

ALEKSANDER GRZYCZUK AND JAROSŁAW GRZYCZUK

ON GENERATORS IN MULTIPLICATIVE GROUP OF THE FIELD  $Z_p$

**ABSTRACT:** *In the paper the following theorem is proved: "Let  $Z_p^*$  be the multiplicative group of the field  $Z_p$ , where  $p=2q+1$  and  $p, q$  are odd primes. Then  $2, q+1, -2^2$  and  $-(q+1)^2$  are generators in the group  $Z_p^*$  if  $p=8k+3$  and  $q, 2q-1, -q^2$  and  $-(2q-1)^2$  are generators in  $Z_p^*$  if  $p=8k+7$ ". This result is an extension of some earlier ones.*

Baum [1] has given an interesting criteria for certain primitive roots. Wilansky [2], using only the Legendre symbol, proved the following result: Let  $p$  and  $q$  are odd primes and  $p=2q+1$ . If  $q \equiv 1 \pmod{4}$ , then  $q+1$  is a primitive root modulo  $p$ , while if  $q \equiv 3 \pmod{4}$ , then  $q$  is a primitive root modulo  $p$ .

In the present note we give some extension of this result proving the following theorem:

**THEOREM.** Let  $Z_p^*$  be the multiplicative group of the field  $Z_p$ , where  $p=2q+1$  and  $p, q$  are odd primes. Then  $2, q+1, -2^2$  and  $-(q+1)^2$  are generators in the group  $Z_p^*$  if  $p=8k+3$  and  $q, 2q-1, -q^2$  and  $-(2q-1)^2$  are generators in  $Z_p^*$  if  $p=8k+7$ .

For the proof of the Theorem we need two lemmas.

**LEMMA 1.** Let  $Z_p^*$  be the multiplicative group of the field  $Z_p$  where  $p=2q+1$  and  $p, q$  are odd primes and let  $NR_p$  be the set of the quadratic non-residues modulo  $p$ . Then the set  $NR_p \setminus \{2q\}$  is

the set of all generators of the group  $Z_p^*$ .

PROOF OF LEMMA 1: Let  $R_p$  be the set of all quadratic residues modulo  $p$ . Then we have that  $R_p$  is a subgroup of  $Z_p^*$  and since  $p=2q+1$  the group  $R_p$  has the order  $q$ . If  $b \in R_p$  then  $b$  is not a generator in  $Z_p^*$ . Since

$$(2q)^{\frac{p-1}{2}} = (p-1)^q \equiv (-1)^q = -1 \pmod{p},$$

hence by Euler Theorem we get  $2q \notin NR_p$ . On the other hand we have

$$(2q)^2 = (p-1)^2 \equiv 1 \pmod{p}$$

and therefore  $2q$  has the order 2 and cannot be a generator in  $Z_p^*$ . But the group  $Z_p^*$  has exactly

$$\varphi(p-1) = \varphi(2q) = q-1$$

generators and therefore the set  $NR_p \setminus \{2q\}$  is the set of all generators in  $Z_p^*$ .

LEMMA 2. Let  $g$  be a generator of the group  $Z_p^*$  where  $p=4k+3$ . Then  $-g^2$  is also a generator in  $Z_p^*$ .

PROOF OF LEMMA 2: Let  $p=4k+3$  and  $g$  be a generator in  $Z_p^*$ . Then we have

$$Z_p^* = \{ g^k ; k=1, 2, \dots, p-1 = 4k+2 \}.$$

By Euler theorem we have

$$g^{\frac{p-1}{2}} = -1 \quad \text{and therefore} \quad g^{2k+1} = -1.$$

From last equality we get

$$(2.1) \quad -g^2 = g^{2k+3}$$

It is easy to see that  $(2k+3, 4k+2=p-1)=1$  and therefore  $g^{2k+3}$  is a generator in  $Z_p^*$  thus by (2.1) Lemma 2 follows.

PROOF OF THE THEOREM. First we remark that if  $p=2q+1$  where  $p, q$  are odd primes then  $p=4m+3$ , because for  $p=4m+1$  the equality  $p=2q+1$  is impossible. Hence  $p=8k+3$  or  $p=8k+7$ . If

$p=8k+3$  then  $\left(\frac{2}{p}\right) = -1$  and the number 2 is a quadratic non-residue modulo  $p$ . From Lemma 1 we get that 2 is a generator in  $Z_p^*$ . On the other hand we have

$$2(q+1) = 2q+2 = 2q+1+1 = p+1 \equiv 1 \pmod{p}$$

and therefore  $q+1$  is a generator in  $Z_p^*$  as the inverse element with respect to 2.

Let  $p=8k+7$ , then  $\left(\frac{2}{p}\right) = +1$  and 2 is not a generator in  $Z_p^*$ . Since there are exactly  $\varphi(p-1)$  generators in  $Z_p^*$  and the element 1 is not a generator thus there exists at least one number  $g$  such that  $(g, p-1) > 1$  and  $g$  is a generator in  $Z_p^*$ . Because  $p=2q+1$  thus  $q|p-1$  and  $(q, p-1) > 1$  and 2 is not a generator thus the number  $q$  must be a generator in  $Z_p^*$ . We have

$$q(2q-1) = q(2q+1-2) = q(p-2) \equiv -2q = 1-p \equiv 1 \pmod{p}.$$

and so  $2q-1$  is a generator in  $Z_p^*$ . The last part of assertion follows from Lemma 2 and the proof is complete.

#### REFERENCES

- [1] J.D. Baum, A note on primitive roots, Math.Mag. 38 (1965) 12-14.
- [2] A. Wilansky, Primitive roots without quadratic reciprocity, Math.Mag. 49 (1976), 146.

1. The first part of the document discusses the importance of maintaining accurate records of all transactions and activities. It emphasizes that proper record-keeping is essential for ensuring transparency and accountability in the organization's operations.

2. The second part of the document outlines the specific procedures and protocols that must be followed when conducting financial transactions. This includes details on how to properly issue invoices, process payments, and maintain accurate ledgers.

3. The third part of the document addresses the role of internal controls in preventing fraud and errors. It describes the various checks and balances that should be implemented to ensure the integrity of the organization's financial data.

4. The fourth part of the document discusses the importance of regular audits and reviews. It explains how these processes can help identify potential weaknesses in the organization's financial management and provide opportunities for improvement.

5. The fifth part of the document provides a summary of the key points discussed and offers final thoughts on the importance of maintaining high standards of financial management.

In conclusion, the document highlights the critical nature of financial management and the need for strict adherence to established procedures and protocols. It encourages all staff members to take their responsibilities seriously and to work together to ensure the organization's financial health and success.