Jan Długosz University in Częstochowa
Scientific Issues, Mathematics XV, Częstochowa 2010

MODULAR NUMBER SYSTEMS IN THE COMPLEX PLANE

Mikhail Selyaninov

Institute of Technical Education and Safety
Jan Długosz University in Częstochowa
al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland
e-mail: m.selianinov@ajd.czest.pl

Abstract. In the present paper, we consider methods of constructing modular number systems (MNS), named also as residue number systems, in the complex plane. The structure of complete sets of residues (CSR) with respect to complex modulo is investigated. For its creation, the effective constructive rule realizing isomorphism of the given CSR and an adequate ring of real integer residues is proposed.

1. Introduction

Procedures over the complex data in modern computer applications to digital signal processing, numerical methods, theoretical mechanics, physics, other sciences are of fundamental importance. Typical representatives of mentioned procedures are, for example, discrete Fourier transforms, spectral analysis, convolution and correlation of complex sequences, algorithms of linear algebra and differential equations etc. In view of exclusive complexity of this type of applied procedures, studies in the field of modular technique of high-speed parallel computations in the complex plane are among the most priority directions of modern computer science and its applications [1–4].

2. Some theoretical foundations

Let us consider the set of integer complex numbers (ICN) often named also as Gaussian: $\Gamma = \{X + iY \mid X,\ Y \in \mathbf{Z};\ i^2 = -1\}$. The set Γ represents a commutative ring without zero divisor and with four dividers of unity: 1; -1; i and $-i$ [1, 2].

Definition 1. The norm of ICN $U = X + iY$ is the square of its magnitude: $\|U\| = X^2 + Y^2$.

Definition 2. The Gaussians differing by multipliers which are the unit dividers are said to be associated.

Definition 3. The unit dividers of ring Γ and units associated with ICN are named trivial dividers.

Definition 4. The Gaussian having nontrivial zero divisor is called composite, otherwise it is named a Gauss prime number (GPN).

The necessary and sufficient condition of simplicity of the ICN $U = X + iY$ is primality of integer real number (IRN) U. This implies that the norm of GPN is a prime IRN or square of prime IRN. In the first case, the real and imaginary parts of the GPN are distinct from zero, and in the second case, the GPN coincides with the prime IRN accurate within unit dividers.

In the ring Γ the Euclidian lemma is formulated as follows [1].

Lemma. For any ICN A and m in Γ there are some q and r such that

$$A = q\ m; \quad \|r\| < \|m\|. \tag{1}$$

It should be noted that, unlike a real case, the condition $\|r\| < \|m\|$ does not ensure the uniqueness of an incomplete quotient q and a residual r in formula (1).

Definition 5. The common divisor d of the ICN $A_1, A_2, \ldots, A_k$ $(k > 1)$ dividing by another common divisor is named the greatest common divisor (GCD) and is designated as $d = (A_1, A_2, \ldots, A_k)$. For any collection of the ICN $A_1, A_2, \ldots, A_k$ a GCD exists accurate within unit dividers.

Definition 6. If $(A_1, A_2, \ldots, A_k) = 1$, then the ICN $A_1, A_2, \ldots, A_k$ are named coprime.

It is obvious that if $A = X + iY$ and $(X, Y) = 1$, then the conjugate ICN A and $\bar{A} = X - iY$ are coprime: $(A,\ \bar{A}) = 1$. For arbitrary ICN A and GPN p the following statement is valid: $(A,\ p)$ does not divide A. Also in the case when ICN $m_1, m_2, \ldots, m_k$ are pairwise prime, then the least common multiple is $[m_1, m_2..., m_k] = M_k = \prod\limits_{i=1}^{k} m_i$.

Following the offered technique of constructing a modular number systems (MNS) [5–7] first of all we study the structure of adjanced classes of factor ring $\Gamma/(m)$, where (m) is a principal ideal generated by some Gaussian

$m = m' + im''$ $(m',\ m'' \in Z)$. We also will study the problem of choice of the complete set of residues (CSR) modulo m.

The given CSR (as distinct from CSR $|\cdot|_m$ in the real case) will be designated as $\langle\cdot|_m$, thus for the set member of CSR being a result of modulo operation over ICN $A \in \Gamma$ a denotation $\langle\ A|_m$ is used. Specifically, in the case whent A vary over Γ, a set of all various residuals r satisfying (1) can be selected as a ring $\langle\cdot|_m$.

Theorem 1. Let $m = m' + im''$ be an arbitrary module from Γ. Two ICN $A = A' + iA''$ and $B = B' + iB''$ belong to the same residue class of factor ring $\Gamma/(m)$ if and only if the same components of pairs ICN $(m'\ A' + m''\ A'';\ m'\ A'' - m''\ A')$ and $(m'\ B' + m''\ B''; m'\ B'' - m''\ B')$ belong to the same classes of factor ring $\Gamma/(\|m\|)$. In other words, the complex congruence

$$A \equiv B\ (mod\ m) \tag{2}$$

is equivalent to simultaneous real congruences

$$\begin{cases} m'A' + m''A'' \equiv m'B' + m''B'', \\ m'A'' - m''A' \equiv m'B'' - m''B'. \end{cases} \tag{3}$$

Proof. At first, we assume that $A,\ B \in (m) \subset \Gamma$. This implies validity of (2) and guarantees existence of some ICN $q = q' + iq''$ such that

$$A - B = q\ m. \tag{4}$$

Multiplying (4) by $\bar{m} = m' - im''$, we obtain

$$(m'(A' - B') + m''(A'' - B''))+$$

$$i((m'(A'' - B'') + m''(A' - B')) = (q' + iq'')\|m\|.$$

It follows that

$$\begin{cases} (m'A' + m''A'') - (m'B' + m''B'') \in (\|m\|) \subset \mathbf{Z}, \\ (m'A'' - m''A') - (m'B'' - m''B') \in (\|m\|) \subset \mathbf{Z}; \end{cases}$$

thus resulting in simultaneous congruences (3). The described operations realized in the reverse sequence from (3) lead to (2). The theorem is proved.

As for any ICN $A = A' + iA''$ the congruence

$$A \equiv \langle A|_m\ (mod\ m) \tag{5}$$

and also the simultaneous congruences

$$\begin{cases}(m'A' + m''A'') \equiv |(m'A' + m''A'')|_{\|m\|}, \\ (m'A'' - m''A') \equiv |(m'A'' - m''A')|_{\|m\|}\end{cases} \tag{6}$$

are true, then from the point of view of the theorem 1 it is natural to assume that the complex residue $\alpha = \langle A|_m$ can be uniquely defined by means of a pair of the real residues

$$(a';\ a'') = (|(m'A' + m''A'')|_{\|m\|};\ |(m'A'' - m''A')|_{\|m\|}).$$

Let us prove the hypothesis validity. Let $\alpha = \alpha' + i\alpha''$ ($\alpha',\ \alpha''\ \in \mathbf{Z}$). By setting $B = \alpha$ in the theorem 1 according to (3), we have

$$\begin{cases}(m'A' + m''A'') \equiv |(m'\alpha' + m''\alpha'')|_{\|m\|}, \\ (m'A'' - m''A') \equiv |(m'\alpha'' - m''\alpha')|_{\|m\|}.\end{cases} \tag{7}$$

Let us demand that the right-hand members of the same congruences of simultaneous congruences (3) and (7) coincide. Then for the real and imaginary components of residue $\langle A|_m$ we obtain the simultaneous equations

$$\begin{cases}m'\alpha' + m''\alpha'' = a', \\ m'\alpha'' - m''\alpha' = a'',\end{cases} \tag{8}$$

which solution is

$$(\alpha',\ \alpha'') = \left(\frac{m'a' + m''a''}{\|m\|};\ \frac{m'a'' - m''a'}{\|m\|}\right). \tag{9}$$

Thus,

$$\alpha = \frac{m'a' + m''a''}{\|m\|} + i\ \frac{m'a'' - m''a'}{\|m\|} = \frac{(m' + im'')(a' + ia'')}{\|m\|}$$

or

$$\langle A|_m = \alpha = \frac{m}{\|m\|}\ \left(|(m'A' + m''A'')|_{\|m\|} + i\ |(m'A'' - m''A')|_{\|m\|}\right). \tag{10}$$

The rule (10) for constructing the CSR $\langle A|_m$ generated by one-to-one correspondence between the ICN (α'; α'') and (a'; a'') (see (8), (9)) can be represented in specified and more constructive form.

Theorem 2. In the case when
a) a module m is a nonnegative IRN ($m' > 1,\ m'' = 0$);
b) a module $m = m' + im''$ is a complex module satisfying the condition $(m',\ m'') = 1$
for the residue $\langle A|_m$ corresponding to the arbitrary ICN $A = A' + iA''$ the followig formulas are true, accordingly,

$$\langle A' + iA''|_m = \langle A'|_m + i\langle A''|_m, \tag{11}$$

$$\langle A' + iA''|_m = \frac{1}{\|m\|}\ \big((m'|m'R_m(A)|_{\|m\|} - m''|m''R_m(A)|_{\|m\|}\big) \\ + i(m'| - m''R_m(A)|_{\|m\|} + m''|m'R_m(A)|_{\|m\|})), \tag{12}$$

where

$$R_m(A) = R_m(A',\ A'') = |A' + JA''|_{\|m\|}\ \left(J = |\frac{m''}{m'}|_{\|m\|}\right). \tag{13}$$

Proof. Let $m = m'$. Then according to (9)

$$\alpha' = \frac{m'a'}{\|m\|} = \frac{1}{m}|mA'|_{m^2} = \frac{1}{m}\left(mA' - \lfloor\frac{mA'}{m^2}\rfloor\ m^2\right) = A' - \lfloor\frac{A'}{m}\rfloor m = |A'|_m,$$

where the integer part of a real number x is designated as $\lfloor x\rfloor$. Similar calculations for a'' give the equality $\alpha'' = |A''|_m$. Thus, in the case a) the equality (11) is true.

Consider now the case b). As $|(m')^2 + (m'')^2|_{\|m\|} = 0$, taking into account (13), we have

$$a' = |m'A' + m''A''|_{\|m\|} = |m'\left(A' + A''\frac{m''}{m'}\right)|_{\|m\|} = |m'R_m(A)|_{\|m\|}, \tag{14}$$

$$a'' = |m'A'' - m''A'|_{\|m\|} = |\frac{(m')^2}{m'}A'' - m''A'|_{\|m\|} = \\ | - \frac{(m'')^2}{m'}\ A'' - m''A'|_{\|m\|} = | - m''R_m(A)|_{\|m\|}. \tag{15}$$

Correctness of expressions (14) and (15) is ensured by the condition $(m',\ \|m\|) = 1$ following from the theorem condition $(m',\ m'') = 1$. Substitution (14) and (15) into (9) leads to the required outcome (12).

Theorem 2 can be also generalized to a case of arbitrary complex module m. However, for computer applications classes of the modules considered in the theorem 2 are the most acceptable.

Theorem 3. The complete set of residues $\langle\cdot|_m$ is isomorphic, correspondingly:

a) to the combinatorial square $(|\cdot|_m)^2$ of the ring $|\cdot|_m$ in the case when a natural module $m > 1$;

b) to the ring $|\cdot|_{\|m\|}$ in the case when $m = m' + im''$ is a complex module satisfying the condition $(m',\ m'') = 1$ with $|\langle\cdot|| = \|m\|$.

Proof. According to the main theorem of modular arithmetic [6, 7] in the case of natural module m, the mapping $f\colon |\cdot|_m \times |\cdot|_m \to \langle\cdot|_m$, which for every $A = A' + iA'' \in \Gamma$ associates to a pair of IRN $(|A'|_m;\ |A''|_m) \in (|\cdot|_m)^2$ a complex residue $\langle A|_m \in \langle\cdot|_m$ defined by formula (11), is bijective. Then on account of surjectivity of mapping $A \to (|A'|_m;\ |A''|_m)$, the cardinality of ring $\langle\cdot|_m$ coincides with the cardinality of a set $|\cdot|_m \times |\cdot|_m$, i.e. $|\langle\cdot||_m = m^2 = \|m\|$.

This formula also takes place in the case when the complex module m satisfies the condition $(m',\ m'') = 1$, because of surjectivity of mapping $A \to R_m(A',\ A'')$ (see (13)) and bijectivity of mapping $f\colon |\cdot|_{\|m\|} \to \langle\cdot|_m$ which for every $A \in \Gamma$ associates the complex residue $\langle A|_m$ formed by a rule (12) with an IRN $R(A',\ A'') \in |\cdot|_{\|m\|}$.

The fact that the specified-above mapping f is an isomorphism of corresponding rings in the case of the real module m is proved by equations

$$\langle\langle A' + iA''|_m + \langle B' + iB''|_m|_m = ||A'|_m + |B'|_m|_m + i||A''|_m + |B''|_m|_m,$$

$$\langle\langle A' + iA''|_m \cdot \langle B' + iB''|_m|_m = ||A'|_m \cdot |B'|_m - |A''|_m \cdot |B''|_m|_m +$$
$$i||A'|_m \cdot |B''|_m + |A''|_m \cdot |B'|_m|_m,$$

and in the case of complex module $m = m' + im''$ such that $(m',\ m'') = 1$, is proved by equations

$$R_m(A + B) = R_m(Re(A + B),\ Im(A + B)) =$$
$$|A' + B' + J(A'' + B'')|_m = |R_m(A) + R_m(B)|_{\|m\|}, \tag{16}$$

$$R_m(A \cdot B) = R_m(Re(A \cdot B),\ Im(A \cdot B)) =$$
$$R_m(A'B' - A''B'',\ A'B'' + A''B') = |A'B' - A''B'' + J(A'B'' + A''B')|_{\|m\|} =$$
$$|A'(B' + JB'') + A''(-B'' + JB')|_{\|m\|} = |A'R_m(B) + A''(J^2B'' + JB')|_{\|m\|} =$$
$$|A'R_m(B) + JA''R_m(B)|_{\|m\|} = |(A' + JA'')R_m(B)|_{\|m\|} =$$
$$|R_m(A)R_m(B)|_{\|m\|}. \tag{17}$$

It follows from (8) that the considered CSR $\langle\cdot|$ is formed by all the ICN $\alpha = \alpha' + i\alpha''$ satisfying simultaneous inequalities

$$\begin{cases} 0 \le m'\alpha' + m''\alpha'' < \|m\|, \\ 0 \le m'\alpha'' - m''\alpha' < \|m\|. \end{cases}$$

Thus, the ring $\langle\cdot|_m$ includes all the ICN arranged in a square with vertexes $A_1 = (0;\ 0)$, $A_2 = (m';\ m'')$, $A_3 = (m' - m'';\ m' + m'')$, $A_4 = (-m'';\ m')$.

For the computer applications of interest are those complex modular number systems (CMNS) for which the ranges $\langle\cdot|_{M_k}$, where $M_k = \prod\limits_{i=1}^{k} m_i$ with $m_1, m_2 ..., m_k$ being pairwise coprime modules, are located in the specified-above squares with the sides parallel to the axes. This means that M_k is an IRN. However, the present condition does not eliminate a possibility of using the ICN as modules $m_i,\ i = 1, 2, \dots, k$.

In particular, for practical applications it is convenient to use the CMNS with modules $m_1, m_2, \dots, m_k$ such that all or part of them are considered as macromodules which represent products of two conjugated ICN, i.e. $m = p\bar{p}$ where $p = p' + ip'',\ \bar{p} = p' - ip'';\ p', p'' \ \in \mathbf{Z}$. In accordance with theorems 2 and 3, it is expedient to select the numbers p and $\bar{p}$ based on conditions $p' > 0,\ p'' > 0$ and $(p',\ p'') = 1$. The last condition guarantees relative primality of the ICN p and $\bar{p}$. Such systems are called quadratic MNS.

References

[1] I.J. Akushsky, V.M. Amerbaev, I.T. Pak. *Bases of Machine Arithmetics of Complex Numbers.* Nauka, Alma-Ata, 1970. (In Russian).

[2] V.M. Amerbaev, I.T. Pak. *Parallel Calculation in Complex Plane.* Nauka, Alma-Ata, 1985. (In Russian).

[3] A.F. Chernyavsky, V.V. Danilevich, A.A. Kolyada, M.Y. Selyaninov. *High-speed Methods and Systems of Digital Information Processing.* Belgosuniversitet, Minsk, 1996. (In Russian).

[4] M. Selyaninov. Modular technique of parallel information processing. *Scientific Issues of Jan Długosz University of Częstochowa, Ser. Mathematics*, **XIII**, 43–52, 2008.

[5] A.A. Kolyada, V.V. Revinsky, M.Y. Selyaninov *et al.* Theoretical bases of modular computing structures on the finite mathematical models. *Modern Problems of Optics, Radiation Materials Science, Informatics, Radiophysics and Electronics. Proc. Sci. Research Inst. Appl. Phys. Probl.* Belgosuniversitet, Minsk, vol. 2, pp. 4–9, 1996. (In Russian).

[6] M.Y. Selyaninov. Theoretical bases of modular codification of algebraic systems. *Proc. Nat. Acad. Sci. Belarus,* No. 1, 114–119, 2002. (In Russian).

[7] M. Selyaninov. Construction of modular number systems with arbitrary finite ranges. *Scientific Issues of Jan Długosz University in Częstochowa, Ser. Mathematics*, **XIV**, 105–115, 2009.