Задача 11. Деление с остатком

Известно, что для любых двух целых ненулевых чисел a, b имеет место теорема о делении с остатком: существуют целое q и целое неотрицательное r такие, что $a = bq + r$, $0 \le r < |b|$. В данной задаче необходимо исследовать, можно ли ввести аналог деления с остатком на различных числовых множествах. Через $\mathbb{C}$ будем обозначать множество комплексных чисел $a + bi$, $i^2 = -1$, где a, b действительные числа. Сложение и умножение комплексных чисел осуществляется следующим образом: $(a + bi) + (c + di) = (a + c) + (b + d)i$,$(a + bi) \cdot (c + di) = (ac - bd) + (bc + ad)i$. Для любого числового множества K черезK_* обозначим множество K без нуля. Через $\mathbb{N}_0$ обозначаем множество всех натуральных чисел в объединении с нулем.

Подмножество K множества комплексных чисел $\mathbb{C}$ назовем *допустимым*, если выполняются следующие условия: 1) K содержит 0 и 1; 2) $a + b$, $a - b$, $ab \in K$ для любых $a, b \in K$; 3) существует функция $f: K \to \mathbb{N}_0$ (т.е. принимающая целые неотрицательные значения) такая, что $f(ab) \ge f(a)$ для любых ненулевых $a, b \in K$.

*Примечание.*Для некоторых множеств вполне может подойти функция $f(a) = |a|$или $f(a) = |a|^2$.

Будем говорить, что в допустимом множестве K имеет место *деление с остатком*, если для любых ненулевых $a, b \in K$ выполняется условие: существуют $q, r \in K$ такие, что $a = bq + r$, $f(r) < f(b)$, при этом число q будем называть неполным частным, а r остатком при делении a на b. В частности, если r= 0, то будем говорить, что aделится на bнацело и писать $\frac{a}{b} = q \in k$.

1. Какие из следующих множеств являются допустимыми?
a) множество целых чисел $\mathbb{Z}$ с функцией $f(a) = |a|$;
b) множество гауссовых чисел $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$;
c) множество чисел вида $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, где $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$.
2. Пусть $d \ne 1$ – целое число, которое не делится на квадрат простого. Определим $\mathbb{Z}[\sqrt{d}]$как множество всех чисел вида $a + b\sqrt{d}$ (где a, b рациональные), которые являются корнями многочленов второй степени с целыми коэффициентами и старшим коэффициентом, равным 1. Найдите явный вид элементов множества $\mathbb{Z}[\sqrt{d}]$ и докажите, что это множество является допустимым с функцией $f: \mathbb{Z}[\sqrt{d}] \to \mathbb{N}_0$, $f(a + b\sqrt{d}) = |a^2 - db^2|$.
3. Исследуйте, на каких множествах из п.1 и 2 имеет место деление с остатком.
4. Пусть K – одно из множеств, определенных в п. 1 и 2, на котором имеет место деление с остатком. Для любых ненулевых $a, b \in K$ таких, что $\frac{a}{b} \notin K$, найдите неполное частное q и остаток r (или предложите алгоритм нахождения q, r).

5. Пусть K – одно из множеств, определенных в п. 1 и 2, на котором имеет место деление с остатком. Найдите наименьшую положительную постоянную α_K такую, что для любых ненулевых $a, b \in K$, $\frac{a}{b} \notin K$, имеет место неравенство $f(r) \leq \alpha_K f(b)$, где r – остаток при делении a на b.
6. Предложите свои обобщения или направления исследования в этой задаче и изучите их. В частности, возможны следующие направления:
   а) найти НОД двух чисел в рассматриваемых множествах K (или предложить алгоритм его нахождения);
   а) найти НОК двух чисел в рассматриваемых множествах K (или описать множество НОК, если их число более одного, или предложить алгоритм его нахождения);

в) применить построенную теорию к решению некоторых диофантовых уравнений во множестве K.

Комментарии и ответы:

1) Каждое из множеств $\mathbb{Z}$,$\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ образует евклидово кольцос соответствующей нормой , т.е. является допустимым.
2) $\mathbb{Z}[\sqrt{d}]$ (в данном случае это множество всех целых алгебраических элементов поля $\mathbb{Q}(\sqrt{d})$, в зарубежной литературе чаще используется обозначение O_K, $K = \mathbb{Q}(\sqrt{d})$)состоит из элементов вида $a + b\sqrt{d}$ (где $a, b \in \mathbb{Z}$) при $d \not\equiv 1(mod\ 4)$и состоит из элементов $\frac{a}{2} + \frac{b}{2}\sqrt{d}$ (где a, b – целые числа одной четности) при $d \equiv 1(mod\ 4)$.
3) Согласно работе [1], кольцо $\mathbb{Z}[\sqrt{d}]$ является евклидовым относительно нормы $Nm(a + b\sqrt{d}) = |a^2 - db^2|$тогда и только тогда, когда$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$. Отметим, что $\mathbb{Z}[\omega] = \mathbb{Z}[\sqrt{-3}]$.
4) Для случаев, указанных в п. 3, эффективный алгоритм деления с остатком приведен в [2].
5) Вообще говоря, деление с остатком в евклидовых кольцах осуществляется неединственным образом (к примеру, $8 = 3 \cdot 2 + 2 = 3 \cdot 3 + (-1)$).Наибольший интерес представляет следующая трактовка:
   Пусть на $\mathbb{Z}[\sqrt{d}]$ задана норма $Nm(\alpha + \beta\sqrt{d}) = |\alpha^2 - d\beta^2|$. При делении с остатком: $a = bq + r$будем выбирать r с наименьшим возможным значением нормы (если таких r несколько, то выбираем любой из них). Требуется подобрать наименьшую постоянную (не зависящую от a,b) $\alpha_{\mathbb{Z}[\sqrt{d}]}$, такую, что $Nm(r) \leq \alpha_{\mathbb{Z}[\sqrt{d}]} Nm(b)$.
   Если $d < 0$,то $\alpha_{\mathbb{Z}[\sqrt{d}]} = \frac{1-d}{4}$при $d \not\equiv 1(mod\ 4)$ и $\alpha_{\mathbb{Z}[\sqrt{d}]} = -\frac{(1-d)^2}{16d}$при $d \equiv 1(mod\ 4)$ (см. теорему 2.3 из работы команды лицей БГУ-1).

Для положительных d постоянную $\alpha_{\mathbb{Z}[\sqrt{d}]}$ можно оценить, используя методы работы [1]. В частности, $\alpha_{\mathbb{Z}[\sqrt{d}]} < 0.996$ для всех евклидовых колец $\mathbb{Z}[\sqrt{d}]$ с рассматриваемой нормой.

6) Также отметим, что выполнение неравенства $\alpha_{\mathbb{Z}[\sqrt{d}]} < 1$ означает, что в данном кольце можно выполнить алгоритм Евклида для чисел a, b за $O(\log N)$ шагов, где $N = \max\{Nm(a), Nm(b)\}$. К примеру, в евклидовом кольце многочленов $\mathbb{R}[x]$ имеем $\alpha_{\mathbb{R}[x]} = 1$, при этом число шагов алгоритма Евклида не является логарифмическим относительно степеней многочленов.

[1] Eggleton R.B., Lacampagne C.B., Selfridge J.L. Euclidean quadratic fields // Amer. Math. Monthly. 1992. Vol. 99 (9). P. 829 – 837.

[2] Васьковский М.М. Полиномиальная эквивалентность вычисления функции Эйлера RSA-модуля и поиска секретного ключа в квадратичных евклидовых кольцах // Минск: БГУ, 2016. Материалы международного конгресса по информатике CSIST’16. С. 427 – 430.