New York Journal of Mathematics

New York J. Math. **31** (2025) 223–237.

Left braces of size p^2q^2

Teresa Crespo

ABSTRACT. We consider relatively prime integer numbers m and n such that each solvable group of order mn has a normal subgroup of order m. We prove that each brace of size mn is a semidirect product of a brace of size m and a brace of size n. We further give a method to classify braces of size mn from the classification of braces of sizes m and n. We apply this result to determine all braces of size p^2q^2, for p and q odd primes satisfying some conditions which hold in particular for p a Germain prime and $q = 2p + 1$.

CONTENTS

1. Introduction 223
2. Left braces of size mn, for $\gcd(m,n) = 1$ 224
3. Braces of size p^2, for p an odd prime number 226
4. Groups of order p^2q^2 227
5. Left braces of size p^2q^2 228
Acknowledgments 237
References 237

1. Introduction

In [10] Rump introduced braces to study set-theoretic solutions of the Yang-Baxter equation. A (left) brace is a triple $(B, +, \cdot)$ where B is a set and $+$ and $\cdot$ are binary operations such that $(B, +)$ is an abelian group, $(B, \cdot)$ is a group and

$$a \cdot (b + c) + a = a \cdot b + a \cdot c,$$

for all $a, b, c \in B$. We call $(B, +)$ the additive group and $(B, \cdot)$ the multiplicative group of the left brace. The cardinal of B is called the size of the brace. If $(B, +)$ is an abelian group, then $(B, +, +)$ is a brace, called trivial brace.

Let B_1 and B_2 be left braces. A map $f : B_1 \to B_2$ is said to be a brace morphism if $f(b + b') = f(b) + f(b')$ and $f(b \cdot b') = f(b) \cdot f(b')$ for all $b, b' \in B_1$. If f is bijective, we say that f is an isomorphism. In that case we say that the braces B_1 and B_2 are isomorphic.

Received January 30, 2024.

2010 *Mathematics Subject Classification.* 16T25, 20D20, 20D45.

Key words and phrases. Left braces, Sylow subgroups, semidirect product, Germain primes.

This work was supported by grant PID2019-107297GB-I00, Ministerio de Ciencia, Innovación y Universidades.

ISSN 1076-9803/2025

We recall the definition of direct and semidirect product of braces as defined in [5] and [11]. Let $(B_1, +, \cdot)$ and $(B_2, +, \cdot)$ be braces and $\tau : (B_2, \cdot) \to \mathrm{Aut}(B_1, +, \cdot)$ be a group morphism. Define in $B_1 \times B_2$ operations $+$ and $\cdot$ by

$$(a, b) + (a', b') = (a + a', b + b'), \quad (a, b) \cdot (a', b') = (a \cdot \tau(b)(a'), b \cdot b').$$

Then $(B_1 \times B_2, +, \cdot)$ is a brace which is called the semidirect product of the braces B_1 and B_2 via τ and will be denoted $B_1 \rtimes_\tau B_2$. If τ is the trivial morphism, then $(B_1 \times B_2, +, \cdot)$ is called the direct product of B_1 and B_2.

We recall that, for a left brace $(B, +, \cdot)$ and each $a \in B$, we have a bijective map $\lambda_a : B \to B$ defined by $\lambda_a(b) = -a + a \cdot b$ which satisfies $\lambda_a(b + c) = \lambda_a(b) + \lambda_a(c)$, $a \cdot b = a + \lambda_a(b)$, $\lambda_{a \cdot b} = \lambda_a \circ \lambda_b$, for any a, b, c in B.

Left braces have been classified for sizes p^2, p^3, for p a prime number ([3]); pq and p^2q, for p and q odd prime numbers ([1, 2, 4, 9]); $2p^2$, for p an odd prime number ([6]); $8p$, for p an odd prime number $\neq 3, 7$ ([7]) and for $12p$, for p an odd prime number ≥ 7 ([8]). In this paper we consider relatively prime integer numbers m and n such that each solvable group of order mn has a normal subgroup of order m. We prove that each brace of size mn is a semidirect product of a brace of size m and a brace of size n. We further give a method to classify braces of size mn from the classification of braces of sizes m and n. This is a generalization of the result obtained in [8] in the case in which m is prime. We apply our result to describe all braces of size p^2q^2, for p and q odd primes satisfying $q > p, q \geq 5, p \mid q - 1, p \nmid q + 1, p^2 \nmid q - 1$. We note that these conditions hold in particular when p is an odd Germain prime and $q = 2p + 1$.

2. Left braces of size mn, for $\gcd(m, n) = 1$

In this section we consider relatively prime integer numbers m and n and assume that each solvable group of order mn has a normal subgroup of order m. We prove that each brace of order mn is a semidirect product $B_1 \rtimes_\tau B_2$, where B_1 is a brace of size m, B_2 is a brace of size n and $\tau : (B_2, \cdot) \to \mathrm{Aut}(B_1, +, \cdot)$ is a group morphism. Moreover, given such B_1 and B_2, we determine when two group morphisms $\sigma, \tau : (B_2, \cdot) \to \mathrm{Aut}(B_1, +, \cdot)$ provide isomorphic braces.

Theorem 2.1. *Let m and n be relatively prime integer numbers such that each solvable group of order mn has a normal subgroup of order m. Then each brace of size mn is a semidirect product of a brace of size m and a brace of size n.*

Proof. Let $(B, +, \cdot)$ be a brace of size mn. Let B_1 and B_2 be its unique additive subgroups of size m and n, respectively. In particular B_1 and B_2 are characteristic subgroups in $(B, +)$. Since, for each $a \in B$, λ_a is an automorphism of $(B, +)$, it leaves B_1 and B_2 setwise invariant. This implies that, for $a, b \in B_1$, we have $ab = a + \lambda_a(b) \in B_1$, as $\lambda_a(b) \in B_1$. Similarly, this can be applied to B_2. So, B_1 and B_2 are subbraces of B and B_1 and B_2 are complements of one another. Let $a \in B_1$ and $b \in B_2$, then

$$ba = {}^b a b \Rightarrow b + \lambda_b(a) = {}^b a + \lambda_{{}^b a}(b).$$

Since the multiplicative group of a brace is always solvable (see [5] Theorem 5.2), our hypothesis implies that $(B_1, \cdot)$ is a normal subgroup of $(B, \cdot)$, hence ${}^b a \in B_1$. Using again that the λ-action leaves B_2 setwise invariant, we obtain $\lambda_{{}^b a}(b) \in B_2$. A comparison of the components shows ${}^b a = \lambda_b(a)$, i.e. under the λ-action, $(B_2, \cdot)$ acts by automorphisms of $(B_1, +)$ and $(B_1, \cdot)$, that is, by brace automorphisms. Analogously

$$ab = ba^b \Rightarrow a + \lambda_a(b) = b + \lambda_b(a^b),$$

where $\lambda_a(b) \in B_2, \lambda_b(a^b) \in B_1$. Comparing components, we obtain $\lambda_a(b) = b$. Therefore $ab = a + \lambda_a(b) = a + b$ for $a \in B_1, b \in B_2$. Also, $ba = {}^b a + \lambda_{{}^b a}(b) = {}^b a + b = \tau_b(a) + b$ for an action $\tau : B_2 \to \mathrm{Aut}(B_1)$.

Finally, for $a, a' \in B_1; b, b' \in B_2$, we have

$$\begin{aligned}(a+b)(a'+b') &= ab(a'+b') = a(ba' - b + bb') = a(\tau_b(a') + bb') \\ &= a\tau_b(a') - a + a(bb') = a\tau_b(a') + bb',\end{aligned}$$

where we have use the brace condition in the second and fourth equalities. Hence

$$B \to B_1 \rtimes_\tau B_2 \,;\; a + b \mapsto (a, b)$$

is indeed a brace morphism.

□

We want to see now when two semidirect products of braces B_1 and B_2 of coprime orders are isomorphic.

Proposition 2.2. *Let B_1, B_2 be braces with $\gcd(|B_1|, |B_2|) = 1$. Consider semidirect products $B_\sigma := B_1 \rtimes_\sigma B_2, B_\tau := B_1 \rtimes_\tau B_2$, for morphisms $\sigma, \tau : (B_2, \cdot) \to \mathrm{Aut}(B_1, +, \cdot)$. An isomorphism $h : B_\sigma \to B_\tau$ is of the form (h_1, h_2), where $h_i \in \mathrm{Aut}(B_i), i = 1, 2$, and h_1 and h_2 satisfy*

$$\tau h_2 = {}^{h_1}\sigma.$$

Proof. The coprimality of $|B_1|$ and $|B_2|$ implies that the B_i are subbraces of B_σ and B_τ and furthermore, $(B_1, +)$ (respectively $(B_2, +)$) is the only subgroup of order m (respectively n) in $(B_\sigma, +)$ and $(B_\tau, +)$. Hence an isomorphism $h : B_\sigma \to B_\tau$ is of the form (h_1, h_2), where $h_i \in \mathrm{Aut}(B_i), i = 1, 2$. For $a, a' \in B_1, b, b' \in B_2$, we have

$$h((a, b) \cdot (a', b')) = h(a\sigma(b)(a'), bb') = (h_1(a\sigma(b)(a')), h_2(bb'))$$

and

$$\begin{aligned}h(a, b) \cdot h(a', b') &= (h_1(a), h_2(b)) \cdot (h_1(a'), h_2(b')) \\ &= (h_1(a)\tau(h_2(b))(h_1(a')), h_2(b)h_2(b')).\end{aligned}$$

We obtain

$$h_1(\sigma(b)(a') = \tau(h_2(b))(h_1(a')).$$

Replacing a' by $h_1^{-1}(a')$ results in the equation

$$h_1(\sigma(b)(h_1^{-1}(a')) = \tau(h_2(b))(a').$$

As a' and b are arbitrary, this implies

$$\tau h_2 = {}^{h_1}\sigma.$$

□

3. Braces of size p^2, for p an odd prime number

In [3] Bachiller obtained the classification of braces of sizes p^2 and p^3, up to isomorphism, for p a prime number. We recall it for braces $(B, +, \cdot)$ of size p^2, for p odd. We note that in this case $(B, \cdot)$ is isomorphic to $(B, +)$. For each brace, we give the group of brace automorphisms and an explicit isomorphism from $(B, \cdot)$ to $(B, +)$.

3.1. $(B, +) \simeq \mathbf{Z}/(p^2)$. There are two braces, up to isomorphism, with additive group isomorphic to $\mathbf{Z}/(p^2)$, the trivial one and a brace with $\cdot$ defined by

$$x_1 \cdot x_2 = x_1 + x_2 + p x_1 x_2.$$

In both cases, $(B, \cdot) \simeq \mathbf{Z}/(p^2)$. In the trivial case, we have

$$\operatorname{Aut} B = \operatorname{Aut}(\mathbf{Z}/(p^2)) \simeq (\mathbf{Z}/(p^2))^*.$$

In the nontrivial case, we have

$$\operatorname{Aut} B = \{k \in (\mathbf{Z}/(p^2))^* \ : \ k \equiv 1 \pmod{p}\}$$

and an isomorphism from $(B, \cdot)$ into $\mathbf{Z}/(p^2)$ is given by $n \mapsto n - pn(n-1)/2$.

3.2. $(B, +) \simeq \mathbf{Z}/(p) \times \mathbf{Z}/(p)$. We write the elements in $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ in vector form. There are two braces, up to isomorphism, with additive group isomorphic to $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$, the trivial one and a brace with $\cdot$ defined by

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + y_1 y_2 \\ y_1 + y_2 \end{pmatrix}.$$

In both cases, $(B, \cdot) \simeq \mathbf{Z}/(p) \times \mathbf{Z}/(p)$. In the trivial case, we have

$$\operatorname{Aut} B = \operatorname{Aut}(\mathbf{Z}/(p) \times \mathbf{Z}/(p)) \simeq \mathrm{GL}(2, p).$$

In the nontrivial case, we have

$$\operatorname{Aut} B = \left\{ \begin{pmatrix} d^2 & b \\ 0 & d \end{pmatrix} \ : \ b \in \mathbf{Z}/(p), d \in (\mathbf{Z}/(p))^* \right\}$$

and an isomorphism from $(B, \cdot)$ into $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ is given by

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x - y(y-1)/2 \\ y \end{pmatrix}.$$

4. Groups of order p^2q^2

We assume now that p and q are primes satisfying $p > 2$, $q > p$ and $q \geq 5$. These hypotheses imply that a group G of order p^2q^2 has a unique normal q-Sylow subgroup S_q of order q^2. Indeed, the number n_q of q-Sylow subgroups of G satisfies $n_q \in \{1, p, p^2\}$ and $n_q \equiv 1 \pmod{q}$. Clearly $q \nmid p-1$ and $q \mid p^2-1$ implies $q \mid p-1$ or $q \mid p+1$ but, if $q > p$, the second condition holds only for $p = 2$ and $q = 3$. We obtain that a group of order p^2q^2 is the semidirect product of a normal subgroup S_q of order q^2 and a subgroup S_p of order p^2. It is then determined by a group G_1 of order q^2, a group G_2 of order p^2 and a morphism $\tau : G_2 \to \operatorname{Aut}(G_1)$. We note that triples (G_1, G_2, τ) and (G_1', G_2', τ') provide isomorphic groups of order p^2q^2 if and only if there exist isomorphisms $f : G_1 \to G_1', g : G_2 \to G_2'$ such that ${}^f\tau = \tau' g$. The groups of order p^2q^2 may then be described by determining the equivalence classes of morphisms $\tau : G_2 \to \operatorname{Aut}(G_1)$ under the relation

$$\tau \sim \tau' \Leftrightarrow \exists (f, g) \in \operatorname{Aut} G_1 \times \operatorname{Aut} G_2 \; : \; {}^f\tau = \tau' g.$$

Let us further assume that p and q satisfy $p \mid q-1$, $p \nmid q+1$ and $p^2 \nmid q-1$. If $G_1 \simeq \mathbf{Z}/(q^2)$ then $\operatorname{Aut} G_1 \simeq (\mathbf{Z}/(q^2))^* \simeq \mathbf{Z}/q(q-1)$. The assumptions $p \mid q-1$ and $p^2 \nmid q-1$ imply that $\operatorname{Aut} G_1$ contains a unique subgroup of order p but no subgroup of order p^2. If $G_1 \simeq \mathbf{Z}/(q) \times \mathbf{Z}/(q)$, then $\operatorname{Aut} G_1 \simeq \mathrm{GL}(2, q)$ and $|\mathrm{GL}(2, q)| = (q+1)q(q-1)^2$. The assumptions $p \mid q-1$, $p \nmid q+1$ and $p^2 \nmid q-1$ imply that $\operatorname{Aut} G_1$ contains elements of order p but no element of order p^2.

Since τ and ${}^f\tau$, for $f \in \mathrm{GL}(2, q)$, give isomorphic groups of order p^2q^2, we need to determine the subgroups of order p of $\mathrm{GL}(2, q)$, up to conjugation. This is done in the following lemma which is easy to prove.

Lemma 4.1. *For λ a fixed generator of the unique subgroup of order p of $\mathbf{Z}/(q)^*$, a system of representatives of the conjugation classes of subgroups of order p of $\mathrm{GL}(2, q)$ is*

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^k \end{pmatrix} \right\rangle, \tag{4.1}$$

for k running over a system of representatives of elements of $(\mathbf{Z}/(p))^*$, different from 1 and -1, under the relation $k \sim \ell$ if and only if $k\ell \equiv 1 \pmod{p}$.

The number of subgroups of order p of $\mathrm{GL}(2, q)$ up to conjugation is then $(p+3)/2$.

We may now describe the groups of order p^2q^2 for primes p and q satisfying the following conditions.

$$q > p, p > 2, q \geq 5, p \mid q-1, p \nmid q+1, p^2 \nmid q-1. \tag{4.2}$$

Lemma 4.2. *Let p and q satisfying* (4.2)*. Let G be a group of order p^2q^2 and let us denote by S_q the unique q-Sylow subgroup of G.*

1) Assume $S_q \simeq \mathbf{Z}/(q^2)$ and let α denote a fixed generator of the unique subgroup of order p of $(\mathbf{Z}/(q^2))^*$. In this case, G is isomorphic to one of the following groups.

1.1) $\mathbf{Z}/(p^2q^2)$*;*

1.2) $\mathbf{Z}/(q^2) \rtimes \mathbf{Z}/(p^2)$ *with product given by*

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 + \alpha^{y_1} x_2, y_1 + y_2);$$

1.3) $\mathbf{Z}/(pq^2) \times \mathbf{Z}/(p)$*;*

1.4) $\mathbf{Z}/(q^2) \rtimes (\mathbf{Z}/(p) \times \mathbf{Z}(p))$ *with product given by*

$$\left(x_1, \left(\begin{smallmatrix} y_1 \\ z_1 \end{smallmatrix}\right)\right) \cdot \left(x_2, \left(\begin{smallmatrix} y_2 \\ z_2 \end{smallmatrix}\right)\right) = \left(x_1 + \alpha^{y_1} x_2, \left(\begin{smallmatrix} y_1+y_2 \\ z_1+z_2 \end{smallmatrix}\right)\right).$$

2) Assume $S_q \simeq \mathbf{Z}/(q) \times \mathbf{Z}/(q)$ and let λ denote a fixed generator of the unique subgroup of order p of $(\mathbf{Z}/(q))^*$. In this case, G is isomorphic to one of the following groups.

2.1) $\mathbf{Z}/(p^2q) \times \mathbf{Z}/(q)$*;*

2.2) one of the $(p+3)/2$ groups $(\mathbf{Z}/(q)\times\mathbf{Z}/(q)) \rtimes_M \mathbf{Z}/(p^2)$ with product given by

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, z_1\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, z_2\right) = \left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + M^{z_1} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, z_1 + z_2\right),$$

where M denotes one of the matrices in (4.1)*.*

2.3) $\mathbf{Z}/(pq) \times \mathbf{Z}/(pq)$*;*

2.4) one of the $(p+3)/2$ groups $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_M (\mathbf{Z}/(p) \times \mathbf{Z}/(p))$, with product given by

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1 \\ t_1 \end{smallmatrix}\right)\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_2 \\ t_2 \end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right) + M^{z_1} \left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1+z_2 \\ t_1+t_2 \end{smallmatrix}\right)\right),$$

where M denotes one of the matrices in (4.1)*;*

2.5) $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_\lambda (\mathbf{Z}/(p) \times \mathbf{Z}/(p))$ *with product given by*

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1 \\ t_1 \end{smallmatrix}\right)\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_2 \\ t_2 \end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix} x_1+\lambda^{t_1} x_2 \\ y_1+\lambda^{z_1+t_1} y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1+z_2 \\ t_1+t_2 \end{smallmatrix}\right)\right).$$

5. Left braces of size p^2q^2

In this section we consider primes p and q satisfying the conditions in (4.2). At the beginning of Section 4, we have seen that, under these assumptions, $m = q^2$ and $n = p^2$ satisfy the conditions in Theorem 2.1. Hence, every brace of size p^2q^2 is the semidirect product of a brace B_1 of size q^2 and a brace B_2 of size p^2. We use the description of braces of order p^2 recalled in Section 3 and Proposition 2.2 to determine all braces of size p^2q^2, for p and q satisfying the conditions (4.2). We note that, in particular, these conditions are satisfied when p is an odd Germain prime and $q = 2p + 1$.

For the description of the multiplicative groups of the braces of size p^2q^2 given below we shall use the explicit isomorphism from $(B_2,\cdot)$ to $(B_2,+)$ given in Sections 3.1 and 3.2, respectively. Using these isomorphisms, one may prove that the description of the action of $\operatorname{Aut} B_2$ on $(B_2,\cdot)$ looks the same as its action on $(B_2,+)$ (see [9] Lemma 7).

5.1. $(B_1,+)=\mathbf{Z}/(q^2)$ and $(B_2,+)=\mathbf{Z}/(p^2)$. In this section we describe braces of size p^2q^2 whose additive law is given by

$$(x_1,x_2)+(y_1,y_2)=(x_1+y_1,x_2+y_2), \tag{5.1}$$

for $x_1,y_1\in B_1; x_2,y_2\in B_2$.

5.1.1. B_1 trivial brace. In this case, $\operatorname{Aut} B_1=(\mathbf{Z}/(q^2))^*$. Since $\operatorname{Aut} B_1$ is abelian, ${}^{h_1}\tau=\tau$, for every morphism τ from $(B_2,\cdot)$ to $\operatorname{Aut} B_1$.

The morphisms from $\mathbf{Z}/(p^2)$ to $\operatorname{Aut} B_1$ are τ_i defined by $1\mapsto\alpha^i$, for α a fixed generator of the unique subgroup of order p of $\operatorname{Aut} B_1$, $0\le i\le p-1$, where $i=0$ corresponds to the trivial morphism.

If B_2 **is trivial,** for $h_2\in\operatorname{Aut} B_2$ defined by $h_2(1)=i$, with $p\nmid i$, we have $\tau_i=\tau_1h_2$. We obtain then two braces, the first one is the direct product of B_1 and B_2, with multiplicative law given by

$$(x_1,x_2)\cdot(y_1,y_2)=(x_1+y_1,x_2+y_2), \tag{5.2}$$

and the second one has multiplicative law given by

$$(x_1,x_2)\cdot(y_1,y_2)=(x_1+\alpha^{x_2}y_1,x_2+y_2), \tag{5.3}$$

for $x_1,y_1\in B_1; x_2,y_2\in B_2; \alpha$ a fixed element of order p of $(\mathbf{Z}/(q^2))^*$.

If B_2 **is nontrivial,** $\operatorname{Aut} B_2=\{k\in(\mathbf{Z}/(p^2))^* : k\equiv 1 \pmod p\}$ and, for the morphisms τ_i defined above we have $\tau_ih_2=\tau_i$, for each $h_2\in\operatorname{Aut} B_2$. We obtain p braces, including the direct product one. Taking into account the isomorphism from $(B_2,\cdot)$ into $\mathbf{Z}/(p^2)$ given in Section 3.1 and that α has order p, their multiplicative laws are given by

$$(x_1,x_2)\cdot(y_1,y_2)=(x_1+\alpha^{ix_2}y_1,x_2+y_2+px_2y_2), \tag{5.4}$$

for $x_1,y_1\in B_1; x_2,y_2\in B_2; i=0,\dots,p-1; \alpha$ a fixed element of order p of $(\mathbf{Z}/(q^2))^*$.

5.1.2. B_1 nontrivial brace. In this case, $\operatorname{Aut} B_1=\{k\in(\mathbf{Z}/(q^2))^* : k\equiv 1 \pmod q\}\simeq\mathbf{Z}/(q)$. Then the unique morphism τ from $(B_2,\cdot)\simeq\mathbf{Z}/(p^2)$ to $\operatorname{Aut} B_1$ is the trivial one. We obtain two braces which are direct products of B_1 and B_2, where B_2 is either trivial or nontrivial. Their multiplicative laws are given by

$$(x_1,x_2)\cdot(y_1,y_2)=(x_1+y_1+qx_1y_1,x_2+y_2), \tag{5.5}$$

$$(x_1,x_2)\cdot(y_1,y_2)=(x_1+y_1+qx_1y_1,x_2+y_2+px_2y_2), \tag{5.6}$$

for $x_1, y_1 \in B_1; x_2, y_2 \in B_2$.

Summing up, we have obtained the following result.

Theorem 5.1. *Let p and q be primes satisfying $q > p, q \geq 5, p \mid q-1$, $p \nmid q+1$ and $p^2 \nmid q-1$. There are $p+4$ braces with additive group $\mathbf{Z}/(p^2q^2)$. Four of them have multiplicative group $\mathbf{Z}/(p^2q^2)$ and the remaining p have multiplicative group $\mathbf{Z}/(q^2) \rtimes \mathbf{Z}/(p^2)$.*

5.2. $(B_1,+) = \mathbf{Z}/(q^2)$ and $(B_2,+) = \mathbf{Z}/(p) \times \mathbf{Z}/(p)$. In this section we describe braces of size p^2q^2 whose additive law is given by

$$\left(x_1, \binom{y_1}{z_1}\right) + \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + x_2, \binom{y_1+y_2}{z_1+z_2}\right), \tag{5.7}$$

for $x_1, x_2 \in B_1; \binom{y_1}{z_1}, \binom{y_2}{z_2} \in B_2$.

5.2.1. B_1 trivial brace. In this case, $\operatorname{Aut} B_1 \simeq (\mathbf{Z}/(q^2))^*$. Since $\operatorname{Aut} B_1$ is abelian, we have ${}^{h_1}\tau = \tau$, for every morphism τ from G_2 to $\operatorname{Aut} B_1$ and $h_1 \in \operatorname{Aut} B_1$.
If B_2 is trivial, every nontrivial morphism $\tau : \mathbf{Z}/(p) \times \mathbf{Z}/(p) \to (\mathbf{Z}/(q^2))^*$ is equal to $\tau_0 h_2$, for $h_2 \in \operatorname{Aut} B_2 \simeq \mathrm{GL}(2,p)$ and τ_0 defined by $\tau_0 \binom{1}{0} = \alpha, \tau_0 \binom{0}{1} = 1$, for α a fixed element of order p in $(\mathbf{Z}/(q^2))^*$. We obtain one brace whose multiplicative law is given by

$$\left(x_1, \binom{y_1}{z_1}\right) \cdot \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + \alpha^{y_1} x_2, \binom{y_1+y_2}{z_1+z_2}\right), \tag{5.8}$$

where α is an element of order p in $\operatorname{Aut} B_1$. Besides, we have the direct product of B_1 and B_2 with multiplicative law given by

$$\left(x_1, \binom{y_1}{z_1}\right) \cdot \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + x_2, \binom{y_1+y_2}{z_1+z_2}\right), \tag{5.9}$$

If B_2 is nontrivial, $\operatorname{Aut} B_2 = \left\{ \begin{pmatrix} d^2 & b \\ 0 & d \end{pmatrix} : d \in (\mathbf{Z}/(p))^*, b \in \mathbf{Z}/(p) \right\}$. Every nontrivial morphism τ from $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ is equal to $\tau_0 g$, for $g \in \mathrm{GL}(2,p)$ and τ_0 defined by $\tau_0 \binom{1}{0} = \alpha, \tau_0 \binom{0}{1} = 1$, for α a fixed element of order p in $\operatorname{Aut} B_1$. By computation, we obtain that, for $g_1, g_2 \in \mathrm{GL}(2,p)$, we have $\tau_0 g_1 = \tau_0 g_2$ if and only if the first rows of g_1 and g_2 are equal. We obtain then that the set of nontrivial morphisms τ from $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ is precisely $\{\tau_0 \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/(p))^*, b \in \mathbf{Z}/(p)\} \cup \{\tau_0 \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} : b \in (\mathbf{Z}/(p))^*\}$. Now, for $\tau := \tau_0 \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \tau' := \tau_0 \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}$, there exists $h_2 \in \operatorname{Aut} B_2$ such that $\tau' h_2 = \tau$ if and only if a'/a is a square; for $\tau := \tau_0 \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \tau' := \tau_0 \begin{pmatrix} 0 & b' \\ 1 & 0 \end{pmatrix}$, there always exists $h_2 \in \operatorname{Aut} B_2$ such that $\tau' h_2 = \tau$; for $\tau := \tau_0 \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \tau' := \tau_0 \begin{pmatrix} 0 & b' \\ 1 & 0 \end{pmatrix}$, there exists no $h_2 \in \operatorname{Aut} B_2$ such that $\tau' h_2 = \tau$. We obtain then three braces. By considering the isomorphism from $(B_2, \cdot)$ into $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ given in Section 3.2, their multiplicative laws are given by

$$\left(x_1, \binom{y_1}{z_1}\right) \cdot \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + \alpha^{y_1 - z_1(z_1-1)/2} x_2, \binom{y_1+y_2+z_1z_2}{z_1+z_2}\right), \tag{5.10}$$

$$\left(x_1, \binom{y_1}{z_1}\right) \cdot \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + \alpha^{a(y_1 - z_1(z_1-1)/2)} x_2, \binom{y_1+y_2+z_1z_2}{z_1+z_2}\right), \tag{5.11}$$

and

$$\left(x_1, \binom{y_1}{z_1}\right) \cdot \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + \alpha^{z_1} x_2, \binom{y_1+y_2+z_1z_2}{z_1+z_2}\right), \tag{5.12}$$

respectively, where α is a fixed element of order p in $\operatorname{Aut} B_1$ and a is a fixed quadratic nonresidue modulo p. Besides, we have the direct product of B_1 and B_2 with multiplicative law given by

$$\left(x_1, \binom{y_1}{z_1}\right) \cdot \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + x_2, \binom{y_1+y_2+z_1z_2}{z_1+z_2}\right), \tag{5.13}$$

5.2.2. B_1 nontrivial brace. In this case, $\operatorname{Aut} B_1 = \{k \in (\mathbf{Z}/(q^2))^* : k \equiv 1 \pmod q\} \simeq \mathbf{Z}/(q)$. Then the unique morphism τ from $G_2 \simeq \mathbf{Z}/(p) \times \mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ is the trivial one. We obtain then just two braces which are the direct product of B_1 and B_2, corresponding to B_2 trivial and B_2 nontrivial. Their multiplicative laws are given by

$$\left(x_1, \binom{y_1}{z_1}\right) \cdot \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + x_2 + qx_1x_2, \binom{y_1+y_2}{z_1+z_2}\right), \tag{5.14}$$

$$\left(x_1, \binom{y_1}{z_1}\right) \cdot \left(x_2, \binom{y_2}{z_2}\right) = \left(x_1 + x_2 + qx_1x_2, \binom{y_1+y_2+z_1z_2}{z_1+z_2}\right), \tag{5.15}$$

Summing up, we have obtained the following result.

Theorem 5.2. *Let p and q be primes satisfying $q > p, q \geq 5, p \mid q-1, p \nmid q+1$ and $p^2 \nmid q-1$. There are eight braces with additive group $\mathbf{Z}/(pq^2)\times\mathbf{Z}/(p)$. Four of them have multiplicative group $\mathbf{Z}/(pq^2) \times \mathbf{Z}/(p)$ and the remaining four have multiplicative group $\mathbf{Z}/(q^2) \rtimes (\mathbf{Z}/(p) \times \mathbf{Z}/(p))$.*

5.3. $(B_1, +) = \mathbf{Z}/(q)\times\mathbf{Z}/(q)$ and $(B_2, +) = \mathbf{Z}/(p^2)$. In this section we describe braces of size p^2q^2 whose additive law is given by

$$\left(\binom{x_1}{y_1}, z_1\right) + \left(\binom{x_2}{y_2}, z_2\right) = \left(\binom{x_1+x_2}{y_1+y_2}, z_1 + z_2\right), \tag{5.16}$$

for $\binom{x_1}{y_1}, \binom{x_2}{y_2} \in B_1, z_1, z_2 \in B_2$.

5.3.1. B_1 trivial brace. In this case, $\operatorname{Aut} B_1 = \mathrm{GL}(2, q)$. Every morphism from $\mathbf{Z}/(p^2)$ to $\operatorname{Aut} B_1 = \mathrm{GL}(2, q)$ is equal to ${}^{h_1}\tau$ for some $h_1 \in \operatorname{Aut} B_1$ and τ defined by $\tau(1) = M^\ell$ for M one of the matrices in (4.1) and $1 \leq \ell \leq p-1$.

If B_2 **is trivial,** $\operatorname{Aut} B_2 = \operatorname{Aut} \mathbf{Z}/(p^2)$. For $\tau : \mathbf{Z}/(p^2) \to \operatorname{Aut} B_1$ defined by $\tau(1) = M$ and $h_2 \in \operatorname{Aut} \mathbf{Z}/(p^2)$, we have $\tau h_2(1) = M^{h_2(1)}$. Hence for morphisms τ, τ' with $\tau(1) = M$ and $\tau'(1) = M^\ell$, one has $\tau \sim \tau'$. We have then one brace for each conjugation class of subgroups of order p in $\mathrm{GL}(2, q)$. We obtain $(p+3)/2$ braces, whose multiplicative laws are given by

$$\left(\binom{x_1}{y_1}, z_1\right) \cdot \left(\binom{x_2}{y_2}, z_2\right) = \left(\binom{x_1}{y_1} + M^{z_1}\binom{x_2}{y_2}, z_1 + z_2\right), \tag{5.17}$$

for M one of the matrices in (4.1). Besides, we obtain the direct product of B_1 and B_2 whose multiplicative law is given by

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), z_1\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), z_2\right) = \left(\left(\begin{smallmatrix} x_1+x_2 \\ y_1+y_2 \end{smallmatrix}\right), z_1 + z_2\right), \tag{5.18}$$

If B_2 is nontrivial, we have $\operatorname{Aut} B_2 = \{k \in (\mathbf{Z}/(p^2))^* \ : \ k \equiv 1 \pmod p\}$. Since a nontrivial morphism τ from $(B_2, \cdot)$ to $\operatorname{Aut} B_1$ sends 1 to an element of order p, we have $\tau h_2 = \tau$ for $h_2 \in \operatorname{Aut} B_2$. As noted above, a nontrivial morphism τ from $\mathbf{Z}/(p^2)$ to $\operatorname{Aut} B_1$ is equal to ${}^{h_1}\tau$ for some $h_1 \in \operatorname{Aut} B_1$ and τ defined by $\tau(1) = M^\ell$ for M one of the matrices in (4.1) and $1 \le \ell \le p-1$. Let us see if for some $\ell \in \{2, \dots, p-1\}$ and some matrix M in (4.1), the matrices M and M^ℓ are conjugate by some element in $\mathrm{GL}(2, q)$. This is so only for $M = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ and $\ell = p-1$. In this case, there are $p-1$ braces for each matrix M different from $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ and $(p-1)/2$ for this last one. By considering the isomorphism from $(B_2, \cdot)$ into $\mathbf{Z}/(p^2)$ given in Section 3.1 and taking into account that M denotes a matrix of order p, we obtain $\dfrac{p+1}{2}(p-1) + \dfrac{p-1}{2} = \dfrac{(p-1)(p+2)}{2}$ braces whose multiplicative laws are given by

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), z_1\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), z_2\right) = \left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right) + M^{\ell z_1} \left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), z_1 + z_2 + p z_1 z_2\right), \tag{5.19}$$

for M one of the matrices in (4.1) and with $1 \le \ell \le p-1$, for $M \neq \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$; $1 \le \ell \le (p-1)/2$, for $M = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$.

Besides, we obtain the direct product of B_1 and B_2 whose multiplicative law is given by

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), z_1\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), z_2\right) = \left(\left(\begin{smallmatrix} x_1+x_2 \\ y_1+y_2 \end{smallmatrix}\right), z_1 + z_2 + p z_1 z_2\right), \tag{5.20}$$

5.3.2. *B_1* nontrivial brace. If B_1 is nontrivial,

$$\operatorname{Aut} B_1 = \left\{ \left(\begin{pmatrix} d^2 & b \\ 0 & d \end{pmatrix} \right) \ : \ b \in \mathbf{Z}/(q), d \in (\mathbf{Z}/(q^2))^* \right\}.$$

The matrices of order p in $\operatorname{Aut} B_1$ are conjugate to some diagonal matrix of the form $\left(\begin{smallmatrix} d^2 & 0 \\ 0 & d \end{smallmatrix}\right)$ with d an element of order p in $(\mathbf{Z}/(q))^*$. For λ a chosen element of order p in $(\mathbf{Z}/(q))^*$, the morphisms τ from $\mathbf{Z}/(p^2)$ to $\operatorname{Aut} B_1$ are given by $\tau(1) = \left(\begin{smallmatrix} \lambda^2 & 0 \\ 0 & \lambda \end{smallmatrix}\right)^\ell$, for $1 \le \ell \le p-1$. We note that $\left(\begin{smallmatrix} \lambda^2 & 0 \\ 0 & \lambda \end{smallmatrix}\right) = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^k \end{smallmatrix}\right)^2$, with $k = (p+1)/2$.

If B_2 is trivial, for $\tau \ : \ \mathbf{Z}/(p^2) \to \operatorname{Aut} B_1$ defined by $\tau(1) = M$, we have $\tau h_2(1) = M^{h_2(1)}$. Hence for morphisms τ, τ' with $\tau(1) = M$ and $\tau'(1) = M^\ell$, one has $\tau \sim \tau'$. We may then reduce to the case where $\tau(1) = \left(\begin{smallmatrix} \lambda^2 & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ and we obtain one brace whose multiplicative law is given by

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), z_1\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), z_2\right) = \left(\left(\begin{smallmatrix} x_1+\lambda^{2z_1} x_2 + \lambda^{2z_1} x_1 x_2 \\ y_1+\lambda^{z_1} y_2 \end{smallmatrix}\right), z_1 + z_2\right). \tag{5.21}$$

Besides, we have the direct product whose multiplicative law is given by

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), z_1\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), z_2\right) = \left(\left(\begin{smallmatrix} x_1+x_2+x_1x_2 \\ y_1+y_2 \end{smallmatrix}\right), z_1 + z_2\right). \tag{5.22}$$

If B_2 is nontrivial, we have $\operatorname{Aut} B_2 = \{k \in (\mathbf{Z}/(p^2))^* \ : \ k \equiv 1 \pmod p\}$, as above. For $h_2 \in \operatorname{Aut} B_2$ and $\tau \ : \ (B_2, \cdot) \to \operatorname{Aut} B_1$, we have $\tau h_2 = \tau$. We obtain then $p-1$ braces. By considering again the isomorphism from $(B_2,\cdot)$ into $\mathbf{Z}/(p^2)$ given in Section 3.1 and taking into account that $\tau(1)$ is a matrix of order p, their multiplicative laws are given by

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, z_1\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, z_2\right) = \left(\begin{pmatrix} x_1+\lambda^{2\ell z_1}x_2+\lambda^{2\ell z_1}x_1x_2 \\ y_1+\lambda^{\ell z_1}y_2 \end{pmatrix}, z_1+z_2+pz_1z_2\right), \tag{5.23}$$

where λ is a fixed element of order p in $(\mathbf{Z}/(q))^*$ and $1 \le \ell \le p-1$. Besides, we have the direct product whose multiplicative law is given by

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, z_1\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, z_2\right) = \left(\begin{pmatrix} x_1+x_2+x_1x_2 \\ y_1+y_2 \end{pmatrix}, z_1+z_2+pz_1z_2\right). \tag{5.24}$$

Summing up, we have obtained the following result.

Theorem 5.3. *Let p and q be primes satisfying $q > p, q \ge 5, p \mid q-1$, $p \nmid q+1$ and $p^2 \nmid q-1$. There are $(p^2+4p+9)/2$ braces with additive group $\mathbf{Z}/(p^2q) \times \mathbf{Z}/(q)$.*

a) There are four such braces with multiplicative group $\mathbf{Z}/(p^2q) \times \mathbf{Z}/(q)$;
b) for each of the matrices M in (4.1) *different from $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ and $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{(p+1)/2} \end{pmatrix}$, there are p such braces with multiplicative group $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_M \mathbf{Z}/(p^2)$;*
c) for $M = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, there are $(p+1)/2$ such braces with multiplicative group $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_M \mathbf{Z}/(p^2)$;
d) for $M = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{(p+1)/2} \end{pmatrix}$, there are $2p$ such braces with multiplicative group $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_M \mathbf{Z}/(p^2)$.

5.4. $(B_1,+) = \mathbf{Z}/(q) \times \mathbf{Z}/(q)$ **and** $(B_2,+) = \mathbf{Z}/(p) \times \mathbf{Z}/(p)$**.** In this section we describe braces of size p^2q^2 whose additive law is given by

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) + \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1+x_2 \\ y_1+y_2 \end{pmatrix}, \begin{pmatrix} z_1+z_2 \\ t_1+t_2 \end{pmatrix}\right), \tag{5.25}$$

for $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \in B_1$; $\begin{pmatrix} z_1 \\ t_1 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix} \in B_2$.

5.4.1. B_1 **trivial brace.** In this case, $\operatorname{Aut} B_1 = \mathrm{GL}(2,q)$. A nontrivial morphism τ from $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ either has an order p kernel or is injective. In the first case, it is equal to ${}^{h_1}\tau$ for some $h_1 \in \operatorname{Aut} B_1$ and τ defined by $\tau(u) = M$, $\tau(v) = \mathrm{Id}$, for some $\mathbf{Z}/(p)$-basis (u,v) of $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$, where M is one of the matrices in (4.1). In the second case, it is equal to ${}^{h_1}\tau$ for some $h_1 \in \operatorname{Aut} B_1$ and τ defined by $\tau(u) = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}, \tau(v) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, for an element λ of order p in $(\mathbf{Z}/(q))^*$ and some basis (u,v) of $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$. Indeed, all subgroups of order p^2 of $\mathrm{GL}(2,q)$ are conjugate, as they are the p-Sylow subgroups of $\mathrm{GL}(2,q)$, and $\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ and $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ are a basis of the subgroup of order p^2 whose elements are diagonal matrices.

If B_2 **is trivial,** we have $\operatorname{Aut} B_2 = \mathrm{GL}(2,p)$. For τ defined by $\tau(u) = M$, $\tau(v) = \mathrm{Id}$, for some $\mathbf{Z}/(p)$-basis (u,v) of $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$, we have $\tau = \tau_0 h_2$, for h_2 defined by $h_2(u) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, h_2(v) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and τ_0 defined by $\tau_0\begin{pmatrix} 1 \\ 0 \end{pmatrix} = M, \tau_0\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathrm{Id}$. We obtain then $(p+3)/2$ braces whose multiplicative laws are given by

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + M^{z_1} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_1+z_2 \\ t_1+t_2 \end{pmatrix}\right), \tag{5.26}$$

for M one of the matrices in (4.1). In the case when τ is injective, for an adequate h_2, we have $\tau = \tau_0 h_2$, for τ_0 defined by $\tau_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}, \tau_0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, where λ is a fixed element of order p in $(\mathbf{Z}/(q))^*$. We obtain then one brace whose multiplicative law is given by

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1+\lambda^{t_1} x_2 \\ y_1+\lambda^{z_1+t_1} y_2 \end{pmatrix}, \begin{pmatrix} z_1+z_2 \\ t_1+t_2 \end{pmatrix}\right), \tag{5.27}$$

for λ a fixed element of order p in $(\mathbf{Z}/(q))^*$. Besides, we have the direct product, whose multiplicative law is given by

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1+x_2 \\ y_1+y_2 \end{pmatrix}, \begin{pmatrix} z_1+z_2 \\ t_1+t_2 \end{pmatrix}\right). \tag{5.28}$$

If B_2 is nontrivial, we have $\operatorname{Aut} B_2 = \left\{\begin{pmatrix} d^2 & b \\ 0 & d \end{pmatrix} : d \in (\mathbf{Z}/(p))^*, b \in \mathbf{Z}/(p)\right\}$, as in Section 5.2.1. Now every morphism τ from $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ with an order p kernel is equal to $\tau_0 g$, for $g \in \mathrm{GL}(2, p)$ and τ_0 defined by $\tau_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = M, \tau_0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathrm{Id}$, for M one of the matrices in (4.1). Similarly as in Section 5.2.1, we obtain that the set of nontrivial morphisms τ from $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ is precisely $\{\tau_0 \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/(p))^*, b \in \mathbf{Z}/(p)\} \cup \{\tau_0 \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} : b \in (\mathbf{Z}/(p))^*\}$. Moreover, again as in Section 5.2.1, under the relation

$$\tau \sim \tau' \Leftrightarrow \exists h_2 \in \operatorname{Aut} B_2 \ : \ \tau' h_2 = \tau,$$

we are left with $\tau_0, \tau_0 \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, for $a \in (\mathbf{Z}/(p))^*$ a non-square element, and $\tau_0 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Now, if $M = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, the matrices M and M^{-1} are conjugate by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}(2, q) = \operatorname{Aut} B_1$. Hence, for $h_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we have ${}^{h_1}\tau_0 = \tau_0 \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ which implies that, if -1 is not a square in $\mathbf{Z}/(p)$, then the orbits corresponding to τ_0 and $\tau_0 \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ coincide. We obtain then two braces corresponding to $M = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ and three corresponding to the other matrices. Summing up, there are $(3/2)(p+3)$ braces if $p \equiv 1 \pmod 4$ and $(3/2)(p+3) - 1$ braces if $p \equiv 3 \pmod 4$. Taking into account the isomorphism from $(B_2, \cdot)$ into $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ given in Section 3.2, the corresponding multiplicative laws are given by

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + M^{z_1 - t_1(t_1-1)/2} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_1+z_2+t_1 t_2 \\ t_1+t_2 \end{pmatrix}\right), \tag{5.29}$$

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + M^{a(z_1 - t_1(t_1-1)/2)} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_1+z_2+t_1 t_2 \\ t_1+t_2 \end{pmatrix}\right), \tag{5.30}$$

and

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_2 \\ t_2 \end{pmatrix}\right) = \left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + M^{t_1} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} z_1+z_2+t_1 t_2 \\ t_1+t_2 \end{pmatrix}\right), \tag{5.31}$$

respectively, where M is one of the matrices in (4.1) and a is a fixed quadratic nonresidue modulo p with the exception that, for $p \equiv 3 \pmod 4$ and $M = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, the braces with multiplicative laws (5.29) and (5.30) are isomorphic.

As established above, an injective morphism τ from $\mathbf{Z}/(p)\times\mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ is equal to ${}^{h_1}\tau$ for some $h_1 \in \mathrm{GL}(2,q)$ and τ defined by $\tau(u) = \left(\begin{smallmatrix}1&0\\0&\lambda\end{smallmatrix}\right), \tau(v) = \left(\begin{smallmatrix}\lambda&0\\0&\lambda\end{smallmatrix}\right)$, for an element λ of order p in $(\mathbf{Z}/(q))^*$ and some $\mathbf{Z}/(p)$-basis (u,v) of $\mathbf{Z}/(p)\times\mathbf{Z}/(p)$. A transversal of $\operatorname{Aut} B_2$ in $\mathrm{GL}(2,p)$ is

$$\left\{\left(\begin{smallmatrix}a&0\\c&1\end{smallmatrix}\right) \;:\; a\in(\mathbf{Z}/(p))^*, c\in\mathbf{Z}/(p)\right\}\cup\left\{\left(\begin{smallmatrix}0&c\\1&0\end{smallmatrix}\right) \;:\; c\in(\mathbf{Z}/(p))^*\right\},$$

hence any injective morphism τ from $\mathbf{Z}/(p)\times\mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ is equivalent under the relation in Proposition 2.2 either to $\tau_{a,c} = \tau_0 h_2$ for $h_2 = \left(\begin{smallmatrix}a&0\\c&1\end{smallmatrix}\right)$ for some $a \in (\mathbf{Z}/(p))^*, c \in \mathbf{Z}/(p)$ or to $\tau_c = \tau_0 h_2$ for $h_2 = \left(\begin{smallmatrix}0&c\\1&0\end{smallmatrix}\right)$ for some $c \in (\mathbf{Z}/(p))^*$, where τ_0 is defined by $\tau_0\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&0\\0&\lambda\end{smallmatrix}\right), \tau_0\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right) = \left(\begin{smallmatrix}\lambda&0\\0&\lambda\end{smallmatrix}\right)$. Now the normalizer of $\left\langle\left(\begin{smallmatrix}1&0\\0&\lambda\end{smallmatrix}\right), \left(\begin{smallmatrix}\lambda&0\\0&\lambda\end{smallmatrix}\right)\right\rangle$ in $\mathrm{GL}(2,q)$ consists of diagonal and anti-diagonal matrices. Conjugation by a diagonal matrix leaves diagonal matrices fixed and for an anti-diagonal h_1 we have ${}^{h_1}\left(\begin{smallmatrix}1&0\\0&\lambda\end{smallmatrix}\right) = \left(\begin{smallmatrix}\lambda&0\\0&1\end{smallmatrix}\right), {}^{h_1}\left(\begin{smallmatrix}\lambda&0\\0&\lambda\end{smallmatrix}\right) = \left(\begin{smallmatrix}\lambda&0\\0&\lambda\end{smallmatrix}\right)$. We obtain then ${}^{h_1}\tau_{a,c} = \tau_{-a,a+c}$, for $h_1 = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ and no further equivalences. This gives $(p(p-1)/2) + p - 1 = (p^2+p-2)/2$ braces. With λ an element of order p in $(\mathbf{Z}(q))^*$, and taking into account the isomorphism from $(B_2,\cdot)$ into $\mathbf{Z}/(p)\times\mathbf{Z}/(p)$ given in Section 3.2, their multiplicative laws are given by

$$\left(\left(\begin{smallmatrix}x_1\\y_1\end{smallmatrix}\right),\left(\begin{smallmatrix}z_1\\t_1\end{smallmatrix}\right)\right)\cdot\left(\left(\begin{smallmatrix}x_2\\y_2\end{smallmatrix}\right),\left(\begin{smallmatrix}z_2\\t_2\end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix}x_1+\lambda^{(z_1-t_1(t_1-1)/2)(a+c)+t_1}x_2\\ y_1+\lambda^{(z_1-t_1(t_1-1)/2)c+t_1}y_2\end{smallmatrix}\right),\left(\begin{smallmatrix}z_1+z_2+t_1t_2\\t_1+t_2\end{smallmatrix}\right)\right), \tag{5.32}$$

for some $(a,c)\in(\mathbf{Z}/(p))^*\times\mathbf{Z}/(p)$ where the braces corresponding to (a,c) and $(-a,a+c)$ are isomorphic, and

$$\left(\left(\begin{smallmatrix}x_1\\y_1\end{smallmatrix}\right),\left(\begin{smallmatrix}z_1\\t_1\end{smallmatrix}\right)\right)\cdot\left(\left(\begin{smallmatrix}x_2\\y_2\end{smallmatrix}\right),\left(\begin{smallmatrix}z_2\\t_2\end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix}x_1+\lambda^{z_1-t_1(t_1-1)/2}x_2\\ y_1+\lambda^{z_1-t_1(t_1-1)/2+ct_1}y_2\end{smallmatrix}\right),\left(\begin{smallmatrix}z_1+z_2+t_1t_2\\t_1+t_2\end{smallmatrix}\right)\right), \tag{5.33}$$

for some $c \in (\mathbf{Z}/(p))^*$. Besides, we have the direct product of B_1 and B_2 with multiplicative law given by

$$\left(\left(\begin{smallmatrix}x_1\\y_1\end{smallmatrix}\right),\left(\begin{smallmatrix}z_1\\t_1\end{smallmatrix}\right)\right)\cdot\left(\left(\begin{smallmatrix}x_2\\y_2\end{smallmatrix}\right),\left(\begin{smallmatrix}z_2\\t_2\end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix}x_1+x_2\\y_1+y_2\end{smallmatrix}\right),\left(\begin{smallmatrix}z_1+z_2+t_1t_2\\t_1+t_2\end{smallmatrix}\right)\right), \tag{5.34}$$

5.4.2. B_1 nontrivial brace. In this case, $\operatorname{Aut} B_1 = \left\{\left(\begin{smallmatrix}d^2&b\\0&d\end{smallmatrix}\right) : d\in(\mathbf{Z}/(q))^*, b\in\mathbf{Z}/(q)\right\} \subset \mathrm{GL}(2,q)$. Since the only subgroup of order p of $\operatorname{Aut} B_1$ is $\left\langle\left(\begin{smallmatrix}\lambda^2&0\\0&\lambda\end{smallmatrix}\right)\right\rangle$, for $\lambda \in (\mathbf{Z}/(q))^*$ of order p, a nontrivial morphism τ from $\mathbf{Z}/(p)\times\mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ has an order p kernel and is defined by $\tau(u) = \left(\begin{smallmatrix}\lambda^2&0\\0&\lambda\end{smallmatrix}\right)$, $\tau(v) = \mathrm{Id}$, for some $\mathbf{Z}/(p)$-basis (u,v) of $\mathbf{Z}/(p)\times\mathbf{Z}/(p)$.

If B_2 is trivial, $\operatorname{Aut} B_2 = \mathrm{GL}(2,p)$. For τ defined by $\tau(u) = \left(\begin{smallmatrix}\lambda^2&0\\0&\lambda\end{smallmatrix}\right)$, $\tau(v) = \mathrm{Id}$, for some basis (u,v) of $(B_2,\cdot) = \mathbf{Z}/(p)\times\mathbf{Z}/(p)$, we have $\tau = \tau_0 h_2$, for h_2 defined by $h_2(u) = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), h_2(v) = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ and τ_0 defined by $\tau_0\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}\lambda^2&0\\0&\lambda\end{smallmatrix}\right), \tau_0\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right) = \mathrm{Id}$. We obtain then one brace, whose multiplicative law is given by

$$\left(\left(\begin{smallmatrix}x_1\\y_1\end{smallmatrix}\right),\left(\begin{smallmatrix}z_1\\t_1\end{smallmatrix}\right)\right)\cdot\left(\left(\begin{smallmatrix}x_2\\y_2\end{smallmatrix}\right),\left(\begin{smallmatrix}z_2\\t_2\end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix}x_1+\lambda^{2z_1}x_2+\lambda^{z_1}y_1y_2\\ y_1+\lambda^{z_1}y_2\end{smallmatrix}\right),\left(\begin{smallmatrix}z_1+z_2\\t_1+t_2\end{smallmatrix}\right)\right), \tag{5.35}$$

for λ a fixed element of order p in $(\mathbf{Z}/(q))^*$. Besides, we have the direct product whose multiplicative law is given by

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1 \\ t_1 \end{smallmatrix}\right)\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_2 \\ t_2 \end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix} x_1+x_2+y_1y_2 \\ y_1+y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1+z_2 \\ t_1+t_2 \end{smallmatrix}\right)\right). \tag{5.36}$$

If B_2 is nontrivial, $\operatorname{Aut} B_2 = \left\{\left(\begin{smallmatrix} d^2 & b \\ 0 & d \end{smallmatrix}\right) : d \in (\mathbf{Z}/(p))^*, b \in \mathbf{Z}/(p)\right\} \subset \mathrm{GL}(2, p)$. As in Section 5.2.1, we obtain that the set of nontrivial morphisms τ from $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ to $\operatorname{Aut} B_1$ is precisely

$$\{\tau_0 \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in (\mathbf{Z}/(p))^*, b \in \mathbf{Z}/(p)\} \cup \{\tau_0 \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right) : b \in (\mathbf{Z}/(p))^*\},$$

for τ_0 defined by $\tau_0 \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \lambda^2 & 0 \\ 0 & \lambda \end{smallmatrix}\right), \tau_0 \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) = \mathrm{Id}$. Again, under the relation in Proposition 2.2, we have three orbits corresponding to the matrices Id, $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$, for a non-square, and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. We obtain then three braces. Taking into account the isomorphism from $(B_2, \cdot)$ into $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ given in Section 3.2, their multiplicative laws are given by

$$\begin{aligned} &\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1 \\ t_1 \end{smallmatrix}\right)\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_2 \\ t_2 \end{smallmatrix}\right)\right) \\ &\quad = \left(\left(\begin{smallmatrix} x_1+\lambda^{2(z_1-t_1(t_1-1)/2)}x_2+\lambda^{z_1-t_1(t_1-1)/2}y_1y_2 \\ y_1+\lambda^{z_1-t_1(t_1-1)/2}y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1+z_2+t_1t_2 \\ t_1+t_2 \end{smallmatrix}\right)\right), \end{aligned} \tag{5.37}$$

$$\begin{aligned} &\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1 \\ t_1 \end{smallmatrix}\right)\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_2 \\ t_2 \end{smallmatrix}\right)\right) \\ &\quad = \left(\left(\begin{smallmatrix} x_1+(a\lambda^2)^{(z_1-t_1(t_1-1)/2)}x_2+\lambda^{z_1-t_1(t_1-1)/2}y_1y_2 \\ y_1+\lambda^{z_1-t_1(t_1-1)/2}y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1+z_2+t_1t_2 \\ t_1+t_2 \end{smallmatrix}\right)\right), \end{aligned} \tag{5.38}$$

for a fixed quadratic nonresidue a modulo p, and

$$\begin{aligned} &\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1 \\ t_1 \end{smallmatrix}\right)\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_2 \\ t_2 \end{smallmatrix}\right)\right) \\ &\quad = \left(\left(\begin{smallmatrix} x_1+\lambda^{(z_1-t_1(t_1-1)/2)}x_2+\lambda^{2(z_1-t_1(t_1-1)/2)}y_1y_2 \\ y_1+\lambda^{2(z_1-t_1(t_1-1)/2)}y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1+z_2+t_1t_2 \\ t_1+t_2 \end{smallmatrix}\right)\right). \end{aligned} \tag{5.39}$$

Besides, we have the direct product with multiplicative law defined by

$$\left(\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1 \\ t_1 \end{smallmatrix}\right)\right) \cdot \left(\left(\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_2 \\ t_2 \end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix} x_1+x_2+y_1y_2 \\ y_1+y_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} z_1+z_2+t_1t_2 \\ t_1+t_2 \end{smallmatrix}\right)\right). \tag{5.40}$$

Summing up, we have obtained the following result.

Theorem 5.4. *Let p and q be primes satisfying $q > p, q \geq 5, p \mid q-1, p \nmid q+1$ and $p^2 \nmid q-1$. There are $\dfrac{p^2+5p}{2}+14$ (resp. $\dfrac{p^2+5p}{2}+13$) braces with additive group $\mathbf{Z}/(pq) \times \mathbf{Z}/(pq)$ if $p \equiv 1 \pmod 4$ (resp. if $p \equiv 3 \pmod 4$).*

a) There are four of them with multiplicative group $\mathbf{Z}/(pq) \times \mathbf{Z}/(pq)$;

b) for each of the matrices M in (4.1) different from $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{(p+1)/2} \end{smallmatrix}\right)$, there are four of them with multiplicative group $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_M (\mathbf{Z}/(p) \times \mathbf{Z}/(p))$;

c) for $M = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$*, there are four (resp. three) such braces with multiplicative group* $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_M (\mathbf{Z}/(p) \times \mathbf{Z}/(p))$*, if* $p \equiv 1 \pmod 4$ *(resp. if* $p \equiv 3 \pmod 4$*);*

d) for $M = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{(p+1)/2} \end{smallmatrix}\right)$*, there are eight of them with multiplicative group* $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_M (\mathbf{Z}/(p) \times \mathbf{Z}/(p))$*;*

e) there are $(p^2 + p)/2$ *of them with multiplicative group* $(\mathbf{Z}/(q) \times \mathbf{Z}/(q)) \rtimes_\lambda (\mathbf{Z}/(p) \times \mathbf{Z}/(p))$*.*

Acknowledgments

I am very grateful to the referee for indications and corrections which helped to improve substantially this manuscript.

References

[1] Acri, E.; Bonatto, M. Skew braces of size pq. *Comm. Algebra* **48** (2020), no. 5, 1872–1881. MR4085764, Zbl 1437.16027, doi: 10.1080/00927872.2019.1709480. 224

[2] Acri, E.; Bonatto, M. Skew braces of size p^2q I: Abelian type. *Algebra Colloq.* **29** (2022), no.2, 297–320. MR4414157, Zbl 1495.16030, doi: 10.1142/S1005386722000244. 224

[3] Bachiller, D. Classification of braces of order p^3. *J. Pure Appl. Algebra* **219** (2015), 3568–3603. MR3320237, Zbl 1312.81099, doi: 10.1016/j.jpaa.2014.12.013. 224, 226

[4] Campedel, E.; Caranti, A.; Del Corso, I. Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: the cyclic Sylow p-subgroup case. *J. Algebra* **556** (2020), 1165–1210. MR4089566, Zbl 1465.12006, doi: 10.1016/j.jalgebra.2020.04.009. 224

[5] Cedó, F. Left Braces: solutions of the Yang-Baxter equation. *Adv. Group Theory Appl.* **5** (2018), 33–90. MR3824447, Zbl 1403.16033, doi: 10.4399/97888255161422. 224, 225

[6] Crespo, T. Hopf Galois structures on field extensions of degree twice an odd prime square and their associated skew left braces. *J. Algebra* **565** (2021), 282–308. MR4150347, Zbl 1464.16025, doi: 10.1016/j.jalgebra.2020.09.005. 224

[7] Crespo, T.; Gil-Muñoz, D.; Rio, A.; Vela, M. Left braces of size $8p$. *J. Algebra* **617** (2023), 317–339. MR4513787, Zbl 1511.16028, doi: 10.1016/j.jalgebra.2022.11.011. 224

[8] Crespo, T.; Gil-Muñoz, D.; Rio, A.; Vela, M. Inducing braces and Hopf Galois structures. *J. Pure Appl. Algebra* **227** (2023), no. 9, Paper No. 107371, 16 pp. MR4559373, Zbl 1526.16027, doi: 10.1016/j.jpaa.2023.107371. 224

[9] Dietzel, C. Braces of order p^2q. *J. Algebra Appl.* **20** (2021), no. 8, Paper No. 2150140, 24 pp. MR4297324, Zbl 1486.16040, doi: 10.1142/S0219498821501401. 224, 229

[10] Rump, W. Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* **307** (2007), 153–170. MR2278047, Zbl 1115.16022, doi: 10.1016/j.jalgebra.2006.03.040. 223

[11] Smoktunowicz, A.; Vendramin, L. *J. Comb. Algebra* **2** (2018), no. 1, 47–86. MR3763907, Zbl 1416.16037, doi: 10.4171/jca/2-1-3. 224

(Teresa Crespo) Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain
teresa.crespo@ub.edu

This paper is available via http://nyjm.albany.edu/j/2025/31-10.html.