A Note on Radamacher Cycles

Antonio Lascurain Orive
lasc@fciencias.unam.mx

Abstract. It is proved that the fields $\mathbb{Z}_p$, $p$ a prime number, can be partitioned into subsets of cardinality three if $p \equiv 2 \mod 3$ (omitting the neutral elements). The subsets are formed by numbers which are related to each other by taking the successor of the dual in an iterated way. The same theorem holds if $p \equiv 1 \mod 3$, except that in this case there are also two equivalence classes of length one. These results are closely related with the Hecke congruence subgroups.

Mathematics Subject Classification: Primary 20H05, 11T30; Secondary 11F06, 12Y05, 11T99, 12E20, 30F35

Keywords: Finite fields, cycle, dual, Radamacher

1. It is well known that the units in $\mathbb{Z}_p$, $p$ a prime number, form a multiplicative cyclic group, however these fields have also other patterns of cyclicity. We show that these fields have remarkable cyclic properties determined by duality and successors. These features are also shared, in some ways, with the rings $\mathbb{Z}_m$, $m \in \mathbb{N}$. It is quite possible that Radamacher [5] was aware of this cyclic properties when he exhibited presentations for the fuchsian groups $\Gamma_0(p)$, $p$ a prime number, that is the transformation group associated to the group of matrices

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid c \equiv 0 \mod p \right\}.$$

Nevertheless, some of the facts described in this note Radamacher only used them as tools and examples and did not stated them as theorems. On the other hand, his work on the presentations of these subgroups of the classical modular group has been superseded by being generalized to the case $\Gamma_0(m)$, $m \in \mathbb{N}$, by Chuman [1] and the author [3]. The last statement follows because the technics
used in all the papers mentioned above are derived from the Reidemeister-
Schreier rewriting process method.

2. One needs some definitions to state the main result. In this paper there will
be no ambiguity in denoting an integer in $\mathbb{Z}$ with the same symbol as its equiva-

cence class in $\mathbb{Z}_m$, so we will do so. Usually, we will take as representatives
in these rings (or fields) the numbers $0, 1, \ldots, m - 1$.

Definition 1 The dual of the number $a \in \mathbb{Z}_p$, $p$ a prime number, $a \neq 0$, is
the only element $b \in \mathbb{Z}_p$, such that

$$ab = -1 \quad \text{in} \quad \mathbb{Z}_p.$$  

The dual $b$ will be denoted by $a^*$.  

Definition 2 The successor of the number $a \in \mathbb{Z}_m$, $m \in \mathbb{N}$, is $a + 1$, if
$a \neq m - 1$, and it is 0, if $a = m - 1$.

Definition 3 Given two numbers $a_1, a_n \in \mathbb{Z}_p - \{0, 1\}$, $a_1$ is related to $a_n$, if
there exists other numbers $a_2, a_3, \ldots, a_{n-1}$ in $\mathbb{Z}_p - \{0, 1\}$, such that
$a_{j+1} = a_j^* + 1$ for all $j \in \{1, 2, \ldots, n - 1\}$.

Now we can state the main result.

Theorem. The relation in Definition 3 is an equivalence relation. Moreover,

a) if $p \equiv 2 \mod 3$ all equivalence classes consist of exactly three numbers;

b) if $p \equiv 1 \mod 3$ there are exactly two classes that consist of just one
number, all the others have cardinality three.

Observe that what the theorem says is that (excluding two numbers, for the
case $p \equiv 1 \mod 3$) if one starts with any non neutral element in $\mathbb{Z}_p$, and
then one takes the successor of the dual in an iterated way, one always returns
to the original number after three steps. This behavior hence provides a cyclic
property of these fields. It is convenient to show a couple of simple examples
before proceeding. For the case of $\mathbb{Z}_5$, there is exactly one equivalence class
of length three $\{2, 3, 4\}$, since $2^* = 2$, $3^* = 3$ and $4^* = 1$. Whereas for $\mathbb{Z}_7$,
one has the equivalence classes $\{2, 4, 6\}$, $\{5\}$ and $\{3\}$. This follows, since
$2^* = 3$, $4^* = 5$, and $6^* = 1$.

3. In order to prove the theorem one needs first to introduce some terminology
and a couple of lemmas.

Given an element $t \in \mathbb{Z}_p - \{0, 1\}$, we write $t_1$ for $t^* + 1$, that is the successor
of the dual, also we denote $t_2 = t_1^* + 1$, and so on. The subset of $\mathbb{Z}_p - \{0, 1\}$

$$\{t, t_1, t_2, \ldots\}$$

constructed this way will be called a cycle.
Lemma 1. Under the hypothesis of the Theorem, all cycles have at most three elements.

Proof. This result is a consequence of a more general result: Given any field $K$ one may define a function $f : K - \{0, 1\} \to K - \{0, 1\}$ by the association $x \to 1 - x^{-1}$, where $0, 1$ denote the neutral elements in the field. Under these hypothesis, a calculation shows that for all non neutral elements in the field, one has that

$$f(f(f(x))) = x.$$  

* Applying this general principle to our context, one proves the lemma. \qed

It is not difficult to check that the relation * also implies that the cycles can not have length two, so all cycles are formed by one or three elements. The next step is to discuss the equation in $\mathbb{Z}_p$

$$t_1 = t.$$  

This means $t^* + 1 = t$ or $t^* = t - 1$, that is

$$(t - 1) t \equiv -1 \mod p,$$

and changing variables

$$s(s + 1) = -1 \in \mathbb{Z}_p.$$  

** Hence, the question is: when consecutive numbers are dual?

It is a remarkable fact that in the general case $m \in \mathbb{N}$, the solutions to the equation ** in $\mathbb{Z}_m$ are in a one to one correspondence with the elliptic points of order three of the Riemann surfaces defined by the Hecke congruence subgroups $\overline{\Gamma}_0(m)$, see [6], [7] and [2]. The next result appears in [2], however for the sake of completeness a proof is included here.

Lemma 2. Given $m$ an odd natural number, there is a bijective correspondence between the square roots of $-3$ in $\mathbb{Z}_m$ and the solutions of the equation ** in $\mathbb{Z}_m$.

Proof. Given $s \in \mathbb{Z}_m$ such that accomplishes ** in $\mathbb{Z}_m$, we prove that $2s + 1$ is a square root of $-3$ in $\mathbb{Z}_m$, and that all such square roots arise this way. The relation ** can be read as $m \mid s^2 + s + 1$. Also

$$m \mid 4s^2 + 4s + 4 = (2s + 1)^2 + 3.$$  

Hence, $2s + 1$ is a square root of $-3$. The association $\psi(s) = 2s + 1$ is clearly injective, to check surjectivity observe that given an odd square root $u$ of $-3$ in $\mathbb{Z}_m$, writing $u = 2s + 1$, the above reasoning also shows that

$$s = \frac{u - 1}{2}$$
A. Lascurain Orive

is a solution to the equation ** in $\mathbb{Z}_m$, and of course $\psi(s) = u$. Whereas, if $u$ is an even square root of $-3$, writing $u + m = 2s + 1$, one gets

$$s = \frac{u + m - 1}{2},$$

is also a solution to ** in $\mathbb{Z}_m$, and $\psi(s) = u$.

Now we may proceed with the proof of the theorem.

**Proof of the Theorem.** The relation in $\mathbb{Z}_p - \{0, 1\}$ is by definition transitive. Using Lemma 1 and the remark appearing after it, it turns out that it is also reflexive and symmetric, thereby it is an equivalence relation.

Consequently, it follows from Lemma 2 that one has only to prove that $-3$ is a quadratic residue in $\mathbb{Z}_p$, if $p = 1$ in $\mathbb{Z}_3$ —and it is not otherwise—, and also that in the first case the number of solutions is exactly two. These facts may be deduced from the quadratic reciprocity law and the distributive properties of the Legendre symbol (cf. [4], Theorem 5.7 and Theorem 5.3).

4. The remarkable and beautiful structure described in the theorem for the fields $\mathbb{Z}_p$ can be generalized to the rings $\mathbb{Z}_m$, $m \in \mathbb{N}$, by extending this set to a larger one that includes some pairs of numbers. It is obtained exactly the same structure of cycles of length three (and one), defined by taking the successor of the dual. The dual of some of the elements which are not units, is a pair of numbers, others are selfdual.

These facts were found by generalizing the work of Radamacher to get presentations of $\Gamma_0(m)$, $m \in \mathbb{N}$, using the Reidemeister-Schreier method. The theory begins at the study of the double cosets in

$$\Gamma_0(m) \setminus PSL(2, \mathbb{Z}) / \Gamma_\infty,$$

where $\Gamma_\infty$ denotes the subgroup of translations of the classical modular group. By selecting the double coset classes, one is able to obtain representatives for the right cosets of $\Gamma_0(m)$ in $PSL(2, \mathbb{Z})$.

The construction of the new bigger set that includes $\mathbb{Z}_m$ becomes natural, when one gets these right cosets from the double cosets. In the process, there is a partition of the non units in $\mathbb{Z}_m$ into two sets: one of them is determined by a choice of representatives in $\mathbb{Z}_w^*$, where $w = \left(\frac{m}{d}\right)$, and $d$ runs over the proper factors of $m$. All these statements can be derived from the proof of Theorem 1 in [3]. The study of these facts would certainly enlight the knowledge of some aspects of cyclicity of the rings $\mathbb{Z}_m$, as it has been exposed here for the fields $\mathbb{Z}_p$. 

\[\Box\]
We conclude this note with two examples. In $\mathbb{Z}_{17}$, one has that $2^* = 8$, $3^* = 11$, $12^* = 7$, $4^* = 4$, $5^* = 10$, $6^* = 14$, $15^* = 9$ and $13^* = 13$. Therefore, $\mathbb{Z}_{17} - \{0, 1\}$ is partitioned into five cycles of cardinality three: $\{16, 2, 9\}$, $\{3, 12, 8\}$, $\{4, 5, 11\}$, $\{6, 15, 10\}$ and $\{7, 13, 14\}$. On the other hand, in $\mathbb{Z}_{19}$, one has $2^* = 9$, $3^* = 6$, $4^* = 14$, $7^* = 8$, $5^* = 15$, $10^* = 17$, $11^* = 12$, and $13^* = 16$. Consequently $\mathbb{Z}_{19} - \{0, 1\}$ has two cycles of length one: $\{8\}$, $\{12\}$ and five cycles of length three: $\{18, 2, 10\}$, $\{3, 7, 9\}$, $\{4, 15, 6\}$, $\{5, 16, 14\}$ and $\{13, 17, 11\}$.

References


Received: April, 2009