Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

O Anel dos Vetores de Witt e o Problema de Waring

por

Abílio Lemos Cardoso Júnior

Brasília
2006

Introdução

Denotamos por $\mathfrak{R}$ um anel comutativo com unidade. Para um inteiro $n > 1$, definimos $g_{\mathfrak{R}}(n)$ como o menor inteiro s para o qual todo elemento de $\mathfrak{R}$ é uma soma de s n-ésimas potências de elementos de $\mathfrak{R}$, se tal inteiro existir, ou ∞ caso contrário. O *problema de Waring* para $\mathfrak{R}$ consiste em decidir se $g_{\mathfrak{R}}(n)$ é finito e estimá-lo, para todo n. Note que o usualmente chamado problema de Waring não é o que chamamos problema de Waring para $\mathbb{Z}$. Para n ímpar, o que chamamos problema de Waring para $\mathbb{Z}$ é freqüentemente conhecido como o problema "mais fácil" de Waring, ou seja, o problema de Waring referente apenas a inteiros positivos.

Em 1770, Waring publicou um trabalho onde afirmou que todo inteiro positivo N pode ser escrito como uma soma de:

(a) no máximo, 4 quadrados;
(b) no máximo, 9 cubos;
(c) no máximo, 19 quartas potências.

Embora ele não tenha apresentado nenhuma demonstração para estas afirmações, talvez, baseado na observação de muitos exemplos, ele suspeitava que, para cada inteiro positivo n, deveria existir um inteiro positivo $g(n)$ tal que todo inteiro positivo N pudesse ser expresso como a soma de, no máximo, $g(n)$ n-ésimas potências positivas.

No mesmo ano, Lagrange demonstrou que todo inteiro é a soma de, no máximo, 4 quadrados.

Em 1909, Hilbert provou, para todo n, a existência de um inteiro positivo $g(n)$, independente de N, com a seguinte propriedade: todo inteiro N pode ser expresso como a soma de, no máximo, $g(n)$ n-ésimas potências. A demonstração de Hilbert prova apenas a existência de $g(n)$, mas não fornece informações sobre o valor de $g(n)$.

Entre 1909 e 1912 Wieferich e Kempner mostraram que, todo inteiro é a soma de, no máximo, 9 cubos. Em 1940 Pillai mostrou que $g(6) = 73$. Em 1964 Chen Jingrun mostrou que $g(5) = 37$. Em 1986 Balusabramanian, Dress e Deshouillers mostraram que $g(4) = 19$.

Alguns resultados foram obtidos mais tarde para o seguinte problema: para p um número primo e n um inteiro positivo, queremos encontrar $\Gamma_p(n)$ de forma que ele seja o menor inteiro positivo s para o qual pode-se resolver não trivialmente a seguinte congruência

$$x_1^n + \cdots + x_s^n \equiv N \pmod{p^l}, \tag{1}$$

para todo inteiro N e todo inteiro positivo l.

Hardy e Littlewood, usando métodos analíticos, mostraram em ([8], p.186, Teorema 12) que para todo p e n,

$$\Gamma_p(n) \leq 4n.$$

Em 1943, I. Chowla [5] mostrou que se $\frac{1}{2}(p-1)$ não divide n, então para todo $\epsilon > 0$,

$$\Gamma_p(n) \ll n^{1-c+\epsilon},$$

onde $c = (103 - 3\sqrt{641})/200$ e $\ll$ denota a desigualdade com uma constante fixa positiva. Posteriormente, Dodson [6] melhorou o expoente para $7/8$.

Se p não divide n, então a solubilidade da congruência (1) é equivalente a solubilidade da congruência

$$x_1^n + \cdots + x_s^n \equiv N \pmod{p}. \tag{2}$$

Agora, se $\Gamma(n,p)$ é definido como o menor s tal que (2) é solúvel não trivialmente para todo N, então Dodson e Tietäväinen [7] mostraram que se $\frac{1}{2}(p-1)$ não divide n, para todo $\epsilon > 0$ vale:

$$\Gamma(n,p) \ll n^{\frac{1}{2}+\epsilon}.$$

Bovey [2] em 1976, generalizou os resultados de Dodson e Tietäväinen para o caso geral p-ádico e provou nas hipóteses da congruência (1) que:

$$\Gamma_p(n) \ll n^{\frac{1}{2}+\epsilon}.$$

Para o problema de Waring sobre corpos finitos consulte [4].

Em 1999, Voloch [3] em trabalho intitulado "On the p-adic Waring's problem", provou alguns resultados para extensões não ramificadas de $\mathbb{Z}_p$. Em particular, Voloch demonstrou que todo inteiro p-ádico é uma soma de 9 pd-ésimas potências, se p for suficientemente grande comparado a d.

Neste trabalho fazemos uma abordagem geral de anel de valorização discreta completo. Depois a partir de um anel comutativo com unidade A, construímos o anel dos vetores de Witt, denotado por $W(A)$, com coeficientes em A, seguindo o método adotado por Fontaine em sua nota sobre a construção dos vetores de Witt [9]. Definimos $W(k)$, onde k é um corpo perfeito de característica p, e mostramos que $W(k)$ é um anel de valorização discreta completo não ramificado. A construção original, realizada por Ernst Witt (1936), pode ser encontrada em [1]. Em seguida tomamos k algébrico sobre $\mathbb{F}_p$ e concluímos que $W(k)$ é, a menos de isomorfismo, a única extensão completa não ramificada de $\mathbb{Z}_p$. Por fim, fazemos uma aplicação do problema de Waring para $W(k)$. De uma forma mais precisa, podemos separar este trabalho da seguinte forma:

No Capítulo 1, apresentamos uma abordagem geral de um anel de valorização discreta completo $\widehat{\mathfrak{A}}$ qualquer, com corpo residual perfeito de característica p, obtendo vários resultados, tais como o conjunto dos representantes de Teichmüller e as operações soma e produto em $\widehat{\mathfrak{A}}$.

No Capítulo 2, construímos o anel dos vetores de Witt de acordo com o Método de Fontaine. Depois definimos $W(k)$ e obtivemos alguns resultados, tais como: a expansão p-ádica de um vetor de Witt e o isomorfismo $W(\mathbb{F}_p) \cong \mathbb{Z}_p$, onde $\mathbb{Z}_p$ é o anel dos inteiros p-ádicos, cujo corpo residual é $\mathbb{F}_p$. Na parte final do capítulo, aplicamos o problema de Waring para $W(k)$, quando k é algébrico sobre $\mathbb{F}_p$. Nestas circunstâncias, concluímos que $W(k)$ é, a menos de isomorfismo, a única extensão completa não ramificada de $\mathbb{Z}_p$. A parte final do capítulo foi baseada no trabalho de Voloch [3] denominado "On the p-adic Waring's problem". Não exibimos todos os resultados deste artigo, devido a sua conexão com a Geometria Algébrica, o que demandaria mais tempo para ser tratado.

Resumo

Neste trabalho, fazemos um estudo geral do anel de valorização discreta completo. Construímos o anel dos vetores de Witt, denotado por $W(A)$, com coeficientes em um anel comutativo com unidade A. Definimos $W(k)$, onde k é um corpo perfeito de característica p, e mostramos que $W(k)$ é um anel de valorização discreta completo não ramificado. Em seguida tomamos k algébrico sobre $\mathbb{F}_p$ e concluímos que $W(k)$ é, a menos de isomorfismo, a única extensão completa não ramificada de $\mathbb{Z}_p$. Por fim, aplicamos o problema de Waring para $W(k)$.

Abstract

In this work we study complete discrete valuation rings. We construct the ring of Witt vectors, denoted by $W(A)$, with components in a commutative ring with unity A. We define $W(k)$, where k is a perfect field of characteristc p, and prove that $W(k)$, defined in this way, is a complete discrete unramified valuation ring. Afterwards, we take k algebraic over $\mathbb{F}_p$ and we conclude that $W(k)$ is, up to isomorphism, the unique complete unramified extension of Z_p. Finally, we apply the Waring's problem to $W(k)$.

Referências Bibliográficas

[1] E. Witt, *Zyklische Körper und Algebren der characteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassem-körper der charakteristik p*, J. Reine Angew. Math., 176 (1936) 126-140

[2] J. D. Bovey, *A note on Waring's problem in p-adic fields*, Acta Arith. 29 (1976) 343-351.

[3] J. F. Voloch, *On the p-adic Waring's problem*, Acta Arith. 90 (1999) 91-95

[4] A. Garcia and J. F. Voloch, *Fermat curves over finite fields*, J. Number Theory (1988) 345-356.

[5] I. Chowla, *On Waring's problem (mod p)*, Proc. Nat. Sci. India, A, 12 (1943) 195-220.

[6] M. M. Dodson, *On Waring's problem in p-adic fields*, Acta Arith. 22 (1973) 315-327.

[7] M. M. Dodson and A. Tietäväinen, *A note on Warig's problem in $GF[p]$*, Acta Arith. to appear.

[8] G. H. Hardy and J. E. Littlewood, *Some problems 'Partitio Numerorum' (IV): The singular series in Waring's problem and the value of the number $G(k)$*, Math. Zeitschr. 12 (1922) 161-188.

[9] Foutaine, preprint, available at `http://www.math.ku.dk/~kiming/lecture_notes/2000-fontaine/witt.pdf`.

[10] D. Mumford, *Lectures on curves on an algebraic surface*, Princeton Univ. Press (1966).

[11] J. P. Serre, *Groupes algébrique et corps des classes*, Hermann (1959).

[12] M. Demazure, P. Gabriel, *Groupes algébriques*, **1**, North-Holland (1971).

[13] J. Dieudonné, *Groupes de Lie et hyperalgébres de Lie sur un corps de charactéristique* $p > 0$ *VII*, Math. Ann., **134** (1957) 114-133.

[14] J. P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[15] J. W. S. Cassels, *Local Fields*, Cambridge University Press, 1986.

[16] M. J. Greenberg, *Lectures on Forms in Many Variables*, University of California, Santa Cruz, 1969.

[17] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966.

[18] S. Shokranian, M. Soares e H. Godinho, *Teoria dos Números*, Editora Universidade de Brasília, 2ª ed., 1999.

[19] O. Zariski and P. Samuel, *Commutative Algebra*, V. II, Springer-Verlag, 1960.

[20] M. D. Larsen and P. J. McCarthy, *Multiplicative Theory of Ideals*, Academic Press, New York and London, 1971.

[21] I. G. Macdonald and M. F. Atiyah, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, University of Oxford, 1969.

[22] P. J. McCarthy, *Algebraic Extensions of Fields*, Chelsea Publishing Company, New York, University of Kansas, 1976.