Abstraction & Application **13** (2015) 1 − 3 UADY

The number of homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$

Javier Diaz-Vargas[a] and Gustavo Vargas de los Santos[b]

Facultad de Matemáticas, Universidad Autónoma de Yucatán, México

[a]javier.diaz@correo.uady.mx, [b]tavo12@hotmail.com

Abstract

Using elementary results of number theory, we determine the number of homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ as additive groups and as rings.

Resumen

Usando resultados elementales de la teoría de números, determinamos el número de homomorfismos de $\mathbb{Z}_n$ a $\mathbb{Z}_m$, como grupos aditivos y como anillos

Keywords and phrases : Homomorphisms, groups, rings, Chinese Remainder Theorem.

2010 *Mathematics Subject Classification* : 11A07

1 Introduction

In order to determine the number of homomorphisms, we do not need to assume previous knowledge from group theory or ring theory, except for the definition of group and ring homomorphism. With respect to number theory, we use some elementary facts on congruences, which can be found on any introductory book such as [2]. Also, although our results are basically the same as those in [1], our proofs are much more basic.

2 Group homomorphisms

Let $f : \mathbb{Z}_n \to \mathbb{Z}_m$ be a group homomorphism. Then, for $x \in \mathbb{Z}_n, f(x) = f(\underbrace{1+1+\cdots+1}_{x}) = xf(1)$, so $f(x) = ax$, for some $a \in \mathbb{Z}_m$. So, the homomorphism is determined by its value $f(1)$ in 1. Hence, we only need to find the values of $a \in \mathbb{Z}_m$ such that the function $f(x) = ax$ is a homomorphism of groups.

If $f(x) = ax$ is a homomorphism, then

$$0 \equiv f(0) \equiv f(\underbrace{1+1+\cdots+1}_{n}) \equiv \underbrace{f(1)+f(1)+\cdots+f(1)}_{n} \equiv nf(1) \equiv na \mod m.$$

Conversely, if $na \equiv 0 \mod m$, for $x, y \in \mathbb{Z}_n$, with $x + y = nq + r$ and $0 \leq r < n$,

$$f(x+y) \equiv f(r) \equiv ar \equiv a(x+y-nq) \equiv ax + ay - anq \equiv ax + ay \equiv f(x) + f(y) \mod m$$

hence $f(x) = ax$ is a homomorphism. Thus, we have established the following lemma.

Lemma 2.1. *The function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $f(x) = ax$ for some $a \in \mathbb{Z}_m$ fixed is a homomorphism of groups if and only if $na \equiv 0 \bmod m$.*

Now, the congruence

$$na \equiv 0 \bmod m$$

has (m, n) solutions, where (m, n) is the $\gcd(m, n)$. In fact, if $d = (m, n)$, then the solutions are given by $a = \dfrac{m}{d}k$, where $k = 0, 1, \ldots, d-1$. Therefore,

Theorem 2.2. *The number of group homomorphisms $f : \mathbb{Z}_n \to \mathbb{Z}_m, f(x) = ax$ is $d = (m, n)$, where $a = \dfrac{m}{d}k$, and $k = 0, 1, \ldots, d-1$.*

3 Ring homomorphisms

Now let $g : \mathbb{Z}_n \to \mathbb{Z}_m$. If g is a ring homomorphism, g is also a group homomorphism, so $g(x) = ax$ for some $a \in \mathbb{Z}_m$. Thus, in the same way as for group homomorphisms, we need to find the values of $a \in \mathbb{Z}_m$ such that $g(x) = ax$ is a ring homomorphism.

If $g(x) = ax$ is a ring homomorphism, then it is a group homomorphism and $na \equiv 0 \mod m$. Also

$$a \equiv g(1) \equiv g(1^2) \equiv g(1)^2 \equiv a^2 \mod m.$$

We will see that these necessary conditions for a function $g : \mathbb{Z}_n \to \mathbb{Z}_m$ to be a homomorphism of rings, are also sufficient. Thus, suppose $na \equiv 0 \mod m$ and $a \equiv a^2 \mod m$. We already know that for $x, y \in \mathbb{Z}_n, g(x+y) = g(x) + g(y)$, since $na \equiv 0 \mod m$. Also, if $xy = nk + r$ with $0 \leq r < n$, then

$$g(xy) \equiv g(r) \equiv ar \equiv a(xy - nk) \equiv axy - ank \equiv a^2xy \equiv (ax)(ay) \equiv g(x)g(y) \mod m.$$

Therefore g is a ring homomorphism. We have proved the following lemma.

Lemma 3.1. *The function $g : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $g(x) = ax, a \in \mathbb{Z}_m$ is a ring homomorphism if and only if*

$$\begin{aligned} na &\equiv 0 \mod m \text{ and} \\ a &\equiv a^2 \mod m. \end{aligned}$$

Thus, to find the number of ring homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$, we must determine the number of solutions of the system of congruences in the Lemma 3.1, above. Now to find the number of solutions of the system of congruences, we will use the theorem below.

Theorem 3.2. *Let $f_1(x), f_2(x), \ldots, f_k(x)$ be polynomials with integral coefficients, and for any positive integer m let $N(m)$ denote the number of solutions of the system of congruences*

$$\begin{aligned} f_1(x) &\equiv 0 \bmod m, \\ f_2(x) &\equiv 0 \bmod m, \\ &\vdots \\ f_k(x) &\equiv 0 \bmod m. \end{aligned}$$

If $m = m_1 m_2$ where $(m_1, m_2) = 1$, then $N(m) = N(m_1)N(m_2)$. If $m = \prod p^\alpha$ is the factorization of m, then $N(m) = \prod N(p^\alpha)$.

Proof. Suppose that $x \in \mathbb{Z}_m$. If $f_1(x) \equiv 0 \bmod m, f_2(x) \equiv 0 \bmod m, \ldots, f_k(x) \equiv 0 \bmod m$, with $m = m_1 m_2$, then $f_1(x) \equiv 0 \bmod m_1, f_2(x) \equiv 0 \bmod m_1, \ldots, f_k(x) \equiv 0 \bmod m_1$. Let a_1 be the only member of $\mathbb{Z}_{m_1}$ for which $x \equiv a_1 \mod m_1$. It follows that $f_1(a_1) \equiv 0 \mod m_1, f_2(a_1) \equiv 0 \mod m_1, \ldots, f_k(a_1) \equiv 0 \mod m_1$. Similarly, there is only one $a_2 \in \mathbb{Z}_{m_2}$ such that $x \equiv a_2 \mod m_2$, and $f_1(a_2) \equiv 0 \mod m_2, f_2(a_2) \equiv 0 \mod m_2, \ldots, f_k(a_2) \equiv 0 \mod m_2$. Thus, for each solution of the system of congruences modulo m we have a pair (a_1, a_2), in which a_i is a solution of the system of congruences modulo m_i, for $i = 1, 2$. Suppose now that $m = m_1 m_2$, where $(m_1, m_2) = 1$, and that for $i = 1, 2$, the numbers $a_i \in \mathbb{Z}_{m_i}$ are such that $f_1(a_i) \equiv 0 \mod m_i, f_2(a_i) \equiv 0 \mod m_i, \ldots, f_k(a_i) \equiv 0 \mod m_i$. By the Chinese Remainder Theorem, there is only one $x \in \mathbb{Z}_m$ such that $x \equiv a_i \mod m_i$, for $i = 1, 2$. Then we conclude that $f_i(x) \equiv 0 \mod m, i = 1, \ldots, k$. We have now established a one-to-one correspondence between the solutions x of the system of congruences modulo m and the pairs (a_1, a_2) of solutions of the system of congruences modulo m_1 and m_2. Hence, $N(m) = N(m_1)N(m_2)$. Repeatedly applying this to the prime factorization of m, we obtain the second assertion of the theorem. □

Now we use this theorem with the polynomials $f_1(a) = na$ and $f_2(a) = a^2 - a$ by first finding the number of solutions for some p^α, with p prime, and then, using the last part of the theorem.

Let p be a prime number and $\alpha > 0$ an integer, $a(a-1) \equiv a^2 - a \equiv 0 \mod p^\alpha$ has at most two solutions $0, 1$. This is so, since $(a, a-1) = 1$, just one of them can be divisible by p, then $(p^\alpha, a) = 1$ or $(p^\alpha, a-1) = 1$. If $(p^\alpha, a) = 1$, then $p^\alpha | a - 1$, so $a \equiv 1 \bmod p^\alpha$. In the other case, $p^\alpha | a$, so $a \equiv 0 \bmod p^\alpha$.

But, 1 is a solution of $f_1(a) \equiv 0 \mod p^\alpha$ if and only if $p^\alpha | n$, while 0 is always a solution. Thus, the system of congruences

$$\begin{aligned} na &\equiv 0 \mod m, \\ a^2 - a &\equiv 0 \mod m \end{aligned}$$

has two solutions if $p^\alpha | n$ otherwise, it has only one solution.

Now, if $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the canonical factorization of m and $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} q$, with $(q, m) = 1$, the number of solutions to $f_1(a) \equiv 0 \mod p_i^{\alpha_i}$ and $f_2(a) \equiv 0 \mod p_i^{\alpha_i}$ is two if $p_i^{\alpha_i} | n$, and one, if $p_i^{\alpha_i} \nmid n$. So the number of solutions is $\prod_{p_i^{\alpha_i} | n} 2 = \prod_{\alpha_i \leq \beta_i} 2 = 2^\ell$, where $\ell = |\{i | \alpha_i \leq \beta_i\}|$, is the number of elements in the set $\{i | \alpha_i \leq \beta_i\}$.

Theorem 3.3. *Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the prime factorización of m and $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} q$, with $(q, m) = 1$. The number of ring homomorphisms $g : \mathbb{Z}_n \to \mathbb{Z}_m$ from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ is 2^ℓ where $\ell = |\{i | \alpha_i \leq \beta_i\}|$.*

Acknowledgment: We thank the referee for his suggestions.

References

[1] J. A. Gallian and J. Van Buskirk, *The number of homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$*, Amer. Math. Monthly 91 (1984), no. 3, 196 – 197.

[2] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley & Sons, Inc., 1991.