Comment.Math.Univ.Carolin. 49,2 (2008)301–307

Moufang loops of odd order $p_1 p_2 \cdots p_n q^3$ with non-trivial nucleus

Andrew Rajah, Kam-Yoon Chong

Abstract. It has been proven by F. Leong and the first author (J. Algebra **190** (1997), 474–486) that all Moufang loops of order $p^\alpha q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$ where p and q_i are odd primes, are associative if $p < q_1 < q_2 < \cdots < q_n$, and

(i) $\alpha \le 3$, $\beta_i \le 2$; or
(ii) $p \ge 5$, $\alpha \le 4$, $\beta_i \le 2$.

The first author also proved that if p and q are distinct odd primes, then all Moufang loops of order pq^3 are associative if and only if $q \not\equiv 1 (\mathrm{mod}\, p)$ (J. Algebra **235** (2001), 66–93). In this paper, we prove that all Moufang loops of order $p_1 p_2 \cdots p_n q^3$ where p_i and q are odd primes, are associative if $p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\mathrm{mod}\, p_i)$, $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$ and the nucleus is not trivial.

Keywords: Moufang loop, order, nonassociative

Classification: Primary 20N05

1. Introduction

A binary system $\langle L, \cdot \rangle$ in which specification of any two of the values x, y, z in the equation $x \cdot y = z$ uniquely determines the third value is called a quasigroup. If it further contains a (two-sided) identity element, then it is called a loop. A loop $\langle L, \cdot \rangle$ is a Moufang loop if it satisfies any one of the following four (equivalent) Moufang identities:

$xy \cdot zx = (x \cdot yz)x$	First Middle Moufang identity
$xy \cdot zx = x(yz \cdot x)$	Second Middle Moufang identity
$x(y \cdot xz) = (xy \cdot x)z$	Left Moufang identity
$(zx \cdot y)x = z(x \cdot yx)$	Right Moufang identity.

From now on, L is defined as a finite Moufang loop.

The research of the first author was supported by grant no. 203/PMATHS/671189 of the Fundamental Research Grant Scheme.

The research of the second author was supported by funding under the Graduate Assistant Scheme from Universiti Sains Malaysia.

In [2], O. Chein proved that all Moufang loops of order p, p^2, pq and p^3 are groups when p and q are primes. M. Purtill in [13] showed that all Moufang loops of odd order pqr and pq^2 are associative for distinct primes p, q and r. Though an error was discovered in his proof of the result for the case $p < q$ (see [14]), this case was later resolved by F. Leong and A. Rajah (see [8]) in 1995.

Soon after this, F. Leong and A. Rajah continued extending that result to Moufang loops of orders with higher powers of primes, that is of orders $p_1^2 p_2^2 \cdots p_m^2$ and $p^4 q_1 q_2 \cdots q_n$ (see [9] and [10]). Finally, in [15], they proved that all Moufang loops of odd order $p^\alpha q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$ where p and q_i are odd primes, are associative if $p < q_1 < q_2 < \cdots < q_n$, and

(i) $\alpha \leq 3$, $\beta_i \leq 2$; or
(ii) $p \geq 5$, $\alpha \leq 4$, $\beta_i \leq 2$.

In year 2001, A. Rajah proved that if p and q are distinct odd primes, then all Moufang loops of order pq^3 are associative if and only if $q \not\equiv 1 (\operatorname{mod} p)$ (see [15]). A natural question that follows from this result is: "Are all Moufang loops of odd order $p_1 p_2 \cdots p_n q^3$ where p_i and q are odd primes, $p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\operatorname{mod} p_i)$ associative as well?" In this paper, we give a positive answer for this question when $p_i \not\equiv 1 (\operatorname{mod} p_j)$ and the nucleus is not trivial.

[Note: An inaccurate version of the above result was presented during the Conference Loops '07. However, in the process of writing this paper, we have corrected the mistake by adding the requirement of a non-trivial nucleus.]

2. Definitions

1. Define

$$zR(x,y) = (zx \cdot y)(xy)^{-1},$$
$$zL(x,y) = (yx)^{-1}(y \cdot xz),$$
$$zT(x) = x^{-1} \cdot zx.$$

   $I(L) = \langle R(x,y), L(x,y), T(x) | x, y \in L \rangle$ is called the inner mapping group of L.
2. L_a, the associator subloop of L, is the subloop generated by all the associators (x,y,z) in L where $(x,y,z) = (x \cdot yz)^{-1}(xy \cdot z)$. We shall also denote $L_a = (L,L,L) = \langle (l_1, l_2, l_3) | l_i \in L \rangle$. Clearly L is associative if and only if $L_a = \{1\}$.
3. Let K be a subloop of L and π a set of primes.

   (i) K is a proper subloop of L if $K \neq L$.
   (ii) K is a normal subloop of L ($K \lhd L$) if $K\theta = \{k\theta \mid k \in K\} = K$ for all $\theta \in I(L)$.

(iii) A positive integer n is a π-number if every prime divisor of n lies in π.
(iv) For each positive integer n, we let n_π be the largest π-number that divides n.
(v) K is a π-loop if the order of every element of K is a π-number.
(vi) K is a Hall π-subloop of L if $|K| = |L|_\pi$.
(vii) K is a Sylow p-subloop of L if K is a Hall π-subloop of L and $\pi = \{p\}$.

4. Let K be a non-trivial normal subloop of L.

   (i) L/K is a proper quotient loop of L.
   (ii) K is a minimal normal subloop of L if for every non-trivial normal subloop M of L, $M \subset K \Rightarrow M = K$.

5. Let K be a proper normal subloop of L. K is a maximal normal subloop of L if for every proper normal subloop M of L, $K \subset M \Rightarrow M = K$.
6. All other definitions follow those in [1].

3. Known results on Moufang loops and groups

Let L be a finite Moufang loop and G a finite group.

(R1) L is diassociative, that is, $\langle x, y\rangle$ is a group for any $x, y \in L$. Moreover, if $(x, y, z) = 1$ for some $x, y, z \in L$, then $\langle x, y, z\rangle$ is a group. [1, p. 117, Moufang's theorem]
(R2) $|K|$ divides $|L|$ for every subloop K of L. [6, p. 50, Theorem 2]
(R3) Suppose $|L|$ is odd, K is a subloop of L, and π is a set of primes. Then

   (a) K is a minimal normal subloop of $L \Rightarrow K$ is an elementary abelian group and $(K, K, L) = \langle (k_1, k_2, l) | k_i \in K, l \in L\rangle = \{1\}$. [5, p. 402, Theorem 7]
   (b) L contains a Hall π-subloop. [5, p. 409, Theorem 12]
   (c) L is solvable. [5, p. 413, Theorem 16]

(R4) Suppose $|L|$ is odd and every proper subloop of L is a group. If there exists a minimal normal Sylow subloop of L, then L is a group. [8, p. 268, Lemma 2]
(R5) Let L be a Moufang loop of odd order such that every proper subloop and quotient loop of L is a group. Suppose Q is a Hall subloop of L such that $(|L_a|, |Q|) = 1$ and $Q \lhd L_aQ$. Then L is a group. [10, p. 564, Lemmas 3 and 9, p. 478, Lemma 1(a)]
(R6) Let L be a nonassociative Moufang loop of odd order such that all proper quotient loops of L are groups. Then:

   (a) L_a is a minimal normal subloop of L; and

(b) L_a lies in every maximal normal subloop M of L. Moreover, $L = M\langle x\rangle$ for any $x \in L - M$.

[11, p. 478, Lemma 1]

(R7) Suppose $|L| = p^3$ where p is a prime. Then L is a group. [2, p. 34, Proposition 1]

(R8) Let L be a Moufang loop of odd order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ where $p_1, p_2, \ldots, p_m$ are distinct primes and $\alpha_i \leq 2$. Then L is a group. [9, p. 882, Theorem]

(R9) Suppose p and q are distinct odd primes. There exists a nonassociative Moufang loop of order pq^3 if and only if $q \equiv 1 (\bmod\, p)$. [15, p. 78, Theorem 1 and 7, p. 86, Theorem 2]

(R10) $|x|$ divides $|L|$ for every $x \in L$. [1, p. 92, Theorem 1.2]

(R11) Let N denote the nucleus of L. Then $N \lhd L$. [1, p. 114, Theorem 2.1]

(R12) $(xn, y, z) = (x, yn, z) = (x, y, zn) = (x, y, z)$ for any $x, y, z \in L$ and $n \in N$. [8, p. 267, Lemma 1]

(R13) If H is a subloop of a finite Moufang loop L, u is an element of L, and d is the smallest positive integer such that $u^d \in H$, then $|\langle H, u\rangle| \geq d|H|$, with equality if and only if each element of $\langle H, u\rangle$ has a unique representation in the form hu^α, where $h \in H$ and $0 \leq \alpha < d$. [3, p. 5, Lemma 0]

(R14) Let L be a Moufang loop and K a normal subloop of L. Then L/K is a group $\Rightarrow L_a \subset K$. [10, Lemma 1(a), p. 563]

(R15) Suppose $|L| = p^\alpha m$ where p is a prime, $(p, m) = 1$, $(p-1, p^\alpha m) = 1$ and L has an element of order p^α. Then $L = P \rtimes K$, a split extension of a normal subloop K of order m with a subloop P of order p^α. [12, p. 39, Theorem 1]

(R16) Sylow's first theorem: If p is a prime and p^α divides $|G|$, then G has a subgroup of order p^α. [7, p. 92, Theorem 2.12.1]

(R17) Sylow's second theorem: If p is a prime and p^n divides $|G|$ but $p^{n+1} \nmid |G|$, then any two subgroups of G of order p^n are conjugates. [7, p. 99, Theorem 2.12.2]

(R18) Sylow's third theorem: The number of p-Sylow subgroups in G, for a given prime p, is of the form $1 + kp$ and divides $|G|$. [7, p. 100, Theorem 2.12.3]

(R19) If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, with $p_1 < p_2 < \cdots < p_k$ odd primes and $\alpha_i > 0$ for all i, then every group of order m is abelian if and only if both the following conditions hold:

(a) $\alpha_i \leq 2$ for all $i \in \{1, 2, \ldots, k\}$; and

(b) $p_j^{\alpha_j} \not\equiv 1 (\bmod\, p_i)$ for any i and j.

[4, p. 239, Lemma 1.8]

4. Main results

Lemma 1. *Let G be a group of order pq where p and q are primes with $p < q$ and $q \not\equiv 1 (\bmod\, p)$. Then there exists P, a normal subgroup of order p in G.*

Proof: By Sylow's first theorem (R16), $\exists P < G$ such that $|P| = p$. Then by Sylow's third theorem (R18), the number of p-Sylow subgroups in G, n_p, is given as $n_p \equiv 1(\operatorname{mod} p)$ where n_p divides $|G|$. Since $|G| = pq$, $n_p = 1$ or pq since $p \not\equiv 1(\operatorname{mod} p)$ and $q \not\equiv 1(\operatorname{mod} p)$.

Suppose $n_p = pq$. Then $n_p \equiv 1(\operatorname{mod} p) \Rightarrow pq \equiv 1(\operatorname{mod} p) \Rightarrow pq - 1 = kp$ for some $k \in \mathbb{N} \Rightarrow p(q-k) = 1$. This is a contradiction. Therefore $n_p = 1$. Then by Sylow's second theorem (R17), $P \triangleleft G$. $\square$

Lemma 2. *Let G be a group of order $p_1p_2\cdots p_n$ where $p_1, p_2, \dots, p_n$ are distinct primes with $p_i \not\equiv 1(\operatorname{mod} p_j)$ for every $i, j \in \{1, 2, \dots, n\}$. Then G is a cyclic group.*

Proof: For the case of $n = 1$, the result is trivial. So we can assume that $n \geq 2$. Now $\forall\, i \in \{1, 2, \dots, n\}$, there exists an element $x_i \in G$ such that $|x_i| = p_i$ by (R3)(b). Write $y = x_1x_2\cdots x_n$. We shall prove that $|y| = |G|$ by induction on n.

Since $y \in G$, by (R10),

$$(*) \qquad |y| \text{ divides } |G|.$$

Now $|y| \leq |G|$ by $(*)$. Suppose $|y| < |G|$. Then by $(*)$, $p_k \nmid |y|$ for some $k \in \{1, 2, \dots, n\}$. Now $y^{|y|} = (x_1x_2\cdots x_{k-1}x_{k+1}\cdots x_n)^{|y|}x_k^{|y|} = 1$ since G is abelian by (R19). Then, since $\langle x_k\rangle \cap \langle x_1x_2\cdots x_{k-1}x_{k+1}\cdots x_n\rangle = \{1\}$, by induction on n, it follows that $x_k^{|y|} = 1$ and hence p_k divides $|y|$. This is a contradiction. Therefore, $|y| = |G|$, that is, G is a cyclic group. $\square$

Lemma 3. *Let n be the smallest positive integer such that there exists a nonassociative Moufang loop L of order $p_1p_2\cdots p_nq^3$, where p_i and q are primes, $2 < p_1 < p_2 < \cdots < q$, $q \not\equiv 1(\operatorname{mod} p_i)$ and $p_i \not\equiv 1(\operatorname{mod} p_j)$. Then*

(a) *$n \geq 2$;*
(b) *every proper subloop and proper quotient loop of L is a group;*
(c) *if $H \triangleleft L$ and $H \neq \{1\}$, then $L_a \triangleleft H$;*
(d) *$|L_a| = q^2$; and*
(e) *$L = \langle x\rangle M$, for some $x \in L$, with $|x| = p_1$, and where M is a maximal normal subloop of order $p_2p_3\cdots p_nq^3$ in L.*

Proof: Suppose $n < 2$. Then L would be a group by (R7) and (R9). This is a contradiction. So $n \geq 2$. This proves (a).

Let H be any proper subloop of L. By (R2), $|H|$ divides $|L|$.

So $|H| = p_{\alpha_1}p_{\alpha_2}\cdots p_{\alpha_m}q^3$ where $\alpha_m < n$ or $|H| = p_{\beta_1}p_{\beta_2}\cdots p_{\beta_k}q^\beta$ where $\beta_k \leq n$ and $\beta \leq 2$. If $|H| = p_{\alpha_1}p_{\alpha_2}\cdots p_{\alpha_m}q^3$, then H is a group since n is the smallest positive integer such that L is a nonassociative Moufang loop. If $|H| = p_{\beta_1}p_{\beta_2}\cdots p_{\beta_k}q^\beta$, then H is a group by (R8). Hence, every proper subloop of L is a group. By the same argument, every proper quotient loop of L is a group too. This proves (b).

If $H \triangleleft L$ and $H \neq \{1\}$, by (R14), $L_a \subset H$ because L/H is a group by (b). Since $L_a \triangleleft L$, L_a is normal in H too. This proves (c).

By (R6)(a), L_a is a minimal normal subloop of L. Then by (R3)(a), L_a is an elementary abelian group. Now, if L_a is a Sylow subloop of L, then L must be a group by (R4). This is a contradiction as L is not associative.

So

$$(*) \qquad |L_a| = q \quad \text{or} \quad q^2.$$

Assume $|L_a| = q$. By Sylow's first theorem (R16), there exists P_1, a subloop of order p_1 in L. Since $L_a \triangleleft L$, $L_a P_1$ is a subloop of L. We also know that

$$|L_a P_1| = \frac{|L_a|\,|P_1|}{|L_a \cap P_1|} = \frac{q p_1}{1} = p_1 q.$$

By Lemma 1, $P_1 \triangleleft L_a P_1$. Also $(|L_a|, |P_1|) = (q, p_1) = 1$. Then by (R5), L is a group. This is a contradiction. Therefore, $|L_a| \neq q$. Hence by $(*)$, $|L_a| = q^2$. This proves (d).

Now $|L/L_a| = p_1 p_2 \cdots p_n q$ and L/L_a is a group by (a). By (R15), there exists a normal p_1-complement M/L_a in L/L_a, where $|M/L_a| = p_2 p_3 \cdots p_n q$. So, $|M| = p_2 p_3 \cdots p_n q^3$ and M is a maximal normal subloop of L . By (R3)(b), there exists an element x of order p_1 in L. By (R10), $x \in L - M$ because $|x|$ does not divide $|M|$. Then by (R6)(b), $L = \langle x \rangle M$. This proves (e). □

Theorem. *Let L be a Moufang loop of order $p_1 p_2 \cdots p_n q^3$, where p_i and q are primes, $2 < p_1 < p_2 < \cdots < q$, $q \not\equiv 1 (\operatorname{mod} p_i)$ and $p_i \not\equiv 1 (\operatorname{mod} p_j)$. Suppose N, the nucleus of L, is not trivial. Then L is a group.*

Proof: Suppose not. Let n be the smallest positive integer such that there exists a nonassociative Moufang loop L of order $p_1 p_2 \cdots p_n q^3$, where p_i and q are primes, $2 < p_1 < p_2 < \cdots < q$, $q \not\equiv 1 (\operatorname{mod} p_i)$ and $p_i \not\equiv 1 (\operatorname{mod} p_j)$; and let L be such a loop. From Lemma 3(d), we know that $|L_a| = q^2$. N is not trivial implies $L_a < N$ by (R11) and Lemma 3(c). By (R2), $|L_a| = q^2$ divides $|N|$. So $|N| \geq q^2$. By Sylow's theorem, L contains a subloop S of order q^3. Thus there exists $y \in S - L_a$ where $|\langle L_a, y \rangle| \geq q^3$ by (R13). By (R3)(b), L contains a Hall subloop T of order $p_1 p_2 \cdots p_n$. By (R8), T is a group. Since $p_i \not\equiv 1 (\operatorname{mod} p_j)$, $T = \langle t \rangle$ for some $t \in L$ by Lemma 2.

Now by (R13), $|\langle L_a, y, t \rangle| = p_1 p_2 \cdots p_n q^3 = |L|$. Thus $L = \langle L_a, y, t \rangle$. Since $L_a \subset N$, $L = \langle N, y, t \rangle = N \langle y, t \rangle$ by (R11). Let $Y = \langle y, t \rangle$. Then $L_a = (L, L, L) = (NY, NY, NY) = (Y, Y, Y) = \{1\}$ by (R12) and (R1), and hence, L is a group. This contradicts our first assumption. This concludes the proof of this theorem. □

5. Open questions

Recommendations for future research:

1. Are all Moufang loops of order $p_1p_2\cdots p_nq^3$, where $p_1, p_2, \ldots, p_n$ and q are distinct odd primes, associative? It was proven in [4] that all such Moufang loops are associative if $q \not\equiv 1 (\mathrm{mod}\, p_1)$ and for each $i > 1$, $q^2 \not\equiv 1 (\mathrm{mod}\, p_i)$. We have proven in this paper that all such Moufang loops are associative if q is the largest prime, $q \not\equiv 1 (\mathrm{mod}\, p_i)$, $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$ and the nucleus is not trivial. So the next case that needs to be considered is that of Moufang loops of the same order and the same conditions but the nucleus is trivial.
2. Are all Moufang loops of order p^2q^3 associative if p and q are odd primes with $p < q$ and $q \not\equiv 1 (\mathrm{mod}\, p)$? The smallest case is $3^2 \cdot 5^3$.

Acknowledgment. The authors wish to thank the referee for his/her recommendations towards the improvement of this paper.

References

[1] Bruck R.H., *A Survey of Binary Systems*, Springer, New York, 1971.
[2] Chein O., *Moufang loops of small order I*, Trans. Amer. Math. Soc. **188** (1974), no. 2, 31–51.
[3] Chein O., *Moufang loops of small order*, Memoirs Amer. Math. Soc. **13** (1978), no. 197, 1–131.
[4] Chein O., Rajah A., *Possible orders of nonassociative Moufang loops*, Comment. Math. Univ. Carolin. **41** (2000), no. 2, 237–244.
[5] Glauberman G., *On loops of odd order II*, J. Algebra **8** (1968), 393–414.
[6] Grishkov A.N., Zavarnitsine A.V., *Lagrange's Theorem for Moufang loops*, Math. Proc. Cambridge Philos. Soc. **139** (2005), 41–57.
[7] Herstein I.N., *Topics in Algebra*, John Wiley & Sons, Inc., New York, 1975.
[8] Leong F., Rajah A., *On Moufang loops of odd order* pq^2, J. Algebra **176** (1995), 265–270.
[9] Leong F., Rajah A., *Moufang loops of odd order* $p_1^2p_2^2\cdots p_m^2$, J. Algebra **181** (1996), 876–883.
[10] Leong F., Rajah A., *Moufang loops of odd order* $p^4q_1\cdots q_n$, J. Algebra **184** (1996), 561–569.
[11] Leong F., Rajah A., *Moufang loops of odd order* $p^\alpha q_1^2\cdots q_n^2r_1\cdots r_m$, J. Algebra **190** (1997), 474–486.
[12] Leong F., Rajah A., *Split extension in Moufang loops*, Publ. Math. Debrecen **52** (1998), no. 1–2, 33–42.
[13] Purtill M., *On Moufang loops of order the product of three odd primes*, J. Algebra **112** (1988), 122–128.
[14] Purtill M., *Corrigendum*, J. Algebra **145** (1992), 262.
[15] Rajah A., *Moufang loops of odd order* pq^3, J. Algebra **235** (2001), 66–93.

School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM Penang, Malaysia

Stamford College, Regent School of Economics, 12th Floor, Bangunan Cahaya Suria, Jalan Tun Tan Siew Sin, 50050 Kuala Lumpur, Malaysia

(*Received* November 2, 2007, *revised* December 28, 2007)