
THE AMERICAN MATHEMATICAL MONTHLY

The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: http://maa.tandfonline.com/loi/uamm20

The Number of Homomorphisms From Z_m Into Z_n

Joseph A. Gallian & James Van Buskirk

To cite this article: Joseph A. Gallian & James Van Buskirk (1984) The Number of Homomorphisms From Z_m Into Z_n, The American Mathematical Monthly, 91:3, 196-197, DOI: 10.1080/00029890.1984.11971375

To link to this article: https://doi.org/10.1080/00029890.1984.11971375

Published online: 05 Feb 2018.

$$S_n(\bar{x} - x_n) = \sum_{i=1}^{n-1} p_i(x_i - x_n) = \sum_{j=1}^{n-1} (x_j - x_{j+1}) S_j \geqslant 0,$$

so $x_n \leqslant \bar{x} \leqslant x_1$. Let m be such that $\bar{x} \in [x_{m+1}, x_m]$. Hereafter, M is to be given its value at $c = \bar{x}$.

We can easily show that the following identity is valid:

$$(4)\quad f\left(\frac{1}{S_n}\sum_{i=1}^{n} p_i x_i\right) - \frac{1}{S_n}\sum_{i=1}^{n} p_i f(x_i) = \sum_{i=1}^{m-1} \left(M(x_i - x_{i+1}) - f(x_i) + f(x_{i+1})\right)\frac{S_i}{S_n}$$
$$+\left(M(x_m - \bar{x}) - f(x_m) + f(\bar{x})\right)\frac{S_m}{S_n}$$
$$+\left(f(\bar{x}) - f(x_{m+1}) - M(\bar{x} - x_{m+1})\right)\frac{\bar{S}_{m+1}}{S_n}$$
$$+\sum_{i=m+1}^{n-1} \left(f(x_i) - f(x_{i+1}) - M(x_i - x_{i+1})\right)\frac{\bar{S}_{i+1}}{S_n}.$$

Now, using (3) and (4) we get (1).

REMARKS. (1) It is known (see for example [**1**] or [**2**]) that from the Jensen-Steffensen Inequality we can obtain some results from [**3**]–[**7**].

(2) R. P. Boas in paper [**8**] has proved the Jensen-Steffensen inequality using inequality (2). A similar proof of the Jensen inequality for convex functions is given, for example, in [**9**] (see also [**8**]).

References

1. J. E. Pečarić, Inverse of Jensen-Steffensen's inequality. Glas. Mat., 16 (36) (1981) 229–233.

2. H. D. Brunk, On an inequality for convex functions, Proc. Amer. Math. Soc., 7 (1956) 817–824.

3. G. Szegö, Über eine Verallgemeinerung des Dirichletschen Integrals, Math. Z., 52 (1950) 676–685.

4. H. F. Weinberger, An inequality with alternating signs, Proc. Nat. Acad. Sci., 38 (1952) 611–613.

5. R. Bellman, On an inequality of Weinberger, this MONTHLY, 60 (1953) 402.

6. I. Olkin, On inequalities of Szegö and Bellman, Proc. Nat. Acad. Sci., 45 (1959) 230–231.

7. R. E. Barlow, A. W. Marshall, and F. Proschan, Some inequalities for starshaped and convex functions, Pacific J. Math., 29 (1969) 19–42.

8. R. P. Boas, The Jensen-Steffensen Inequality, Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz., no. 302—319 (1970) 1–8.

9. G. H. Hardy, J. E. Littlewood, and G. Pólya, Inequalities, Cambridge, 1934.

THE NUMBER OF HOMOMORPHISMS FROM Z_m INTO Z_n

JOSEPH A. GALLIAN AND JAMES VAN BUSKIRK
Department of Mathematical Sciences, University of Minnesota, Duluth, MN 55812

Although several abstract algebra textbooks (see, for example, [**2**, p. 118] and [**3**, p. 190]) ask their readers to determine the number of group homomorphisms from Z_m into Z_n for particular values of m and n, the authors are not aware of any which ask for a solution to the general problem nor the corresponding problem for ring homomorphisms. This is a bit surprising, since these problems are natural ones and their solutions require only elementary facts from group theory, ring theory, and number theory. In this note, we solve both of these problems.

Consider the group-homomorphism case first. It is clear that the order of the image of a group homomorphism from Z_m into Z_n must divide both m and n and, therefore, is a divisor of $\gcd(m, n)$. Also, if k is a common divisor of m and n, then Z_n has a unique subgroup of order k, and this subgroup has $\phi(k)$ generators, where ϕ is the Euler phi function. Now, noting that in order to specify a group homomorphism from Z_m onto a subgroup H of Z_n it is necessary and sufficient to map the integer 1 to a generator of H, we see that the number of group homomorphisms from Z_m into Z_n is simply $\sum_{k \mid \gcd(m,n)} \phi(k)$. It follows from number theory [**1**, p. 85] that this sum is $\gcd(m, n)$. So, we have proved the following.

THEOREM. *The number of group homomorphisms from* Z_m *into* Z_n *is* $\gcd(m, n)$.

Next, we consider the corresponding problem for the rings. That is, we seek a formula for the number of ring homomorphisms from the ring Z_m into the ring Z_n. First, note, as in the group case, that a ring homomorphism is completely determined by its action on 1. Also, since 1 is an idempotent in Z_m, the image of 1 must be an idempotent in Z_n. Let $n = q_1^{t_1} \cdots q_s^{t_s}$ be the prime-power decomposition of n. Then, Z_n is naturally ring-isomorphic to the direct sum $Z_{q_1^{t_1}} \oplus \cdots \oplus Z_{q_s^{t_s}}$. Next, observe that any ring homomorphism from Z_m into Z_n induces a ring homomorphism from Z_m into $Z_{q_i^{t_i}}$ for $i = 1, \ldots, s$. Now, suppose a is an element of Z_n and a is a (ring) homomorphic image of 1 in Z_m. In the direct sum, let a correspond to $(a_1, a_2, \ldots, a_s)$, where each $a_i \in Z_{q_i^{t_i}}$. Then, each a_i is an idempotent of $Z_{q_i^{t_i}}$, and, therefore, each a_i is 0 or 1. This shows that there are at most 2^s ring homomorphisms from Z_m into Z_n. But, because a ring homomorphism is a group homomorphism, it must also be true that the additive order of a_i divides m. Conversely, if $(a_1, a_2, \ldots, a_s)$ is any member of the direct sum, where each $a_i = 0$ or 1 and the additive order of a_i divides m, then there is a ring homomorphism from Z_m into $Z_{q_1^{t_1}} \oplus \cdots \oplus Z_{q_s^{t_s}}$ which carries 1 to $(a_1, a_2, \ldots, a_s)$. So, the number of ring homomorphisms from Z_m into Z_n is simply the number of s-tuples which meet these two conditions. Since the (additive) order of 0 is 1 and the (additive) order of 1 in $Z_{q_i^{t_i}}$ is $q_i^{t_i}$, we may take $a_i = 0$ or 1 when $q_i^{t_i}$ divides m, and we must take $a_i = 0$ when $q_i^{t_i}$ does not divide m. But, $q_i^{t_i}$ does not divide m if and only if q_i does divide $n/\gcd(m, n)$. Thus, letting $\omega(a)$ denote the number of distinct prime divisors of the integer a, we have proved the following.

THEOREM. *The number of ring homomorphisms from* Z_m *into* Z_n *is* $2^{\omega(n) - \omega(n/\gcd(m,n))}$.

Notice that the number of group homomorphisms from Z_m into Z_n is the same as the number of group homomorphisms from Z_n into Z_m, while the corresponding statement for rings is not true.

References

1. Jeanne Agnew, Explorations in Number Theory, Brooks/Cole, Monterey, CA, 1972.
2. John B. Fraleigh, A First Course in Abstract Algebra, 2nd ed., Addison-Wesley, Reading, MA, 1976.
3. Otto Schilling and W. Stephen Piper, Basic Abstract Algebra, Allyn & Bacon, Rockleigh, NJ, 1975.

MISCELLANEA

122.

I asked him what kind of mathematics he did. He couldn't decide whether or not to tell me. He did mention that at Berkeley he was in a favorable position to study two of the esoteric wonders of our time, subjects only an adept might begin to penetrate. Pure mathematics and the state of California. There were no analogies from the real world that might help him explain either of these.

—Don DeLillo in *The Names*, Alfred A. Knopf, New York, 1982.