involve
a journal of mathematics

A combinatorial proof of a decomposition property of reduced residue systems

Yotsanan Meemark and Thanakorn Prinyasart

msp

2016 vol. 9, no. 3

INVOLVE 9:3 (2016)
dx.doi.org/10.2140/involve.2016.9.361

A combinatorial proof of a decomposition property of reduced residue systems

Yotsanan Meemark and Thanakorn Prinyasart

(Communicated by Filip Saidak)

In this paper, we look at three common theorems in number theory: the Chinese remainder theorem, the multiplicative property of the Euler totient function, and a decomposition property of reduced residue systems. We use a grid of squares to give simple transparent visual proofs.

1. Introduction

Let m and n be positive integers. Construct an $m \times n$ grid of squares. We place the sequence of positive integers $1, 2, 3, \ldots$ into the grid beginning with the upper left-hand corner cell and moving from the cell numbered i to the cell numbered $i+1$ by going one box down and one to the right. If this is not possible (at the last row or the rightmost column of our $m \times n$ table), we wrap around to the opposite edge and continue. It is easy to see that the i-th row has numbers that are congruent to i modulo m and the j-th column has numbers that are congruent to j modulo n.

We observe that two positive integers x and y fill the same cell if and only if $x \equiv y \bmod m$ and $x \equiv y \bmod n$, which is equivalent to $x - y$ is divisible by $[m, n]$, the least common multiple of m and n. From this, it follows that there is a repetition after we get to $[m, n]$ and, of course, that $[m, n]$ is the first integer to arrive at the lower right-hand corner. Thus we have the positive integers from 1 to $[m, n]$ in the table. Notice that we can number all mn boxes in this way if and only if m and n are relatively prime. This follows from $(m, n)[m, n] = mn$. Here (m, n) denotes the greatest common divisor of m and n. When $m = 3$ and $n = 5$, the above explanation can be illustrated by a glued 3×5 table and a discrete torus, which appear in [Terras 1999]; see Figure 1.

In what follows, we point out some applications of this elementary construction. It provides not only a visual verification of two common theorems in number theory, namely, the Chinese remainder theorem and the multiplicative property of the Euler

MSC2010: 11A07.
Keywords: Chinese remainder theorem, reduced residue system.

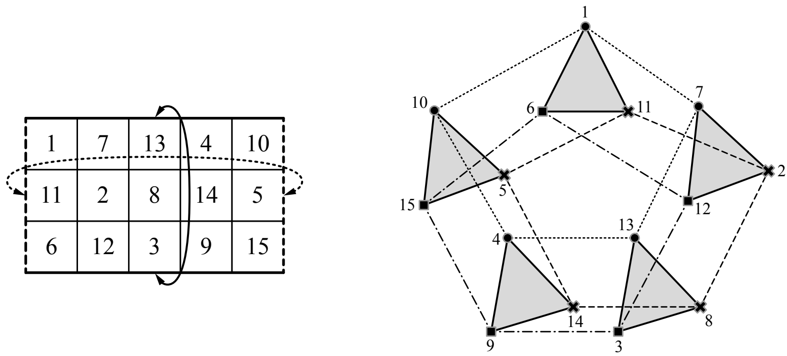

Figure 1. A glued 3×5 table and its corresponding discrete torus.

totient ϕ-function, but also gives a constructive proof for a decomposition property of reduced residue systems, to be defined below. The results are presented in Sections 2 and 3, respectively.

2. The Chinese remainder theorem

Let $d = (m, n)$. We can split the $m \times n$ table into $(m/d) \times (n/d)$ subtables so that each of them is a square $d \times d$ table as shown in Figure 2.

By the above filling method, each subtable has numbers only in its diagonal. For example, the upper left-hand corner subtable will be filled with integers from 1 to d. We move from one subtable to another by going one subtable down and one

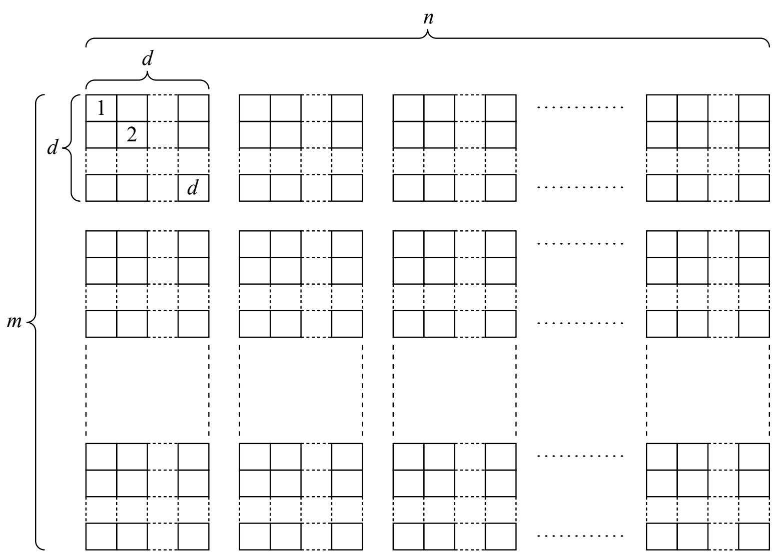

Figure 2. Our division of the $m \times n$ table into $d \times d$ subtables, where $d = (m, n)$.

to the right and wrap around as explained before. Hence a square $d \times d$ subtable can be viewed as a block in an $(m/d) \times (n/d)$ table. Since $(m/d, n/d) = 1$, all $d \times d$ cells have the subsequence

$$(l-1)d + 1, (l-1)d + 2, \ldots, ld \quad \text{for some } l \in \left\{1, 2, \ldots, \frac{mn}{d^2}\right\}$$

in their diagonals. Thus, the $m \times n$ table is transformed into an $(m/d) \times (n/d)$ table with $(m/d, n/d) = 1$ and we can now number all of the mn/d^2 boxes with $1, 2, \ldots, mn/d^2$. Now observe that the integers in the original table appear only in the positions $(k + id, k + jd)$, where $k \le d, i \le m/d - 1$ and $j \le n/d - 1$. In other words, the positions of the integers are (a, b) with $a \equiv b \bmod d$, that is, $d \mid (a - b)$. Furthermore, as mentioned earlier, there is a repetition of solutions modulo $[m, n]$. Therefore we have proved the Chinese remainder theorem:

Theorem 1. *Let m and n be positive integers. For integers a and b, the congruences*

$$x \equiv a \bmod m \quad \textit{and} \quad x \equiv b \bmod n$$

admit a simultaneous solution if and only if (m, n) divides $a - b$. Moreover, if a solution exists, then it is unique modulo $[m, n]$.

The result when $(m, n) = 1$ was also described by Ledet [2007]. We demonstrate Theorem 1 by the following example.

Example 2. Let $m = 6$ and $n = 8$. Then $(m, n) = 2$ and $[m, n] = 24$. Filling the 6×8 table with the numbers from 1 to 24 as previously described, we obtain

1		19		13		7	
	2		20		14		8
9		3		21		15	
	10		4		22		16
17		11		5		23	
	18		12		6		24

According to this table, one easily sees that $x \equiv 22 \bmod 24$ is a simultaneous solution for $x \equiv 4 \bmod 6$ and $x \equiv 6 \bmod 8$, and there is no x for which both $x \equiv 5 \bmod 6$ and $x \equiv 4 \bmod 8$. □

If m is a positive integer, the *Euler totient function* $\phi(m)$ is defined to be the number of positive integers not exceeding m which are relatively prime to m. By a *reduced residue system modulo* m, we mean any set of $\phi(m)$ integers, pairwise incongruent modulo m, each of which is relatively prime to m. Notice that if p is a prime, then $\phi(p) = p - 1$ and $\{1, 2, \ldots, p - 1\}$ is a reduced residue system modulo p. It is also immediate that $\phi(p^s) = p^s - p^{s-1}$ for all $s \in \mathbb{N}$.

Next, we investigate the decomposition property of the reduced residue systems by our combinatorial technique. Let $a = mn$, where m and n are positive integers.

We arrange the positive integers $1, 2, \dots, [m, n]$ into the $m \times n$ grid of squares by using the above filling method and delete the i-th rows and j-th columns of the table for all i and j with $(m, i) > 1$ and $(n, j) > 1$. For a better understanding of this construction, one may erase all even (second, fourth, ...) rows and all even columns of the table in Example 2. Recall that the i-th row has numbers that are congruent to i modulo m and the j-th column has numbers that are congruent to j modulo n.

Let l be a remaining positive integer in the table. Notice that $l \equiv i \bmod m$ with $(m, i) = 1$ and $1 \le i \le m$; that is, $l = i + km$ for some nonnegative integer k. Since $(m, i) = 1$, there exist integers x and y such that $mx + iy = 1$. Consequently, we choose $x' = x - ky \in \mathbb{Z}$ and $y' = y \in \mathbb{Z}$. Then $mx' + ly' = 1$, so we have $(l, m) = 1$. Similarly, we can show that $(l, n) = 1$. Since $a = mn$, we also have $(l, a) = 1$. Hence all positive integers left in the table after deletion are relatively prime to a and less than $[m, n]$.

For $(m, n) = 1$, we can place the positive integers from 1 to $[m, n] = mn = a$ in the $m \times n$ grid by the means above. Erase the i-th rows that are not relatively prime to m and cross out the j-th columns that are not relatively prime to n. Then we obtain $\phi(m)\phi(n)$ undeleted cells and eliminate all numbers that are not relatively prime to m and n. Since $(m, n) = 1$, the entries left in the table coincide with positive integers less than and relatively prime to a, so the number of these entries is equal to $\phi(a)$. Hence we can conclude the well-known multiplicative property of the Euler totient ϕ-function, namely, if $(m, n) = 1$, then $\phi(mn) = \phi(a) = \phi(m)\phi(n)$. This combinatorial proof is the one given in the famous book on number theory [Niven et al. 1991]. Since $\phi(p^s) = p^s - p^{s-1} = p^s(1 - p^{-1})$ when p is a prime and $s \ge 1$, the multiplicative property gives a formula for computing

$$\phi(M) = M \prod_{p \mid M} (1 - p^{-1})$$

for any positive integer M.

3. Decomposition property of reduced residue systems

Let m' be the product of primes in m not in n with the same exponents that they have in m. It is easy to see that m' and n are relatively prime. Place the positive integers from 1 to $m'n$ in the $m' \times n$ grid and erase the rows that are not relatively prime to m' and the columns that are not relatively prime to n. Let l be a positive integer left in the table after deletion. Then $(l, m') = 1 = (l, n)$. Assume that there exists a prime p dividing l and $a = mn$. Thus $p \mid m$ or $p \mid n$. But $(l, n) = 1$, so p is not in n and thus p is in m. Therefore $p \mid m'$, which contradicts the fact that $(l, m') = 1$. Hence the remaining $\phi(m')\phi(n)$ positive integers in the table are relatively prime to a. Consider them as a $\phi(m') \times \phi(n)$ matrix. The set of all members in each row of this matrix is a reduced residue system modulo n and $x \equiv y \mod n$ for all integers x and y that are in the same column.

Let A_0 be the above $\phi(m') \times \phi(n)$ matrix and

$$A_i = A_0 + i \begin{bmatrix} m'n & \dots & m'n \\ \vdots & \ddots & \vdots \\ m'n & \dots & m'n \end{bmatrix}_{\phi(m') \times \phi(n)} \qquad \text{for } i = 0, 1, \dots, \frac{\phi(mn)}{\phi(m')\phi(n)} - 1.$$

The identity $\phi(M) = M \prod_{p|M} (1 - p^{-1})$ shows that

$$\frac{\phi(mn)}{\phi(m')\phi(n)} = \frac{m}{m'},$$

so the index i ranges from 0 up to $m/m' - 1$, which implies that the entries of A_i do not exceed a. It is also obvious that each entry in A_i is relatively prime to a. We augment A_0 by the matrices

$$A_1, \dots, A_{\frac{\phi(a)}{\phi(m')\phi(n)} - 1},$$

respectively, to form a new $(\phi(a)/\phi(n)) \times \phi(n)$ matrix. Then the entries of this matrix are integers from 1 to a, relatively prime to a, with the condition that the set of the entries in each row is a reduced residue system modulo n and $x \equiv y \mod n$ for all integers x and y that are in the same column. Hence we have a constructive proof for a theorem on a decomposition property of reduced residue systems modulo a summarized as follows.

Theorem 3. *Let S be a residue system modulo a, and let $n \geq 1$ be a divisor of a. Then we have the following decompositions of S:*

(1) *S is the union of $\phi(a)/\phi(n)$ disjoint sets, each of which is a reduced residue system modulo n.*

(2) *S is the union of $\phi(n)$ disjoint sets, each of which consists of $\phi(a)/\phi(n)$ numbers congruent to each other modulo n.*

Remark. Another proof of this theorem and its application on character sums can be found in Apostol's book [1976].

Example 4. Consider $a = 48$ with $m = 6$ and $n = 8$. Since $8 = 2^3$ and $6 = 2 \cdot 3$, let $m' = 3$. Filling a 3×8 table with numbers by our technique, we obtain

1	10	19	4	13	22	7	16
17	2	11	20	5	14	23	8
9	18	3	12	21	6	15	24

Delete the rows that contain numbers not relatively prime to 3 and the columns that contain numbers not relatively prime to 8. We have then the 2×4 matrix formed from the remaining numbers given by

$$A = \begin{bmatrix} 1 & 19 & 13 & 7 \\ 17 & 11 & 5 & 23 \end{bmatrix}.$$

Augment this matrix with $\phi(3) = 2$ rows obtained by adding $m'n$ to all entries of A, so we finally reach the decomposition

$$A' = \begin{bmatrix} 1 & 19 & 13 & 7 \\ 17 & 11 & 5 & 23 \\ 25 & 43 & 37 & 31 \\ 41 & 35 & 29 & 47 \end{bmatrix}$$

as desired. □

Acknowledgments

This work grows out of Prinyasart's mini-project at Chulalongkorn University written under the direction of Meemark, to whom he expresses his gratitude. Prinyasart was supported in part by the Development and Promotion of Science and Technology Talents Project.

References

[Apostol 1976] T. M. Apostol, *Introduction to analytic number theory*, Springer, New York, 1976. MR 0434929 Zbl 0335.10001

[Ledet 2007] A. Ledet, "Faro shuffles and the Chinese remainder theorem", *Math. Mag.* **80**:4 (2007), 283–289. MR 2356580 Zbl 1219.05002

[Niven et al. 1991] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., Wiley, New York, 1991. MR 1083765 Zbl 0742.11001

[Terras 1999] A. Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts **43**, Cambridge Univ. Press, 1999. MR 1695775 Zbl 0928.43001

Received: 2011-10-16 Revised: 2014-12-21 Accepted: 2015-06-23

yotsanan.m@chula.ac.th *Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok 10330, Thailand*

thanakorn_dpst@hotmail.com *Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok 10330, Thailand*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2016 is US $160/year for the electronic version, and $215/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2016 vol. 9 no. 3