MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 197
JANUARY 1992, PAGES 347–353

SOME DIVISIBILITY PROPERTIES OF THE SUBGROUP COUNTING FUNCTION FOR FREE PRODUCTS

MICHAEL GRADY AND MORRIS NEWMAN

Dedicated to the memory of D. H. Lehmer

ABSTRACT. Let G be the free product of finitely many cyclic groups of prime order. Let M_n denote the number of subgroups of G of index n. Let C_p denote the cyclic group of order p, and C_p^k the free product of k cyclic groups of order p. We show that M_n is odd if C_2^4 occurs as a factor in the free product decomposition of G. We also show that if C_3^3 occurs as a factor in the free product decomposition of G and if C_2 is either not present or occurs to an even power, then $M_n \equiv 0 \bmod 3$ if and only if $n \equiv 2 \bmod 4$. If, on the other hand, C_3^3 occurs as a factor, and C_2 also occurs as a factor, but to an odd power, then all the M_n are $\equiv 1 \bmod 3$. Several conjectures are stated.

1. INTRODUCTION

A recurrence formula for the number of subgroups of a given index in a free group of finite rank was given by M. Hall [5]. This was generalized to the case of a free product of finitely many cyclic groups by I. M. S. Dey [2], and to the general case of an arbitrary group by K. Wohlfahrt [9]. These numbers possess a wealth of fascinating arithmetic properties. For instance, the number of subgroups of index n in the classical modular group is odd if and only if n is of the form $2^k - 3$ or $2(2^k - 3)$ [6]. To cite another example, the number of subgroups of index $2p - 1$ in the Hecke group H_p, p prime, is $2p - 1$ [4]. That these numbers are interesting is evident from Table 1 in the Appendix (included here as a representative example) which lists them for H_{41}, for all indices ≤ 100.

In this paper we prove a number of congruence properties, and state several conjectures.

C_p will denote the cyclic group of order p. C_p^k will stand for the free product $C_p * C_p * \cdots * C_p$ of k copies of C_p. Then the classical modular group is $C_2 * C_3$, and H_p is $C_2 * C_p$.

2. THE HALL AND DEY FORMULAS

Let M_n denote the number of subgroups of index n in some specified group G. Then, if G is a free group of rank r, $M_1 = 1$ and

Received July 16, 1990; revised October 2, 1990.
1991 *Mathematics Subject Classification.* Primary 11B50, 20E06.

0025-5718/92 $1.00 + $.25 per page

$$M_n = n(n!)^{r-1} - \sum_{i=1}^{n-1} (n-i)!^{r-1} M_i, \qquad n \geq 2. \tag{1}$$

If $G = C_{p_1} * C_{p_2} * \cdots * C_{p_k}$, then $M_1 = 1$ and

$$M_n = \frac{h(n)}{(n-1)!} - \sum_{i=1}^{n-1} \frac{h(n-i)}{(n-i)!} M_i, \qquad n \geq 2, \tag{2}$$

where

$$h(n) = \tau_{p_1}(n)\, \tau_{p_2}(n) \cdots \tau_{p_k}(n),$$

and $\tau_{p_i}(n)$ is the number of homomorphisms of C_{p_i} into the symmetric group S_n.

Both (1) and (2) have an equivalent formulation in terms of generating functions.

For Dey's formula (2), let

$$g = \sum_{n=0}^{\infty} M_{n+1} x^n, \qquad f = \sum_{n=0}^{\infty} \frac{h(n)}{n!} x^n, \tag{3}$$

where $h(0)$ is defined to be 1. Then

$$g = \frac{f'}{f}. \tag{4}$$

This simple expression is useful in a variety of counting arguments (see [3, 4], for example).

3. Congruence properties, and the theorems

Parity phenomena are rather obvious for free groups of finite rank. In fact, all the M_n are odd, in this case. This follows trivially by induction from Hall's formula (1), when considered modulo 2. In fact, the behavior of these numbers can be determined (in principle) for any modulus, since (1) then becomes a linear recurrence of fixed length with constant coefficients. For example, choosing 5 as the modulus and the rank as 2, the recurrence becomes

$$M_n \equiv 4M_{n-1} + 3M_{n-2} + 4M_{n-3} + M_{n-4}, \qquad n \geq 5, \tag{5}$$

with initial values

$$M_1 \equiv 1, \quad M_2 \equiv 3, \quad M_3 \equiv 3, \quad M_4 \equiv 1.$$

The period of this sequence is 62, which determines the behavior of the indices modulo 5 completely. For example, this implies that M_n is divisible by 5 if and only if

$$n \equiv 9,\ 12,\ 19,\ 24,\ 33,\ 39,\ 41,\ 42,$$
$$45,\ 47,\ 49,\ 52,\ 58,\ 59,\ 60 \bmod 62.$$

In the same way, it is easy to show that for a free group of rank p, where p is a prime, M_n satisfies $M_n \equiv 1 \bmod p$ for all n.

The group-theoretic significance of results of this type is rather obscure.

Establishing congruence patterns for free products tends to be more challenging, since equation (2) is less convenient than (1) for that purpose. Instead of appealing to (2) directly, W. W. Stothers in [6] derives a formula for M_n for the modular group via coset diagrams. This formula is then used to prove the parity result mentioned above. These methods were extended in [8] and [7].

An interesting alternative approach was given by C. Godsil, W. Imrich, and R. Razen in [3]. They obtain a recurrence formula for $\frac{\tau_2(n)\tau_3(n)}{n!}$, and from this a recurrence for M_n via equations (3) and (4). Congruence properties are then deduced from this recurrence. The same reference mentions that the number of free subgroups of index n in $\mathrm{SL}_2(\mathbb{Z})$ is always even. This follows from a formula given by W. Imrich in [8].

T. Müller has found that $\mathrm{SL}_2(\mathbb{Z})$ exhibits the same parity pattern as the modular group [10], and more generally that similar patterns hold for a variety of free products of finite groups for which the amalgamated subgroup has odd cardinality.

In what follows we will show that Dey's formula reduces to a linear recurrence modulo p when the factors are appropriately chosen. This enables us to prove the following theorems:

Theorem 1. *Suppose that C_2^4 occurs as a factor in the free product decomposition of G. Then M_n is odd for all $n \geq 1$.*

Theorem 2. *Suppose that C_3^3 occurs as a factor in the free product decomposition of G. If C_2 does not occur as a factor, or enters to an even power, then $M_n \equiv 0 \bmod 3$ if and only if $n \equiv 2 \bmod 4$. If, on the other hand, C_2 enters to an odd power, then $M_n \equiv 1 \bmod 3$ for all n, so that M_n is never divisible by 3 in this case.*

The proofs require a number of lemmas.

Lemma 1. *The number $\tau_2(n)^4$ contains a higher power of 2 in its prime power factorization than does $n!$, for all $n > 1$.*

Proof. Let 2^{r_n} be the exact power of 2 dividing $n!$, and let 2^k be the largest power of 2 less than or equal to n, so that

$$r_n = \left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \cdots + \left[\frac{n}{2^k}\right].$$

Clearly, if $n = 2^k$, then $r_n = 2^k - 1 = n - 1$, but otherwise, $r_n < n - 1$.

From S. Chowla et al. [1] we have $\tau_2(n) \equiv 0 \bmod 2^s$ for any s such that $s \leq (n+2)/4$. Thus, if $n \equiv 2 \bmod 4$, we may choose $s = (n+2)/4$ and deduce that $\tau_2(n)^4 \equiv 0 \bmod 2^{n+2}$. Since $n+2 > r_j$ for $j = n$, $n+1$, $n+2$, or $n+3$ (even in the case $n+2 = 2^k$), the result follows. □

We can now prove Theorem 1. We have $M_1 = 1$, and by Lemma 1 and formula (2),

$$M_n \equiv M_{n-1} \bmod 2, \qquad n > 1.$$

The result now follows trivially, by induction.

The next lemma is considerably more difficult to prove.

Lemma 2. *If $n \geq 9s - 3$, then $\tau_3(n) \equiv 0 \bmod 3^{2s}$.*

Proof. We shall prove inductively the compound proposition: If $n \geq 9s-3$, then $\tau_3(n) \equiv 0 \bmod 3^{2s}$, and for $n \equiv 1 \bmod 3$,

$$\tau_3(n) \equiv \tau_3(n-1) \mod 3^{2s+1}.$$

This proposition may be verified by direct computation for $s = 1, 2$. For brevity, let T_n now denote $\tau_3(n)$. Iteration of the fundamental recursion

$$T_n = T_{n-1} + (n-1)(n-2)T_{n-3}$$

gives

$$T_n = xT_{n-7} + yT_{n-8} + zT_{n-9}, \tag{6}$$

where

$$\begin{aligned} x = x(n) &= 3n^4 - 42n^3 + 210n^2 - 441n + 351, \\ y = y(n) &= 3n^4 - 54n^3 + 342n^2 - 903n + 882, \\ z = z(n) &= n^6 - 27n^5 + 289n^4 - 1569n^3 + 4579n^2 - 6927n + 4536. \end{aligned}$$

Suppose that $n \geq 9(s+1)-3$. Then by the induction hypothesis, T_{n-7}, T_{n-8}, and T_{n-9} are all divisible by 3^{2s}; and we wish to show that $T_n \equiv 0 \bmod 3^{2s+2}$. So let $k = 2s$, $T_{n-7} = 3^k a$, $T_{n-8} = 3^k b$, $T_{n-9} = 3^k c$. We must show that

$$xa + yb + zc \equiv 0 \mod 9.$$

Working modulo 9, we have

$$\begin{aligned} x &\equiv 3n^4 + 3n^3 + 3n^2, \\ y &\equiv 3n^4 - 3n, \\ z &\equiv n^6 + n^4 - 3n^3 - 2n^2 + 3n. \end{aligned}$$

It is readily verified that $z \equiv 0 \bmod 9$ for all n and that $x \equiv y \equiv 0 \bmod 9$ unless $n \equiv 2 \bmod 3$. So let $n \equiv 2 \bmod 3$. Then $T_n \equiv 3a + 6b \equiv 0 \bmod 9$ requires $a \equiv b \bmod 3$; i.e., $T_{n-7} \equiv T_{n-8} \bmod 3^{k+1}$. By virtue of (6), this last congruence becomes

$$\begin{aligned} &x_1 T_{n-14} + y_1 T_{n-15} + z_1 T_{n-16} \\ &\quad \equiv x_2 T_{n-15} + y_2 T_{n-16} + z_2 T_{n-17} \mod 3^{k+1}, \end{aligned}$$

where we do not bother to write down the coefficients explicitly, but note that x_1, y_1, z_1 are to be evaluated at $n-7 \equiv 1 \bmod 3$, and x_2, y_2, z_2 are to be evaluated at $n-8 \equiv 0 \bmod 3$. By the induction hypothesis, $T_{n-14}, \ldots, T_{n-17}$ are all divisible by 3^{k-2}. It is a simple matter to show that $x(m) \equiv 0 \bmod 27$ when $m \equiv 0$ or $1 \bmod 3$, and that $y(m) \equiv 0 \bmod 27$ when $m \equiv 1 \bmod 3$. Thus, it remains to prove that

$$(z_1 - y_2)T_{n-16} \equiv z_2 T_{n-17} \mod 3^{k+1}.$$

Let $T_{n-16} = 3^{k-2}a$, $T_{n-17} = 3^{k-2}b$. By the induction hypothesis, $T_{n-16} \equiv T_{n-17} \bmod 3^{k-1}$, which implies that $a \equiv b \bmod 3$. But $z_2 \equiv 0 \bmod 9$, and

$$\begin{aligned} z_1(n+1) - y_2(n) &= n^6 - 21n^5 + 166n^4 - 609n^3 + 1009n^2 - 546n \\ &\equiv n^6 - 3n^5 + 4n^4 - 6n^3 + n^2 - 6n \mod 9, \end{aligned}$$

which is clearly $\equiv 0 \bmod 9$ when $n \equiv 0 \bmod 3$. This completes the proof. □

We use this lemma to prove

Lemma 3. *The number* $\tau_3(n)^3$ *contains a higher power of* 3 *in its prime power factorization than does* $n!$, *for all* $n > 2$.

Proof. Let 3^{r_n} be the exact power of 3 dividing $n!$, and let 3^k be the largest power of 3 less than or equal to n, so that

$$r_n = \left[\frac{n}{3}\right] + \left[\frac{n}{3^2}\right] + \cdots + \left[\frac{n}{3^k}\right].$$

Then $r_n \leq (n-1)/2$, with equality only when $n = 3^k$. Suppose that $n \equiv 6 \bmod 9$, and $s = (n+3)/9$. By Lemma 2,

$$\tau_3(n)^3 \equiv 0 \mod 3^{(6n+18)/9}.$$

But $(6n+18)/9 > r_j$ for $j = n, n+1, \ldots, n+8$ and $n > 9$. Direct computation verifies the lemma for $n = 1, 2, \ldots, 9$. This completes the proof. □

We can now prove Theorem 2. Suppose, first, that C_2 does not occur as a factor in the free product decomposition of G. Then if p is a prime > 2 such that C_p does occur as a factor, the fact that $\tau_p(1) = \tau_p(2) = 1$ together with Lemma 3 implies that

$$M_n \equiv 2M_{n-1} + M_{n-2} \bmod 3, \qquad n > 2, \tag{7}$$

with initial values $M_1 \equiv 1 \bmod 3$, $M_2 \equiv 0 \bmod 3$. This linear recurring sequence has period 8 and produces the values

$$1, 0, 1, 2, 2, 0, 1, 1, 0, \ldots$$

so that $M_n \equiv 0 \bmod 3$ if and only if $n \equiv 2$ or $6 \bmod 8$; or what is the same thing, if and only if $n \equiv 2 \bmod 4$.

Now suppose that C_2^k does occur as a factor in the free product decomposition of G. Formula (7) is affected by this and becomes instead

$$M_n \equiv 2M_{n-1} + 2^k M_{n-2} \bmod 3, \qquad n > 2, \tag{8}$$

with initial values $M_1 \equiv 1 \bmod 3$, $M_2 \equiv 2^k - 1 \bmod 3$. If k is even, the recurrence is unaffected and the desired conclusion holds. If k is odd, however, we find in this case that all the M_n satisfy $M_n \equiv 1 \bmod 3$. This completes the proof.

4. Conjectures

We conclude this paper by listing some plausible conjectures, which are backed up by some massive calculations.

Conjecture 1. *If* C_2^2 *occurs as a factor in the free product decomposition of* G, *then* M_n *is odd for all* n.

Conjecture 2. *Let* $G = C_p^2 * C_{p_1} * \cdots * C_{p_k}$, *where* $p_i \geq p$ *for all* i. *Then the residue of* M_n *modulo* p *for* G *is the same as for the group* C_p^2, *and this is given recursively by*

$$M_n \equiv -\sum_{i=1}^{p-1} \frac{1}{(p-i)!} M_{n-p+i} \bmod p, \qquad n > p-1. \tag{9}$$

Thus, for example, the group $C_2^2 * C_3^2$ has all M_n odd, and $M_n \equiv 0 \bmod 3$ if and only if $n \equiv 2 \bmod 4$.

Conjecture 3. *Let* p_1, p_2 *be primes, and suppose that* $p_1 \equiv 1 \bmod q$, *where* q *is a prime. Let* $G = C_{p_1} * C_{p_2}$. *Then* $M_n \equiv 0 \bmod q$ *for all* n *such that* $n \not\equiv 1 \bmod q$, $n \not\equiv p_2 \bmod q$.

Appendix

Table 1

The function Mn is the number of subgroups of index n of the Hecke group $H(41)$, the free product of a cyclic group of order 2 and a cyclic group of order 41 · Mn is 1 for $n = 1, 2$, and is 0 for $n = 3, 4, \ldots, 40$.

n	Mn
41	500105497690148365394164736
42	305265665006768519387180 8512
43	91895987247083033876830208 00
44	18185704908693293295620341760
45	26605567147947965997877324800
46	30684062537576457523098011648
47	29046727489502070108332322816
48	23206310044391063713060454400
49	15965502174441030847895051520
50	96049932973622201850573440 00
51	51132476359557326606269562 88
52	24319918454634524228463656 96
53	10413667543202075754857216 00
54	40406229228982525436814336 0
55	14279758637868805811333120 0
56	46177414574549290217127936
57	13711274707917574713174912
58	37509655609023688209600 00
59	94752766724394860290560 0
60	22158727068581376998400 0
61	48030419173229974715520
62	9669193392957415299840
63	1808183585903333184000
64	314645432937402777600
65	50898945451150836000
66	7667062835484926016
67	1072808269367542272
68	139716581918028800
69	16858019231136960
70	1890020973276800
71	195302218611968
72	18695344352256
73	1634310005900
74	131754038520
75	9541116000
76	633442368
77	36592556
78	1926600
79	82160
80	3200
81	81
82	54244392327189216972391108743544032308566006629481142930217 3698
83	47193135726410003694995858339701617072266948372792458305 06954240
84	20394558391041910084364370737774577370079277452472143590761431040
85	58366814703260040549315958464995086264884454105320124609304985600
86	12443758331710319723080836506930515411345227453486078578759041024 0
87	21079669210506767631027749963099257165600829925834913111544011161 6
88	29552524245918889373569054482986055475024164901103738300972138496 0
89	35264711339744556332513429432116980044272143218007203781687640064 0
90	36560901845074229314906325863787721762641746502319977851551744000 0
91	33452099781581017604258291604316751714975891862960996836227153920 0
92	27347241784795651221646200553144882809159157938002377838291845120 0
93	20174806739270538012338025257861823925689219680782042783742951424 0
94	13541641248855227629318146800517165364655038110791887573496365056 0
95	83268423490801113887128378022781441560556679176648989993861120000
96	47181037122994202406619926137577333046941929607442593668608819200
97	24757449861030329499521590344703990734983602083960099275373281280
98	12083167101655322150101011754513036933215073150832541218916597760
99	55060541034695926013559017450891863091048485283045235385329254 40
100	23503787901383610592336101112283416504666888304212120358092800 00

ACKNOWLEDGMENT

The authors are indebted to the referee for several helpful comments and for drawing our attention to reference [10].

BIBLIOGRAPHY

1. S. Chowla, I. N. Herstein, and K. Moore, *On recursions connected with symmetric groups. I*, Canad. J. Math **3** (1951), 328–334.
2. I. M. S. Dey, *Schreier systems in free products*, Proc. Glasgow Math. Assoc. **7** (1965), 61–79.
3. C. Godsil, W. Imrich, and R. Razen, *On the number of subgroups of given index in the modular group*, Monatsh. Math. **87** (1979), 273–280.
4. M. Grady and M. Newman, *Counting subgroups of given index in Hecke groups*, Contemp. Math., Amer. Math. Soc. (to appear).
5. M. Hall, *Subgroups of finite index in free groups*, Canad. J. Math. **1** (1949), 187–190.
6. W. W. Stothers, *The numbers of subgroups of given index in the modular group*, Proc. Roy. Soc. Edinburgh Sect. A **78** (1977), 105–112.
7. ———, *Subgroups of finite index in a free product with amalgamated subgroup*, Math. Comp. **36** (1981), 653–662.
8. W. Imrich, *On the number of subgroups of a given index in* $SL_2(\mathbb{Z})$, Arch. Math. **31** (1978), 224–231.
9. K. Wohlfahrt, *Über einen Satz von Dey und die Modulgruppe*, Arch. Math. **29** (1977), 455–457.
10. T. Müller, *Kombinatorische Aspekte endlich erzeugter virtuell freier Gruppen*, Dissertation, Johann Wolfgang Goethe-Universität, 1989.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CALIFORNIA 93106

E-mail address: newman%henri@hub.ucsb.edu