SCHUR–ZASSENHAUS ON SKEW BRACES

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Anna Rio

08-2023

SCHUR-ZASSENHAUS

- Let G be a finite group and write $|G| = ab$ where $(a, b) = 1$.

  If G has a normal subgroup G_1 of order a (normal Hall subgroup)

  then it has a subgroup G_2 of order b.

  The group G is the semidirect product $G_1 \rtimes G_2$ where G_2 acts on G_1 by conjugation

- Any two subgroups of order b in G are conjugate to each other

- $|G| = 12p$ b=12 a=p prime $p \geq 7$

  Sylow $\Longrightarrow$ unique (normal) p-Sylow $\Longrightarrow G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes G_2$ G_2 of order 12

  - If B is a brace of size 12p, the additive and the multiplicative groups are of this kind

"SCHUR-ZASSENHAUS" SKEW BRACES

- $(B, \cdot, \circ)$ skew left brace of size np, p odd prime
- Hypothesis: all groups of size np have a normal subgroup of order p.
- Additive group $(B, \cdot)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \rtimes E$
- Multiplicative group $(B, \circ)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \rtimes F$
- E,F groups of order n

- Aim 1: show that E, F are the additive and multiplicative group of a brace of size n
- Aim 2: obtain all braces of size np from the family of braces of size n

SKEW BRACES DOUBLE SEMIDIRECT PRODUCT

- A, B skew left braces $\lambda_a(x) = a^{-1} \cdot a \circ x$ $\lambda_a \in \mathrm{Aut}(A, \cdot\,)$
- $\sigma : (B, \cdot\,) \to \mathrm{Aut}(A, \cdot\,, \circ\,)$ $\tau : (B, \circ\,) \to \mathrm{Aut}(A, \cdot\,, \circ\,)$ group homomorphisms
- In $A \times B$ additive structure of the semidirect product $(A, \cdot\,) \rtimes_\sigma (B, \cdot\,)$

$$(a, b) \cdot (a', b') = (a \cdot \sigma(b)(a'), b \cdot b')$$

multiplicative structure of the semidirect product $(A, \circ\,) \rtimes_\tau (B, \circ\,)$

$$(a, b) \circ (a', b') = (a \circ \tau(b)(a'), b \circ b')$$

- Assume $\sigma(b_1 \circ b_2) = \tau(b_1)\sigma(b_2)\tau(b_1)^{-1}\sigma(b_1) = \sigma(b_2)^{\tau(b_1)}\sigma(b_1)$

  and $\sigma(b_2)^{\tau(b_1)}$ commutes with every λ_a
- Then $(A \times B, \cdot\,, \circ\,)$ is a skew brace.

EXAMPLE

- A trivial brace $\lambda_a = Id$
- $\sigma : (B, \cdot) \to \mathrm{Aut}(A)$ $\tau : (B, \circ) \to \mathrm{Aut}(A)$ group homomorphisms
- In $A \times B$ additive structure of the semidirect product $(A, \cdot) \rtimes_\sigma (B, \cdot)$

$$(a, b) \cdot (a', b') = (a\,\sigma(b)(a'), b \cdot b')$$

multiplicative structure of the semidirect product $(A, \circ) \rtimes_\tau (B, \circ)$

$$(a, b) \circ (a', b') = (a\,\tau(b)(a'), b \circ b')$$

- If $\mathrm{Aut}(A)$ is abelian $\tau(b_1)\sigma(b_2)\tau(b_1)^{-1}\sigma(b_1) = \sigma(b_2)\sigma(b_1) = \sigma(b_1)\sigma(b_2)$

  and $\sigma(b_2)^{\tau(b_1)} = \sigma(b_2)$ commutes with every λ_a ✔

- If $\sigma(b_1 \circ b_2) = \sigma(b_1)\sigma(b_2)$ then $(A \times B, \cdot, \circ)$ is a skew brace.

SIZE NP

- A trivial brace $\mathbb{Z}_p$ $\quad$ $\mathrm{Aut}(A)=\mathbb{Z}_p^*$ is abelian
- $(B, \cdot, \circ)$ skew brace of size n
- $\sigma : (B, \cdot, \circ) \to \mathbb{Z}_p^*$ brace homomorphism
- $\tau : (B, \circ) \to \mathbb{Z}_p^*$ group homomorphism
- There is a skew brace with additive structure $\mathbb{Z}_p \rtimes_\sigma (B, \cdot)$ and multiplicative structure $\mathbb{Z}_p^* \rtimes_\tau (B, \circ)$
- From braces of size n, we can construct braces of size np $\quad$ All? $\quad$ How many?

ALL?

- Proposition $(B_{np}, \cdot, \circ)$ a skew brace such that $(B_{np}, \cdot) = N_p N_1$ and $(B_{np}, \circ) = G_p G_1$
  Then $(N_1, \cdot)$, $(G_1, \circ)$ are the additive and multiplicative structures of a brace B_n and
  $\sigma : N_1 \to \mathrm{Aut}(N_p)$ is a brace morphism

- Brace condition $x \circ (y \cdot z) = (x \circ y) \cdot x^{-1} \cdot (x \circ y)$
- …
- $(m + \tau(a)(n + \sigma(b)r),\ a \circ b \cdot c) = (m + \tau(a)n + \sigma(a \circ b)\sigma(a^{-1})\tau(a)r,\ a \circ b \cdot a^{-1} \cdot a \circ c)$
- Equality of second components gives brace B_n
- Equality of first components gives σ brace morphism
- Remark: $G_1 = \{(a, \lambda_a) \mid a \in N_1\}$ $a \circ b = a\lambda_a(b)$ $\sigma(a \circ b) = \sigma(a)\sigma(b) \iff \sigma\lambda_a = \sigma \quad \forall a$

HOW MANY?

- $(B_n, \cdot, \circ)$ brace size n $\quad \sigma : (B_n, \cdot, \circ) \to \mathbb{Z}_p^* \quad \tau : (B_n, \circ) \to \mathbb{Z}_p^*$
- In $\mathbb{Z}_p \times B_n$ two brace structures
- $(m, a) \cdot (n, b) = (m + \sigma(a)n, a \cdot b)$

$$(m, a) \circ (n, b) = \begin{cases} (m + \tau(a)n,\ a \circ b) \\ (\sigma(b)m + \tau(a)\sigma(a)n,\ a \circ b) \end{cases}$$

$$\lambda_x(y) = x^{-1} \cdot (x \circ y) = (-\sigma(a^{-1})m, a^{-1}) \cdot (m, a) \circ (n, b) = \begin{cases} (\sigma(a^{-1})\tau(a)n,\ \lambda_a(b)) \\ (\tau(a)n - \sigma(a^{-1})m + \sigma(a^{-1})\sigma(b)m,\ \lambda_a(b)) \end{cases}$$

(x, λ_x) in the holomorph

CLASSIFY AND COUNT: HOLOMORPH REFORMULATION

- Aim: Regular subgroups of $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$
- Automorphisms semidirect product $N = \mathbb{Z}_p \rtimes_\sigma E$ (following Curran, 2008)
  - $M = \begin{pmatrix} k & \gamma \\ 0 & \lambda \end{pmatrix}$ $k \in \mathbb{Z}_p^*$ $\lambda \in \mathrm{Aut}(E)$ such that $\sigma\lambda = \sigma$ $\gamma : E \to \mathbb{Z}_p$ 1-cocycle
  - Action on N $\begin{pmatrix} k & \gamma \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} m \\ a \end{pmatrix} = \begin{pmatrix} km + \gamma(a) \\ \lambda(a) \end{pmatrix}$
  - Schur Zassenhaus: subgroups of order n are conjugates of E by elements in $\mathbb{Z}_p$ leaves us with the coboundaries $\gamma_i(a) = i - \sigma(a)i, \quad i \in \mathbb{Z}_p$ (trivial σ, get $\times$)
- Order of $\mathrm{Aut}(N) = p(p-1)s$ $s = \#\{\lambda \in \mathrm{Aut}(E) : \sigma\lambda = \sigma\} = \#\Sigma_\sigma$ stabilizer of σ under the action of $\mathrm{Aut}(E)$ on $\mathrm{Hom}(E, \mathbb{Z}_p^*)$ (orbit gives $\mathbb{Z}_p \rtimes_{\sigma'} E \simeq N$)

CLASSIFY AND COUNT: HOLOMORPH REFORMULATION

$$\mathrm{Hol}(N) = \mathrm{Hol}(\mathbb{Z}_p \rtimes_\sigma E) = \left\{ [\begin{pmatrix} m \\ a \end{pmatrix}, M] \qquad m \in \mathbb{Z}_p,\ a \in E,\ M \in \mathrm{Aut}(\mathbb{Z}_p \rtimes_\sigma E) \right\}$$

$$[u, M_u][v, M_v] = [u \cdot M_u v,\ M_u M_v]$$

- <u>Brace of size n data</u>
  - $(E, \cdot\,)$ group
  - $F = \{(a, \lambda_a) : a \in E\}$ regular subgroup of Hol(E)
  - $\tau \in \mathrm{Hom}(F, \mathbb{Z}_p^*)$ $\qquad$ $\sigma \in \mathrm{Hom}(E, \mathbb{Z}_p^*)$ such that $\sigma\lambda_a = \sigma$ for all $a \in E$

CLASSIFY AND COUNT: HOLOMORPH REFORMULATION

$$\mathrm{Hol}(\mathbb{Z}_p \rtimes_\sigma E) = \left\{ [\begin{pmatrix} m \\ a \end{pmatrix}, M] \quad m \in \mathbb{Z}_p,\ a \in E,\ M \in \mathrm{Aut}(\mathbb{Z}_p \rtimes_\sigma E) \right\}$$

- Regular subgroups $\{(x, \lambda_x) : x \in N\}$

$$G(\sigma, \tau) = \left\{ [\begin{pmatrix} m \\ a \end{pmatrix}, \begin{pmatrix} \sigma(a)^{-1}\tau(a, \lambda_a) & 0 \\ 0 & \lambda_a \end{pmatrix}] \quad m \in \mathbb{Z}_p, a \in E \right\}$$

$$G(\sigma, \tau)' = \left\{ [\begin{pmatrix} m \\ a \end{pmatrix}, \begin{pmatrix} \tau(a, \lambda_a) & \gamma_{-\sigma(a^{-1})m} \\ 0 & \lambda_a \end{pmatrix}] \quad m \in \mathbb{Z}_p, a \in E \right\}$$

CLASSIFY AND COUNT

- Are regular subgroups of $\mathrm{Hol}(\mathbb{Z}_p \rtimes_\sigma E)$ isomorphic to $\mathbb{Z}_p \rtimes_\tau F$
- We have $G(1,\tau) = G(1,\tau)'$ for any τ
- For a nontrivial σ, $G(\sigma,\tau)$ and $G(\sigma,\tau)'$ are not conjugate in $\mathrm{Hol}(\mathbb{Z}_p \rtimes_\sigma E)$
- Theorem: Any regular subgroup of $\mathrm{Hol}(N)$ isomorphic to $\mathbb{Z}_p \rtimes_\tau F$ is conjugate to $G(\sigma,\tau)$ or $G(\sigma,\tau)'$ by an element of $\mathrm{Aut}(N)$
  - Regularity

$$\begin{array}{cccc} \nu_{k,l}: & \mathbb{Z}_p & \longrightarrow & \mathrm{Hol}(N) \\ & m & \rightarrow & \left[\begin{pmatrix} m \\ 1 \end{pmatrix}, \begin{pmatrix} 1 & \gamma_{lm} \\ 0 & 1 \end{pmatrix}\right] \end{array} \qquad \begin{array}{cccc} \Psi_\alpha: & F & \longrightarrow & \mathrm{Hol}(N) \\ & (a,\lambda_a) & \rightarrow & \left[\begin{pmatrix} 0 \\ a \end{pmatrix}, \begin{pmatrix} \alpha(a) & 0 \\ 0 & \lambda_a \end{pmatrix}\right] \end{array}$$

  - Conjugacy classes of images by elements in $\mathrm{Aut}(N)$
  - Isomorphic to $\mathbb{Z}_p \rtimes_\tau F$

CLASSIFY AND COUNT

- F, F' not conjugate in Hol(E) , images by Ψ_α not conjugate in Hol(N)

- Count different brace structures: determine conjugation orbits in the families $\{G(\sigma,\tau)\}_{\sigma,\tau}$ and $\{G(\sigma,\tau)'\}_{\sigma,\tau}$ (isomorphism classes of braces structures)

- σ up to brace automorphisms of $(B_n, \cdot\,, \circ\,)$,
- τ up to brace automorphisms of $(B_n, \circ\,)$

ALGORITHM

- Goal: determine all skew braces of size np from skew braces of size n
- Step 0 (Precomputation) Determine isomorphism classes of groups E of order n and the number of braces of size n of each type (E,F), F in a system of representatives for conjugacy classes (by Aut(E)) of regular subgroups of Hol(E)
- For every E compute stabilisers Σ_σ for action$(g, \sigma) \to \sigma g$ of Aut(E) on Hom(E,$\mathbb{Z}_p^*$)
- Fix a pair (E,F) as brace B_n
- **Output**: number of braces of size np having additive group isomorphic to $\mathbb{Z}_p \rtimes E$ and multiplicative group isomorphic to $\mathbb{Z}_p \rtimes F$

ALGORITHM

- **Step 1** Determine $\mathrm{Hom}(B_n, \mathbb{Z}_p^*) = \left\{ \sigma \in \mathrm{Hom}(E, \mathbb{Z}_p^*) : \ \pi_2(F) \subseteq \Sigma_\sigma \right\}$ $\quad (\ \sigma\lambda_a = \sigma \ )$
- **Step 2** Determine $\mathrm{Aut}(B_n) = \left\{ g \in \mathrm{Aut}(E) : \ \Phi_g(F) = F \right\}$

  Φ_g inner automorphism of Hol(E) acting $\Phi_g(x, \lambda) = (gx, g\lambda g^{-1})$
- **Step 3** Compute orbits of the action $(g, \sigma) \to \sigma g$ of $\mathrm{Aut}(B_n)$ on $\mathrm{Hom}(B_n, \mathbb{Z}_p^*)$

  The orbit of $\sigma = 1$, direct product, has a single element. The remaining orbits will give rise to two different braces. Number of additive structures is the number of orbits
- **Step 4** For each σ in a system of representatives of the above orbits, compute orbits of the action $(g, \tau) \to \tau\Phi_g$ of $(\mathrm{Aut}(B_n) \cap \Sigma_\sigma)$ on $\mathrm{Hom}(F, \mathbb{Z}_p^*)$

  The number of multiplicative structures is twice the number of orbits except for trivial σ, when we get a single one

NUMBER OF BRACES OF SIZE NP

- The number of additive structures is

$$\sum_{(B_n,\cdot)} \frac{1}{|\mathrm{Aut}(B_n)|} \sum_{\sigma \in \mathrm{Hom}(B_n, \mathbb{Z}_p^*)} |\mathrm{Stab}_{\mathrm{Aut}(B_n)}(\sigma)|$$

- The total amount of braces of size np is

$$\sum_{(B_n,\cdot)} \left(\frac{1}{|A_1|} \sum_{\tau \in H} |\mathrm{Stab}_{A_1}(\tau))| + 2 \sum_{\sigma \neq 1} \frac{1}{|A_\sigma|} \sum_{\tau \in H} |\mathrm{Stab}_{A_\sigma}(\tau)| \right)$$

H=$\mathrm{Hom}((B_n, \circ), \mathbb{Z}_p^*)$, $\sigma \in \mathrm{Hom}(B_n, \mathbb{Z}_p^*)$ runs over a system of representatives for additive structures and $A_\sigma = \mathrm{Aut}(B_n) \cap \mathrm{Stab}_{\mathrm{Aut}(B_n,\cdot)}(\sigma)$

- Using Burnside formula, can be given in terms of fixed points of actions

N=12 PRECOMPUTATION

$E \backslash F$	C_{12}	$C_6 \times C_2$	A_4	$D_{2\cdot 6}$	Dic_{12}
C_{12}	1	1	0	2	1
$C_6 \times C_2$	1	1	1	1	1
A_4	0	2	4	0	2
$D_{2\cdot 6}$	2	2	0	4	2
Dic_{12}	2	2	0	4	2

Braces of size 12

N=12 PRECOMPUTATION

- $E = C_{12}$ $\mathrm{Aut}\,E = \langle 5\rangle \times \langle 7\rangle = \mathbb{Z}_{12}^*$ $\mathrm{Hom}(E, \mathbb{Z}_p^*) \simeq \langle \zeta_D\rangle$ $D = \gcd(12, p-1)$ $\sigma(c) = \zeta_d^j$

k	d	$\varphi(d)$	Orbit of $\sigma = (d, j \bmod d)$	Σ_σ
12	1	1	1	$\mathrm{Aut}(E)$
6	2	1	1	$\mathrm{Aut}(E)$
4	3	2	$1 \xrightarrow{5} 2$	$\{1,7\}$
3	4	2	$1 \xrightarrow{7} 3$	$\{1,5\}$
2	6	2	$1 \xrightarrow{5} 5$	$\{1,7\}$
1	12	4	$1 \xrightarrow{5} 5 \xrightarrow{11} 7 \xrightarrow{5} 11$	$\{1\}$

The number of isomorphism classes of semidirect products $\mathbb{Z}_p \rtimes C_{12}$ is equal to the number of divisors of gcd(12,p-1)

- $E = C_6 \times C_2 = \langle a\rangle \times \langle b\rangle$ $\mathrm{Aut}\,E = D_{2\cdot 6} = \langle g_1, g_2\rangle$ $\mathrm{Hom}(E, \mathbb{Z}_p^*) \simeq \langle \zeta_D\rangle \times \{\pm 1\}$ $D = \gcd(6, p-1)$

k	d	Orbit of $\sigma = (j \bmod d, i \bmod 2)$	Σ_σ			
12	1	$(1,0)$	$\mathrm{Aut}(E)$			
6	2	$(1,0) \xrightarrow{g_2} (0,1) \xrightarrow{g_2} (1,1)$	$g_2^m\langle g_2^3, g_1\rangle g_2^{-m}$	$= \langle g_2^3,\ g_2^{2m} g_1\rangle$	$m = 0,1,2$	$C_2 \times C_2$
4	3	$(1,0) \xrightarrow{g_2} (2,0)$	$g_2^m\langle g_2^2, g_1\rangle g_2^{-m}$	$= \langle g_2^2,\ g_2^{2m} g_1\rangle$	$m = 0,1$	S_3
2	6	$(1,0) \xrightarrow{g_2} (2,1) \xrightarrow{g_2} (1,1) \xrightarrow{g_2} (5,0) \xrightarrow{g_2} (4,1) \xrightarrow{g_2} (5,1)$	$g_2^m\langle g_1\rangle g_2^{-m}$	$= \langle\ g_2^{2m} g_1\rangle$	$m = 0,1,2$	C_2

N=12 PRECOMPUTATION

- $E = A_4$ $\quad \mathrm{Aut}\,E = S_4 \quad \mathrm{Hom}(E, \mathbb{Z}_p^*) \simeq \langle \zeta_3 \rangle$

k	d	Orbit of $\sigma = j \bmod 3$	Stabiliser Σ_σ
12	1	0	S_4
4	3	$1 \xrightarrow{\phi_{(1,2)}} 2$	A_4

- $E = D_{2\cdot 6}$ $\quad \mathrm{Aut}\,E = D_{2\cdot 6} \quad \mathrm{Hom}(E, \mathbb{Z}_p^*) \simeq V_4$

	k	d	Orbit of σ	Stabiliser Σ_σ
	12	1	$(1, 1)$	$\mathrm{Aut}(E)$
Cyclic	6	2	$(1, -1)$	$\mathrm{Aut}(E)$
Dihedral	6	2	$(-1, -1) \xrightarrow{g_2} (-1, 1)$	$\langle g_1, g_2^2 \rangle \simeq D_{2\cdot 3}$

- $E = Dic_{12}$ $\quad \mathrm{Aut}\,E = D_{2\cdot 6} \quad \mathrm{Hom}(E, \mathbb{Z}_p^*) \simeq \langle \zeta_D \rangle \quad D = \gcd(4, p-1)$

k	d	Orbit of $\sigma = (d, j)$	Stabiliser Σ_σ
12	1	$(1, 1)$	$\mathrm{Aut}(E)$
6	2	$(2, 1)$	$\mathrm{Aut}(E)$
3	4	$(4, 1) \underset{g_2^3}{\xrightarrow{g_1}} (4, 3)$	$\langle g_2^2, g_1 g_2 \rangle \simeq D_{2\cdot 3}$

12P EXAMPLE $E = D_{12}$ $F = C_6 \times C_2$

- $E = \langle r, s \rangle$ $\quad \mathrm{Aut}\, E = D_{2\cdot 6} = \langle g_1, g_2 \rangle$ $\quad \Sigma_\sigma = \mathrm{Aut}(E)$ or $\langle g_1, g_2^2 \rangle$

- 2 regular subgroups in Hol(E) isomorphic to $C_6 \times C_2$

$$F_1 = \langle a_1 = (r, Id),\ b_1 = (s, g_1) \rangle \qquad \pi_2 = \langle g_1 \rangle \subset \Sigma_\sigma$$

$$F_2 = \langle a_2 = (r, g_2^4),\ b_2 = (s, Id) \rangle \qquad \pi_2 = \langle g_2^4 \rangle \subset \Sigma_\sigma$$

- g_2^3 brace automorphism in both cases $\Longrightarrow$ orbits give 3 additive structures
$\sigma = (\sigma(r), \sigma(s)) = (1,1), (1, -1), (-1,1)$

- In both cases $\mathrm{Aut}(B) = \{ g \in \mathrm{Aut}(E) :\ \Phi_g(F) = F \} = \langle g_2^3, g_1 \rangle$

$$\Phi_{g_1}(a) = a^5 \quad \Phi_{g_1}(b) = b \quad \Phi_{g_2^3}(a) = a \quad \Phi_{g_2^3}(b) = a^3 b$$

12P EXAMPLE E= D_{12} F=$C_6 \times C_2$

- Action of $\mathrm{Aut}(B)=\langle g_2^3, g_1\rangle$ on $\mathrm{Hom}(F, \mathbb{Z}_p^*)$ (same for both F)
- $\tau = (j \mod d, i \mod 2)$

$d=2$ $(0,1)\bullet \circlearrowleft$ $(1,0)\bullet \overset{g_2^3}{\longleftrightarrow} \bullet (1,1)$

$d=3$ $(1,0)\bullet \overset{g_1}{\longleftrightarrow} \bullet (2,0)$

$d=6$ $(2,1)\bullet \overset{g_1}{\longleftrightarrow} \bullet (4,1)$

$$\begin{array}{ccc} (1,0)\bullet & \overset{g_1}{\longleftrightarrow} & \bullet(5,0) \\ g_2^3 \updownarrow & & \updownarrow g_2^3 \\ (1,1)\bullet & \overset{g_1}{\longleftrightarrow} & \bullet(5,1) \end{array}$$

But action was restricted to $\mathrm{Aut}(B) \cap \Sigma_\sigma$

For σ of order 6 with dihedral kernel $g_2^3 \notin \Sigma_\sigma$ and in first and last case orbits split.

12P EXAMPLE $E = D_{12}$ $F = C_6 \times C_2$

- The number of braces with additive group $N = \mathbb{Z}_p \rtimes D_{12}$ and multiplicative group $G = \mathbb{Z}_p \rtimes (C_6 \times C_2)$ is as shown in the following table (we need $p \equiv 1 \bmod 12/k$ for a kernel of size k to occur)

$N \backslash G$	$\mathbf{Z}_p \times (C_6 \times C_2)$	$\mathbf{Z}_p \rtimes_6 (C_6 \times C_2)$	$\mathbf{Z}_p \rtimes_4 (C_6 \times C_2)$	$\mathbf{Z}_p \rtimes_2 (C_6 \times C_2)$	
$\mathbf{Z}_p \times D_{2\cdot 6}$	2	4	2	4	*2#orbits*
$\mathbf{Z}_p \rtimes_6^c D_{2\cdot 6}$	4	8	4	8	*4#orbits*
$\mathbf{Z}_p \rtimes_6^d D_{2\cdot 6}$	4	12	4	12	

TOTAL NUMBERS

- If $p \equiv 11 \pmod{12}$

	C_{12}	$C_6 \times C_2$	A_4	$D_{2\cdot 6}$	Dic_{12}	
C_{12}	6	9	0	21	6	
$C_6 \times C_2$	6	8	1	17	6	
A_4	0	4	4	0	4	
$D_{2\cdot 6}$	12	34	0	90	12	
Dic_{12}	12	18	0	42	12	
	36	73	5	170	40	**324**

- If $p \equiv 7 \pmod{12}$

	C_{12}	$C_6 \times C_2$	A_4	$D_{2\cdot 6}$	Dic_{12}	
C_{12}	36	54	0	21	6	
$C_6 \times C_2$	36	46	8	17	6	
A_4	0	32	32	0	4	
$D_{2\cdot 6}$	24	68	0	90	12	
Dic_{12}	24	36	0	42	12	
	120	236	40	170	40	**606**

- If $p \equiv 5 \pmod{12}$

	C_{12}	$C_6 \times C_2$	A_4	$D_{2\cdot 6}$	Dic_{12}	
C_{12}	17	9	0	21	17	
$C_6 \times C_2$	9	8	1	17	9	
A_4	0	4	4	0	6	
$D_{2\cdot 6}$	18	34	0	90	18	
Dic_{12}	34	18	0	42	34	
	78	73	5	170	84	**410**

- If $p \equiv 1 \pmod{12}$

	C_{12}	$C_6 \times C_2$	A_4	$D_{2\cdot 6}$	Dic_{12}	
C_{12}	94	54	0	21	17	
$C_6 \times C_2$	54	46	8	17	9	
A_4	0	32	32	0	6	
$D_{2\cdot 6}$	36	68	0	90	18	
Dic_{12}	68	36	0	42	34	
	252	236	40	170	84	**782**

We prove the conjecture Bardakov, Neshchadim and Yadav

$$s(12p) = \begin{cases} 324 & \text{if } p \equiv 11 \pmod{12}, \\ 410 & \text{if } p \equiv 5 \pmod{12}, \\ 606 & \text{if } p \equiv 7 \pmod{12}, \\ 782 & \text{if } p \equiv 1 \pmod{12}. \end{cases}$$

T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela,

Double semidirect products and skew left braces of size *np* (submitted)