A NUMBER THEORY PROBLEM CONCERNING FINITE GROUPS AND RINGS

Ian G. Connell

(received March 5, 1963)

Let $f_1(n)$ denote the number of abelian groups of order n and $f_2(n)$ the number of semi-simple rings with n elements. What can be said about the magnitude of $f_i(n)$? We shall prove that one can expect, on the average, about 2.3 groups and 2.5 rings of the kind stated for a given order.* First we state without proof the two relevant structure theorems (which are readily available in standard texts).

Let G be an abelian group of order $n = q_1^{e_1} q_2^{e_2} \ldots$ where the q_i are the distinct primes dividing n. Then G is the direct product of groups G_i of order $q_i^{e_i}$ and each G_i is in turn a direct product of cyclic groups G_{ij} of orders $q_i^{e_{ij}}$ such that

$$\sum_j e_{ij} = e_i .$$

G determines uniquely the set of integers $\{q_i^{e_{ij}}\}$, and conversely, each such set determines a G unique (up to isomorphism).

---

* I find I have been anticipated in the group case by Erdős and Szekeres [1]; however my method is different from theirs and I believe the ring case is new.

Canad. Math. Bull. vol. 7, no. 1, January 1964

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

It follows immediately that

$$f_1(n) = p_1(e_1)p_1(e_2)\ldots$$

where $p_1(n)$ is the usual partition function. Obviously $f_1(n)$ is multiplicative, that is, if the g.c.d. $(m,n) = 1$ then $f_1(mn) = f_1(m)f_1(n)$.

Let R be a ring with $n = q_1^{e_1} q_2^{e_2} \ldots$ elements which is semi-simple, that is has zero radical. Then R is the direct product of rings R_i of $q_i^{e_i}$ elements and each R_i is the direct product of rings R_{ij} of $q_i^{e_{ij}}$ elements where R_{ij} is the full ring of $r_{ij} x r_{ij}$ matrices over the finite field* $GF(q_i^{s_{ij}})$, and

$$\sum_j e_{ij} = \sum_j r_{ij}^2 s_{ij} = e_i .$$

R determines uniquely the set of pairs $\{(r_{ij}, q_i^{s_{ij}})\}$, and conversely each such set determines a unique semi-simple R.

Again we see that $f_2(n)$ is multiplicative and

$$f_2(n) = p_2(e_1)p_2(e_2)\ldots$$

where $p_2(n)$ is a modified partition function defined as follows. Let $\delta(n)$ denote the number of squares dividing n:

$$\delta(n) = \sum_{d^2 | n} 1 .$$

* In the general theorem one has skew fields but in our case they are finite and therefore commutative.

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

Then $p_2(n)$ is the number of partitions of n, where we now recognize $\delta(m)$ different 'kinds' of the integer m when it occurs as a summand in a partition. For example, the partition

$$12 + 4 + 1$$

contributes 1 to $p_1(17)$ but 4 to $p_2(17)$ corresponding to

$$12 + 4 + 1$$

$$3.2^2 + 4 + 1$$

$$12 + 2^2 + 1$$

$$3.2^2 + 2^2 + 1 .$$

If R has q^{17} elements then $12 + 4 + 1$ corresponds to the direct product

$$GF(q^{12}) \times GF(q^4) \times GF(q) ;$$

$3.2^2 + 4 + 1$ corresponds to

$$GF(q^3)_2 \times GF(q^4) \times GF(q) ,$$

where the subscript 2 indicates the ring of 2×2 matrices; and so on.

The generating function for $p_1(n)$ is well known:

$$P_1(x) = \prod_{n=1}^{\infty} (1 - x^n)^{-1} = \sum_{n=0}^{\infty} p_1(n)x^n$$

(where $p_1(0) = 1$), and a moment's consideration shows that

$$P_2(x) = \prod_{n=1}^{\infty} (1 - x^n)^{-\delta(n)} = \sum_{n=0}^{\infty} p_2(n)x^n$$

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

(where $p_2(0) = 1$). Clearly

$$P_2(x) = P_1(x)P_1(x^4)P_1(x^9) \ldots .$$

The generating function for $f_i(n)$ is of the Dirichlet series type; formally,

$$\sum_{n=1}^{\infty} f_1(n)n^{-s} = \prod_p \{ 1 + p_1(1)p^{-s} + p_1(2)p^{-2s} + \ldots \}$$

(where the product is extended over all primes)

$$= \prod_p P_1(p^{-s})$$

$$= \prod_p \prod_{n=1}^{\infty} (1 - p^{-ns})^{-1}$$

$$= \prod_{n=1}^{\infty} \prod_p (1 - p^{-ns})^{-1}$$

$$= \prod_{n=1}^{\infty} \zeta(ns) ,$$

where $\zeta(s)$ is the Riemann ζ-function; and similarly for $f_2(n)$. Thus we have the formal identities

$$Z_1(s) = \prod_{n=1}^{\infty} \zeta(ns) = \sum_{n=1}^{\infty} f_1(n)n^{-s}$$

$$Z_2(s) = \prod_{n=1}^{\infty} \zeta(ns)^{\delta(n)} = \sum_{n=1}^{\infty} f_2(n)n^{-s} .$$

Note $$Z_2(s) = Z_1(s)Z_1(4s)Z_1(9s) \ldots .$$

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

In order to deal with the two cases simultaneously, we write $\delta_1(n) = 1$, $\delta_2(n) = \delta(n)$. We regard $Z_i(s)$ as being defined by the infinite product. $s = \sigma + i\tau$ is a complex variable.

PROPOSITION. $Z_i(s)$ is a regular function of s for $\sigma > 0$ except for poles of order $\delta_i(n)$ at $1/n$ $(n = 1, 2, \ldots)$. The line $\sigma = 0$ is a natural boundary. The series

$$\Sigma\, f_i(n) n^{-s}$$

converges absolutely for $\sigma > 1$ to $Z_i(s)$.

Proof. The first statement will follow if we prove for $N = 1, 2, \ldots$ that $Z_i(s)$ is regular for $\sigma \geq 2/(N+1)$ except for poles of order $\delta_i(n)$ at $1/n$ $(n = 1, 2, \ldots, [(N+1)/2])$. Since $\zeta(s)$ is regular except for a simple pole (with residue 1) at $s = 1$, this will follow if we prove that the product

$$Z_i(s)/Z_i(s,N) = \prod_{n=N+1}^{\infty} \{1 + (\zeta(ns) - 1)\}^{\delta_i(n)},$$

where $$Z_i(s,N) = \prod_{n=1}^{N} \zeta(ns)^{\delta_i(n)},$$

is uniformly convergent in the half-plane $\sigma \geq 2/(N+1)$, and this will be guaranteed if the sum

$$\sum_{n=N+1}^{\infty} |\zeta(ns) - 1|^{\delta_i(n)}$$

converges uniformly. Since $n\sigma \geq 2$,

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

$$
\begin{aligned}
|\zeta(ns) - 1| &= |2^{-ns} + 3^{-ns} + \dots| \\
&\le 2^{-n\sigma} + 3^{-n\sigma} + \dots \\
&= (1 - 2^{1-n\sigma})^{-1} (1 - 2^{-n\sigma} + 3^{-n\sigma} - \dots) - 1 \\
&< (1 - 2^{1-n\sigma})^{-1} - 1 = (2^{n\sigma - 1} - 1)^{-1} \\
&\le 2^{-n\sigma} 4 \quad (\le 1),
\end{aligned}
$$

whence

$$\sum_{n=m}^{\infty} |\zeta(ns) - 1|^{\delta_i(n)} < 4 \sum_{n=m}^{\infty} 2^{-n\sigma}$$

for any $m \ge N + 1$, which clearly proves the uniform convergence.

$\zeta(s)$ has infinitely many zeros $s_1, s_2, \dots$ in the strip $0 < \sigma < 1$, and the conjugate of a zero is also a zero. Thus $Z_i(s)$ has zeros at s_k/n, $(k, n = 1, 2, \dots)$ and it follows readily that each point on the line $\sigma = 0$ is a limit point of zeros, thus an essential singularity, and therefore $\sigma = 0$ is a natural boundary.

Each of the finitely many series $\zeta(ns)$ in the product $Z_i(s,N)$ is absolutely convergent for $\sigma > 1$ and therefore the terms may be rearranged to give

$$Z_i(s,N) = \sum_{n=1}^{\infty} f_i(n,N) n^{-s}$$

where the series is absolutely convergent and $1 \le f_i(n,N) \le f_i(n)$, with $f_i(n,N) = f_i(n)$ for $n \le N$. Thus

$$\sum_{n=1}^{N} f_i(n) n^{-\sigma} < \sum_{n=1}^{\infty} f_i(n,N) n^{-\sigma}$$

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

$$= \prod_{n=1}^{N} \zeta(n\sigma)^{\delta_i(n)}$$

$$< Z_i(\sigma) .$$

Hence the series $\Sigma f_i(n)n^{-\sigma}$ of positive terms is bounded above and is therefore convergent for any $\sigma > 1$. Because of the convergence of $\Sigma f_i(n, N)n^{-\sigma}$ and of the product $Z_i(\sigma)$ we clearly have

$$\sum_{n=1}^{\infty} f_i(n)n^{-\sigma} > \sum_{n=1}^{\infty} f_i(n, N)n^{-\sigma}$$

$$> Z_i(\sigma) - \varepsilon$$

for arbitrary $\varepsilon > 0$ and N sufficiently large, so that $\Sigma f_i(n)n^{-\sigma}$ converges to $Z_i(\sigma)$ for $\sigma > 1$. It follows [2] that $\Sigma f_i(n)n^{-s}$ converges absolutely to $Z_i(s)$ for $\sigma > 1$. This completes the proof.

$Z_i(s)$ has a simple pole at $s = 1$; let the residue be C_i. Then since $\zeta(s)$ has residue 1 at $s = 1$, we have

$$C_1 = \zeta(2)\,\zeta(3) \ldots \zeta(n) \ldots = 2.294842 \ldots$$

$$C_2 = \zeta(2)\,\zeta(3)\,\zeta(4)^2 \ldots \zeta(n)^{\delta(n)} \ldots = 2.499598 \ldots$$

(expressions for the residues at the other poles can be given without difficulty). We now appeal to Ikehara's theorem [3, p. 125]: If

$$F(s) = \sum_{n=1}^{\infty} a_n n^{-s}, \quad a_n \geq 0$$

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

is convergent for $\sigma > 1$, and $F(s)$ is regular on $\sigma = 1$ except for a simple pole with residue C at $s = 1$, then

$$a_1 + a_2 + \ldots + a_n \sim Cn ,$$

(where, as usual, $f(n) \sim g(n)$ means that

$$\lim_{n\to\infty} f(n)/g(n)$$

exists and has the value 1).

The conditions are satisfied by $Z_i(s)$ and we have

COROLLARY.

$$f_i(1) + f_i(2) + \ldots + f_i(n) \sim C_i n .$$

Hence, on the average, there are C_1 abelian groups and C_2 semi-simple rings of each order.

Erdős and Szekeres show that the error in the above asymptotic formula in the case $i = 1$ is $O(\sqrt{n})$. I would conjecture that a more detailed analysis of $Z_i(s)$ should yield

$$f_i(1) + f_i(2) + \ldots + f_i(n) = C_{i1} n + 2C_{i2} n^{1/2}$$
$$+ \ldots + kC_{ik} n^{1/k} + O(n^{1/(k+1)}) ,$$

where C_{ik} is the residue of $Z_i(s)$ at $s = 1/k$.

The behaviour of $f_i(n)$ itself is of course quite erratic; thus, if n is square-free $f_i(n) = 1$, but on the other hand $f_i(2^m) = p_i(m)$. It is well-known that

$$p_1(m) \sim \frac{1}{4m\sqrt{3}} e^{K_1\sqrt{m}}$$

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

where $$K_1 = \pi\sqrt{\frac{2}{3}},$$

and therefore (for arbitrary $\varepsilon > 0$)

$$f_1(n) > \frac{(1-\varepsilon)A}{\log n} e^{B\sqrt{\log n}},$$

for infinitely many values of n,

where $$A = \frac{\log 2}{4\sqrt{3}}, \qquad B = \pi\sqrt{\frac{2}{3\log 2}}.$$

For the ring case we will obtain only a much cruder result. From above we have

$$\log p_1(m) \sim \pi\sqrt{\frac{2}{3}} \cdot \sqrt{m}$$

and we expect a somewhat larger value for $\log p_2(m)$; we now prove

$$\log p_2(m) \sim \frac{\pi^2}{3}\sqrt{m}.$$

For $0 < x < 1$ we have*

$$\log P_2(x) = \sum_{n=1}^{\infty} -\delta(n)\log(1 - x^n)$$

$$= \sum_{n=1}^{\infty} \delta(n) \sum_{m=1}^{\infty} \frac{x^{mn}}{m}$$

$$= \sum_{m=1}^{\infty} \frac{1}{m} \sum_{n=1}^{\infty} \delta(n)\, x^{mn}$$

* All the series in what follows are convergent for $0 < x < 1$, and the transformations can be justified by standard elementary theorems.

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

$$= \sum_{m=1}^{\infty} \frac{1}{m}\left\{\frac{x^m}{1-x^m} + \frac{x^{4m}}{1-x^{4m}} + \frac{x^{9m}}{1-x^{9m}} + \ldots\right\} .$$

Using

$$kx^{k-1}(1-x) \le 1-x^k \le k(1-x)$$

wherever necessary,

$$\sum_{m=1}^{\infty} \frac{1}{m} \frac{x^{t^2 m}}{1-x^{t^2 m}} < \sum_{m=1}^{\infty} \frac{1}{m^2} \frac{x}{t^2(1-x)}$$

$$= \frac{\pi^2}{6} \frac{x}{t^2(1-x)}$$

$$< \frac{\pi^2}{6t^2(1-x)}$$

and therefore

$$\log P_2(x) < \frac{\pi^2}{6(1-x)} \sum_{t=1}^{\infty} \frac{1}{t^2}$$

$$= \frac{\pi^4/36}{1-x} .$$

On the other hand,

$$\log P_2(x) > \sum_{m=1}^{\infty} \frac{1}{m} \sum_{t=1}^{\infty} \frac{x^{mt^2}}{mt^2(1-x)}$$

$$= \frac{1}{1-x} \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{t=1}^{\infty} \frac{x^{mt^2}}{t^2}$$

$$> \frac{1}{1-x} \frac{\pi^2}{6} \frac{\pi^2}{6} (1-\varepsilon)$$

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

for arbitrary $\varepsilon > 0$ provided x is sufficiently close to 1 (by Abel's theorem on the continuity of power series). Hence

$$\log P_2(x) \sim \frac{\pi^4/36}{1 - x}$$

as $x \to 1-$.

We now appeal to the following Tauberian theorem: If $a_n \geq 0$ and

$$\log \Sigma a_n x^n \sim \frac{C}{1 - x}$$

as $x \to 1-$, then

$$\log (a_0 + a_1 + \ldots + a_n) \sim 2\sqrt{Cn} .$$

If the a_n are monotone increasing (as our $p_2(n)$) it is easy to see that this implies

$$\log a_n \sim 2\sqrt{Cn} .$$

Thus

PROPOSITION.

$$\log p_2(n) \sim \frac{\pi^2}{3} \sqrt{n} .$$

We mention finally the identity (familiar in the case $i = 1$)

$$np_i(n) = \sum_{k=1}^{n} a_i(k)p_i(n - k)$$

where

$$a_i(k) = \sum_{d|k} d\, \delta_i(d)$$

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press

obtained by logarithmic differentiation of

$$\Pi(1 - x^n)^{-\delta_i(n)} = \Sigma\, p_i(n) x^n$$

and comparing coefficients. This recurrence relation was used to calculate $p_2(n)$ up to $n = 100$; although the values of $p_2(n)$ tended to be very 'round', no congruence property of the Ramanujan type was noticed.

REFERENCES

1. P. Erdős and G. Szekeres, Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem. Acta Litt. Sci. Szeged, v. 7(1934), pp. 95-102.

2. G.H. Hardy and M. Riesz, The General Theory of Dirichlet Series. Cambridge Tract No. 18.

3. N. Wiener, The Fourier Integral.

McGill University

https://doi.org/10.4153/CMB-1964-002-1 Published online by Cambridge University Press