УДК 681.142

В.А. КРАСНОБАЕВ, д-р техн. наук, А.А. ЗАМУЛА, д-р техн. наук, В.Н. ШЛОКИН

МЕТОДЫ ОПРЕДЕЛЕНИЯ ВЫЧЕТОВ ЧИСЕЛ В КОМПЛЕКСНОЙ ЧИСЛОВОЙ ОБЛАСТИ

Введение

Повышение производительности компьютерных систем и компонент обработки целочисленных данных (КСКОЦД), функционирующих в двоичной позиционной системе счисления (ПСС), связано, прежде всего, с увеличением рабочих частот элементов и использованием моделей и методов формального синтеза, временных мультипараллельных систем и программ [1 – 3]. В то же время теоретически и практически показано, что использование непозиционной системы счисления в остаточных классах (СОК) позволяет кардинально повысить производительность и улучшить другие технические характеристики КСКОЦД [3 – 5]. Как показали исследования, важным является факт эффективного использования СОК в гиперкомплексной числовой области [6, 7].

Обобщением целых рациональных чисел являются целые комплексные (гауссовы) числа (КЧ). Целые гауссовы числа образуют кольцо: их сумма, разность и произведение также являются (как и числа в СОК) целыми гауссовыми числами. На основе свойств СОК были разработаны патентоспособные компоненты компьютерной системы обработки целочисленных данных в комплексной области [8 – 10]. В настоящее время растет интерес к непозиционной системе счисления в СОК среди разработчиков информационно-телекоммуникационных систем, реализующих процессы формирования, передачи и обработки сигналов – физических переносчиков данных, криптографического преобразования данных, сжатия видеоинформации и т. д. [11 – 19].

Цель статьи – рассмотрение методов практического определения вычетов целочисленных данных в комплексной числовой области.

Основная часть

В СОК для комплексной числовой области значения остатков КЧ представляются комплексными и вещественными вычетами по комплексным основаниям. Обработка целочисленных данных, представленных в комплексной области, основывается на результатах теоремы 1 [3].

Теорема 1. В комплексной числовой области со взаимно простыми комплексными основаниями $\dot{m}_1, \dot{m}_2, ..., \dot{m}_n$ любое представимое комплексное число $\dot{A} = a + bi$ единственным образом представляется в СОК совокупностью своих наименьших комплексных вычетов $\dot{a}_1, \dot{a}_2, ..., \dot{a}_n$ по основаниям системы.

Перед рассмотрением методов определения вычетов целочисленных данных в комплексной числовой области определим условия делимости целых КЧ [3]. Так, комплексное целое число вида $\dot{A} = a + bi$ будет считаться кратным комплексному модулю $\dot{m} = p + qi$ ($\dot{m}$ будет называться делителем числа $\dot{A}$), если частное $\frac{\dot{A}}{\dot{m}}$ является целым комплексным числом, т. е. должно выполняться условие

$$\frac{\dot{A}}{\dot{m}} = \frac{a+bi}{p+qi} = \frac{(a+bi)\cdot(p-qi)}{p^2+q^2} = \frac{a\cdot p+b\cdot q}{p^2+q^2} + \frac{b\cdot p-a\cdot q}{p^2+q^2} i. \qquad (1)$$

Очевидно, что выражение (1) будет целым КЧ, если выполняется условие

$$\begin{cases} (a\cdot p+b\cdot q) \equiv 0 \bmod (p^2+q^2), \\ (b\cdot p-a\cdot q) \equiv 0 \bmod (p^2+q^2). \end{cases} \qquad (2)$$

Пусть $\dot{S} = e + fi$ такое КЧ, что значение $\dot{A} - \dot{S}$ делится на число $\dot{m}$, тогда $\dot{S}$ является вычетом КЧ $\dot{A}$ по комплексному модулю $\dot{m}$, т.е. выполняется сравнение

$$\dot{A} \equiv \dot{S} (\mathrm{mod}\, \dot{m}), \tag{3}$$

где $N = p^2 + q^2$ – норма модуля $\dot{m} = p + qi$.

Пример 1. Определить делимость КЧ $\dot{A} = 17 + 7i$ на комплексный модуль $\dot{m} = 3 + 2i$.

Определяем следующие значения: $N = p^2 + q^2 = 3^2 + 2^2 = 13$; $a \cdot p + b \cdot q = 17 \cdot 3 + 7 \cdot 2 = 51 + 14 = 65$; $b \cdot p - a \cdot q = 7 \cdot 3 - 2 \cdot 17 = -13$. Условия (2) выполняются, т.е. $65 \equiv 0 \mathrm{mod} 13$ и $-13 \equiv 0 \mathrm{mod} 13$. Таким образом, КЧ $\dot{A} = 17 + 7i$ делится на комплексный модуль $\dot{m} = 3 + 2i$ без остатка.

Пример 2. Определить делимость КЧ $\dot{A} = 1 + i$ на комплексный модуль $\dot{m} = 1 + 2i$.

Определяем следующие значения: $N = p^2 + q^2 = 1^2 + 2^2 = 5$; $a \cdot p + b \cdot q = 1 \cdot 1 + 1 \cdot 2 = 3$ и $b \cdot p - a \cdot q = 1 \cdot 1 - 1 \cdot 2 = -1$. В этом случае, $3 \equiv 3 \mathrm{mod} 5$ и $(-1) \equiv 4 \mathrm{mod} 5$. Таким образом, имеем, что $3 \neq 4$, т.е. условия (2) не выполняются. В этом случае КЧ $\dot{A} = 1 + i$ не делится нацело на комплексный модуль $\dot{m} = 1 + 2i$, т.е. существует ненулевой остаток $x + yi$.

Метод определения комплексного вычета $x + iy$ целого комплексного числа $\dot{A} = a + bi$ по комплексному модулю $\dot{m} = p + qi$

Для понимания метода определения комплексного вычета целого комплексного числа по комплексному модулю рассмотрим следующую теорему 2 [3].

Теорема 2. Пусть даны КЧ $\dot{A} = a + bi$ и комплексный модуль $\dot{m} = p + qi$, и при этом выполняются следующие сравнения:

$$\begin{cases} (a \cdot p + b \cdot q) \equiv (x \cdot p + y \cdot q) \mathrm{mod} (p^2 + q^2), \\ (b \cdot p - a \cdot q) \equiv (y \cdot p - x \cdot q) \mathrm{mod} (p^2 + q^2). \end{cases} \tag{4}$$

Тогда $\dot{A} = (x + yi) \mathrm{mod}\, \dot{m}$, т.е. значение $x + yi$ является комплексным вычетом КЧ $\dot{A}$ по комплексному модулю $\dot{m}$.

Доказательство. Делим КЧ $\dot{A} - (x + yi)$ на модуль $\dot{m} = p + qi$. Получим

$$\frac{\dot{A} - (x + yi)}{\dot{m}} = \frac{(a - x) + (b - y)i}{p + qi} = \frac{[(a - x) + (b - y)i]}{p^2 + q^2} =$$

$$= \frac{(a - x) \cdot p + (b - y) \cdot q}{p^2 + q^2} + \frac{(b - y) \cdot p - (a - x) \cdot q}{p^2 + q^2} i.$$

Для того чтобы в результате операции деления получилось целое КЧ, должно иметь место сравнение

$$\begin{cases} [(a - x) \cdot p + (b - y) \cdot q] \equiv 0 \mathrm{mod} (p^2 + q^2), \\ [(b - y) \cdot p - (a - x) \cdot q] \equiv 0 \mathrm{mod} (p^2 + q^2). \end{cases} \tag{5}$$

Или

$$\begin{cases} (a \cdot p - x \cdot p + b \cdot q - y \cdot q) \equiv 0 \mathrm{mod} (p^2 + q^2), \\ (b \cdot p - y \cdot p - a \cdot q - x \cdot q) \equiv 0 \mathrm{mod} (p^2 + q^2). \end{cases} \tag{6}$$

Из (6) имеем, что

$$\begin{cases} [(a \cdot p + b \cdot q) - (x \cdot p + y \cdot q) \equiv 0 \mathrm{mod} (p^2 + q^2), \\ [(b \cdot p - a \cdot q) - (y \cdot p - x \cdot q)] \equiv 0 \mathrm{mod} (p^2 + q^2). \end{cases} \tag{7}$$

Сравнение (7) эквивалентно сравнению (4). Что и требовалось доказать. Таким образом,

число $x+yi$ является вычетом КЧ $\dot{A}=a+bi$ по модулю $\dot{m}=p+qi$.

Метод определения комплексного вычета состоит в решении сравнений (4) путем реализации совокупности операций, входящих в сравнения (7).

Приведем конкретные примеры определения $x+yi$ любого КЧ $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$

Пример 3. Определить вычет $x+yi$ числа $\dot{A}=15+2i$ по модулю $\dot{m}=3+2i$ ($N=p^2+q^2=9+4=13$). В соответствии с выражением (4) запишем систему сравнений в виде

$$\begin{cases}(15\cdot 3+2\cdot 2)\equiv(3x+2y)\bmod 13,\\ 2\cdot 3-15\cdot 2\equiv(3y-2x)\bmod 13.\end{cases}$$

Или

$$\begin{cases}49\equiv(3x+2y)\bmod 13,\\ -24\equiv(3y-2x)\bmod 13.\end{cases}$$

В этом случае имеем систему из двух сравнений с двумя неизвестными вида

$$\begin{cases}3x+2y\equiv 49\bmod 13,\\ 3y-2x\equiv -24\bmod 13.\end{cases}$$

С учетом того, что $49(\bmod 13)=10$ и $-24(\bmod 13)=2$ получим систему из двух линейных уравнений

$$\begin{cases}3x+2y=10,\\ -2x+3y=2.\end{cases}$$

Решение этой системы из двух линейных уравнений будет состоять из двух значений $x=2$ и $y=2$. В этом случае искомый вычет (результат) $x+yi$ равен числу $x+yi=2+2i$. Таким образом, вычет $x+yi$ КЧ $\dot{A}=15+2i$ по модулю $\dot{m}=3+2i$ равен $x+yi=2+2i$. Или можно записать результат решения в виде сравнения $(15+2i)\equiv(2+2i)\bmod(3+2i)$.

Пример 4. Определить вычет $x+yi$ числа $\dot{A}=1+i$ по модулю $\dot{m}=1+2i$ ($N=p^2+q^2=1+4=5$).

В соответствии с (4) составим и решим систему сравнений

$$\begin{cases}(1\cdot 1+1\cdot 2)\equiv(x\cdot 1+y\cdot 2)\bmod 5,\\ (1\cdot 1-1\cdot 2)\equiv(y\cdot 1-x\cdot 2)\bmod 5.\end{cases}$$

$$\begin{cases}(x+2\cdot y)\equiv 3(\bmod 5),\\ (-2\cdot x+y)\equiv -1(\bmod 5).\end{cases}$$

$$\begin{cases}x+2\cdot y\equiv 3(\bmod 5),\\ -2\cdot x+y\equiv 4(\bmod 5).\end{cases}$$

$$\begin{cases}x+2\cdot y=3,\\ -2\cdot x+y=4.\end{cases}$$

$$x=3-2\cdot y,$$

$$-2\cdot(3-2\cdot y)+y=4,$$

$$-6+4y+y=4,$$

$$5\cdot y=10,$$

$$y=2.$$

$$x = 3 - 2 \cdot y,$$

$$x = 3 - 2 \cdot 2 = -1 (\mathrm{mod}\, 5),$$

$$x = 4.$$

Таким образом: $(x + yi) = 4 + 2i$, т.е. $\dot{A} = (x + yi) \bmod \dot{m}$. Или результат можно записать в виде сравнения $(1+i) \equiv (4+2i) \bmod (1+2i)$.

Пример 5. Определить вычет $x + yi$ числа $\dot{A} = 15 + 2i$ по модулю $\dot{m} = 1 + 2i$ ($N = 5$; $a = 15$, $b = 2$; $p = 1$, $q = 2$).

В соответствии с выражением (4) составим систему сравнений в виде

$$\begin{cases} (15 \cdot 1 + 2 \cdot 2) \equiv (x \cdot 1 + 2 \cdot y) \bmod 5, \\ (2 \cdot 1 - 15 \cdot 2) \equiv (y \cdot 1 - x \cdot 2) \bmod 5. \end{cases}$$

$$\begin{cases} 19 \equiv (x + 2 \cdot y) \bmod 5, \\ (-28) \equiv (-2 \cdot x + y) \bmod 5. \end{cases}$$

Систему сравнений представим как систему из двух линейных уравнений

$$\begin{cases} x + 2 \cdot y = 19, \\ -2 \cdot x + y = -28. \end{cases}$$

Решение системы уравнений будет представлено в виде $x = 15$, $y = 2$. Т.е. решение $\dot{A} \equiv (x + yi) \bmod \dot{m}$ представится в виде $(15 + 2i) \equiv (15 + 2i) \bmod (1 + 2i)$.

Пример 6. Найти комплексный вычет $x + yi$ комплексного числа $\dot{A} = 2 + i$ по комплексному модулю $\dot{m} = 1 + 2i$.

В соответствии с выражением (4) составим систему сравнений в виде

$$\begin{cases} (2 \cdot 1 + 1 \cdot 2) \equiv (x \cdot 1 + y \cdot 2) \bmod 5, \\ (1 \cdot 1 - 2 \cdot 2) \equiv (y \cdot 1 - x \cdot 2) \bmod 5. \end{cases}$$

Или

$$\begin{cases} 4 \equiv (x + 2y) \bmod 5, \\ (-3) \equiv (y - 2x) \bmod 5. \end{cases}$$

На основании системы сравнений составим и решим систему двух линейных уравнений

$$\begin{cases} x + 2 \cdot y = 19, \\ -2 \cdot x + y = 2, \end{cases}$$

$$x = 4 - 2y,$$

$$-2 \cdot (4 - 2y) + y = 2,$$

$$-8 + 4y + y = 2,$$

$$5y = 10,$$

$$y = 2.$$

В этом случае $x = 4 - 2y = 4 - 4 = 0$, а вычет (остаток) равен $x + yi = 0 + 2i = 2i$. Т.е. результат $x + yi = 2i$ решения сравнения $\dot{A} \equiv (x + yi) \bmod \dot{m}$ можно представить следующим образом: $(2 + i) \equiv (2i) \bmod (1 + 2i)$.

Метод определение наименьшего комплексного вычета $x+iy$ комплексного числа $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$

Известно, что для КЧ не определены понятия "больше" и "меньше". Однако в математике представляется возможным формально (например, формально полагают, что $0!=1$) определить понятие наименьшего комплексного вычета по комплексного модулю. Основная идея такого определения состоит в том, что поскольку определение комплексного вычета распространяется на системы вещественных сравнений (4), то потребовав, чтобы $x\cdot p+y\cdot q$ и $y\cdot p-x\cdot q$ были соответственно наименьшими вычетами по модулю $N=p^2+q^2$, получим вполне определенное КЧ $x+yi$, которое формально можно назвать наименьшим вычетом числа $\dot{A}$ по модулю $\dot{m}$, т.е. предполагается, что

$$\begin{aligned} x\cdot p+y\cdot q &\le p^2+q^2-1,\\ y\cdot p-x\cdot q &\le p^2+q^2-1. \end{aligned} \tag{8}$$

При этом различают наименьшие вычеты и абсолютно наименьшие вычеты. В первом случае предполагается, что $x\cdot p+y\cdot q$ и $y\cdot p-x\cdot q$ являются натуральными числами, не превосходящими значения p^2+q^2-1. Во втором случае предполагается, что эти величины могут быть как положительными, так и отрицательными, но не превосходящими по абсолютной величине значения $\frac{p^2+q^2}{2}$ [3].

Если найдены наименьшие вычеты выражений

$$\begin{cases} \Gamma=(a\cdot p+b\cdot q)\bmod(p^2+q^2);\\ \Gamma'=(b\cdot p-a\cdot q)\bmod(p^2+q^2), \end{cases} \tag{9}$$

то наименьший вычет числа $\dot{A}$ по модулю $\dot{m}$

$$x+yi=\frac{\Gamma\cdot p-\Gamma'\cdot q}{p^2+q^2}+\frac{\Gamma'\cdot p+\Gamma\cdot q}{p^2+q^2}i, \tag{10}$$

где Γ и Γ' – наименьшие положительные вычеты по вещественному модулю $N=p^2+q^2$; Γ и Γ' могут принимать значения вещественных чисел $0,1,...,N-1$.

Согласно (4) получаем систему из 2-х линейных сравнений с двумя неизвестными:

$$\begin{cases} \Gamma\equiv(x\cdot p+y\cdot q)\bmod(p^2+q^2);\\ \Gamma'\equiv(y\cdot p-x\cdot q)\bmod(p^2+q^2). \end{cases} \tag{11}$$

Как и ранее, наименьший вычет $x+yi$ числа $\dot{A}=a+bi$ по модулю $\dot{m}=p+qi$ равен и обозначается как $(a+bi)\equiv(x+yi)\bmod\dot{m}$. Установлено, что наименьший вычет $x+yi$ любого КЧ $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$ определяется исходя из решения системы двух вещественных сравнений (11).

Приведем конкретные примеры определения наименьшего вычета $x+yi$ любого КЧ $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$.

Пример 7. Определить наименьший вычет $x+yi$ числа $\dot{A}=15+2i$ по модулю $\dot{m}=1+2i$ ($a=15$, $b=2$; $p=1$, $q=2$; $N=p^2+q^2=1^2+2^2=5$).

По формуле (10) определим значение $x+yi$, где значения Γ и Γ' определяются в соответствии с формулой (9):

$$\Gamma=(a\cdot p+b\cdot q)\bmod N=(15\cdot1+2\cdot2)\bmod5=19(\bmod5)=4;$$

$$\Gamma'=(b\cdot p-a\cdot q)\bmod N=(2\cdot1-15\cdot2)\bmod5=(-28)\bmod5=(-3)\bmod5=2.$$

По формуле (10) определяем наименьший вычет $x+yi$, т.е.

$$x+yi=\frac{\Gamma\cdot p+\Gamma'\cdot q}{N}+\frac{\Gamma'\cdot p+\Gamma\cdot q}{N}i=\frac{4\cdot 1-2\cdot 2}{5}+\frac{2\cdot 1+4\cdot 2}{5}i=2i\,.$$

Пример 8. Определить наименьший вычет $x+yi$ КЧ $\dot{A}=15+2i$ по комплексному модулю $\dot{m}=3+2i$ ($a=15,\ b=2;\ p=3,\ q=2;\ N=p^2+q^2=13$).

Определим значения Γ и Γ' (формула (9))

$$\Gamma=(15\cdot 3+2\cdot 2)\bmod 13=49(\bmod 13)=10\,;$$

$$\Gamma'=(2\cdot 3-15\cdot 2)\bmod 13=(-24)\bmod 13=(-11)\bmod 13=2\,.$$

Наименьший вычет $x+yi$ определяется в соответствии с формулой (10)

$$x+yi=\frac{10\cdot 3-2\cdot 2}{13}+\frac{2\cdot 3+10\cdot 2}{13}i=2+2i\,.$$

Отметим, что исходя из соотношений (9), между значениями Γ и Γ' существует аналитическая зависимость. Установим данную зависимость, необходимую для использования ее при определения наименьшего вычета $x+yi$ КЧ $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$. Для этого умножим первое сравнение (11) на p, а второе на число q. Получим следующую совокупность сравнений

$$\Gamma\cdot p\equiv p\cdot(x\cdot p+y\cdot q)\bmod(p^2+q^2)\,,$$
$$\Gamma'\cdot q\equiv q\cdot(y\cdot p-x\cdot q)\bmod(p^2+q^2).$$

После этого производим вычитание второго сравнения из первого

$$(\Gamma\cdot p-\Gamma'\cdot q)\equiv\left[p\cdot(x\cdot p+y\cdot q)-q\cdot(y\cdot p-x\cdot q)\right]\bmod(p^2+q^2)\,.$$

Получим следующее сравнение

$$(\Gamma\cdot p-\Gamma'\cdot q)\equiv(p^2\cdot x+p\cdot y\cdot q-q\cdot y\cdot p+q^2\cdot x)\bmod(p^2+q^2)$$

или

$$x\cdot(p^2+q^2)\equiv(\Gamma\cdot p-\Gamma'\cdot q)\bmod(p^2+q^2)\,.$$

В итоге имеем, что

$$\Gamma'\cdot q\equiv\Gamma\cdot p\bmod(p^2+q^2)\,. \qquad (12)$$

В [3] показано, что если p и q – взаимно простые числа (НОД $(\mathrm{p,q})=1$), то сравнение (12) имеет одно решение:

$$\Gamma'\equiv t\cdot\Gamma\bmod N\,, \qquad (13)$$

где $t=\frac{p+z\cdot(p^2+q^2)}{q}$, причем z таково, что $t<N$ – целое число, меньшее значения нормы N. Величина t определяется подбором (перебором) соответствующего значения z.

Метод определения наименьшего комплексного вычета $x+iy$ комплексного числа $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$ состоит в определении значения (10), путем реализации совокупности операций при решении сравнений (11).

Пример 9. Определить все возможные пары значений Γ и Γ' при модуле $\dot{m}=p+qi=1+2i$. Определить значения Γ' из сравнения $\Gamma'\equiv(t\cdot\Gamma)\bmod N$ для $\dot{m}=p+qi=1+2i$ (формула (13)).

В этом случае $t=\frac{p+z\cdot N}{q}$, при этом $z<N$ – целое число. Для данного модуля $\dot{m}=p+qi=1+2i$ имеем, что

$$t=\frac{p+z\cdot(p^2+q^2)}{q}=\frac{1+z\cdot(1+4)}{2}=\frac{1+z\cdot 5}{2}=\frac{1+1\cdot 5}{2}=3.$$

Очевидно, что значение t будет целым числом в случае, когда $z=1$, т.е. в этом случае $t=3$. Рассчитанные значения Γ и Γ' даны в табл. 1.

Таблица 1

Γ	$\Gamma'\equiv(3\cdot\Gamma)\bmod 5$ $(t=3)$	Γ	$\Gamma'\equiv(3\cdot\Gamma)\bmod 5$ $(t=3)$
0	0	3	4
1	3	4	2
2	1	–	–

В соответствии с полученными результатами и на основании выражения (10) определим наименьшие комплексные вычеты $x+yi$ КЧ $a+bi$ по комплексному модулю $\dot{m}=1+2i$ (где $\Gamma=\overline{1,N-1}$).

$\Gamma=0;\ \Gamma'=0.\ x+yi=\frac{0}{5}+\frac{0}{5}=0+0i=0;$

$\Gamma=1;\ \Gamma'=3.\ x+yi=\frac{1\cdot 1-3\cdot 2}{5}+\frac{3\cdot 1+1\cdot 2}{5}i=-1+i;$

$\Gamma=2;\ \Gamma'=1.\ x+yi=\frac{2\cdot 1-1\cdot 2}{5}+\frac{1\cdot 1+2\cdot 2}{5}i=i;$

$\Gamma=3;\ \Gamma'=4.\ x+yi=\frac{3\cdot 1-4\cdot 2}{5}+\frac{4\cdot 1+3\cdot 2}{5}i=-1+2i;$

$\Gamma=4;\ \Gamma'=2.\ x+yi=\frac{4\cdot 1-2\cdot 2}{5}+\frac{2\cdot 1+4\cdot 2}{5}i=2i.$

В табл. 2 представлена совокупность наименьших комплексных вычетов по модулю $\dot{m}=1+2i$.

Таблица 2

Γ	Γ'	x	y	Наименьшие вычеты x+yi
0	0	0	0	0
1	3	-1	1	-1+i
2	1	0	1	i
3	4	-1	2	-1+2i
4	2	0	2	2i

Пример 10. Определить все возможные пары значений Γ и Γ' для модуля $\dot{m}=p+qi=3+4i$. $N=3^2+4^2=25$. Так как НОД (3, 4)=1, то в данном случае имеем, что

$$t=\frac{p+z\cdot N}{q}=\frac{3+1\cdot 25}{4}=7.$$

В соответствии с (13), имеем $\Gamma'\equiv 7\cdot\Gamma(\bmod 25)$, что и определяет возможные пары чисел Γ и Γ' (табл. 3).

Таблица 3

Г	$\Gamma' \equiv (7 \cdot \Gamma) \bmod 25$	Г	$\Gamma' \equiv (7 \cdot \Gamma) \bmod 25$	Г	$\Gamma' \equiv (7 \cdot \Gamma) \bmod 25$
0	0	9	13	18	1
1	7	10	20	19	8
2	14	11	2	20	15
3	21	12	9	21	22
4	3	13	16	22	4
5	10	14	23	23	11
6	17	15	5	24	18
7	24	16	12	–	–
8	6	17	19	–	–

Метод определения вещественного вычета h целого комплексного числа $\dot{A} = a + bi$ по комплексному модулю $\dot{m} = p + qi$

В СОК есть возможность представить комплексные числа в образе их вещественных вычетов, т.е. установить изоморфизм между комплексными и вещественными вычетами чисел. Это дает возможность заменить арифметические операции над целыми гауссовыми числами аналогичными операциями над системой вещественных чисел по вещественным модулям, равным нормам выбранных комплексных оснований СОК. В этом аспекте существует такая актуальная задача, как преобразование остатков числа в СОК из комплексной числовой области в вещественную числовую область. Данная задача преобразования числа в СОК из комплексной числовой области в вещественную область решается путем использования результатов первой фундаментальной теореме Гаусса.

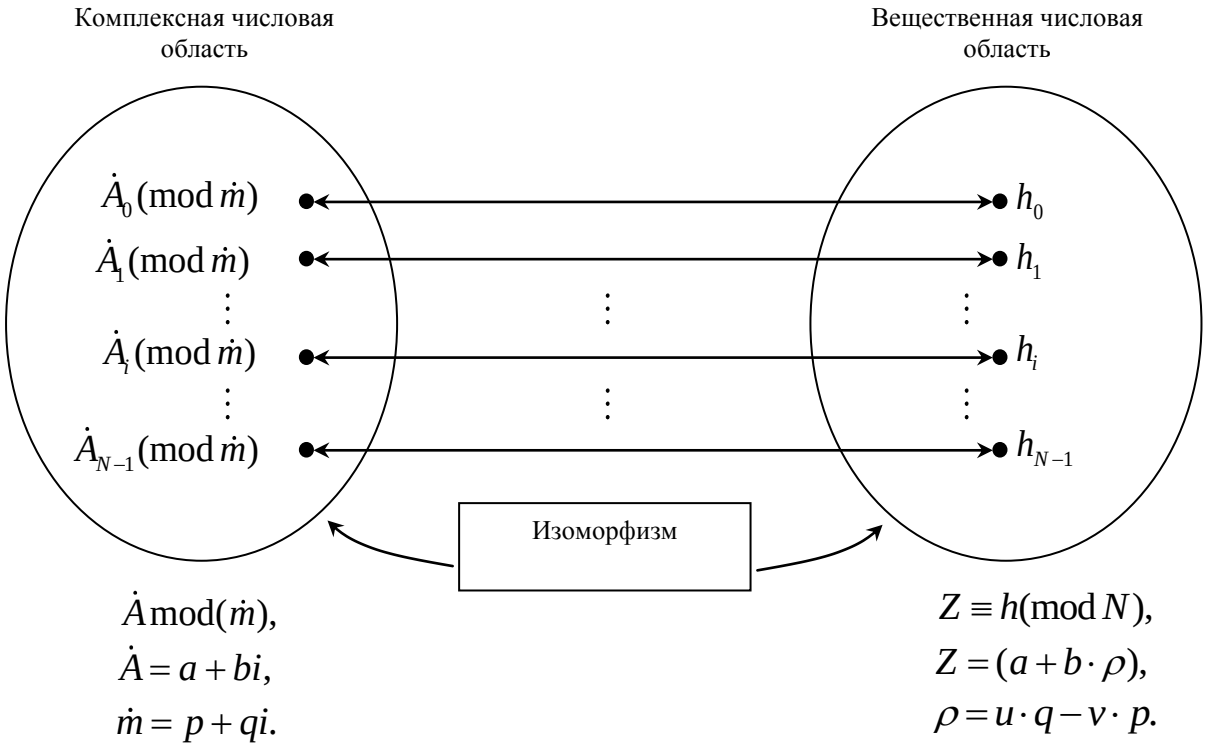
Первая фундаментальная теорема Гаусса

Здесь мы подошли к одному из наиболее интересных и важных вопросов теории целых комплексных чисел – к определению класса наименьших вычетов и связанной с этим первой фундаментальной теоремой Гаусса об изоморфизме между множеством вещественных и комплексных вычетов чисел.

Изложенный материал подводит к первой фундаментальной теореме Гаусса. Теорема 3 устанавливает изоморфизм между комплексными и вещественными вычетами.

Теорема 3. По заданному комплексному модулю $\dot{m} = p + qi$, норма N которого равна $N = p^2 + q^2$ и для которого p и q являются взаимно простыми числами, каждое целое КЧ $\dot{A} = a + bi$ по комплексному модулю $\dot{m}$ сравнимо с одним и только одним вещественным вычетом из ряда чисел $\overline{0, N-1}$, т.е. имеем, что $\dot{A} \equiv h(\bmod \dot{m})$.

На рисунке представлена схема соответствия произвольного комплексного вычета $\dot{A} \ (\bmod \dot{m})$ вещественному h вычету $\mathrm{Z} \equiv h(\bmod N)$.



Доказательство. Из теории чисел известно, что для двух взаимно простых чисел p и q можно найти такие два целых числа u и v, что выполняется условие

$$u \cdot p + v \cdot q = 1. \tag{14}$$

Покажем справедливость следующего тождества:

$$i = u \cdot p - v \cdot q + \dot{m} \cdot (v + ui). \tag{15}$$

Действительно

$$\begin{aligned} i &= u \cdot q - v \cdot p + (p + q \cdot i) \cdot (v + u \cdot i) = \\ &= u \cdot q - v \cdot p + (p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i + q \cdot u \cdot i^2) = \\ &= u \cdot q - v \cdot p + (p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i - q \cdot u) = \\ &= u \cdot q - q \cdot u - v \cdot p + p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i = \\ &= (u \cdot p + v \cdot q) \cdot i. \end{aligned}$$

С учетом выражения (14) имеем, что $i = i$. Таким образом тождество (15) справедливо.
Пусть дано КЧ $\dot{A} = a + bi$. Тогда с учетом (15) получим

$$\begin{aligned} a + bi &= a + b \cdot [u \cdot q - v \cdot p + \dot{m} \cdot (v + ui)] = \\ &= a + (u \cdot q - v \cdot p) \cdot b + \dot{m} \cdot (v \cdot b + u \cdot bi)]. \end{aligned} \tag{16}$$

Обозначим через h наименьший положительный вещественный вычет числа $a + (u \cdot q - v \cdot p) \cdot b$ по модулю N, т.е.

$$h \equiv [a + (u \cdot q - v \cdot p) \cdot b] \mathrm{mod}\, N. \tag{17}$$

Запишем выражение (17) в виде равенства

$$a + (u \cdot q - v \cdot p) \cdot b = h + s \cdot N. \tag{18}$$

Или запишем равенство (18) в виде

$$h + s \cdot N = h + s(p + qi) \cdot (p - qi) = h + \dot{m} \cdot (p \cdot s - q \cdot si). \tag{19}$$

Тогда, с учетом (16), будет выполняться равенство

$$a+bi = h+\dot{m}\cdot(p\cdot s-q\cdot si)+\dot{m}\cdot(v\cdot b+u\cdot bi) = \\ = h+\dot{m}\cdot\left[p\cdot s+v\cdot b+(u\cdot b-q\cdot s)i\right],$$

или в форме сравнения

$$(a+bi)\equiv h(\mathrm{mod}\,\dot{m}).$$

Таким образом, доказано, что наименьший комплексный вычет $x+yi$ КЧ $a+bi$ сравним по модулю m с одним и только одним из вещественных чисел $0, 1, 2, ..., N-1$.

Докажем, методом от противного, что это вещественное число единственное. Допустим, что имеются два сравнения:

$$(a+bi)\equiv h_1(\mathrm{mod}\,\dot{m}),$$
$$(a+bi)\equiv h_2(\mathrm{mod}\,\dot{m}).$$

На основании свойства сравнений имеем

$$h_1\equiv h_2(\mathrm{mod}\,\dot{m})$$

или

$$(h_1-h_2)\equiv 0(\mathrm{mod}\,\dot{m}),$$

т. е. $(h_1-h_2)=\dot{m}\cdot(e+f\cdot i)$. (20)

Из (20) следует выполнение равенства ($\dot{m}=p+qi$):

$$(h_1-h_2)=(p+qi)\cdot(e+fi).$$

Умножим обе части этого равенства на величину $p-q\cdot i$. Получим, что

$$(h_1-h_2)\cdot(p-qi)=(p+qi)\cdot(p-qi)\cdot(e+fi),$$
$$(h_1-h_2)\cdot(p-qi)=(p^2+q^2)\cdot(e+fi),$$
$$(h_1-h_2)\cdot(p-qi)=N\cdot(e+fi),$$
$$(h_1-h_2)\cdot p-(h_1-h_2)\cdot qi=N\cdot e+N\cdot fi.$$

Последнее выражение эквивалентно следующим двум вещественным равенствам:

$$\begin{cases}(h_1-h_2)\cdot p=N\cdot e,\\(h_1-h_2)\cdot q=-N\cdot f.\end{cases} \quad (21)$$

Так как КЧ равны между собой, то равны и их вещественные и мнимые части. Умножив первое равенство (21) на u и второе – на v и потом сложим их. Получим

$$(h_1-h_2)\cdot(u\cdot p+v\cdot q)=N\cdot(e\cdot u-f\cdot v).$$

Принимая во внимание выражение (14) ($u\cdot p+v\cdot q=1$) следует, что

$$(h_1-h_2)\equiv N\cdot(e\cdot u-f\cdot v),$$

или

$$(h_1-h_2)\equiv 0(\mathrm{mod}\,N). \quad (22)$$

Так как по предположению $h_1, h_2 < N$, то сравнение (22) возможно только в случае $h_1=h_2$. Таким образом, исключается возможность существования двух различных чисел h_1 и h_2, меньших N, которые были бы сравнимы с числом $a+bi$ по модулю $\dot{m}$. Имеется только одно такое h число, которое определяется из сравнения (17) и представляется в виде сравнения

$$[a+(u\cdot q-v\cdot p)\cdot b]\equiv h(\mathrm{mod}\,N). \qquad (23)$$

При этом используется обозначение $\mathrm{Z}=(a+b\cdot\rho)$, где выражение $\rho=u\cdot q-v\cdot p$, посредством которого устанавливается соответствие между комплексным и вещественным вычетом по модулю $\dot{m}=p+qi$, называется коэффициентом изоморфизма (КИ). В этом случае выражение (23) представится в виде

$$\mathrm{Z}\equiv h(\mathrm{mod}\,N). \qquad (24)$$

На основании данных табл. 2 по формулам (23) и (24) определим значения вещественных вычетов $Z_i\equiv h_i(\mathrm{mod}\,N)$ $(i=\overline{0,N-1})$, соответствующих наименьшим комплексным вычетам $x+yi$ по модулю $\dot{m}=1+2i$. Вначале определим значение коэффициента изоморфизма $\rho=u\cdot q-v\cdot p=u\cdot 2-v\cdot 1$. Значения u и v определяются из известного в теории чисел соотношения $u\cdot p+v\cdot q=1$, т.е. $u\cdot 1+v\cdot 2=1$. Путем подбора (перебора) определяем, что $u=-1$, а $q=1$. Таким образом, $\rho=(-1)\cdot 2-1\cdot 1=-3$, или $(-3)\,\mathrm{mod}\,5=2$ $(N=p^2+q^2=1^2+2^2=5)$.

Определим исходные значения наименьших вещественных вычетов h_i, изоморфных наименьшим комплексным вычетам, представленных в табл. 2.

Для $\dot{A}=0+0i$. $Z_0=a+b\rho=0+0\cdot\rho=0$. $h_0\equiv 0(\mathrm{mod}\,5)$.

Для $\dot{A}=-1+i$. $Z_1=-1+1\cdot(-3)=-4$. $h_1\equiv 1(\mathrm{mod}\,5)$.

Для $\dot{A}=i$. $Z_2=0+1\cdot(-3)=-3$. $h_2\equiv 2(\mathrm{mod}\,5)$.

Для $\dot{A}=-1+2\cdot i$. $Z_3=-1+2\cdot(-3)=-1-6=-7$. $h_3\equiv 3(\mathrm{mod}\,5)$.

Для $\dot{A}=2\cdot i$. $Z_4=0+2\cdot(-3)=-6$. $h_3\equiv 4(\mathrm{mod}\,5)$.

Результаты вычислений наименьших вещественных значений остатков (вычетов) h_i сведены в табл. 4.

Таблица 4

Наименьшие комплексные вычеты x+yi	КИ	Значение $Z_i=a+b\cdot\rho$	Вещественные вычеты $h_i(Z_i\equiv h_i(modN);\ i=\overline{0,N-1}$
0	2	0	0
-1+i	2	-4	1
i	2	-3	2
-1+2i	2	-7	3
2i	2	-6	4

На основе результатов теоремы Гаусса нетрудно показать следующее соотношения между наименьшими комплексными и вещественными вычетами. Пусть для двух чисел $\dot{A}_1=a_1+b_1i$ и $\dot{A}_2=a_2+b_2i$ существуют такие значения чисел h_1 и h_2, $h_\pm$ и $h_\times$, что если $\dot{A}_1\equiv h_1(\mathrm{mod}\,\dot{m})$ и $\dot{A}_2\equiv h_2(\mathrm{mod}\,\dot{m})$, то выполняются соотношения $\dot{A}_1\pm\dot{A}_2\equiv h_\pm(\mathrm{mod}\,\dot{m})$ и $\dot{A}_1\cdot\dot{A}_2\equiv h_\times(\mathrm{mod}\,\dot{m})$. Тогда $h_\pm\equiv(h_1\pm h_2)\,\mathrm{mod}\,N$ и $h_\times\equiv(h_1\cdot h_2)\,\mathrm{mod}\,N$, где $N=p^2+q^2$.

Приведем примеры решения сравнений в комплексной области, т.е. примеры определение наименьших вещественных вычетов h комплексных чисел $\dot{A}=a+bi$ по комплексным модулям $\dot{m}=p+qi$.

Пример 11. Решить сравнение $(16+7i)\equiv h\,\mathrm{mod}(5+2i)$. Т.е. необходимо найти наименьший вещественный вычет h комплексного числа $16+7i$ по комплексному модулю $5+2i$.

Поскольку НОД $(5,2)=1$, то условие первой фундаментальной теоремы Гаусса выполня-

ется, следовательно, существует полная система вещественных вычетов по модулю $N = p^2 + q^2 = 5^2 + 2^2 = 29$. Вещественный вычет h определяется из сравнения (24), т.е.

$$(16 + 7 \cdot \rho) \equiv h (\mathrm{mod}\, 29).$$

Коэффициент изоморфизма $\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 5$. Значения u и v определяются из условия равенства (14) подбором значений u, v. Определили, что $u = 1$ и $v = -2$. Проверка соотношения (14) показала, что $1 \cdot 5 + (-2) \cdot 2 = 5 - 4 = 1$.

В этом случае КИ $\rho = 1 \cdot 2 - (-2) \cdot 5 = 2 + 10 = 12$. Поэтому $Z = 16 + 7 \cdot \rho = 16 + 7 \cdot 12 = 100$. Решим сравнение $100 \equiv h (\mathrm{mod}\, 29)$ и получим $h \equiv 13 (\mathrm{mod}\, 29)$. В общем виде можно записать, что $16 + 7i \equiv 13 \mathrm{mod}(5 + 2i)$.

Пример 12. Решить сравнение $(1 + i) \equiv h \,\mathrm{mod}(1 + 2i)$. Или, необходимо найти наименьший вещественный вычет h комплексного числа $1 + i$ по комплексному модулю $1 + 2i$.

В этом случае НОД $(p, q) = (1, 2) = 1$. $N = p^2 + q^2 = 1 + 2^2 = 5$. $\dot{A} \equiv h (\mathrm{mod}\, \dot{m})$. $h \equiv (a + b \cdot \rho) \bmod N$.

Значение КИ $\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 1$, а значения u и v определяются из соотношения (14)

$$u \cdot p + v \cdot q = 1, \qquad u \cdot 1 + v \cdot 2 = 1, \text{ т.е.} \qquad u = -1,\ v = 1.$$

Таким образом $\rho = (-1) \cdot 2 - 1 \cdot 1 = -2 - 1 = -3$.

$$h = 1 + 1 \cdot 2 = 3.$$
$$x + yi = 4 + 2i \;\square\; h = 3,$$
$$\text{т.е. } (1 + i) \equiv 3 \mathrm{mod}(1 + 2i).$$

Рассмотрим примеры 13 и 14 определения комплексного и вещественного вычетов целого комплексного числа по комплексному модулю $\dot{m} = 1 + 2i$ с контролем правильности решения задачи. Исходные данные для контроля представлены в табл. 5.

Таблица 5

Г	$\Gamma' = 3 \cdot \Gamma (\mathrm{mod}\, 5)$, $(t = 3)$	Наименьшие комплексные вычеты $x + yi$ по комплексному модулю $\dot{m} = 1 + 2i$ комплексного числа $\dot{A} = a + bi$	Вещественные вычеты h по модулю $N = p^2 + q^2 = 5$
0	0	$0 + 0i$	0
1	3	$-1 + i$	1
2	1	i	2
3	4	$-1 + 2i$	3
4	2	$2i$	4

Пример 13А. Определить комплексный вычет $x + yi$ КЧ $\dot{A} = 1 + i$ по комплексному модулю $\dot{m} = 1 + 2i$, т.е. найти $\dot{A} \equiv (x + yi) \bmod \dot{m}$ ($a = 1$, $b = 1$; $p = 1$, $q = 2$; $N = 5$). По формуле (4) имеем, что

$$\begin{cases} (1 \cdot 1 + 1 \cdot 2) \equiv (x \cdot 1 + y \cdot 2) \bmod 5, \\ (1 \cdot 1 - 1 \cdot 2) \equiv (y \cdot 1 - x \cdot 2) \bmod 5. \end{cases}$$

$$\begin{cases} 3 = x + 2y, \\ -1 = -2x + y. \end{cases}$$

$$x = 3 - 2y,$$
$$-1 = -2 \cdot (3 - 2y) + y,$$
$$-1 = -6 + 4y + y,$$
$$5y = 5,$$
$$y = 1.$$
$$x = 3 - 2y = 3 - 2 = 1;\ x = 1.$$

Ответ: комплексный вычет $x+yi$ КЧ $\dot{A}=1+i$ по комплексному модулю $\dot{m}=1+2i$ равен комплексному числу $x+yi=1+i$.

Пример 13Б. Определить наименьший вычет $x+yi$ КЧ $\dot{A}=1+i$ по комплексному модулю $\dot{m}=1+2i$, т.е. определить значение $1+i\equiv(x+yi)\bmod(1+2i)$ ($a=1$, $b=1$; $p=1$, $q=2$; $N=5$). По формуле (10) имеем, что

$$\Gamma=(1\cdot1+1\cdot2)\bmod5=3;\ \Gamma'=(1\cdot1-1\cdot2)\bmod5=(-1)\bmod5=4.$$

$$x+yi=\frac{3\cdot1-4\cdot2}{5}+\frac{4\cdot1+3\cdot2}{5}i=-\frac{5}{5}+\frac{10}{5}i=-1+2i.$$

Таким образом, наименьший вычет $x+yi$ КЧ $\dot{A}=1+i$ по комплексному модулю $\dot{m}=1+2i$ равен значению $x+yi=-1+2i$. Это решение можно представить в виде $(1+i)\equiv(-1+2i)\bmod(1+2i)$.

Пример 13В. Решить сравнение $\dot{A}\equiv h\bmod\dot{m}$ вида $(1+i)\equiv h\bmod(1+2i)$ ($a=1$, $b=1$; $p=1$, $q=2$; $N=5$), формулы (14), (23), (24))

$$u\cdot p+v\cdot q=1,\ u=-1,$$
$$u\cdot1+v\cdot2=1.\ v=1.$$
$$\rho=u\cdot q-v\cdot p.$$
$$Z=a+b\cdot\rho,$$
$$Z\equiv h\bmod N.$$
$$\rho=(-1)\cdot2-1\cdot1=-2-1=-3.$$
$$Z=1+1\cdot(-3)=-2.$$
$$\mathrm{h}\equiv(-2)\bmod5=3.$$

Таким образом, вещественный вычет h КЧ $\dot{A}=1+i$ по комплексному модулю $\dot{m}=1+2i$ равен величине $h=3$.

Проверка. Проведем проверку полученных результатов. В примере 13Б получили наименьший комплексный вычет $(-1+2i)$, а в примере 13В получим вещественный вычет $h=3$. В соответствии с данными табл. 5 имеем, что $(-1+2i)\sim3$. Что и требовалось показать.

Пример 14А. Определить комплексный вычет $x+yi$ КЧ $\dot{A}=3+4i$ по комплексному модулю $\dot{m}=1+2i$. $N=p^2+q^2=1^2+2^2=5$.

В соответствии с выражением (4) составим систему сравнений в виде

$$\begin{cases}(3\cdot1+4\cdot2)\equiv(x\cdot1+y\cdot2)\bmod5,\\(4\cdot1-3\cdot2)\equiv(y\cdot1-x\cdot2)\bmod5.\end{cases}$$

Или

$$\begin{cases}11\equiv(x+2y)\bmod5,\\(-2)\equiv(-2x+y)\bmod5.\end{cases}$$

На основании системы сравнений составим систему из двух линейных уравнений

$$\begin{cases}x+2y=11,\\-2x+y=+3,\end{cases}$$

так, как $(-2)=3\bmod5$.

$$x=11-2y,$$
$$-2\cdot(11-2\cdot y)+y=3,$$
$$-22+4y+y=3,$$
$$5y=25,$$
$$y=5.$$

$$x = 11 - 2y = 11 - 10 = 1.$$

Таким образом, имеем, что комплексный вычет $x + yi$ КЧ $\dot{A} = 3 + 4i$ по комплексному модулю $\dot{m} = 1 + 2i$ равен значению $x + yi = 1 + 5i$.

Пример 14Б. Определить наименьший комплексный вычет $x + yi$ КЧ $\dot{A} = 3 + 4i$ по комплексному модулю $\dot{m} = 1 + 2i$. $N = 5$.

В соответствии с выражением (10) имеем, что наименьший комплексный вычет равен значению

$$(x + yi) = \frac{\Gamma \cdot p - \Gamma' \cdot q}{N} + \frac{\Gamma' \cdot p + \Gamma \cdot q}{N} i.$$

Предварительно определим значения Γ и Γ' (см. формулы (9)):

$$\Gamma = (a \cdot p + b \cdot q) \bmod N = (3 \cdot 1 + 4 \cdot 2) \bmod 5 = 11 (\bmod 5) = 1;$$
$$\Gamma' = (b \cdot p - a \cdot q) \bmod N = (4 \cdot 1 - 3 \cdot 2) \bmod 5 = (-2) \bmod 5 = 3.$$

В этом случае имеем, что

$$(x + yi) = \frac{1 \cdot 1 - 3 \cdot 2}{5} + \frac{3 \cdot 1 + 1 \cdot 2}{5} = -\frac{5}{5} + \frac{5}{5} = -1 + i.$$

Таким образом, наименьший комплексный вычет $x + yi$ КЧ $\dot{A} = 3 + 4i$ по комплексному модулю $\dot{m} = 1 + 2i$ равен значению $-1 + i$.

Пример 14В. Определить вещественный вычет h КЧ $\dot{A} = 3 + 4i$ по модулю $\dot{m} = 1 + 2i$. $N = 5$. Или можно сформулировать задачу следующим образом. Решить сравнение вида $(3 + 4i) \equiv h \bmod (1 + 2i)$.

В соответствии с выражением (24) имеем, что $(a + b\rho) \equiv h (\bmod N)$, где КИ $\rho = u \cdot q - v \cdot p$. На основе формулы (14) определим значения u и v

$$u \cdot p + v \cdot q = 1 \text{ или } u \cdot 1 + v \cdot 2 = 1.$$

Так, при значениях $u = -1$ и $v = 1$ выполните условие (14), т.е. $(-1) \cdot 1 + 1 \cdot 2 = 1$.

На основании расчетов получим, что $\rho = u \cdot q - v \cdot p = (-1) \cdot 2 - 1 \cdot 1 = -3$.

$$\mathrm{Z} = (a + b \cdot \rho) = 3 + 4 \cdot (-3) = -9.$$

Имеем $(a + b\rho) \equiv h (\bmod N)$ или $(-9) \equiv 1 (\bmod 5)$. Т.е. $h = 1$.

Таким образом, имеем решение сравнения в виде $(3 + 4i) \equiv 1 \bmod (1 + 2i)$.

Проверка. В примере 14Б получили наименьший комплексный вычет $(-1 + i)$, а в примере 14В получим вещественный вычет $h = 1$. В соответствии с данными табл. 5 имеем, что $(-1 + i) \sim 1$. Что и требовалось показать.

Выводы

Рассмотрены методы:

- определения комплексного вычета целого комплексного числа по комплексному модулю;
- определения наименьшего комплексного вычета целого комплексного числа по комплексному модулю;
- определения вещественного вычета целого комплексного числа по комплексному модулю, основанный на использование результатов первой фундаментальной теоремы Гаусса.

Приведены конкретные примеры определения вычетов целочисленных данных в комплексной числовой области. На основании представленных методов разработано устройство для их технической реализации [20]. На устройство получен патент Украины на изобретение,

что подтверждает новизну и практическую ценность результатов исследований. Выводы и результаты, полученные в статье, целесообразно использовать при реализации задач и алгоритмов в СОК для комплексной числовой области. Использование представленных методов способствует повышению эффективности использования СОК для быстрой реализации целочисленных операций в комплексной числовой области.

Список литературы: 1. *Синтез* и анализ параллельных процессов в адаптивных времяпараметризованных вычислительных системах / Г. А. Поляков, С. И. Шматков, Е. Г, Толстолужская, Д. А. Толстолужский. – Харьков : ХНУ им. В. Н. Каразина, 2012. -672с. *2. Филиппенко И. Г.* Взаимодействующие нейроавтоматы и нейроавтоматно-вычислительные структуры : под ред. О. Г. Руденко. – К. : Каравелла, 2015, 440 с. *3. Акушский И. Я., Юдицкий Д. И.* Машинная арифметика в остаточных классах. – М. : Сов. радио, 1968. – 440 с. *4. Krasnobayev V. A., Koshman S. A., Mavrina M. A.* A method for increasing the reliability of verification of data represented in a residue number system // Cybernetics and Systems Analysis. – November 2014. – Volume 50, Issue 6, pp 969-976. 5. *Krasnobayev V. A., Yanko A. S., Koshman S.* A. A Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. – January 2016. – Volume 52, Issue 1, pp. 145-150. *6. Карл Фридрих Гаусс.* Труды по теории чисел. – М. : Академия наук СССР, 1959. – 979 с. 7. *Применение* гиперкомплексных чисел в теории инерциальной навигации. Автономные системы / Онищенко С. М. – Киев : Наук. думка, 1983. - 208с. 8. *ДП* на корисну модель № 33672 України, МПК G 06 F 7/49 (2008.01) / Кошман С.О., Сіора О.А., Хері Алі Абдуллах, Краснобаєв В.А. Пристрій для множення комплексних чисел у модулярній системі числення; № u 2008 01356. Заявл. 04.02.2008. Опубл. 10.07.2008, Бюл. № 13. – 8с. 9. *ДП* на корисну модель № 40905 України, МПК G 06 F 7/00 (2009) / Кошман С.О., Барсов В.І., Сіора О.А., Краснобаєв В.А. Пристрій для піднесення комплексних чисел в квадрат за комплексним модулем у модулярній системі числення. № u 2008 14308. Заявл. 12.12.2008. Опубл. 27.04.2009, Бюл. № 8.-5с. 10. *ДП* на корисну модель № 33672 України, МПК G 06 F 7/49 (2008.01) / Кошман С.О., Сіора О.А., Хері Алі Абдуллах, Краснобаєв В.А. Пристрій для множення комплексних чисел у модулярній системі числення; № u 2008 01356. Заявл. 04.02.2008. Опубл. 10.07.2008, Бюл. № 13.-8с. 11.*Kuznetsov, O., Gorbenko, Y., Kolovanova, I.* Combinatorial properties of block symmetric ciphers key schedule. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 55-58. DOI: 10.1109/INFOCOMMST.2016.7905334. 12. *Kuznetsov, O., Lutsenko, M., Ivanenko, D.* Strumok stream cipher: Specification and basic properties // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 59-62. DOI: 10.1109/INFOCOMMST.2016.7905335. 13. *Kuznetsov, A.A., Smirnov, A.A., Danilenko, D.A., Berezovsky, A.* The statistical analysis of a network traffic for the intrusion detection and prevention systems // Telecommunications and Radio Engineering. – Volume 74, 2015, Issue 1, pages 61-78. DOI: 10.1615/TelecomRadEng.v74.i1.60. *Karpenko O., Kuznetsov A., Sai V., Stasev Yu.* Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. – Volume 71, 2012 Issue 1. pages 91-98. DOI: 10.1615/TelecomRadEng.v71.i1.100. 14. *Yuriy Izbenko, Vladislav Kovtun, Alexandr Kuznetsov.* The design of boolean functions by modified hill climbing method // Information technology – New Generation, 2009. ITNG'2009. Proceedings of the 6th International Conference on Information Technology: New Generations, April 27-29, Las Vegas, Nevada, USA., pp: 356-361. DOI: 10.1007/s10559-007-0052-8. 15. *Naumenko, N.I., Stasev, Yu.V., Kuznetsov, A.A.* Methods of synthesis of signals with prescribed properties // Cybernetics and Systems Analysis, Volume 43, Issue 3, May 2007, Pages 321-326. DOI: 10.1007/s10559-007-0052-8. *Stasev Yu.V., Kuznetsov A.A., Nosik A.M.* Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1 – 11. DOI: 10.1007/s10559-007-0021-2. 16. *Stasev Yu. V., Kuznetsov A.A.* Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes // Cybernetics and Systems Analysis, Volume 41, Issue 3, May 2005, Pages 354 – 363. DOI: 10.1007/s10559-005-0069-9. 17. *I. D. Gorbenko, A. G. Kachko, K. A. Pogrebnyak, L. V. Makutonin* Analysis, assessment and proposals regarding the method for generation of system parameters in ntru-like asymmetric systems // Telecommunications and Radio Engineering, Volume 76, 2017, p. 511-520. DOI: 10.1615/ TelecomRadEng.v76.i6.50. 18. *T. O. Grinenko, O. P. Narezhniy, I. D. Gorbenko* Methods for measuring the noise power spectral density of the random number generator quantum radio optical system // Telecommunications and Radio Engineering, Volume 76, 2017, pages 635-651 DOI: 10.1615/TelecomRadEng.v76.i7.60. 19. *Gorbenko I.D., Zamula A.A., Semenko Ye.A.* Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. – Volume 75, 2016 Issue 2. pages 169–178. 20. *Патент* на винахід № 114063, Україна, МПК G 06 F 7/72 (2006.01), H 03 M 7/18 (2006.01). Краснобаєв В. А., Горбенко І. Д., Янко А. С., Кошман С. А., Мороз С. О., Горбенко Ю. І Пристрій для визначення лишків дійсних та комплексних чисел у системі залишкових класів. № a 2016 06697. Заявл. 21.06.2016. Опубл. 10.04.2017, Бюл. № 7. – 7с.

Харьковский национальный
университет имени В.Н.Каразина

Поступила в редколлегию 11.12.2017