Conspectus materiae tomi XIX, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange

Address of the Editorial Board and of the exchange

Die Adresse der Schriftleitung und des Austausches

Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, Warszawa 1

Les volumes IV et suivants sont à obtenir chez

Volumes from IV on are available at

Die Bände IV und folgende sind zu beziehen durch

Томы IV и следующие можно получить через

Ars Polona-Ruch, Krakowskie Przedmieście 7, Warszawa 1

Prix d'un fascicule   Price of an issue   Preis für ein Heft   Цена номера

$ 4.00

Les volumes I–III sont à obtenir chez

Volumes I–III are available at

Die Bände I–III sind zu beziehen durch

Томы I–III можно получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

W R O C Ł A W S K A   D R U K A R N I A   N A U K O W A

ACTA ARITHMETICA
XIX (1971)

Non-principal divisors among the values of polynomials

by

C. R. MacCluer (East Lansing, Mich.)

Let k be a number field and let $f(X)$ be a primitive polynomial of degree n with rational integral coefficients whose values $f(x)$ at rational integers x have no common factor. A. Schinzel has asked:

Are there infinitely many integers of the form $f(x)$ all of whose prime divisors in k are principal?

The answer is yes for linear f according to a recent result of C. J. Parry [1]. In contrast, as I point out here, the answer is sometimes no for f non-linear, at least *no for polynomials f which possess polynomial factors in k with non-principal content.* For suppose in $k[X]$ that

$$f(X) = F(X)\cdot\frac{G(X)}{d}$$

where F and G have integral coefficients, where d is an integer, and where $F(X)$ has non-principal content $\operatorname{cont}F$. Then because f is primitive, as ideals

$$d = \operatorname{cont}F\cdot\operatorname{cont}G$$

and so for each rational integer x, as ideals

$$f(x) = F(x)(\operatorname{cont}F)^{-1}G(x)(\operatorname{cont}G)^{-1}$$

where $F(x)(\operatorname{cont}F)^{-1}$ is not principal. In short, for each integer x some prime factor of $f(x)$ in k is non-principal!

This phenomenon can of course occur only when f is non-monic.

But when do such polynomials $f(x)$ exist? Always! For suppose k has class number $h(k) > 1$. Let $\mathfrak{p}$ be a non-principal prime of k. We may assume that $\mathfrak{p}$ is of degree 1 over the rational prime p. Let $\mathfrak{a}$ be any integral ideal of k such that $\mathfrak{p}\mathfrak{a}$ is principal. Recall that $\mathfrak{a}$ can be chosen prime to any prescribed ideal. Assume then that

$$(\mathfrak{a}, p) = 1$$

and let

$$(\theta) = \mathfrak{p}\mathfrak{a}.$$

Then necessarily, θ is integral but not rational. Let $g(X) = \operatorname{Irr}(\theta, Q) = X^m + c_{m-1}X^{m-1} + \ldots + c_1X + c_0$ be the minimal polynomial for θ in $Z[X]$. Since the absolute norm

$$\|\theta\| = |c_0| = \|\mathfrak{p}\mathfrak{a}\| = \|\mathfrak{p}\|\cdot\|\mathfrak{a}\| = pa,$$

$$(p, a) = 1$$

and so

$$f(X) = p^{-1}g(pX)$$

is primitive with rational integral coefficients! Since we may choose $\mathfrak{a}$ prime to any prime $q \leqslant n$, the values $f(x)$ need not possess a non-trivial common divisor.

For any number field k with class number $h(k) > 1$, construct $f(X)$ as above. Then every value $f(x)$ has at least one non-principal prime divisor in k.

For θ/p is a root of $f(X) = 0$ and hence in $k[X]$,

$$f(X) = (pX - \theta)\frac{G(X)}{p}$$

where $F(X) = pX - \theta$ has non-principal content $\mathfrak{p}$.

Specializing, let $k = Q(\sqrt{-5})$, $p = 2$, and $\theta = 1 + \sqrt{-5}$. Then

$$f(X) = 2X^2 - 2X + 3$$

always has non-principal divisors in $Q(\sqrt{-5})$. This can be seen directly by translating Artin reciprocity for the class field $Q(\sqrt{5}, i)/Q(\sqrt{-5})$ into residues modulo 20.

Reference

[1] C. J. Parry, *On a problem of Schinzel concerning principal divisors in arithmetic progressions*, Acta Arith. 19 (1971), pp. 215–222.

MICHIGAN STATE UNIVERSITY

Received on 23. 2. 1970 (40)

ACTA ARITHMETICA
XIX (1971)

Primitive representation of a binary quadratic form as a sum of four squares

by

JOHN L. HUNSUCKER (Athens, Ga.)

1. If an integral binary quadratic form f of nonzero determinant is representable as a sum of four squares, i.e., in the form $(r_1x+s_1y)^2 + \ldots + (r_4x+s_4y)^2$ where $r_1, \ldots, s_4$ are integers, then f can be written as ef', where e is a positive integer, $f' = [a, 2t_0; b] = ax^2 + 2t_0xy + by^2$, $(a, t_0, b) = 1$, $a > 0$, $ab - t_0^2 > 0$. L. J. Mordell showed that such a form is representable as a sum of four squares if and only if $ab - t_0^2$ is not of the form $4^h(8n+7)$. H. Braun gave an expression for the number $r_4(f)$ of such representations, and G. Pall and O. Taussky found a simpler expression which showed that for fixed f' (with $r_4(f') \neq 0$), $r_4(ef')/r_4(f')$ is a factorable function of e. We will here prove a like result for $r_4'(ef')/r_4'(f')$, where $r_4'(\ldots)$ denotes the number of *primitive* representations, in which the g.c.d. of the six determinants $r_is_j - r_js_i$ is unity; and we will find simple formulas for $r_4'(f)$, and related results.

2. Let B_1 denote the matrix of ef', $c = ab - t_0^2$, $b_1 = e^2c$,

$$E = \operatorname{adj} B_1 = eR, \qquad R = \begin{bmatrix} b & -t_0 \\ -t_0 & a \end{bmatrix}. \tag{1}$$

Our work will be based on an algorithm due to G. Pall ([3], § 3). The algorithm is simplest for the study of primitive representations of a form in k variables by one in n variables, when $k = 1$ or $n-1$. In our case, $n = 4$ and $k = 2$, and we have to locate the integral symmetric positive-definite matrices G of determinant b_1 for which

$$KEK' \equiv -G \pmod{b_1} \tag{2}$$

has integral solution matrices K (of order 2). By (2) the g.c.d. e of the elements of E must divide the elements of G. But Pall's algorithm (see (13)–(14) of [3]) requires in the case where the determinant of the representing form is 1 that

$$L'GL \equiv -E \pmod{b_1} \tag{3}$$

be solvable for L. Hence the g.c.d. of the elements of G is also e.