Расширяй и властвуй.
И причем здесь информатика?

Емиж Ислам

Кавказский математический центр Адыгейского государственного университета

В детстве все было натуральнее

$$1, 2, 3, 4, 5, 6 \ldots$$

$(\mathbb{N}, +, -)$, причем $''-''$ определен не всегда.

В детстве все было натуральнее

$$1, 2, 3, 4, 5, 6 \ldots$$

$(\mathbb{N}, +, -)$, причем $''-''$ определен не всегда.

Задача

"У Пети было 2 яблока, Вася дал ему еще несколько в итоге у Пети стало 6 яблок. Сколько яблок дал Вася?"

В детстве все было натуральнее

$$1, 2, 3, 4, 5, 6 \ldots$$

$(\mathbb{N}, +, -)$, причем $''-''$ определен не всегда.

Задача

"У Пети было 2 яблока, Вася дал ему еще несколько, в итоге у Пети стало 6 яблок. Сколько яблок дал Вася?"

$$2 + x = 6$$

$$2 + x - 2 = 6 - 2$$

$$x = 4$$

Задача

"Вася был должен Пете 6 яблок. Вася то занимал яблоки у Пети, то отдавал и теперь должен ему 2 яблока. На сколько изменилась долг Васи?"

Задача

"Вася был должен Пете 6 яблок. Вася то занимал яблоки у Пети, то отдавал и теперь должен ему 2 яблока. На сколько изменила долг Васи?"

$$6 + x = 2$$

$$6 + x - 6 = 2 - 6 \ \ !!?$$

Расширительное поле экспериментов

Добавим решение уравнения $6 + x = 2$ и обозначим его (-4).
Более общим образом, добавим решения уравнений вида

$$A + x = B$$

Расширительное поле экспериментов

Добавим решение уравнения $6 + x = 2$ и обозначим его (-4).
Более общим образом добавим решения уравнений вида

$$A + x = B$$

$$\dots -5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5 \dots$$

$(\mathbb{Z}, +, -)$ – целые числа, обе операции определены всегда. Решаются все уравнения вида $A + x = B$!!!

Уравнения наносят ответный удар!

Новые операции $(\cdot, \setminus)$, причем деление по аналогии с вычитанием опеределено не всегда.

Уравнения наносят ответный удар!

Новые операции $(\cdot, \setminus)$, причем деление по аналогии с вычитанием опередено не всегда.

Задача

"У Пети было 3 корзнки с яблоками в каждой из которых одинаковое число яблок. Вася добавим пете 5 яблок, в итоге у Пети стало 35 яблок. Сколько яблок в каждый корзинке?"

Уравнения наносят ответный удар!

Новые операции $(\cdot, \backslash)$, причем деление по аналогии с вычитанием опередено не всегда.

Задача

"У Пети было 3 корзнки с яблоками в каждой из которых одинаковое число яблок. Вася добавим пете 5 яблок, в итоге у Пети стало 35 яблок. Сколько яблок в каждый корзинке?"

$$3x + 5 = 35$$

$$3x = 30$$

$$x = 10$$

Задача

"Петя начал производство сидра. Для тестовой партии он изготовил 10л сидра. Далее из трех кранов по одному литру в час начала вытекать новая партия. Через сколько времени у Пети будет 30 литров сидра ?"

Задача

"Петя начал производство сидра. Для тестовой партии он изготовил 10л сидра. Далее из трех кранов по одному литру в час начала вытекать новая партия. Через сколько часов у Пети будет 30 литров сидра ?"

$$3x + 10 = 30$$

$$3x = 20 \ \ !!?$$

Рациональный подход

Добавим решение уравнения $3x + 10 = 30$ и обозначим его $\frac{20}{3}$.
Более общим образом, добавим решения уравнений вида

$$Ax + B = C$$

Рациональный подход

Добавим решение уравнения $3x + 10 = 30$ обозначим его $\frac{20}{3}$.
Более общим образом, добавим решения уравнений вида

$$Ax + B = C$$

$$\dots, \frac{-7}{2}, \dots, \frac{-4}{3}, \dots, \frac{0}{1}, \dots, \frac{1}{100}, \dots \frac{10}{1}, \dots$$

$(\mathbb{Q}, +, -, \cdot, \setminus)$ – рациональные числа, все четыре операции определены всегда. Решаются все уравнения вида $Ax + B = C$!!!

Мнительность

Квадратные уравнения...

$$Ax^2 + Bx + C = D$$

или, что то же самое,

$$Ax^2 + Bx + C = 0$$

Мнительность

Квадратные уравнения...

$$Ax^2 + Bx + C = D$$

или, что то же самое,

$$Ax^2 + Bx + C = 0$$

$$x^2 + \frac{B}{A}x + \frac{C}{A} = 0$$

$$(x + \frac{B}{4A})^2 = \frac{B^2 - 4AC}{4A^2}$$

Мнительность

Квадратные уравнения...

$$Ax^2 + Bx + C = D$$

или, что то же самое,

$$Ax^2 + Bx + C = 0$$

$$x^2 + \frac{B}{A}x + \frac{C}{A} = 0$$

$$(x + \frac{B}{4A})^2 = \frac{B^2 - 4AC}{4A^2}$$

Не всегда имеет решение, например, при $B = 0, A = 1, C = 1$.

$$x^2 = -1$$

Добавим решение уравнения $x^2 = -1$ и обозначим его $\pm i$ – мнимая единица.

Добавим решение уравнения $x^2 = -1$ и обозначим его $\pm i$ – мнимая единица. Тогда получится новое множество чисел которое имеет вид:

$$a_n i^n + a_{n-1} i^{n-1} + \cdots + a_0,$$

где a_i обычные действительные числа.

Добавим решение уравнения $x^2 = -1$ и обозначим его $\pm i$ – мнимая единица.
Тогда получится новое множество чисел которое имеет вид:

$$C = a_n i^n + a_{n-1} i^{n-1} + \cdots + a_0,$$

где a_i обычные действительные числа.
Но мы знаем, что $i^2 + 1 = 0$. Поэтому выделяя из C часть делящуюся на $i^2 + 1 = 0$, получим, что $C = b_0 + b_1 i$.

Пример

$$C = -3i^5 + \frac{1}{2}i^3 + i^2 - \frac{1}{8}$$

$$C = (i^2 + 1)(-3i^3 + \frac{7}{2}i + 1) - \frac{7}{2}i - \frac{9}{8}$$

$$C = -\frac{7}{2}i - \frac{9}{8}$$

Со сложением все понятно

$$(a_0 + a_1 i) + (b_0 + b_1 i) = (a_0 + b_0) + (a_1 + b_1)i$$

А, что с умножением?

Со сложением все понятно

$$(a_0 + a_1 i) + (b_0 + b_1 i) = (a_0 + b_0) + (a_1 + b_1)i$$

А, что с умножением?

$$(a_0 + a_1 i)(b_0 + b_1 i) = a_0 b_0 + a_0 b_1 i + a_1 b_0 i + a_1 b_1 (i)^2$$

Со сложением все понятно

$$(a_0 + a_1 i) + (b_0 + b_1 i) = (a_0 + b_0) + (a_1 + b_1)i$$

А, что с умножением?

$$(a_0 + a_1 i)(b_0 + b_1 i) = a_0 b_0 + a_0 b_1 i + a_1 b_0 i + a_1 b_1 (i)^2 =$$

$$= a_0 b_0 - a_1 b_1 + (a_0 b_1 + a_1 b_0)i - a_1 b_1 (i^2 + 1) = a_0 b_0 - a_1 b_1 + (a_0 b_1 + a_1 b_0)i$$

Получаем числа вида $a + bi$ с операциями сложения и умножения. Причем также определены операции вычитания и, что самое главное, деления.
Мы получили $(\mathbb{C}, +, -, \cdot, \setminus)$ – комплексные числа.

Получаем числа вида $a + bi$ с операциями сложения и умножения. Причем также определены операции вычитания и, что самое главное, деления.
Мы получили $(\mathbb{C}, +, -, \cdot, \setminus)$ – комплексные числа.
Решаются все уравнения вида

$$Ax^2 + Bx + C = D$$

Теорема (Основная теорема алгебры)

Любой многочлен ненулевой степени над полем комплексных чисел имеет корень.

И вновь продолжается бой

$$\ldots, \ -5, -4, -3, -2, -1, \ 0, \ 1, \ 2, \ 3, \ 4, \ 5, \ \ldots$$

И вновь продолжается бой

$$\ldots,\ -5, -4, -3, -2, -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ \ldots$$

С точки зрения остатаков деления на 5

$$\ldots,\ [0], [1], [2], [3], [4],\ [0],\ [1],\ [2],\ [3],\ [4],\ [0],\ \ldots$$

И вновь продолжается бой

$$\ldots,\ -5, -4, -3, -2, -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ \ldots$$

С точки зрения остатаков деления на 5

$$\ldots,\ [0], [1], [2], [3], [4],\ [0],\ [1],\ [2],\ [3],\ [4],\ [0],\ \ldots$$

остатки хорошо скалдываются и умножаются:

$$[1] + [2] = [3],\ \ [3] + [4] = [7] = [2]$$

$$[1][3] = [3],\ \ [2][3] = [1],\ \ [4][2] = [8] = [3]$$

И сердцу тревожно в груди

Можно делить и вычитать!!

$$[1] = [-4],\ \ [2] = [-3],\ \ [3] = [2],\ \ [4] = [-1]$$

$$[2][3] = [1],\ \ [4][4] = [16] = [1]$$

И сердцу тревожно в груди

Можно делить и вычитать!!

$$[1] = [-4],\ \ [2] = [-3],\ \ [3] = [2],\ \ [4] = [-1]$$

$$[2][3] = [1],\ \ [4][4] = [16] = [1]$$

Решаются все уравнения вида

$$Ax + B = C$$

Но уравнение $x^2 + 3 = 0$ решений не имеет

Но уравнение $x^2 + 3 = 0$ решений не имеет

$$[0]^2 + [3] = [3]$$

$$[1]^2 + [3] = [4]$$

$$[2]^2 + [3] = [2]$$

$$[3]^2 + [3] = [2]$$

$$[4]^2 + [3] = [2]$$

Старого пса новым приемам не научишь

Добавим α – решенеие уравнения $x^3 + 3 = 0$. Получим формальные выражения вида

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0$$

Старого пса новым приемам не научишь

Добавим α – решенеие уравнения $x^3 + 3 = 0$. Получим формальные выражения вида

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0$$

По аналогии с комплексными числами имеем, что каждое число представимо ввиде $b_0 + b_1\alpha$. Сложение и умножение имеют вид

$$(a_0 + a_1\alpha) + (b_0 + b_1\alpha) = (a_0 + b_0) + (a_1 + b_1)\alpha$$

$$(a_0 + a_1\alpha)(b_0 + b_1\alpha) = a_0b_0 + a_0b_1\alpha + a_1b_0\alpha + a_1b_1\alpha^2 =$$

$$= (a_0b_0 - 3a_1b_1) + (a_0b_1 + a_1b_0)\alpha$$

- Bierbrauer J. Introduction to coding theory. – Chapman and Hall/CRC, 2016.
- Niederreiter H. Coding theory and cryptology. – World Scientific, 2002. – T. 1.
- Lidl R., Niederreiter H. Finite fields and their applications //Handbook of algebra. – North-Holland, 1996. – T. 1. – C. 321-363.
- Aumasson J. P. Serious cryptography: a practical introduction to modern encryption. – No Starch Press, Inc, 2024.
- Стругацкий А.Н., Стругацкий Б.Н. "За миллиард лет до конца света"