Subgroup commutativity degree of $PSL(2, p^n)$

M. Farrokhi D. G. and F. Saeedi

Ferdowsi University of Mashhad

Payam Noor University of Isfahan
March 7-9, 2012

Definition

Let G be a finite group. Then the *subgroup commutativity degree* of G is

$$scd(G) = \frac{|\{(H,K) \in L(G) \times L(G) : HK = KH\}|}{|L(G)|^2},$$

where $L(G)$ denotes the lattice of all subgroups of G.

Definitions

Definition

Let G be a finite group. Then the *subgroup commutativity degree* of G is

$$scd(G) = \frac{|\{(H,K) \in L(G) \times L(G) : HK = KH\}|}{|L(G)|^2},$$

where $L(G)$ denotes the lattice of all subgroups of G.

Example

Definitions

Definition

Let G be a finite group. Then the *subgroup commutativity degree* of G is

$$scd(G) = \frac{|\{(H,K) \in L(G) \times L(G) : HK = KH\}|}{|L(G)|^2},$$

where $L(G)$ denotes the lattice of all subgroups of G.

Example

(1) If G is a finite Dedekind group, then $scd(G) = 1$.

Definitions

Definition

Let G be a finite group. Then the *subgroup commutativity degree* of G is

$$scd(G) = \frac{|\{(H,K) \in L(G) \times L(G) : HK = KH\}|}{|L(G)|^2},$$

where $L(G)$ denotes the lattice of all subgroups of G.

Example

(1) If G is a finite Dedekind group, then $scd(G) = 1$.

(2) If $G = A_5$ is the alternating group of degree five, then $scd(G) = \frac{861}{3481}$.

Definitions

Theorem (Tărnăuceanu, 2009)

The subgroup commutativity degree of dihedral group D_{2^n} is

$$scd(D_{2^n}) = \frac{(n-2)2^{n+2} + n2^{n+1} + (n-1)^2 + 8}{(n-1+2^n)^2}.$$

Definitions

Theorem (Tărnăuceanu, 2009)

The subgroup commutativity degree of dihedral group D_{2^n} is

$$scd(D_{2^n}) = \frac{(n-2)2^{n+2} + n2^{n+1} + (n-1)^2 + 8}{(n-1+2^n)^2}.$$

Theorem (Tărnăuceanu, 2009)

The subgroup commutativity degree of generalized quaternion group Q_{2^n} is

$$scd(Q_{2^n}) = \frac{(n-3)2^{n+1} + n2^n + (n-1)^2 + 8}{(n-1+2^{n-1})^2}.$$

Definitions

Theorem (Tărnăuceanu, 2009)

The subgroup commutativity degree of dihedral group D_{2^n} is

$$scd(D_{2^n}) = \frac{(n-2)2^{n+2} + n2^{n+1} + (n-1)^2 + 8}{(n-1+2^n)^2}.$$

Theorem (Tărnăuceanu, 2009)

The subgroup commutativity degree of generalized quaternion group Q_{2^n} is

$$scd(Q_{2^n}) = \frac{(n-3)2^{n+1} + n2^{n} + (n-1)^2 + 8}{(n-1+2^{n-1})^2}.$$

Theorem (Tărnăuceanu, 2009)

The subgroup commutativity degree of semi-dihedral group SD_{2^n} is

$$scd(SD_{2^n}) = \frac{(n-3)2^{n+1} + n2^{n} + (3n-2)2^{n-1} + (n-1)^2 + 8}{(n-1+3\cdot 2^{n-2})^2}.$$

Definition

A group G is *factorized* if $G = HK$ for two subgroups H and K of G and such an expression is called a *factorization*. The number of factorizations of G is denoted by $F_2(G)$ and is called the *factorization number* of G.

Definition

A group G is *factorized* if $G = HK$ for two subgroups H and K of G and such an expression is called a *factorization*. The number of factorizations of G is denoted by $F_2(G)$ and is called the *factorization number* of G.

Remark

If G is a finite group, then

$$scd(G) = \frac{1}{|L(G)|^2} \sum_{H \leq G} F_2(H) = \frac{1}{|L(G)|^2} \sum_{H \in L^*(G)} \mathcal{N}_H F_2(H),$$

where $L^*(G)$ is the set of representatives of isomorphism classes of subgroups of G and $\mathcal{N}_H$ is the number of subgroups of G isomorphic to H, for each subgroup H of G.

Preliminaries

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

(1) *Elementary abelian p-groups;*

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

(1) *Elementary abelian p-groups;*

(2) *Cyclic groups of order m, where m is a divisor of $(p^n \pm 1)/d$ and $d = \gcd(p-1, 2)$;*

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

(1) *Elementary abelian p-groups;*

(2) *Cyclic groups of order m, where m is a divisor of* $(p^n \pm 1)/d$ *and* $d = \gcd(p-1, 2)$*;*

(3) *Dihedral group of order* $2m$*, where m is as defined in* (2)*;*

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

(1) *Elementary abelian p-groups;*

(2) *Cyclic groups of order m, where m is a divisor of $(p^n \pm 1)/d$ and $d = \gcd(p-1, 2)$;*

(3) *Dihedral group of order $2m$, where m is as defined in (2);*

(4) *Alternating group A_4 if $p > 2$ or $p = 2$ and $n \equiv 0 \pmod 2$;*

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

(1) *Elementary abelian p-groups;*

(2) *Cyclic groups of order m, where m is a divisor of $(p^n \pm 1)/d$ and $d = \gcd(p-1, 2)$;*

(3) *Dihedral group of order 2m, where m is as defined in (2);*

(4) *Alternating group A_4 if $p > 2$ or $p = 2$ and $n \equiv 0 \pmod 2$;*

(5) *Symmetric group S_4 if $p^{2n} \equiv 1 \pmod{16}$;*

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

(1) *Elementary abelian p-groups;*

(2) *Cyclic groups of order m, where m is a divisor of $(p^n \pm 1)/d$ and $d = \gcd(p-1, 2)$;*

(3) *Dihedral group of order $2m$, where m is as defined in (2);*

(4) *Alternating group A_4 if $p > 2$ or $p = 2$ and $n \equiv 0 \pmod 2$;*

(5) *Symmetric group S_4 if $p^{2n} \equiv 1 \pmod{16}$;*

(6) *Alternating group A_5 if $p = 5$ or $p^{2n} \equiv 1 \pmod 5$;*

Preliminaries

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

(1) *Elementary abelian p-groups;*

(2) *Cyclic groups of order m, where m is a divisor of $(p^n \pm 1)/d$ and $d = \gcd(p-1, 2)$;*

(3) *Dihedral group of order $2m$, where m is as defined in (2);*

(4) *Alternating group A_4 if $p > 2$ or $p = 2$ and $n \equiv 0 \pmod 2$;*

(5) *Symmetric group S_4 if $p^{2n} \equiv 1 \pmod{16}$;*

(6) *Alternating group A_5 if $p = 5$ or $p^{2n} \equiv 1 \pmod 5$;*

(7) *A semi-direct product of an elementary abelian p-group of order p^m and a cyclic group of order k, where k is a divisor of $p^m - 1$ and $p^n - 1$;*

Theorem (L. E. Dickson, 1958)

Any subgroup of $PSL(2, p^n)$ is isomorphic to one of the following families of groups:

(1) *Elementary abelian p-groups;*

(2) *Cyclic groups of order m, where m is a divisor of $(p^n \pm 1)/d$ and $d = \gcd(p-1, 2)$;*

(3) *Dihedral group of order $2m$, where m is as defined in (2);*

(4) *Alternating group A_4 if $p > 2$ or $p = 2$ and $n \equiv 0 \pmod 2$;*

(5) *Symmetric group S_4 if $p^{2n} \equiv 1 \pmod{16}$;*

(6) *Alternating group A_5 if $p = 5$ or $p^{2n} \equiv 1 \pmod 5$;*

(7) *A semi-direct product of an elementary abelian p-group of order p^m and a cyclic group of order k, where k is a divisor of $p^m - 1$ and $p^n - 1$;*

(8) *The group $PSL(2, p^m)$ if m is a divisor of n, or the group $PGL(2, p^m)$ if $2m$ is a divisor of n.*

Theorem

If $G = PSL(2, p^n)$, then there exist subgroups $\mathcal{H}$, $\mathcal{K}$ and $\mathcal{L}$ of G such that

$$G = \bigcup_{g \in G} \mathcal{H}^g \cup \bigcup_{g \in G} \mathcal{K}^g \cup \bigcup_{g \in G} \mathcal{L}^g,$$

$\mathcal{H}$ is a Sylow p-subgroup of G, which is elementary abelian of order p^n, $\mathcal{K}$ is cyclic of order $(p^n - 1)/d$ and $\mathcal{L}$ is cyclic of order $(p^n + 1)/d$, where $d = \gcd(p - 1, 2)$. Moreover

$$[G : N_G(\mathcal{H})] = p^n + 1,$$
$$[G : N_G(\mathcal{K})] = p^n(p^n + 1)/2,$$

and

$$[G : N_G(\mathcal{L})] = p^n(p^n - 1)/2.$$

Theorem (M. Farrokhi D. G., 2012)

If $G=\mathbb{Z}_p^n$ is an elementary abelian p-group, then

$$F_2(G)=\sum_{0\leq i+j\leq n} p^{ij}\begin{bmatrix} n \\ i,j \end{bmatrix}_p,$$

where

$$\begin{bmatrix} n \\ i,j \end{bmatrix}_p=\frac{(p^n-1)\cdots(p-1)}{(p^i-1)\cdots(p-1)(p^j-1)\cdots(p-1)(p^{n-i-j}-1)\cdots(p-1)}$$

is a Gaussian trinomial integer.

Theorem (M. Farrokhi D. G. and F. Saeedi, 2012)

If $G = \mathbb{Z}_n$ is a cyclic group, then

$$F_2(G) = \prod_{i=1}^{m} (2\alpha_i + 1),$$

where $n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$.

Theorem (M. Farrokhi D. G. and F. Saeedi, 2012)

If $G = \mathbb{Z}_n$ is a cyclic group, then

$$F_2(G) = \prod_{i=1}^{m}(2\alpha_i + 1),$$

where $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$.

Theorem

Theorem (M. Farrokhi D. G. and F. Saeedi, 2012)

If $G = \mathbb{Z}_n$ is a cyclic group, then

$$F_2(G) = \prod_{i=1}^{m} (2\alpha_i + 1),$$

where $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$.

Theorem

(1) *If $G = A_4$, then $F_2(G) = 27$.*

Theorem (M. Farrokhi D. G. and F. Saeedi, 2012)

If $G=\mathbb{Z}_n$ is a cyclic group, then

$$F_2(G)=\prod_{i=1}^{m}(2\alpha_i+1),$$

where $n=p_1^{\alpha_1}\ldots p_m^{\alpha_m}$.

Theorem

(1) *If $G=A_4$, then $F_2(G)=27$.*

(2) *If $G=S_4$, then $F_2(G)=177$.*

Theorem (M. Farrokhi D. G. and F. Saeedi, 2012)

If $G = \mathbb{Z}_n$ is a cyclic group, then

$$F_2(G) = \prod_{i=1}^{m}(2\alpha_i + 1),$$

where $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$.

Theorem

(1) *If $G = A_4$, then $F_2(G) = 27$.*

(2) *If $G = S_4$, then $F_2(G) = 177$.*

(3) *If $G = A_5$, then $F_2(G) = 237$.*

Theorem (M. Farrokhi D. G. and F. Saeedi, 2012)

Let $G = D_{2n}$ be a dihedral group. Then

$$F_2(G) = \begin{cases} \phi_n + 2\delta_n, & odd\ \ n, \\ \phi_n + 2\phi_{\frac{n}{2}} + 2\delta_n, & even\ \ n, \end{cases}$$

where

$$\phi_n = \prod_{i=1}^{m} \left(2\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} - 1 \right)$$

and

$$\delta_n = \prod_{i=1}^{m} \left(\alpha_i + \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right)$$

for $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$.

Theorem (M. Farrokhi D. G. and F. Saeedi, 2012)

Let $G = PSL(2, p^n)$ be a projective special linear group. Then

$$F_2(G) = \begin{cases} 2|L(G)| + 2p^n(p^{2n} - 1) - 1, & p = 2, n > 1, \\ 2|L(G)| + p^n(p^{2n} - 1) - 1, & p > 2 \textit{ and } (p^n - 1)/2 \textit{ is odd}, \\ & p^n \neq 3, 7, 11, 19, 23, 59, \\ 2|L(G)| - 1, & p > 2 \textit{ and } (p^n - 1)/2 \textit{ is even}, \\ & p^n \neq 5, 9, 29 \end{cases}$$

and

$$F_2(G) = 17, 27, 237, 1141, 2033, 4935, 17223, 48261, 68799, 780695$$

if

$$p^n = 2, 3, 5, 7, 9, 11, 19, 23, 29, 59,$$

respectively.

Theorem (M. Farrokhi D. G. and F. Saeedi, 2012)

Let $G=PGL(2,p^n)$ $(p>2)$ be a projective general linear group and M be the unique subgroup of G isomorphic to $PSL(2,p^n)$. Then

$$F_2(G)=\begin{cases}3p^n(p^{2n}-1)+4|L(G)|-2|L(M)|-3, & n \text{ even or } p\equiv 1 \pmod 4,\\ 4p^n(p^{2n}-1)+4|L(G)|-2|L(M)|-3, & n \text{ odd and } p\equiv 3 \pmod 4\end{cases}$$

if $p^n>29$ and $F_2(G)$ equals

$$177, 1103, 3083, 4919, 15549, 14529, 31093, 58429, 111567, 99527, 144297, 192349$$

if p^n equals

$$3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29,$$

respectively.

Let F be a field, $F^* = F \setminus \{0\}$ and $E \subseteq F$. Then

Let F be a field, $F^* = F \setminus \{0\}$ and $E \subseteq F$. Then

- (E) denotes the subfield generated by E,

Let F be a field, $F^* = F \setminus \{0\}$ and $E \subseteq F$. Then

- (E) denotes the subfield generated by E,
- E^+ denotes an additive subgroup F,

Let F be a field, $F^* = F \setminus \{0\}$ and $E \subseteq F$. Then

- (E) denotes the subfield generated by E,
- E^+ denotes an additive subgroup F,
- $E^\times$ denotes a multiplicative subgroup F^*,

Let F be a field, $F^* = F \setminus \{0\}$ and $E \subseteq F$. Then

- (E) denotes the subfield generated by E,
- E^+ denotes an additive subgroup F,
- $E^\times$ denotes a multiplicative subgroup F^*,
- $E \leq F$ indicates that E is a subfield of F,

Let F be a field, $F^* = F \setminus \{0\}$ and $E \subseteq F$. Then

- (E) denotes the subfield generated by E,
- E^+ denotes an additive subgroup F,
- $E^\times$ denotes a multiplicative subgroup F^*,
- $E \leq F$ indicates that E is a subfield of F,
- $E^+ \leq F^+$ indicates that E is an additive subgroup of F,

Let F be a field, $F^* = F \setminus \{0\}$ and $E \subseteq F$. Then

- (E) denotes the subfield generated by E,
- E^+ denotes an additive subgroup F,
- $E^\times$ denotes a multiplicative subgroup F^*,
- $E \leq F$ indicates that E is a subfield of F,
- $E^+ \leq F^+$ indicates that E is an additive subgroup of F,
- $E^\times \leq F^\times$ indicates that E is a multiplicative subgroup of F^*.

For a subgroup H of $\mathcal{H}$ and a subgroup K of $\mathcal{K}$, the associated additive and multiplicative subgroups E_H^+ and $E_K^\times$ of H and K of $F = GF(p^n)$ are defined as follows, respectively,

$$E_H^+ = \left\{ x \in F : \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mathcal{Z} \in H \right\}$$

and

$$E_K^\times = \left\{ y \in F : \begin{bmatrix} y & 0 \\ 0 & y^{-1} \end{bmatrix} \mathcal{Z} \in K \right\},$$

where $\mathcal{Z}$ denotes the center of $SL(2, p^n)$.

A vector space V over a field E is denoted by V/E. Moreover, if $U \subseteq V$ and $E \leq F$ is a subfield of F, then $U/E \leq V/E$ indicates that U is a subspace of V as vector spaces over E.

A vector space V over a field E is denoted by V/E. Moreover, if $U \subseteq V$ and $E \leq F$ is a subfield of F, then $U/E \leq V/E$ indicates that U is a subspace of V as vector spaces over E.

The following numbers will be used in the next theorem.

$$\Xi_n(V, F; E_1, E_2) = \sum_{\substack{V=U_1+U_2 \\ U_1/E_1 \leq V/E_1 \\ U_2/E_2 \leq V/E_2}} \left(\frac{|V|}{|U_1|} \cdot \frac{|V|}{|U_2|} \right)^n = \sum_{\substack{V=U_1+U_2 \\ U_1/E_1 \leq V/E_1 \\ U_2/E_2 \leq V/E_2}} \frac{|V|^n}{|U_1 \cap U_2|^n},$$

where V is a vector space over the field F and E_1, E_2 are subfields of F.

Theorem

Let $S = H \rtimes K$ be a subgroup of $PSL(2, p^n)$, where H is an elementary abelian p-group of order p^m and K is a cyclic group whose order divides $p^m - 1$ and $p^n - 1$. Then

$$F_2(S) = \sum_{K=XY} \Xi_1\left(H, (E_K^{\times 2}); (E_X^{\times 2}), (E_Y^{\times 2})\right).$$

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Theorem (L. E. Dickson, 1958)

The number of subgroups of $PSL(2, p^n)$ of a given type is

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Theorem (L. E. Dickson, 1958)

The number of subgroups of $PSL(2, p^n)$ of a given type is

(1) $\mathcal{N}_1 = (p^n + 1)\sum_{m=1}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_p$,

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Theorem (L. E. Dickson, 1958)

The number of subgroups of $PSL(2, p^n)$ of a given type is

(1) $\mathcal{N}_1 = (p^n + 1)\sum_{m=1}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_p,$

(2) $\mathcal{N}_2 = \frac{p^n(p^n+1)}{2}\left(\tau\left(\frac{p^n-1}{d}\right) - 1\right) + \frac{p^n(p^n-1)}{2}\left(\tau\left(\frac{p^n+1}{d}\right) - 1\right),$

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Theorem (L. E. Dickson, 1958)

The number of subgroups of $PSL(2, p^n)$ of a given type is

(1) $\mathcal{N}_1 = (p^n + 1) \sum_{m=1}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_p,$

(2) $\mathcal{N}_2 = \frac{p^n(p^n+1)}{2} \left(\tau\left(\frac{p^n-1}{d}\right) - 1\right) + \frac{p^n(p^n-1)}{2} \left(\tau\left(\frac{p^n+1}{d}\right) - 1\right),$

(3) $\mathcal{N}_3 = \frac{1}{2}|G| \left(\frac{d}{p^n-1}\sigma\left(\frac{p^n-1}{d}\right) + \frac{d}{p^n+1}\sigma\left(\frac{p^n+1}{d}\right) - 2\right),$

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Theorem (L. E. Dickson, 1958)

The number of subgroups of $PSL(2, p^n)$ of a given type is

(1) $\mathcal{N}_1 = (p^n + 1) \sum_{m=1}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_p$,

(2) $\mathcal{N}_2 = \frac{p^n(p^n+1)}{2} \left(\tau \left(\frac{p^n-1}{d} \right) - 1 \right) + \frac{p^n(p^n-1)}{2} \left(\tau \left(\frac{p^n+1}{d} \right) - 1 \right)$,

(3) $\mathcal{N}_3 = \frac{1}{2}|G| \left(\frac{d}{p^n-1} \sigma \left(\frac{p^n-1}{d} \right) + \frac{d}{p^n+1} \sigma \left(\frac{p^n+1}{d} \right) - 2 \right)$,

(4) $\mathcal{N}_4 = \frac{1}{12}|G|$ *if* $p > 2$ *and it is zero otherwise,*

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Theorem (L. E. Dickson, 1958)

The number of subgroups of $PSL(2, p^n)$ of a given type is

(1) $\mathcal{N}_1 = (p^n + 1)\sum_{m=1}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_p,$

(2) $\mathcal{N}_2 = \frac{p^n(p^n+1)}{2}\left(\tau\left(\frac{p^n-1}{d}\right) - 1\right) + \frac{p^n(p^n-1)}{2}\left(\tau\left(\frac{p^n+1}{d}\right) - 1\right),$

(3) $\mathcal{N}_3 = \frac{1}{2}|G|\left(\frac{d}{p^n-1}\sigma\left(\frac{p^n-1}{d}\right) + \frac{d}{p^n+1}\sigma\left(\frac{p^n+1}{d}\right) - 2\right),$

(4) $\mathcal{N}_4 = \frac{1}{12}|G|$ *if* $p > 2$ *and it is zero otherwise,*

(5) $\mathcal{N}_5 = \frac{1}{12}|G|$ *if* $p^n \equiv -1 \pmod 8$ *and it is zero otherwise,*

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Theorem (L. E. Dickson, 1958)

The number of subgroups of $PSL(2,p^n)$ of a given type is

(1) $\mathcal{N}_1 = (p^n+1)\sum_{m=1}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_p$,

(2) $\mathcal{N}_2 = \frac{p^n(p^n+1)}{2}\left(\tau\left(\frac{p^n-1}{d}\right)-1\right) + \frac{p^n(p^n-1)}{2}\left(\tau\left(\frac{p^n+1}{d}\right)-1\right)$,

(3) $\mathcal{N}_3 = \frac{1}{2}|G|\left(\frac{d}{p^n-1}\sigma\left(\frac{p^n-1}{d}\right) + \frac{d}{p^n+1}\sigma\left(\frac{p^n+1}{d}\right)-2\right)$,

(4) $\mathcal{N}_4 = \frac{1}{12}|G|$ *if* $p>2$ *and it is zero otherwise,*

(5) $\mathcal{N}_5 = \frac{1}{12}|G|$ *if* $p^n \equiv -1 \pmod 8$ *and it is zero otherwise,*

(6) $\mathcal{N}_6 = \frac{1}{30}|G|$ *if* $p^n \equiv \pm 1 \pmod{10}$ *and it is zero otherwise,*

Let $\mathcal{N}_i$ be the number of subgroups of type (i) in Dickson's theorem.

Theorem (L. E. Dickson, 1958)

The number of subgroups of $PSL(2, p^n)$ of a given type is

(1) $\mathcal{N}_1 = (p^n + 1)\sum_{m=1}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_p$,

(2) $\mathcal{N}_2 = \frac{p^n(p^n+1)}{2}\left(\tau\left(\frac{p^n-1}{d}\right) - 1\right) + \frac{p^n(p^n-1)}{2}\left(\tau\left(\frac{p^n+1}{d}\right) - 1\right)$,

(3) $\mathcal{N}_3 = \frac{1}{2}|G|\left(\frac{d}{p^n-1}\sigma\left(\frac{p^n-1}{d}\right) + \frac{d}{p^n+1}\sigma\left(\frac{p^n+1}{d}\right) - 2\right)$,

(4) $\mathcal{N}_4 = \frac{1}{12}|G|$ *if* $p > 2$ *and it is zero otherwise,*

(5) $\mathcal{N}_5 = \frac{1}{12}|G|$ *if* $p^n \equiv -1 \pmod 8$ *and it is zero otherwise,*

(6) $\mathcal{N}_6 = \frac{1}{30}|G|$ *if* $p^n \equiv \pm 1 \pmod{10}$ *and it is zero otherwise,*

(8) $\mathcal{N}_8 = |G|\left(\sum_{m|n} \frac{1}{|PSL(2,p^m)|} + \sum_{2m|n} \frac{1}{|PGL(2,p^m)|}\right)$.

Lemma

If $S = H \rtimes K$ is a subgroup of $PSL(2, p^n)$, where H is an elementary abelian p-group of order p^m and K is a cyclic group whose order divides $p^m - 1$ and $p^n - 1$, then

$$\mathcal{N}_S = p^n(p^n + 1)\frac{1}{p^{m_K l}} \begin{bmatrix} \frac{n}{m_K} \\ l \end{bmatrix}_{p^{m_K}},$$

where $p^{m_K} = |(E_K^{\times})|$ and $m = m_K l$.

Theorem

The number of subgroups of $PSL(2,p^n)$ of type (7) is

$$\mathcal{N}_7 = p^n(p^n+1)\left(\sum_{m|n} \alpha_{p,m}\beta_{p^m,\frac{n}{m}} - \beta_{p,n}\right),$$

where

$$\alpha_{p,m} = |\{h : dh | p^m - 1, dh \nmid p^k - 1, k < m, k|m\}|,$$

is the number of generators of the field $GF(p^m)$ in $GF(p^m)^d$ and

$$\beta_{p^m,\frac{n}{m}} = \frac{1}{p^n}\sum_{l=1}^{\frac{n}{m}} \begin{bmatrix} \frac{n}{m} \\ l \end{bmatrix}_{p^m} p^{ml} = \frac{1}{|V|}\sum_{0 \neq U \leq V} |U|,$$

in which $V = GF(p^n)/GF(p^m)$ is a vector space of dimension n/m over a field of order p^m.

Corollary

The number of subgroups of the group G is

$$|L(G)| = 1 + \mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3 + \mathcal{N}_4 + \mathcal{N}_5 + \mathcal{N}_6 + \mathcal{N}_7 + \mathcal{N}_8.$$

Let $L_i^*(G)$ be the set of representatives of isomorphism classes of subgroups of $G = PSL(2, p^n)$ of type (i) in Dickson's Theorem and

$$\mathcal{N}_i' = \sum_{S \in L_i^*(G)} \mathcal{N}_S F_2(S)$$

for $i = 1, \ldots, 8$.

Let $L_i^*(G)$ be the set of representatives of isomorphism classes of subgroups of $G = PSL(2, p^n)$ of type (i) in Dickson's Theorem and

$$\mathcal{N}_i' = \sum_{S \in L_i^*(G)} \mathcal{N}_S F_2(S)$$

for $i = 1, \ldots, 8$.

Theorem

The subgroup commutativity degree of $G = PSL(2, p^n)$ is

$$scd(G) = \frac{1 + \mathcal{N}_1' + \mathcal{N}_2' + \mathcal{N}_3' + \mathcal{N}_4' + \mathcal{N}_5' + \mathcal{N}_6' + \mathcal{N}_7' + \mathcal{N}_8'}{(1 + \mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3 + \mathcal{N}_4 + \mathcal{N}_5 + \mathcal{N}_6 + \mathcal{N}_7 + \mathcal{N}_8)^2}.$$

Problem

Give an explicit formula for the numbers $\alpha_{p,m}$.

Problem

Give an explicit formula for the numbers $\alpha_{p,m}$.

Problem

Give an explicit formula for the numbers $\Xi_n(V, F; E_1, E_2)$. Is there a close formula for the special cases $n = 0, 1$?

Problem

Give an explicit formula for the numbers $\alpha_{p,m}$.

Problem

Give an explicit formula for the numbers $\Xi_n(V, F; E_1, E_2)$. Is there a close formula for the special cases $n = 0, 1$?

Conjecture

A finite group whose subgroup commutativity degree exceeds $\frac{861}{3481}$ is solvable.

References I

- M. Blaum, Factorizations of the simple groups $PSL_3(q)$ and $PSU_3(q^2)$, *Arch. Math.*, **40** (1983), 8–13.
- L. E. Dickson, *Linear Groups With an Exposition of the Galois Field Theory*, Dover Publications, Inc., New York, 1958.
- M. Farrokhi D. G., Factorization numbers of finite abelian groups, submitted.
- The GAP Group, GAP-Groups, *Algorithms and Programming, Version 4.4.12, 2008*, (http://www.gap-system.org/).
- T. R. Gentchev, Factorizations of the sporadic simple groups, *Arch. Math.*, **47** (1986), 97–102.
- T. R. Gentchev, Factorizations of the groups of Lie type of Lie rank 1 or 2, *Arch. Math.*, **47** (1986), 493–499.

- W. H. Gustafson, What is the probability that two groups elements commute?, *Amer. Math. Monthly*, **80** (1973), 1031–1304.
- B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.
- N. Ito, On the factorizations of the linear fractional group $LF(2, p^n)$, *Acta Sci. Math. (Szeged)*, **15** (1953), 79–84.
- M. Tărnăuceanu, Subgroup commutativity degrees of finite groups, *J. Algebra*, **321**(9) (2009), 2508–2520.
- M. Tărnăuceanu, Addendum to "Subgroup commutativity degrees of finite groups" [J. Algebra 321 (9) (2009) 2508–2520], *J. Algebra*, **337**(9) (2011), 363–368.
- K. B. Tchakerian and T. R. Gentchev, Factorizations of the groups $G_2(q)$, *Arch. Math.*, **44** (1985), 230–232.

F. Saeedi and M. Farrokhi D. G., Factorization numbers of some finite groups, *Glasgow Math. J.*, Published online: 12 December 2011.

Thank You