Journal of Number Theory 170 (2017) 35–45

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the addition of squares of units modulo n

Mohsen Mollahajiaghaei

Department of Mathematics, University of Western Ontario, London, Ontario, N6A 5B7, Canada

ARTICLE INFO

Article history:
Received 27 March 2016
Received in revised form 10 June 2016
Accepted 11 June 2016
Available online 2 August 2016
Communicated by David Goss

MSC:
11B13
05C50

Keywords:
Ring of residue classes
Squares of units
Adjacency matrix
Walks
Paley graph

ABSTRACT

Let $\mathbb{Z}_n$ be the ring of residue classes modulo n, and let $\mathbb{Z}_n^*$ be the group of its units. 90 years ago, Brauer obtained a formula for the number of representations of $c \in \mathbb{Z}_n$ as the sum of k units. Recently, Yang and Tang (2015) [6] gave a formula for the number of solutions of the equation $x_1^2 + x_2^2 = c$ with $x_1, x_2 \in \mathbb{Z}_n^*$. In this paper, we generalize this result. We find an explicit formula for the number of solutions of the equation $x_1^2 + \cdots + x_k^2 = c$ with $x_1, \ldots, x_k \in \mathbb{Z}_n^*$.

1. Introduction

Let $\mathbb{Z}_n$ be the ring of residue classes modulo n, and let $\mathbb{Z}_n^*$ be the group of its units. Let $c \in \mathbb{Z}_n$, and let k be a positive integer. Brauer in [1] gave a formula for the number of solutions of the equation $x_1 + \cdots + x_k = c$ with $x_1, \ldots, x_k \in \mathbb{Z}_n^*$. In [4] Sander found the number of representations of a fixed residue class mod n as the sum of two units

E-mail address: mmollaha@uwo.ca.

http://dx.doi.org/10.1016/j.jnt.2016.06.013
0022-314X/

in $\mathbb{Z}_n$, the sum of two non-units, and the sum of mixed pairs, respectively. In [3] the results of Sander were generalized into an arbitrary finite commutative ring, as sum of k units and sum of k non-units, with a combinatorial approach.

The problem of finding explicit formulas for the number of representations of a natural number n as the sum of k squares is one of the most interesting problems in number theory. For example, if $k = 4$, then Jacobi's four-square theorem states that this number is $8\sum_{m|c} m$ if c is odd and 24 times the sum of the odd divisors of c if c is even. See [5] and the references given there for historical remarks.

Recently, Tóth [5] obtained formulas for the number of solutions of the equation

$$a_1x_1^2 + \cdots + a_kx_k^2 = c,$$

where $c \in \mathbb{Z}_n$, and x_i and a_i all belong to $\mathbb{Z}_n$.

Now, consider the equation

$$x_1^2 + \cdots + x_k^2 = c, \tag{1}$$

where $c \in \mathbb{Z}_n$, and x_i are all units in the ring $\mathbb{Z}_n$. We denote the number of solutions of this equation by $\mathcal{S}_{sq}(\mathbb{Z}_n, c, k)$. In [6] Yang and Tang obtained a formula for $\mathcal{S}_{sq}(\mathbb{Z}_n, c, 2)$. In this paper we provide an explicit formula for $\mathcal{S}_{sq}(\mathbb{Z}_n, c, k)$, for an arbitrary k. Our approach is combinatorial with the help of spectral graph theory.

2. Preliminaries

In this section we present some graph theoretical notions and properties used in the paper. See, e.g., the book [2]. Let G be an additive group with identity 0. For $S \subseteq G$, the *Cayley graph* $X = Cay(G, S)$ is the directed graph having vertex set $V(X) = G$ and edge set $E(X) = \{(a, b); b - a \in S\}$. Clearly, if $0 \notin S$, then there is no loop in X, and if $0 \in S$, then there is exactly one loop at each vertex. If $-S = \{-s; s \in S\} = S$, then there is an edge from a to b if and only if there is an edge from b to a.

Let $\mathbb{Z}_n^{*2} = \{x^2; x \in \mathbb{Z}_n^*\}$. The *quadratic unitary Cayley graph* of $\mathbb{Z}_n$, $G^2_{\mathbb{Z}_n} = Cay(\mathbb{Z}_n; \mathbb{Z}_n^{*2})$, is defined as the directed Cayley graph on the additive group of $\mathbb{Z}_n$ with respect to $\mathbb{Z}_n^{*2}$; that is, $G^2_{\mathbb{Z}_n}$ has vertex set $\mathbb{Z}_n$ such that there is an edge from x to y if and only if $y - x \in \mathbb{Z}_n^{*2}$. Then the out-degree of each vertex is $|\mathbb{Z}_n^{*2}|$.

Let G be a graph, and let $V(G) = \{v_1, \ldots, v_n\}$. The *adjacency matrix* A_G of G is defined in a natural way. Thus, the rows and the columns of A_G are labeled by $V(G)$. For i, j, if there is an edge from v_i to v_j then $a_{v_iv_j} = 1$; otherwise $a_{v_iv_j} = 0$. We will write it simply A when no confusion can arise. For the graph $G^2_{\mathbb{Z}_n}$ the matrix A is symmetric, provided that -1 is a square mod n.

We write J_m for the $m \times m$ all 1-matrix. The identity $m \times m$ matrix will be denoted by I_m.

The complete graph on m vertices with loop at each vertex is denoted by K^l_m. Thus, the adjacency matrix of K^l_m is J_m.