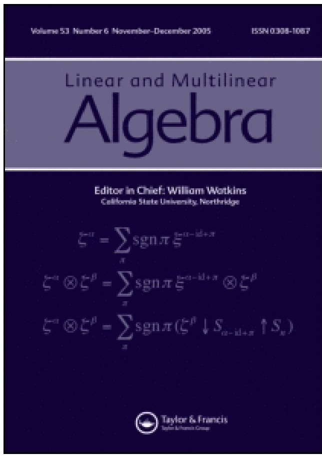

Linear and Multilinear Algebra
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713644116

Arithmetic of subgroup counting in some free products

B. Sury [a]
[a] School of Mathematics, Tata Institute of Fundamental Research, Mumbai, Homi Bhabha Road, India

Online Publication Date: 01 September 1998

To cite this Article: Sury, B. (1998) 'Arithmetic of subgroup counting in some free products', Linear and Multilinear Algebra, 44:4, 347 — 355

To link to this article: DOI: 10.1080/03081089808818570
URL: http://dx.doi.org/10.1080/03081089808818570

Linear and Multilinear Algebra, Vol. 44, pp. 347–355
Reprints available directly from the publisher
Photocopying permitted by license only

Arithmetic of Subgroup Counting in Some Free Products

B. SURY

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India

Communicated by M. Newman

(Received 25 November 1997)

Some arithmetic properties of the sequence M_n of subgroups of index n in some free products are studied. For the free product $\mathbb{Z}/2 * \mathbb{Z}/2 * \mathbb{Z}/2$, an explicit recurrence relation is obtained for the M_n's from which one deduces the corollary: M_n is always odd. For the free product $\mathbb{Z}/3 * \mathbb{Z}/3$, again an explicit recurrence is obtained for the M_n's from which one deduces: M_n is odd if, and only if, n is of the form 2^s-3. The mod 3 behaviour of M_n is periodic *viz.*, $M_n \equiv M_{n+8} \bmod 3$; the first eight values of M_n are $1, 0, 1, 2, 2, 0, 2, 1$ mod 3.

Keywords: Free products; subgroup counting

Mathematical Reviews Subject Classification: 20E06, 20D60

INTRODUCTION

Our purpose is to study some arithmetic properties of the sequence M_n of subgroups of finite index in free products of some cyclic groups. The modular group is one example that has been studied by several authors ([St, GIR]). Recently, Grady and Newman ([GN1, GN2, GN3]) have made a study of the free products of cyclic groups of prime orders. In contrast with the earlier papers, they study properties of the sequence M_n modulo appropriate primes p without actually getting a recurrence for the M_n. Here, and in what follows, M_n stands for the number of subgroups of index n in the given group. They prove the existence of a linear recurrence for M_n modulo p when $(\mathbb{Z}/p) * (\mathbb{Z}/p)$ is a free factor and $p > 3$. For the prime $p = 2$ (respectively 3), they prove that a similar recurrence exists mod p provided $(\mathbb{Z}/2) * (\mathbb{Z}/2) * (\mathbb{Z}/2) * (\mathbb{Z}/2)$ (respectively $(\mathbb{Z}/3) * (\mathbb{Z}/3) * (\mathbb{Z}/3)$) occurs as a free factor. In this note, we prove some results complementing those of [GN1, GN2, GN3] *viz.*, the following.

We get explicit recurrence formulae for M_n for the groups $(\mathbb{Z}/2) * (\mathbb{Z}/2) * (\mathbb{Z}/2)$ and $(\mathbb{Z}/3) * (\mathbb{Z}/3)$.

Then, we use these to prove:

For $G = (\mathbb{Z}/2) * (\mathbb{Z}/2) * (\mathbb{Z}/2)$, M_n is odd for all n.

For $G = (\mathbb{Z}/3) * (\mathbb{Z}/3)$, M_n is odd if, and only if, n is of the form $2^s - 3$.

The mod 3 behaviour of M_n is periodic *viz.*, $M_n \equiv M_{n+8} \bmod 3$; the first 8 values of M_n modulo 3 are $1, 0, 1, 2, 2, 0, 2, 1$.

The starting point is a formula of Dey.

Let G be any finitely generated group. Denote by h_n, the number of homomorphisms of G into S_n, and by α_n, the number $h_n/n!$. Dey's formula states that the sequences M_n and α_n are related by

$$\alpha_0 M_n + \alpha_1 M_{n-1} + \cdots + \alpha_{n-1} M_1 = n\alpha_n$$

where α_0 is taken to be 1.

The method of [GN3] is to prove that when G is a free product of cyclic groups, the rational numbers α_n are in $p\mathbb{Z}_p$ for $n \geq p$, provided $\mathbb{Z}/p$ occurs as a factor at least 2 times (respectively 4, 3 times) when $p > 3$ (respectively $p = 2$ or 3).

This elegant method does not work in our cases – indeed, for $(\mathbb{Z}/3) * (\mathbb{Z}/3)$, $\alpha_{3^k} \notin \mathbb{Z}_3$ *and similarly, for* $(\mathbb{Z}/2) * (\mathbb{Z}/2) * (\mathbb{Z}/2)$, $\alpha_{2^k} \notin \mathbb{Z}_2$ *for arbitrarily large* k. So, one has to get an appropriate recurrence relation among the M_n's themselves.

Let p be a prime. Let us recall that the number $\tau_p(n)$ of elements of exponent p in S_n is given recursively by

$$\tau_p(n) = \tau_p(n-1) + \frac{(n-1)!}{(n-p)!}\tau_p(n-p)$$

with $\tau_p(0) = \cdots = \tau_p(p-1) = 1$.

Thus, if $G = \mathbb{Z}/p_1 * \mathbb{Z}/p_2 * \cdots * \mathbb{Z}/p_r$ is a free product, the number $h_n(G)$ of homomorphisms of G into S_n is $\tau_{p_1}(n) \cdots \tau_{p_r}(n)$. One can prove that the numbers $\alpha_n = h_n/n!$ satisfy a recurrence (with polynomials in n as coefficients)[1] of order, at the most $p_1 p_2 \dots p_r$.

1. ON THE GROUP $G = (\mathbb{Z}/2) * (\mathbb{Z}/2) * (\mathbb{Z}/2)$

Let $a_n = \tau_2(n)/n!$, where the number $\tau_2(n)$ of involutions in S_n is given recursively by $\tau_2(n) = \tau_2(n-1) + (n-1)\tau_2(n-2)$. Then, $na_n = a_{n-1} + a_{n-2}$. This gives, $a_{n-2}^2 = (na_n - a_{n-1})^2 = n^2 a_n^2 + a_{n-1}^2 - 2na_n a_{n-1}$. On the other hand, $a_n + a_{n-1} = (n+1)a_{n+1}$ gives, on squaring, an expression for $a_n a_{n-1}$. Eliminating the $a_n a_{n-1}$ term from the two equations, one gets the recurrence

$$nb_n = nb_{n-1} + nb_{n-2} - (n-2)b_{n-3}$$

where $b_n = (n!)a_n^2 = \tau_2(n)^2/n!$. We notice that this gives easily the generating function $\Sigma_{n\geq 0} M_{n+1} t^n$ for the group $(\mathbb{Z}/2) * (\mathbb{Z}/2)$ to be $(1+2t-t^2)/(1-t)^2(1+t)$. This leads us to the well known result for $G = (\mathbb{Z}/2) * (\mathbb{Z}/2)$ that, M_n is n or $n+1$ according as n is odd or even. This was first proved by Stothers by a graphical method.

Let us return to the case $G = (\mathbb{Z}/2) * (\mathbb{Z}/2) * (\mathbb{Z}/2)$. We have the two recurrences for $a_n = \tau_2(n)/n!$ and $b_n = \tau_2(n)^2/n!$:

$$na_n = a_{n-1} + a_{n-2} \tag{1}$$

$$nb_n = nb_{n-1} + nb_{n-2} - (n-2)b_{n-3} \tag{2}$$

We are interested in a recurrence for $\alpha_n = h_n(G)/n! = \tau_2(n)^3/n! = (n!)a_n b_n$. We will write $c_n = a_n b_n$. The Eqs. (1) and (2) give,

$$\begin{aligned} n^2 c_n &= na_{n-1}b_n + na_{n-2}b_{n-1} + nc_{n-2} - (n-2)a_{n-2}b_{n-3} \\ &= na_{n-1}b_n + na_{n-2}b_{n-1} + nc_{n-2} - c_{n-3} - a_{n-4}b_{n-3} \end{aligned}$$

Therefore

$$n^2 c_n - nc_{n-2} + c_{n-3} = na_{n-1}b_n + na_{n-2}b_{n-1} - a_{n-4}b_{n-3} \tag{3}$$

[1] This observation has already been made in [GIR].

Using (2) with n replaced by $n + 1$, we get on simplifying

$$\begin{aligned}(n+1)nc_n + (n+1)c_{n-1} - nc_{n-2} \\ = (n+1)na_nb_{n+1} - (n+1)a_{n-2}b_{n-1} + a_{n-3}b_{n-2}\end{aligned} \tag{4}$$

Let us write L_3 and L_4 for the left hand sides of these two equations. Changing n to $n + 1$ in (3) and adding with (4), one gets

$$L_3^+ + L_4 = (n+1)^2 a_nb_{n+1} + (n+1)a_{n-1}b_n - (n+1)a_{n-2}b_{n-1} \tag{5}$$

Here, we have written L_3^+ to mean the expression for L_3 when n is changed to $n+1$. We shall adopt this convention for any L_i.

Changing n to $n+2$ in (3) and eliminating $a_{n-2}b_{n-1}$ from the resulting equation and (5), we have

$$\begin{aligned}(n+1)L_3^{++} - L_3^+ - L_4 =& (n+2)(n+1)a_{n+1}b_{n+2} \\ &+ (n+1)a_nb_{n+1} - (n+1)a_{n-1}b_n\end{aligned} \tag{6}$$

Similarly, we have

$$L_6^+ - L_4^{++} = (n+2)a_{n+1}b_{n+2} + a_nb_{n+1} - a_{n-1}b_n \tag{7}$$

Thus, we see from Eqs. (5), (6) and (7) that

$$\frac{L_6}{n+1} = \frac{L_5^+}{n+2} = L_7$$

Writing out the expressions for the L's in terms of the c_i's, we have two recurrences:

$$\begin{aligned}(n+1)^2(n+2)^2c_{n+2} =& 2(n+2)(n+1)^2c_{n+1} + 2(n+2)(n+1)^2c_n \\ &- 2(n+1)^2c_{n-1} - (n-1)(n+2)c_{n-2}\end{aligned} \tag{8}$$

$$\begin{aligned}(n+1)(n+2)(n+3)^2c_{n+3} =& (n+1)(n+2)(3n+7)c_{n+2} \\ &+ 2(n+1)(n^2+4n+5)c_{n+1} \\ &- 2(n+1)(2n+3)c_n \\ &- (n-1)(n+1)c_{n-1} + (n-1)c_{n-2}\end{aligned} \tag{9}$$

The corresponding recurrences for $\alpha_n = (n!)c_n$ are:

$$n(n+1)\alpha_{n+1} = 2n(n+1)\alpha_n + 2n^2(n+1)\alpha_{n-1} - 2n^2(n-1)\alpha_{n-2} - (n+1)(n-1)(n-2)^2\alpha_{n-3} \quad (10)$$

$$(n+3)\alpha_{n+3} = (3n+7)\alpha_{n+2} + 2(n^2+4n+5)\alpha_{n+1} - 2(n+1)(2n+3)\alpha_n - n(n-1)(n+1)\alpha_{n-1} + n(n-1)^2\alpha_{n-2} \quad (11)$$

One can translate these recurrences into equations for the generating function $f(t) = \Sigma_{n\geq 0}\ \alpha_n t^n$. Further, Dey's formula can be rewritten as $f'(t)/f(t) = M(t) := \Sigma_{n\geq 0}\ M_{n+1}t^n$, and, in fact one can write any $f^{(k)}(t)/f(t)$ in terms of $M(t)$. For example, $f^{(2)}(t)/f(t) = M'(t) + M(t)^2$, $f^{(3)}(t)/f(t) = M(t)^3 + 3M(t)M'(t) + M^{(2)}(t)$, $f^{(4)}(t)/f(t) = M(t)^4 + 6M'(t)M(t)^2 + 4M(t)M^{(2)}(t) + 3(M'(t))^2 + M^{(3)}(t)$ *etc.* When we do that, we get:

THEOREM 1 *For the group $G = (\mathbb{Z}/2) * (\mathbb{Z}/2) * (\mathbb{Z}/2)$, the numbers M_n of subgroups of index n satisfy the equations*

$$\begin{aligned}4 - 8t - 8t^2 = {} & (-4 - 20t + 28t^2 + 52t^3)M(t) \\ & + (1 - 2t - 14t^2 + 16t^3 + 52t^4)(M'(t) + M(t)^2) \\ & + (-2t^3 + 2t^4 + 14t^5)(M(t)^3 + 3M(t)M'(t) + M^{(2)}(t)) \\ & + t^6(M(t)^4 + 6M'(t)M(t)^2 + 4M(t)M^{(2)}(t) \\ & + 3(M'(t))^2 + M^{(3)}(t))\end{aligned} \quad (12)$$

$$\begin{aligned}-1 - 4t + 6t^2 - 2t^4 = {} & (-1 + 3t + 6t^2 - 14t^3 - 6t^4 + 10t^5)M(t) \\ & + (2t^3 - 4t^4 - 6t^5 + 7t^6)(M'(t) + M(t)^2) \\ & + (-t^6 + t^7)(M(t)^3 + 3M(t)M'(t) + M^{(2)}(t))\end{aligned} \quad (13)$$

Here $M(t)$ is the formal power series $\Sigma_{n\geq 0}\ M_{n+1}t^n$.

As a matter of fact, we can obtain (12) (but not (13)) by directly finding a recurrence for a_n^3. Equations (12) and (13) can be regarded as recurrence equations for the M_n if we compare like powers of t. As we shall see shortly, it is Eq. (13) that proves useful for us.

COROLLARY *M_n is odd for any n.*

Proof We read Eq. (13) modulo 2. To start with, we can compare the coefficients of $t^i, 0 \leq i \leq 4$ to obtain $M_1 = 1$, $M_2 = 7$, $M_3 = 21$, $M_4 = 107$ and $M_5 = 425$. Let $n \geq 5$ and we assume that M_r is odd for all $r \leq n$. Let us read the coefficient of t^n modulo 2 in (13).

For n even and n odd, we get, respectively, the congruences

$$\begin{aligned} M_{n+1} \equiv M_n &+ M_{n-4} + M^2_{(n-4)/2} \\ &+ M_2 M_{n-6} + M_4 M_{n-8} + \cdots + M_{n-6} M_2 \\ &+ M_1 M_{n-4} + M_3 M_{n-6} + \cdots + M_{n-5} M_2 \\ &+ M_1 M^2_{(n-4)/2} + M_3 M^2_{(n-6)/2} + \cdots + M_{n-5} M^2_1 \\ &+ M_2 M^2_{(n-6)/2} + M_4 M^2_{(n-8/2)} + \cdots + M_{n-6} M^2_1 \end{aligned}$$

and

$$\begin{aligned} M_{n+1} \equiv M_n & \\ &+ M_1 M_{n-5} + M_3 M_{n-7} + \cdots + M_{n-6} M_2 \\ &+ M_2 M_{n-5} + M_4 M_{n-7} + \cdots + M_{n-5} M_2 \\ &+ M_2 M^2_{(n-5)/2} + M_4 M^2_{(n-7)/2} + \cdots + M_{n-5} M^2_1 \\ &+ M_1 M^2_{(n-5)/2} + M_3 M^2_{(n-7)/2} + \cdots + M_{n-6} M^2_1 \end{aligned}$$

It follows by induction that M_{n+1} is odd. This proves the corollary[2].

2. ON THE GROUP $G = (\mathbb{Z}/3) * (\mathbb{Z}/3)$

In this section, we denote by a_n, the rational number $\tau_3(n)/n!$. Then, we have

$$na_n = a_{n-1} + a_{n-3} \tag{14}$$

[2] Interestingly, (12) turns out to be not amenable for a similar argument as it gives only an expression of nM_{n+1} in terms of M_i, $i \leq n$.

Multiplying by $(n-1)$ and using (14) with n replaced by $n-1$, one gets

$$n(n-1)a_n - a_{n-2} = (n-1)a_{n-3} + a_{n-4} \tag{15}$$

Squaring, we get

$$\begin{aligned} n^2(n-1)^2 a_n^2 + a_{n-2}^2 - 2n(n-1)a_n a_{n-2} \\ = a_{n-4}^2 + (n-1)^2 a_{n-3}^2 + 2(n-1)a_{n-3}a_{n-4} \end{aligned} \tag{16}$$

Equation (14) with n replaced by $n+1$ gives, on squaring,

$$2a_n a_{n-2} = (n+1)^2 a_{n+1}^2 - a_n^2 - a_{n-2}^2$$

Similarly, we have

$$(n-3)^2 a_{n-3}^2 + a_{n-4}^2 - 2(n-3)a_{n-3}a_{n-4} = a_{n-6}^2$$

Feeding the expressions for $a_n a_{n-2}$ and for $a_{n-3}a_{n-4}$ from these equations into (16), one has a recurrence for the a_n^2. Writing it in terms of $\alpha_n = (n!)a_n^2$, one gets

$$\begin{aligned} (n+1)\alpha_{n+1} = {} & (n^2 - n + 1)\alpha_n + (n^2 - n + 1)\alpha_{n-2} \\ & - 2(n-1)(n-2)^2\alpha_{n-3} - 2(n-2)^2\alpha_{n-4} \\ & + (n-1)(n-2)(n-4)(n-5)\alpha_{n-6} \end{aligned} \tag{17}$$

This can be written in terms of the generating function $f(t) = \Sigma_{n \geq 0} \alpha_n t^n$ which, in turn, yields for the generating function $M(t) := \Sigma_{n \geq 0} M_{n+1} t^n$, the following:

THEOREM 2 *For the group $G = \mathbb{Z}/3 * \mathbb{Z}/3$, the generating function $M(t) := \Sigma_{n \geq 0} M_{n+1} t^n$ satisfies the equation*

$$\begin{aligned} 1 + 3t^2 - 4t^3 - 8t^4 + 40t^6 = {} & (1 - 4t^3 + 20t^4 + 10t^5 - 140t^7)M(t) \\ & + (-t^2 - t^4 + 14t^5 + 2t^6 - 92t^8) \\ & (M'(t) + M(t)^2) + (2t^6 - 18t^9) \\ & (M(t)^3 + 3M(t)M'(t) + M^{(2)}(t)) \\ & - t^{10}(M(t)^4 + 6M'(t)M(t)^2 + 4M(t)M^{(2)}(t) \\ & + 3(M'(t))^2 + M^{(3)}(t)) \end{aligned} \tag{18}$$

Remark The first values of M_n are $1, 0, 4, 8, 5, 36, 98, 112, 490$, 1560, $2464, 8768, \ldots$. This suggests the curious question as to whether $M_n \equiv 0$ mod n whenever $n \not\equiv 0$ mod 3.

From the theorem, we get:

COROLLARY 1 *M_n is odd if, and only if, n is of the form* $2^s - 3$.

Proof As before, we can compare the coefficients of the first few powers of t in (18) to get $M_1 = 1$, $M_2 = 0$, $M_3 = 4$, $M_4 = 8$, $M_5 = 5$ and $M_6 = 36$, and will apply induction to prove the corollary. We read (18) modulo 3, and look at the coefficient of t^n for $n > 6$. Assume that the assertion of the corollary holds for M_r when $r \leq n$. We have

$$\begin{aligned} 0 \equiv M_{n+1} &+ (n-1)(M_n + M_{n-2}) \\ &+ a(M_{n/2}^2 + M_{n-2/2}^2) + b(M_{k+1}^4 + M_{2k+2}^2) \end{aligned}$$

where a is 0 or 1 according as n is odd or even, and b is 1 or 0 according as $n = 4k + 10$ for some k, or not.

This implies immediately that M_{n+1} is even, for any odd n.
If $n = 2k > 6$, this reads

$$M_{2k+1} + M_{k-1} \equiv a(M_k + M_{k-3/2})$$

where $a = 1$ if $k \geq 5$ is odd, and, $a = 0$ otherwise. Hence, it follows by another induction argument that $M_{2k+1} + M_{k-1}$ is even.

Now, $2k + 1$ is of the form $2^s - 3$ if, and only if, $k - 1$ is of the same form. This proves the corollary.

We prove now

COROLLARY 2 *The mod 3 behaviour of M_n is periodic viz., $M_n \equiv M_{n+8}$ mod 3.*

The first 8 values of M_n modulo 3 are $1, 0, 1, 2, 2, 0, 2, 1$.

Proof As before, we can read the Eq. (18) for the M_n's mod 3. Now, we apply induction to prove the statement

$$M_{r+1} \equiv M_{r-1} - M_r$$

This is easily checked for the first few values of n. We assume the induction hypothesis that the above congruence holds for any $2 \leq r < n$.

The Eq. (18) reads mod 3,

$$
\begin{aligned}
0 \equiv\ & M_{n+1} - M_{n-2} - M_{n-3} + M_{n-4} + M_{n-6} \\
& \begin{cases} +M_n + M_{n-3} - M_{n-4} - M_{n-6} & \text{if n } \equiv 0 \\ -M_{n-2} + M_{n-4} & \text{if n } \equiv 1 \\ -M_n + M_{n-2} - M_{n-3} + M_{n-6} & \text{if n } \equiv 2 \end{cases} \\
& \begin{cases} +M_{n-3} - M^3_{n-3/3} & \text{if } n \equiv 0 \\ 0 & \text{otherwise} \end{cases} \\
& + M_3M_{n-9} + M_6M_{n-12} + \cdots\cdots\cdots\cdots \\
& - M_1^3M_{n-9} - M_2^3M_{n-12} - \cdots\cdots\cdots\cdots \\
& - M_1M_{n-1} - M_2M_{n-2} - \cdots - M_{n-1}M_1 \\
& - M_1M_{n-3} - M_2M_{n-4} - \cdots - M_{n-3}M_1 \\
& - M_1M_{n-4} - M_2M_{n-5} - \cdots - M_{n-4}M_1 \\
& - M_1M_{n-5} - M_2M_{n-6} - \cdots - M_{n-5}M_1 \\
& + M_1M_{n-7} + M_2M_{n-8} + \cdots + M_{n-7}M_1
\end{aligned}
$$

On using the induction hypothesis, this easily proves $M_{n+1} \equiv M_{n-1} - M_n$, and the corollary follows.

Acknowledgements

I would like to thank Morris Newman for sending me his papers which really got me interested in this subject.

References

[GIR] Godsil, C., Imrich, W. and Razen, R. (1979). On the number of subgroups of given index in the modular group, *Mh. Math.*, **87**, 273–280.

[GN1] Grady, M. and Newman, M. (1992). Some divisibility properties of the subgroup counting function for free products, *Math. Comp.*, **58**, 347–353.

[GN2] Counting subgroups of given index in Hecke groups (1993). *Contemp. Math., Amer. Math. Soc.*, **143**, 431–436.

[GN3] Residue periodicity in subgroup counting functions (1994). *Contemp. Math., Amer. Math. Soc.*, **166**, 265–273.

[St] Stothers, W. W. (1977). The number of subgroups given index in the modular groups, *Proc. Royal Soc.*, Edinburgh, **78A**, 105–112.