big[\big(\mathrm{CF}(\bar{k}) \cap \bar{k}(\zeta)\big) \cap \boldsymbol{Q}(\zeta) : \boldsymbol{Q}\big].$$

Now because $(\Delta, m) = 1$ no prime can ramify in the extension $\big(\mathrm{CF}(\bar{k}) \cap \bar{k}(\zeta) \cap \boldsymbol{Q}(\zeta)\big)/\boldsymbol{Q}$ and so this has degree 1, hence $\mathrm{CF}(\bar{k}) \cap \bar{k}(\zeta) = \bar{k}$. We can thus apply Theorem I to get infinitely many primes $p \equiv a \bmod m$ which split principally and completely in $\bar{k}$ and hence also split principally and completely in k.

REMARK. *It is worth noting that there are always infinitely many positive rational primes $p \equiv 1 \bmod m$ (for any m) which split principally and completely in any number field k.*

Proof. By the Čebotarev density theorem the set of primes which split completely in $\mathrm{CF}(\bar{k})\,(\zeta)$ has positive density. Each of these primes p splits completely in $\boldsymbol{Q}(\zeta)$ so

$$p \equiv 1 \bmod m.$$

However, each factor $\mathfrak{p}$ of p in $\bar{k}$ gains degree 1 in $\mathrm{CF}(\bar{k})$. Thus p splits principally and completely in $\bar{k}$ and hence also in k.

Resolution of the linear case. As we have just seen, there are infinitely many primes $p \equiv a \bmod m$ that split principally in k provided the modulus m contains no primes that ramify in k. On the other hand, we have seen that there are no primes $p \equiv 3 \bmod 40$ that split principally in $\boldsymbol{Q}(\sqrt{10})$, a field in which both 2 and 5 ramify. We shall soon see that the nonexistence of such primes is not solely because of the ramification of the factors 2 or 5 of $m = 40$, but because $m = 40$ has at least two distinct prime factors, both of which are ramified. For

THEOREM II. *Let $k/\boldsymbol{Q}$ be galois, l be a prime, $(a, l) = 1$, and $(m', l) = 1$; then for any $n \geqslant 1$ there are infinitely many positive rational primes p which split principally in k with*

$$p \equiv a \bmod l^n$$

and

$$p \equiv 1 \bmod m'.$$

Once that we have proved Theorem II we have an immediate solution to Question I for $k/\mathbf{Q}$ galois. That is:

THEOREM III. *If $k/\mathbf{Q}$ is galois and $(a, m) = 1$, then there are infinitely many rational integers*

$$x \equiv a \bmod m$$

all of whose prime factors split principally in k.

Later I will show that the assumption of normality on $k/\mathbf{Q}$ can be deleted. But now I prove Theorem II via two lemmas.

LEMMA II. *Let M/L and N/L be finite extensions of the number field L. Suppose M/L and MN/L are galois and $M \cap N = L$. Let $\mathfrak{P}$ be a prime of MN such that the degree of $\mathfrak{P}_N = \mathfrak{P} \cap N$ over L equals 1. Let $\mathfrak{p} = \mathfrak{P} \cap M$. Then the order of $\left[\frac{M/L}{\mathfrak{p}}\right]$ is precisely the order of $\left[\frac{MN/N}{\mathfrak{P}}\right]$.*

Proof. We first note that we have an isomorphism between the galois groups $G(MN/N)$ and $G(M/L)$ and that the isomorphism is given by restriction map

$$\sigma \mapsto \sigma|_M.$$

Let $\left[\frac{MN/L}{\mathfrak{P}}\right] = \sigma$. Since the degree of $\mathfrak{P}_N$ over L is 1, it follows that

$$\left[\frac{MN/N}{\mathfrak{P}}\right] = \left[\frac{MN/L}{\mathfrak{P}}\right] = \sigma$$

and so $\sigma \in G(MN/N)$. Thus the order of σ equals the order of $\sigma|_M$. But from the definition of the Frobenius symbol

$$\sigma|_M = \left[\frac{M/L}{\mathfrak{p}}\right].$$

LEMMA III. *Let $k/\mathbf{Q}$ be a finite galois extension and l a rational prime. Let $\mathfrak{L}$ be a prime divisor of l in the class field $\mathrm{CF}(k)$ of k with inertia field $I = I(\mathfrak{L})$ over $\mathbf{Q}$. Finally let $\mathfrak{P}$ be a prime of $\mathrm{CF}(k)$ unramified over $\mathbf{Q}$.*

If the degree of the prime $\mathfrak{P}_I = \mathfrak{P} \cap I$ is 1 over $\mathbf{Q}$ (or even over $k \cap I$), then the prime

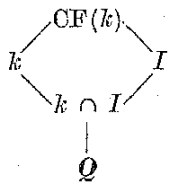
$$\mathfrak{p} = \mathfrak{P} \cap k$$

is principal in k. Moreover, the rational prime

$$p = \mathfrak{P} \cap \mathbf{Q}$$

splits principally in k.

Proof. We have the following diagram:



Recall that $\mathrm{CF}(k)/\mathbf{Q}$ is galois.

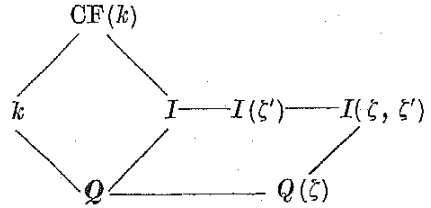
Note that $k \cap I$ is the inertia field of $\mathfrak{L} \cap k$ over Q and since $\mathrm{CF}(k)/k$ is unramified,

$$[\mathrm{CF}(k) : I] = [k : (k \cap I)].$$

Since $k/(k \cap I)$ is normal it follows that $\mathrm{CF}(k) = kI$.

By Lemma II it follows that the order of $\left[\frac{\mathrm{CF}(k)/I}{\mathfrak{P}}\right]$ equals the order of $\left[\frac{k/(k \cap I)}{\mathfrak{p}}\right]$ equals f, say. Now since the degree of $\mathfrak{P}_I$ over $k \cap I$ is 1, the degree of $\mathfrak{P}$ over $k \cap I$ is f. But the degree of $\mathfrak{p}$ over $k \cap I$ is also f so $\mathfrak{p}$ must gain degree 1 in the extension $\mathrm{CF}(k)/k$. Thus $\mathfrak{p}$ is principal in k and since k is normal, p must split principally in k.

Proof of Theorem II. We let ζ be a primitive l^n-th root of unity and ζ' a primitive m' root of unity. We have



where I is as in Lemma II. Now $I(\zeta') \cap \mathbf{Q}(\zeta) = \mathbf{Q}$, since l is totally ramified in $\mathbf{Q}(\zeta)$ yet has an unramified prime factor in $I(\zeta')$. Hence

$$G(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong G(I(\zeta, \zeta')/I(\zeta')).$$

Thus the substitution $\sigma_a(\zeta) = \zeta^a$ is an automorphism of $I(\zeta, \zeta')/I(\zeta')$. By the Čebotarev density theorem, the set of primes $\mathfrak{p}$ of $I(\zeta')$ with Artin symbol

$$\left(\frac{I(\zeta, \zeta')/I(\zeta')}{\mathfrak{p}}\right) = \sigma_a$$

has positive density. Since almost all primes of $I(\zeta')$ are of degree 1 over Q, we need only consider such linear primes. However, if $\mathfrak{p}$ is such a prime, then

$$p = \|\mathfrak{p}\| \equiv a \bmod l^n$$

and

$$p \equiv 1 \bmod m'.$$

Let $\mathfrak{p}_I = \mathfrak{p} \cap I$; then the degree of $\mathfrak{p}_I$ over Q is 1. So by Lemma III, p must split principally in k which proves Theorem II.

I will now show that the assumption of normality on k/Q can be deleted.

LEMMA IV. *Let k be an arbitrary number field and $\bar{k}$ be the galois closure of k. Suppose l is a rational prime and $\mathfrak{L}$ is a prime factor of l in $\mathrm{CF}(\bar{k})$. Take $I = I(\mathfrak{L})$ to be the inertia field of $\mathfrak{L}$ over Q and $T = T(\mathfrak{L})$ the inertia group. Then*

$$T \cap G\big(\mathrm{CF}(\bar{k})/\mathrm{CF}(k)\big) = T \cap G\big(\mathrm{CF}(\bar{k})/k\big).$$

Proof. Let I' and I'' be the inertia fields of $\mathfrak{L}$ over k and $\mathrm{CF}(k)$ respectively. Since $\mathrm{CF}(k)/k$ is unramified, it follows that $\mathrm{CF}(k) \subset I'$, and so $I' = I''$. However,

$$G\big(\mathrm{CF}(\bar{k})/I'\big) = T \cap G\big(\mathrm{CF}(\bar{k})/k\big)$$

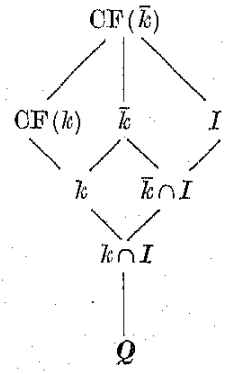
and

$$G\big(\mathrm{CF}(\bar{k})/I''\big) = T \cap G\big(\mathrm{CF}(\bar{k})/\mathrm{CF}(k)\big).$$

With the same notation we now have

LEMMA V. *If $\mathfrak{P}$ is any prime of $\mathrm{CF}(\bar{k})$ such that $\left[\dfrac{\mathrm{CF}(\bar{k})/Q}{\mathfrak{P}}\right] \in T$, then $\mathfrak{p} = \mathfrak{P} \cap k$ is principal in k.*

Proof. We have the following diagram



Say $\left[\dfrac{\mathrm{CF}(\bar{k})/Q}{\mathfrak{P}}\right] = \sigma$ and that the degree of $\mathfrak{p}$ over Q is f_1, then

$$\left[\frac{\mathrm{CF}(\bar{k})/k}{\mathfrak{P}}\right] = \sigma^{f_1} \in G\big(\mathrm{CF}(\bar{k})/k\big) \cap T.$$

Hence

$$\sigma^{f_1} \in G\big(\mathrm{CF}(\bar{k})/\mathrm{CF}(k)\big) \cap T$$

by Lemma IV. Thus $\mathfrak{p} = \mathfrak{P} \cap k$ gains degree 1 in $\mathrm{CF}(k)/k$.

COROLLARY II. *If $\left[\dfrac{\mathrm{CF}(\bar{k})/Q}{\mathfrak{P}}\right] \in T$, then $p = \mathfrak{P} \cap Q$ splits principally in k.*

Proof. In the preceding proof we can replace k by any of its conjugate fields $\sigma(k)$ and $\mathrm{CF}(k)$ by $\mathrm{CF}\big(\sigma(k)\big)$ and get that $\mathfrak{p}_\sigma = \mathfrak{P} \cap \sigma(k)$ is principal. Say $\mathfrak{p}_\sigma = \sigma(\alpha)$. Then $\sigma^{-1}(\mathfrak{p}_\sigma) = \alpha$ is principal in k. But $\sigma^{-1}(\mathfrak{P})$ lies above $\sigma^{-1}(\mathfrak{p}_\sigma)$ and since the galois group acts transitively on the primes of $\mathrm{CF}(\bar{k})$ dividing p, it follows that all prime factors of p are principal in k.

And so finally we have

THEOREM IV. *If k is an arbitrary field and $(a, m) = 1$, then there are infinitely many rational integers*

$$x \equiv a \bmod m$$

all of whose prime factors split principally in k.

Proof. Using the result of the preceding corollary we can now retrace the proof of Theorem II and the desired result follows.

It is now possible to strengthen Corollary I. Specifically I shall prove

THEOREM V. *Let k be a number field with discriminant Δ. If m is a positive integer with $(m, \Delta) = l^n$, where l is prime, then for each a with $(a, m) = 1$ there are infinitely many primes*

$$p \equiv a \bmod m$$

which split principally in k.

Proof. Let $\mathfrak{L}$ be a prime factor of l in $\mathrm{CF}(\bar{k})$ and take $I = I(\mathfrak{L})$ to be the inertia field of $\mathfrak{L}$. If ζ is an mth root of unity, then

$$Q(\zeta) \cap I = Q$$

hence the substitution

$$\sigma_a\colon\ \zeta \mapsto \zeta^a$$

is in $G\big(I(\zeta)/I\big)$.

Now the set of linear primes P of I with

$$\left(\frac{I(\zeta)/I}{P}\right) = \sigma_a$$

has positive density. But

$$p = \|P\|_I \equiv a \bmod m$$

and by Corollary II p splits principally in k.

References

[1] E. Artin, *Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz*, Abh. Math. Sem. Hamburg 7 (1930), p. 51.

[2] C. R. MacCluer, *Non-principal divisors among the values of polynomials*, Acta Arith. (to appear).

MICHIGAN STATE UNIVERSITY
East Lansing, Michigan

Received on 15. 3. 1970

ACTA ARITHMETICA
XIX (1971)

Bounds for solutions of diagonal equations

by

JANE PITMAN (Adelaide, South Australia)

1. Introduction. In the first part of this paper (§ 2 to § 7) I shall prove the following theorem for the case $k \geqslant 4$.

THEOREM 1. *Let k be an integer, $k \geqslant 2$, and let n be the integer defined by*

$$(1)\qquad \begin{cases} n = 2^k+1 & \text{if} \quad 2 \leqslant k \leqslant 11, \\ n \geqslant 2k^2(2\log k + \log\log k + 3) + 1 > n-1 & \text{if} \quad k \geqslant 12. \end{cases}$$

Then for any $\theta > 0$ there exists a constant c_θ, depending only on θ and k, with the following property. If $\lambda_1, \ldots, \lambda_n$ are non-zero integers which are not all of the same sign if k is even, then the Diophantine equation

$$(2)\qquad \lambda_1 x_1^k + \lambda_2 x_2^k + \ldots + \lambda_n x_n^k = 0$$

has a solution in non-zero integers such that

$$(3)\qquad |\lambda_1 x_1^k| + \ldots + |\lambda_n x_n^k| < c_\theta |\lambda_1 \lambda_2 \ldots \lambda_n|^{k\psi+\theta},$$

where

$$(4)\qquad \psi = \begin{cases} \frac{1}{2} & \text{if} \quad 2 \leqslant k \leqslant 11, \\ 1 & \text{if} \quad k \geqslant 12. \end{cases}$$

The case $k = 2$ of the theorem (which is a modified form of a theorem of Cassels [3]) was proved by Birch and Davenport [2] and was used in their proof of a corresponding result on diagonal quadratic inequalities [1]. The case $k = 3$ was proved by Pitman and Ridout [11] and used similarly in the proof of a corresponding result on cubic inequalities. The proof for the case $k \geqslant 4$ is a straightforward generalization of the proof of Theorem 1 of [11]. The theorem for $k \geqslant 4$ is an essential preliminary to my proof [10] of a theorem (Theorem A in § 9 below) which gives a bound for the least non-trivial solution of the Diophantine inequality

$$(5)\qquad |\lambda_1 x_1^k + \ldots + \lambda_n x_n^k| < 1,$$

where n is defined by (1), and $\lambda_1, \ldots, \lambda_n$ are real numbers which satisfy $|\lambda_i| \geqslant 1$ for all i and which are not all of the same sign if k is even. From