Divulgaciones Matemáticas Vol. 7 No. 1 (1999), pp. 13–18

A Note on Waring's Number Modulo 2^n

Una Nota sobre el Número de Waring Módulo 2^n

Julio Subocz (jsubocz@hydra.math.luz.ve)
Departamento de Matemática y Computación
Facultad de Ciencias. Universidad del Zulia
Apartado 526. Maracaibo. Venezuela

Abstract

The Waring number of the integers modulo m with respect to k-th powers, denoted by $\rho(m,k)$, is the smallest r such that every integer is a sum of r k-th powers modulo m. This number is also the diameter of an associated Cayley graph, called the Waring graph. In this paper this number is computed when m is a power of 2. More precisely the following result is obtained:

Let n, s and b be natural numbers such that b is odd, $s \geq 1$ and $n \geq 4$. Put $k = b2^s$. Then

(i) if $s \geq n-2$, then $\rho(2^n,k) = 2^n - 1$.

(ii) if $k \geq 6$ and $s \leq n-3$, then $\rho(2^n,k) = 2^{s+2}$.

Key words and phrases: Waring number, Cayley graph, diameter.

Resumen

El número de Waring de los enteros módulo m con respecto a las potencias k-ésimas, denotado $\rho(m,k)$, es el menor r tal que todo entero es la suma de r potencias k-ésimas módulo m. Este número es también el diámetro de un grafo de Cayley asociado, llamado el grafo de Waring. En este trabajo se calcula este número cuando m es una potencia de 2. Más precisamente se obtiene el siguiente resultado:

Sean n, s y b números naturales tales que b es impar, $s \geq 1$ y $n \geq 4$. Sea $k = b2^s$. Entonces

(i) si $s \geq n-2$, entonces $\rho(2^n,k) = 2^n - 1$.

(ii) si $k \geq 6$ y $s \leq n-3$, entonces $\rho(2^n,k) = 2^{s+2}$.

Palabras y frases clave: número de Waring, grafo de Cayley, diámetro.

Recibido 1998/11/07. Revisado 1999/03/07. Aceptado 1999/03/11.
MSC (1991): Primary 11P05; Secondary 05C25.

1 Introduction

Let R be a ring and k a natural number. The *Waring number* $\rho(R,k)$ is the smallest n such that $\{x_1^k + x_2^k + \cdots + x_n^k : x_i \in R, 1 \leq i \leq n\} = R$. The determination of this number is a generalization of the classical Waring problem. Here we give a brief survey of this problem for finite R. We'll denote by Z_m the ring of integers modulo m. Cauchy proved in [1] that $\rho(Z_p,k) \leq k$, for all prime numbers p. In [2] Chowla, Mann and Straus obtained the bound $\rho(Z_p,k) \leq \lfloor k/2 \rfloor + 1$, for p prime and $k \neq (p-1)/2$. Schwarz obtained in [9] similar results for any finite field in which every element is a sum of k-th powers. Heilbronn conjectured in [6] that $\sup_p\{\rho(Z_p,k) : k \neq (p-1)/2\} = O(\sqrt{k})$, for p prime. The reader can find details about this problem in [3]. The best known result is the following theorem of Dodson and Tietäväinen [3]: for p prime, $\rho(Z_p,k) < 68(\log k)^2\sqrt{k}$.

Helleset showed in [7] that the Waring number for a finite field is the covering radius of a certain code. The Waring number in Z_n where n is not necessarily a prime, is studied by C. Small in [10] and [11], where it is calculated for $k \leq 5$, while upper bounds are obtained for other k's.

We have $\rho(Z_m,k) = \max_p \rho(Z_{p^{n_p}},k)$, where p^{n_p} is the greatest power of the prime p dividing m [8, remark in proof of Theorem 1]. In graphic terms the Waring number is the diameter of a certain Cayley graph, where the group is the underlying additive group of a ring with respect to the set of k-th powers. While studying the connectivity and diameter of such graphs for the rings Z_m, we found that the case $m = 2^n$ is particularly simple and does not require the relatively difficult theorems of connectivity or Additive Theory.

We obtain here, using simple combinatorial arguments, the exact value of the Waring number $\rho(Z_n,k)$ for any k, when n is a power of 2. In particular, it is always a power of 2, apart from a few exceptions.

2 Preliminaries

We restrict ourselves to abelian groups. We'll use the following well known lemma (see [8], Theorem 1.1):

Lemma 2.1. *Let G be a finite abelian group containing two subsets A and B such that $|A| + |B| \geq |G| + 1$. Then $A + B = G$.*

Let G be a finite abelian group containing a subset S. Let $\mathrm{Cay}(G,S)$ denote the graph (G,E), where $E = \{(x,y) : y - x \in S\}$. $\mathrm{Cay}(G,S)$ is known as the *Cayley graph* defined on G by S.

Remark 2.2. The Cayley graph $\mathrm{Cay}(G, S)$ is not necessarily symmetric. In fact, it is symmetric if and only if $S = -S$.

Remark 2.3. $\mathrm{Cay}(G, S)$ is (strongly) connected if and only if S is a set of generators of G.

The diameter of $\mathrm{Cay}(G, S)$ will be denoted by $\rho(\mathrm{Cay}(G, S))$. We can see easily that $\rho(\mathrm{Cay}(G, S)) = \min\{j : \{0\} \cup S \cup S + S \cup \ldots \cup jS\} = G$, or equivalently $\rho(\mathrm{Cay}(G, S)) = \min\{j : j(S \cup \{0\}) = G\}$, where the notation jS means $\{x_1 + x_2 + \cdots + x_j : x_i \in S\}$.

When G is the underlying additive group of a ring R and S is the set of k-th powers of R, $\mathrm{Cay}(G, S)$ is called a *Waring graph* (this term is used by Hamidoune [4, 5]; these graphs were also studied by Babai).

Henceforth we'll study the case $R = Z_m$, that is the ring of residues modulo m.

The (additive) subgroup of G generated by an element $x \in G$ will be denoted by $\langle x \rangle$.

Let m and k be natural numbers. Let us put $\rho(m, k)$ for $\rho(Z_m, k)$. We clearly have $\rho(m, k) = \rho(\mathrm{Cay}(Z_m, Z_m^k))$. In order to study also the representation using only powers of the units, let's define $\rho^1(m, k) = \rho(\mathrm{Cay}(Z_m, U^k))$, where U is the set of units of Z_m.

Lemma 2.4. *Let k, n and m be natural numbers. Then*

(i) $\rho(m, k) \leq \rho^1(m, k)$

(ii) If $k \geq n$, then $\rho(2^n, k) = \rho^1(2^n, k)$.

Proof. Being $\mathrm{Cay}(Z_m, U^k)$ a subgraph of $\mathrm{Cay}(Z_m, Z_m^k))$, inequality (i) follows. Equality (ii) follows since $U^k = (Z_m^k) \setminus \{0\}$, for $k \geq n$. □

Remark 2.5. Note that if n divides m then $\rho(n, k) \leq \rho(m, k)$. Actually, if $\pi : Z_m \longrightarrow Z_n$ is the canonical morphism, one verifies easily that $\pi(Z_m^k) = Z_n^k$. Put $r = \rho(m, k)$. By the definitions, we have $rZ_m^k = Z_m$. Therefore $rZ_n^k = r\pi(Z_m^k) = \pi(rZ_m^k) = \pi(Z_m) = Z_n$. It follows that $\rho(m, k) \geq \rho(n, k)$.

Lemma 2.6. *Let G be an abelian group whose order is a power of two, and let k be an odd integer, $k > 2$. Let ϕ_k be the endomorphism of G defined by $\phi_k(x) = x^k$. Then*

(i) if G is cyclic and $k = 2$, then $|Im(\phi_k)| = |G|/2$.

(ii) if k is odd, then ϕ_k is an automorphism.

The proof of this lemma is left as an exercise.

3 Diameter modulo 2^n

In what follows σ denotes the canonical mapping from Z onto Z_{2^n}.

Lemma 3.1. *Let n, b and s be natural numbers such that b is odd and let $k = b2^s$. Then,*

(i) $\rho^1(2^n, b) = 2$, $b > 1$.

(ii) $U^k = \sigma(1) + \langle\sigma(2^{s+2})\rangle$.

(iii) $\rho^1(2^n, k) = \rho^1(2^n, 2^s)$.

Proof. By Lemma 2.6, $U^b = U$. We have clearly $|U^b \cup \{0\}| = 2^{n-1} + 1$. By Lemma 2.1, $2(U^b \cup \{0\}) = Z_{2^n}$. Therefore $\rho^1(2^n, b) = 2$. This proves (i).

It is obvious that U is a direct product of the subgroups $\{\sigma(1), -\sigma(1)\}$ and $\sigma(1) + \langle\sigma(4)\rangle$. Therefore U^2 is a subgroup of the cyclic group $\sigma(1) + \langle\sigma(4)\rangle$ with order 2^{n-3}. This subgroup is unique and hence $U^2 = \sigma(1) + \langle\sigma(2^3)\rangle$. Therefore the result holds for $s = 1$. Suppose it is proved for s. We may assume $s + 2 < n$, since otherwise the result holds trivially. By Lemma 2.6, $U^{2^{(s+1)}}$ is a cyclic subgroup of $U^{2^s} = \sigma(1) + \langle\sigma(2^{s+2})\rangle$ with order 2^{n-s-3}. Therefore $U^{2^{(s+1)}} = \sigma(1) + \langle\sigma(2^{s+3})\rangle$. This proves (ii). The statement (iii) follows now since $U^k = (U^b)^{2^s} = U^{2^s}$, by Lemma 2.6. $\square$

We prove now our main result.

Theorem 3.2. *Let n, s and b be natural numbers such that b is odd, $s \geq 1$ and $n \geq 4$. Let $k = b2^s$. Then the following holds:*

(i) If $s \geq n - 2$ then $\rho(2^n, k) = \rho^1(2^n, k) = 2^n - 1$.

(ii) If $s \leq n - 3$ then $\rho^1(2^n, k) = 2^{s+2}$.

(iii) If $k \geq 6$ and $s \leq n - 3$ then $\rho(2^n, k) = 2^{s+2}$.

Proof. We prove first (i). Suppose $s \geq n - 2$. By Lemma 3.1(ii) we have $U^k = \sigma(1) + \langle\sigma(2^{s+2})\rangle = \{\sigma(1)\}$. It follows easily that $(Z_{2^n})^k = \{\sigma(0), \sigma(1)\}$, because $2^s \geq n$. Therefore $\rho(2^n, k) = \rho^1(2^n, k) = 2^n - 1$.

We prove now (ii). Suppose $s \leq n-3$. By Lemma 3.1(ii) we have $t(U^k) = t\sigma(1) + t\langle\sigma(2^{s+2})\rangle = \sigma(t) + \langle\sigma(2^{s+2})\rangle$. It follows that

$$t(\{0\} \cup (\sigma(1) + \langle\sigma(2^{s+2})\rangle)) =$$
$$\{0\} \cup (\sigma(1) + \langle\sigma(2^{s+2})\rangle) \cup (\sigma(2) + \langle\sigma(2^{s+2})\rangle) \cup \ldots \cup (\sigma(t) + \langle\sigma(2^{s+2})\rangle).$$

Clearly $|\sigma(i) + \langle\sigma(2^{s+2})\rangle| = 2^{n-s-2}$ and $|t(\{0\} \cup (\sigma(1) + \langle\sigma(2^{s+2})\rangle))| = \min(2^n, 1 + t2^{n-s-2})$. It follows that

$$\rho^1(2^n, 2^s) = \left\lceil \frac{2^n - 1}{2^{n-s-2}} \right\rceil = 2^{s+2}.$$

It remains to show (iii). Suppose $k \geq 6$ and $s \leq n - 3$. We have clearly $s + 3 \leq k$ and $s + 3 \leq n$. By (ii), Lemma 2.4 and Remark 2.5 we have $2^{s+2} = \rho^1(2^n, k) \geq \rho(2^n, k) \geq \rho(2^{s+3}, k)$. By Lemma 2.4 and (ii) $\rho(2^{s+3}, k) = 2^{s+2}$. Therefore $\rho(2^n, k) = 2^{s+2}$. □

In order to give a complete account of the Waring number modulo 2^n we need to consider the cases $k = 2$ and $k = 4$. The study of sums of squares modulo n is due essentially to Gauss. See Small's paper [8, Theorem 3.1]. For fourth powers modulo n, a solution is given in Small [9, Theorems 3, 3']. In our notation the corresponding results are summarized as follows:

Theorem 3.3. $\rho(2^2, 2) = 3$,
$\rho(2^n, 2) = 4$, *for all* $n \geq 3$,
$\rho(2^3, 4) = 7$,
$\rho(2^n, 4) = 15$, *for all* $n \geq 4$.

Acknowledgements

This research was carried out while the author was visiting the UFR-921-Equipe Combinatoire at Université Pierre et Marie Curie (Paris). It was partially supported by PCP-Info (CEFI-CONICIT).

References

[1] Cauchy, A. *Recherches sur les nombres*, J. Ecole Polytechnique, **9**(1813), 99–116.

[2] Chowla, S., Mann, H. B., Straus, E. G. *Some Applications of the Cauchy-Davenport Theorem*, Norske Vid. Selsk. Forh. (Trondheim) **32**(1959), 74–80.

[3] Dodson, M. M., Tietäväinen, A. *A Note on Waring's Problem in GF(p)*, Acta Arithmetica XXX(1976), 158–167.

[4] Hamidoune,Y. O. *The Waring's Graph and its Diameter*, Conference Notes, Caracas, 1993.

[5] Hamidoune,Y. O. *Additive Group Theory Applied to Network Topology*, Preprint, 1994.

[6] Heilbronn, H. *Lecture Notes on Additive Number Theory mod* p, California Institute of Technology, 1964.

[7] Helleseth, T. *The Covering Radius of Cyclic Linear Codes and Arithmetic Codes*, Discrete Applied. Math. **11**(1987), 157–173.

[8] Mann, H. B. *ADDITION THEOREMS: The Addition Theorems of Group Theory and Number Theory*, Interscience, New York, 1965.

[9] Schwarz, S. *On Waring's problem for finite fields*, Quart. J. Math. Oxford **19**(1948), 123–128.

[10] Small, C. *Waring's problem mod* n, Amer. Math. Month., January (1977), 12–25.

[11] Small, C. *Solution of Waring's problem mod* n, Amer. Math. Month., May (1977), 356–359.