Daraus hat man aus (7.5) für $t^* > c_{31}$

$$|V| \geqslant \left(\frac{1}{\log t^*}\right)^{c_{32}\log\log t^*} = e^{-c_{32}(\log\log t^*)^2}.$$

Mit Berücksichtigung von (6.9) ist weiter

$$c_{19}\frac{\xi^{1-\sigma^*}\log t^*}{(t^*)^{309/320}} > \frac{1}{e^{c_{32}(\log\log t^*)^2}} > \frac{\log t^*}{t^{*1/320}}.$$

Also endlich

$$\xi^{1-\sigma^*} > t^{*19/20}$$

und nach (6.5), (6.4), (6.6), ist

$$\tfrac{19}{20}\log t^* < (1-\sigma^*)\log\xi = (1-\sigma^*)(k+2)\lambda \leqslant (1-\sigma^*)\tfrac{54}{4}\log\omega_1^{-1}(\log t^{*4/a}).$$

Daraus folgt

$$1-\sigma^* \geqslant \frac{19}{270}\cdot\frac{\log t^*}{\log\omega_1^{-1}(\log t^{*4/a})},$$

was der Annahme (6.1) widerspricht. Damit ist unser Satz bewiesen. Um Satz I′ zu bekommen, genügt es nur die Abschätzung (8.5) auf (1.12) anzuwenden.

Die Abschätzung in (8.5) ist eigentlich ganz grob. Es muß so sein, weil wir zu wenig von der Funktion $\eta_1(\tau)$ angenommen haben. Wenn wir die Methoden der Differentialrechnung auf die Abschätzung von (3.1) bzw. (8.6) anwenden wollen, dann zeigt sich, dass die Lokalisation des Maximums in (8.6), von dem, wie schnell die Ableitung $\eta_1'(\tau)$ zu Null strebt abhängen muß. Auf diesem Weg könnte man eine Verbesserung von (1.13) erwarten, jedoch auf Kosten zusätzlicher Bedingungen für die Funktion $\eta_1(\tau)$.

Literaturverzeichnis

[1] P. Erdös, *On new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc, Nat. Acad. Sci. USA 35 (1949), S. 374-384.

[2] A. E. Ingham, *The distribution of prime numbers*, Cambridge 1932.

[3] A. Selberg, *An elementary proof of the prime-number theorem*, Ann. Math. Princeton, II. 50 (1949), S. 305-313.

[4] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen* Budapest 1953.

UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU
ADAM MICKIEWICZ UNIVERSITÄT IN POZNAŃ

Reçu par la Rédaction le 22. 8. 1960

ACTA ARITHMETICA
VI (1961)

The easier Waring problem in algebraic number fields

by

ROSEMARIE M. STEMMLER* (Urbana, Ill.)

I. Introduction. Let K be an algebraic number field of degree n, $n = n_1+2n_2$, and J its ring of integers. Let $K^{(1)}, K^{(2)}, \ldots, K^{(n)}$ be the n conjugate fields of K, $K^{(r)}$ $(r = 1, 2, \ldots, n_1)$ being real and $K^{(r)}$, $K^{(r+n_2)}$ $(r = n_1+1, \ldots, n_1+n_2)$ being conjugate complex. Let J_m be the group generated under addition by the m-th powers of the integers of K, where $m \geqslant 2$. Actually J_m is a ring. We define $v(m; K)$ as the least value of s for which every integer ν in J_m is representable in the form

$$\nu = \pm\lambda_1^m \pm \lambda_2^m \pm \ldots \pm \lambda_s^m,$$

where $\lambda_1, \lambda_2, \ldots, \lambda_s$ are integers of K. By the easier Waring problem we mean the problem of determining $v(m; K)$.

If there exists an identity

$$\sum_{k=1}^{r} e_k(a_k x + b_k)^m = cx + d, \quad c \neq 0, \quad e_k = \pm 1 \quad (k = 1, 2, \ldots, r)$$

with rational integral coefficients, we see that J_m consists of certain residue classes modulo c. We let $\Delta_K(m, c)$ be the least value of s such that every member of J_m is congruent modulo c to an integer of the form $\pm\lambda_1^m \pm \ldots \pm \lambda_s^m$, where $\lambda_1, \lambda_2, \ldots, \lambda_s$ are integers in K. Then clearly

$$v(m; K) \leqslant r + \Delta_K(m, c).$$

From the $(m-1)$-th difference of x^m we have

$$\sum_{k=0}^{m-1}(-1)^{m-1-k}\binom{m-1}{k}(x+k)^m = m!x + \tfrac{1}{2}(m-1)m!,$$

* Doctoral dissertation, University of Illinois, Urbana, Illinois. This research was supported by the U. S. Office of Naval Research. Thanks are due to Professor P. T. Bateman for his help and encouragement.

which is an identity of the type desired. As

$$\sum_{k=0}^{m-1}\binom{m-1}{k}=2^{m-1}, \quad \text{we have} \quad v(m;K)\leqslant 2^{m-1}+\Delta_K(m,m!).$$

Since the order of $J/(m!)$ is finite, it is easy to see that $v(m;K)$ is finite.

When m is prime we shall produce upper bounds for $v(m;K)$ which do not depend on the field K; specifically

$$v(2;K)=3,$$

$$v(3;K)\leqslant 6,$$

$$v(q;K)\leqslant 2^{q-1}+(q-1)/3+1 \text{ when } q \text{ is a prime greater than 3.}$$

When m is not prime we only show that

$$v(m;K)\leqslant n(2m-1)+1+2^{m-1} \quad \text{when } m \text{ is odd,}$$

$$v(m;K)\leqslant n(4m-1)+1+2^{m-1} \quad \text{when } m \text{ is even.}$$

At the same time we establish the fact that when $s>n(4m-1)$ the congruence

$$\lambda_1^m+\ldots+\lambda_s^m\equiv \nu \pmod{P^a}$$

has primitive solutions in integers $\lambda_1,\ldots,\lambda_s$ for every integer ν in J_m and for every prime ideal P and every positive integer a; from this we may conclude that the singular series in Waring's problem has a positive lower bound when the number of summands exceeds $n(4m-1)$.

Another problem suggesting itself is the comparison of values of $v(m;K)$ with known upper and lower bounds for $v(m;R)$, where R is the rational number field. We show that there do exist algebraic number fields K in which $v(m;K)$ is less than $v(m;R)$. This is natural to suspect in fields containing appropriate m-th roots of rational integers. The question is open whether, on the other hand, there are fields in which more m-th powers are needed to express the integers of J_m than is the case in the rational number field.

Greek letters $\alpha,\beta,\ldots$ will denote algebraic integers in K, $\alpha^{(j)}$ being the j-th conjugate of α in $K^{(j)}$. If P is a prime integral ideal in K, $P^a||\alpha$ will mean $P^a\mid\alpha$, $P^{a+1}\nmid\alpha$.

Of course results on the easier Waring problem follow from the work of Siegel, Peck, Ayoub, and Tatuzawa on the Waring problem proper ([8], [11], [7], [1], [12]). However, except for fields of low degree over the rationals, the results so obtained are poorer than the results obtained directly in this paper. In fact, the strong dependence on the field degree which occurs in the known results for the Waring problem proper is the main difficulty in the subject at the present time. The present paper shows that by going over to the easier Waring problem we can at least partially eliminate this dependence on the field degree.

II. Determination of $v(2;K)$ for all algebraic number fields. In this section we shall prove that $v(2;K)=3$. We first establish 3 as an upper bound. Then we determine for every field K some integer which belongs to J_2 but cannot be represented as the sum of two integers of the form $\pm\lambda^2$.

THEOREM 1. *$v(2;K)\leqslant 3$ for any K.*

Proof. For any integers α and β in K we have

$$\alpha^2\equiv-\alpha^2 \pmod 2$$

and

$$(\alpha+\beta)^2\equiv\alpha^2+\beta^2 \pmod 2.$$

Therefore every element of J_2 is congruent to a square modulo 2 or $\Delta(2,2!)=1$. Since

$$2x+1=(x+1)^2-x^2,$$

every element in the residue class modulo 2 represented by 1 is the difference of two squares. Therefore every number in J_2 is expressible by not more than 3 squares.

Theorems 2 and 3 give sufficient conditions for an integer not to be representable as the difference or sum, respectively, of 2 squares.

THEOREM 2. *Let P be a prime ideal in K such that $P^a||2$, and let b be a rational integer such that $1\leqslant b\leqslant a$. If α is an integer in K such that $P^{2b-1}||\alpha$, then α is not expressible as the difference of 2 integral squares.*

Proof. Assume α is the difference of 2 integral squares, that is

$$\alpha=\beta^2-\gamma^2=(\beta+\gamma)(\beta-\gamma).$$

We have

$$\beta+\gamma\equiv\beta-\gamma \pmod 2$$

which implies

$$\beta+\gamma\equiv\beta-\gamma \pmod{P^j}$$

whenever $1\leqslant j\leqslant a$.

There exist non-negative rational integers b' and b'' satisfying the conditions

$$P^{b'}||(\beta+\gamma), \quad P^{b''}||(\beta-\gamma).$$

Now $\max(b', b'') < a$; for if $\max(b', b'') \geqslant a$, then

$$\beta - \gamma \equiv 0 \pmod{P^a} \quad \text{and} \quad \beta + \gamma \equiv 0 \pmod{P^a},$$

and therefore $P^{2a} | a$, contradicting $P^{2b-1} || a$, since $2a > 2b-1$. Therefore $\beta + \gamma \equiv \beta - \gamma \pmod{P^{\max(b,b')}}$, and so $b' = b''$, which is impossible since $b' + b''$ must equal $2b-1$.

THEOREM 3. *If $\sqrt{-1}$ is not in K, then there exist infinitely many prime ideals P in K such that any integer containing an odd power of P in its prime ideal factorization is not the sum of two squares.*

Proof. Applying a theorem stated by Hecke ([4], p. 251), we conclude that there are infinitely many odd prime ideals P in K such that -1 is not congruent to a square modulo P. If a contains an odd power of P in its prime ideal factorization, a cannot be decomposed into a sum of two squares. For assume on the contrary that $a = \beta^2 + \gamma^2$ and

$$(a) = (\beta^2 + \gamma^2) = P^{2a-1} C,$$

where β and γ are integers, a is a positive integer, and $(C, P) = 1$. Then

$$\beta^2 \equiv -\gamma^2 \pmod{P^{2a-1}}.$$

Since -1 is not congruent to a square modulo P, this is impossible unless $P | \beta$ and $P | \gamma$, which implies $P^2 | \beta^2$ and $P^2 | \gamma^2$. If $a = 1$, this contradicts $P || a$. If $a > 1$ and P^{2b} is the highest even power of P dividing both β^2 and γ^2, let Φ be a number in K such that $(\Phi)P$ is an integral ideal relatively prime to P (cf. [4], p. 97). Then $\Phi^b \beta$ and $\Phi^b \gamma$ are integers and

$$\Phi^{2b} a = (\Phi^b \beta)^2 + (\Phi^b \gamma)^2.$$

But $2a - 1 > 2b$, and therefore

$$(\Phi^b \beta)^2 \equiv -(\Phi^b \gamma)^2 \pmod{P}.$$

As P does not divide both $\Phi^b \beta$ and $\Phi^b \gamma$, this is again contradictory. Thus we have the theorem.

Now we are able to prove the main result of this section.

THEOREM 4. $v(2; K) = 3$ *for any* K.

Proof. From Theorem 1 we know that $v(2; K) \leqslant 3$ always. We treat the problem of the lower bound in two cases:

Case 1. *K contains $\sqrt{-1}$.*

From the basic identity we know that the ideal $2J$ is contained in the ring J_2. The prime $2 = -\sqrt{-1}(1+\sqrt{-1})^2$, and therefore there exists a prime ideal factor P of 2 in K such that $P^{2a} || 2$. If $(a) = 2PC$, where C is an ideal prime to $2P$ chosen so as to make $2PC$ principal, the

integer a is not the difference of 2 squares by Theorem 2. But a is not the sum of 2 squares either, for if $a = \beta^2 + \gamma^2$ for integral β and γ, then

$$a = \beta^2 - (\sqrt{-1}\gamma)^2,$$

that is, a is the difference of two squares.

Case 2. *K does not contain $\sqrt{-1}$.*

By Theorem 3 there exists a prime ideal Q in K such that $(Q, 2) = 1$ and such that any integer containing an odd power of Q in its prime ideal factorization is not representable as the sum of 2 squares. We put

$$(a) = \begin{cases} 2QC_1, & \text{where } (C_1, 2Q) = 1, \text{ if all the prime ideal factors of} \\ & 2 \text{ have odd multiplicity,} \\ 2QPC_2, & \text{where } (C_2, 2Q) = 1, \text{ if } P \text{ is a prime ideal factor of} \\ & 2 \text{ having even multiplicity,} \end{cases}$$

C_1 and C_2 being ideals chosen to obtain in each case a principal ideal (a). Then a belongs to $2J$ and therefore to J_2, but by Theorems 2 and 3 a cannot be decomposed into a sum or difference of 2 squares. In both cases a cannot be expressed as $-\beta^2 - \gamma^2$, because then $-a$ would be the sum of β^2 and γ^2 and yet have the same prime ideal factorization as a. Therefore $v(2; K) \geqslant 3$ in Case 1 and in Case 2, which proves the theorem.

III. Upper bounds for $v(q; K)$ when q is an odd prime. We shall suppose throughout this section that q denotes an odd prime, p a prime. A formula for an upper bound of $v(q; K)$ will be developed which is independent of the field K; the cases $q = 3$ and $q = 5$ will be examined separately in order to obtain slightly better results than those given by the general formula. Theorems 5, 6 and 7 deal with arbitrary integers m rather than q.

DEFINITION. If P is a prime ideal in K, let $J_m(P)$ be the set of integers ν in K such that the congruence $\nu \equiv \pm\lambda_1^m(j) \pm \lambda_2^m(j) \pm \ldots \pm \lambda_s^m(j) \pmod{P^j}$ has integral solutions $\lambda_1(j), \lambda_2(j), \ldots, \lambda_s(j)$ in K for all positive integers j and some positive integer s depending on ν and j.

If $P^t || m!$, let $J'_m(P)$ be the set of integers ν in K such that the congruence $\nu \equiv \pm\lambda_1^m \pm \lambda_2^m \pm \ldots \pm \lambda_s^m \pmod{P^t}$ has a solution in integers $\lambda_1, \ldots, \lambda_s$ in K for some positive integer s depending on ν. Both $J_m(P)$ and $J'_m(P)$ are rings.

DEFINITION. If A is an integral ideal in K, an integral solution $\lambda_1, \ldots, \lambda_s$ in K of a congruence

$$\nu \equiv \pm\lambda_1^m \pm \lambda_2^m \pm \ldots \pm \lambda_s^m \pmod{A}$$

is called *primitive* if $(\lambda_1, \lambda_2, \ldots, \lambda_s, A) = 1$.

THEOREM 5. *If $P^c \| m$, if i is a positive integer equal to or greater than $2c+1$, and the congruence*

$$(*) \qquad v \equiv \lambda_1^m + \lambda_2^m + \ldots + \lambda_r^m - \lambda_{r+1}^m - \ldots - \lambda_s^m \pmod{P^i},$$

has a primitive integral solution $\lambda_1, \lambda_2, \ldots, \lambda_s$ in K, where $s \geqslant r \geqslant 0$, $s > 0$, then the congruence

$$v \equiv \lambda_1^m + \ldots + \lambda^m - \lambda_{r+1}^m - \ldots - \lambda_s^m \pmod{P^{i+1}}$$

also has a primitive integral solution $\lambda_1, \lambda_2, \ldots, \lambda_s$ in K.

Proof. We may assume that $(\lambda_1, P) = 1$ and that λ_1^m carries the plus-sign in the congruence (*). Let

$$\lambda_1 = \lambda(i), \qquad \alpha = v - \lambda_2^m - \lambda_3^m - \ldots - \lambda_r^m + \lambda_{r+1}^m + \ldots + \lambda_s^m.$$

Then

$$\alpha \equiv \lambda^m(i) \pmod{P^i},$$

and it will suffice to show that there exists an integer $\lambda(i+1)$ in K such that $(\lambda(i+1), P) = 1$ and $\alpha \equiv \lambda^m(i+1) \pmod{P^{i+1}}$. If $\alpha \equiv \lambda^m(i) \pmod{P^{i+1}}$, we take $\lambda(i+1) = \lambda(i)$. If not, let δ_i and ϱ_i be integers satisfying the relations

$$\delta_i m = \varrho_i \big(\alpha - \lambda^m(i)\big), \qquad P \nmid \varrho_i.$$

Take $\lambda(i+1) = \lambda(i) + \delta_i \sigma_i$, choosing σ_i such that

$$\alpha \equiv \lambda^m(i+1) \pmod{P^{i+1}},$$

that is, such that

$$\alpha \equiv \big(\lambda(i) + \delta_i \sigma_i\big)^m \equiv \lambda^m(i) + m \delta_i \lambda^{m-1}(i) \sigma_i \pmod{P^{i+1}}.$$

(As $P^{i-c} \| \delta_i$, succeeding terms in the binomial expansion are divisible by at least P^{2i-2c}, and since $i \geqslant 2c+1$, $2i-2c \geqslant i+1$.) Thus we choose σ_i such that

$$\alpha - \lambda^m(i) \equiv \varrho_i \big(\alpha - \lambda^m(i)\big) \lambda^{m-1}(i) \sigma_i \pmod{P^{i+1}},$$

a congruence which will hold if

$$\varrho_i \lambda^{m-1}(i) \sigma_i \equiv 1 \pmod{P}.$$

Since $P \nmid \varrho_i \lambda^{m-1}(i)$, σ_i can be chosen as required. Furthermore, $(\lambda(i+1), P) = 1$.

We have as a consequence to this theorem the fact that if $(v, P) = 1$, then v belongs to $J_m(P)$ if and only if (*) has an integral solution in K for $i = 2c+1$ and some integers r and s, $s \geqslant r \geqslant 0$, $s > 0$. Theorem 5 will actually be applied only when $c = 0$, that is, when $P \nmid m$.

THEOREM 6. *Let $m! = P_1^{i_1} P_2^{i_2} \ldots P_j^{i_j}$, where $P_a \neq P_b$ if $a \neq b$. Then*

$$J_m = \bigcap_{P \mid m!} J_m(P) = \bigcap_{P \mid m!} J'_m(P);$$

and if

$$v \equiv \lambda_1^m(i) + \ldots + \lambda_r^m(i) - \lambda_{r+1}^m(i) - \ldots - \lambda_s^m(i) \pmod{P_i^{i_i}}$$

has an integral solution $\lambda_1(i), \ldots, \lambda_r(i), \ldots, \lambda_s(i)$ in K for $i = 1, 2, \ldots, j$ and every v in J_m, then $\Delta(m, m!) \leqslant s$.

Proof. Obviously $J_m \subseteq \bigcap_{P \mid m!} J_m(P) \subseteq \bigcap_{P \mid m!} J'_m(P)$. On the other hand, suppose v belongs to $\bigcap_{P \mid m!} J'_m(P)$. Then there exist integral solutions $\mu_1(i), \ldots, \mu_{s_i}(i)$ in K of

$$v \equiv \mu_1^m(i) + \ldots + \mu_{r_i}^m(i) - \mu_{r_i+1}^m(i) - \ldots - \mu_{s_i}^m(i) \pmod{P_i^{i_i}}$$

for $i = 1, 2, \ldots, j$. Let $r = \max_i r_i$, $s = \max_i (s_i - r_i) + r$. Thus there exist solutions $\lambda_1(i), \ldots, \lambda_s(i)$ of $v \equiv \lambda_1^m + \ldots + \lambda_r^m - \lambda_{r+1}^m - \ldots - \lambda_s^m \pmod{P_i^{i_i}}$. We can solve

$$\lambda_k \equiv \lambda_k(i) \pmod{P_i^{i_i}}$$

for $k = 1, 2, \ldots, r, r+1, \ldots, s$; $i = 1, 2, \ldots, j$.

Then

$$v \equiv \lambda_1^m + \ldots + \lambda_r^m - \lambda_{r+1}^m - \ldots - \lambda_s^m \pmod{m!}.$$

Since $(m!)J$ is part of J_m, v belongs to J_m. Therefore $\bigcap_{P \mid m!} J'_m(P) \subseteq J_m$, and we have proved the first part of the theorem. The second part follows immediately, if we apply again the well-known theorem on the simultaneous solution of congruences.

Theorems 5 and 6 together show a method for calculating an upper bound of $v(m; K)$. If $P_i^{i_i} \| m!$, we determine numbers r_i and s_i such that every v in J_m is congruent to a sum $\lambda_1^m + \ldots + \lambda_{r_i}^m - \lambda_{r_i+1}^m - \ldots - \lambda_{s_i}^m$ modulo $P_i^{i_i}$. If $t_i \leqslant 2c_i+1$, where $P_i^{c_i} \| m$, we examine the ring J_m modulo $P_i^{i_i}$. If $t_i > 2c_i+1$, we consider J_m modulo $P_i^{2c_i+1}$. Instead of limiting ourselves to primitive solutions, we usually find u and v such that for any v in J_m

$$v \equiv \lambda_1^m + \ldots + \lambda_u^m - \lambda_{u+1}^m - \ldots - \lambda_v^m \pmod{P_i^{2c_i+1}}$$

has some integral solution $\lambda_1, \lambda_2, \ldots, \lambda_v$ in K. If $(v, P_i) = 1$, this solution will be primitive; if $P_i \mid v$, we may be able to describe particular primitive solutions of the congruence for every such v, and we can then take $r_i = u$, $s_i = v$. But if $P_i \mid v$ and a primitive solution is not at hand,

we know that there is a solution $\lambda_1, \ldots, \lambda_v$ for $v-1$ in place of v, i.e., which satisfies the congruence

$$v \equiv 1+\lambda_1^m+\ldots+\lambda_u^m-\lambda_{u+1}^m-\ldots-\lambda_v^m \pmod{P_i^{2c_i+1}}.$$

By theorem 5 we conclude that we can take $r_i = u+1$, $s_i = v$. By Theorem 6 finally

$$\Delta(m, m!) \leqslant \max_i r_i + \max_i (s_i - r_i).$$

THEOREM 7. *If P is a prime ideal dividing the rational prime p, $P \nmid m$, $p < m$, and $s \geqslant m$, then the congruence*

$$v \equiv \lambda_1^m+\lambda_2^m+\ldots+\lambda_s^m \pmod{P}$$

has a primitive integral solution $\lambda_1, \lambda_2, \ldots, \lambda_s$ in K for every v in J_m. If $p > m$ the conclusion holds when $s \geqslant m+1$.

Proof. The theorem is an application of a theorem by Tornheim ([13]); however, we shall prove it for our case in a slightly different manner which will more easily yield Theorem 8. Let $NP = p^f$. Let the multiplicative group G of non-zero elements of the residue class field modulo P, which is cyclic, be represented by $\zeta, \zeta^2, \ldots, \zeta^{p^f-1} \equiv 1 \pmod{P}$. The subgroup M of G consisting of m-th powers has index $(p^f-1, m) = t$ and may be represented by $\zeta^t, \zeta^{2t}, \ldots, \zeta^{p^f-1}$. If on forming all possible sums of two elements of M we do not obtain a residue class $\zeta^i \bmod P$ where $i \not\equiv 0 \pmod{t}$, then one m-th power suffices to represent all elements of J_m modulo P. If this is not the case, then at least an entire coset of M in G has its elements expressible as the sum of two elements of M. Such a coset determined by ζ^i contains every ζ^j where $j \equiv i \pmod{t}$. For if

$$\zeta^i \equiv \zeta^{rt}+\zeta^{ut} \pmod{P}$$

then

$$\zeta^j \equiv \zeta^{i+at} \equiv (\zeta^{rt}+\zeta^{ut})\zeta^{at} \equiv \zeta^{(r+a)t}+\zeta^{(u+a)t} \pmod{P}.$$

Continuing in this way we determine those cosets for which three, four, ..., m-th powers are needed by taking all possible sums of three, four, ..., m-th powers. If no new coset is obtained by sums of r m-th powers, no larger number of powers will produce one, because any sum of r m-th powers would be congruent modulo P to a sum of fewer than r m-th powers. Therefore the maximum number of summands needed $\leqslant$ number of cosets of M in G, which is $t \leqslant m$. So we have primitive solutions $\lambda_1, \lambda_2, \ldots, \lambda_s$ when $P \nmid v$ and $s \geqslant m$. However, when $v \equiv 0 \pmod{P}$ and $p < m$, $v \equiv 1^m+1^m+\ldots+1^m \equiv p \pmod{P}$, and this is a primitive solution of the required form. Finally, when $v \equiv 0 \pmod{P}$ and $p > m$, then by the first part of the theorem there is a primitive solution of the congruence with $v-1$ in place of v when $s \geqslant m$. Therefore the congruence as given may be solved primitively when $s \geqslant m+1$.

THEOREM 8. *If P is a prime ideal dividing the rational prime p, $P \nmid q$, and the multiplicative order $\operatorname{ord}_q p$ of p modulo q is j, then the congruence $v \equiv \lambda_1^q+\lambda_2^q+\ldots+\lambda_s^q \pmod{P}$ has a primitive integral solution $\lambda_1, \lambda_2, \ldots, \lambda_s$ in K for every v in J_m, provided $s \geqslant (q-1)/j+1$.*

Proof. The index of M in G is either 1 or q. If it is 1, the conclusion follows. We shall assume that the index is q and that $\zeta, \zeta^2, \ldots, \zeta^{p^f-1}$ represent the coprime residue classes modulo P. If the minimum number of q-th powers needed modulo P to express the elements of a coset of M is equal to or greater than 2, then it is the same for j cosets of M in G. For assume that

$$\zeta^l \equiv \lambda_1^q+\lambda_2^q+\ldots+\lambda_s^q \pmod{P}, \qquad l \not\equiv 0 \pmod{q}.$$

Then

$$\zeta^{lp} \equiv (\lambda_1^q+\ldots+\lambda_s^q)^p \equiv (\lambda_1^p)^q+\ldots+(\lambda_s^p)^q \pmod{P}$$

since $p \left| \binom{p}{j} \right.$ for $j = 1, 2, \ldots, p-1$.

Therefore each of the cosets of M in G represented by

$$\{\zeta^i \mid i \equiv lp \pmod{q}\}, \{\zeta^i \mid i \equiv lp^2 \pmod{q}\}, \ldots, \{\zeta^i \mid i \equiv lp^j \equiv l \pmod{q}\},$$

consists of elements that are expressible as sums of s q-th powers modulo P. From the proof of Theorem 7 we know that if any coset needs a minimum of $s \geqslant 3$ powers to express its elements in the desired form, then there must be a coset requiring $s-1$ powers. Therefore the maximum number of summands from M needed to express the elements in any coset cannot exceed $(q-1)/j+1$.

If $P \mid v$, we have this primitive solution:

$$v \equiv 1^q+(-1)^q \pmod{P},$$

and as $(q-1)/j+1 \geqslant 2$, we have succeeded in demonstrating the existence of primitive solutions in every case and proved the theorem.

It is now almost immediate that we have the main theorem of this section.

THEOREM 9. *If q is an odd prime, then $v(q; K) \leqslant 2^{q-1}+1+(q-1)/\min_{p<q}(\operatorname{ord}_q p)$, where $\operatorname{ord}_q p$ denotes the multiplicative order of the prime number p modulo q.*

If $q \geqslant 7$, $v(q; K) \leqslant 2^{q-1}+1+(q-1)/3$.

Proof. We have

$$-\lambda^q = (-\lambda)^q, \quad (\lambda_1+\lambda_2)^q \equiv \lambda_1^q+\lambda_2^q \pmod q$$

because $q \left| \binom{q}{i} \right.$ for $i = 1, 2, \ldots, q-1$. Therefore every element of J_q is congruent to a q-th power modulo q. For other primes dividing $q!$ we apply Theorem 8. Then the first inequality above follows from the basic identity and Theorems 5 and 6.

To derive the second inequality we calculate the lower bound 3 for $\operatorname{ord}_q p$ when $p < q$. If the order of some such p is 2, then $p^2 \equiv 1 \pmod q$, that is, $q|(p+1)(p-1)$, which is possible only when $q = 3$, $p = 2$, an occurrence precluded by the hypothesis; and we have the theorem.

We proceed now to calculate upper bounds for $v(3; K)$ and $v(5; K)$.

THEOREM 10. *$v(3; K) \leqslant 5$ unless 2 has a prime ideal factor of even degree $\geqslant 4$ or more than one ramified factor. In every instance $v(3; K) \leqslant 6$. If 3 has an unramified prime factor of first degree, then $v(3; K) \geqslant 4$.*

Proof. $v(3; K) \leqslant 6$ by Theorem 9. Now assume that 2 has only prime ideal factors of odd degree or of degree 2, at most one of which is ramified. Let $P|2$, $NP = 2^f$, f being odd. The multiplicative group G of the residue class field modulo P is generated by the residue class of an integer ζ of multiplicative order 2^f-1 modulo P. The subgroup M has index 1 in G since 2^f-1 is not divisible by 3. Therefore every integer is congruent to an integral cube modulo P.

If $P|2$ and $NP = 2^2$, the cube of any integer relatively prime to P is congruent to 1 modulo P, since 3 is the order of G. Also $1^3 \pm 1^3 \equiv 0^3 \pmod P$. Again every element of J_3 is congruent to an integral cube modulo P.

If no factor of 2 is ramified, we have therefore that if ν is in J_3, then ν is congruent to a cube modulo 2. As in the case of general q,

$$\pm\lambda_1^3 \pm \lambda_2^3 \equiv (\pm\lambda_1 \pm \lambda_2)^3 \pmod 3,$$

which implies that ν is congruent to a cube modulo 3. Therefore ν is congruent to a cube modulo 6, and with the identity $6x = (x+1)^3 + (x-1)^3 - 2x^3$ we get $v(3; K) \leqslant 5$.

Now assume 2 has one ramified prime ideal factor P, where $P^t || 2$. If ν is in J_3, we know as before that $\nu \equiv \lambda^3 \pmod P$ for some λ. If $(\nu, P) = 1$, then, by Theorem 5, $\nu \equiv \lambda'^3 \pmod{P^t}$ for some appropriate integer λ'. As ν is congruent to a cube modulo 3 and ν is also congruent to a cube modulo Q for any prime ideal Q dividing 2 and different from P, ν is congruent to a cube modulo 6. Using the identity above, ν can be expressed with not more than five integral cubes. But if $P|\nu$, then $(\nu-3, P) = 1$ and $\nu-3$ is congruent to an integral cube modulo 6, i.e., $\nu-3 = 6\xi+\lambda^3$. The identity

$$6x+3 = x^3-(x-4)^3+(2x-5)^3-(2x-4)^3$$

shows that four integral cubes suffice to express integers of the form $6\xi+3$, so that five will do for ν. Thus the first part of the theorem is proved. We have in particular that $v(3; K) \leqslant 5$ if K is quadratic or cubic.

The lower bound 4 for $v(3; K)$ if $P||3$ for some P with $NP = 3$ is obtained by considering the residue classes modulo P^2. The multiplicative group G of coprime residue classes modulo P^2 has $NP^2-NP = 6$ elements and is therefore cyclic. The only cubes in G may be represented by ± 1. Since P is not ramified in 3, we see that the integers $0, 1, \ldots, 7, 8$ represent the full residue system modulo P^2 and that any integers congruent to 4 or 5 modulo P^2 cannot be expressed by fewer than 4 cubes. This completes the theorem.

THEOREM 11. *$v(5; K) \leqslant 10$ for any K.*

Proof. We use the identity

$$(x+3)^5-2(x+2)^5+x^5+(x-1)^5-2(x-3)^5+(x-4)^5 = 720x-360.$$

The only primes dividing $6! = 720$ are 2, 3, and 5. Now 2 and 3 are both of multiplicative order 4 modulo 5, and if ν is in J_5, then $\nu \equiv \lambda^5 \pmod 5$ for some integer λ. By Theorem 8, $\nu \equiv \lambda_1^5+\lambda_2^5 \pmod P$ has a primitive integral solution λ_1, λ_2 for every P dividing 2 or 3 (we take $\nu \equiv 1^5 + (-1)^5 \pmod P$ if $(\nu, P) \neq 1$). Therefore by Theorems 5 and 6 every residue class modulo 720 is representable by a sum of two fifth-power residues. The identity yields eight fifth-powers for every element in the residue class represented by 360. Therefore $v(5; K) \leqslant 10$.

IV. Upper bounds for $v(m; K)$ when m is arbitrary. Turning now to the case of arbitrary m, we shall find an upper bound to $v(m; K)$ which is not a function of m alone but depends also on the degree n of the field K. The method is shifted from the discussion of congruences modulo powers of prime ideals to congruences modulo powers of the principal ideals generated by rational primes. The main result is applied to the singular series in the generalization of Waring's problem to algebraic number fields. Brief mention will be given to some instances in which a lower bound for $v(m; K)$ is easily found.

LEMMA. *If p is a rational prime such that $p^f || m$, i is a positive integer and $i > 1$ when $p = 2$, then all coefficients of the polynomial*

$$(x+p^i y)^m - mp^i x^{m-1} y - x^m$$

are divisible by p^{i+f+1}.

Proof. The terms of the polynomial are

$$\binom{m}{k} x^{m-k}(p^i y)^k, \qquad k = 2, 3, \ldots, m.$$

The order to which p divides $k!$ is

$$\sum_{j=1}^{\infty}\left[\frac{k}{p^j}\right] < \sum_{j=1}^{\infty}\frac{k}{p^j} = \frac{k}{p-1}\begin{cases}\leqslant \frac{k}{2} & \text{when } p \text{ is odd},\\ \leqslant k & \text{when } p = 2.\end{cases}$$

Therefore, when p is odd, the order to which p divides $\binom{m}{k}p^{ik}$ is greater than

$$f+ki-\frac{k}{2} \geqslant f+\frac{k}{2}\,i \geqslant f+i.$$

And when $p = 2$, the order to which 2 divides $\binom{m}{k}2^{ik}$ is greater than

$$f+ki-k \geqslant f+2(i-1) \geqslant f+i.$$

For the remainder of this section, whenever $p^f \| m$ we shall define

$$w = \begin{cases} f+1 & \text{if } p \text{ is an odd prime},\\ f+2 & \text{if } p = 2.\end{cases}$$

Then we have

THEOREM 12. *If $p^f \| m$, and a is relatively prime to p and congruent to an integral m-th power modulo p^w, then a is congruent to an integral m-th power modulo any power of p.*

Proof. Suppose $\beta^m \equiv a \pmod{p^j}$, where $j \geqslant f+1$ if p is odd, $j \geqslant f+2$ if p is even. By the lemma,

$$(\beta + p^{j-f}\gamma)^m \equiv a \pmod{p^{j+1}},$$

provided

$$\beta^m + \frac{m}{p^f}\beta^{m-1}p^j\gamma \equiv a \pmod{p^{j+1}}.$$

The latter congruence will hold if

$$\frac{m}{p^f}\beta^{m-1}\gamma \equiv \frac{a-\beta^m}{p^j} \pmod{p},$$

a congruence which is soluble for γ because $(m\beta^{m-1}/p^f, p) = 1$.

THEOREM 13. *If p is any prime and u is any positive integer, every element in J_m is congruent modulo p^u to a sum of $n(4m-1)+1 = s(n, m)$ integral m-th powers, at least one of which is relatively prime to p. If m is odd, this is true also for $s(n, m) = n(2m-1)+1$.*

Proof. Let $p^f \| m$. By Theorem 12, the theorem will be proved if we can show that every integer in J_m is congruent to a sum of not more than $n(4m-1)+1$ integral m-th powers modulo p^w, at least one of which is relatively prime to p. If p is odd, it will be shown that actually only $n(2m-1)+1$ such summands suffice.

The numbers of J_m form modulo p^w an additive abelian group of order s, where $s \mid p^{nw}$. Let $\eta_1^m, \eta_2^m, \ldots, \eta_d^m$ be a minimal set of m-th powers generating this group. Let the additive order of η_1^m be $q_1 = p^{j_1}$ and the index of the subgroup

$$\{\eta_1^m, \eta_2^m, \ldots, \eta_k^m\} \quad \text{in the subgroup} \quad \{\eta_1^m, \eta_2^m, \ldots, \eta_{k+1}^m\}$$

be $q_{k+1} = p^{j_{k+1}}$ for $k = 1, 2, \ldots, d-1$. Then $j_k \geqslant 1$ for every k, since we have selected a minimal set, and the linear forms

$$x_1\eta_1^m + x_2\eta_2^m + \ldots + x_d\eta_d^m \qquad (x_k = 0, 1, \ldots, q_k-1;\ k = 1, 2, \ldots, d)$$

represent all numbers of J_m modulo p^w. Define

$$m_p = 2m-1 \quad \text{if } p \text{ is odd},$$
$$m_2 = 4m-1.$$

It is known ([5], pp. 19-20) that every positive rational integer is congruent to a sum

$$y_1^m + y_2^m + \ldots + y_{m_p}^m \pmod{p^i} \qquad (i = 1, 2, \ldots)$$

for rational integers $y_1, y_2, \ldots, y_{m_p}$. Therefore every element of J_m is congruent to a sum of not more than

$$S_p = \sum_{k=1}^{d} \min(q_k-1, m_p)$$

integral m-th powers modulo p^w. The upper bound for S_p established in the following lemma will then give the result of the theorem. (We need the extra summand in order to guarantee that at least one of the m-th powers is relatively prime to p.)

LEMMA. *If $p^f \| m$, $q_k = p^{j_k}$ $(k = 1, 2, \ldots, d)$, and $q_1 q_2 \ldots q_d \leqslant p^{nw}$, then*

$$\max S_p = \max \sum_{k=1}^{d} \min(q_k-1, m_p) \leqslant nm_p,$$

the maximum being taken over the sets of positive integers $d, j_1, j_2, \ldots, j_d$ *satisfying* $\sum_{k=1}^{d} j_k \leqslant nw$.

Proof. We need consider only the case $\sum_{k=1}^{d} j_k = nw$, that is, $q_1 q_2 \ldots q_d = p^{nw}$. Now suppose

$$q_i q_j = q' \quad \text{and} \quad q_i \leqslant p^{w-1},\ q_j \leqslant p^{w-1} \quad \text{for some } i,\ j \text{ with } 1 \leqslant i, j \leqslant d.$$

Then

$$\min(q_i - 1, m_p) + \min(q_j - 1, m_p) = q_i + q_j - 2,$$

since

$$p^{w-1} \begin{cases} \leqslant m & \text{if } p \text{ is odd,} \\ \leqslant 2m & \text{if } p \text{ is even.} \end{cases}$$

But

$$q_i + q_j - 2 \leqslant 2p^{w-1} - 2 < m_p$$

and

$$q_i + q_j - 2 < q_i q_j - 1 = q' - 1$$

since q_i and q_j are positive integers greater than 1.

Therefore

$$\min(q_i - 1, m_p) + \min(q_j - 1, m_p) < \min(q' - 1, m_p).$$

Thus S_p cannot be maximum as long as more than one q_k is equal to or less than p^{w-1}, and we may therefore assume

$$p^{w(d-1)+1} \leqslant p^{nw},$$

which implies $d \leqslant n$. Therefore the result follows.

Theorem 13 is an improvement of Lemma 3 of Siegel ([8]) and enables us to get a positive lower bound for the singular series in Waring's Problem for algebraic number fields when the number of summands exceeds $n(4m-1)$.

The following is the main result of this section.

Corollary. *If* n *is the degree of* K,

$$v(m; K) \leqslant 2^{m-1} + n(4m-1) + 1 \quad \text{if } m \text{ is even},$$

$$v(m; K) \leqslant 2^{m-1} + n(2m-1) + 1 \quad \text{if } m \text{ is odd}.$$

Let

$$r = \begin{cases} n(4m-1)+1 & \text{if } m \text{ is even,} \\ n(2m-1)+1 & \text{if } m \text{ is odd,} \end{cases}$$

and $m! = p_1^{u_1} p_2^{u_2} \ldots p_j^{u_j}$, where $p_1, \ldots, p_j$ are distinct primes. By theorem 13 any ν in J_m is congruent modulo $p_i^{u_i}$ to a sum of r integral m-th powers, at least one of which is relatively prime to P_i $(i = 1, 2, \ldots, j)$. Thus $\Delta(m, m!) \leqslant r$. Together with the basic identity this yields the corollary.

Theorem 14. *If* $2m+1$ *is a prime and* $2m+1$ *has at least one prime ideal factor* P *of first degree, then* $v(m; K) \geqslant m$.

Proof. The coprime residue class group modulo P is cyclic of order $2m$ and may be represented by $1, 2, \ldots, 2m$; the m-th powers modulo P are congruent to 0, 1 and -1. Integers congruent to m modulo P cannot be expressed with fewer than m m-th powers.

This theorem applies to the rational case, in particular.

V. Existence of algebraic number fields K for which $v(m; K) < v(m; R)$. We shall show now by an example that there exist algebraic number fields in which every element of J_m is expressible by fewer m-th powers than is the case in the rational number field. It is known that $9 \leqslant v(4; R) \leqslant 12$. But

Theorem 15. $v(4; R(\sqrt[4]{3})) \leqslant 8$.

Lemma. *If* $P^k \| 2$, *then the 4-th powers modulo* P^{3k} *may be represented by*

$$(\gamma_0 + \gamma_1 \pi + \ldots + \gamma_{k-1} \pi^{k-1})^4,$$

where π *is an integer exactly divisible by the prime ideal* P *and* γ_j *runs over a complete residue system modulo* P *for* $j = 0, 1, \ldots, k-1$.

Proof. The 4-th powers are representable modulo P^{3k} by

$$(\gamma_0 + \gamma_1 \pi + \ldots + \gamma_{3k-1} \pi^{3k-1})^4 \equiv (\gamma_0 + \gamma_1 \pi + \ldots + \gamma_i \pi^i)^4 \pmod{P^{3k}},$$

where $i \leqslant 3k-1$ and i may be determined as follows. The multinomial coefficients appearing in the expansion of the left-hand member of the congruence are

$$\frac{4!}{1!1!1!1!} \equiv 0 \pmod{P^{3k}}, \quad \frac{4!}{1!1!2!} \equiv 0 \pmod{P^{2k}},$$

$$\frac{4!}{3!1!} \equiv 0 \pmod{P^{2k}}, \quad \frac{4!}{2!2!} \equiv 0 \pmod{P^k}.$$

Therefore i can be taken as the largest integer $\leqslant 3k-1$ for which at least one of the following two statements is true:

$$\frac{4!}{3!1!} \pi^i \not\equiv 0 \pmod{P^{3k}}, \quad \frac{4!}{2!2!} \pi^{2i} \not\equiv 0 \pmod{P^{3k}}.$$

Thus i can be taken as the largest integer $\leqslant 3k-1$ for which

$$2k+i \leqslant 3k-1 \quad \text{or} \quad k+2i \leqslant 3k-1,$$

that is,

$$i \leqslant k-1 \quad \text{or} \quad i \leqslant (2k-1)/2 = k-\tfrac{1}{2}.$$

This implies that we may take $i = k-1$.

We return to the proof of Theorem 15. From the identity

$$4!x+36 = (x+3)^4-3(x+2)^4+3(x+1)^4-x^4,$$

we conclude that in $R(\sqrt[4]{3})$ every integer congruent to 12 modulo 24 can be decomposed into 4 integers of the form $\pm\lambda^4$ modulo 24. To prove our theorem, it will then only be necessary to show that all numbers of J_4 in $R(\sqrt[4]{3})$ are congruent modulo 24 to sums of four or fewer integers of the form $\pm\lambda^4$.

Now $3 = (\sqrt[4]{3})^4$, and so $(\sqrt[4]{3})$ is a prime ideal of first degree. Every integer in $R(\sqrt[4]{3})$ is congruent to 0, 1 or 2 modulo $(\sqrt[4]{3})$. Therefore every integer is congruent modulo $\sqrt[4]{3}$ to a sum of at most three integral 4-th powers, at least one of which is not divisible by $\sqrt[4]{3}$, and by Theorem 5 every integer is congruent to the sum of three 4-th powers modulo 3.

We shall prove that modulo 8 every element of J_4 is congruent to a sum of three integral 4-th powers plus a term $\pm\mu^4$. Now, since the minimal equation for $\sqrt[4]{3}+1$ is $x^4-4x^3+6x^2-4x-2 = 0$, we have that $(\sqrt[4]{3}+1)^4$ is two times a unit, so that we may apply the lemma with $k = 4$ and $\pi = \sqrt[4]{3}+1$. Thus the 4-th powers are congruent modulo 8 to

$$(\varepsilon_0+\varepsilon_1\pi+\varepsilon_2\pi^2+\varepsilon_3\pi^3)^4$$

where $\varepsilon_i = 0$ or 1 $(i = 0, 1, 2, 3)$. The 4-th powers are congruent modulo 8 to one of the following: 0, 1,

$$\begin{aligned}
\alpha &= 1+4\pi+6\pi^2+4\pi^3+\pi^4,\\
\beta &= 1+4\pi^2+6\pi^4+\pi^8,\\
\gamma &= 1+4\pi^3+6\pi^6,\\
\delta &= 1+4\pi+2\pi^2+7\pi^4+2\pi^6+\pi^8,\\
\varepsilon &= 1+4\pi+6\pi^2+\pi^4+2\pi^6,\\
\zeta &= 1+4\pi^2+4\pi^3+6\pi^4+2\pi^6+\pi^8,\\
\eta &= 1+4\pi+2\pi^2+4\pi^3+7\pi^4+\pi^8,\\
\vartheta &= \pi^4, \quad \iota = \pi^8, \quad \varkappa = \pi^4+\pi^8+6\pi^6.
\end{aligned}$$

Now a complete residue system modulo 8 is also obtained from the numbers $a_0+a_1\pi+a_2\pi^2+a_3\pi^3$, where a_i runs over $0, 1, 2, \ldots, 7$ $(i = 0, 1, 2, 3)$. For the total number of residues modulo 8 expressible in this way is $8^4 = 2^{12}$; and

$$a_0+a_1\pi+a_2\pi^2+a_3\pi^3 \equiv b_0+b_1\pi+b_2\pi^2+b_3\pi^3 \pmod 8$$

if and only if $a_i \equiv b_i \pmod 8$ $(i = 0, 1, 2, 3)$. This last follows from the fact that if $(a_i-b_i)\pi^i = c_i\pi^i$, then the non-zero terms in the expression

$$c_0+c_1\pi+c_2\pi^2+c_3\pi^3$$

are divisible by different powers of P.

Using the relation $\pi^4 = 4\pi^3-6\pi^2+4\pi+2$, we express the set of 4-th powers modulo 8 in the form $c_0+c_1\pi+c_2\pi^2+c_3\pi^3$ and get

$$0,\ 1,\ \alpha-3,\quad \beta-1,\quad \gamma-1+4\pi^2+4\pi^3,\quad \delta-3+4\pi^2+4\pi^3,$$

$$\varepsilon-3+4\pi^2+4\pi^3,\quad \zeta-1+4\pi^2+4\pi^3,\quad \eta-3,$$

$$\vartheta-2+4\pi+2\pi^2+4\pi^3,\quad \iota-4,\quad \varkappa-6+4\pi+6\pi^2+4\pi^3.$$

The additive group generated by this set modulo 8 consists of the residue classes represented by the numbers $a_0+a_1\pi+a_2\pi^2+a_3\pi^3$ with the possible values taken on by a_0, a_1, a_2, a_3 modulo 8 listed in the table below:

	a_0	a_1	a_2	a_3
(i)	arbitrary	0	0	0
(ii)	arbitrary	0	4	4
(iii)	arbitrary	4	2	4
(iv)	arbitrary	4	6	4
(v)	arbitrary	0	4	0
(vi)	arbitrary	4	6	0
(vii)	arbitrary	4	2	0
(viii)	arbitrary	0	0	4

At most two summands from $\{1, 3, 4\}$ express any rational integer modulo 8. Since γ falls under (ii), ϑ under (iii), $\varkappa$ under (iv), $\vartheta+\vartheta$ under (v), $\vartheta+\varepsilon$ under (vi), and $\varkappa+\zeta$ under (vii), any element of J_4 falling in one of the classifications (i)-(vii), is congruent modulo 8 to a sum of at most four 4-th powers of integers.

Classification (viii) is somewhat special. If $a_0 \neq 4$, then either

$$a_0+4\pi^3 \equiv 2\vartheta+\gamma+k(a_0) \pmod 8, \quad \text{where} \quad k(a_0) = 0, 1, 3 \text{ or } 4,$$

or

$$a_0+4\pi^3 \equiv 2\vartheta+\delta+k'(a_0)(\mathrm{mod}\,8), \quad \text{where} \quad k'(a_0) = 0, 1, 3 \text{ or } 4.$$

However, $4+4\pi^3$ is not congruent to a sum of four 4-th powers modulo 8, and we must allow one minus-sign:

$$4+4\pi^3 \equiv 2\vartheta+\gamma-1(\mathrm{mod}\,8).$$

In any case, if ν is in J_4 then there exist integers $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3, \mu_4$ in K such that

$$\nu \equiv \lambda_1^4+\lambda_2^4+\lambda_3^4(\mathrm{mod}\,3)$$

and

$$\nu \equiv \mu_1^4+\mu_2^4+\mu_3^4\pm\mu_4^4(\mathrm{mod}\,8).$$

Therefore there exist integers $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ with

$$\gamma_i \equiv \lambda_i(\mathrm{mod}\,3), \quad \gamma_i \equiv \mu_i(\mathrm{mod}\,8) \quad (i = 1, 2, 3),$$

$$\gamma_4 \equiv 0(\mathrm{mod}\,3), \quad \gamma_4 \equiv \mu_4(\mathrm{mod}\,8).$$

Then

$$\nu \equiv \gamma_1^4+\gamma_2^4+\gamma_3^4\pm\gamma_4^4(\mathrm{mod}\,24),$$

and we have the theorem.

VI. Relation of $v(m;K)$ to $g(m;K)$ in totally complex fields. We call a number ν of K *totally positive* if $\nu^{(j)} > 0$ $(j = 1, 2, \ldots, n_1)$. Let $g(m;K)$ be the least number s such that the equation $\nu = \lambda_1^m+\lambda_2^m+\ldots+\lambda_s^m$ has an integral solution $\lambda_1, \lambda_2, \ldots, \lambda_s$ in K, each λ_i being totally positive or zero $(i = 1, 2, \ldots, s)$, for every totally positive ν of J_m. Now when K is totally complex, every integer in K is totally positive. Given the existence of $v(m;K)$, which we have demonstrated in the preceding pages, the existence of $g(m;K)$ will therefore follow if we can show that -1 is the sum of a bounded number of m-th powers. We shall show this in this section and thus obtain an elementary proof of the existence of $g(m;K)$ for totally complex fields. In particular, if $\sqrt[m]{-1}$ is in K, $v(m;K) = g(m;K)$. In the example of the Gaussian integers with $m = 4$ we shall find actual upper bounds of $v\big(4; R(\sqrt{-1})\big)$ and $g\big(4; R(\sqrt{-1})\big)$.

THEOREM 16. *In totally complex fields K (that is, fields for which $n_1 = 0$) the existence of $v(m;K)$ implies the existence of $g(m;K)$.*

Proof. Let $\omega_1, \omega_2, \ldots, \omega_{2k}$ be an integral basis of K if $n = 2k$. The system of $2k$ linear equations in the $2k$ unknowns $x_1, \ldots, x_{2k}$

$$x_1 \mathrm{Re}\,\omega_1^{(1)}+\ldots+x_{2k}\mathrm{Re}\,\omega_{2k}^{(1)} = \cos\pi/m$$
$$x_1 \mathrm{Re}\,\omega_1^{(2)}+\ldots+x_{2k}\mathrm{Re}\,\omega_{2k}^{(2)} = \cos\pi/m$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$x_1 \mathrm{Re}\,\omega_1^{(k)}+\ldots+x_{2k}\mathrm{Re}\,\omega_{2k}^{(k)} = \cos\pi/m$$
$$x_1 \mathrm{Im}\,\omega_1^{(1)}+\ldots+x_{2k}\mathrm{Im}\,\omega_{2k}^{(1)} = \sin\pi/m$$
$$x_1 \mathrm{Im}\,\omega_1^{(2)}+\ldots+x_{2k}\mathrm{Im}\,\omega_{2k}^{(2)} = \sin\pi/m$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$x_1 \mathrm{Im}\,\omega_1^{(k)}+\ldots+x_{2k}\mathrm{Im}\,\omega_{2k}^{(k)} = \sin\pi/m$$

has a unique solution in real numbers $x_1, x_2, \ldots, x_{2k}$.

Let $T = 2k\max\limits_{i,j}|\omega_i^{(j)}|$ and choose $R > T\csc\pi/2m$. If we set

$$\Phi = x_1\omega_1+x_2\omega_2+\ldots+x_{2k}\omega_{2k},$$
$$\Phi^{(j)} = x_1\omega_1^{(j)}+x_2\omega_2^{(j)}+\ldots+x_{2k}\omega_{2k}^{(j)},$$

then

$$\Phi^{(j)} = e^{\frac{\pi\sqrt{-1}}{m}} \quad (j = 1, 2, \ldots, k),$$

$$\Phi^{(j)} = e^{\frac{-\pi\sqrt{-1}}{m}} \quad (j = k+1, k+2, \ldots, 2k).$$

The integer

$$\beta = [Rx_1]\omega_1+[Rx_2]\omega_2+\ldots+[Rx_{2k}]\omega_{2k}$$

satisfies the inequality

$$|R\Phi^{(j)}-\beta^{(j)}| < 2k\max_{i,j}|\omega_i^{(j)}| = T.$$

This implies

$$\frac{\pi}{m}-\mathrm{Arc\,sin}\frac{T}{R} < \arg\beta^{(j)} < \frac{\pi}{m}+\mathrm{Arc\,sin}\frac{T}{R} \quad (j = 1, 2, \ldots, k).$$

But $\mathrm{Arc\,sin}\,T/R < \pi/2m$ by our choice of T and thus

$$\frac{\pi}{2m} < \arg\beta^{(j)} < \frac{3\pi}{2m} \quad (j = 1, 2, \ldots, k).$$

Since the arguments of the first k conjugates of β lie in the open interval $(\pi/2m, 3\pi/2m)$ and the arguments of the remaining conjugates lie

in $(-\pi/2m, -3\pi/2m)$, the arguments of the conjugates of β^m have negative real part. Now β^m is an integer of K satisfying the equation

$$(x-\beta^{(1)m})(x-\overline{\beta^{(1)m}})(x-\beta^{(2)m})(x-\overline{\beta^{(2)m}})\dots(x-\beta^{(k)m})(x-\overline{\beta^{(k)m}})$$
$$= \prod_{i=1}^{k}\{x^2-(\beta^{(i)m}+\overline{\beta^{(i)m}})x+\beta^{(i)m}\overline{\beta^{(i)m}}\} = 0.$$

Each of these k quadratic factors has positive coefficients, whence the equation

$$x^{2k}+a_1x^{2k-1}+\dots+a_{2k} = 0$$

which is satisfied by β^m and its conjugates has positive integral coefficients $a_1, a_2, \dots, a_{2k}$. The equation

$$-a_{2k} = (\beta^{2k})^m+a_1(\beta^{2k-1})^m+\dots+a_{2k-1}\beta^m$$

expresses the negative integer $-a_{2k}$ as a sum of $1+\sum_{i=1}^{2k-1}a_i$ integral m-th powers. If $v(m;K) = s$, then every integer in J_m is expressible in the form $\pm\lambda_1^m\pm\lambda_2^m\pm\dots\pm\lambda_s^m$. Now

$$-1 = -a_{2k}+(a_{2k}-1)1^m,$$

implying that -1 is a sum of $\sum_{i=1}^{2k}a_i$ integral m-th powers and hence that every integer in J_m is expressible as a *sum* of not more than

$$s\sum_{i=1}^{2k}a_i \ m\text{-th powers.}$$

Therefore $g(m;K)$ exists.

The essence of the proof was the demonstration of the existence of some negative integer which was a sum of integral m-th powers. Such an integer is easy to find in the case of the Gaussian integers: $-1 = (\sqrt{-1})^2$, $-1 = (-1)^3$, $-4 = (1+\sqrt{-1})^4$, $(-1) = (-1)^5$, $-1 = (\sqrt{-1})^6$, $(-1) = (-1)^7$, $-1054 = (2+\sqrt{-1})^8+(2-\sqrt{-1})^8$, for example. In particular we have

THEOREM 17. $v(4;R(\sqrt{-1})) \leqslant 10$. $g(4;R(\sqrt{-1})) \leqslant 14$.

Proof. We have the identity

$$24x+36 = (x+3)^4+3(x+1)^4-3(x+2)^4-x^4.$$

Now

$$-4 = (1-\sqrt{-1})^4,$$

and so

$$24x+36 = (x+3)^4+(1-\sqrt{-1})^4(x+2)^4+(x+2)^4+3(x+1)^4-x^4.$$

To show that $v(4;R(\sqrt{-1})) \leqslant 10$, we must therefore show that every integer in J_4 is congruent to $\pm\lambda_1^4\pm\lambda_2^4\pm\lambda_3^4$ modulo 24 for some integers $\lambda_1, \lambda_2, \lambda_3$. Since the discriminant of $R(\sqrt{-1})$ is -4 and

$$\left(\frac{-4}{3}\right) = -1,$$

3 is a prime ideal of second degree. The only 4-th powers modulo 3 are 0, 1 and -1; they generate themselves under addition. Therefore every integer of J_4 is congruent to a 4-th power modulo 3.

Next we examine J_4 modulo 8. Clearly $2 = -\sqrt{-1}(1+\sqrt{-1})^2$. By the lemma to Theorem 15 the 4-th powers modulo 8 are representable by

$$(\varepsilon_0+\varepsilon_1\pi)^4 \qquad (\varepsilon_0, \varepsilon_1 = 0, 1)$$

with $\pi = 1-\sqrt{-1}$. Furthermore $\pi^2 = 2(\pi-1)$ and the expressions $a_0+a_1\pi$ represent all residue classes modulo 8 if we let a_0 and a_1 run over full rational residue systems modulo 8. The 4-th powers modulo 8 are represented by

$$0, 1, 4,$$
$$1+4\pi+6\pi^2+4\pi^3+\pi^4 \equiv 1 \pmod 8.$$

The ring generated by these consists of the rational integers modulo 8. At most three summands from the set $\{0, \pm1, 4\}$ express every rational integer modulo 8. Therefore three 4-th powers suffice modulo 24, giving $v(4;R(\sqrt{-1})) \leqslant 10$. Now

$$-x^4 = (1+\sqrt{-1})^4x^4+3x^4,$$

and from the identity we get $24x+36$ as a sum of ten 4-th powers. Four elements from the set $\{0, 1, 4\}$ express any number in J_4 modulo 8. We deduce $g(4;R(\sqrt{-1})) \leqslant 14$. This may be compared with the result of Niven ([6]) that $g(4;R(\sqrt{-1})) \leqslant 18$.

References

[1] R. G. Ayoub, *On the Waring-Siegel theorem*, Canadian J. Math. 5 (1953), pp. 439-450.

[2] W. H. J. Fuchs and E. M. Wright, *The "easier" Waring problem*, Quart. J. Math. (Oxford) 10 (1939), pp. 190-209.

[3] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, third edition, Oxford 1954.

[4] E. Hecke, *Vorlesungen ueber die Theorie der Algebraischen Zahlen*, Leipzig 1923.

[5] E. Landau, *Ueber einige neuere Fortschritte der Additiven Zahlentheorie*, Cambridge 1937.

[6] I. Niven, *Sums of 4-th powers of Gaussian integers*, Bull. Amer. Math. Soc. 47 (1941), pp. 923-926.

[7] L. G. Peck, *Diophantine equations in algebraic number fields*, Amer. J. Math. 71 (1949), pp. 387-402.

[8] C. L. Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math. 66 (1944), pp. 122-136.

[9] — *Additive Theorie der Zahlkörper. I*, Math. Ann. 87 (1922), pp. 1-35.

[10] — *Additive Theorie der Zahlkörper. II*, Math. Ann. 88 (1923), pp. 184-210.

[11] — *Sums of m-th powers of algebraic integers*, Annals of Math. (2) 46 (1945), pp. 313-339.

[12] T. Tatuzawa, *On the Waring problem in an algebraic number field*, J. Math. Soc. Japan 10 (1958), pp. 322-341.

[13] L. Tornheim, *Sums of n-th powers in fields of prime characteristic*, Duke Math. J. 4 (1938), pp. 359-362.

[14] E. M. Wright, *An easier Waring's problem*, Journal London Math. Soc. 9 (1934), pp. 267-272.

UNIVERSITY OF ILLINOIS

Reçu par la Rédaction le 21. 8. 1960

ACTA ARITHMETICA
VI (1961)

Remarques sur le travail de M. J. W. S. Cassels „On a diophantine equation"

par

W. Sierpiński (Warszawa)

Dans son travail *On a diophantine equation* qui a paru dans ce volume, p. 47-52, M. J. W. S. Cassels démontre le théorème suivant:

Théorème I. *Le système d'équations*

$$r+s+t = rst = 1 \tag{1}$$

n'a pas de solutions en nombres rationnels r, s, t.

It est à remarquer que la question de savoir s'il existe trois nombres rationnels dont la somme ainsi que le produit soient égaux à 1 a été posée en 1956 par M. Werner Mnich; voir Elemente der Mathematik XI (1956), p. 134, où A. Schinzel démontre aussi que pour tout nombre naturel donné $s > 3$ il existe une infinité de systèmes de s nombres rationnels $x_1, x_2, \ldots, x_s$, tels que

$$x_1+x_2+\ldots+x_s = x_1x_2\ldots x_s = 1. \tag{2}$$

Par exemple, pour $s = 4$, les nombres

$$x_1 = -\frac{1}{n^2-1}, \quad x_2 = \frac{n^2}{n^2-1}, \quad x_3 = \frac{1-n^2}{n}, \quad x_4 = \frac{n^2-1}{n},$$

où $n = 2, 3, 4, \ldots$, satisfont aux conditions (2).

L'équivalence des théorèmes I et II de M. Cassels est démontrée dans mon article *Sur quelques problèmes non résolus d'arithmétique* paru dans L'Enseignement Mathématique, tome V, fasc. 4 (1959), p. 221-222.

En 1957 dans le journal Matematyka paraissant à Varsovie, X, Nr. 1 (45), p. 55, W. Mnich a posé la question de savoir si l'équation

$$\frac{x}{y}+\frac{y}{z}+\frac{z}{x} = 1 \tag{3}$$

a des solutions en nombres entiers x, y, z.