A Plain Approach to Teach Modular Arithmetic

Masachika Miyata[1], and Takatomi Miyata[2]

***Abstract* – This paper emphasizes the advantage to use the operational notation for modular arithmetic which we proposed, using additional definition and formulas. The domain of the operators is not the set of the integers or the polynomials but the set of the real numbers or the z-transform of the right-sided sequences.**

Index Terms – Operational notation, Chinese remainder theorem, cyclic code encoder, two-sided z transform, rational expression.

INTRODUCTION

Modular arithmetic [1] has been used in many fields of information science and signal processing, as cyclic codes [2], exponentiation-based cryptography [3], number theoretic filters [4], etc. Although computation in modular arithmetic is rather simple, it is not easy for beginners to understand underlying principles. Then we proposed operational notation and showed computation examples [5].

In our prior paper we tried to show as many examples as possible, we cannot explain the reason why we emphasize such notation is preferable for beginners compared with traditional notation, which is described in this paper.

OPERATIONAL NOTATION

Consider the following simpler example of Chinese remainder theorem.

$$|k|_{15} = \left|\left(10|k|_3 + 6|k|_5\right)\right|_{15} \qquad (1)$$

where $|k|_n = k \bmod n$. It is easy for students to confirm this identity for given values of k such as $k = 7,\ 50,\ -13$.

However most of them may say, "It seems to be true, but why is it true for each k?" Our notation is as follows.

Let Γx be the maximum integer not greater than x, and $\Delta x = x - \Gamma x$. Then

$$50 = 3 \times 16 + 2$$

is expressed as

$$50 = 3\Gamma\frac{50}{3} + 3\Delta\frac{50}{3}.$$

Similarly

$$|k|_n = n\Delta\frac{k}{n} \qquad (2)$$

and hence

$$\begin{aligned} &15\Delta\frac{1}{15}\left(10\cdot 3\Delta\frac{k}{3} + 6\cdot 5\Delta\frac{k}{5}\right) \\ &= 15\Delta\left(2\Delta\frac{k}{3} + 2\Delta\frac{k}{5}\right) \\ &= 15\Delta\left(2\cdot\frac{k}{3} - 2\Gamma\frac{k}{5} + 2\cdot\frac{k}{3} - 2\Gamma\frac{k}{5}\right) \\ &= 15\Delta\frac{1}{15}(2\cdot 5 + 2\cdot 3)k \\ &= 15\Delta\left(\frac{k}{15} + k\right) \end{aligned} \qquad (3)$$

Probably, no student will say "Why ?"

A more helpful expression to find a proof of Chinese remainder theorem is

$$|k|_{15} = \left|\left(5|5|_3^{-1}|k|_3 + 3|3|_5^{-1}|k|_5\right)\right|_{15} \qquad (4)$$

or

$$\begin{aligned} \Delta\frac{k}{15} &= \Delta\frac{1}{15}\left(5(\nabla_3 5)3\Delta\frac{k}{3} + 3(\nabla_5 3)5\Delta\frac{k}{5}\right) \\ &= \Delta\frac{1}{15}\left(5\nabla_3 5 + 3\nabla_5 3\right)k \end{aligned} \qquad (5)$$

where $\nabla_n k = |k|_n^{-1}$ denotes the integer m such that

$$|mk|_n = 1 \quad (0 \le m < n)$$

Let $f(k) = 5|5|_3^{-1}|k|_3 + 3|3|_5^{-1}|k|_5$. In application to

(a) If $|f(1)|_3 = |f(1)|_5 = 1$, then $|f(1)|_{15} = 1$.

(b) If $|f(1)|_{15} = 1$ and $f(k) = f(1)k$, then $|f(k)|_{15} = |k|_{15}$,

(5) is preferable to (4), because an equation

$$\left|(i|k|_3 + j|k|_5)\right|_{15} = \left|(i+j)k\right|_{15}$$

may not be true in general. The advantage to use Δ is based on its domain which is not the set of the integers $\mathbb{Z}$ but the set of the real numbers $\mathbb{R}$ as shown in (3). Remark the domain of ∇_n is not $\mathbb{R}$ but $\mathbb{Z}$, and $\nabla_n k$ is the number such that

[1] Masachika Miyata, Division of Engineering Foundations, Kanazawa Institute of Technology, m-miyata@neptune.kanazawa-it.ac.jp
[2] Takatomi Miyata, Department of Information and Computer Science, Kanazawa Institute of Technology, takatomi-miyata@neptune.kanazawa-it.ac.jp

$$\Delta\left(\frac{k}{n}\nabla_n k\right)=\frac{1}{n},\ \ \Delta\nabla_n k=\Gamma\left(\frac{1}{n}\nabla_n k\right)=0 \quad (6)$$

Operational notation is useful for precise and brief expression as mentioned in our prior paper. To emphasize this fact, we show a revised derivation of Hayashi's theorem [3].

$$\begin{aligned}|k|_n &= n\Delta\frac{(n+1)(n+2)}{n}\left(\frac{k}{n+1}-\frac{k}{n+2}\right)\\ &= n\Delta\left(\frac{n+2}{n}|k|_{n+1}\right.\\ &\qquad \left.-\frac{n+1}{n}|k|_{n+2}+\frac{(n+1)(n+2)}{n}m\right)\\ &= \left|\left(2|k|_{n+1}-|k|_{n+2}+2m\right)\right|_n\end{aligned}$$

where $m=\Gamma\frac{k}{n+1}-\Gamma\frac{k}{n+2}$.

FORMULAS

In this section, we show several formulas and an effective example of modular arithmetic for polynomials. Although the coefficient field can be the set of the real numbers [5], we assume that every coefficient is either 0 or 1 hereafter.

Let Ω_n be the set of the two-sided z-transform of right-sided sequences such that

$$\Omega_n=\left\{\sum_{k=n}^{\infty}x_k z^{-k};\ x_k\in\{0,1\}\right\} \quad (7)$$

and Γ and Δ be operators defined by

$$\Gamma\left(\sum_{k=-\infty}^{\infty}x_k z^{-k}\right)=\sum_{k=-\infty}^{0}x_k z^{-k} \quad (8)$$

$$\Delta X(z)=X(z)-\Gamma X(z) \quad (9)$$

where $X(z)\in\Omega_n$ and n may be negative. When $X(z)$ is in Ω_0, $X(z)$ is said to be causal. It is easy to prove

$$X(z)+X(z)=0 \quad (10)$$

$$\Delta 0=\Delta 1=0 \quad (11)$$

$$\Delta\{X(z)+\Gamma Y(z)\}=\Delta X(z) \quad (12)$$

$$\Delta X(z)\Gamma Y(z)=\Delta\{\Delta X(z)\}\Gamma Y(z) \quad (13)$$

where $\Delta X(z)\Gamma Y(z)=\Delta\{X(z)\Gamma Y(z)\}$. From (9) to (12), primitive relations $\Delta\Gamma=0$ and $\Delta\Delta=\Delta$ are obtained without using (8).

As shown in our prior paper a delayed word of a cyclic code generated by $G(z)=\Gamma G(z)$ is expressed as

$$z^{-m}W(z)=z^{-m}\left\{z^m X(z)+G(z)\Delta\frac{z^m X(z)}{G(z)}\right\}$$

A simple implementation of the delayed remainder

$$z^{-m}\left\{z^m X(z) \bmod G(z)\right\}=z^{-m}G(z)\Delta\frac{X(z)}{z^{-m}G(z)}$$

is shown in Fig.1. It is well known that the same output can be obtained by the circuit shown in Fig.2, which suggests a generalized transfer function like $\Delta\dfrac{1}{1+(1+z^{-m}G(z))\Gamma}$.

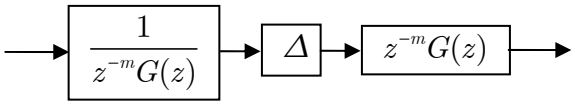

FIGURE 1
PLAIN IMPLEMENTATION

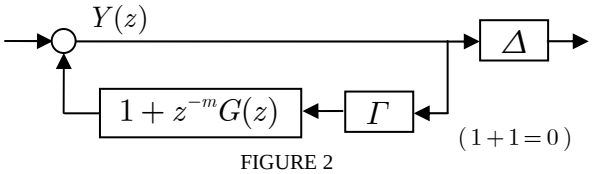

FIGURE 2
PRACTICAL IMPLEMENTATION

The fact that these circuits are equivalent is proved as follows.

$$(\Gamma+\Delta)Y(z)=(1+z^{-m}G(z))\Gamma Y(z)+X(z)$$

$$\Gamma Y(z)=\frac{X(z)+\Delta Y(z)}{z^{-m}G(z)}$$

$$0=\Delta\Gamma Y(z)=\Delta\frac{X(z)+\Delta Y(z)}{z^{-m}G(z)}$$

$$\frac{\Delta Y(z)}{z^{-m}G(z)}=\Delta\frac{\Delta Y(z)}{z^{-m}G(z)}=\Delta\frac{X(z)}{z^{-m}G(z)}$$

$$\Delta Y(z)=z^{-m}G(z)\Delta\frac{X(z)}{z^{-m}G(z)}$$

where $\Gamma z^{-m}G(z)=1$ and $\Delta G(z)=0$ are assumed, and then $1/z^{-m}G(z)\in\Omega_0$ as well as $z^{-m}G(z)\in\Omega_0$.

CONCLUSION

Properties of modular arithmetic are explained from the view point of signal processing using operational notation which is easy for beginners to apply to practical problems.

REFERENCES

[1] Knuth, D. E., *The Art of Computer Programming*, vol.2, 3rd ed., Addison-Wesley, 1997.

[2] Peterson, W. W., *Error-Correcting Codes*, MIT Press, 1961.

[3] Hayashi, A., "A new fast modular multiplication method and its application to modular exponentiation-based cryptography," *IEICE Trans.*, Vol.J81-A, No.10, Oct. 1998, pp.1372-1376.(in Japanese)

[4] Agarwal, R. C. and Burrus, C. S., "Number theoretic transforms to implement fast digital convolution," *Proc. IEEE*, Vol.63, pp.550-560, 1975.

[5] Miyata, M., "WIP --- Operational notation of fractions for signal processing", 34th *ASEE/IEEE Frontiers in Education conference*, T1D-15, 2004.