Quasigroups and Related Systems **18** (2010), 1 − 6

Finite GS–quasigroups

Yahya Amad and M. Aslam Malik

Abstract. This paper is concerned with the determination of the set of possible orders of finite GS-quasigroups. Also some examples of finite GS-quasigroups are given.

1. Introduction

The following definition of GS-quasigroups was given by V.Volenec in [4] and [1].

Definition 1.1. A quasigroup $(Q,\cdot)$ is said to be *GS-quasigroup* (*golden section quasigroup*) if the equalities

$$\begin{aligned} aa &= a, \\ a(ab\cdot c)\cdot c &= b, \\ a\cdot(a\cdot bc)c &= b \end{aligned}$$

hold for all its elements.

The study of GS-quasigroups in [4] is motivated by:

Example 1.2. Let $\mathbb{C}$ be set of complex numbers and $*$ an operation on set $\mathbb{C}$ defined by:

$$a*b=\frac{1-\sqrt{5}}{2}a+\frac{1+\sqrt{5}}{2}b.$$

Let us regard complex numbers as points of the Euclidean plane, then the point b divides the pair a and $a*b$ in the ratio of golden section, which justifies the term of GS-quasigroups.

Here, we'll give some examples of finite GS-quasaigroups, and determine: *for which positive integer n there exists a $GS-quasigroup$ of order n?*

We require the following elementary results, whose proofs are simple.

2000 Mathematics Subject Classification:
Keywords: golden section, square free, finite quasigroup.

Lemma 1.3. *Let* $(G_1, \cdot_1), (G_2, \cdot_2), \ldots, (G_n, \cdot_n)$ *be* $GS-$ *quasigroups, and* $\circ$ *be the operation defined on* $G = G_1 \times G_2 \times \ldots \times G_n$ *by:*

$$(x_1, x_2, \ldots, x_n) \circ (y_1, y_2, \ldots, y_n) = (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2, \ldots, x_n \cdot_n y_n).$$

Then $(G, \circ)$ *is a* $GS-$ *quasigroup.*

Therefore, if GS-quasigroups of orders $k_1, k_2, \ldots, k_n$ exist, then a GS-quasigroup of order $k_1 k_2 \cdots k_n$ exists.

The following characterization of GS-quasigroups was given in [4].

Theorem 1.4. *A* $GS-$ *quasigroup on the set* Q *exists if and only if on the same set exists a commutative group* $(Q, +)$ *with an automorphism* φ *satisfying the identity*

$$(\varphi \circ \varphi)(x) - \varphi(x) - x = 0. \tag{1}$$

Then

$$a \cdot b = a + \varphi(b - a). \tag{2}$$

2. Commutative GS-quasigroups

By using Theorem 1.4 to study commutative GS-quasigroups we want to find all commutative groups $(Q, +)$ with an automorphism φ satisfying (1) and with the additional condition that the operation $\cdot$ defined by (2) is commutative. The commutativity of $\cdot$ implies

$$a + \varphi(b - a) = b + \varphi(a - b).$$

Thus

$$\varphi(b - a) - \varphi(a - b) = b - a,$$

and consequently

$$\varphi(x) + \varphi(x) = x \tag{3}$$

for all $x \in Q$.

From (1) it follows $\varphi(\varphi(x)) + \varphi(\varphi(x)) = \varphi(x) + \varphi(x) + x + x$, which by (3) gives $\varphi(x) = x + x + x$. Substituting this to (3) we get,

$$x + x + x + x + x + x = x.$$

Therefore, $x+x+x+x+x=0$ for all $x \in Q$, i.e., each element of the group $(Q,+)$ is of order 5 or 1. The only finite groups which satisfy that condition are $(\mathbb{Z}_5)^n$, and the group of order 1.

On the other hand, if $x+x+x+x+x=0$, for all $x \in Q$, then $\varphi(x)=x+x+x=-x-x$, i.e. $\varphi(x)=3x=-2x$ is an automorphism satisfying (1) and the operation defined by (2) is commutative.

Thus we have proved:

Theorem 2.1. *The only non-trivial finite commutative $GS-$ quasigroups are the quasigroups obtained in the technique described in Theorem* 1.4 *from the group* $(\mathbb{Z}_5)^n$, *for some* $n \in \mathbb{N}$.

From each group $(\mathbb{Z}_5)^n$ we obtain unique GS-quasigroup of order 5^n.

Example 2.2. From the group $(\mathbb{Z}_5)^2$ and the automorphism $\varphi(x)=3x=-2x$ we obtain the GS-quasigroup of order 25:

$\cdot_{25}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	0	3	1	4	2	15	18	16	19	17	5	8	6	9	7	20	23	21	24	22	10	13	11	14	12
1	3	1	4	2	0	18	16	19	17	15	8	6	9	7	5	23	21	24	22	20	13	11	14	12	10
2	1	4	2	0	3	16	19	17	15	18	6	9	7	5	8	21	24	22	20	23	11	14	12	10	13
3	4	2	0	3	1	19	17	15	18	16	9	7	5	8	6	24	22	20	23	21	14	12	10	13	11
4	2	0	3	1	4	17	15	18	16	19	7	5	8	21	9	22	20	23	21	24	12	10	13	11	14
5	15	18	16	19	17	5	8	6	9	7	20	23	21	24	22	10	13	11	14	12	0	3	1	4	2
6	18	16	19	17	15	8	6	9	7	5	23	21	24	22	20	13	11	14	12	10	3	1	4	2	0
7	16	19	17	15	18	6	9	7	5	8	21	24	22	20	23	11	14	12	10	13	1	4	2	0	3
8	19	17	15	18	16	9	7	5	8	6	24	22	20	23	21	14	12	10	13	11	4	2	0	3	1
9	17	15	18	16	19	7	5	8	6	9	22	20	23	21	24	12	10	13	11	14	2	0	3	1	4
10	5	8	6	9	7	20	23	21	24	22	10	13	11	14	12	0	3	1	4	2	15	18	16	19	17
11	8	6	9	7	5	23	21	24	22	20	13	11	14	12	10	3	1	4	2	0	18	16	19	17	15
12	6	9	7	5	8	21	24	22	20	23	11	14	12	10	13	1	4	2	0	3	16	19	17	15	18
13	9	7	5	8	6	24	22	20	23	21	14	12	10	13	11	4	2	0	3	1	19	17	15	18	16
14	7	5	8	6	9	22	20	23	21	24	12	10	13	11	14	2	0	3	1	4	17	15	18	16	19
15	20	23	21	24	22	10	13	11	14	12	0	3	1	4	2	15	18	16	19	17	5	8	6	9	7
16	23	21	24	22	20	13	11	14	12	10	3	1	4	2	0	18	16	19	17	15	8	6	9	7	5
17	21	24	22	20	23	11	14	12	10	13	1	4	2	0	3	16	19	17	15	18	6	9	7	5	8
18	24	22	20	23	21	14	12	10	13	11	4	2	0	3	1	19	17	15	18	16	9	7	5	8	6
19	22	20	23	21	24	12	10	13	11	14	2	0	3	1	4	17	15	18	16	19	7	5	8	6	9
20	10	13	11	14	12	0	3	1	4	2	15	18	16	19	17	5	8	6	9	7	20	23	21	24	22
21	13	11	14	12	10	3	1	4	2	0	18	16	19	17	15	8	6	9	7	5	23	21	24	22	20
22	11	14	12	10	13	1	4	2	0	3	16	19	17	15	18	6	9	7	5	8	21	24	22	20	23
23	14	12	10	13	11	4	2	0	3	1	19	17	15	18	16	9	7	5	8	6	24	22	20	23	21
24	12	10	13	11	14	2	0	3	1	4	17	15	18	16	19	7	5	8	6	9	22	20	23	21	24

2. Cyclic groups

The automorphism $\varphi(x) = mx$ (m is relatively prime to n) of the group $\mathbb{Z}_n$ satisfies (1) if and only if $m^2 - m - 1 \equiv 0(\text{mod}\, n)$.

Now by using Quadratic Reciprocity Law we want to find for which $n \in \mathbb{N}$ the quadratic congruence has solution m (in that case m and n are relatively prime).

Since $m^2 - m - 1$ is odd, n cannot be even. Therefore, it seems appropriate to begin by considering the congruence

$$m^2 - m - 1 \equiv 0(\text{mod}\, p),$$

where p is an odd prime and $gcd(1, p) = 1$. The assumption that p is an odd prime implies that $gcd(4, p) = 1$. Thus, the quadratic congruence is equivalent to

$$4(m^2 - m - 1) \equiv 0(\text{mod}\, p).$$

Now, completing the square we obtain

$$4(m^2 - m - 1) = (2m - 1)^2 - 5$$

The last quadratic congruence may be expressed as

$$(2m - 1)^2 \equiv 5(\text{mod}\, p).$$

Now, putting $y = 2m - 1$ in last congruence, we get

$$y^2 \equiv 5(modp)$$

Thus, 5 is quadratic residue of p if and only if $p = \pm 1(\text{mod}\, 5)$. So, that the solutions are all primes of the form $p = 5l \pm 1$, $l \in \mathbb{Z}$. Factors of $m^2 - m - 1$ are all primes of the form $p = 5l \pm 1$.

This proves the following:

Theorem 2.1. *The cyclic group $\mathbb{Z}_n$ has an automorphism that satisfies* (1) *if and only if its order n is a product of primes from the set* $\{5l \pm 1\}$, *where $l \in \mathbb{Z}$, i.e., if and only if n is an odd integer with any prime factor is congruent to* ± 1 *modulo* 5.

Example 2.2. The group $\mathbb{Z}_{11}$ has two such automorphisms: $\varphi(x) = 4x$ and $\varphi(x) = 8x$. So, we obtain two GS-quasigroups of order 11.

One induced by $\varphi(x) = 4x$:

$\cdot_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	4	8	1	5	9	2	6	10	3	7
1	8	1	5	9	2	6	10	3	7	0	4
2	5	9	2	6	10	3	7	0	4	8	1
3	2	6	10	3	7	0	4	8	1	5	9
4	10	3	7	0	4	8	1	5	9	2	6
5	7	0	4	8	1	5	9	2	6	10	3
6	4	8	1	5	9	2	6	10	3	7	0
7	1	5	9	2	6	10	3	7	0	4	8
8	9	2	6	10	3	7	0	4	8	1	5
9	6	10	3	7	0	4	8	1	5	9	2
10	3	7	0	4	8	1	5	9	5	6	10

and one induced by $\varphi(x) = 8x$:

$\cdot_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	8	5	2	10	7	4	1	9	6	3
1	4	1	9	6	3	0	8	5	2	10	7
2	8	5	2	10	7	4	1	9	6	3	0
3	1	9	6	3	0	8	5	2	10	7	4
4	5	2	10	7	4	1	9	6	3	0	8
5	9	6	3	0	8	5	2	10	7	4	1
6	2	10	7	4	1	9	6	3	0	8	5
7	6	3	0	8	5	2	10	7	4	1	9
8	10	7	4	1	9	6	3	0	8	5	2
9	3	0	8	5	2	10	7	4	1	9	6
10	7	4	1	9	6	3	0	8	5	2	10

Remark 2.3. Let p be an odd prime and suppose $k \geqslant 1$. If $(a, p) = 1$, then $x^2 \equiv a (\operatorname{mod} p^k)$ has either no solutions or exactly two solutions, according as $x^2 \equiv a (\operatorname{mod} p)$ is or not solvable.

Corollary 2.4. *The cyclic group $\mathbb{Z}_{p^k}$ has an automorphism satisfying* (1) *if and only if p is a prime from the set $\{5l \pm 1 : l \in \mathbb{Z}\}$, i.e., if and only if $p \equiv \pm 1 (\operatorname{mod} 5)$.*

3. Conclusions

The following theorem is simple but crucial.

Theorem 3.1. *Let G be a commutative group of order $m_1 m_2$, where m_1 and m_2 are relatively prime positive integers, with an automorphism φ satisfying* (1)*. Then there exist groups G_1 and G_2 such that $G = G_1 \times G_2$, $|G_1| = m_1$, $|G_2| = m_1$ with automorphisms satisfying* (1).

Example 3.2. The group $\mathbb{Z}_{55} = \mathbb{Z}_5 \times \mathbb{Z}_{11}$ has two automorphisms $\varphi(x) = 8x$ and $\varphi(x) = 48x$ satisfying (1). $\mathbb{Z}_5$ and $\mathbb{Z}_{11}$ have automorphisms $\varphi(x) = 3x$ and $\varphi(x) = 4x$, $\varphi(x) = 8x$ satisfying (1), respectively.

So, for GS-quasigroups of orders 5^k and p^k, where p is a prime of the form $5l \pm 1$ there is no any GS-quasigroup of order p^k such that $p \neq 5l \pm 1$.

Thus the final result:

Theorem 3.3. *Let $n = \prod_{i=1}^{n} l_i$ be square free number. Then a $GS-$quasigroup of order n exists if and only if each prime factor of n is congruent to ± 1 modulo 5, i.e., if and only if $l_i \equiv \pm 1 (\bmod 5)$ for all $1 \leqslant i \leqslant n$.*

Acknowledgment. The authors wishes to thank Lyudmyla Turowska professor and Torbjörn Lundh associate professor at the Department of Mathematics of Chalmers University of Technology and Göteborg University for very valuable suggestions. Special thanks for Dr. Shahid S. Siddiqi and Dr. Muhammad Sharif.

References

[1] **Z. Kolar-Begović and V. Volenec**, *DGS-trapezoids in GS-quasigroups*, Math. Commun. **8** (2003), 215 − 218.

[2] **Z. Kolar-Begović and V. Volenec**, *Affine regular dodecahedron in GS-quasigroups*, Quasigroups and Related Systems **13** (2005), 229 − 236.

[3] **Z. Kolar-Begović and V. Volenec**, *GS-deltoids in GS-quasigroups*, Math. Commun. **10** (2005), 117 − 122.

[4] **V. Volenec**, *GS-quasigroups*, Čas. pěst. mat. **115** (1990), 307 − 318.

[5] **V. Volenec and Z. Kolar**, *GS-trapezoids in GS-quasigroups*, Math. Commun. **7** (2002), 143 − 158.

[6] **V. Volenec and Z. Kolar-Begović**, *Affine-regular pentagons in GS-quasigroups*, Quasigroups and Related System **12** (2004), 103 − 112.

[7] **V. Volenec and Z. Kolar-Begović**, *Affine regular decagons in GS-quasigroups*, Comment. Math. Univ. Carolin. **49** (2008), 383 − 395.

Received July 27, 2009

Y.Amad:
Department of Mathematical Sciences, Chalmers University of Technology and University of Gothenburg, SE-41296, Gothenburg, Sweden, E-mail: yahyamajeed2001@hotmail.com
M.A.Malik:
Department of Mathematics, University of the Punjab, Quaid-e-Azam Campus, Lahore-54590, Pakistan, E-mail: malikpu@yahoo.com