A combinatorial proof of the Chinese remainder theorem over the Gaussian integers

Peeravas Sriburi
Thammanoon Puirod & Yotsanan Meemark
Mahidol Wittayanusorn School, Nakhon pathom/Thailand, sriburipeeravas@gmail.com

1. Introduction

In this project, we look at two theorems in (Dresden & Dymàček, 2005); the complete residue system modulo the least common multiple of two Gaussian integers, and the generalised Chinese remainder theorem to the Gaussian integers. We aim to give new proofs to these following statements of the above two theorems respectively:

Theorem 1. *Let* $\gamma_1 = d_1(a_1 + b_1 i)$, $\gamma_2 = d_2(a_2 + b_2 i)$ *be Gaussians integers, then*

$$\mathbb{Z}[i]_{/\langle [\gamma_1,\gamma_2] \rangle} = \{x + yi \mid 0 \le x < [d_1(a_1^2 + b_1^2), d_2(a_2^2 + b_2^2)], \; 0 \le y < [d_1, d_2]\}$$

Theorem 2. *Let* x, m_1, m_2, a_1, a_2 *be Gaussian integers, the congruence*

$$x \equiv a_1 (\mathrm{mod}\, m_1) \text{ and } x \equiv a_2 (\mathrm{mod}\, m_2)$$

Admit a simultaneous solution if and only if (m_1, m_2) *divides* $a_1 - a_2$. *Moreover, if a solution exists, then it is unique in modulo* $[m_1, m_2]$

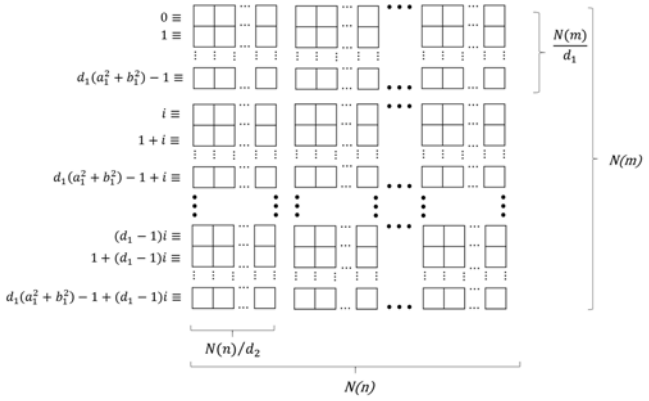
In order to accomplish this project, we use a grid of squares method modified from (Meemark and Prinyasart, 2016) to give a new simple transparent visual proof.

2. Content

Let $\gamma_1 = d_1(a_1 + b_1 i)$ and $\gamma_2 = d_2(a_2 + b_2 i)$ where $(a_1, b_1) = 1 = (a_2, b_2)$ for $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $d_1, d_2 \in \mathbb{Z}$ be Gaussian integers. Construct a $N(\gamma_1) \times N(\gamma_2)$ grid of squares. We split the grid to $d_1 d_2$ blocks, which each has a size of $N(\gamma_1)/d_1 \times N(\gamma_2)/d_2$ We place the sequence of Gaussian integers $0, i, 2i, 3i, \ldots$ into every cell in each block beginning with the upper-left-hand corner block and moving from the block numbered i the block numbered $i+1$ by going one block down and one to the right. If this is not possible (at the last-row block or the rightmost-column block of our $N(\gamma_1) \times N(\gamma_2)$ table), we wrap around to the opposite edge and continue. In any block numbered k that has been placed by the Gaussian integers $k-1$, we add the sequence of integers $0, 1, 2, 3, \ldots$ to its cells in the same way as explained before but we begin at the position $(u+1, v+1)$, where $u \equiv d_1 \lfloor (k-1)/d_1 \rfloor i (\mathrm{mod}\, N(\gamma_1)/d_1)$ and $v \equiv d_2 \lfloor (k-1)/d_2 \rfloor i (\mathrm{mod}\, N(\gamma_2)/d_2)$. We remove Gaussian integers in every of cells that has not been added by the sequence of integers.

Consider this following lemma in (Dresden & Dymàček, 2005): *let* $a, b \in \mathbb{Z}$ *and* $k \in \mathbb{Z}$ *where* $(a,b) = 1$, *the equivalence classes of* $\mathbb{Z}[i]_{/\langle ak+bki \rangle}$ *is* $\{[x + yi] \mid 1 \le x \le k(a^2 + b^2), 0 \le y < k\}$.

By applying the above lemma, we represent row n in the original table with the Gaussian integer $(n - 1 - \lfloor d_1(n-1)/N(\gamma_1) \rfloor) + \lfloor d_1(n-1)/N(\gamma_1) \rfloor i$ and we represent column with the Gaussian integer $(m - 1 - \lfloor d_1(m-1)/N(\gamma_1) \rfloor) + \lfloor d_1(m-1)/N(\gamma_1) \rfloor i$. It can be clearly seen that each row and column is represented by the different element in $\mathbb{Z}[i]_{/\langle \gamma_1 \rangle}$ and $\mathbb{Z}[i]_{/\langle \gamma_2 \rangle}$ respectively so that all numbers in the same row belongs to the same class of $\mathbb{Z}[i]_{/\langle \gamma_1 \rangle}$, as well as all numbers in the same column belongs to $\mathbb{Z}[i]_{/\langle \gamma_2 \rangle}$ as shown in the following Figure



3. Results

1. If u is a number in the table, then $u \in \{x + yi \mid 0 \le x < [d_1(a_1^2 + b_1^2), d_2(a_2^2 + b_2^2)], \; 0 \le y < [d_1, d_2]\}$. Moreover, two numbers appeared in the same cell if and only if they are congruent in modulo $[\gamma_1, \gamma_2]$. Hence,

$$\mathbb{Z}[i]_{/\langle [\gamma_1,\gamma_2] \rangle} = \{x + yi \mid 0 \le x < [d_1(a_1^2 + b_1^2), d_2(a_2^2 + b_2^2)], \; 0 \le y < [d_1, d_2]\}.$$

2. Numbers in the table appear only in the positions (a,b) where $a = Dq_1 + r$ and $b = Dq_2 + r$ for $D = (\gamma_1, \gamma_2)$, $q_1, q_2 \in \mathbb{Z}[i]$ so that $D \mid (a-b)$. Since numbers in the positions (a,b) are congruent with a modulo γ_1 and are congruent with b modulo γ_2, they are solutions to the congruence

$$x \equiv a \pmod{\gamma_1} \text{ and } x \equiv b \pmod{\gamma_2}$$

Since there is a repetitions of number as shown in result 1, the solutions are unique in modulo $[\gamma_1, \gamma_2]$. Hence we have proven the statement of the Chinese remainder theorem over the Gaussian integers;

"Let x, m_1, m_2, a_1, a_2 be Gaussian integers, the congruence

$$x \equiv a_1 \pmod{m_1} \text{ and } x \equiv a_2 \pmod{m_2}$$

Admit a simultaneous solution if and only if (m_1, m_2) divides $a_1 - a_2$. Moreover, if a solution exists, then it is unique in modulo $[m_1, m_2]$"

4. Conclusion

Our new proof gives the same result as (Dresden & Dymàček, 2005) does; it can determine the complete residue system modulo the least common multiple of two Gaussian integers. It also can prove the generalised Chinese remainder theorem to the Gaussian integers. Instead of proving the theorems number theoretically by using Dresden and Dymàček (2005), this new proof employs a simple grid of square, which is easier to visualise and understand to solve both theorems.

Our new proof is also basically a general form of Meemark and Prinyasart (2016). In case imaginary parts are both zero, the table remains only upper-left-hand corner block, which is the proof of the Chinese remainder theorem over integers.

5. Acknowledgement

This project is a part of Mahidol Wittayanusorn School's curriculum growing under supervision of Dr.Thammanoon Puirod and Prof.Dr. Yotsanan Meemark, to whom their express their gratitude. We would like to thank the Junior Science Talent Project and The Young Scientists Competition for subsidy.