**International Journal of Algebra, Vol. 5, 2011, no. 20, 965 - 975**

# Moufang Loops of Odd Order $p_1^2p_2^2\cdots p_n^2q^3$

**Andrew Rajah and Wing Loon Chee**

School of Mathematical Sciences, Universiti Sains Malaysia
11800 USM, Penang, Malaysia
andy@cs.usm.my, wlchee@usm.my

**Abstract**

It has been shown that for distinct odd primes $p_1, p_2, \ldots, p_n$ and $q$, all Moufang loops of order $p_1p_2\cdots p_nq^3$ are groups if and only if $q$ is not congruent to 1 modulo $p_i$ for each $i$. In this paper, we extend that result to include Moufang loops of order $p_1^2p_2^2\cdots p_n^2q^3$.

**Mathematics Subject Classification:** 20N05

**Keywords:** Moufang loop, order, nonassociative

## 1 Introduction

A loop is a Moufang loop if it satisfies the Moufang identity $(x \cdot y) \cdot (z \cdot x) = [x \cdot (y \cdot z)] \cdot x$. It is known that Moufang loops are inverse property loops [2]. Hence, any associative Moufang loop is, in fact, a group. Further, in [2], Bruck showed that if a Moufang loop contains three (fixed) elements that associate in some order, then they generate an associative subloop (a group). A corollary of this theorem is that, Moufang loops are diassociative, i.e., any two (fixed) elements in a Moufang loop generate a group. One can see that there is a very close relationship between Moufang loops and groups.

One of the natural questions arising from the observation of the above theorems is: "For a positive integer $n$, does there exist a nonassociative Moufang loop of order $n$?". If yes, then it would be interesting to construct such a one to compare its properties with groups of order $n$. The process of construction, however, involves studying its known properties and somehow establishing a product rule between any pair of elements in that Moufang loop. Such a nonassociative Moufang loop of order $n$ can even be used to construct a nonassociative Moufang loop of order $mn$ for any positive integer $m$. This is done by using the direct product of the nonassociative Moufang loop of order $n$ with any group of order $m$. (Therefore, if it is known that all Moufang loops of order $mn$ are associative, then all Moufang loops of order $m$ (and $n$) must also be associative.)

Chein [3] showed a method of constructing nonassociative Moufang loops of order $2m$ by using nonabelian groups of order $m$. Finally, Chein and the first author [4] resolved the even case: All Moufang loops of order $2m$ are associative if and only if all groups of order $m$ are abelian. For the odd case, the existence of nonassociative Moufang loops of order $3^4$ and $p^5$ for every prime $p > 3$ has been shown by Bol [1] and Wright [17] respectively. In 2001, the first author has constructed the entire class of nonassociative Moufang loops of order $pq^3$ for every pair of distinct odd primes $p$ and $q$ by showing that they exist if and only if $q \equiv 1 \pmod{p}$. Much work has also been done in the "opposite" direction, i.e., in proving the nonexistence of nonassociative Moufang loops of particular orders. We give below two results that are of significance to our research. For odd primes $p_1, \ldots, p_k, q, r_1, \ldots, r_s$ with $p_1 < \cdots < p_k < q < r_1 < \cdots < r_s$, all Moufang loops of the following orders are associative:

(i) $q^4 r_1^2 r_2^2 \cdots r_s^2$ if $q > 3$ [12]; and

(ii) $p_1 p_2 \cdots p_k q^3 r_1 r_2 \cdots r_s$ if $q \not\equiv 1 \pmod{p_i}$ for all $i \in \{1, 2, \ldots, k\}$ [16].

(We wish to remind the reader that every Moufang loop whose order is a divisor of the above two integers is also associative.)

We therefore can conclude that hereto the only remaining unresolved cases for Moufang loops of odd order can be written as:

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k} q^{\beta} r_1^{\gamma_1} \cdots r_s^{\gamma_s},$$

where

$$\begin{aligned}
&p_1 < \cdots < p_k < q < r_1 < \cdots < r_s \text{ are odd primes}; \quad k \geq 1; \\
&1 \leq \alpha_i \leq 4 \ (\alpha_1 \leq 3 \text{ if } p_1 = 3); \quad 3 \leq \beta \leq 4; \quad \gamma_i \leq 2; \\
&\text{there exists some } \alpha_i \geq 2 \text{ or } \gamma_i = 2 \text{ if } \beta = 3; \\
&q \not\equiv 1 \pmod{p_i} \text{ for all } i = 1, \ldots, k; \text{ and} \\
&p_j \not\equiv 1 \pmod{p_i} \text{ for all } i < j \text{ if } 3 \leq \alpha_j \leq 4.
\end{aligned}$$

In view of the existence of nonassociative Moufang loops of odd order $pq^3$ when $q \equiv 1 \pmod{p}$, we continue with the study of Moufang loops of order $p^2 q^3$ where $p$ and $q$ are distinct odd primes with $q \not\equiv 1 \pmod{p}$. In this paper, we give a complete resolution for Moufang loops of odd order $p_1^2 p_2^2 \cdots p_n^2 q^3$.

## 2 Definitions and Notations

Below are some relevant basic definitions and notations. For those not listed, we refer the reader to [2] and [14].

**Definition 2.1.** A ***quasigroup*** $\langle L,\cdot\rangle$ is a binary system in which specification of any two of the values $x,y,z$ in the equation $x\cdot y=z$ uniquely determines the third value. If it further contains an identity element, then it is called a ***loop***.

**Definition 2.2.** A loop $\langle L,\cdot\rangle$ is a ***Moufang loop*** if it satisfies any one of the following (equivalent) Moufang identities:

$$\begin{aligned} xy\cdot zx &= (x\cdot yz)x && \text{Middle Moufang identity,}\\ x(y\cdot xz) &= (xy\cdot x)z && \text{Left Moufang identity,}\\ (zx\cdot y)x &= z(x\cdot yx) && \text{Right Moufang identity.}\end{aligned}$$

**Definition 2.3.** Let $K$ be a subloop of a loop $L$. $K$ is a ***normal subloop*** of $L$ (or $K$ is normal in $L$), if $xK=Kx$, $x(yK)=(xy)K$ and $(Kx)y=K(xy)$ for all $x,y\in L$. We denote this by $K\trianglelefteq L$.

**Definition 2.4.** Let $L$ be an inverse property loop. Define

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

$I(L)=\langle T(x),L(x,y),R(x,y)\mid x,y\in L\rangle$ is called the ***inner mapping group*** of $L$.

**Remark 2.5.** Let $K$ be a subloop of an inverse property loop $L$. $K$ is a normal subloop of $L$ if $K\theta=\{k\theta\mid k\in K\}=K$ for all $\theta\in I(L)$.

**Definition 2.6.** Let $K$ be a normal subloop of a loop $L$.

(a) $K$ is a ***minimal normal subloop*** of $L$ if $K$ is not trivial and the only normal subloop properly contained in $K$ is the trivial subloop.

(b) $K$ is a ***maximal normal subloop*** of $L$ if $K$ is a proper subloop of $L$ and the only normal subloop properly containing $K$ is the whole loop $L$.

**Definition 2.7.** Let $K$ be a subloop of a finite power associative loop $L$ and $\pi$ a set of primes.

(a) A positive integer $n$ is a ***$\pi$-number*** if every prime divisor of $n$ lies in $\pi$.

(b) $K$ is a ***$\pi$-loop*** if the order of every element of $K$ is a $\pi$-number.

(c) $K$ is a ***Hall $\pi$-subloop*** of $L$ if $K$ is a $\pi$-loop and $|K|$ is the largest $\pi$-number that divides $|L|$.

(d) $K$ is a ***Sylow p-subloop*** of $L$ if $K$ is a Hall $\pi$-subloop of $L$ and $\pi = \{p\}$.

**Remark 2.8.** Power associativity of a loop guarantees that the order of every element in the loop is well-defined.

**Definition 2.9.** The ***associator*** of three (fixed) elements $x, y, z$ in a loop $L$ is the unique element $(x, y, z)$ in $L$ such that $xy \cdot z = (x \cdot yz)(x, y, z)$. The ***associator subloop*** of $L$, denoted by $L_a$, is the subloop generated by all associators in $L$.

**Definition 2.10.** The ***nucleus*** of a loop $L$, denoted by $N(L)$ or simply $N$, is the subloop consisting of all $n \in L$ such that $(n, x, y) = (x, n, y) = (x, y, n) = 1$ for all $x, y \in L$.

**Definition 2.11.** Let $K$ be a subloop of a loop $L$. The ***centraliser*** of $K$ in $L$, denoted by $C_L(K)$, is the set consisting of all $\ell \in L$ such that $\ell k = k\ell$ for all $k \in K$.

## 3 Known Results

**Lemma 3.1.** *Let $L$ be a Moufang loop. Then $N \trianglelefteq L$* [2, p. 114, Theorem 2.1].

**Lemma 3.2.** *Let $L$ be a Moufang loop and $K$ a normal subloop of $L$. Suppose $L/K$ is a group, then $L_a \subseteq K$* [11, p. 563, Lemma 1].

**Lemma 3.3.** *Let $L$ be a finite Moufang loop. Suppose $K$ is a subloop of $C_L(L_a)$ and $(|K|, |L_a|) = 1$. Then $K \subseteq N$* [12, p. 480, Lemma 5].

**Lemma 3.4.** *Let $L$ be a finite Moufang loop.*

(a) *Suppose $|L| = p^\alpha m$ where $p$ is a prime, $(p, m) = (p - 1, p^\alpha m) = 1$ and $L$ has an element of order $p^\alpha$. Then there exists a subloop $P$ of order $p^\alpha$ and a normal subloop $M$ of order $m$ in $L$ such that $L = PM$.*

(b) *Suppose $|L| = p^2 m$ where $p$ is the smallest prime dividing $|L|$ and $(p, m) = 1$. Then there exists a subloop $P$ of order $p^2$ and a normal subloop $M$ of order $m$ in $L$ such that $L = PM$.*

[13, p. 39, Theorem 1; and p. 40, Theorem 2]

**Lemma 3.5.** *Let $L$ be a Moufang loop of odd order. Then $L$ contains a Hall $\pi$-subloop where $\pi$ is any set of primes* [5, p. 409, Theorem 12].

**Lemma 3.6.** *Let $L$ be a Moufang loop of odd order. Suppose $H \trianglelefteq K \trianglelefteq L$ and $H$ is a Hall subloop of $K$, then $H \trianglelefteq L$* [10, p. 879, Lemma 1].

**Lemma 3.7.** *Let $L$ be a Moufang loop of odd order and $K$ a normal subloop of $L$. Suppose $K \subseteq N$. Then $C_L(K) \trianglelefteq L$ and $|L/C_L(K)|$ divides $|\mathrm{Aut}(K)|$* [8, p. 33, Theorem 3(a)].

**Lemma 3.8.** *Let $L$ be a Moufang loop of odd order and $K$ a normal Hall subloop of $L$. Suppose $K = \langle x\rangle L_a$ for some $x \in K - L_a$ and $L_a \subseteq N$. Then $K \subseteq N$* [16, Lemma 3.17].

**Lemma 3.9.** *Let $L$ be a nonassociative Moufang loop of odd order. Then $L_a$ is a minimal normal subloop of $L$ and an elementary abelian group* [5, p. 402, Theorem 7; and 12, p. 478, Lemma 1(a)].

**Lemma 3.10.** *Let $L$ be a nonassociative Moufang loop of odd order and $M$ a maximal normal subloop of $L$. Suppose all proper subloops and proper quotient loops of $L$ are groups. Then*

(a) *$L_a$ is a Sylow subloop of $N \Rightarrow L_a = N$* [12, p. 480, Lemma 6].

(b) *$L_a$ is cyclic $\Rightarrow L_a \subseteq N$* [12, p. 480, Lemma 4].

(c) *$(k, w, \ell) = 1$ for all $k \in L_a$, $w \in M$, $\ell \in L \Rightarrow L_a \subseteq N$* [12, p. 479, Lemma 3].

(d) *$(k, w, \ell) \neq 1$ for some $k \in L_a$, $w \in M$, $\ell \in L \Rightarrow L_a$ contains a proper nontrivial subloop which is normal in $M$* [16, Lemma 3.19].

**Lemma 3.11.** *Let $L$ be a Moufang loop of odd order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ where $p_1, p_2, \ldots, p_n$ are primes, $p_1 < p_2 < \cdots < p_n$ and $1 \leq \alpha_n \leq 2$. Suppose all proper subloops and proper quotient loops of $L$ are groups, and $L$ contains a normal Sylow $p_n$-subloop. Then $L$ is a group* [10, p. 879, Lemma 3].

**Lemma 3.12.** *Let $L$ be a Moufang loop of odd order and every proper subloop of $L$ is a group.*

(a) *If there exists a minimal normal Sylow subloop in $L$, then $L$ is a group* [9, p. 268, Lemma 2].

(b) *If $N$ contains a Hall subloop of $L$, then $L$ is a group* [11, p. 564, Lemma 2].

**Lemma 3.13.** *Let $L$ be a Moufang loop of odd order, $K$ a minimal normal subloop of $L$ and $H$ a Hall subloop of $L$. Suppose all proper subloops and proper quotient loops of $L$ are groups, $(|K|, |H|) = 1$ and $H \trianglelefteq KH$. Then $L$ is a group* [11, p. 564, Lemma 3].

**Lemma 3.14.** *Let $L$ be a Moufang loop of order $p_1p_2\cdots p_nq^3$ where $p_1, p_2, \ldots, p_n$ and $q$ are distinct odd primes and $q \not\equiv 1 \pmod{p_i}$ for all $i$. Then $L$ is a group* [16, Theorem].

# 4 New Results

**Lemma 4.1.** *Let $L$ be a Moufang loop of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ where $p_1, p_2, \ldots, p_n$ are odd primes with $p_1 < p_2 < \cdots < p_n$ and $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}^+$.*

(a) *Suppose $\alpha_i \leq 2$ for all $i$. Then there exists a set of normal subloops $H_i \trianglelefteq L$ where $|H_i| = p_i^{\alpha_i}p_{i+1}^{\alpha_{i+1}}\cdots p_n^{\alpha_n}$ for every $i \in \{1, 2, \ldots, n\}$.*

(b) *Suppose there exists some $\alpha_k \geq 3$ such that for every $i < k$, $\alpha_i \leq 2$. Then there exists a set of normal subloops $H_i \trianglelefteq L$ where $|H_i| = p_i^{\alpha_i}p_{i+1}^{\alpha_{i+1}}\cdots p_n^{\alpha_n}$ for every $i \in \{1, 2, \ldots, k\}$.*

*Proof.* Suppose $\alpha_i \leq 2$ for all $i$. Write $L = H_1$. Clearly $H_1 \trianglelefteq L$. Now since $p_1, p_2, \ldots, p_n$ are distinct odd primes and $p_1$ is the smallest of these primes, $(p_1, p_2^{\alpha_2}\ p_3^{\alpha_3}\cdots p_n^{\alpha_n}) = 1 = (p_1 - 1, p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n})$. (If $\alpha_1 = 1$, Lemma 3.5 guarantees the existence of an element of order $p_1$ in $L$.) Thus by Lemma 3.4, there exists a normal subloop $H_2$ in $L$ such that $|H_2| = p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_n^{\alpha_n}$. By a similar manner, we can show that there exists $H_3 \trianglelefteq H_2$ such that $|H_3| = p_3^{\alpha_3}p_4^{\alpha_4}\cdots p_n^{\alpha_n}$. Repeating this procedure, we will finally get a subloop $H_n$ of order $p_n$ normal in $H_{n-1}$. Hence, a series of normal subloops is obtained as below:

$$H_n \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_3 \trianglelefteq H_2 \trianglelefteq H_1 = L,$$

where $|H_i| = p_i^{\alpha_i}p_{i+1}^{\alpha_{i+1}}\cdots p_n^{\alpha_n}$.

Since $H_i \trianglelefteq H_{i-1} \trianglelefteq H_{i-2}$ and $H_i$ is a Hall subloop of $H_{i-1}$, by Lemma 3.6, $H_i \trianglelefteq H_{i-2}$. Now $H_i \trianglelefteq H_{i-2} \trianglelefteq H_{i-3}$ and $H_i$ is a Hall subloop of $H_{i-2}$. Again by Lemma 3.6, $H_i \trianglelefteq H_{i-3}$. Tracing along the series above, we can show that $H_i \trianglelefteq L$ for every $i$. This proves (a).

Suppose there exists some $\alpha_k \geq 3$ such that for every $i < k$, $\alpha_i \leq 2$. Then, using a similar process as above, we can obtain a series of normal subloops:

$$H_k \trianglelefteq H_{k-1} \trianglelefteq \cdots \trianglelefteq H_3 \trianglelefteq H_2 \trianglelefteq H_1 = L,$$

where $|H_i| = p_i^{\alpha_i}p_{i+1}^{\alpha_{i+1}}\cdots p_n^{\alpha_n}$. Again, by using Lemma 3.6 several times, we can prove (b). □

**Theorem 4.2.** *Let $L$ be a Moufang loop of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}q^3$ where $p_1, p_2, \ldots, p_n$ and $q$ are odd primes with $p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 \pmod{p_i}$ and $1 \leq \alpha_i \leq 2$. Then $L$ is a group.*

*Proof.* Suppose not. Let $L$ be the smallest counterexample, i.e., for any proper divisor $m$ of $|L|$, all Moufang loops of order $m$ are groups. Then by Lagrange's theorem [6], all proper subloops and proper quotient loops of $L$ are groups. Also by Lemma 3.14, $\alpha_i = 2$ for at least one value of $i \in \{1, 2, \ldots, n\}$.

By Lemma 4.1(b), there exists a normal subloop $Q$ of order $q^3$ in $L$. Since $L/Q$ is a group, $L_a \subseteq Q$ by Lemma 3.2. Therefore, by Lagrange's theorem and Lemma 3.12(a),

$$|L_a| = q \text{ or } q^2.$$

**Case 1.** $|L_a| = q$.

Since $L_a$ is cyclic, by Lemma 3.10(b), $L_a \subseteq N$. Hence, $|N| \geq q$.

Suppose $q^3$ divides $|N|$. Then by Lemma 3.5, there exists a subloop $H$ of order $q^3$ in $N$. Since $H$ is a Hall subloop of $L$, by Lemma 3.12(b), $L$ would be a group . Thus $q^3$ cannot divide $|N|$. Similarly, we can shown that $p_i^{\alpha_i}$ cannot divide $|N|$ for each $i \in \{1, 2, \ldots, n\}$.

**Case 1.1.** $q^2$ divides $|N|$.

Then $|N| = q^2m$ where $m$ is a divisor of $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$. By Lemma 3.1, $N \trianglelefteq L$. Now

$$|L/N| = \left(\frac{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}}{m}\right) q.$$

By Lemma 3.4(a), there exists $K_1/N \trianglelefteq L/N$ where $|K_1/N| = \frac{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}}{m}$. Hence, $K_1 \trianglelefteq L$ and $|K_1| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}q^2$. Since $L_a \trianglelefteq L$ by Lemma 3.9 and $L_a \subseteq N \subseteq K_1$, $L_a \trianglelefteq K_1$. Thus, $|K_1/L_a| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}q$. By Lemma 3.4(a), there exists $K_2/L_a \trianglelefteq K_1/L_a$ where $|K_2/L_a| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$. So $K_2 \trianglelefteq K_1$ and $|K_2| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}q$. Again by Lemma 3.4(a), there exists $P_1 \trianglelefteq K_2$ where $|P_1| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$. Since $P_1 \trianglelefteq K_2 \trianglelefteq K_1 \trianglelefteq L$ and $P_1$ is a Hall subloop of $K_2$ and $K_1$, $P_1 \trianglelefteq L$ by Lemma 3.6. Then $L/P_1$ is a proper quotient loop, which is a group. Therefore, by Lemma 3.2, $L_a \subseteq P_1$, contrary to Lagrange's theorem.

**Case 1.2.** $q^2$ does not divide $|N|$.

Then, since $q$ divides $|N|$, $|N| = qm$ where $m$ is a divisor of $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$.

Suppose $m \neq 1$. Since $q \not\equiv 1 \pmod{p_i}$ for all $i$, by Lemma 3.4(a), there exists a normal subloop $P_2$ of order $m$ in $N$. Since $P_2$ is a normal Hall subloop of $N$ and $N \trianglelefteq L$, by Lemma 3.6, $P_2 \trianglelefteq L$. Now $L/P_2$ is a group and hence, $L_a \subseteq P_2$ by Lemma 3.2. This violates Lagrange's theorem. So $m = 1$, i.e., $|N| = q$.

Since $L_a \subseteq N$ and $|L_a| = q$, $L_a = N$. By Lemma 3.7, $|L/C_L(N)|$ divides $|\mathrm{Aut}(N)|$. As $|\mathrm{Aut}(N)| = q - 1$, we get

$$|C_L(N)| = \frac{k|L|}{q-1} = \frac{kp_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}q^3}{q-1}$$

for some positive integer $k$. Since $q \not\equiv 1 \pmod{p_i}$ for all $i$, $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ divides $|C_L(N)|$. By Lemma 3.5, there exists a subloop $P_3$ of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ in $C_L(N)$. Then $P_3 \subseteq N$ by Lemma 3.3. This violates Lagrange's theorem.

**Case 2.** $|L_a| = q^2$.

Since $L_a \trianglelefteq L$, $|L/L_a| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q$. By Lemma 3.4(a), there exists a normal subloop $M/L_a$ of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ in $L/L_a$. Hence, $|M| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q^2$ and $M \trianglelefteq L$. In fact, $M$ is a maximal normal subloop of $L$.

**Case 2.1.** $(k, w, \ell) = 1$ for all $k \in L_a$, $w \in M$, $\ell \in L$.

By Lemma 3.10(c), $L_a \subseteq N$. Since $|Q| = q^3$, $|L_a| = q^2$ and $L_a \trianglelefteq Q$, $Q = \langle x \rangle L_a$ for some $x \in Q - L_a$. Also $(|Q|, |L/Q|) = (q^3, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}) = 1$. Then by Lemma 3.8, $Q \subseteq N$. But $Q$ is also a Hall subloop of $L$. Then, $L$ would be a group by Lemma 3.12(b), contrary to our assumption.

**Case 2.2.** $(k, w, \ell) \neq 1$ for some $k \in L_a$, $w \in M$, $\ell \in L$.

By Lemma 3.10(d), there exists $S$, a proper nontrivial subloop of $L_a$ which is normal in $M$. Since $|L_a| = q^2$, $|S| = q$. Now $|M/S| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q$. By Lemma 3.4(a), there exists a normal subloop $K_3/S$ of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ in $M/S$. Thus, $|K_3| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q$ and $K_3 \trianglelefteq M$. Again by Lemma 3.4(a), there exists a normal subloop $P_4$ of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ in $K_3$. Since $P_4$ is a normal Hall subloop of $K_3$ and $K_3 \trianglelefteq M$, by Lemma 3.6, $P_4 \trianglelefteq M$. Now $L/M$ is a group and hence, $L_a \subseteq M$ by Lemma 3.2. So $M = L_a P_4$ and $P_4 \trianglelefteq L_a P_4$. Also $P_4$ is a Hall subloop of $L$ and $(|L_a|, |P_4|) = (q^2, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}) = 1$. By Lemma 3.13, $L$ is a group, contrary to assumption.

Therefore, nevertheless, $L$ is a group. □

**Theorem 4.3.** *Let $L$ be a Moufang loop of order $p_1^{\alpha_1} \cdots p_m^{\alpha_m} q^3 r_1^{\beta_1} \cdots r_n^{\beta_n}$ where $p_1, \ldots, p_m, q, r_1, \ldots, r_n$ are odd primes with $p_1 < \cdots < p_m < q < r_1 < \cdots < r_n$, $q \not\equiv 1 \pmod{p_i}$ and $1 \leq \alpha_i, \beta_i \leq 2$. Then $L$ is a group.*

*Proof.* Let $L$ be the smallest counterexample. By Lagrange's theorem, every proper subloop and proper quotient loop of $L$ is a group. Also by Theorem 4.2 and Lemma 3.14, $n \geq 1$ and there exists some $\alpha_i = 2$ or $\beta_i = 2$.

Now by Lemma 3.9, $L_a$ is a minimal normal subloop of $L$ and is an elementary abelian group. Since $L$ is not a group, $L_a$ is not a Sylow subloop of $L$ by Lemma 3.12(a). So the possible values for $|L_a|$ are $p_i$ (if $\alpha_i = 2$), $q$, $q^2$ and $r_i$ (if $\beta_i = 2$).

**Case 1.** $|L_a| = p_i$.

Since $\alpha_i \leq 2$, by Lemma 4.1(b), there exists a normal subloop $K_1$ of order $q^3 r_1^{\beta_1} \cdots r_n^{\beta_n}$ in $L$. Hence $L/K_1$ is a group and by Lemma 3.2, $L_a \subseteq K_1$. This contradicts Lagrange's theorem.

**Case 2.** $|L_a| = q$ or $q^2$.

Now $|L/L_a| = p_1^{\alpha_1}\cdots p_m^{\alpha_m}q^\theta r_1^{\beta_1}\cdots r_n^{\beta_n}$ where $\theta = 1$ or $2$. Then by Lemma 4.1(a), there exists $K_2/L_a \trianglelefteq L/L_a$ where $|K_2/L_a| = r_n^{\beta_n}$. So $|K_2| = q^\theta r_n^{\beta_n}$ and $K_2 \trianglelefteq L$. Again by Lemma 4.1(a), there exists $R_1 \trianglelefteq K_2$ where $|R_1| = r_n^{\beta_n}$. Since $R_1 \trianglelefteq K_2 \trianglelefteq L$ and $R_1$ is a Hall subloop of $K_2$, by Lemma 3.6, $R_1 \trianglelefteq L$. Hence, $L/R_1$ is a group and $L_a \subseteq R_1$ by Lemma 3.2. This violates Lagrange's theorem.

**Case 3.** $|L_a| = r_i$, $i \neq n$, $(\beta_i = 2)$.

By Lemma 3.5, there exists a subloop $R_2$ of order $r_n^{\beta_n}$ in $L$. Since $L_a \trianglelefteq L$, $L_aR_2$ is a subloop of $L$ and $|L_aR_2| = r_i^2r_n^{\beta_n}$. By Lemma 4.1(a), $R_2 \trianglelefteq L_aR_2$. Hence, $L$ is a group by Lemma 3.13. This is a contradiction.

**Case 4.** $|L_a| = r_n$, $(\beta_n = 2)$.

Since $L_a$ is cyclic, $L_a \subseteq N$ by Lemma 3.10(b).

Suppose $r_n^2$ divides $|N|$. Then $N$ contains a Hall subloop of order $r_n^2$. Hence $L$ is a group by Lemma 3.12(b). Contrary to assumption.

So $L_a$ is a Sylow subloop of $N$. By Lemma 3.10(a), $L_a = N$. By Lemma 3.7, $|L/C_L(N)|$ divides $|\mathrm{Aut}(N)|$. As $|\mathrm{Aut}(N)| = r_n - 1$, we get

$$|C_L(N)| = \frac{k|L|}{r_n - 1} = \frac{kp_1^{\alpha_1}\cdots p_m^{\alpha_m}q^3r_1^{\beta_1}\cdots r_n^2}{r_n - 1}$$

for some positive integer $k$. Since $(r_n^2, r_n - 1) = 1$, $r_n^2$ divides $|C_L(N)|$.

Suppose $|C_L(N)| \neq r_n^2$. Then there exists $K_3 < C_L(N)$ where $|K_3| = |C_L(N)|/r_n^2$. Hence by Lemma 3.3, $K_3 \subseteq N$. This violates Lagrange's theorem.

So $|C_L(N)| = r_n^2$. Now $C_L(N)$ is a Sylow $r_n$-subloop normal in $L$. Thus by Lemma 3.11, $L$ is a group. This is a contradiction.

Therefore, nevertheless, $L$ is a group. □

**Corollary.** *Let $p_1, p_2, \ldots, p_n$ and $q$ be distinct odd primes. All Moufang loops of order $p_1^2p_2^2\cdots\ p_n^2q^3$ are associative if and only if $q \not\equiv 1 \pmod{p_i}$ for all $i$.*

*Proof.* For $p_i > q$, it is clear that $q \not\equiv 1 \pmod{p_i}$; and if $p_i < q$, $q \not\equiv 1 \pmod{p_i}$ is a sufficient condition as assured by the Theorem 4.3. Suppose $q \equiv 1 \pmod{p_i}$ for some (fixed) $i \in \{1, 2, \ldots, n\}$. Then by [15], there exists a nonassociative Moufang loop of order $p_iq^3$. Hence by using the direct product of this nonassociative Moufang loop with any group of order $(p_1^2p_2^2\cdots p_n^2)/p_i$, we get a nonassociative Moufang loop of order $p_1^2p_2^2\cdots p_n^2q^3$. Thus the condition $q \not\equiv 1 \pmod{p_i}$ for all $i$, is a necessary one. □

# 5 Open Problems

Are all Moufang loops of order $p^3q^3$ and $pq^4$ associative if $p$ and $q$ are odd primes with $p < q$ and $q \not\equiv 1 \pmod{p}$? The smallest unsolved case is for $p = 3$ and $q = 5$.

## ACKNOWLEDGMENTS

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 the Universiti Sains Malaysia (USM) Fellowship Scheme.

## References

[1] G. Bol, Gewebe und gruppen, *Math. Ann.*, **114** (1937), 414–431.

[2] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, New York, 1971.

[3] O. Chein, Moufang loops of small order I, *Trans. Amer. Math. Soc.*, **188**(2) (1974), 31–51.

[4] O. Chein and A. Rajah, Possible orders of nonassociative Moufang loops, *Comment. Math. Univ. Carolin.*, **41**(2) (2000), 237–244.

[5] G. Glauberman, On loops of odd order II, *J. Algebra*, **8** (1968), 393–414.

[6] A. N. Grishkov and A. V. Zavarnitsine, Lagrange's Theorem for Moufang loops, *Math. Proc. Camb. Phil. Soc.*, **139** (2005), 41–57.

[7] F. Leong, Moufang loops of order $p^4$, *Nanta Math.*, **7** (1974), 33–34.

[8] F. Leong, The devil and angel of loops, *Proc. Amer. Math. Soc.*, **54** (1976), 32–34.

[9] F. Leong and A. Rajah, On Moufang loops of odd order $pq^2$, *J. Algebra*, **176** (1995), 265–270.

[10] F. Leong and A. Rajah, Moufang loops of odd order $p_1^2 p_2^2 \cdots p_m^2$, *J. Algebra*, **181** (1996), 876–883.

[11] F. Leong and A. Rajah, Moufang loops of odd order $p^4 q_1 \cdots q_n$, *J. Algebra*, **184** (1996), 561–569.

[12] F. Leong and A. Rajah, Moufang loops of odd order $p^\alpha q_1^2 \cdots q_n^2 r_1 \cdots r_m$, *J. Algebra*, **190** (1997), 474–486.

[13] F. Leong and A. Rajah, Split extension in Moufang loops, *Publ. Math. Debrecen*, **52**(1-2) (1998), 33–42.

[14] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann Verlag, Berlin, 1990.

[15] A. Rajah, Moufang loops of odd order $pq^3$, *J. Algebra*, **235** (2001), 66–93.

[16] A. Rajah and W. L. Chee, Moufang loops of odd order $p_1 p_2 \cdots p_n q^3$, *Bull. Malays. Math. Sci. Soc. (2)* **34** (2) (2011), 369–377.

[17] C. R. B. Wright, Nilpotency conditions for finite loops, *Illinois J. Math.*, **9** (1965), 399–409.

**Received: December, 2010**