Uniform Distribution Theory **2** (2007), no.2, 1–17

uniform distribution theory

AN APPLICATION OF RAMANUJAN SUMS TO EQUIREPARTITION MODULO AN ODD INTEGER

Éric Balandraud

ABSTRACT. Following a result of Myerson on finite fields, we prove that for an odd number $n \geqslant 3$, the $2^{\phi(n)/2}$ sums:

$$\pm 1 \pm 2 \cdots \pm i \cdots \pm (n-1)/2\,,$$

where the terms i are all the invertibles modulo n from 1 to $(n-1)/2$, are distributed among the classes modulo n as uniformly as possible.

We also determine and prove that the distribution of the $2^{(n-1)/2}$ sums:

$$\pm 1 \pm 2 \cdots \pm (n-1)/2\,,$$

where all the elements from 1 to $(n-1)/2$ are represented once, is also asymptotically equidistributed.

Communicated by Vasil Grozdanov

Introduction

In 1979, Myerson proved [3] that for a prime p, the sums:

$$\pm 1 \pm 2 \cdots \pm (p-1)/2\,,$$

are as uniformly distributed as possible among the residue classes modulo p.

Theorem 1 (Myerson)**.** *Let p be a prime number. For any $x \in \mathbb{Z}/p\mathbb{Z}$, the number N_x of ways of choosing the signs so that $\pm 1 \pm 2 \cdots \pm (p-1)/2 \equiv x \pmod p$ is:*

$$\begin{array}{ll} \textit{if} \quad x \neq 0 & N_x = \frac{1}{p}\left(2^{(p-1)/2} - \left(\frac{2}{p}\right)\right), \\ \textit{else} & N_0 = \frac{1}{p}\left(2^{(p-1)/2} - \left(\frac{2}{p}\right)\right) + \left(\frac{2}{p}\right), \end{array}$$

where $\left(\frac{2}{p}\right)$ is the Legendre symbol.

2000 Mathematics Subject Classification: 11B50, 11N69, 05A15.
Keywords: Ramanujan sum, Euler totient, Jacobi symbol, primitive root of unity.

Myerson's work is a prequel to a generalization for a more general type of sums related to multiplicative subgroups of a finite field, see also [4]. In this article we will focus our interest on the same type of sums considered in a cyclic group of odd order. We will prove the two following generalizations of Myerson result:

Theorem 2. *Let $n \geqslant 3$ be an odd integer. For any $x \in \mathbb{Z}/n\mathbb{Z}$, the number N_x of writings of x as a sum $\pm 1 \pm 2 \cdots \pm i \cdots \pm (n-1)/2$, where the terms i are all invertibles from 1 to $(n-1)/2$, is:*

$$\begin{array}{ll} \text{if } x \neq 0 & N_x = \frac{1}{n}\left(2^{\phi(n)/2} - \chi_2(n)\right), \\ \text{else} & N_0 = \frac{1}{n}\left(2^{\phi(n)/2} - \chi_2(n)\right) + \chi_2(n), \end{array}$$

$$\text{where } \chi_2(n) = \left| \begin{array}{ll} 1 & \text{if there are two distinct primes dividing } n \\ \left(\frac{2}{p}\right) & \text{if } n = p^\alpha \text{ for a prime } p. \end{array} \right.$$

Theorem 3. *Let $n \geqslant 3$ be an odd integer and $p(n)$ be its least prime divisor, for any $x \in \mathbb{Z}/n\mathbb{Z}$, the number M_x of writings of x as a sum $\pm 1 \pm 2 \cdots \pm (n-1)/2$, where the terms i are all residues from 1 to $(n-1)/2$, is:*

$$M_x = \frac{1}{n} \sum_{b|n} c(x,b) \left(\frac{2}{b}\right) 2^{\left(\frac{n}{b}-1\right)/2},$$

where $\left(\frac{2}{b}\right)$ is the Jacobi symbol and $c(x,b) = \sum_{\substack{i=1 \\ (i,b)=1}}^{b} \zeta^{xi}$, with ζ be a primitive n-th root of unity, is a Ramanujan sum. Moreover, we have:

$$\left| M_x - \frac{1}{n} 2^{(n-1)/2} \right| < 2^{\left(\frac{n}{p(n)}-1\right)/2}.$$

Notice that if n is a prime number, the numbers N_x and M_x are the same and Theorem 2 and 3 coincide with Myerson result. In the first section, we present the problem and define the unknowns, the numbers of writings looked for. In the second part, we introduce the basic properties of Ramanujan sums, that will be used in the continuation of this article. All this properties (but the last one) can be found in most introductory books on arithmetical functions, see for instance [2]. The third section provides a linear system that involves in the same time Ramanujan sums and the unknowns of our problem. The fourth section gives a more simple expression of some products that form the constant term of our linear system. This expression will enable us to give a simple expression of our unknowns in the fifth section, that is the proofs of Theorem 2 and 3. Finally, we give some examples in annex of these linear systems.

1. The problem

Let us consider an odd number $n \geqslant 3$. For any $x \in \mathbb{Z}/n\mathbb{Z}$, we denote by N_x:

$$N_x = \left| \left\{ \begin{array}{c} (\epsilon_1, \ldots, \epsilon_i, \ldots, \epsilon_{(n-1)/2}) \in \{-1,1\}^{\phi(n)/2} \\ \text{where the indices } i \text{ are the invertibles} \\ \text{modulo } n \text{ from 1 to } (n-1)/2. \end{array} \;\middle|\; \sum_{\substack{i=1 \\ (i,n)=1}}^{(n-1)/2} \epsilon_i i = x \pmod{n} \right\} \right|,$$

the number of writings of x as sum of the invertibles, where exactly one of any invertible or its opposite appears.

We also denote by M_x:

$$M_x = \left| \left\{ (\epsilon_1, \ldots, \epsilon_{(n-1)/2}) \in \{-1,1\}^{(n-1)/2} \;\middle|\; \sum_{i=1}^{(n-1)/2} \epsilon_i i = x \pmod{n} \right\} \right|,$$

the number of writings of x as a sum where exactly one of all element or its opposite appears.

We would like to give an expression of the n numbers N_x and of the n numbers M_x. First, we give a simple lemma that proves that some of the numbers we are considering are equal.

Lemma 1. *Let $n \geqslant 3$ be an odd number. Let x, y be two elements of $\mathbb{Z}/n\mathbb{Z}$. If $(n,x) = (n,y)$, then $N_x = N_y$, and $M_x = M_y$.*

Proof. If $(n,x) = (n,y)$, then there exists an element $\lambda \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $x = \lambda y$. We define the following function:

$$f : \left| \begin{array}{ccc} \{1, \ldots, (n-1)/2\} & \to & \{1, \ldots, (n-1)/2\} \\ i & \mapsto & \epsilon_{(\lambda,i)}.\lambda.i, \end{array} \right. .$$

where $\epsilon_{(\lambda,i)}$ is $+1$ if $i.\lambda \in \{1, \ldots, (n-1)/2\}$ and -1 otherwise.

This function is a one-to-one correspondence, between all elements from $\{1, \ldots, (n-1)/2\}$. Moreover, its restriction to the set of all invertible elements to itself is also a one-to-one correspondance.

From a writing $(\epsilon_1, \ldots, \epsilon_{(n-1)/2})$ of y, we compute a writing of x:

$$\begin{array}{lll} & \sum_{i=1}^{(n-1)/2} \epsilon_i i & = y \\ \iff & \sum_{i=1}^{(n-1)/2} \epsilon_i.\lambda.i & = \lambda y \\ \iff & \sum_{i=1}^{(n-1)/2} \epsilon_{(\lambda,i)}.\epsilon_i.f(i) & = x \\ \iff & \sum_{j=1}^{(n-1)/2} \epsilon_{\left(\lambda, f^{-1}(j)\right)}.\epsilon_{f^{-1}(j)}.j & = x, \end{array}$$

namely the writing $\left(\epsilon_{(\lambda, f^{-1}(j))}\epsilon_{f^{-1}(j)}\right)$ of x.

This correspondance is one-to-one from the writings of y and the writings of x. □

Since Lemma 1 proves that for $x \in \mathbb{Z}/n\mathbb{Z}$, we have $N_x = N_{(x,n)}$ and $M_x = M_{(x,n)}$, we will from now on only consider the quantities N_b and M_b, where b is a divisor of n. If $\tau(n)$ is the number of divisors of n, there are $\tau(n)$ numbers to determine in each family $(N_b)_{b|n}$ and $(M_b)_{b|n}$. Notice that in this notation the number N_n is the number that was before N_0.

2. Ramanujan sums

Let n be any positive integer, and ζ be a primitive n-th root of unity. We denote the Ramanujan sum:

$$c(d,n) = \sum_{\substack{i=1 \\ (i,n)=1}}^{n} \zeta^{di}.$$

Remark 1. We can notice that $c(d,n) = c\big((d,n),n\big)$, where (d,n) is the gcd of d and n.

Two particular cases of Ramanujan sums are:

- If $n|d$, then $c(d,n) = \sum_{\substack{i=1 \\ (i,n)=1}}^{n} 1 = \phi(n)$, which is Euler totient.
- If $(d,n) = 1$, then $c(d,n) = \sum_{\substack{i=1 \\ (i,n)=1}}^{n} \zeta^i = \mu(n)$, which is Möbius function.

Apart from its last lemma (Lemma 4), all this section gives some well-known properties of Ramanujan sums without proofs. The proofs can be found, for instance, in [2]. We conclude this part with an original lemma that will be of particular use for the continuation of this article.

Lemma 2. *We have:*

$$c(d,n) = \sum_{\delta|(d,n)} \delta\mu(n/\delta).$$

This lemma proves moreover that the Ramanujan sums are integers.

Corollary 1. *For any integers d, n, m such that $(n,m) = 1$, we have:*

$$c(d,nm) = c(d,n)c(d,m).$$

Corollary 1 together with Remark 1 ensures that the determination of a Ramanujan sum depends only on the sums $c(p^\beta, p^\alpha)$. This enables us to give a multiplicative formula for Ramanujan sums:

Lemma 3. *For any integers d and n, we have:*

$$c(d,n) = \frac{\phi(n)\mu\big(n/(d,n)\big)}{\phi\big(n/(d,n)\big)}.$$

We present now an original lemma that will be of particular interest in our context:

Lemma 4. *Let d and n be any non-zero integers, p be a prime number, then $c(d,n) \equiv c(pd,n) \pmod{p^{\beta+1}}$, where β is the integer such that $p^\beta | d$ and $p^{\beta+1} \nmid d$.*

Proof. If $(d,n) = (pd,n)$, then from Remark 1, we have $c(d,n) = c(pd,n)$. We will from now on suppose that $(d,n) \neq (pd,n)$. Then necessarily p divides n and we have $(pd,n) = p(d,n)$. Therefore there exists an non-zero integer α such that $p^\alpha \mid n$ and $p^{\alpha+1} \nmid n$.

Moreover if we note β the integer such that $p^\beta | d$ and $p^{\beta+1} \nmid d$, we have $\beta < \alpha$.

From Lemma 3, we have:

$$c(d,n) = c(d/p^\beta, n/p^\alpha)c(p^\beta, p^\alpha),$$

and

$$c(pd,n) = c(d/p^\beta, n/p^\alpha)c(p^{\beta+1}, p^\alpha).$$

It suffices then to prove that $c(p^\beta, p^\alpha)$ and $c(p^{\beta+1}, p^\alpha)$ are equal modulo $p^{\beta+1}$. This lies on a simple application of the formula:

$$c(p^\beta, p^\alpha) = \frac{\phi(p^\alpha)\mu(p^{\alpha-\beta})}{\phi(p^{\alpha-\beta})}\,.$$

We consider the three different cases:

- If $\beta < \alpha - 2$, then $c(p^\beta, p^\alpha) = 0$ and $c(p^{\beta+1}, p^\alpha) = 0$.
- If $\beta = \alpha - 2$, then necessarily $\alpha \geqslant 2$. In this case, we have $c(p^\beta, p^\alpha) = 0$ and $c(p^{\beta+1}, p^\alpha) = -p^{\alpha-1} = -p^{\beta+1} \equiv 0 \pmod{p^{\beta+1}}$.
- If $\beta = \alpha - 1$, then $c(p^\beta, p^\alpha) = -p^{\alpha-1} = -p^\beta$ and $c(p^{\beta+1}, p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\beta+1} - p^\beta$, thus $c(p^\beta, p^\alpha) \equiv c(p^{\beta+1}, p^\alpha) \pmod{p^{\beta+1}}$.

□

3. The divisor system

In order to determine our unknowns, N_b and M_b, with $b \mid n$, we present in this section a two linear systems, that accept this numbers as their solutions.

Proposition 1. *Let $n \geqslant 3$ be an odd integer. For any divisor d of n, the $\tau(n)$ numbers N_b satisfy the equation:*

$$L_d : \sum_{b|n} c(d,b) N_{\frac{n}{b}} = \prod_{\substack{i=1 \\ (i,n)=1}}^{(n-1)/2} \left(\zeta^{id} + \zeta^{-id}\right).$$

Similarly, the $\tau(n)$ numbers M_b satisfy the equation:

$$L'_d : \sum_{b|n} c(d,b) M_{\frac{n}{b}} = \prod_{i=1}^{(n-1)/2} \left(\zeta^{id} + \zeta^{-id}\right).$$

P r o o f. By definition of the number N_x, we have:

$$\prod_{\substack{i=1 \\ (i,n)=1}}^{(n-1)/2} (\zeta^{id} + \zeta^{-id}) = \sum_{x=1}^{n} N_x \zeta^{dx} = \sum_{b|n} \sum_{\substack{x=1 \\ (x,n)=\frac{n}{b}}}^{n} N_x \zeta^{dx}.$$

Using Lemma 1, we know that all the N_x in the second sum are equal to $N_{\frac{n}{b}}$. We can factorize by $N_{\frac{n}{b}}$ and rewrite the sum on the multiples of $\frac{n}{b}$.

$$= \sum_{b|n} N_{\frac{n}{b}} \sum_{\substack{i=1 \\ (i,b)=1}}^{b} \zeta^{di\frac{n}{b}} = \sum_{b|n} N_{\frac{n}{b}} \sum_{\substack{i=1 \\ (i,b)=1}}^{b} \left(\zeta^{\frac{n}{b}}\right)^{di}.$$

Since ζ is a primitive n-th root of unity, for any b dividing n, $\zeta^{\frac{n}{b}}$ is a primitive b-th root of unity. Thus we recognize in the last sum the definition of $c(d,b)$.

$$= \sum_{b|n} c(d,b) N_{\frac{n}{b}}.$$

Similarly, by definition of the M_x and the same computation, we have:

$$\begin{aligned} \prod_{i=1}^{(n-1)/2} (\zeta^{id} + \zeta^{-id}) &= \sum_{x=1}^{n} M_x \zeta^{dx} = \sum_{b|n} \sum_{\substack{x=1 \\ (x,n)=\frac{n}{b}}}^{n} M_x \zeta^{dx} \\ &= \sum_{b|n} M_{\frac{n}{b}} \sum_{\substack{i=1 \\ (i,b)=1}}^{b} \zeta^{di\frac{n}{b}} = \sum_{b|n} c(d,b) M_{\frac{n}{b}}. \end{aligned}$$

□

For each family $(N_b)_{b|n}$ and $(M_b)_{b|n}$, we have a linear system of $\tau(n)$ equations with $\tau(n)$ unknowns. In these two systems, the coefficients of the unknowns are the same, only the constant differ. The following proposition will ensure that it would bring us, in both cases, to a complete determination of the N_b and M_b.

Proposition 2. *Let $n \geqslant 3$ be an odd number, we have:*

$$\left|\left(c(d,b)\right)_{\substack{d|n\\b|n}}\right| = \prod_{d|n} d = n^{\tau(n)/2},$$

and this determinant is non null.

Moreover, we have:

$$\left(c(d,b)\right)^{-1}_{\substack{d|n\\b|n}} = \frac{1}{n}\left(c\left(\frac{n}{d},\frac{n}{b}\right)\right)_{\substack{d|n\\b|n}}.$$

The index set of our matrices and vectors are the divisors of n, in the following we will consider these divisors in increasing order.

P r o o f. Let D be the diagonal matrix of order $\tau(n)$, where $D_{d,d} = d$. Naturally $|D| = \prod_{d|n} d = n^{\tau(n)/2}$.

Let us now consider the characteristic matrix of divisibility:

$$\chi = \begin{pmatrix} 1 & \cdots & \epsilon(d,b) \\ & \ddots & \vdots \\ (0) & & 1 \end{pmatrix},$$

where $\epsilon(d,b) = 1$ if $d \mid b$ and $\epsilon(d,b) = 0$ otherwise. Naturally, as χ is a triangular matrix with only 1 on its diagonal, we have: $|\chi| = 1$.

Moreover, from the definition of the Möbius function μ, we easily can compute χ^{-1}:

$$\chi^{-1} = \begin{pmatrix} 1 & \cdots & \epsilon'(d,b) \\ & \ddots & \vdots \\ (0) & & 1 \end{pmatrix},$$

where $\epsilon'(d,b) = \mu(b/d)$ if $d \mid b$ and $\epsilon'(d,b) = 0$ otherwise.

The result holds on the product $\chi^{\mathrm{t}} \cdot D \cdot \chi^{-1}$.

First, we can compute the product:

$$\chi^{\mathrm{t}} \cdot D = \begin{pmatrix} 1 & & (0) \\ \vdots & \ddots & \\ m(d,b) & \cdots & n \end{pmatrix},$$

where $m(d,b) = b$ if $b \mid d$ and $m(d,b) = 0$ otherwise.

Therefore, if we denote $C = \chi^{\mathrm{t}} \cdot D \cdot \chi^{-1}$, we have $C_{d,b} = \sum_{\substack{\delta \mid d \\ \delta \mid b}} \delta \mu(b/\delta)$

From Lemma 2, we have $C_{d,b} = c(d,b)$. Consequently:

$$\left| \left(c(d,b) \right)_{\substack{d \mid n \\ b \mid n}} \right| = \left| \chi^{\mathrm{t}} \cdot D \cdot \chi^{-1} \right| = \left| \chi^{\mathrm{t}} \right| \, \left| D \right| \, \left| \chi^{-1} \right| = \left| \prod_{d \mid n} d \right|.$$

We will denote D' the diagonal matrix with $D'_{d,d} = \frac{n}{d}$. It is clear that $D^{-1} = \frac{1}{n} D'$. Therefore, we have:

$$C^{-1} = \frac{1}{n} \chi \cdot D' \cdot (\chi^{-1})^{\mathrm{t}}.$$

The product $\chi.D'$ gives the matrix:

$$\chi \cdot D' = \begin{pmatrix} n & \cdots & m'(d,b) \\ & \ddots & \vdots \\ (0) & & 1 \end{pmatrix},$$

where $m'(d,b) = \frac{n}{b}$ if $d \mid b$ and $m'(d,b) = 0$ otherwise. The matrix $(\chi^{-1})^{\mathrm{t}}$ is:

$$(\chi^{-1})^{\mathrm{t}} = \begin{pmatrix} 1 & & (0) \\ \vdots & \ddots & \\ \epsilon''(d,b) & \cdots & 1 \end{pmatrix}$$

where $\epsilon''(d,b) = \mu(d/b)$ if $b \mid d$ and $\epsilon''(d,b) = 0$ otherwise.

Therefore:

$$C^{-1}_{d,b} = \frac{1}{n} \sum_{\substack{\delta / d \mid \delta \\ b \mid \delta}} \frac{n}{\delta} \mu(\delta/b)$$

Changing the index δ to n/δ':

$$= \frac{1}{n} \sum_{\substack{\delta' \mid \frac{n}{d} \\ \delta' \mid \frac{n}{b}}} \delta' \mu\left(\frac{n}{b\delta'} \right)$$

Using Lemma 2, we conclude:

$$= \frac{1}{n} c\left(\frac{n}{d}, \frac{n}{b} \right).$$

□

Remark 2. Given two divisors d and b of n, the product of C and C^{-1} leads to the well-known orthogonality property (Theorem 2.8 in [2]):

$$\sum_{\delta|n} c\left(d,\frac{n}{\delta}\right) c\left(\delta,\frac{n}{b}\right) = \begin{vmatrix} n & \text{if } d=b,\\ 0 & \text{otherwise.}\end{vmatrix}$$

4. The products

The goal of this section is the simplification of the products:

$$a_n(d) = \prod_{\substack{i=1\\(i,n)=1}}^{(n-1)/2} \left(\zeta^{id}+\zeta^{-id}\right) \quad \text{and} \quad b_n(d) = \prod_{i=1}^{(n-1)/2} \left(\zeta^{id}+\zeta^{-id}\right).$$

In this part the oddness of n plays a crucial point.

By Proposition 1, this products can be defined as a linear combination of integers $a_n(d) = \sum_{b|n} c(d,b)N_{\frac{n}{b}}$ and $b_n(d) = \sum_{b|n} c(d,b)M_{\frac{n}{b}}$, thus they are elements of $\mathbb{Z}$.

Lemma 5. *Let $n \geqslant 3$ be an odd number and d a divisor of n, we have:*

$$\textit{if} \quad d \neq n : a_n(d) \in \{-1,1\}, \quad \textit{else}: \quad a_n(n) = 2^{\phi(n)/2},$$
$$\textit{and} \quad b_n(d) = 2^{(d-1)/2} b_{\frac{n}{d}}(1), \quad \textit{and} \quad b_n(1) \in \{-1,1\}.$$

P r o o f. The n-th root of unity ζ is an integer of the ring $\mathbb{Q}(\zeta)$, this is also the case of ζ^{-1}. Thus for any integer i, $\zeta^i+\zeta^{-i}$ is an integer of $\mathbb{Q}(\zeta)$.

If $n \mid i$, naturally, $\zeta^i+\zeta^{-i} = 2$. This already gives the determination of $a_n(n) = 2^{\phi(n)/2}$ and $b_n(n) = 2^{(n-1)/2}$ because all factors in this products are equal to 2.

If $n \nmid i$ then $n \nmid 2i$, which implies that $\zeta^{2i} \neq 1$. We consider the following product: (Notice that as n is odd, $2n-2 \equiv 0 \mod 4$.)

$$\begin{aligned}(\zeta^i+\zeta^{-i})\left(\sum_{j=0}^{(2n-2)/4} \zeta^{(4j+1)i}\right) &= \sum_{j=0}^{(2n-2)/4} \zeta^{(4j+2)i} + \sum_{j=0}^{(2n-2)/4} \zeta^{(4j)i}\\ &= \sum_{j=0}^{n} \zeta^{2ji} = \frac{1-\zeta^{2n+2i}}{1-\zeta^{2i}} = 1.\end{aligned}$$

Therefore $\zeta^i+\zeta^{-i}$ is a unit of $\mathbb{Q}(\zeta)$.

If we consider a divisor $d \neq n$ of n and the product $a_n(d) = \prod_{\substack{i=1\\(i,n)=1}}^{(n-1)/2} \left(\zeta^{id}+\zeta^{-id}\right)$,

we observe that the condition $(i,n)=1$ implies that each factor is a unit of $\mathbb{Q}(\zeta)$. The product being an element of $\mathbb{Z}$, it belongs to $\{-1,1\}$.

If we consider a divisor $d \neq n$ of n and the product $b_n(d)=\prod_{i=1}^{(n-1)/2}\left(\zeta^{id}+\zeta^{-id}\right)$, we observe that the indices i for which $n \mid id$, are the $(d-1)/2$ multiples of $\frac{n}{d}$ that belong to $\left[1,(n-1)/2\right]$. Therefore the product $b_n(d)$ is the product of $2^{(d-1)/2}$, with a product of units $b'_n(d)=\prod_{\substack{i=1\\ \frac{n}{d}\nmid i}}^{(n-1)/2}\left(\zeta^{id}+\zeta^{-id}\right)$. Since $b_n(d)$ is an element of $\mathbb{Z}$, $b'_n(d)$ belongs to $\{-1,1\}$.

It remains to prove that $b'_n(d)=b_{\frac{n}{d}}(1)$. In order to establish this, we observe that if $\frac{n}{d}\nmid i$:

$$\zeta^{id}+\zeta^{-id}=\zeta^{d(i+\frac{n}{d})}+\zeta^{-d(i+\frac{n}{d})}=\zeta^{d(\frac{n}{d}-i)}+\zeta^{-d(\frac{n}{d}-i)}.$$

Therefore, decomposing the product that define $b'_n(d)$, we have:

$$\begin{aligned} b'_n(d)=\prod_{\substack{i=1\\ \frac{n}{d}\nmid i}}^{\frac{n-1}{2}}\left(\zeta^{id}+\zeta^{-id}\right) &= \left(\prod_{i=1}^{(\frac{n}{d}-1)/2}\left(\left(\zeta^{d}\right)^{i}+\left(\zeta^{d}\right)^{-i}\right)\right)^{2((d-1)/2)+1} \\ &= \left(b_{\frac{n}{d}}(1)\right)^{2((d-1)/2)+1}=b_{\frac{n}{d}}(1). \end{aligned}$$

The last equality is due to the fact that $b_{\frac{n}{d}}(1)\in\{-1,1\}$. □

To give a further determination of our products $a_n(d)$ and $b_n(d)$, we will need the following lemma. In its proof, we use the classical result that gives precision of the multiplicative structure of cyclic group, this is fully explained in [1].

Lemma 6. *Let $n \geqslant 3$ be an odd number, we have:*

$$2^{\phi(n)/2}\equiv\left|\begin{array}{ll} 1 & \bmod n \quad \textit{if there is two distinct primes dividing } n \\ \left(\frac{2}{p}\right) & \bmod n \quad \textit{if } n=p^{\alpha}. \end{array}\right.$$

Proof. Let us first consider the case where n is the power of a odd prime number $n=p^{\alpha}$. The group $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{*}$ is a cyclic group of order $\phi(p^{\alpha})$, so $2^{\phi(p^{\alpha})/2} \mod p^{\alpha}$ belongs to $\{-1,1\}$. Moreover, we have:

$$2^{\phi(p^{\alpha})/2}=2^{p^{\alpha-1}(p-1)/2}=\left(2^{(p-1)/2}\right)^{p^{\alpha-1}}$$

But this last expression is $\left(\left(\frac{2}{p}\right)\right)^{p^{\alpha-1}}\equiv\left(\frac{2}{p}\right) \pmod p$, because p is an odd prime. Then necessarily we have:

$$2^{\phi(p^{\alpha})/2}\equiv\left(\frac{2}{p}\right)\pmod{p^{\alpha}}.$$

Let us now consider the case where there are two distinct primes dividing n. Let $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ be the decomposition of n as a product of primes. As there are at least two distinct primes dividing n, we have $s \geqslant 2$.

The group $(\mathbb{Z}/n\mathbb{Z})^*$ is isomorphic to the product of the cyclic groups $\prod_{i=1}^{s} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$. Therefore the exponent e of the group $(\mathbb{Z}/n\mathbb{Z})^*$ is the least common multiple of the $\phi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1)$.

But, for any i_o from 1 to s, we have:

$$\frac{\phi(n)}{2} = p_{i_o}^{\alpha_{i_o}-1}\big(p_{i_o}-1\big)\frac{\prod_{\substack{i=1\\ i\neq i_o}}^{s} p_i^{\alpha_i-1}(p_i-1)}{2}.$$

As $s \geqslant 2$, the product in the right-hand-side is never empty. As n is odd, all the p_i's are odd prime numbers, so the fraction is an integer. We can conclude that $\frac{\phi(n)}{2}$ is a multiple of e. Finally, n being an odd number, we know that 2 belongs to $(\mathbb{Z}/n\mathbb{Z})^*$ and consequently, we have:

$$2^{\phi(n)/2} \equiv 1 \pmod{n}.$$

□

We define the function χ_2:

$$\chi_2 : \left| \begin{array}{ccc} 2\mathbb{N}^* + 1 & \to & \{-1, 1\} \\ n & \mapsto & \left| \begin{array}{ll} 1 & \text{if there are two distinct primes dividing } n \\ \left(\frac{2}{p}\right) & \text{if } n = p^{\alpha}. \end{array} \right. \end{array} \right.$$

Now, with the help of this last lemma and the definition of function χ_2, we can give a full determination of the products $a_n(d)$ and $b_n(d)$:

Proposition 3. *Let $n \geqslant 3$ be an odd number and d a divisor of n, we have:*

$$\textit{if} \quad d \neq n : a_n(d) = \chi_2(n), \quad \textit{else} : \quad a_n(n) = 2^{\phi(n)/2},$$

$$\textit{and} \quad b_n(d) = \left(\frac{2}{\frac{n}{d}}\right) 2^{(d-1)/2}.$$

Proof. Let us first consider the case of the numbers $a_n(d)$. Lemma 4 proves that for a prime p and any integers d and b, we have: $c(d, b) \equiv c(pd, b) \pmod{p}$. Then for a prime p dividing n and for any other divisor d of n:

$$\sum_{b|n} c(d, b) N_{\frac{n}{b}} \equiv \sum_{b|n} c(pd, b) N_{\frac{n}{b}} \pmod{p}.$$

What means that $a_n(d) \equiv a_n(pd) \pmod{p}$.

Moreover, we already have proven in Lemma 5 that:

- $a_n(n) = 2^{\phi(n)/2}$
- if $d \neq n$ $a_n(d) \in \{-1, 1\}$.

Lemma 6 shows $a_n(n) \equiv \chi_2(n) \pmod{n}$, therefore for any prime divisor p of n, we also have $a_n(n) \equiv \chi_2(n) \pmod{p}$. An induction on the divisors of n proves that for any divisor d of n, $d \neq n$, we have $a_n(d) = \chi_2(n)$.

Let us now consider the case of $b_n(d)$. Since we have proven in Lemma 5 that $b_n(d) = 2^{(d-1)/2} b_{\frac{n}{d}}(1)$, it suffices to calculate $b_n(1)$:

$$b_n(1) = \prod_{i=1}^{(n-1)/2} \left(\zeta^i + \zeta^{-i}\right) = \prod_{d|n} \prod_{\substack{i=1 \\ (i,n)=d}}^{(n-1)/2} \left(\zeta^i + \zeta^{-i}\right)$$

$$= \prod_{d|n} \prod_{\substack{i=1 \\ (i,\frac{n}{d})=1}}^{(\frac{n}{d}-1)/2} \left(\left(\zeta^d\right)^i + \left(\zeta^d\right)^{-i}\right)$$

Since ζ^d is a $\frac{n}{d}$-th root of unity, we recognize in the inner product the definition of $a_{\frac{n}{d}}(1)$:

$$= \prod_{d|n} a_{\frac{n}{d}}(1) = \prod_{d|n} a_d(1) = \prod_{\substack{p \text{ prime} \\ p^\alpha | n \\ p^{\alpha+1} \nmid n}} \left(\frac{2}{p}\right)^\alpha$$

What is the definition of the Jacobi symbol:

$$= \left(\frac{2}{n}\right).$$

□

Remark 3. The last computation of $b_n(1)$ stands on the context of our system, but it can be computed directly. Indeed, $b_n(1)$ can be interpreted as a product of cosinus:

$$b_n(1) = 2^{(n-1)/2} \prod_{i=1}^{(n-1)/2} \cos(2i\pi/n).$$

Since we already know that it is an element of $\{-1, 1\}$, it suffices to count the number of negative factors. We deduce from this count the exact same formula for the numbers $b_n(d)$.

5. Conclusion

With all the tools that have been prepared in the previous sections, we are ready to present the proofs of Theorem 2 and 3:

5.1. Proofs of Theorem 2 and 3

P r o o f o f T h e o r e m 2. From Lemma 1, it suffices to determine the $\tau(n)$ numbers N_b, with $b \mid n$. If we note N the vector $(N_n, \dots, N_1)^{\mathrm{t}}$, that holds $\tau(n)$ coordinates $N_{\frac{n}{b}}$ indexed on the divisor of n, C the $\tau(n) \times \tau(n)$ matrix $\big(c(d,b)\big)_{\substack{d|n \\ b|n}}$ and A the vector $\big(a_n(1), \dots, a_n(n)\big)^{\mathrm{t}}$. Proposition 1 gives the relation:

$$C.N = A\,.$$

Since Proposition 2 proves that the matric C is invertible and that $C^{-1} = \frac{1}{n}\big(c(\frac{n}{d}, \frac{n}{b})\big)_{\substack{d|n \\ b|n}}$, we have the relation: $C^{-1}.A = N$.

Moreover from Proposition 3, A is the sum of the two vectors

$$A_1 = \chi_2(n)(1, \dots, 1) \text{ and } A_2 = \big(0, \dots, 0, 2^{\phi(n)/2} - \chi_2(n)\big)^{\mathrm{t}}.$$

Then N is the sum of the two vectors $C^{-1}.A_1$ and $C^{-1}.A_2$.

Since for any divisor d of n, $c(d,1) = 1$, the vector A_1 is colinear to the first column of C, then $C^{-1}.A_1 = \big(\chi_2(n), 0, \dots, 0\big)^{\mathrm{t}}$. Moreover, for any divisor d of n, $c(\frac{n}{d}, \frac{n}{n}) = c(\frac{n}{d}, 1) = 1$, the last column of C^{-1} is $\frac{1}{n}(1, \dots, 1)^{\mathrm{t}}$. Thus, we have $C^{-1}.A_2 = \frac{1}{n}\big(2^{\phi(n)/2} - \chi_2(n)\big)(1, \dots, 1)^{\mathrm{t}}$.

Finally, we have:

$$\begin{pmatrix} N_n \\ \vdots \\ N_1 \end{pmatrix} = \begin{pmatrix} \frac{1}{n}\left(2^{\phi(n)/2} - \chi_2(n)\right) + \chi_2(n) \\ \frac{1}{n}\left(2^{\phi(n)/2} - \chi_2(n)\right) \\ \vdots \\ \frac{1}{n}\left(2^{\phi(n)/2} - \chi_2(n)\right) \end{pmatrix}.$$

□

Theorem 3 gives an exact formula for the numbers M_x and an upper bound for the difference to their mean.

P r o o f o f T h e o r e m 3. From Lemma 1, it suffices to determine the $\tau(n)$ numbers M_b, with $b \mid n$. If we note M the vector $(M_n, \dots, M_1)^{\mathrm{t}}$, that holds $\tau(n)$ coordinates $M_{\frac{n}{b}}$ indexed on the divisor of n, C the $\tau(n) \times \tau(n)$ matrix $\big(c(d,b)\big)_{\substack{d|n \\ b|n}}$ and B the vector $\big(b_n(1), \dots, b_n(n)\big)^{\mathrm{t}}$. Proposition 1 gives the relation:

$$C.M = B.$$

Since Proposition 2 proves that the matrix C is invertible and that $C^{-1} = \frac{1}{n}\big(c\left(\frac{n}{d},\frac{n}{b}\right)\big)_{\substack{d|n\\b|n}}$, we have the relation: $C^{-1}.B = M$.

Propositions 2 and 3 give $M_{\frac{n}{d}} = \frac{1}{n}\sum_{b|n} c\big(\frac{n}{d},\frac{n}{b}\big)\left(\frac{2}{\frac{n}{b}}\right)2^{(b-1)/2}$, what can be rewritten:

$$M_d = \frac{1}{n}\sum_{b|n} c\big(d,b\big)\left(\frac{2}{b}\right)2^{\left(\frac{n}{b}-1\right)/2}.$$

Remark 1 asserts that for any $x \in \mathbb{Z}/n\mathbb{Z}$, we have: $c(x,n) = c\big((x,n),n\big)$. Thus for any $x \in \mathbb{Z}/n\mathbb{Z}$, we have:

$$M_x = \frac{1}{n}\sum_{b|n} c(x,b)\left(\frac{2}{b}\right)2^{\left(\frac{n}{b}-1\right)/2}.$$

The term of this sum that is given for the divisor 1 of n, is the mean part: $\frac{1}{n}2^{(n-1)/2}$. Let us note $R_x = M_x - \frac{1}{n}2^{(n-1)/2} = \frac{1}{n}\sum_{\substack{b|n\\b\neq 1}} c\big(x,b\big)\left(\frac{2}{b}\right)2^{\left(\frac{n}{b}-1\right)/2}$. We can evaluate the ratio $\frac{R_x}{2^{\left(\frac{n}{p(n)}-1\right)/2}}$:

$$\left|\frac{R_x}{2^{(\frac{n}{p(n)}-1)/2}}\right| = \left|\frac{1}{n}\sum_{\substack{b|n\\b\neq 1}} c(x,b)\left(\frac{2}{b}\right)2^{\left(\frac{n}{b}-1\right)/2-\left(\frac{n}{p(n)}-1\right)/2}\right|$$
$$\leqslant \frac{1}{n}\sum_{\substack{b|n\\b\neq 1}}\big|c(x,b)\big|2^{\frac{n}{2}\left(\frac{1}{b}-\frac{1}{p(n)}\right)}$$

Since $p(n)$ is the least prime divisor of n, for any divisor $b \neq 1$ of n, we have $\frac{1}{b} - \frac{1}{p(n)} \leqslant 0$. Thus, we have the inequality:

$$\leqslant \frac{1}{n}\sum_{\substack{b|n\\b\neq 1}}\big|c(x,b)\big|$$

Since $c(x,b)$ is by definition a sum of $\phi(b)$ numbers of modulus 1, we have: $\big|c(x,b)\big| \leqslant \phi(b)$, then:

$$\leqslant \frac{1}{n}\sum_{\substack{b|n\\b\neq 1}}\phi(b) < 1.$$

□

Notice that if n is a prime number, then for any $x \in \mathbb{Z}/n\mathbb{Z}$ we have $N_x = M_x$ and Theorem 3 asserts that the difference $|M_x - \frac{1}{n}2^{(n-1)/2}|$ is less than 1, this is also what Theorem 2 asserts. Moreover, we have:

$$0 < \frac{2^{\left(\frac{n}{p(n)}-1\right)/2}}{\frac{1}{n}2^{(n-1)/2}} = n2^{\frac{n}{2}\left(\frac{1}{p(n)}-1\right)}$$

Since n is an odd number, $p(n) \geqslant 3$, then:

$$\leqslant n2^{-\frac{n}{3}} \xrightarrow[n\to\infty]{} 0.$$

This statement allows us to consider Theorem 3 as a theorem of equidistribution.

5.2. Comments on generalizations

The case of any finite abelian ring of odd cardinality can also be discussed, but a simple calculation in the ring $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ proves that there is not equidistribution on the elements of the sums $\sum \pm i$, where i belongs to a set of representatives of all classes modulo the multiplicative subgroup $\{1, -1\}$. Nevertheless an equivalent of Lemma 1 remains true in this context.

When n is an even number, in the cyclic group of order n, it is clear that all sums $\pm 1 \cdots \pm i \cdots \pm (n-2)/2$ or $\pm 1 \cdots \pm n/2$ have the same parity, therefore at most half of the residue classes modulo n can accept such a writing and a result of equirepartition cannot be expected. Moreover a result of strict equirepartition restricted on the elements of the same parity is generaly false. Strangely, in the case of a power of 2, the non-zero numbers M_x are all equal, while the non-zero numbers N_x are not. This will be the subject of a further work.

Acknowledgements. The author would like to thank A. Chadozeau for his helpfull comments.

Annex

We give here some examples of the systems we solve in this article: The system that appears in [3] holds for a prime p:

$$\left|\begin{array}{lcl} N_p - N_1 & = & (\frac{2}{p}) \\ N_p + (p-1)N_1 & = & 2^{(p-1)/2}. \end{array}\right.$$

We give two characteristic examples: The first one is the case where n is the cube of a odd prime, $n = p^3$.

$$\left|\begin{array}{lllll} N_{p^3} & -N_{p^2} & & & = \left(\frac{2}{p}\right) \\ N_{p^3} & +(p-1)N_{p^2} & -pN_p & & = \left(\frac{2}{p}\right) \\ N_{p^3} & +(p-1)N_{p^2} & +(p^2-p)N_p & -p^2N_1 & = \left(\frac{2}{p}\right) \\ N_{p^3} & +(p-1)N_{p^2} & +(p^2-p)N_p & +(p^3-p^2)N_1 & = 2^{p^2(p-1)/2}. \end{array}\right.$$

The second example is the case where n is the product of two distinct primes, $n = pq$.

$$\left|\begin{array}{llllll} N_{pq} & -N_p & -N_q & +N_1 & = & 1 \\ N_{pq} & +(q-1)N_p & -N_q & -(q-1)N_1 & = & 1 \\ N_{pq} & -N_p & +(p-1)N_q & -(p-1)N_1 & = & 1 \\ N_{pq} & +(q-1)N_p & +(p-1)N_q & +(q-1)(p-1)N_1 & = & 2^{(q-1)(p-1)/2}. \end{array}\right.$$

We can also consider the corresponding systems for the M_d: The first one, $n = p^3$:

$$\left|\begin{array}{lllll} M_{p^3} & -M_{p^2} & & & = \left(\frac{2}{p}\right) \\ M_{p^3} & +(p-1)M_{p^2} & -pM_p & & = 2^{(p-1)/2} \\ M_{p^3} & +(p-1)M_{p^2} & +(p^2-p)M_p & -p^2M_1 & = 2^{(p^2-1)/2}\left(\frac{2}{p}\right) \\ M_{p^3} & +(p-1)M_{p^2} & +(p^2-p)M_p & +(p^3-p^2)M_1 & = 2^{(p^3-1)/2}. \end{array}\right.$$

The second one, $n = pq$:

$$\left|\begin{array}{llllll} M_{pq} & -M_p & -M_q & +M_1 & = & \left(\frac{2}{pq}\right) \\ M_{pq} & +(q-1)M_p & -M_q & -(q-1)M_1 & = & 2^{(q-1)/2}\left(\frac{2}{p}\right) \\ M_{pq} & -M_p & +(p-1)M_q & -(p-1)M_1 & = & 2^{(p-1)/2}\left(\frac{2}{q}\right) \\ M_{pq} & +(q-1)M_p & +(p-1)M_q & +(q-1)(p-1)M_1 & = & 2^{(pq-1)/2}. \end{array}\right.$$

REFERENCES

[1] MARCUS, D.A.: *Number Fields*, Universität text, Springer-Verlag, VIII, New York-Heidelberg, 1977.

[2] MCCARTHY P.J.: *Introduction to Arithmetical Functions*, Universität text, Springer-Verlag, VII, New York 1986.

[3] MYERSON, G.: *A combinatorial problem in finite fields, I*, Pacific J. Math. **82** (1979), 179-187.
[4] MYERSON, G.: *A combinatorial problem in finite fields, II*, Quart. J. Math. Oxford Ser. (2), **31** (1980), no. 122, 219-231.

Received June 14, 2007
Accepted July 15, 2007

Éric Balandraud
Université Bordeaux 1
Institut de Mathématiques
de Bordeaux UMR 5251
Batimet A33, equipe A2X,
351 Cours de la liberation
F 33405 Talence Cedex
FRANCE
E-mail: Eric.Balandraud@math.u-bordeaux1.fr