On commutative loops of order pq with metacyclic inner mapping group and trivial center

Přemysl Jedlička

Abstract. Using a construction of commutative loops with metacyclic inner mapping group and trivial center described by A. Drápal, we enumerate presumably all such loops of order pq, for p and q primes.

Keywords: commutative loops, construction of loops, matrices over finite fields, quadratic extensions

Classification: 20N05 Quasigroups and loops

Let Q be a set with a binary operation $*$. We denote by L_a and R_a the mappings $x \mapsto ax$ and $x \mapsto xa$ respectively. We say that Q is a quasigroup if every L_a as well as every R_a is a bijection. We say that a quasigroup Q is a loop, if there exists an element, usually denoted by 1, such that $L_1 = R_1 = \mathrm{id}_Q$.

The group generated by all the bijections L_a and R_a is called the multiplication group of Q. The subgroup of it that consists of those bijections that fix the element 1 is called the inner mapping group and is denoted by $\mathrm{Inn}(Q)$. The subset of Q consisting of all the fixed points of $\mathrm{Inn}(Q)$ is called the center of Q and is denoted by $Z(Q)$.

Aleš Drápal has been working on a classification of all loops with metacyclic inner mapping group and trivial center. Of the six constructions he has found, exactly one yields commutative loops [1]. This construction was analyzed by Denis Simon and the author [2], giving a more description in the specific case of automorphic loops.

Here we continue the study and we focus on generic loops. There are different cases that are tractable under different conditions. Nevertheless, all the considerations can be applied on $\mathbb{Z}_p$, giving us presumably complete enumeration of commutative loops of order pq with a metacyclic inner mapping group and a trivial center:

Theorem. *Let $p \leqslant q$ be two primes. The number of centerless loops of order $p \cdot q$ that arise from Drápal's construction is, up to isomorphism,*

- $q-2$ *if* $p=2$;
- $(q-p+2)/2$ *if p is an odd divisor of* $q+1$;

The research was supported by the Grant Agency of the Czech Republic, grant no. 201/07/P015.

- $(q-p+1)/2$ *if* p *is an even divisor of* $q+1$ *and* $p>2$*;*
- $(q-p)/2$ *if* p *is an odd divisor of* $q-1$*;*
- $(q-p-1)/2$ *if* p *is an even divisor of* $q-1$ *and* $p>2$*;*
- 0 *otherwise.*

The article is organized as follows: Section 1 introduces Drápal's construction and recalls what we know about it from previous studies. Other sections deal with specific cases. Section 2 considers the easiest case: case $p=2$. For other p's, there is a quadratic polynomial constructed; in Section 3 we analyze what happens if the polynomial has only one root and in Section 4 we study the most complicated case — two different roots of the polynomial.

1. Drápal's construction

In this section we introduce the main topic of our paper, the construction of loops given by Aleš Drápal in [1]. These loops were constructed so that their inner mapping groups are metacyclic and their centers are trivial. We present here the definition as well as the most important results of [2] where the construction was analyzed.

The entire construction is based on a specific mapping, called a 0-bijective mapping; and in fact it was these mappings that were analyzed in [2] rather than the loops themselves. It shall be similar in this article.

Definition. Let R be a commutative ring and let f be a partial mapping $R \to R$. We shall say that f is 0-*bijective* if

(1) $f^i(0)$ is defined for each $i \geq 1$;
(2) for each $i \geq 1$ there exists a unique $y \in R$ such that $f^i(y)$ is defined and equal to 0 — we denote this element $f^{-i}(0)$; and
(3) $f(0) \in R^*$.

We say that a 0-bijective partial mapping f is of 0-*order* k, if k is the smallest positive integer such that $f^k(0)=0$. We say that it is of 0-order ∞ if $f^k(0) \neq 0$ for all k.

Only some 0-bijections are used in the construction: those of the form $f(x) = (sx+1)/(tx+1)$, for some elements s and t in R, with $s-t$ invertible. We shall denote these mappings $f_{s,t}$. They serve for the following construction:

Theorem 1 (Drápal [1])**.** *Let M be a faithful module over a commutative ring R and let $f_{s,t} : R \to R$, for some $s,t \in R$ with $s-t \in R^*$, be a 0-bijective mapping of 0-order k. Then we can define a commutative loop Q on the set $M \times \mathbb{Z}_k$ as follows:*

$$(a,i)\cdot(b,j) = \left(\frac{a+b}{1+tf^i_{s,t}(0)f^j_{s,t}(0)}, i+j\right).$$

The loop is denoted $M[s,t]$. Its inner mapping group is the semidirect product $tM \rtimes G$, where $G = \left\langle 1+tf^i_{s,t}(0)f^j_{s,t}(0)\right\rangle \leq R^*$. The center of the loop is trivial if and only if $t \in R^*$.

Example. Let M be a module over a commutative ring R where 2 is invertible. Let $s = 1$ and $t = -3$. Then it is easy to see that $f^3_{1,-3}(0) = 0$ and hence $M[1, -3]$ is a loop defined on the set $M \times \mathbb{Z}_3$.

It is crucial to understand which numbers can be possibly obtained as 0-orders of $f_{s,t}$, given a ring R. For a ring $\mathbb{Z}_n$, this was nearly solved in [2]:

Proposition 2 (Jedlička, Simon [2]). *Let $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_m^{r_m}$ be the prime factorization of a positive integer and let $k > 1$ be an integer. Then there exist s and $t \in \mathbb{Z}_n$ such that $f_{s,t}$ is a 0-bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ of 0-order k only if there exist $k_1, \dots, k_m$ and $\varepsilon_1, \dots, \varepsilon_m$ satisfying the three conditions:*

- *$\varepsilon_i \in \{-1, 0, 1\}$, $k_i = k_i' p^{e_i}$, where $k_i' \mid (p_i + \varepsilon_i)$ and $e_i < r_i$, for all $1 \le i \le m$;*
- *if $\varepsilon_i = 0$ and $p_i > 3$, for some i, then $k_i = p_i^{r_i}$;*
- *the least common multiple of $k_1, \dots, k_m$ is k.*

The necessity of the conditions follows from the results of [2] too, although it is not explicitly stated there; the article is focused primarily on the case $s = 1$.

In this article, we are able to say more about the generic case, i.e. the case $s \neq 1$. However, this understanding is not good enough to give a nice explicit formula (as we had it in the case $s = 1$ in [2]) but it is sufficient to guess how many loops are there up to isomorphism. For this we need the following isomorphism criterion:

Proposition 3 (Drápal [1]). *Let R be a commutative ring, let $s, t \in R^*$ be such that the mapping $f_{s,t}$ is a 0-bijection of a 0-order k. For any $\bar{s}, \bar{t} \in R^*$, there exists an isomorphism between $R[s,t]$ and $R[\bar{s}, \bar{t}]$ if there exists $1 \le r < k$, $r \in \mathbb{Z}_k^*$ such that $d = f^r_{s,t}(k)$, $\bar{t} = td^2$ and $\bar{s} = 1 + ds - d$. This condition is necessary and sufficient, if $(R, +)$ is a cyclic group.*

The natural limitation of the theorem is that it can give us the exact answer about isomorphism classes only if the base structure is a ring with a cyclic addition. This is the main reason why we restrain our focus to the loops of order pq. In some other cases we can obtain a partial result too but usually we have a one-sided bound only.

2. Case $k = 2$

We focus first on the easy case when $k = 2$. This case is specific and has to be dealt with separately.

Lemma 4. *A mapping $f_{s,t}$ is of 0-order 2 if only if $s = -1$ and $t + 1 \in R^*$.*

Proof: Easily $f_{s,t}(0) = 1$ and $f^2_{s,t}(0) = \frac{s+1}{t+1}$. □

Proposition 5. *Let $R = \mathbb{Z}_n$, $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$. Then there exist $\prod (p_i - 2) p^{e_i - 1}$ non-isomorphic centerless loops of order $2n$ given by Theorem 1.*

Proof: We have seen in Lemma 4 that $f_{s,t}$ is of 0-order 2 if and only if $s=-1$ and $t+1 \in R^*$. Moreover, the loop so obtained has a trivial center if and only if $t \in R^*$. We want to measure the size of the set $\{t \in R^*;\ t+1 \in R^*\}$. If $n = p^e$, for p a prime, then the set consists of all the elements that are congruent neither to 0 nor to -1 modulo p; there are $(p-2)p^{e-1}$ such numbers in $\mathbb{Z}_{p^e}$. If n is a product then we use the Chinese remainder theorem to obtain the formula.

According to Proposition 3, given s and t in R^*, we obtain all isomorphic loops through $d = f^r_{s,t}(0)$, $\bar{s} = 1 + ds - s$ and $\bar{t} = td^2$, where $1 \le r < k$. Since here $k = 2$, the only choice is $r = 1$ and $d = 1$. Hence each loop is isomorphic only to itself. $\square$

3. Case $k > 2$, discriminant zero

In the following two sections we investigate the generic case, $k \ge 3$. These sections depend heavily on the results of [2]. We studied there the matrix $\left(\begin{smallmatrix} s & 1 \\ t & 1 \end{smallmatrix}\right)$. Its characteristic polynomial is $P_{s,t} = x^2 - (s+1)x + s - t$, with roots λ and μ, not necessarily distinct. Since $s - t$ is invertible, both roots must be invertible.

We work with the discriminant of the polynomial, which is a technique that works only if 2 is an invertible element. This is not a major obstacle in our main goal: studying loops over $\mathbb{Z}_p$ for p prime. It is easy to see directly that no non-associative construction can be obtained over $\mathbb{Z}_2$.

In this section we focus on the case $\lambda = \mu$, that means $t = -\left(\frac{s-1}{2}\right)^2$. This case was, for fields, already well described in [2].

Proposition 6 ([2]). *Let K be a field of characteristic $p \ne 2$. Assume $t = -\left(\frac{s-1}{2}\right)^2$ and $s \ne -1$. Then $f_{s,t}$ is a 0-bijection if and only if $s = 1$ or s does not belong to the prime field. In that case, the 0-order of $f_{s,t}$ is p.*

The pair $s = 1$ and $t = 0$ gives a group. Hence, if we work in a q-element field, with $q = p^n$, there are exactly $q - p$ choices of s yielding a non-associative loop. We would like to know, how many loops are obtained, up to isomorphism. Here, Proposition 3 can give an upper bound only. But first we need the following remark:

Lemma 7. *Let R be a commutative ring and let $s - 1 \in R^*$. Then the mapping $d \mapsto 1 + ds - d$ is an injective mapping from R to R.*

Proof: $1 + ds - d = 1 + d's - d'$ if and only if $d(s-1) = d'(s-1)$. $\square$

Corollary 8. *Let K be a field, $s \in K \setminus \{0,1\}$, $t \in K^*$ such that $x \mapsto \frac{sx+1}{tx+1}$ is of 0-order k. Then $K[s,t]$ is isomorphic to at least $\varphi(k)$ loops of type $K[\bar{s},\bar{t}]$, for some $\bar{s}, \bar{t} \in K^*$. Moreover, if $(K,+)$ is a cyclic group then $K[s,t]$ is isomorphic to exactly $\varphi(k)$ such loops.*

Proof: The elements $d_r = f^r(0)$, $1 \le r < k$, $r \in \mathbb{Z}_k^*$ are pairwise different non-zero elements from K. Hence the elements $s_r = 1 + d_r s - d_r$ are pairwise different, according to Lemma 7, and therefore, according to Proposition 3, $R[s,t]$

is isomorphic to at least $\varphi(k)$ loops, namely $R[s_r, t_r]$, with $t_r = td_r^2$. The rest follows immediately. $\square$

Proposition 9. *If $K = \mathbb{F}_{p^n}$, $p > 2$, then there exist at most $\frac{p^n - p}{p-1}$ non-associative loops of order p^{n+1}, obtained via Theorem 1.*

Proof: A mapping $f_{s,t}$ can be a 0-bijection of a 0-order p only if $t = -\left(\frac{s-1}{2}\right)^2$: it was proved in [2] and it will be repeated in the next section. Therefore, according to Proposition 6, there are $p^n - p$ choices of s and t giving raise to a non-associative loop of order p^{n+1}.

Using Corollary 8, we see that each loop is isomorphic to at least $p-1$ loops (including itself) hence there are at most $(p^n - p)/(p-1)$ isomorphism classes. $\square$

In practice, there are fewer isomorphism classes than the bound computed. The reason for that is that not every automorphism of $(K, +)$ is a field automorphism.

4. Case $k > 2$, discriminant nonzero

In this section, we investigate the case $\lambda \neq \mu$, enumerating the loops so obtained. The main result is obtained just for fields $\mathbb{F}_p$, for p a prime because otherwise the situation is much more complicated. First we recapitulate the results obtained in [2].

Lemma 10 ([2])**.** *Let s, t be in R such that $f_{s,t}$ is of 0-order $k > 2$. Denote $\zeta = \lambda/\mu$. Then the following holds:*

- (i) *ζ is a k-th primitive root of unity;*
- (ii) *the element ζ either belongs to R or it is a norm one element lying in a quadratic extension of R;*
- (iii) $t = \frac{(\zeta - s)(\zeta s - 1)}{(\zeta + 1)^2}$;
- (iv) $f_{s,t}^i(0) = \frac{\lambda^i - \mu^i}{\lambda^i(1-\mu) - \mu^i(1-\lambda)}$.

If R happens to be a finite field $\mathbb{F}_q$ then there are two possibilities: either ζ lies in $\mathbb{F}_q$ and this is equivalent to $k \mid (q-1)$; or ζ lies in $\mathbb{F}_{q^2}$ and $N(\zeta) = 1$: it is not difficult to see (and it was better explained in [2]) that this situation is equivalent to $k \mid (q+1)$.

In order to understand the necessary and sufficient conditions for $f_{s,t}$ being a 0-bijection of a 0-order k, we need to rewrite $f_{s,t}^i$ in terms of the element ζ.

Lemma 11. *Let s, t, λ, μ and ζ be as in the previous lemma. Then*

- (i) $\lambda = \frac{s+1}{\zeta+1} \cdot \zeta$, $\mu = \frac{s+1}{\zeta+1}$;
- (ii) $f_{s,t}^i(0) = \frac{(\zeta^i - 1)(\zeta + 1)}{\zeta^i(\zeta - s) - (1 - \zeta s)}$.

Proof: (i) Clearly $\lambda + \mu = s + 1$ and $\lambda\mu = \frac{\zeta(s+1)^2}{(\zeta+1)^2} = \frac{s\zeta^2 + 2s\zeta + s - s\zeta^2 + s^2\zeta + \zeta - s}{(\zeta+1)^2} = s - t$.

(ii) We evaluate

$$f^i_{s,t}(0) = \frac{\lambda^i - \mu^i}{\lambda^i(1-\mu) - \mu^i(1-\lambda)} = \frac{\left(\frac{s+1}{\zeta+1}\right)^i (\zeta^i - 1)}{\left(\frac{s+1}{\zeta+1}\right)^i \left(\zeta^i(1-\frac{s+1}{\zeta+1}) - (1-\frac{s+1}{\zeta+1}\zeta)\right)}$$
$$= \frac{\zeta^i - 1}{(\zeta+1)^{-1}\left(\zeta^i(\zeta+1-s-1) - (\zeta+1-\zeta s-\zeta)\right)} = \frac{(\zeta^i-1)(\zeta+1)}{\zeta^i(\zeta-s) - (1-\zeta s)}.$$

□

It is clearer now when $f_{s,t}$ is of 0-order k. One of the conditions is that the numerator of $f^i_{s,t}(0)$ is zero if and only if k divides i. This is clearly equivalent to ζ being a k-th primitive root of unity. The second condition is that the denominator is always invertible. This condition is more difficult to describe but if we focus our attention on fields only, things become clearer since there is just one non-invertible element.

Corollary 12. *Let K be a field of characteristic different from 2. Let $s \neq -1$, $s - t \in K^*$ and $t \neq -(\frac{s+1}{2})^2$. Let λ and μ be the roots of $P_{s,t}$. Then $f_{s,t}$ is of 0-order k if and only if*

- *$\zeta = \lambda/\mu$ is a primitive k-th root of unity and*
- *$\frac{1-\zeta s}{\zeta - s} \notin \langle\zeta\rangle$.*

Proof: The first condition was already stated in Proposition 10. The second condition comes from Lemma 11(ii): the denominator must be invertible hence non-zero in a field. Therefore $\zeta^i(\zeta - s) \neq (1-\zeta s)$ and $\frac{1-\zeta s}{\zeta - s} \neq \zeta^i$ for any $i \in \mathbb{Z}$. The necessity and sufficiency of the conditions is then evident. □

Corollary 12 explains why we restrain our focus on fields only. Now, as we have said above, there are two cases: if the discriminant of $P_{s,t}$ is a square in K then ζ lies in K; otherwise ζ lies in a quadratic extension and is of norm 1. Nevertheless, both cases can be treated simultaneously. We denote by $O = \{x \in \bar{K};\ [K(x) : K] \leq 2\ \&\ N(x) = 1\}$ (in other words, O shall be the set of all possible ζ's if the discriminant is not a square, enriched by 1 and -1).

Lemma 13. *Let K be a field of characteristic different from 2.*
(i) *Suppose $\zeta \in K^*$. The mapping $\psi : s \mapsto \frac{1-\zeta s}{\zeta - s}$ is a bijection $K \setminus \{\zeta, \zeta^{-1}, -1\} \to K \setminus \{0, 1, \zeta\}$.*
(ii) *Suppose $\zeta \in O$. The mapping $\psi : s \mapsto \frac{1-\zeta s}{\zeta - s}$ is a bijection $K \setminus \{-1\} \to O \setminus \{1, \zeta\}$.*

Proof: (i) The mapping ψ is clearly invertible with ζ not belonging neither to the domain of ψ nor to the domain of ψ^{-1}. Hence ψ is a bijection of $K \setminus \{\zeta\}$. The elements -1 and ζ^{-1} are taken out from the domain on purpose, with $\psi(-1) = 1$ and $\psi(\zeta^{-1}) = 0$.

(ii) The mapping ψ is an injective mapping from K to $\bar{K}$. First we prove that $\frac{1-\zeta s}{\zeta-s} = \zeta \cdot \frac{\zeta^{-1}-s}{\zeta-s}$ belongs to O: element ζ is of norm one hence ζ and ζ^{-1} are conjugated and therefore $\zeta+\zeta^{-1} \in K$. Now $(\zeta^{-1}-s)\cdot(\zeta-s) = 1+s^2-s(\zeta+\zeta^{-1}) \in K$ and $(\zeta^{-1}-s)+(\zeta-s) = (\zeta+\zeta^{-1})-2s \in K$, proving that $\zeta - s$ and $\zeta^{-1}-s$ are conjugated and, therefore, have the same norm. Hence $\zeta \cdot \frac{\zeta^{-1}-s}{\zeta-s}$ is of norm one and lies in O.

As in (i), ζ is not in the image of ψ since the inverse mapping is $\psi^{-1} : x \mapsto \frac{1-\zeta x}{\zeta-x}$. At last, we want to prove that the fraction is in K. Indeed,

$$\frac{1-\zeta x}{\zeta - x} = \frac{(1-\zeta x)(\zeta^{-1}-x^{-1})}{(\zeta-x)(\zeta^{-1}-x^{-1})} = \frac{(\zeta+\zeta^{-1})-(x+x^{-1})}{2-(\zeta^{-1}x+\zeta x^{-1})}$$

which lies in K since (ζ,ζ^{-1}), (x,x^{-1}) and $(\zeta^{-1}x,\zeta x^{-1})$ are conjugated pairs. Hence ψ is onto. $\square$

First we want to know, how many choices of the parameters s and t give raise to a non-associative loop of order $k\cdot q$, based on a field $\mathbb{F}_q$. We are not interested in the case $t=0$ since the loop so obtained is a group.

Proposition 14. *Let $K = \mathbb{F}_q$, with q odd, and let us denote by $\bar{q}$ either $q-1$ or $q+1$. Then, for each $k \geq 3$ dividing $\bar{q}$, there exist exactly $\varphi(k)\cdot\frac{\bar{q}-k}{2}$ choices of s and t such that $t \neq 0$ and $f_{s,t}$ is of order k.*

Proof: We know that $s \neq -1$ from Section 2, since then $k=2$. We know that $t \neq -\left(\frac{s-1}{2}\right)^2$ from Section 3 since then k divides q and not $\bar{q}$. Hence the polynomial $P_{s,t}$ has two different roots λ and μ.

There exist exactly $\varphi(k)$ choices of ζ, primitive k-th root of unity in K. However, if we fix s then ζ and ζ^{-1} give the same value of t, using the formula from Proposition 10. On the other hand, the values of s and t identify ζ uniquely, up to the $\lambda \leftrightarrow \mu$ symmetry. Hence, for each $s \neq -1$, there is a 2-to-1 correspondence between the values of ζ and t. And therefore, there are $\varphi(k)/2$ choices of t such that the first condition of Corollary 12 is fulfilled (for a more detailed reasoning see [2]). As a conclusion, there are $\varphi(k)\cdot(q-1)/2$ choices of s and t that satisfy the first condition of Corollary 12.

We fix ζ and we count the following: the inverse image of $\langle\zeta\rangle$ under the mapping ψ from Lemma 13 (that ψ that corresponds to our choice of ζ) has size $k-2$ since the group generated by ζ has k elements. These values of s that belong to $\psi^{-1}(\langle\zeta\rangle)$ do not satisfy the second condition of Corollary 12. Values $s=\zeta$ and $s=\zeta^{-1}$ (in the case $\zeta \in K$) are not taken either since these are those two giving $t=0$. But any other choice, that means any $s \in K \setminus \{\psi^{-1}(\langle\zeta\rangle),\zeta,\zeta^{-1},-1\}$, together with the appropriate t, satisfies the second condition of Corollary 12 and gives a 0-bijection of 0-order k. If k divides $q-1$, the size of this set is $q-(k-2)-3 = q-k-1$, if k divides $q+1$, the size of the set is $q-(k-2)-1 = q-k+1$.

Taken together, there are $\varphi(k)\cdot(\bar{q}-k)$ choices of ζ and s that satisfy both conditions of Corollary 12 and hence $\varphi(k)\cdot(\bar{q}-k)/2$ choices of t and s. $\square$

Proposition 15. *Let $K = \mathbb{F}_q$, with q odd, and let $\bar{q}$ be either $q+1$ or $q-1$. Let $k > 2$ be a divisor of $\bar{q}$. Then there exist at most $\lceil(\bar{q}-k)/2\rceil$ non-isomorphic loops of order kq obtained as $K[s,t]$ for some $s, t \in K^*$. The number is attained if q is a prime.*

Proof: We have to split the proof in two parts: $s = 1$ and $s \neq 1$. If k is odd then there exist exactly $\varphi(k)/2$ choices of t such that the loop $K[1,t]$ is of order kq. All these loops are isomorphic (see [2]). If k is even then there exists no loop $K[1,t]$ of an even order (see [2]).

Now, according to Propositions 14 and the first part of the proof, there are

$$\frac{\varphi(k)}{2} \cdot (\bar{q} - k) \quad \text{if } k \text{ is even}, \qquad \frac{\varphi(k)}{2} \cdot (\bar{q} - k - 1) \quad \text{if } k \text{ is odd},$$

choices of numbers $s \neq 1$ and $t \neq 0$, such that $\mathbb{Z}_q[s,t]$ is of order kq. This number can be written as $\varphi(k) \cdot \lfloor \frac{\bar{q}-k}{2} \rfloor$. We also notice that $s = 0$ leads to $\frac{1-\zeta s}{\zeta - s} \in \langle \zeta \rangle$ and hence all the choices satisfy $s \neq 0$ as well.

Now, according to Corollary 8, the size of each isomorphism class is at most $\varphi(k)$ (respectively exactly $\varphi(k)$ if q is a prime). Hence there are at most (respectively exactly) $\lfloor \frac{\bar{q}-k}{2} \rfloor$ isomorphism classes for $s \neq 1$.

If we add the case $s = 1$, we obtain the number $\lceil \frac{\bar{q}-k}{2} \rceil$. □

5. Summary

Our goal was to enumerate the number of loops of order pq. Here is the conclusion.

Theorem 16. *Let q be an odd prime and $k > 1$. The number of centerless loops based on $\mathbb{Z}_q$ of order $k \cdot q$ that arise from the construction of Theorem 1 is,*

- *$q - 2$ if $k = 2$;*
- *$(q - k + 2)/2$ if k is an odd divisor of $q + 1$;*
- *$(q - k + 1)/2$ if k is an even divisor of $q + 1$ and $k > 2$;*
- *$(q - k)/2$ if k is an odd divisor of $q - 1$;*
- *$(q - k - 1)/2$ if k is an even divisor of $q - 1$ and $k > 2$;*
- *0 otherwise.*

Proof: The case $k = 2$ was discussed in Proposition 5. Proposition 9 gave no non-associative loop based on $\mathbb{Z}_q$ hence the last possibility is Section 4. According to Lemma 10, there is either $k \mid q - 1$ or $k \mid q + 1$. Proposition 15 states that the number of loops is then $\lceil(\bar{q} - k)/2\rceil$. □

This proposition slightly differs from the one announced in the introduction. But it is more general only: the 0-order of a 0-bijection cannot exceed the size of the ring and hence loops of order pq with $p \leq q$ must be constructed by a 0-bijection of the 0-order p on a commutative ring of q elements. Hence the proposition from the introduction is an immediate consequence.

Acknowledgement. The research was aided with the package LOOPS [3] of the computer program GAP.

References

[1] Drápal A., *A class of commutative loops with metacyclic inner mapping groups*, Comment. Math. Univ. Carolin. **49**,3 (2008), 357–382.

[2] Jedlička P., Simon D., *Commutative automorphic loops of order pq*, preprint.

[3] Nagy G., Vojtěchovský P., *LOOPS: Computing with quasigroups and loops*, version 2.1.0, package for GAP, `http://www.math.du.edu/loops`.

Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 165 21 Prague 6 – Suchdol, Czech Republic

E-mail: jedlickap@tf.czu.cz

(*Received* September 24, 2009, *revised* February 2, 2010)