DOI: 10.2478/auom-2014-0004
An. Şt. Univ. Ovidius Constanţa
VERSITA
Vol. 22(1),2014, 41–44

Combinatorics on Finite Fields: the sign repartition for the quadratic residues

Şerban Bărcănescu

Abstract

In the present paper we present the equivalence between the combinatorial determination of the sign repartition for the quadratic residues and non-residues to the computation of the class number of certain quadratic extensions of the field of rationals.

1 Introduction

Let p be a prime odd number and g be a primitive root mod p, i.e. g is a fixed generator of the multiplicative cyclic group of the prime field of characteristics p , denoted by F_p^* . In what follows we fix the canonical halbsystems of the "positive" Pos(p) $= \{1, 2, ..., \frac{p-1}{2}\}$ elements and of the "negative" Neg(p)$=\{\frac{p+1}{2}, ..., p-1\} = \{-\frac{p-1}{2}, ..., -2, -1\}$ elements of the field F_p . We have the partition :

$F_p = Pos(p) \cup \{0\} \cup Neg(p)$.

Also, let $R =< g^{2k} | k = 0, 1, ..., \frac{p-3}{2} >$(residues) be the subgroup of the quadratic residues mod p and $N =< g^{2k+1} | k = 0, 1, ..., \frac{p-3}{2} >$(non-residues) be its only residue class in F_p^*. We are interested in the repartition of the elements of $R$and N between Pos(p) and Neg(p) (a sample of such a situation is given by the well-known elementary proof of the gaussian criterion for the Legendre symbol). As such, the problem can not be solved with elementary

Key Words: quadratic residues, quadratic fields, class numbers
2010 Mathematics Subject Classification: Primary:11F20, 11R11, 11R29; Secondary:11B30
Received: October, 2013.
Revised: November, 2013.
Accepted: December, 2013.

(and even not elementary) tools , but at least we can hope to solve the *enumeration* problem which naturally arises in this context.

2 Results

We begin with

Lemma 2.1. *Let d be a divisor of $p-1$ and $F_p^* = C_0 \cup C_1 \cup .... \cup C_{d-1}$ be the partition of F_p^* in residue classes after its unique subgroup C_0 of index d .Then:*

(i) for odd d : $-1 \in C_0$

(ii) for even d : $-1 \in C_0$ or $-1 \in C_{\frac{d}{2}}$

Proof. Let $-1 \in C_h$ for a certain $h(mod\, d)$. Then $-C_h = (-1)C_h \subset C_h.C_h = C_{2h}$ and since they have equal cardinality we have $-C_h = C_{2h}$. By the same reason $-C_{2h} = C_{3h}$. But $-C_{2h} = C_h$ because of the 2-periodicity of changing the sign (sign rule in a field). Then $C_{3h} = C_h$ so $3h \equiv h(\text{mod } d)$ and it follows $2h \equiv 0 \ (\text{mod } d)$.□

In particular, for $d = 2$ we have the :

Corollary 2.1. *(erster erganzunssatz)*

With the above notations:

$-1 \in R$ if $p \equiv 1$ (mod 4) , therefore $-R = R$ and $-N = N$

$-1 \in N$ if $p \equiv 3$ (mod 4), therefore $-R = N$ and $-N = R$ □.

Let now $R^+ = R \cap Pos(p)$,$R^- = R \cap Neg(p)$,so we have the partition :

(1) $R = R^+ \cup R^-$

and similarly $N^+ = N \cap Pos(p)$, $N^- = N \cap Neg(p)$, so we have the partition :

(2)$N = N^+ \cup N^-$.

For simplicity we denote :

$a = card(R^+)$ and $b = card(N^+)$.

Proposition 2.1. *For $p \equiv 1$ (mod 4) : $a = b = \frac{p-1}{4}$.*

Proof.

Multiplication by (-1) on F_p^* has a double efect in this case :

(i) -residue = residue and - non residue= non residue (Cor. 1)

(ii) $-Pos(p) = Neg(p)$

Moreover, the multiplication by (-1) is a permutation of F_p^* so using (1) and (2), together with $a + b = \frac{p-1}{2}$ we get :

$card(R^+) = card(R^-) = card(N^+) = card(N^-)\square$

So , in case $p \equiv 1 \pmod 4$ we have a simple and complete answer concerning the enumeration of the sign repartition between the quadratic residues and non residues mod p .

However , in case $p \equiv 3 (\text{mod } 4)$ we only have the relation :

$a + b = \frac{p-1}{2}$.

In order to determine a and b in this case we need another relation, the simplest of which would be an estimation of the difference $a - b$. Let us for the moment denote by $\Delta(p)$ this difference.

Making the computations in a mathematical package (for instance, under SAGE) we easily obtain the following estimations:

$\Delta(7) = 1, \Delta(11) = \Delta(19) = \Delta(23) = \Delta(31) = \Delta(43) = \Delta(67) = \Delta(163) = \Delta(307) = 3$, $\Delta(47) = \Delta(79) = \Delta(103) = \Delta(127) = \Delta(179) = 5$, $\Delta(71) = \Delta(151) = \Delta(223) = 7$, $\Delta(59) = \Delta(83) = \Delta(107) = \Delta(139) = \Delta(199) = \Delta(211) = \Delta(283) = ... = \Delta(1423) = 9$, $\Delta(131) = \Delta(227) = \Delta(239) = ... = \Delta(111723) = 15$, $\Delta(191) = \Delta(263) = 13$,..., $\Delta(599) = 25$, ...,
$\Delta(1019) = \Delta(1439) = 39$,..., $\Delta(1399) = 27$,..., $\Delta(1427) = 45$,..., $\Delta(1447) = 23$....

As we can see, these results make plausible the following property:

(P) If $p \equiv 3 (\text{mod } 4)$ then $\Delta(p)$ is positive and odd.

In fact, the property (P) is true and more , we have the following remarkable result ([1] , ch.V, par.4,pag.346), formulated using the above notations and conventions:

Theorem 2.1. *Let p be a prime number such that $p \equiv 3$ (mod 4). Let $h = ordCl(\mathbb{Q}(\sqrt{p^*}))$ be the class number of the quadratic number field generated by $p^* = (-1)^{\frac{p-1}{2}} p$.*

Then :

(i) $h = a - b$ for $p \equiv 7$(mod 8)

(ii) $h = \frac{1}{3}(a - b)$ for $p \equiv 3$(mod 8).

Moreover , h is allways odd.$\square$

Solving the resulting linear system for a and b , whose first equation is always :

$a + b = \frac{p-1}{2}$ and the second is given by the above Theorem, we obtain:

Proposition 2.2. *The sign repartition enumeration for the quadratic residues and non residues modulo p is :*

(1) $a = b = \frac{p-1}{4}$ if $p \equiv 1$ (mod 8) or $p \equiv 5$ (mod 8)

(ii.1) $a = \frac{p-1}{4} + \frac{3}{2}h$, $b = \frac{p-1}{4} - \frac{3}{2}h$ if $p \equiv 3$ (mod 8)

(ii.2) $a = \frac{p-1}{4} + \frac{1}{2}h$, $b = \frac{p-1}{4} - \frac{1}{2}h$ if $p \equiv 7$ (mod 8)

where h is the class number of the quadratic number field $\mathbb{Q}(\sqrt{-p})$.$\square$

Remark 2.1. *Because of the linearity of the expresions above, we see that in fact the determination of the sign repartition enumeration is equivalent to the computation of the class number of the quadratic number field generated by* $\sqrt{-p}$.

If we compute h *by using the values of* a *and* b *obtained from the system* $a+b=\frac{p-1}{2}$ *and the numerical values of* $\Delta(p)=a-b$ *listed above , the values of the class number* h *result immediately and are in accordance to the usual tables of its values , e.g.:*

$h(7)=1, h(11)=1, h(19)=1, h(23)=3, h(31)=341)=1, h(47)=5, h(59)=3, h(167)=11$ *,...,*

$h(191)=13, h(599)=25, h(1019)=13, h(1439)=39$ *...* ■.

Acknowledgement.

The publication of this paper is supported by the grants PN-II-ID-WE-2012-4-161 and PN-II-ID-WE-2012-4-169.

References

[1] Z.I.Borevitch and I.R.Schafarevich-Number Theory, Academic Press, (1966).

Şerban BĂRCĂNESCU
Simion Stoilow Institute of Mathematics of the Romanian Academy, Research Unit 5, P.O. Box 1-764, Bucharest 014700, Romania
Email:Serban.Barcanescu@imar.ro