Тривиум, осенний семестр 2019 г.

Часть I. Числа и многочлены.

факультет математики, НИУ ВШЭ

1. Школьная алгебра

Если хотите освежить в памяти школьную алгебру — читайте замечательную книгу [Алгебра], начиная с любой страницы и до конца.

Задача 1. Переведите обыкновенную дробь в десятичную, а десятичную дробь — в обыкновенную:

$$\text{(а) } \frac{5}{7}; \qquad \text{(б) } 1,3(12).$$

Задача 2. Как быстро вычислить суммы

$$\text{(а) } 1+2+3+\ldots+99+100; \qquad \text{(б) } 1+2+2^2+\ldots+2^9+2^{10}?$$

Задача 3. Перемножьте

$$\text{(а) } (1-x)(1+x+x^2+\ldots+x^{10}); \qquad \text{(б) } (1+x)(1+x^2)(1+x^4)\ldots(1+x^{1024});$$
$$\text{(в) } (1+x+x^2+\ldots+x^{10})(1-x+x^2-\ldots+x^{10}); \qquad \text{(г) } (1-x)(1+x+x^2+\ldots).$$

Задача 4 (Теорема Безу)**.** (а) Докажите, что многочлен $f(x)$ делится на двучлен $x-a$ тогда и только тогда, когда $f(a)=0$.

(б) Делится ли многочлен $100x^{100}+99x^{99}+\ldots+2x^2+x-5050$ на $x-1$?

Задача 5. Выделите полный квадрат в выражениях

$$\text{(а) } x^2+2x-6; \qquad \text{(б) } x^2+3x+1;$$
$$\text{(в) } 2x^2+5x-3; \qquad \text{(г) } -x^2-2x+1.$$

Задача 6. Представьте выражения в виде суммы или разности не более чем двух квадратов

$$\text{(а) } x^2+2xy-3y^2; \qquad \text{(б) } x^2+xy+y^2;$$
$$\text{(в) } 2x^2+4xy+2y^2; \qquad \text{(г) } xy.$$

Задача 7. Сделайте подстановку $x=y+1$ в многочлене $x^4+x^3+x^2+1$.

Задача 8. Иррационально ли число

$$\text{(а) } \sqrt{2}; \qquad \text{(б) } (1+\sqrt{2})(1-\sqrt{2}); \ \text{(в) } \sqrt{3};$$
$$\text{(г) } \sqrt[3]{2}; \qquad \text{(д) } \sqrt{2}+\sqrt{3}; \qquad \text{(е) } \frac{3}{1+\sqrt[3]{2}}-\sqrt[3]{4}+\sqrt[3]{2}?$$

Задача 9. Решите уравнения:

$$\text{(а) } 2x^4+7x^3+4x^2+7x+2=0 \qquad \text{(б) } 3x^4+6x^3-x^2-4x-9=0;$$
$$\text{(в) } x^4+3x^3-2x^2-7x+3=0.$$

(Решения есть в книге [Алгебра, с. 109].)

Задача 10 (Конкурс Квантика, 2019)**.** Можно ли из 1000 чисел $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{1000}$ выбрать 8 чисел и записать их в ряд так, чтобы разности между соседними числами были одинаковы?

Задача 11. *Египетской дробью*[1] называется сумма

$$\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n},$$

где $a_1, \ldots, a_n$ — строго возрастающая последовательность натуральных чисел. Докажите, что можно найти сколь угодно длинную египетскую дробь, слагаемые которой образуют арифметическую прогрессию.

Задача 12 ($\star$ Древнегреческий школьный папирус, 4 век н.э.)**.** Выберите из 100 чисел $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{100}$ несколько так, чтобы их сумма была равна

$$\text{(а) } \frac{4}{19}; \qquad \text{(б) } \frac{3}{19}.$$

2. Бином Ньютона

Про бином Ньютона можно почитать [Алгебра, с. 40] или послушать [Алгебра и геометрия, Лекция 2].

Задача 13. (а) Выпишите первые 10 строк в треугольнике Паскаля.

(б) Что получится после раскрытия скобок и приведения подобных членов в выражении $(x+y)^7$?

(в) Вычислите 11^7.

Задача 14. Докажите, что каждое число a в треугольнике Паскаля, уменьшенное на 1, равно сумме всех чисел, заполняющих параллелограмм, ограниченный теми правой и левой диагоналями, на пересечении которых стоит число a (сами эти диагонали в рассматриваемый параллелограмм не включаются).

Задача 15. Найдите явную формулу (без троеточия и знака суммы) для

(а)

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}.$$

(б)

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

(в)

$$\sum_{k=0}^{n-1} \binom{2n}{2k+1}.$$

(г)

$$\binom{n}{k} + \binom{n-1}{k} + \ldots + \binom{k}{k}.$$

(д)

$$\sum_{k=0}^{n-1} (-1)^k \binom{2n}{2k+1}.$$

---

[1]Такая форма записи рациональных чисел была популярна в Древнем Египте и Древней Греции. Сохранилось много папирусов, например, знаменитый математический папирус Ринда, с таблицами перевода обыкновенных дробей в египетские.

Задача 16. (а) Докажите, что $(a+b\sqrt{2})^n$, где a и b — целые, также имеет вид $p_n+q_n\sqrt{2}$ для некоторых целых p_n и q_n.

(б) Найдите рекуррентную формулу для чисел p_n и q_n из пункта (а) в случае, когда $a=b=1$, и вычислите $\frac{p_6}{q_6}$[2].

(в)* Докажите, что последовательность дробей $\frac{p_n}{q_n}$ из пункта (б) сходится к $\sqrt{2}$.

Задача 17. (а) Докажите, что биномиальный коэффициент $\binom{n}{k}$ равен количеству способов выбрать k элементов из n-элементного множества.

(б) Докажите формулу

$$\binom{n}{0}^2+\binom{n}{1}^2+\ldots+\binom{n}{k}^2=\binom{2n}{k}.$$

(Подсказка: используйте, что $\binom{n}{k}=\binom{n}{n-k}$.)

3. Простые числа, неприводимые многочлены и разложение на множители

Про делимость целых чисел и многочленов можно почитать [Алгебра, с. 47], [Арифметика] или послушать [Алгебра и геометрия, Лекция 4].

Задача 18. Разложите на простые множители числа 111, 1111, 8051, 9991, 11111, 111111.

Задача 19. Примените решето Эратосфена, чтобы найти все целые простые числа в диапазоне от 1 до 120.

Задача 20. Разложите на неприводимые множители в кольце многочленов $\mathbb{R}[x]$ многочлены:

$$\text{(а) } x^2+2x-6; \qquad \text{(б) } x^2+3x+1;$$
$$\text{(в) } 2x^2+5x-3; \qquad \text{(г) } -x^2-2x+1.$$

Задача 21. Разложите на неприводимые множители в кольце многочленов $\mathbb{Q}[x]$ многочлены:

$$\text{(а) } x^2-2; \qquad \text{(б) } x^3-2; \qquad \text{(в) } x^4+4;$$
$$\text{(г) } x^4+4x^2+x+6; \qquad \text{(д) } x^4+3x^3-2x^2-7x+3.$$

Определение 1. *Поле $\mathbb{F}_2$ из двух элементов состоит из двух элементов, обозначаемых 0 и 1, которые складываются и умножаются по следующим правилам:*

$$0+0=1+1=0, \quad 0+1=1+0=1; \quad 0\cdot 0=0\cdot 1=1\cdot 0=0, \quad 1\cdot 1=1.$$

Задача 22. Примените решето Эратосфена, чтобы найти все неприводимые многочлены степени не выше пяти с коэффициентами в поле из двух элементов.

Задача 23. Является ли многочлен x^5+x+1 неприводимым над

$$\text{(а) } \mathbb{F}_2; \qquad \text{(б) } \mathbb{Q}?$$

Задача 24. (а) Докажите, что простых целых чисел бесконечно много.

(б) Докажите для любого заданного поля $\mathbb{F}$, что существует бесконечно много неприводимых многочленов со старшим коэффициентом 1 и остальными коэффициентами из $\mathbb{F}$. Если не знаете определения абстрактного поля, то можете считать, что $\mathbb{F}=\mathbb{F}_2$, $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$.

[2] Вы можете проверить свой ответ, измерив отношение длины и ширины листа бумаги формата A4. Это отношение в точности равно $\frac{p_6}{q_6}$.

Задача 25. (а) Классифицируйте все неприводимые многочлены над $\mathbb{R}$ и над $\mathbb{C}$. (Подсказка: используйте основную теорему алгебры.)

(б) Приведите пример неприводимого многочлена степени 5 над полем из двух элементов.

(в)* Докажите, что над полем из двух элементов существует неприводимый многочлен любой заданной степени.

Задача 26 ($\star$)**.** (а) Докажите, что простых чисел вида $4k+3$, где k — целое, бесконечно много.

(б) Докажите, что простых чисел вида $4k+1$ бесконечно много.

Задача 27. (а) Докажите, что если число 2^n-1 простое, то n обязательно является простым числом. (Простые числа вида 2^n-1 называются *простыми числами Мерсенна.*)

(б) Верно ли обратное?

Задача 28. (а) Докажите, что если число 2^n+1 простое, то n обязательно является степенью двойки, то есть, $n=2^m$ для некоторого натурального m. (Простые числа вида $2^{2^m}+1$ называются *простыми числами Ферма*[3].)

(б) Верно ли обратное?

4. Алгоритм Евклида

Про алгоритм Евклида можно почитать [Арифметика] или послушать [Алгебра и геометрия, Лекция 4].

Задача 29. Найдите НОД (наибольший общий делитель) чисел:

(а) $a=20, b=13$; (б) $a=126, b=91$ (в) $a=77695236973, b=6003722857$.

(г) Для каждой пары чисел a и b из пунктов (а), (б) и (в) найдите все такие целые x и y, что
$$ax+by=\text{НОД}(a,b).$$

Задача 30. Птицефабрика фасует яйца в коробки, рассчитанные либо на дюжину[4] яиц, либо на 25 яиц. Сможет ли птицефабрика отсчитать покупателю ровно 401 яйцо, используя только такие коробки? Предполагается, что в каждой коробке лежит ровно столько яиц, на сколько она рассчитана.

Задача 31. Найдите все решения в целых числах диофантова уравнения
$$16x+27y=214.$$

Задача 32. (а) Найдите НОД многочленов $x^{30}-1$ и x^8-1.

(б) Найдите все такие многочлены f и g с рациональными коэффициентами, что
$$(x^{30}-1)f+(x^2-1)g=\text{НОД}(f,g)$$

Задача 33. Найдите такие многочлены f и g с рациональными коэффициентами, что
$$(x^3-2)f+(2+x+x^2)g=1,$$
и при этом степень многочленов f и g не больше 2.

---

[3]Самое большое известное простое число Ферма — это 65537.

[4]Дюжина — это 12, гросс — это 12^2, а масса — это 12^3 (по-видимому, именно в этом смысле слово масса вошло в идиомы “масса народа” или “масса дел”). Раньше двенадцатеричная система счисления была довольно популярна.

Задача 34. Найдите такие рациональные числа a, b и c, что
$$\frac{1}{(2+\sqrt[3]{2}+\sqrt[3]{4})} = a + b\sqrt[3]{2} + c\sqrt[3]{4}.$$
(Подсказка: Возьмите в качестве a, b и c коэффициенты многочлена f из предыдущей задачи.)

Задача 35. Решите сравнение
$$100x \equiv 999 \pmod{1001},$$
то есть найдите такое целое число x от 0 до 1000, что $100x$ имеет остаток 999 при делении на 1001.

Задача 36. Решите уравнения в целых числах.

(а) $173x + 95y = 7$; (б) $57x + 102y = 3$; (в) $91x + 1001y = 6$.

Задача 37. Решите уравнения в натуральных числах.

(а) $173x + 95y = 20000$; (б) $57x + 102y = 10000$.

Задача 38 (Задача Фробениуса о монетах)**.** Макнаггетсы обычно продаются в коробках по 6, 9 и 20 штук.

(а) Можно ли купить ровно 43 макнаггетса, используя только такие коробки?[5]

(б) Докажите, что любое количество макнаггетсов строго больше чем 43 купить можно.

5. Вычеты и основная теорема арифметики

Про основную теорему арифметики и вычеты можно почитать [Арифметика], [Алгебра, с. 136] или послушать [Алгебра и геометрия, Лекция 4].

Задача 39. (а) Найдите последние две цифры числа 2^{65537}.

(б) Найдите коэффициент при x и свободный член многочлена $(x+1)^{65537}$ в кольце многочленов $\mathbb{F}_2[x]$.

Задача 40. (а) Докажите, что ни одно из чисел вида $4k+3$, где k — целое, нельзя представить в виде суммы двух квадратов натуральных чисел.

(б) Докажите, что ни одно из чисел вида 10^{3k+1} нельзя представить в виде суммы двух кубов натуральных чисел.

Задача 41. Докажите, что уравнение
$$x^2 + y^2 + z^2 = 999999$$
не имеет решений в целых числах.

Задача 42. (а) Докажите, что если произведение двух целых чисел ab делится на простое число p, и при этом a не делится на p, то b делится на p. Доказательство не должно опираться на основную теорему арифметики. (Подсказка: решите диофантово уравнение $ax + py = 1$ и умножьте обе части на b.)

(б) Докажите, что для любого простого числа p и любого целого числа a, которое не делится на p, сравнение
$$au \equiv 1 \pmod{p}$$

[5] Ответ можно узнать, посмотрев видеоролик “How to order 43 Chicken McNuggets” канала Numberphile.

разрешимо в целых числах.

(в) Решите сравнение
$$2u \equiv 1 \pmod{37}.$$
(Иными словами, вычислите $\frac{1}{2}$ в поле вычетов $\mathbb{Z}/37\mathbb{Z}$ по модулю 37.[6])

Определение 2. *Скажем, что два многочлена f и g с коэффициентами в поле $\mathbb{F}$ сравнимы по модулю многочлена $h \in \mathbb{F}[x]$, если $f - g$ делится на h.*

Задача 43. (а) Докажите, что если произведение двух неприводимых многочленов ab с коэффициентами в поле $\mathbb{F}$ делится на неприводимый многочлен p, и при этом a не делится на p, то b делится на p.

(б) Докажите, что для любого неприводимого многочлена p и любого многочлена a, который не делится на p, сравнение
$$au \equiv 1 \pmod{p}$$
разрешимо в кольце многочленов $\mathbb{F}[x]$.

(в) Решите сравнение
$$(2 + x + x^2)u \equiv 1 \pmod{(x^3 - 2)}.$$
(Иными словами, вычислите $\frac{1}{2+x+x^2}$ в поле вычетов $\mathbb{F}[x]/(x^3-2)$ по модулю $x^3 - 2$.[7])

Задача 44. Сформулируйте и докажите основную теорему арифметики для кольца целых чисел $\mathbb{Z}$ и кольца многочленов $\mathbb{F}[x]$, где $\mathbb{F}$ — поле.

Задача 45. Докажите, что уравнение $15x^2 - 7y^2 = 9$ не имеет решений в целых числах.

Задача 46. Для каких остатков a по модулю p сравнение
$$x^2 \equiv a \pmod{p}$$
разрешимо в целых числах, если p равно

(а) 5, (б) 13, (в) 23?

Задача 47. Докажите, что если p — нечётное простое число, то сравнение
$$x^2 \equiv a \pmod{p}$$
разрешимо в целых числах ровно для половины всех ненулевых остатков a по модулю p.

Задача 48. Докажите, что сравнение
$$x^2 + y^2 + z^2 \equiv 0 \mod p$$
имеет нетривиальное решение в целых числах (*тривиальное решение* — это решение $x \equiv y \equiv z \equiv 0 \mod p$).

Задача 49. Докажите, что сравнение $x^2 \equiv -1 \mod p$ не имеет решений в целых числах тогда и только тогда, когда $p \equiv 3 \mod 4$.

---

[6] Обозначение $\mathbb{Z}/n\mathbb{Z}$ для множества вычетов по модулю n неслучайно совпадает с обозначением для факторгруппы группы $\mathbb{Z}$ по подгруппе $n\mathbb{Z}$.

[7] Обозначение $\mathbb{F}[x]/(f(x))$ для множества вычетов по модулю $f(x)$ неслучайно совпадает с обозначением для факторкольца кольца $\mathbb{F}[x]$ по главному идеалу, порождённому многочленом $f(x)$.

6. Китайская теорема об остатках и малая теорема Ферма

Задача 50. (а) Пусть p и q — два взаимно простых целых числа. Найдите такие целые числа x и y, что $px \equiv 1 \pmod q$ и $qy \equiv 1 \pmod p$. (Подсказка: решите диофантово уравнение $px + qy = 1$.)

(б) Решите пункт (а), заменив целые числа на многочлены с коэффициентами в поле.

Задача 51. (а) Докажите китайскую теорему об остатках: если p и q два взаимно простых числа, то остаток целого числа n при делении на pq однозначно определяется его остатками $n \pmod p$ и $n \pmod q$ при делении на p и q, соответственно.

(б) Сформулируйте и докажите китайскую теорему об остатках для многочленов.

(в) Используя задачу 50, предложите алгоритм вычисления $n \pmod{pq}$ по $n \pmod p$ и $n \pmod q$.

(г) Используя, что

$$718865222040754575648532881408 = n^{13}$$

для некоторого целого n, найдите n без калькулятора.

Задача 52. (а) Найдите все решения в $\mathbb{Z}$ системы сравнений

$$n \equiv 5 \pmod 8, \quad n \equiv 2 \pmod 7.$$

(б) Найдите все решения в $\mathbb{Q}[x]$ системы сравнений

$$f(x) \equiv x \pmod{(x^3-2)}, \quad f(x) \equiv 2 \pmod{(x-1)}.$$

Задача 53. Найдите все решения системы сравнений

$$x \equiv 5 \pmod 8, \quad x \equiv 2 \pmod 7, \quad x \equiv 3 \pmod{15}.$$

Задача 54. Найдите натуральное число x, не превосходящее 120, такое что

$$x \equiv 1 \pmod 8, \quad x \equiv 2 \pmod 5, \quad x \equiv 0 \pmod 3.$$

Задача 55. Найдите квадратный многочлен f с рациональными коэффициентами, такой что

$$f(1) = 2, \quad f(2) = 20, \quad f(3) = 200.$$

Подсказка: решите систему сравнений

$$f(x) \equiv 2 \pmod{(x-1)}, \quad f(x) \equiv 20 \pmod{(x-2)}, \quad f(x) \equiv 200 \pmod{(x-3)}.$$

Задача 56. Найдите многочлен $f(x) \in \mathbb{R}[x]$ степени не выше трёх, значения которого в точках 0, 1, 2 и 3 совпадают со значениями функции

$$\text{(а) } 2^x; \quad \text{(б) } \frac{1}{x+1}; \quad \text{(в) } \sin(\frac{\pi x}{2}).$$

Задача 57. Разложите рациональные функции над $\mathbb{R}$ в сумму простейших дробей. Простейшая дробь — это функция вида $\frac{r(x)}{f(x)^n}$, где $f(x)$ — неприводимый многочлен, $r(x)$ — многочлен, степень которого строго меньше чем степень многочлена f, а n — натуральное число:

$$\text{(а) } \frac{x^2+1}{x^2-1}; \quad \text{(б) } \frac{2x^3+x}{x^3+x}; \quad \text{(в) } \frac{2x^2-x-7}{x^3-5x^2+6x}; \quad \text{(в) } \frac{x^n+1}{(x+1)^n}.$$

Задача 58. (а) Докажите, что для любого простого числа $p \neq 2, 5$ найдётся такое натуральное число k, что $10^k - 1$ делится на p.

(б) Докажите, что обыкновенная дробь $\frac{1}{p}$ представляется бесконечной периодической десятичной дробью. Чему может быть равен её период?

Задача 59. Пусть p — простое число.

(а) Докажите "тождество ленивого школьника":

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

(б) Докажите малую теорему Ферма: $n^p - n$ делится на p для любого натурального n.

(в) Будет ли простым число $257^{1092} + 1092$?

Задача 60. Найдите такое натуральное число a, что его степени a, a^2, a^3,…, a^{16} дают все возможные ненулевые остатки при делении на 17.

Задача 61 ($\star$). Пусть $p, q \in \mathbb{N}$ — различные простые числа. Докажите, что сравнение

$$p^x + q^y \equiv 1 \pmod{pq}$$

разрешимо в натуральных числах.

7. Комплексные числа и целые гауссовы числа

Про комплексные числа можно почитать [Математика, раздел 2.5.1-2.5.3], [Комплексные числа] или послушать [Алгебра и геометрия, Лекция 6]. Про целые гауссовы числа можно почитать [Арифметика].

Задача 62. Сумма двух чисел равна 10, а произведение — 40. Найдите эти числа.

Задача 63. Вычислите (то есть представьте в виде $a + bi$ для вещественных a и b):

(а) $(1+i)^8$; (б) $\frac{1}{3+4i}$.

Задача 64. Нарисуйте на комплексной плоскости множество точек, удовлетворяющих условиям:

(а) $\mathrm{Re}\, z = 1$; (б) $|z| = 3$; (в) $\mathrm{Re}\, z \geq 1$, $\mathrm{Im}\, z \geq 2$, $|z| \leq 3$.

Задача 65. Для комплексного числа z определим преобразование плоскости M_z таким образом: каждая точка w переходит в точку $z \cdot w$.

(а) Во сколько раз преобразование M_z для $z = 1 - \sqrt{3}i$ увеличивает расстояния на комплексной плоскости?

(б) Докажите, что M_z при $z \neq 0$ является преобразованием подобия, то есть увеличивает все расстояния в одинаковое число раз.

(в) Пусть $|z| = 1$. Докажите, что в этом случае преобразование M_z является поворотом. На какой угол?

Задача 66. (а) Проверьте, что при умножении комплексных чисел их модули перемножаются, а аргументы складываются.

(б) Выведите из пункта (а) формулу для $\cos(\varphi + \psi)$ и $\sin(\varphi + \psi)$.

Задача 67. (а) Докажите, что если целые числа m и n представляются в виде суммы двух полных квадратов, то их произведение mn тоже представляется в виде суммы двух полных квадратов (и даже двумя способами).

(б)* Докажите, что неотрицательный вещественный многочлен можно представить как сумму двух квадратов вещественных многочленов. (Подсказка: используйте основную теорему алгебры.)

Задача 68 (Формула Муавра)**.** Выпишите формулу для комплексных корней степени n из единицы, используя тригонометрическую форму комплексного числа. Получите явную формулу (в радикалах), когда $n = 3$, 4, 5.

Задача 69. Можно ли ввести на комплексных числах отношение порядка $>$, согласованное со сложением и умножением? (Последнее означает, что для всех $a, b, c \in \mathbb{C}$
(1) из $a > b$ следует $a + c > b + c$; (2) из $a > 0$ и $b > 0$ следует, что $ab > 0$.)

Задача 70. Вычислите
$$\frac{(1+i\sqrt{3})^{2018}}{(1+i)^{4024}}.$$

Задача 71. Нарисуйте на плоскости множество точек z, удовлетворяющих уравнению
$$|z-1| = 2|z+1|.$$

Задача 72. Докажите, что всякое комплексное число является квадратом некоторого комплексного числа.

Задача 73. Найдите все комплексные решения уравнения
$$\text{(а) } z^2 = \sqrt{2} + i\sqrt{2}; \quad \text{(б) } z^2 = 1 + i\sqrt{3}.$$

Задача 74. Найдите все комплексные решения уравнения
(а) $z^3+3z^2+3z+3 = 0$; (б) $z^4+4 = 0$; (в) $(z+i)^4 = (z-i)^4$; (г) $z^4+(z-4)^4 = 32$.

Задача 75. Найдите сумму квадратов длин всех диагоналей в правильном семиугольнике, вписанном в единичную окружность (сторона не считается диагональю).

Задача 76 ($\star$)**.** Докажите, что число $\frac{2+i}{2-i}$ не является корнем n-ой степени из единицы ни для какого натурального n.

Определение 3. *Кольцо целых гауссовых чисел $\mathbb{Z}[i]$ состоит из всех комплексных чисел вида $m + ni$, где m и n — целые числа.*

Задача 77. Разложите 30 на простые множители в кольце целых гауссовых чисел.

Задача 78. Какие из простых чисел 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 останутся простыми в кольце $\mathbb{Z}[i]$?

Задача 79. Пусть γ — целое гауссово число. Введём отношение эквивалентности $\sim_\gamma$ на $\mathbb{Z}[i]$ по правилу: $z \sim_\gamma w$, если $z - w$ делится на γ.

(а) Нарисуйте по одному представителю для каждого класса эквивалентности при $\gamma = 2, 3$ и 5.

(б) Найдите количество классов эквивалентности при $\gamma = 3 - 2i$.

Задача 80. ($\star$) (а) Сформулируйте и докажите основную теорему арифметики для кольца целых гауссовых чисел.

(б) Докажите, что простое число $p \in \mathbb{Z}$ представляется в виде суммы двух полных квадратов тогда и только тогда, когда $p \equiv 1 \mod 4$ или $p = 2$.

Список литературы

[Комплексные числа] В.И. Арнольд, *Геометрия комплексных чисел, кватернионов и спинов*, МЦНМО 2002

[Алгебра] И.М. Гельфанд и А. Шень, *Алгебра*, МЦНМО 2017

[Арифметика] Л.А.Калужин, *Основная теорема арифметики*, М., “Наука”, 1969

[Алгебра и геометрия] В.А. Кириченко, *Основания алгебры и геометрии*, онлайн курс

[Математика] Р. Курант, Г. Роббинс, *Что такое математика?*, МЦНМО 2013