THE FINITE GOLDBACH PROBLEM IN ALGEBRAIC NUMBER FIELDS

ECKFORD COHEN

1. **Introduction.** Let F be an algebraic number field of degree n over the rational field, and let A represent a proper ideal of F ($A \neq 0$ or 1). Denoting by $R(A)$ the ring of residue classes (mod A), we propose in this paper to investigate the representability of the elements of $R(A)$ as sums of primes in $R(A)$.

The present paper extends to algebraic number fields of arbitrary degree a problem considered previously in the case of the rational field. We state the main results proved in the rational case. For this purpose, suppose that m is a rational integer, $m > 1$, and that $R(m)$ is the ring of residue classes (mod m).

THEOREM 1a. *There exists an s such that every element of $R(m)$ is a sum of s primes of $R(m)$ if and only if m has at least two distinct prime factors. For such m, the minimum value M of s is given by $M=2$ if m is odd, by $M=3$ if m is even and has at least two distinct odd prime factors or if m is twice an odd prime power, and by $M=4$ if m is of the form $m=2^{\mu}p^{\lambda}$ where $\lambda \geqq 1$, $\mu > 1$, and p is an odd prime.*

THEOREM 2a. *Every number of $R(m)$ is representable as a sum of at most three primes in $R(m)$ if and only if m has at least two distinct prime factors. Every number of $R(m)$ is a sum of at most two primes in $R(m)$ if and only if m is odd with at least two distinct prime factors or m is even and is of the form $m=2^{\mu}p$, $\mu \geqq 1$, p an odd prime.*

The generalizations of Theorems 1a and 2a to algebraic number fields are furnished, respectively, by Theorems 1 and 2 of §3. A glance at the statements of these theorems will reveal entirely new features that prove the rational field to be quite special for the problem under consideration. The method of the paper, while in general paralleling that of [2], involves a new type of result, contained in Lemma 6, which makes it possible to employ the results for the rational case in deducing the more general theorems.

The final section is concerned with the *finite Goldbach property*, a term used in connection with fields whose residue class rings possess a property corresponding to the celebrated Goldbach hypothesis for

Presented to the Society, February 28, 1953 and December 29, 1954; received by the editors May 6, 1955.

ordinary integers. (For a precise definition see §4.) A criterion for such fields is established in Theorem 4, from which it follows that the rational field possesses the finite Goldbach property (Corollary 1).

2. **Notation, terminology, and preliminary lemmas.** The notation F, n, A, and $R(A)$ will have the same significance in the rest of the paper as in the Introduction. The usual notation $N(A)$ for the norm of an ideal A will also be used.

In our later discussion it will be necessary to distinguish between prime ideals of norm $=2$ and those of norm $\neq 2$. We shall say, therefore, that a prime ideal P is of *type* I if $N(P) > 2$ and of *type* II if $N(P) = 2$. Using this terminology, the canonical factorization of A will be written

$$A = P_1^{\lambda_1} \cdots P_h^{\lambda_h} Q_1^{\mu_1} \cdots Q_k^{\mu_k} \qquad (\lambda_i > 0,\ \mu_j > 0), \tag{2.1}$$

the P_i and Q_j denoting distinct prime ideals of types I and II, respectively $(l = h+k > 0)$.

We next choose ideals C_i, D_j, all prime to A, $1 \leqq i \leqq h$, $1 \leqq j \leqq k$, and such that $\alpha_i = P_i C_i$ and $\beta_j = Q_j D_j$ are principal. On the basis of this notation and [1, Lemma 2], one has the following result.

LEMMA 1. *Every element ρ of $R(A)$ may be represented in the form*

$$\rho = \alpha_1^{a_1} \cdots \alpha_h^{a_h} \beta_1^{b_1} \cdots \beta_k^{b_k} \xi, \qquad (\xi, A) = 1, \tag{2.2}$$

the exponents a_i and b_j being uniquely determined by the conditions $0 \leqq a_i \leqq \lambda_i$, $0 \leqq b_j \leqq \mu_j$.

From an ideal-theoretic point of view, the ring $R(A)$ is a finite (principal ideal) ring with distinct prime ideals generated by $\alpha_1, \cdots, \alpha_h, \beta_1, \cdots, \beta_k$. This fact may be restated as

LEMMA 2. *The primes of $R(A)$ are the elements of the form $\pi_i = \alpha_i \xi$, $\pi_j' = \beta_j \xi$, $(i = 1, \cdots, h; j = 1, \cdots, k, (\xi, A) = 1)$.*

We point out that there is no loss of generality in this paper in assuming ρ to have the representation

$$\rho = \zeta_u \tau_v \xi, \qquad \zeta_u = \prod_{i=1}^{u} \alpha_i^{d_i}, \qquad \tau_v = \prod_{j=1}^{v} \beta_j^{e_j} \qquad (\xi, A) = 1, \tag{2.3}$$

where $h \geqq u \geqq 0$, $k \geqq v \geqq 0$, $\lambda_i \geqq d_i > 0$, $u_j \geqq e_j > 0$. We shall say that ρ is a unit of $R(A)$ if $(\rho, A) = 1$, and is *composite* in case it is neither a unit nor a prime. The symbol ξ will at all times be used to indicate a unit. In addition, A will be termed *absolutely even* in case $k > 0$ (2.1).

Vacuous products and sums will be denoted as usual by 1 and 0, respectively.

By the preceding discussion, the following lemma is evident.

Lemma 3. *An element ρ is a sum of s primes in $R(A)$ if and only if there exist elements $\gamma_1, \cdots, \gamma_s$ from the set (α_i, β_j), repetitions permitted, such that the congruence*

$$(2.4) \qquad \rho \equiv \gamma_1\xi_1 + \cdots + \gamma_s\xi_s$$

has a solution (mod A) *in ξ_i prime to A.*

If such a solution of (2.4) exists, then the congruence will be termed *solvable* (mod A). If further we denote the number of solutions of (2.4) to the modulus B by $N_s(\rho, B)$, then the factorability of this function (mod B) leads to the following result.

Lemma 4. *The congruence* (2.4) *is solvable* (mod A) *if and only if it is solvable* (mod $P_i^{\lambda_i}$) *and* (mod $Q_j^{\mu_j}$), $h \geqq i \geqq 1$, $k \geqq j \geqq 1$.

Thus, the problem of representing ρ as a sum of primes in $R(A)$ reduces to the question of the solvability of (2.4) to the modulus P^λ, where P^λ ranges over the maximal prime-power divisors of A. In this connection, we have the following result, proved in [1, §4, Corollary 2];

Suppose P to be of norm $N(P) = p^f$, p a rational prime, and suppose further that $(\gamma_i, P) = 1$ if $t \geqq i$ $(s \geqq t > 0)$, $(\gamma_i, P) \neq 1$ if $i > t$. Then

$$(2.5) \qquad N_s(\rho, P^\lambda) = p^{f(\lambda s - s - \lambda)}(p^f - 1)^{s-t}\{(p^f - 1)^t + q(\rho)\,\epsilon(t)\},$$

where $q(\rho) = -1$ or $p^f - 1$ according as $p \not\equiv or \equiv 0$ (mod P), *and $\epsilon(t) = 1$ or -1 according as t is even or odd.*

Therefore, one may deduce

Lemma 5. *Under the conditions of the preceding result, $N_s(\rho, P^\lambda) = 0$ if and only if one of the following holds:*

$$(2.6) \qquad \begin{array}{lll} P \textit{ is of type } \mathrm{I}, & \rho \equiv 0 \pmod{P}, & t = 1; \\ P \textit{ is of type } \mathrm{II}, & \rho \equiv 0 \pmod{P}, & t \textit{ odd}; \\ P \textit{ is of type } \mathrm{II}, & \rho \not\equiv 0 \pmod{P}, & t \textit{ even}. \end{array}$$

The following observation is useful in the proofs: If $\lambda > 0$ and $\gamma \equiv 0 (\text{mod } P)$, $\gamma \not\equiv 0 (\text{mod } P^2)$, then the congruence $\gamma\rho' \equiv \gamma\xi_1 + \cdots + \gamma\xi_s (\text{mod } P^\lambda)$ is solvable, if and only if $\rho' \equiv \xi_1 + \cdots + \xi_s (\text{mod } P^{\lambda-1})$ is solvable.

3. **Sums of primes in** $R(A)$. We shall refer to the quantities h, k,

λ_i, μ_j, u, v, d_i, e_j (2.3), as the *integral parts* of ρ in $R(A)$. Suppose now that A' is a proper ideal of an algebraic number field F' of (arbitrary) degree n' relative to the rational field. On the basis of Lemmas 3 and 5, we are led to

LEMMA 6. *If the corresponding integral parts of ρ in $R(A)$ and ρ' in $R(A')$ are equal, then ρ' is a sum of s primes in $R(A')$ if and only if ρ is a sum of s primes in $R(A)$.*

This lemma makes it possible to use the results proved in the rational case in treating algebraic number fields of degree >1. In particular, it is only necessary to consider values of $k\geqq 2$, because the cases $k=0$ and 1 have already been treated in the rational case.

THEOREM 1. *There exists an $s\geqq 1$ such that all elements of $R(A)$ are expressible as sums of s primes in $R(A)$ if and only if $l>1$, $h>0$. For such ideals A, the minimum value M of s is given by $M=2$ if $k=0$ and $h\geqq 2$; by $M=3$ if* (i) *$k=1$ and $h\geqq 2$, if* (ii) *$h=k=\mu_1=1$, or if* (iii) *$k=2$ and $h\geqq 1$; by $M=4$ if $h=k=1$, and $\mu_1>1$; and by $M=k$ if $k\geqq 3$ and $h\geqq 1$.*

(*Note.* In the following proof the quantities γ_c will be used as in Lemma 3 to denote elements chosen from among the α_i and β_j.)

PROOF. By Theorem 1a and the remarks following Lemma 6, we may consider the theorem proved in case $k=0$ or 1. In the remainder of the proof we shall therefore suppose that $k\geqq 2$.

If $h=0$ and $s=2S$, then consider the congruence,

$$\rho \equiv \gamma_1\xi_1 + \cdots + \gamma_{2S}\xi_{2S} \qquad (S > 0). \tag{3.1}$$

In case $\rho=\tau_{k-1}\xi$, β_k must appear among the γ's an odd number of times if (3.1) is to be solvable (mod $Q_k^{\mu_k}$), while each β_j $(j<k)$ must appear an even number of times, or not at all, to insure solvability (mod $Q_j^{\mu_j}$), (Lemma 5). This is impossible; therefore, by Lemmas 3 and 4, $\tau_{k-1}\xi$ is not a sum of an even number of primes in $R(A)$. In a similar fashion, one may observe that the congruence

$$\rho \equiv \gamma_1\xi_1 + \cdots + \gamma_{2S+1}\xi_{2S+1} \qquad (S \geqq 0) \tag{3.2}$$

cannot be solvable (mod A) if $\rho=\tau_2\xi$. Therefore $\tau_2\xi$ cannot be represented as a sum of an odd number of primes in $R(A)$, and the assertion regarding $h=0$ is proved.

In what remains we may suppose $h\geqq 1$. Placing $k=2$, the congruence

$$\zeta_h\beta_1^{e_1}\xi \equiv \gamma_1\xi_1 + \gamma_2\xi_2 \pmod{A} \tag{3.3}$$

cannot be solvable, because β_2 must appear exactly once as a coefficient on the right, with the result that neither β_1 nor the α_i can appear at all (Lemmas 4 and 5). Thus $M \neq 2$ in this case. The value $M=3$ will suffice in all cases, however, since the following congruences are all solvable (Lemmas 3, 4 and 5).

$$
\begin{aligned}
\zeta_u \xi &\equiv \alpha_1\xi_1 + \beta_1\xi_2 + \beta_1\xi_3 \pmod{A},\\
\zeta_u \beta_1^{e_1} \xi &\equiv \beta_1\xi_1 + \beta_2\xi_2 + \beta_2\xi_3 \pmod{A},\\
\zeta_u \beta_1^{e_1}\beta_2^{e_2} \xi &\equiv \alpha_1\xi_1 + \beta_1\xi_2 + \beta_2\xi_3 \pmod{A}.
\end{aligned}
\tag{3.4}
$$

Using the same type of argument as above, we note that if $s<k$, the congruences

$$\xi \equiv \gamma_1\xi_1 + \cdots + \gamma_s\xi_s \pmod{A}, \qquad s \text{ even}, \tag{3.5}$$

$$\zeta_k\xi \equiv \gamma_1\xi_1 + \cdots + \gamma_s\xi_s \pmod{A}, \qquad s \text{ odd}, \tag{3.6}$$

cannot be solvable. Hence for all A for which M exists, $M \geqq k$.

To complete the proof, one must show that every element of $R(A)$ is a sum of k primes when $k \geqq 3$ and $h \geqq 1$. If $s=k=2S\geqq 4$, then as above, (3.1) is solvable (mod A) for the following values of ρ and γ_i $(i=1, \cdots, s)$:

(1) $\rho = \zeta_u\tau_v\xi, \quad \gamma_i = \beta_{v+i} \quad (i = 1, \cdots, k-v;\ 0 \leqq v < k-1),$
$\gamma_i = \alpha_1 \quad (i > k-v);$

(2) $\rho = \zeta_u\tau_{k-1}\xi, \quad \gamma_1 = \gamma_2 = \gamma_3 = \beta_k, \quad \gamma_i = \alpha_1 \quad (i > 3);$

(3) $\rho = \zeta_u\tau_k\xi, \quad \gamma_1 = \gamma_2 = \beta_1, \quad \gamma_i = \alpha_1 \quad (i > 2).$

If $s=k=2S+1\geqq 3$; then (3.2) is solvable (mod A) in these cases:

(1) $\rho = \zeta_u\xi, \quad \gamma_1 = \alpha_1, \quad \gamma_i = \beta_1 \quad (i > 1);$

(2) $\rho = \zeta_u\tau_1\xi, \quad \gamma_1 = \beta_1, \quad \gamma_i = \beta_2 \quad (i > 1);$

(3) $\rho = \zeta_u\tau_v\xi, \quad \gamma_i = \beta_i \quad (i \leqq v \leqq k), \quad \gamma_i = \alpha_1 \quad (i > v > 1).$

Application of Lemma 3 proves the theorem.

The generalization of Theorem 2a to algebraic number fields is contained in

THEOREM 2. *There exists an H such that every element of $R(A)$ is a sum of at most H primes in $R(A)$ if and only if A is neither a prime-power ideal $(l=1)$ nor is of the form $A=Q_1^{\mu_1} \cdots Q_{2t+1}^{\mu_{2t+1}}$ $(h=0,$ k odd). For all other proper ideals A, the number H may be chosen to be $H=H'$, where $H'=2$ if $k=0$; $H'=3$ if $h\geqq 1$ and $k=1$, 2, or 3; $H'=4$ in case* (i) *$h\geqq 1$ and $k=4$, 5, or 6, and in case* (ii) *$h=0$, $k=2$; $H'=j+1$ if $h\geqq 1$, $k=2j+1\geqq 7$; $H'=j$ if $h\geqq 1$, $k=2j\geqq 8$; and $H'=2j$ if $h=0$,*

$k=2j\geqq 4$. *The minimum value* θ *of* H *is given by* $\theta=H'$ *with these exceptions*: $\theta=2$ *in case* (i) $h=k=\lambda_1=1$, *and in case* (ii) $h=0$, $k=2$, $\mu_1=\mu_2=1$; $\theta=3$ *in case* (i) $k=2$, $h=0$, *and either* $\mu_1=1$, $\mu_2\neq 1$ *or* $\mu_1\neq 1$, $\mu_2=1$, *and in case* (ii) $k=4$, $h\geqq 1$, *and either* $h\neq 1$ *or* $\mu_i=1$ *for at least one* i.

The proof of this theorem will be omitted since the method, although rather involved, is similar to that developed in detail in the proof of Theorem 1. We mention that if $k\geqq 8$, $h\geqq 1$, then it can be shown in case $k=2j$, that every element of $R(A)$ is a sum of either $j-1$ or j primes of $R(A)$, while if $k=2j+1$, that every element of $R(A)$ is a sum of either $j-1$, j, or $j+1$ primes.

4. Sums of two primes in $R(A)$ and the finite Goldbach property. Using the same sort of argument as in the proof of Theorem 1, the following two statements concerning sums of finite primes can be proved. If $k\geqq 2$, $h=0$, an element $\rho=\zeta_u\tau_v\xi$ is a sum of two primes in $R(A)$ if and only if either

$$\begin{aligned} &v = k-2,\\ &v = k,\ e_j > 1 \text{ (for at least one } j\text{), or}\\ &v = k,\ \mu_j = e_j = 1 \text{ (for at least one } j\text{).}\end{aligned} \tag{4.1}$$

If $k\geqq 2$, $h\geqq 1$, then an element ρ is *not* a sum of two primes in $R(A)$ if and only if either

$$\begin{aligned} &u = h, \qquad v = k-1;\\ &k-2 > v \geqq 0;\ \text{or}\\ &v = k, \qquad u = 0, \qquad h = 1, \qquad \mu_j > e_j = 1 \qquad (\text{all } j).\end{aligned} \tag{4.2}$$

Suppose now that A is an absolutely even ideal (§2). An element ρ will be called absolutely even in $R(A)$ if $v>0$, that is, provided A and ρ have in common a prime ideal divisor of type II. Corresponding to the statement of the ordinary Goldbach problem, we shall say that the ring $R(A)$ possesses the *Goldbach property*, provided A is absolutely even, and every composite, absolutely even ρ of $R(A)$ is a sum of two primes in $R(A)$. We shall also say that the field F possesses the *finite Goldbach property* if F contains at least one prime ideal of type II and if for every absolutely even A of F, $R(A)$ possesses the Goldbach property.

THEOREM 3. *The ring* $R(A)$ *possesses the Goldbach property if and only if* A *has but one distinct prime divisor of type* II *or if* A *is of the form* $A=Q_1Q_2$.

PROOF. That every composite, absolutely even ρ of $R(A)$ is a sum of two primes in $R(A)$, provided $k=1$, follows from Theorem 3 of [2] and Lemma 6 above. This is not the case for A with $k>1$, $h\geqq 1$, because, by (4.2), ρ is not a sum of two primes in $R(A)$ when $u=h$, $v=k-1$. A similar observation holds for $h=0$, $k\geqq 3$ by (4.1). In the remaining case, $h=0$, $k=2$, it also follows by (4.1) that $\tau_1\xi$ is not a sum of two primes in $R(A)$; further, $\tau_1\xi$ is always a prime only if $\mu_1=\mu_2=1$. In the latter case, however, $\tau_2\xi$ must be a sum of two primes in $R(A)$.

It thus follows that the finite Goldbach property holds in F if and only if F contains a single prime ideal of type II. This is restated as

THEOREM 4. *An algebraic number field of degree n over the rational field possesses the finite Goldbach property if and only if the rational integer* 2 *is the nth power of a prime ideal of F* $(2=Q^n)$.

COROLLARY 1. *The rational field Z possesses the finite Goldbach property.*

In the case of quadratic fields $Z(d^{1/2})$, d square-free, it is recalled [3] that the integer 2 is the square of a prime ideal, or otherwise, according as d is not or is $\equiv 1 \pmod 4$. Hence one may state the following corollary to Theorem 4.

COROLLARY 2. *The quadratic field $Z(d^{1/2})$, d square-free, possesses the finite Goldbach property if and only if $d\equiv 2$ or* 3 (mod 4).

BIBLIOGRAPHY

1. Eckford Cohen, *Congruence representations in algebraic number fields*, Trans. Amer. Math. Soc. vol. 75 (1953) pp. 444–470.

2. ———, *A finite analogue of the Goldbach problem*, Proc. Amer. Math. Soc. vol. 5 (1954) pp. 478–483.

3. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, 1923, p. 110.

UNIVERSITY OF TENNESSEE