О ПРЕДСТАВЛЕНИИ ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ В СИСТЕМЕ СЧИСЛЕНИЯ ПИТТИ

Богданов П.С.
Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет)

Аннотация

В работе рассматривается алгоритм представления целых гауссовых чисел в канонической системе счисления с основанием $\alpha = i - 1$, основанный на делении с остатком, синтезируются алгоритмы реализации основных арифметических операций над числами в рассматриваемой системе счисления.

Ключевые слова: каноническая система счисления, деление с остатком по норме.

Введение

Решение разнообразных задач цифровой обработки сигналов, распознавания образов, машинного зрения, компьютерной оптики и т. д. сводится в конечном итоге к выполнению различных операций над целыми числами. «То, каким образом мы выполняем арифметические действия, тесно связано с тем, каким образом мы представляем числа, с которыми работаем» [1]. Достаточно подробные исторические обзоры возникновения и развития различных систем счисления, не всегда совпадающих с традиционными позиционными системами счисления со степенным базисом, а также непосредственного применения их к задачам информатики приведены в книге Д. Кнута [1].

Главным критерием всех алгоритмов обработки информации является скорость их выполнения, которая также в значительной степени определяется выбором системы счисления. При этом важную роль играет способ представления числа в выбранной системе счисления. Хорошо известен алгоритм определения представления целых элементов квадратичных полей в так называемых «канонических» системах счисления, основанный на рекуррентных соотношениях [2], однако для некоторых квадратичных полей реализуем и другой алгоритм – алгоритм деления с остатком по норме. Существует лишь конечное множество квадратичных полей, в которых возможна реализация указанного алгоритма. Дополнительную привлекательность такому подходу придаёт «вариабельность» множества цифр в разложении числа в системах счисления с комплексным основанием, что, например, обеспечивает дополнительную криптостойкость системы кодирования по методу работы [3] или новые алгоритмы параллельного вычисления произведения больших целых чисел методом, описанным в монографии [4].

В настоящей работе рассматриваются основные конструктивные особенности такого подхода на примере кольца целых гауссовых чисел и бинарной системы счисления с основанием $\alpha = i - 1$.

1. Основные определения

Определение 1. Пусть $Q(\sqrt{d})$ есть квадратичное поле [1]:

$$Q(\sqrt{d}) = \left\{ z = a + b\sqrt{d};\ a, b \in Q \right\},$$

где d – целое число, свободное от квадратов, то есть не делящееся на неединичный квадрат целого числа. Если для элемента $z = a + b\sqrt{d} \in Q(\sqrt{d})$ его норма и след есть целые числа:

$$\mathrm{Norm}(z) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in Z,$$
$$\mathrm{Tr}(z) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in Z,$$

то этот элемент называется целым алгебраическим числом поля $Q(\sqrt{d})$, в отличие от «обычных» целых чисел, которые называются целыми рациональными числами [4].

Определение 2. Целое алгебраическое число $\alpha = A \pm \sqrt{d}$ называется основанием канонической системы счисления в кольце $Z\left(\sqrt{d}\right)$ целых элементов поля $Q(\sqrt{d})$, если любой целый элемент этого поля однозначно представим в форме конечной суммы

$$z = \sum_{j=0}^{k(z)} a_j \alpha^j,$$
$$a_j \in I = \left\{0, 1, ..., \left|\mathrm{Norm}(\alpha)\right| - 1\right\}.$$

Пара $\{\alpha, I\}$ называется канонической системой счисления в кольце $Z\left(\sqrt{d}\right)$, а I – алфавитом этой системы [4].

Известен алгоритм представления целых чисел в канонических системах счисления с основанием $\alpha = A + \sqrt{d}$, основанный на рекуррентных соотношениях [2], а именно при $d < 0, d \equiv 2, 3 \pmod 4$ для целого рационального числа $z = z_1 + z_2\sqrt{d}$ цифры $a_k(z)$ его представления

$$z = \sum_{k=0}^{n(z)} a_k(z) \cdot \alpha^k$$

вычисляются рекуррентно:

$$s_{k+1}(z) = 2A \cdot \left[\frac{s_k(z)}{\mathrm{Norm}(\alpha)}\right] - \left[\frac{s_{k-1}(z)}{\mathrm{Norm}(\alpha)}\right], \quad k \geq 0,$$
$$s_{-1}(z) = \mp z_2 \mathrm{Norm}(\alpha),$$
$$s_0(z) = z_1 \mp z_2 A,$$
$$a_k(z) \equiv s_k(z) \left(\mathrm{mod}\, \mathrm{Norm}(\alpha)\right).$$

Для кольца целых гауссовых чисел, то есть для комплексных чисел с целыми действительной и мнимой частями, система счисления с основанием $\alpha = \pm i - 1$была введена Питти [1]. В этом случае предыдущие рекуррентные соотношения принимают вид

$$\begin{aligned} & s_{k+1}(z) = -2 \cdot \left[\frac{s_k(z)}{2} \right] - \left[\frac{s_{k-1}(z)}{2} \right], \quad k \geq 0, \\ & s_{-1}(z) = 0, \\ & s_0(z) = z, \\ & a_k(z) \equiv s_k(z) (\mathrm{mod}\, 2). \end{aligned} \tag{1}$$

2. Алгоритм деления с остатком

Кроме указанного алгоритма, основанного на рекуррентных соотношениях (1), возможно представление целых гауссовых чисел в системе счисления с основанием α с помощью алгоритма деления с остатком. Эта возможность вытекает из того, что в кольце $Z(i)$ целых гауссовых чисел из поля $Q(i) = Q(\sqrt{-1})$ имеет место деление с остатком по норме.

Определение 3. Говорят, что в кольце P имеет место алгоритм деления с остатком по норме [5], если на отличных от нуля элементах $\beta \in P$ определена функция Norm(β), принимающая целые неотрицательные значения, так, что выполняются следующие условия:

- если $\beta \neq 0$ делится на α, то $\mathrm{Norm}(\beta) \geq \mathrm{Norm}(\alpha)$;
- для любых элементов α и $\beta \neq 0$ в P существуют такие γ и r, что $\beta = \gamma \cdot \alpha + r$, причём либо $r = 0$, либо $\mathrm{Norm}(\alpha) \geq \mathrm{Norm}(r)$.

Следует отметить, что в случае алгоритма деления с остатком возможна неоднозначность представления числа в данной системе счисления за счёт варьирования множества «допустимых» цифр.

Действительно, рассматривая в качестве делителя число $\alpha = i - 1$, $\mathrm{Norm}(\alpha) = 2$, получаем, что для любого целого гауссова числа $\beta \in Z(i) \subset Q(i)$ существуют $\gamma_0, r_0 \in Z(i)$, где $\mathrm{Norm}(r_0) < \mathrm{Norm}(\alpha)$, такие, что выполняется равенство

$$\beta = \gamma_0 \cdot \alpha + r_0. \tag{2}$$

При этом числа γ_0 и r_0 определяются неоднозначно. Это обусловлено тем, что существует несколько различных остатков r_0, имеющих одну и ту же норму. Именно: при $\mathrm{Norm}(r_0) = 0$ необходимо и $r_0 = 0$, но для $\mathrm{Norm}(r_0) = 1$ $r_0 = \pm 1; \pm i$.

Решив проблему неоднозначного выбора частного γ_0 и остатка r_0, можно обосновать единственность представления числа в данной системе счисления при использовании алгоритма деления с остатком с заданным алфавитом «цифр» или отказаться от этой однозначности в задачах криптографии [3].

3. Сходимость алгоритма вычисления цифр

Нетрудно показать справедливость следующего утверждения.

Лемма 1. Если ограничиться рассмотрением всего лишь двух остатков 0 и 1 разной нормы, то представление числа $\beta = a + bi; a, b \in Z$ в виде (2) единственно, причём, если сумма $a + b$ – чётная, то $r_0 = 0$; если $a + b$ – нечётная, то $r_0 = 1$. В этом случае частное γ_0 определяется формулой

$$\gamma_0 = \frac{(\beta - r_0)\overline{\alpha}}{2}, \tag{3}$$

где $\overline{\alpha} = -i - 1$, или

$$\gamma_0 = -\frac{1}{2}\left((a - b - r_0) + i(a + b - r_0)\right). \tag{4}$$

Пусть теперь

$$\begin{aligned} & \beta = \gamma_0 \cdot \alpha + r_0; \\ & \gamma_0 = \gamma_1 \cdot \alpha + r_1; \\ & \ldots\ldots\ldots\ldots\ldots; \\ & \gamma_{n-1} = \gamma_n \cdot \alpha + r_n. \end{aligned} \tag{5}$$

Ясно, что если в формулах (5) найдется такое *n*, что $\gamma_n = 0$, то

$$\beta = r_n \alpha^n + r_{n-1} \alpha^{n-1} + \ldots + r_1 \alpha + r_0,$$

где $r_k \in \{0; 1\}$; $k = 0; 1; \ldots; n$, то есть тогда возможно единственное представление числа β в системе с основанием α и алфавитом $I = \{0; 1\}$.

Для доказательства существования такого представления сначала покажем справедливость следующего утверждения.

Лемма 2. При делении произвольного целого гауссова числа $\beta = a + bi; a, b \in Z$ на число α с остатком 0 или 1, а также при делении на α частных $\gamma_0, \gamma_1, \ldots$ из формул (5) найдётся такое значение *n*, при котором $\mathrm{Norm}(\gamma_n) \leq 1$.

Доказательство. Действительно, при $r_0 = 0$ $\mathrm{Norm}(\gamma_0) = \frac{1}{2}\mathrm{Norm}(\beta)$, то есть если $\beta \neq 0$, то норма частного γ_0 меньше нормы делимого β.

Если $r_0 = 1$, то неравенство $\mathrm{Norm}(\gamma_0) < \mathrm{Norm}(\beta)$ равносильно условию

$$(a + 1)^2 + b^2 > 2, \tag{6}$$

которое справедливо при всех $\beta \in Z(i)$, $\mathrm{Norm}(\beta) \geq 2$, кроме $\beta = -2 \pm i$ (исключительные случаи). Для этих чисел частное γ_0 от деления β на число α имеет норму $\mathrm{Norm}(\gamma_0) = \mathrm{Norm}(\beta) = 5$. Далее, с возрастанием номера *n*, норма частных убывает, и для $\beta = -2 + i$ $\mathrm{Norm}(\gamma_1) = 1$, а для $\beta = -2 - i$ $\mathrm{Norm}(\gamma_2) = 1$.

Таким образом, норма частного в неисключительных случаях всегда меньше нормы делимого, и, следовательно, через конечное число шагов она станет меньше либо равна 1. Во всех исключительных случаях показано, что через конечное число шагов норма частного также станет меньше либо равна 1. ■

Итак, найдётся такое значение n, при котором $\mathrm{Norm}(\gamma_n)=0$, следовательно, $\gamma_n=0$, либо $\mathrm{Norm}(\gamma_n)=1$, то есть $\gamma_n=\pm1;\pm i$. Для всех этих значений γ_n легко проверить, что через конечное число шагов появится частное $\gamma_m=0$. Поэтому из равенств (5) получается однозначное разложение числа β по степеням числа $\alpha=i-1$:

– для $\gamma_n=0$

$$\beta=r_n\alpha^n+r_{n-1}\alpha^{n-1}+\ldots+r_1\alpha+r_0,$$

$$r_k\in\{0;1\};\quad k=0;1;\ldots;n;$$

– для $\gamma_n=1$

$$\beta=1\cdot\alpha^{n+1}+r_n\alpha^n+r_{n-1}\alpha^{n-1}+\ldots+r_1\alpha+r_0,$$

$$r_k\in\{0;1\};\quad k=0;1;\ldots;n.$$

Из доказанных лемм непосредственно следует основная теорема.

Теорема 1. Любое целое гауссово число $\beta=a+bi;\ a,b\in Z$ можно представить единственным образом в системе счисления с основанием $\alpha=i-1$, используя для этого цифры 0 и 1.

Отсюда легко следует алгоритм записи целого гауссова числа $\beta=a+bi;\ a,b\in Z$ в системе счисления с основанием $\alpha=i-1$

1. Если сумма $a+b$ чётная, то $r_0=0$; если $a+b$ нечётная, то $r_0=1$.

2. Вычисляем γ_0 по формуле (4). Если $\gamma_0=0$, то алгоритм закончен; если $\gamma_0\neq0$ и $\mathrm{Norm}(\gamma_0)>\mathrm{Norm}(\alpha)-1$, то записывая γ_0 в виде $\gamma_0=a_0+b_0i$, переходим к пункту 1. В случае если $\gamma_0\in\{\pm1,\pm i\}$, то для представления γ_0 используем следующие формулы:

$$i=\alpha^1+\alpha^0;\ -i=\alpha^2+\alpha^1+\alpha^0;$$

$$-1=\alpha^4+\alpha^3+\alpha^2+\alpha^0.$$

Таким образом, в результате одной итерации алгоритма мы получаем запись числа $\beta=\gamma_0\cdot\alpha+r_0$. На следующей итерации вместо числа β используется γ_0.

4. Реализация арифметических операций с целыми числами в системе счисления с основанием α

Рассмотрим алгоритмы сложения и умножения целых чисел в системе счисления с основанием α.

Каждое целое рациональное число, записанное в системе счисления с основанием α, можно рассматривать как многочлен относительно α, коэффициентами которого могут быть 0 и 1.

4.1. Сложение

При сложении двух чисел в системе счисления с основанием α, иначе говоря, двух многочленов, получаем новый многочлен с коэффициентами 0, 1 или 2. При этом, поскольку $2=\alpha^3+\alpha^2=1100_\alpha$, то слагаемое вида $2\cdot\alpha^k$ преобразуется по формуле

$$2\cdot\alpha^k=\left(\alpha^3+\alpha^2\right)\cdot\alpha^k=\alpha^{k+3}+\alpha^{k+2}. \qquad (7)$$

В некоторых случаях преобразование суммы двух чисел с использованием формулы (7) приводит к многочлену бесконечно большой степени с повторяющимся блоком коэффициентов (зацикливанию).

Например:

$$\alpha^2+2\cdot\alpha+2=\alpha^2+2\cdot(\alpha+1)=$$

$$=\alpha^4+2\cdot\alpha^3+2\cdot\alpha^2=\alpha^2\left(\alpha^2+2\cdot\alpha+2\right)=$$

$$=\ldots=\alpha^{2n}\left(\alpha^2+2\cdot\alpha+2\right)=\ldots\quad n\in N.$$

Несложно убедиться, что рассмотренный многочлен равен нулю при $\alpha=i-1$, то есть при возникновении блока цифр 122 в сумме двух чисел его можно заменить набором 000.

Очевидно, что любой многочлен от α, корнем которого является $\alpha=i-1$, также будет обращаться в нуль.

Таким образом, любой «нулевой» многочлен должен делиться на выражение

$$(\alpha-i+1)\cdot(\alpha+i+1)=\alpha^2+2\cdot\alpha+2.$$

Из сказанного выше следует алгоритм сложения двух чисел, записанных в системы счисления с основанием α.

Алгоритм 1.

Шаг 1. Складываем по разрядам два данных числа. При этом в записи суммы может присутствовать цифра 2, не входящая в алфавит системы счисления. Тогда переходим к шагу 2, иначе получаем искомую сумму.

Шаг 2. Используем формулу (7) для каждой 2 в записи числа (по одному разу для каждого разряда), при этом в записи может появиться и цифра 3. После этого, двигаясь от нулевого разряда, находим первую цифру справа, большую единицы. Эта цифра и все другие, стоящие слева от неё, определяют некоторый многочлен $P(x)$. Если $P(x)$ делится на $x^2+2\cdot x+2$ без остатка, то считаем его «нулевым», если с остатком, то повторяем шаг 2, учитывая, что $3=\alpha^3+\alpha^2+1=1101_\alpha$.

Если в сумме не осталось цифр больших 1, то получаем искомый результат.

Пример 1. $22=110011011100_\alpha$,

$$8=111000000_\alpha.$$

Найдём сумму этих чисел.

1)
1 1 0 0 1 1 0 1 1 1 0 0
+
1 1 1 0 0 0 0 0 0
1 1 0 1 2 2 0 1 1 1 0 0
2)
1 1 0 1 2 2 0 1 1 1 0 0 = 1 2 2 2 0 0 0 1 1 1 0 0

Многочлен x^3+2x^2+2x+2 не делится без остатка на многочлен $x^2+2\cdot x+2$, поэтому повторяем шаг 2):

1 2 2 2 0 0 0 1 1 1 0 0 = 1 2 3 1 0 0 0 0 0 1 1 1 0 0.

(Заметим, что можно поступить иначе, а именно, либо в записи 1 1 0 1 2 2 0 1 1 1 0 0 заменить «нулевой» блок 122 блоком 000; либо в записи 1 2 2 2 0 0 0 1 1 1 0 0 отбросить слева «нулевой» блок 122, и, преобразуя оставшуюся 2, получить результат: 1 1 0 0 0 0 0 1 1 1 0 0).

Многочлен x^2+2x+3 не делится без остатка на многочлен $x^2+2\cdot x+2$, поэтому ещё раз повторяем шаг 2):

1 2 3 1 0 0 0 0 0 1 1 1 0 0 = 1 2 2 0 1 1 0 0 0 0 0 1 1 1 0 0

Многочлен x^2+2x+2 делится без остатка на многочлен $x^2+2\cdot x+2$, поэтому получаем результат 0 1 1 0 0 0 0 0 1 1 1 0 0 = 1 1 0 0 0 0 0 1 1 1 0 0, то есть $30=110000011100_\alpha$.

4.2. Умножение

Поскольку «алфавит» системы счисления с основанием α состоит из цифр 0 и 1, то умножение чисел *a* и *c* в этой системе счисления сводится к сложению *m* чисел, где *m* – количество единиц в записи числа *c*. Складываемые числа получаются из числа *a* следующим образом. При умножении числа на 1, стоящую в разряде, соответствующем α^n, к записи числа *a* справа добавляется *n* нулей. Числа, полученные при умножении на единицы некоторых разрядов, складываются последовательно по два числа в соответствии с алгоритмом сложения.

Пример 2.

$4=111010000_\alpha$,

$3=1101_\alpha$.

Найдём произведение этих чисел.

111010000
x 1101
111010000
+ 11101000000
11212010000 = 122110010000 = 110010000
+ 111010000000
111120010000 = 122100010000 = 100010000

Таким образом, $12=4\cdot 3=100010000_\alpha$.

4.3. Инверсия знака

Для получения алгоритма изменения знака числа, записанного в системе счисления с основанием α, докажем лемму.

Лемма 3. Если целое рациональное число β представлено в системе счисления с основанием $\alpha=i-1$ в виде

$$\beta=\sum_{j=0}^{n}a_j\alpha^j,\ a_j\in\{0,1\}, \tag{8}$$

то $a_{4l+1}=0$ и $a_{4l+2}=a_{4l+3}$, где $0\le l\le\left[\frac{n}{4}\right]$.

Доказательство. Формулу (8) можно записать так $\beta=\sum_{l=0}^{\left[\frac{n}{4}\right]}\alpha^{4l}\left(a_{4l+3}\alpha^3+a_{4l+2}\alpha^2+a_{4l+1}\alpha^1+a_{4l+0}\alpha^0\right)$

или

$$\beta=\sum_{l=0}^{\left[\frac{n}{4}\right]}(-4)^l\left(a_{4l+3}(2+2i)+a_{4l+2}(-2i)+\right.$$
$$\left.+a_{4l+1}(i-1)+a_{4l+0}\right). \tag{9}$$

Известно [1], что любое целое рациональное β можно однозначно представить в системе счисления с основанием -4, используя цифры 0,1,2,3:

$$\beta=\sum_{j=0}^{m}\beta_j(-4)^j. \tag{10}$$

Покажем, что в равенстве (9) за счёт выбора цифр $a_{4l+3}, a_{4l+2}, a_{4l+1}, a_{4l}$ скобка

$$\left(a_{4l+3}(2+2i)+a_{4l+2}(-2i)+a_{4l+1}(i-1)+a_{4l+0}\right)$$

может принимать любое значение из множества $\{0,1,2,3\}$. Действительно, полагая $a_{4l+1}=0$ и $a_{4l+2}=a_{4l+3}$, имеем

$$\left(a_{4l+3}(2+2i)+a_{4l+2}(-2i)+a_{4l+1}(i-1)+\right.$$
$$\left.+a_{4l+0}\right)=2a_{4l+3}+a_{4l+0}.$$

Здесь, придавая значения 0 и 1 коэффициентам a_{4l} и a_{4l+3}, получаем любое из необходимых значений суммы $2a_{4l+3}+a_{4l+0}\in\{0,1,2,3\}$.

Таким образом, (9) можно рассматривать как представление β в системе счисления с основанием -4, то есть мы доказали существование таких цифр $a_{4l+3}, a_{4l+2}, a_{4l+1}, a_{4l}$, при которых имеет место (9), а значит и (8). В силу того, что представление (8) в системе счисления с основанием α- единственно, лемма доказана. ■

С помощью доказанной выше леммы, а также условия равенства нулю суммы противоположных чисел $\beta=\sum_{j=0}^{n}a_j\alpha^j$ и $-\beta=\sum_{l=0}^{k}b_l\alpha^l$, получается следующий алгоритм изменения знака числа.

Алгоритм 2.

Шаг 1. Если $a_0 = 0$, то $b_0 = a_0 = b_1 = a_1 = 0, j = 2$ и переходим к шагу 2, иначе $j = 0$, и переходим к **Шагу 3**.

Шаг 2.

2.0. Если j больше длины числа β, то работа алгоритма завершена.

2.1. Если $a_j = 0$, то $b_j = a_j = b_{j+1} = a_{j+1} = 0, j = j + 2$, и переходим к **Шагу 3**.

2.2. Если $a_j = 1$, то

$$b_j = a_j = b_{j+1} = a_{j+1} = 1, b_{j+2} \equiv a_{j+2} + 1 (\mathrm{mod}\, 2),$$

$$b_{j+3} = a_{j+3} = 0, \; j = j + 4,$$

и переходим к **Шагу 2**.

Шаг 3. $b_j = a_j, b_{j+1} = a_{j+1} = 0$.

3.1. Если $a_j = 0$,

то $j = j + 2$ и переходим к **Шагу 2**.

3.2. Если $a_j = 1$, то

$$b_{j+2} \equiv a_{j+2} + 1 (\mathrm{mod}\, 2), b_{j+3} \equiv a_{j+3} + 1 (\mathrm{mod}\, 2),$$

$$b_{j+4} \equiv a_{j+4} + 1 (\mathrm{mod}\, 2), b_{j+5} = a_{j+5} = 0, \; j = j + 6,$$

и переходим к **Шагу 2**.

Например, если $\beta = 7 = 111011101_\alpha$, то согласно шагу 3, получаем

$$b_0 = 1, b_1 = 0, b_2 = 0, \; b_3 = 0, b_4 = 0, b_5 = 0,$$

и затем в соответствии с шагом 2:

$$b_6 = b_7 = 1, b_8 = 0, b_9 = 0.$$

Работа алгоритма завершена:

$$-\beta = 11000001_\alpha = -7.$$

Заключение

В работе подробно рассмотрены алгоритмы представления целых элементов (в том числе и обычных целых чисел) и реализации основных арифметических операций в кольце целых гауссовых чисел.

В отличие от метода работы [2], для представления чисел в системе счисления с комплексным основанием используется факт наличия в этом кольце алгоритма деления с остатком по норме.

Предложенный подход достаточно легко обобщается на случай других квадратичных расширений, для элементов которых есть алгоритмы деления с остатком по норме [5] и на случай небинарных систем счисления.

Рассмотренный подход обеспечивает дополнительную криптостойкость системы кодирования по методу работы [3] или новые алгоритмы параллельного вычисления произведения больших целых чисел методом, описанным в монографии [4].

Литература

1. **Кнут, Д.** Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы / Д. Кнут; пер. с англ. – М.: Мир, 1977. – 727 с.
2. **Kovacs, A.** Generalized binary number system / A. Kovacs // Annales Univ. Sci. Budapest, Sect. Comp. – 2001. – Vol. 20. – P. 195-206.
3. **Fedoseev, V.** Cryptography and Canonical Number Systems in Quadratic Fields / V. Fedoseev, V. Chernov // Machine Graphic & Vision. – 2006. – Vol. 15(3/4). – P. 363-372.
4. **Чернов, В.М.** Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов. – М.: ФИЗМАТЛИТ, 2007. – 264 с.
5. **Боревич, З.И.** Теория чисел / З.И. Боревич, И.Р. Шафаревич, – 3 изд., доп. – М.: Наука, 1885. – 504 с.

References

1. **Knuth, D.E.** The art of computer programming. Vol. 2: Seminumerical algorithms / D.E. Knuth. – Addison-Wesley, Reading, Mass., 1969.
2. **Kovacs, A.** Generalized binary number system / A. Kovacs // Annales Univ. Sci. Budapest, Sect. Comp. – 2001. –Vol. 20. – P. 195-206.
3. **Fedoseev, V.** Cryptography and Canonical Number Systems in Quadratic Fields / V. Fedoseev, V. Chernov // Machine Graphic & Vision. – 2006. – Vol. 15(3/4). – P. 363-372.
4. **Chernov, V.M.** Arithmetical methods of synthesis of fast algorithms of Discrete orthogonal Transforms / V.M. Chernov. – Moscow: “Fizmatlit” Publisher, 2007. – 264 p. – (in Russian).
5. **Borevich, Z.I.** Number theory / Z.I. Borevich, I. R. Shafarevich; third edition. – Moscow, “Science” Publisher, 1885. – 504 p. – (in Russian).

GAUSSIAN INTEGERS REPRESENTATION IN PITTI’S NUMBER SYSTEM

P. S. Bogdanov
S. P. Korolyov Samara State Aerospace University

Abstract

In this paper the algorithm of representation of Gaussian integers in a canonical numerical system with the basis $\alpha = i - 1$, based on division with remainder is considered. Algorithms of performance of the basic arithmetic operations with numbers in the chosen numerical system are offered.

Key words: canonical numerical system, norm division with remainder**.**

Сведения об авторе

Богданов Павел Сергеевич, 1989 года рождения, студент Самарского государственного аэрокосмического университета имени академика С.П. Королёва. Область научных интересов: обработка изображений, программирование, прикладная математика.
e-mail: *poulsmb@rambler.ru*

Pavel Sergeevich Bogdanov (b. 1989) student of S. P. Korolyov Samara State Aerospace University *(SSAU)*. Research interests are image processing, programming, applied mathematics.

Поступила в редакцию 1 декабря 2010 г.