

Что можно делать с вещественными числами и нельзя делать с целыми числами

Ю. В. МАТИЯСЕВИЧ

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова РАН

<http://logic.pdmi.ras.ru/~yumat>

Что можно делать с вещественными числами и нельзя делать с целыми числами

Ю. В. МАТИЯСЕВИЧ

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова РАН

<http://logic.pdmi.ras.ru/~yumat>

Что можно делать с вещественными числами и нельзя делать с целыми числами

Часть 2. Десятая проблема Гильберта

Ю. В. МАТИЯСЕВИЧ

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова РАН

<http://logic.pdmi.ras.ru/~yumat>

Давид Гильберт, *“Математические проблемы”*, [1900]

Давид Гильберт, “*Математические проблемы*”, [1900]

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Давид Гильберт, “*Математические проблемы*”, [1900]

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; *требуется указать общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет.*

Диофантовы уравнения

Определение. Диофантово уравнение имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофантовы уравнения

Определение. Диофантово уравнение имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

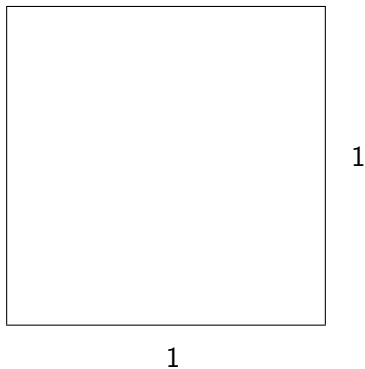
Греческий математик *Диофант* жил, скорее всего, в 3-ем веке нашей эры.

Полиномиальные уравнения у древних греков

$$x^2 = 2$$

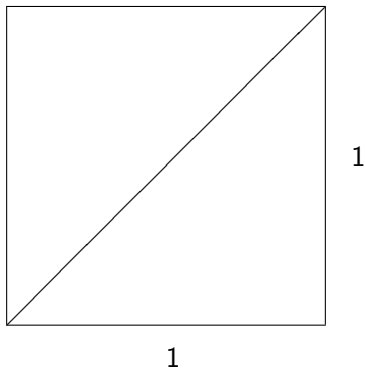
Полиномиальные уравнения у древних греков

$$x^2 = 2$$



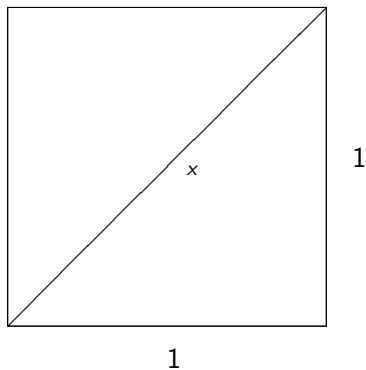
Полиномиальные уравнения у древних греков

$$x^2 = 2$$



Полиномиальные уравнения у древних греков

$$x^2 = 2$$



Давид Гильберт, “Математические проблемы”, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; *требуется указать общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет.*

Давид Гильберт, “Математические проблемы”, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; *требуется указать общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в **целых рациональных числах** или нет.*

Целые рациональные числа

Давид Гильберт, “Математические проблемы”, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; *требуется указать общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет.*

Целые рациональные числа – это числа $0, \pm 1, \pm 2, \pm 3, \dots$

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Можно также ограничиться только решениями в положительных целых числах или только в неотрицательных целых числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Можно также ограничиться только решениями в положительных целых числах или только в неотрицательных целых числах

От Диофанта до Гильберта

Диофант жил – когда?

От Диофанта до Гильберта

Диофант жил, скорее всего, в 3-ем веке нашей эры.

От Диофанта до Гильберта

Диофант жил, скорее всего, в 3-ем веке нашей эры.

Гильберт сформулировал проблемы – когда?

От Диофанта до Гильберта

Диофант жил, скорее всего, в 3-ем веке нашей эры.

Гильберт сформулировал проблемы в 1900 году

Давид Гильберт, *“Математические проблемы”*, [1900]

Давид Гильберт, “Математические проблемы”, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано **произвольное** диофантово уравнение с **произвольным** числом неизвестных и целыми рациональными коэффициентами; *требуется указать **общий метод**, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет.*

Массовые проблемы

В современной терминологии 10-я проблема Гильберта является **массовой проблемой**, то есть проблемой, состоящей из счетного числа вопросов, на каждый из которых требуется дать ответ ДА или НЕТ. Суть массовой проблемы состоит в требовании найти **единый универсальный** метод, который позволял бы ответить на любой из этих вопросов.

Массовые проблемы

В современной терминологии 10-я проблема Гильберта является **массовой проблемой**, то есть проблемой, состоящей из счетного числа вопросов, на каждый из которых требуется дать ответ ДА или НЕТ. Суть массовой проблемы состоит в требовании найти **единый универсальный** метод, который позволял бы ответить на любой из этих вопросов.

Среди двадцати трёх “Математических проблем” Гильберта 10-я является единственной массовой проблемой

Массовые проблемы

В современной терминологии 10-я проблема Гильберта является **массовой проблемой**, то есть проблемой, состоящей из счетного числа вопросов, на каждый из которых требуется дать ответ ДА или НЕТ. Суть массовой проблемы состоит в требовании найти **единый универсальный** метод, который позволял бы ответить на любой из этих вопросов.

Среди двадцати трёх “Математических проблем” Гильберта 10-я является единственной массовой проблемой и она может рассматриваться как проблема информатики.

Массовые проблемы

В современной терминологии 10-я проблема Гильберта является **массовой проблемой**, то есть проблемой, состоящей из счетного числа вопросов, на каждый из которых требуется дать ответ ДА или НЕТ. Суть массовой проблемы состоит в требовании найти **единый универсальный** метод, который позволял бы ответить на любой из этих вопросов.

Среди двадцати трёх “Математических проблем” Гильберта 10-я является единственной массовой проблемой и она может рассматриваться как проблема информатики.

Ответ

Сегодня мы знаем, что 10-я проблема Гильберта решения не имеет. Это означает, что она неразрешима как массовая проблема:

Ответ

Сегодня мы знаем, что 10-я проблема Гильберта решения не имеет. Это означает, что она неразрешима как массовая проблема:

Теорема (Неразрешимость 10-й проблемы Гильберта) *Не существует алгоритма, который по узлавал бы по произвольному диофантову уравнению, имеет ли оно решения.*

Ответ

Сегодня мы знаем, что 10-я проблема Гильберта решения не имеет. Это означает, что она неразрешима как массовая проблема:

Теорема (Неразрешимость 10-й проблемы Гильберта) *Не существует алгоритма, который по узлавал бы по произвольному диофантову уравнению, имеет ли оно решения.*

В этом смысле говорят об **отрицательном решении** 10-й проблемы Гильберта.

Давид Гильберт, *“Математические проблемы”*, [1900]

Давид Гильберт, *“Математические проблемы”*, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; требуется указать **общий метод, следуя которому можно было бы в конечное число шагов узнать**, имеет ли данное уравнение решение в целых рациональных числах или нет.

Первая неразрешимая массовая проблема в чистой математике



А. А. МАРКОВ (сын)
1903–1979



EMIL L. POST
1897–1954

Recursively enumerable sets of positive integers and their decision problems. *Bulletin AMS*, **50**, 284–316 (1944); reprinted in: *The Collected Works of E. L. Post*, Davis, M. (ed), Birkhäuser, Boston, 1994.

Hilbert's 10th problem "begs for an unsolvability proof"



EMIL L. POST
1897–1954

Хронология

Хронология

- ▶ Начало 50-х годов: гипотеза, которую выдвинул Martin Davis.

Хронология

- ▶ Начало 50-х годов: гипотеза, которую выдвинул Martin Davis.
- ▶ Начало 60-х годов: частичный прогресс, который достигли Martin Davis, Hilary Putnam и Julia Robinson.

Хронология

- ▶ Начало 50-х годов: гипотеза, которую выдвинул Martin Davis.
- ▶ Начало 60-х годов: частичный прогресс, который достигли Martin Davis, Hilary Putnam и Julia Robinson.
- ▶ 1970 год: последний шаг сделал Ю.Матиясевич.

An e-mail

An e-mail

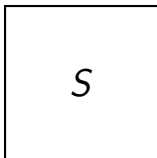
Dear Professor,

you are wrong. I am a brilliant young programmer and last night I wrote a sophisticated program in Java##. My program solves Hilbert's tenth problem in the `__positive__` sense. Namely, for every Diophantine equation given as input, the program will print 1 or 0 depending on whether the equation has a solution or not.

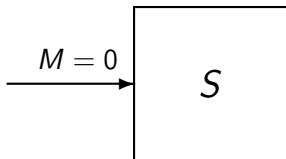
The attachment contains my ingenious program. You can run it on your favorite Diophantine equations and see how fast my program works.

Have a fun, Professor!

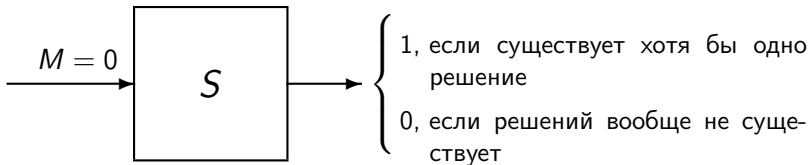
Точка зрения студента



Точка зрения студента

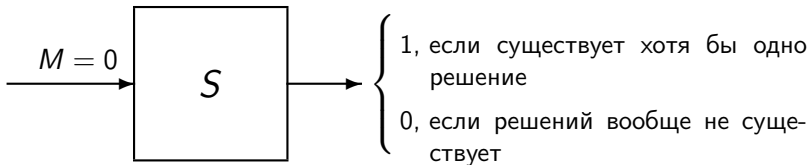


Точка зрения студента



Точка зрения студента

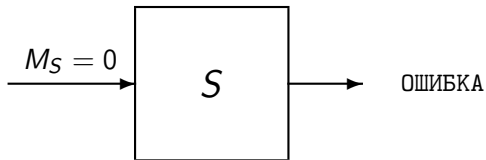
Для любого многочлена M :



Точка зрения профессора:

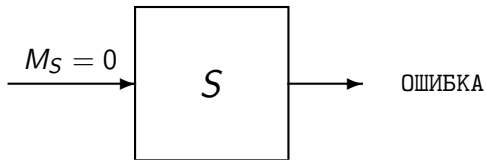
Точка зрения профессора:

Существует многочлен M_S такой, что



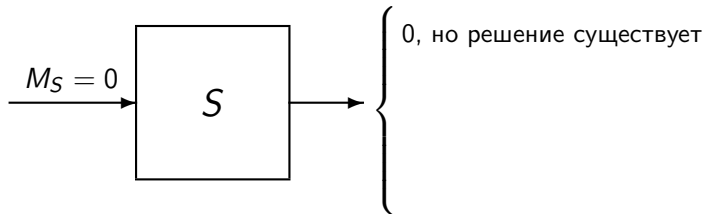
Точка зрения профессора:

Существует многочлен M_S такой, что



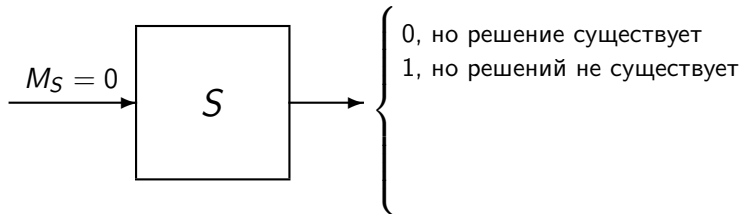
Точка зрения профессора:

Существует многочлен M_S такой, что



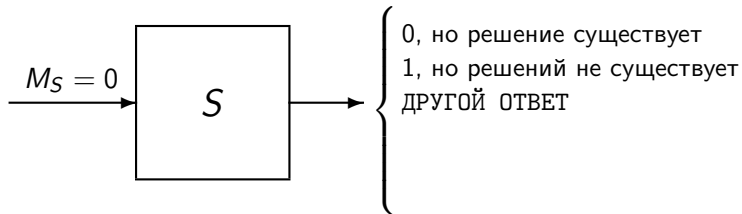
Точка зрения профессора:

Существует многочлен M_S такой, что



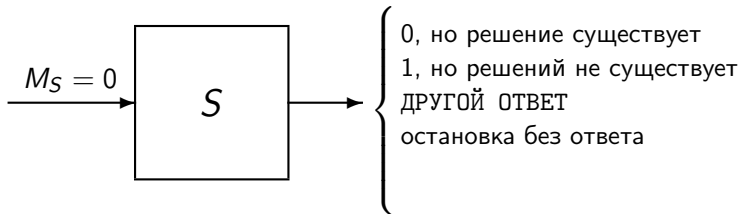
Точка зрения профессора:

Существует многочлен M_S такой, что



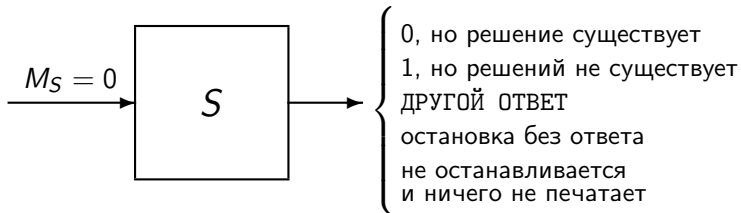
Точка зрения профессора:

Существует многочлен M_S такой, что



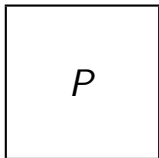
Точка зрения профессора:

Существует многочлен M_S такой, что

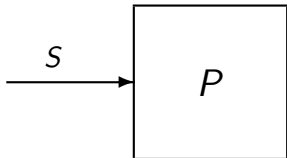


Программа профессора

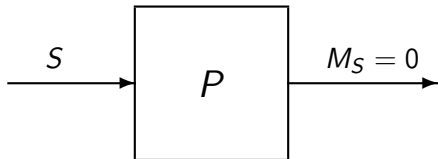
Программа профессора



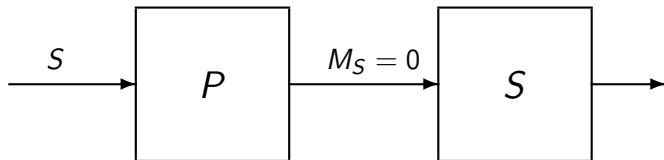
Программа профессора



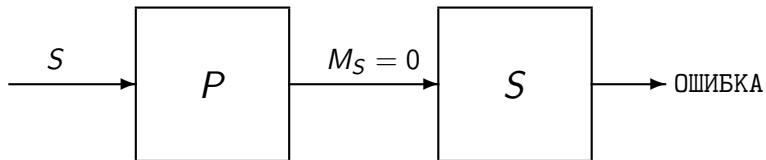
Программа профессора



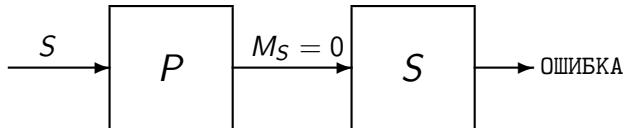
Программа профессора



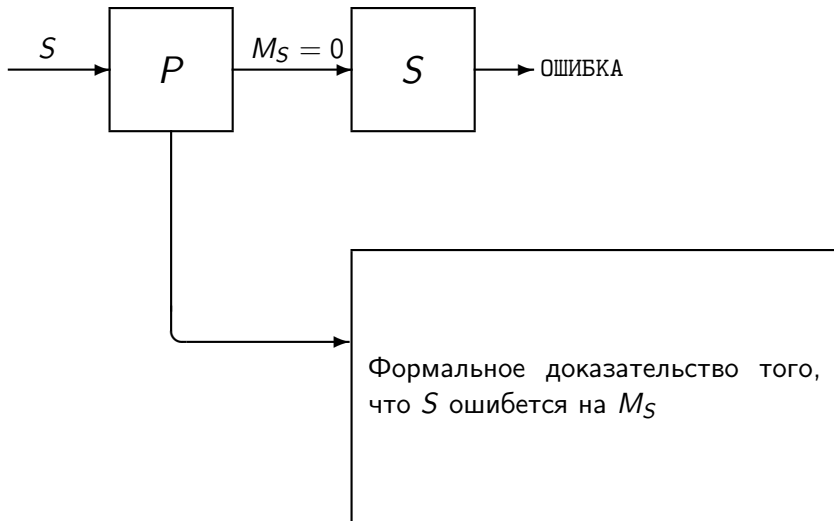
Программа профессора



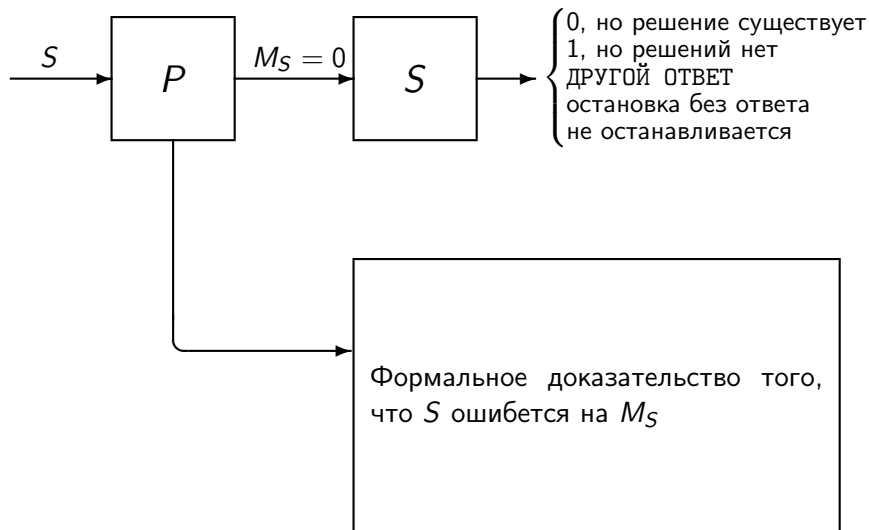
Усовершенствованная программа профессора



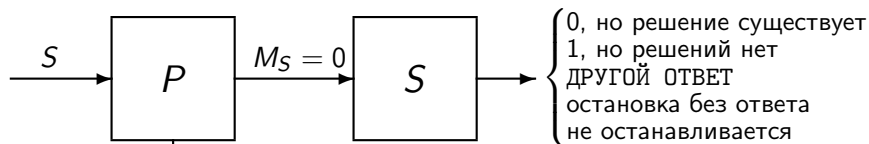
Усовершенствованная программа профессора



Усовершенствованная программа профессора



Усовершенствованная программа профессора



Доказательство того, что:

- ▶ если S выдает 0, то уравнение $M_S = 0$ имеет решение
- ▶ если S выдает 1, то уравнение $M_S = 0$ решений не имеет

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Можно также ограничиться только решениями в положительных целых числах или только в неотрицательных целых числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

$$M(x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Можно также ограничиться только решениями в положительных целых числах или только в неотрицательных целых числах

Натуральные числа против целых

$$(x + 1)^3 + (y + 1)^3 = (z + 1)^3$$

Натуральные числа против целых

$$(x + 1)^3 + (y + 1)^3 = (z + 1)^3$$

Имеет ли это уравнение решение в целых числах?

Натуральные числа против целых

$$(x + 1)^3 + (y + 1)^3 = (z + 1)^3$$

Имеет ли это уравнение решение в целых числах?

Да, и это тривиально: $y = -1$, $z = x$.

Натуральные числа против целых

$$(x + 1)^3 + (y + 1)^3 = (z + 1)^3$$

Имеет ли это уравнение решение в целых числах?

Да, и это тривиально: $y = -1$, $z = x$.

Имеет ли это уравнение решение в неотрицательных целых числах?

Натуральные числа против целых

$$(x + 1)^3 + (y + 1)^3 = (z + 1)^3$$

Имеет ли это уравнение решение в целых числах?

Да, и это тривиально: $y = -1$, $z = x$.

Имеет ли это уравнение решение в неотрицательных целых числах?

Нет, не имеет, но это нетривиально (частный случай Великой теоремы Ферма).

От целых чисел к натуральным

Диофантово уравнение

$$P(x_1, \dots, x_m) = 0$$

имеет решение в целых числах $x_1, \dots, x_m$ тогда и только тогда, когда диофантово уравнение

$$P(p_1 - q_1, \dots, p_m - q_m) = 0.$$

имеет решение в натуральных числах $p_1, \dots, p_m, q_1, \dots, q_m$.

От целых чисел к натуральным

Диофантово уравнение

$$P(x_1, \dots, x_m) = 0$$

имеет решение в целых числах $x_1, \dots, x_m$ тогда и только тогда, когда диофантово уравнение

$$P(p_1 - q_1, \dots, p_m - q_m) = 0.$$

имеет решение в натуральных числах $p_1, \dots, p_m, q_1, \dots, q_m$.

Говорят, что массовая проблема распознавания разрешимости диофантовых уравнений в целых числах **сводится** к массовой проблеме распознавания разрешимости диофантовых уравнений в натуральных числах.

От натуральных чисел к целым

Диофантово уравнение

$$P(p_1, \dots, p_m) = 0$$

имеет решение в натуральных числах тогда и только тогда, когда диофантово уравнение

$$P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \dots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0.$$

имеет решение в целых числах.

От натуральных чисел к целым

Диофантово уравнение

$$P(p_1, \dots, p_m) = 0$$

имеет решение в натуральных числах тогда и только тогда, когда диофантово уравнение

$$P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \dots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0.$$

имеет решение в целых числах.

Теорема (Joseph-Louis Lagrange [1770], знал и Pierre Fermat, но не опубликовал) *Каждое натуральное число является суммой четырех квадратов.*

От натуральных чисел к целым

Диофантово уравнение

$$P(p_1, \dots, p_m) = 0$$

имеет решение в натуральных числах тогда и только тогда, когда диофантово уравнение

$$P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \dots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0.$$

имеет решение в целых числах.

Теорема (Joseph-Louis Lagrange [1770], знал и Pierre Fermat, но не опубликовал) *Каждое натуральное число является суммой четырех квадратов.*

Таким образом, массовая проблема распознавания разрешимости диофантовых уравнений в натуральных целых числах **сводится к** массовой проблеме распознавания разрешимости диофантовых уравнений в целых числах.

Натуральные числа против целых

У нас есть два сведения:

- ▶ массовая проблема распознавания разрешимости диофантовых уравнений в целых числах **сводится** к массовой проблеме распознавания разрешимости диофантовых уравнений в натуральных числах.
- ▶ массовая проблема распознавания разрешимости диофантовых уравнений в натуральных целых числах **сводится к** массовой проблеме распознавания разрешимости диофантовых уравнений в целых числах.

Натуральные числа против целых

У нас есть два сведения:

- ▶ массовая проблема распознавания разрешимости диофантовых уравнений в целых числах **сводится** к массовой проблеме распознавания разрешимости диофантовых уравнений в натуральных числах.
- ▶ массовая проблема распознавания разрешимости диофантовых уравнений в натуральных целых числах **сводится к** массовой проблеме распознавания разрешимости диофантовых уравнений в целых числах.

Таким образом, массовая проблема распознавания разрешимости диофантовых уравнений в целых числах **эквивалентна** массовой проблеме распознавания разрешимости диофантовых уравнений в натуральных числах.

Натуральные числа против целых

У нас есть два сведения:

- ▶ массовая проблема распознавания разрешимости диофантовых уравнений в целых числах **сводится** к массовой проблеме распознавания разрешимости диофантовых уравнений в натуральных числах.
- ▶ массовая проблема распознавания разрешимости диофантовых уравнений в натуральных целых числах **сводится к** массовой проблеме распознавания разрешимости диофантовых уравнений в целых числах.

Таким образом, массовая проблема распознавания разрешимости диофантовых уравнений в целых числах **эквивалентна** массовой проблеме распознавания разрешимости диофантовых уравнений в натуральных числах.

Мы будем заниматься решением уравнений в **натуральных числах** $0, 1, 2, \dots$

Давид Гильберт, “Математические проблемы”, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и **целыми рациональными** коэффициентами; требуется указать *общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет.*

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \dots, a_n, x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которого разделены на две группы:

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \dots, a_n, x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которого разделены на две группы:

- ▶ параметры $a_1, \dots, a_n$;

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \dots, a_n, x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которого разделены на две группы:

- ▶ **параметры** $a_1, \dots, a_n$;
- ▶ **неизвестные** $x_1, \dots, x_m$.

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \dots, a_n, x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которого разделены на две группы:

- ▶ **параметры** $a_1, \dots, a_n$;
- ▶ **неизвестные** $x_1, \dots, x_m$.

Рассмотрим множество $\mathcal{M}$ такое, что

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{ M(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \}.$$

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \dots, a_n, x_1, \dots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которого разделены на две группы:

- ▶ **параметры** $a_1, \dots, a_n$;
- ▶ **неизвестные** $x_1, \dots, x_m$.

Рассмотрим множество $\mathcal{M}$ такое, что

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{ M(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \}.$$

Множества, имеющие такие *представления* называются **диофантовыми**.

Примеры диофантовых множеств

Примеры диофантовых множеств

- ▶ Множество всех полных квадратов, представлено уравнением

Примеры диофантовых множеств

- ▶ Множество всех полных квадратов, представлено уравнением

$$a - x^2 = 0$$

Примеры диофантовых множеств

- ▶ Множество всех полных квадратов, представлено уравнением

$$a - x^2 = 0$$

- ▶ Множество всех составных чисел, представлено уравнением

Примеры диофантовых множеств

- ▶ Множество всех полных квадратов, представлено уравнением

$$a - x^2 = 0$$

- ▶ Множество всех составных чисел, представлено уравнением

$$a - (x_1 + 2)(x_2 + 2) = 0$$

Примеры диофантовых множеств

- ▶ Множество всех полных квадратов, представлено уравнением

$$a - x^2 = 0$$

- ▶ Множество всех составных чисел, представлено уравнением

$$a - (x_1 + 2)(x_2 + 2) = 0$$

- ▶ Множество всех нестепеней числа 2, представлено уравнением

Примеры диофантовых множеств

- ▶ Множество всех полных квадратов, представлено уравнением

$$a - x^2 = 0$$

- ▶ Множество всех составных чисел, представлено уравнением

$$a - (x_1 + 2)(x_2 + 2) = 0$$

- ▶ Множество всех нестепеней числа 2, представлено уравнением

$$a - (2x_1 + 3)x_2 = 0$$

Программа Диофанта

Программа Диофанта

$$\exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$

Программа Диофанта

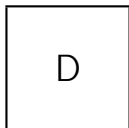
$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$

Программа Диофанта

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$

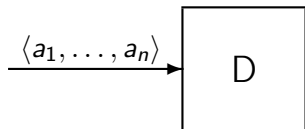
Программа Диофанта

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$



Программа Диофанта

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$



Программа Диофанта

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$



Программа Диофанта

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$

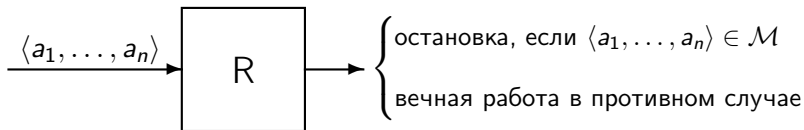


```
for (y=0;;y++)  
  for (x1=0;x1<y;x1++)  
    .....  
    for (xm=0;xm<y;xm++)  
      if (P(a1,...,an,x1,...,xm)=0) STOP
```

Перечислимые множества

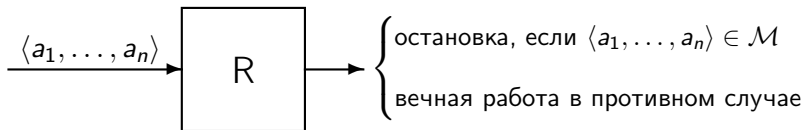
Перечислимые множества

Определение. Множество $\mathcal{M}$, состоящее из n -ок натуральных чисел называется **перечислимым**, если можно написать программу R , такую что



Перечислимые множества

Определение. Множество $\mathcal{M}$, состоящее из n -ок натуральных чисел называется **перечислимым**, если можно написать программу R , такую что



Эквивалентное определение. Множество $\mathcal{M}$, состоящее из n -ок натуральных чисел называется **перечислимым**, если можно написать программу P которая (работая бесконечно долго) будет печатать только элементы множества $\mathcal{M}$ и напечатает каждое из них, быть может, много раз.

Вторая программа Диофанта

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$

Вторая программа Диофанта

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff \exists x_1 \dots x_m \{ P(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \}$$

```
for (y=0;;y++)
  for (a1=0;a1<y;a1++)
    .....
    for (an=0;an<y;an++)
      for (x1=0;x1<y;x1++)
        .....
        for (xm=0;xm<y;xm++)
          if (P(a1,...,an,x1,...,xm)=0)
            print(a1,...,an)
```

Пример

$$P(a_1, x_1, x_2) = a_1 - (x_1 + 2)(x_2 + 2)$$

Пример

$$P(a_1, x_1, x_2) = a_1 - (x_1 + 2)(x_2 + 2)$$

```
for y do
  for a1 to y do
    for x1 to y do
      for x2 to y do
        if a1 - (x1 + 2)*(x2 + 2)=0 then
          print(a1) fi
        od od od od
```

Пример

$$P(a_1, x_1, x_2) = a_1 - (x_1 + 2)(x_2 + 2)$$

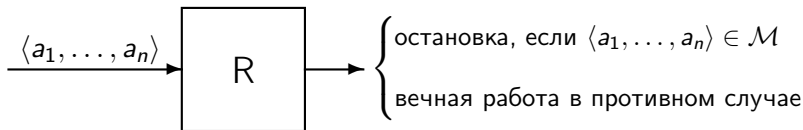
```
for y do
  for a1 to y do
    for x1 to y do
      for x2 to y do
        if a1 - (x1 + 2)*(x2 + 2)=0 then
          print(a1) fi
        od od od od
```

4, 4, 4, 6, 6, 4, 6, 6, 4, 6, 6, 8, 8, 4, 6, 6, 8, 8, 9, 4, 6, 6, 8, 8, 9,
10, 10, 4, 6, 6, 8, 8, 9, 10, 10, 4, 6, 6, 8, 8, 9, 10, 10, 12, 12, 12,
12, 4, 6, 6, ...

Перечислимые множества

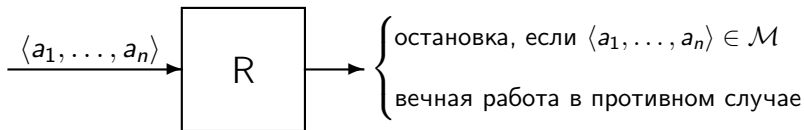
Перечислимые множества

Определение. Множество $\mathcal{M}$, состоящее из n -ок натуральных чисел называется **перечислимым**, если можно написать программу R , такую что



Перечислимые множества

Определение. Множество $\mathcal{M}$, состоящее из n -ок натуральных чисел называется **перечислимым**, если можно написать программу R , такую что



Эквивалентное определение. Множество $\mathcal{M}$, состоящее из n -ок натуральных чисел называется **перечислимым**, если можно написать программу P которая (работая бесконечно долго) будет печатать только элементы множества $\mathcal{M}$ и напечатает каждое из них, быть может, много раз.

Гипотеза Martin'a Davis'a

Гипотеза Martin'a Davis'a

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Гипотеза Martin'a Davis'a

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Гипотеза М. Davis'а (начало 50-х). *Каждое перечислимое множество является диофантовым.*

Гипотеза Martin'a Davis'a

Тривиальный факт. Каждое диофантово множество является перечислимым.

Гипотеза М. Davis'a (начало 50-х). Каждое перечислимое множество является диофантовым.

Гипотеза М. Davis'a была доказана в 1970 году.

DPRM-теорема. Понятия *перечислимое множество* и *диофантово множество* совпадают.

Гипотеза Martin'a Davis'a

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Гипотеза М. Davis'a (начало 50-х). *Каждое перечислимое множество является диофантовым.*

Гипотеза М. Davis'a была доказана в 1970 году.

DPRM-теорема. *Понятия перечислимое множество и диофантово множество совпадают.*

Martin Davis, Hilary Putnam, Julia Robinson, Юрий Матиясевич

Перечисление диофантовых уравнений

$$M_1(a, \bar{x}) = 0, \quad \dots, \quad M_k(a, \bar{x}) = 0, \quad \dots$$

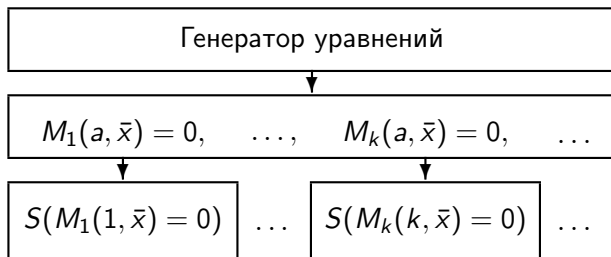
Программа профессора

Генератор уравнений

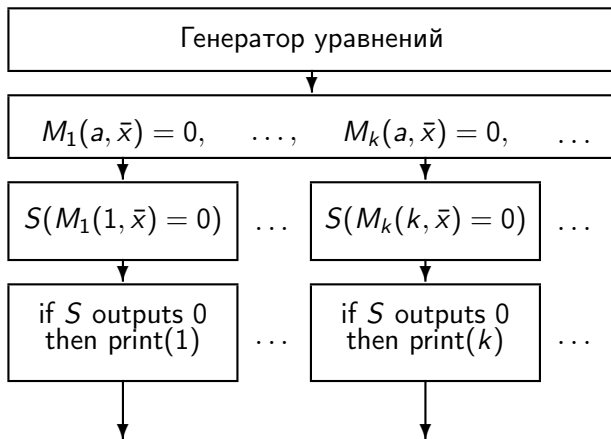


$$M_1(a, \bar{x}) = 0, \quad \dots, \quad M_k(a, \bar{x}) = 0, \quad \dots$$

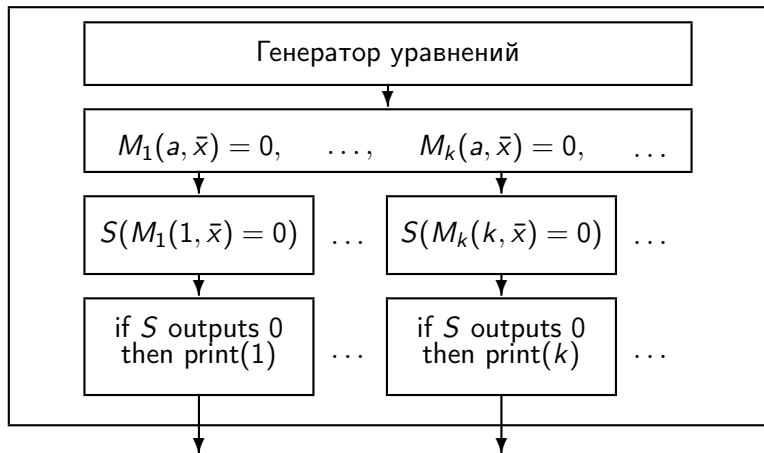
Программа профессора



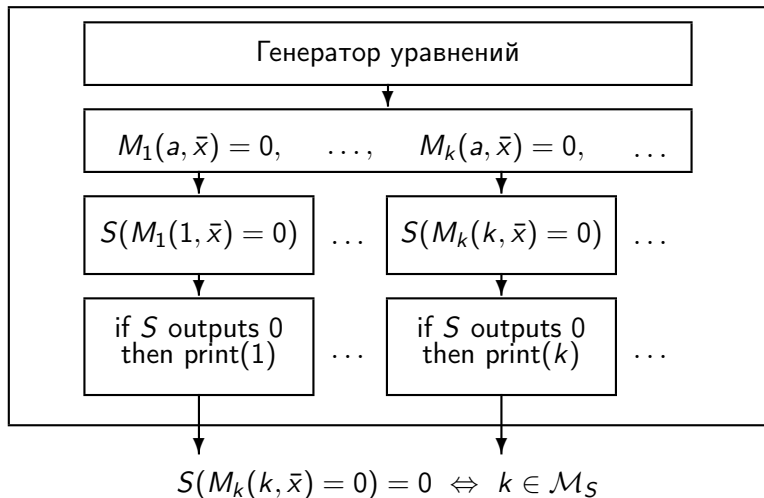
Программа профессора



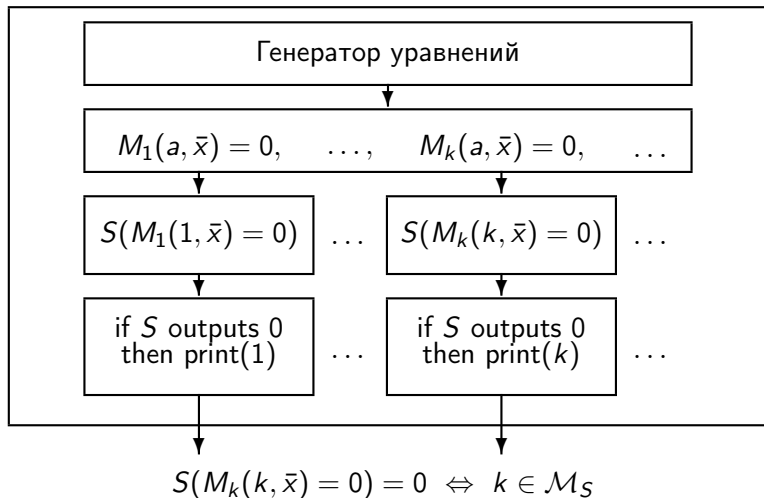
Программа профессора



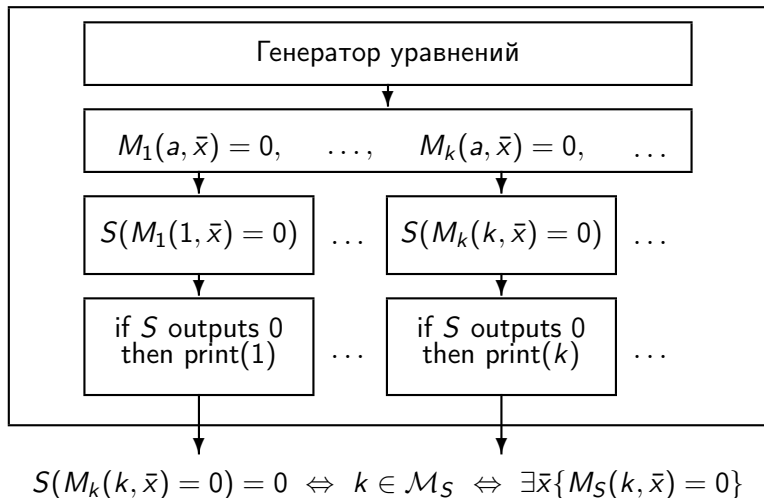
Программа профессора



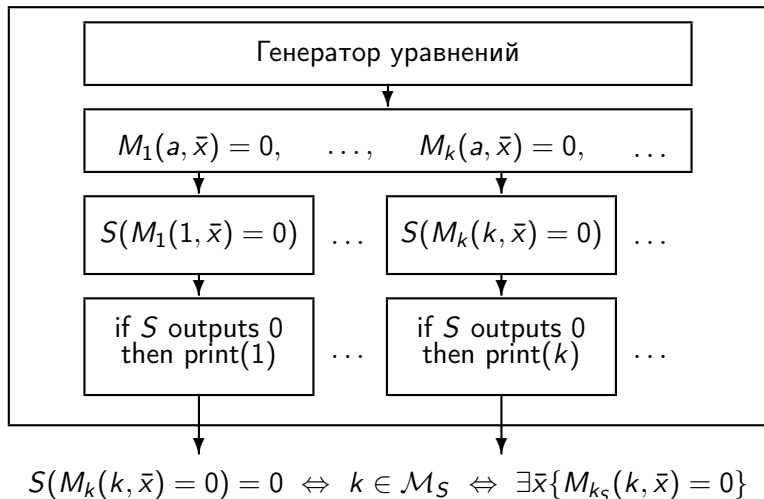
Программа профессора



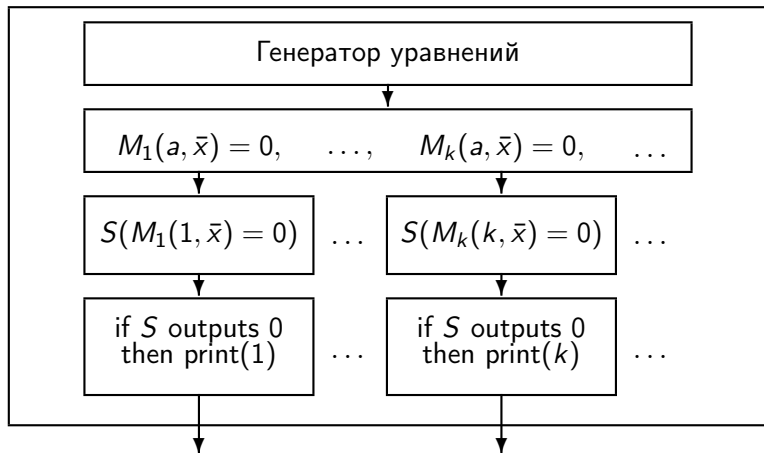
Программа профессора



Программа профессора



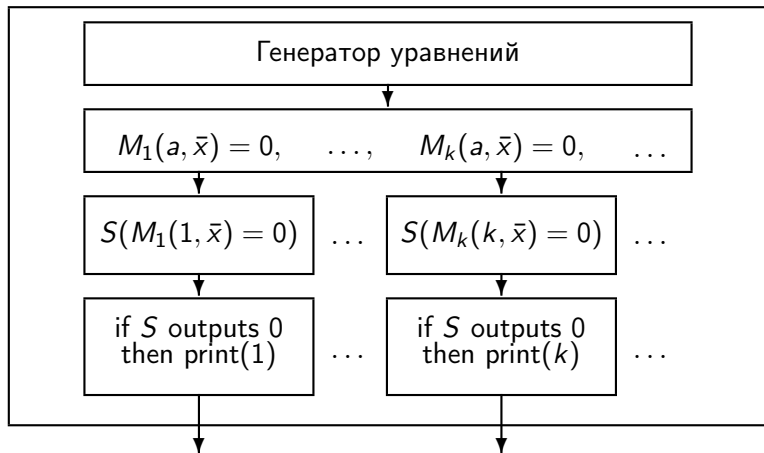
Программа профессора



$$S(M_k(k, \bar{x}) = 0) = 0 \Leftrightarrow k \in \mathcal{M}_S \Leftrightarrow \exists \bar{x} \{M_{k_S}(k, \bar{x}) = 0\}$$

$$S(M_{k_S}(k_S, \bar{x}) = 0)$$

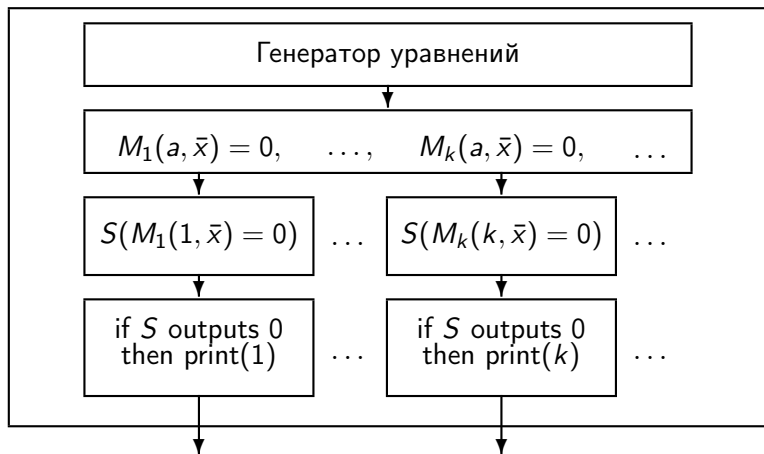
Программа профессора



$$S(M_k(k, \bar{x}) = 0) = 0 \Leftrightarrow k \in \mathcal{M}_S \Leftrightarrow \exists \bar{x} \{M_{k_S}(k, \bar{x}) = 0\}$$

$$S(M_{k_S}(k_S, \bar{x}) = 0) = ?$$

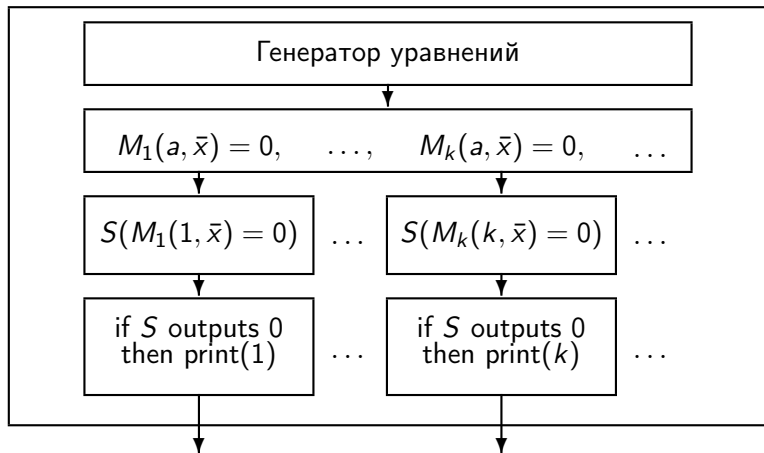
Программа профессора



$$S(M_k(k, \bar{x}) = 0) = 0 \Leftrightarrow k \in \mathcal{M}_S \Leftrightarrow \exists \bar{x} \{M_{k_S}(k, \bar{x}) = 0\}$$

$$S(M_{k_S}(k_S, \bar{x}) = 0) = 0$$

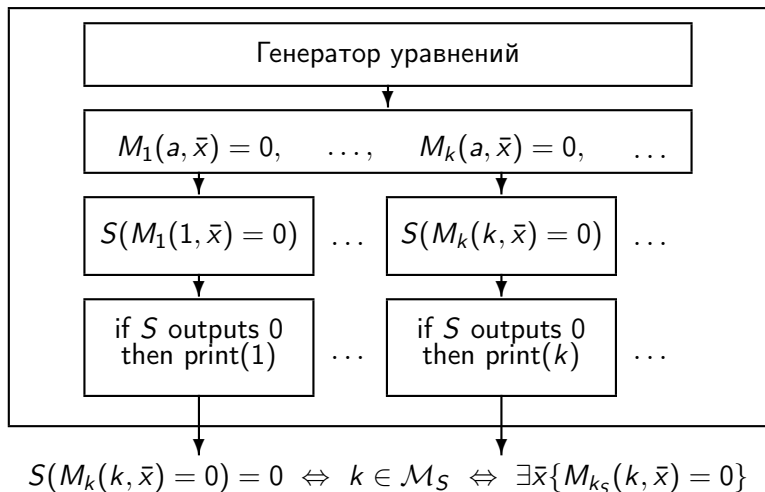
Программа профессора



$$S(M_k(k, \bar{x}) = 0) = 0 \Leftrightarrow k \in \mathcal{M}_S \Leftrightarrow \exists \bar{x} \{M_{k_S}(k, \bar{x}) = 0\}$$

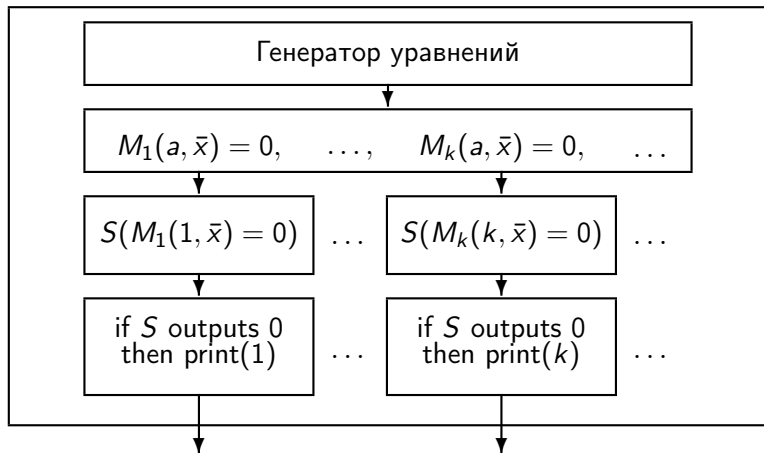
$$S(M_{k_S}(k_S, \bar{x}) = 0) = 0 \Rightarrow k_S \in \mathcal{M}_S$$

Программа профессора



$$S(M_{k_S}(k_S, \bar{x}) = 0) = 0 \Rightarrow k_S \in \mathcal{M}_S \Rightarrow \exists \bar{x} \{M_{k_S}(k_S, \bar{x}) = 0\}$$

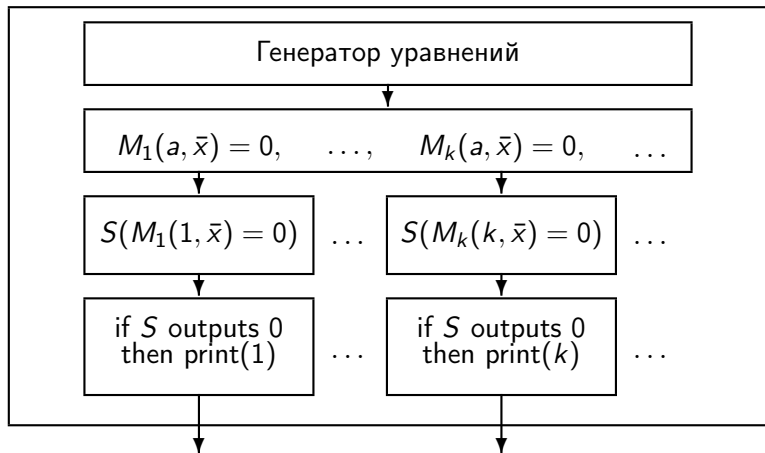
Программа профессора



$$S(M_k(k, \bar{x}) = 0) = 0 \Leftrightarrow k \in \mathcal{M}_S \Leftrightarrow \exists \bar{x} \{M_{k_S}(k, \bar{x}) = 0\}$$

$$S(M_{k_S}(k_S, \bar{x}) = 0) = 1$$

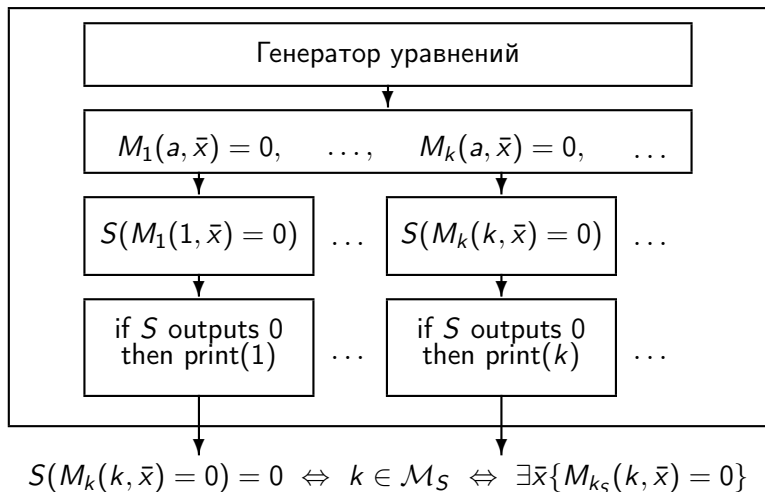
Программа профессора



$$S(M_k(k, \bar{x}) = 0) = 0 \Leftrightarrow k \in \mathcal{M}_S \Leftrightarrow \exists \bar{x} \{M_{k_S}(k, \bar{x}) = 0\}$$

$$S(M_{k_S}(k_S, \bar{x}) = 0) = 1 \Rightarrow k_S \notin \mathcal{M}_S$$

Программа профессора



$$S(M_{k_S}(k_S, \bar{x}) = 0) = 1 \Rightarrow k_S \notin \mathcal{M}_S \Rightarrow \neg \exists \bar{x} \{M_{k_S}(k_S, \bar{x}) = 0\}$$

Универсальное уравнение

Универсальное уравнение

Список всех однопараметрических уравнений:

$$M_1(a, x_1, \dots) = 0, \dots, M_k(a, x_1, \dots) = 0, \dots$$

Универсальное уравнение

Список всех однопараметрических уравнений:

$$M_1(a, x_1, \dots) = 0, \dots, M_k(a, x_1, \dots) = 0, \dots$$

$$\langle a, k \rangle \in \mathfrak{U} \Leftrightarrow \exists x_1, \dots \{M_k(a, x_1, \dots) = 0\}$$

Универсальное уравнение

Список всех однопараметрических уравнений:

$$M_1(a, x_1, \dots) = 0, \dots, M_k(a, x_1, \dots) = 0, \dots$$

$$\langle a, k \rangle \in \mathfrak{U} \Leftrightarrow \exists x_1, \dots \{M_k(a, x_1, \dots) = 0\}$$

$$\langle a, k \rangle \in \mathfrak{U} \Leftrightarrow \exists y_1 \dots y_n \{U(a, k, y_1, \dots, y_n) = 0\}$$

Универсальное уравнение

Список всех однопараметрических уравнений:

$$M_1(a, x_1, \dots) = 0, \dots, M_k(a, x_1, \dots) = 0, \dots$$

$$\langle a, k \rangle \in \mathfrak{U} \Leftrightarrow \exists x_1, \dots \{M_k(a, x_1, \dots) = 0\}$$

$$\langle a, k \rangle \in \mathfrak{U} \Leftrightarrow \exists y_1 \dots y_n \{U(a, k, y_1, \dots, y_n) = 0\}$$

$$\exists x_1, \dots \{M_k(a, x_1, \dots) = 0\} \Leftrightarrow \exists y_1 \dots y_n \{U(a, k, y_1, \dots, y_n) = 0\}$$

Текущие рекорды

Задача о решении произвольного параметрического диофантова уравнения может быть сведена к решению эквивалентного диофантова уравнения, имеющего степень D и N неизвестных, где в качестве $\langle D, N \rangle$ можно взять любую из следующих пар:

$\langle 4, 58 \rangle, \langle 8, 38 \rangle, \langle 12, 32 \rangle, \langle 16, 29 \rangle, \langle 20, 28 \rangle, \langle 24, 26 \rangle, \langle 28, 25 \rangle, \langle 36, 24 \rangle,$
 $\langle 96, 21 \rangle, \langle 2668, 19 \rangle, \langle 2 \times 10^5, 14 \rangle, \langle 6.6 \times 10^{43}, 13 \rangle, \langle 1.3 \times 10^{44}, 12 \rangle,$
 $\langle 4.6 \times 10^{44}, 11 \rangle, \langle 8.6 \times 10^{44}, 10 \rangle, \langle 1.6 \times 10^{45}, 9 \rangle.$

Непростой многочлен для простых чисел

Теорема (J.P.Jones, D.Sato, H.Wada, D.Wiens, [1976])

Множество всех простых чисел – это в точности множество всех положительных значений, принимаемых многочленом

$$(k+2) \{ \begin{aligned} &1 - [wz + h + j - q]^2 \\ &- [(gk + 2g + k + 1)(h + j) + h - z]^2 \\ &- [2n + p + q + z - e]^2 \\ &- [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 \\ &- [e^3(e+2)(a+1)^2 + 1 - o^2]^2 \\ &- [(a^2 - 1)y^2 + 1 - x^2]^2 \\ &- [16r^2y^4(a^2 - 1) + 1 - u^2]^2 - [n + l + v - y]^2 \\ &- [((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 \\ &- [(a^2 - 1)l^2 + 1 - m^2]^2 \\ &- [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 \\ &- [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2 \\ &- [ai + k + 1 - l - i]^2 \\ &- [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \} \end{aligned}$$

при натуральных значениях 26 переменных $a, b, c, \dots, x, y, z$.

Диофантовы машины

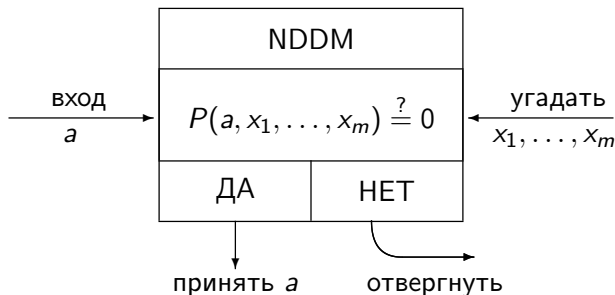
Формализация недетерминизма

Leonard Adleman и Kenneth Manders [1976] ввели понятие **недетерминированной диофантовой машины**, NDDM .

Диофантовы машины

Формализация недетерминизма

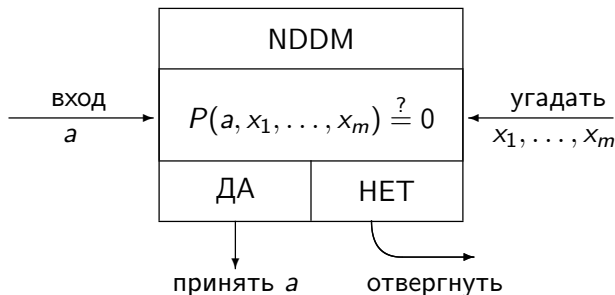
Leonard Adleman и Kenneth Manders [1976] ввели понятие **недетерминированной диофантовой машины**, NDDM .



Диофантовы машины

Формализация недетерминизма

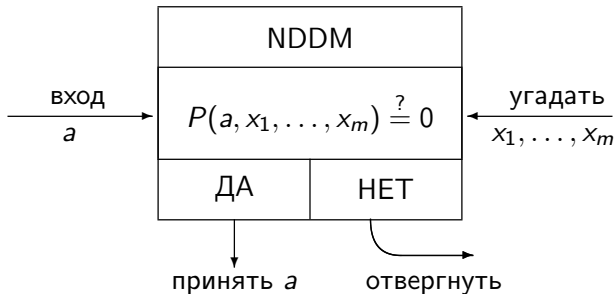
Leonard Adleman и Kenneth Manders [1976] ввели понятие **недетерминированной диофантовой машины**, NDDM .



DPRM-теорема: NDDM имеют такую же вычислительную силу как, например, машины Тьюринга, то есть любое множество, принимаемое некоторой машиной Тьюринга, принимается некоторой NDDM, и, очевидно, наоборот.

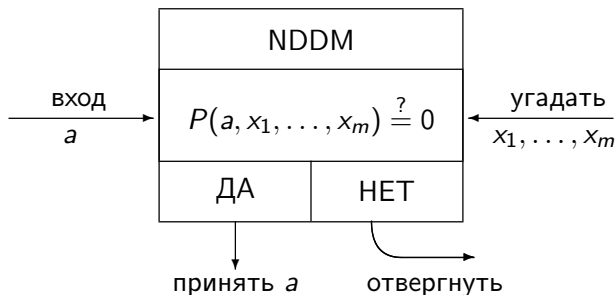
Диофантова сложность

Определения



Диофантова сложность

Определения



$\text{SIZE}(a)$ = минимально возможное значение $|x_1| + \dots + |x_m|$, где $|x|$ обозначает длину двоичной записи x .

Диофантова сложность

D vs NP

Leonard Adleman и Kenneth Manders [1975] ввели в рассмотрение класс **D** состоящий из множеств $\mathcal{M}$ имеющих представления вида

$$a \in \mathcal{M} \iff$$

$$\iff \exists x_1 \dots x_m [P(a, x_1, \dots, x_m) = 0 \ \& \ |x_1| + \dots + |x_m| \leq |a|^k].$$

Диофантова сложность

D vs NP

Leonard Adleman и Kenneth Manders [1975] ввели в рассмотрение класс **D** состоящий из множеств $\mathcal{M}$ имеющих представления вида

$$a \in \mathcal{M} \iff$$

$$\iff \exists x_1 \dots x_m [P(a, x_1, \dots, x_m) = 0 \ \& \ |x_1| + \dots + |x_m| \leq |a|^k].$$

Открытая проблема. $\mathbf{D} \stackrel{?}{=} \mathbf{NP}$.

Давид Гильберт, *“Математические проблемы”*, [1900]

Вместе с тем бывает и так, что мы добиваемся ответа при недостаточных предпосылках, или идя в неправильном направлении, и вследствие этого не достигаем цели. Тогда возникает задача доказать неразрешимость данной проблемы при принятых предпосылках и выбранном направлении. Такие доказательства невозможности проводились еще старыми математиками, например, когда они обнаруживали, что отношение гипотенузы равнобедренного прямоугольного треугольника к его катету есть иррациональное число. В новейшей математике доказательства невозможности решений определенных проблем играют выдающуюся роль; там мы констатируем, что такие старые и трудные проблемы, как доказательство аксиомы о параллельных, как квадратура круга или решение уравнения пятой степени в радикалах, получили все же строгое, вполне удовлетворяющее нас решение, хотя и в другом направлении, чем то, которое сначала предполагалось.

Этот удивительный факт наряду с другими философскими основаниями создает у нас уверенность, которую разделяет, несомненно, каждый математик, но которую до сих пор никто не подтвердил доказательством, — уверенность в том, что каждая определенная математическая проблема непременно должна быть доступна строгому решению или в том смысле, что удастся получить ответ на поставленный вопрос, или же в том смысле, что будет установлена невозможность ее решения и вместе с тем доказана неизбежность неудачи всех попыток ее решить.

DPR-теорема

DPR-теорема

Теорема (Martin Davis, Hilary Putnam, Julia Robinson [1961]). Для каждого перечислимого множества можно построить его экспоненциально диофантово представление:

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff$$

$$\exists x_1 \dots x_m \{ E_L(a_1, \dots, a_n, x_1, \dots, x_m) = E_R(a_1, \dots, a_n, x_1, \dots, x_m) \}$$

где E_L и E_R – выражения, построенные по традиционным правилам из переменных и конкретных натуральных чисел с помощью операций сложения, умножения и **возведения в степень**.

DPR-теорема

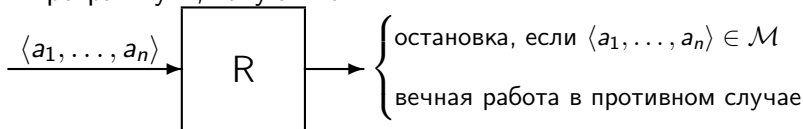
Теорема (Martin Davis, Hilary Putnam, Julia Robinson [1961]). Для каждого перечислимого множества можно построить его **экспоненциально диофантово представление**:

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff$$

$$\exists x_1 \dots x_m \{ E_L(a_1, \dots, a_n, x_1, \dots, x_m) = E_R(a_1, \dots, a_n, x_1, \dots, x_m) \}$$

где E_L и E_R – выражения, построенные по традиционным правилам из переменных и конкретных натуральных чисел с помощью операций сложения, умножения и **возведения в степень**.

Определение. Множество $\mathcal{M}$, состоящее из n -ок натуральных чисел называется **перечислимым**, если можно написать программу R , такую что



DPR-теорема

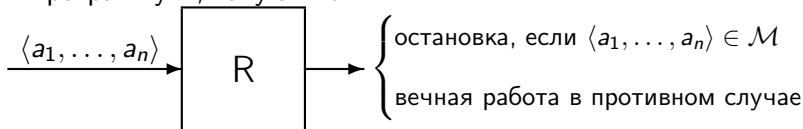
Теорема (Martin Davis, Hilary Putnam, Julia Robinson [1961]). Для каждого перечислимого множества можно построить его **экспоненциально диофантово представление**:

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \iff$$

$$\exists x_1 \dots x_m \{ E_L(a_1, \dots, a_n, x_1, \dots, x_m) = E_R(a_1, \dots, a_n, x_1, \dots, x_m) \}$$

где E_L и E_R – выражения, построенные по традиционным правилам из переменных и конкретных натуральных чисел с помощью операций сложения, умножения и **возведения в степень**.

Определение. Множество $\mathcal{M}$, состоящее из n -ок натуральных чисел называется **перечислимым**, если можно написать программу R , такую что



An e-mail

An e-mail

Dear Professor,

you are wrong. I am a brilliant young programmer and last night I wrote a sophisticated program in `Java##`. My program solves Hilbert's tenth problem in the `__positive__` sense. Namely, for every Diophantine equation given as input, the program will print 1 or 0 depending on whether the equation has a solution or not.

The attachment contains my ingenious program. You can run it on your favorite Diophantine equations and see how fast my program works.

Have a fun, Professor!

Регистровые машины

Регистровые машины

Регистровая машина имеет конечное количество **регистров** $R_1, \dots, R_n$ каждый из которых может содержать произвольно большое натуральное число.

Регистровые машины

Регистровая машина имеет конечное количество **регистров** $R_1, \dots, R_n$ каждый из которых может содержать произвольно большое натуральное число. Машина выполняет **программу** состоящую из конечного числа **инструкций** снабженных **метками** $S_1, \dots, S_m$. Когда машина выполняет инструкцию с меткой S_k , мы говорим, что машина находится в **состоянии** S_k .

Регистровые машины

Регистровая машина имеет конечное количество **регистров** $R_1, \dots, R_n$ каждый из которых может содержать произвольно большое натуральное число. Машина выполняет **программу** состоящую из конечного числа **инструкций** снабженных **метками** $S_1, \dots, S_m$. Когда машина выполняет инструкцию с меткой S_k , мы говорим, что машина находится в **состоянии** S_k .

Инструкции бывают трёх типов:

Регистровые машины

Регистровая машина имеет конечное количество **регистров** $R_1, \dots, R_n$ каждый из которых может содержать произвольно большое натуральное число. Машина выполняет **программу** состоящую из конечного числа **инструкций** снабженных **метками** $S_1, \dots, S_m$. Когда машина выполняет инструкцию с меткой S_k , мы говорим, что машина находится в **состоянии** S_k .

Инструкции бывают трёх типов:

I. $S_k: R_\ell + +; S_i$

Регистровые машины

Регистровая машина имеет конечное количество **регистров** $R_1, \dots, R_n$ каждый из которых может содержать произвольно большое натуральное число. Машина выполняет **программу** состоящую из конечного числа **инструкций** снабженных **метками** $S_1, \dots, S_m$. Когда машина выполняет инструкцию с меткой S_k , мы говорим, что машина находится в **состоянии** S_k .

Инструкции бывают трёх типов:

- I. $S_k: R_\ell + +; S_i$
- II. $S_k: R_\ell - -; S_i; S_j$

Регистровые машины

Регистровая машина имеет конечное количество **регистров** $R_1, \dots, R_n$ каждый из которых может содержать произвольно большое натуральное число. Машина выполняет **программу** состоящую из конечного числа **инструкций** снабженных **метками** $S_1, \dots, S_m$. Когда машина выполняет инструкцию с меткой S_k , мы говорим, что машина находится в **состоянии** S_k .

Инструкции бывают трёх типов:

- I. $S_k: R_\ell + +; S_i$
- II. $S_k: R_\ell - -; S_i; S_j$
- III. $S_k: \text{STOP}$

Регистровые машины

Регистровая машина имеет конечное количество **регистров** $R_1, \dots, R_n$ каждый из которых может содержать произвольно большое натуральное число. Машина выполняет **программу** состоящую из конечного числа **инструкций** снабженных **метками** $S_1, \dots, S_m$. Когда машина выполняет инструкцию с меткой S_k , мы говорим, что машина находится в **состоянии** S_k .

Инструкции бывают трёх типов:

- I. $S_k: R_\ell + +; S_i$
- II. $S_k: R_\ell - -; S_i; S_j$
- III. $S_k: \text{STOP}$

Lambek [1961], Melzak [1961], Minsky [1961], Minsky [1967],
Shepherdson и Sturgis [1963]

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

Начальное состояние S1

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

Начальное состояние S1

Начальное содержимое регистров R1=a, R2=0

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

Начальное состояние S1

Начальное содержимое регистров R1=a, R2=0

В каком случае машина остановится?

Протокол

Протокол

	q	$\dots$	$t + 1$	t	$\dots$	0
S_1	$s_{1,q}$	$\dots$	$s_{1,t+1}$	$s_{1,t}$	$\dots$	$s_{1,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_k	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_m	$s_{m,q}$	$\dots$	$s_{m,t+1}$	$s_{m,t}$	$\dots$	$s_{m,0}$

$$s_{k,t} = \begin{cases} 1, & \text{если на шаге } t \text{ машина была в состоянии } k \\ 0 & \text{в противном случае} \end{cases}$$

Протокол

	q	$\dots$	$t + 1$	t	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_k	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R1	$r_{1,q}$	$\dots$	$r_{1,t+1}$	$r_{1,t}$	$\dots$	$r_{1,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R ℓ	$r_{\ell,q}$	$\dots$	$r_{\ell,t+1}$	$r_{\ell,t}$	$\dots$	$r_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R n	$r_{n,q}$	$\dots$	$r_{n,t+1}$	$r_{n,t}$	$\dots$	$r_{n,0}$

$r_{\ell,t}$ – это содержимое ℓ -го регистра на шаге t

Протокол

	q	$\dots$	$t + 1$	t	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Sk	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$R\ell$	$r_{\ell,q}$	$\dots$	$r_{\ell,t+1}$	$r_{\ell,t}$	$\dots$	$r_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_1	$z_{1,q}$	$\dots$	$z_{1,t+1}$	$z_{1,t}$	$\dots$	$z_{1,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_ℓ	$z_{\ell,q}$	$\dots$	$z_{\ell,t+1}$	$z_{\ell,t}$	$\dots$	$z_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_n	$z_{n,q}$	$\dots$	$z_{n,t+1}$	$z_{n,t}$	$\dots$	$z_{n,0}$

$$z_{\ell,t} = \begin{cases} 1, & \text{если } r_{\ell,t} > 0 \\ 0 & \text{в противном случае} \end{cases}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$r_{1,t+1} =$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t}$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} = (1 - z_{1,t})s_{2,t}$$

$$s_{1,0} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} = (1 - z_{1,t})s_{2,t}$$

$$s_{1,0} = 1$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} = (1 - z_{1,t})s_{2,t}$$

$$s_{1,0} = 1 \quad s_{2,0} = \dots = s_{m,0} = 0$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} = (1 - z_{1,t})s_{2,t}$$

$$s_{1,0} = 1 \quad s_{2,0} = \dots = s_{m,0} = 0$$

$$r_{1,0} =$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} = (1 - z_{1,t})s_{2,t}$$

$$s_{1,0} = 1 \quad s_{2,0} = \dots = s_{m,0} = 0$$

$$r_{1,0} = a$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} = (1 - z_{1,t})s_{2,t}$$

$$s_{1,0} = 1 \quad s_{2,0} = \dots = s_{m,0} = 0$$

$$r_{1,0} = a \quad r_{2,0} = \dots = r_{n,0} = 0$$

$$s_{m,q} = 1$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} = (1 - z_{1,t})s_{2,t}$$

$$s_{1,0} = 1 \quad s_{2,0} = \dots = s_{m,0} = 0$$

$$r_{1,0} = a \quad r_{2,0} = \dots = r_{n,0} = 0$$

$$s_{m,q} = 1 \quad s_{1,q} = \dots = s_{m-1,q} = 0$$

Пример

S1:R1--; S2; S8	S4:R1--; S5; S6	S7:R1++; S6
S2:R1--; S3; S9	S5:R1--; S3; S8	S8:R1++; S8
S3:R2++; S4	S6:R2--; S7; S1	S9:STOP

$$r_{1,t+1} = r_{1,t} + s_{7,t} + s_{8,t} - z_{1,t}s_{1,t} - z_{1,t}s_{2,t} - z_{1,t}s_{4,t} - z_{1,t}s_{5,t}$$

$$r_{2,t+1} = r_{2,t} + s_{3,t} - z_{2,t}s_{6,t}$$

$$s_{1,t+1} = (1 - z_{2,t})s_{6,t} \quad s_{2,t+1} = z_{1,t}s_{1,t}$$

$$s_{3,t+1} = z_{1,t}s_{2,t} + z_{1,t}s_{5,t} \quad s_{4,t+1} = s_{3,t} \quad s_{5,t+1} = z_{1,t}s_{4,t}$$

$$s_{6,t+1} = (1 - z_{4,t})s_{4,t} + s_{7,t} \quad s_{7,t+1} = z_{2,t}s_{6,t}$$

$$s_{8,t+1} = (1 - z_{1,t})s_{1,t} + s_{8,t} \quad s_{9,t+1} = (1 - z_{1,t})s_{2,t}$$

$$s_{1,0} = 1 \quad s_{2,0} = \dots = s_{m,0} = 0$$

$$r_{1,0} = a \quad r_{2,0} = \dots = r_{n,0} = 0$$

$$s_{m,q} = 1 \quad s_{1,q} = \dots = s_{m-1,q} = 0$$

Новые значения регистров

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^{+} s_{k,t} - \sum_{\ell}^{-} z_{\ell,t} s_{k,t}$$

Новые значения регистров

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^{+} s_{k,t} - \sum_{\ell}^{-} z_{\ell,t} s_{k,t}$$

где $\sum_{\ell}^{+}$ -суммирование ведется по всем инструкциям вида

$$Sk : R\ell ++; Si,$$

Новые значения регистров

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^{+} s_{k,t} - \sum_{\ell}^{-} z_{\ell,t} s_{k,t}$$

где $\sum_{\ell}^{+}$ -суммирование ведется по всем инструкциям вида

$$Sk : R\ell ++; Si,$$

а $\sum_{\ell}^{-}$ -суммирование – по всем инструкциям вида

$$Sk : R\ell --; Si; Sj.$$

Новые состояния

$$s_{d,t+1} = \sum_d^+ s_{k,t} + \sum_d^- z_{\ell,t} s_{k,t} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t}$$

Новые состояния

$$s_{d,t+1} = \sum_d^+ s_{k,t} + \sum_d^- z_{\ell,t} s_{k,t} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t}$$

где $\sum_d^+$ -суммирование ведется по всем инструкциям вида

$$Sk : R\ell ++; Sd,$$

Новые состояния

$$s_{d,t+1} = \sum_d^+ s_{k,t} + \sum_d^- z_{\ell,t} s_{k,t} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t}$$

где $\sum_d^+$ -суммирование ведется по всем инструкциям вида

$$Sk : R\ell ++; Sd,$$

$\sum_d^-$ -суммирование ведется по всем инструкциям вида

$$Sk : R\ell --; Sd; Sj,$$

Новые состояния

$$s_{d,t+1} = \sum_d^+ s_{k,t} + \sum_d^- z_{\ell,t} s_{k,t} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t}$$

где $\sum_d^+$ -суммирование ведется по всем инструкциям вида

$$Sk : R\ell ++; Sd,$$

$\sum_d^-$ -суммирование ведется по всем инструкциям вида

$$Sk : R\ell --; Sd; Sj,$$

а $\sum_d^0$ -суммирование – по всем инструкциям вида

$$Sk : R\ell --; Si; Sd.$$

Начальные значения

Начальные значения

Всегда начинаем в состоянии S1:

$$s_{1,0} = 1,$$

$$s_{2,0} = \dots = s_{m,0} = 0.$$

Начальные значения

Всегда начинаем в состоянии S1:

$$s_{1,0} = 1,$$

$$s_{2,0} = \dots = s_{m,0} = 0.$$

(Единственная) входная величина a помещается в регистр R1:

$$r_{1,0} = a,$$

Начальные значения

Всегда начинаем в состоянии S1:

$$s_{1,0} = 1,$$

$$s_{2,0} = \dots = s_{m,0} = 0.$$

(Единственная) входная величина a помещается в регистр R1:

$$r_{1,0} = a,$$

все остальные регистры пусты:

$$r_{2,0} = \dots = r_{n,0} = 0.$$

Остановка

S_m является единственной командой STOP:

$$s_{m,q} = 1,$$

$$s_{1,q} = \dots = s_{m-1,q} = 0.$$

При остановке все регистры пусты:

$$r_{1,q} = \dots = r_{n,q} = 0.$$

Протокол

	q	$\dots$	$t+1$	t	$\dots$	0
S_k	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
R_ℓ	$r_{\ell,q}$	$\dots$	$r_{\ell,t+1}$	$r_{\ell,t}$	$\dots$	$r_{\ell,0}$
Z_ℓ	$z_{\ell,q}$	$\dots$	$z_{\ell,t+1}$	$z_{\ell,t}$	$\dots$	$z_{\ell,0}$

Протокол

	q	$\dots$	$t + 1$	t	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_k	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R_ℓ	$r_{\ell,q}$	$\dots$	$r_{\ell,t+1}$	$r_{\ell,t}$	$\dots$	$r_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_ℓ	$z_{\ell,q}$	$\dots$	$z_{\ell,t+1}$	$z_{\ell,t}$	$\dots$	$z_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

$$s_k = \sum_{t=0}^q s_{k,t} b^t$$

Протокол

	q	$\dots$	$t + 1$	t	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_k	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R_ℓ	$r_{\ell,q}$	$\dots$	$r_{\ell,t+1}$	$r_{\ell,t}$	$\dots$	$r_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_ℓ	$z_{\ell,q}$	$\dots$	$z_{\ell,t+1}$	$z_{\ell,t}$	$\dots$	$z_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

$$= s_k = \sum_{t=0}^q s_{k,t} b^t$$

Протокол

	q	$\dots$	$t + 1$	t	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_k	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R_ℓ	$r_{\ell,q}$	$\dots$	$r_{\ell,t+1}$	$r_{\ell,t}$	$\dots$	$r_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_ℓ	$z_{\ell,q}$	$\dots$	$z_{\ell,t+1}$	$z_{\ell,t}$	$\dots$	$z_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

$$= s_k = \sum_{t=0}^q s_{k,t} b^t$$

$$= r_\ell = \sum_{t=0}^q r_{\ell,t} b^t$$

Протокол

	q	$\dots$	$t + 1$	t	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_k	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R_ℓ	$r_{\ell,q}$	$\dots$	$r_{\ell,t+1}$	$r_{\ell,t}$	$\dots$	$r_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_ℓ	$z_{\ell,q}$	$\dots$	$z_{\ell,t+1}$	$z_{\ell,t}$	$\dots$	$z_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

$$= s_k = \sum_{t=0}^q s_{k,t} b^t$$

$$= r_\ell = \sum_{t=0}^q r_{\ell,t} b^t$$

$$= z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

Протокол

	q	$\dots$	$t + 1$	t	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_k	$s_{k,q}$	$\dots$	$s_{k,t+1}$	$s_{k,t}$	$\dots$	$s_{k,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R_ℓ	$r_{\ell,q}$	$\dots$	$r_{\ell,t+1}$	$r_{\ell,t}$	$\dots$	$r_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_ℓ	$z_{\ell,q}$	$\dots$	$z_{\ell,t+1}$	$z_{\ell,t}$	$\dots$	$z_{\ell,0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

$$b = 2^{c+1}$$

$$= s_k = \sum_{t=0}^q s_{k,t} b^t$$

$$= r_\ell = \sum_{t=0}^q r_{\ell,t} b^t$$

$$= z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k$$

$$a \& b = \sum_{k=0}^{\infty} a_k b_k 2^k$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^+ s_{k,t} - \sum_{\ell}^- z_{\ell,t} s_{k,t}$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^+ s_{k,t} - \sum_{\ell}^- z_{\ell,t} s_{k,t}$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^+ s_{k,t} - \sum_{\ell}^- z_{\ell,t} s_{k,t}$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^+ s_{k,t} - \sum_{\ell}^- z_{\ell,t} s_{k,t}$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$r_{\ell,t+1} b^{t+1} = r_{\ell,t} b^{t+1} + \sum_{\ell}^+ s_{k,t} b^{t+1} - \sum_{\ell}^- z_{\ell,t} s_{k,t} b^{t+1}$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$\sum_{t=0}^{q-1} r_{\ell,t+1} b^{t+1} = \sum_{t=0}^{q-1} (r_{\ell,t} b^{t+1} + \sum_{\ell}^+ s_{k,t} b^{t+1} - \sum_{\ell}^- z_{\ell,t} s_{k,t} b^{t+1})$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$\sum_{t=0}^{q-1} r_{\ell,t+1} b^{t+1} = \sum_{t=0}^{q-1} (r_{\ell,t} b^{t+1} + \sum_{\ell}^+ s_{k,t} b^{t+1} - \sum_{\ell}^- z_{\ell,t} s_{k,t} b^{t+1})$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$\sum_{t=0}^{q-1} r_{\ell,t+1} b^{t+1} = \sum_{t=0}^{q-1} (r_{\ell,t} b^{t+1} + \sum_{\ell}^+ s_{k,t} b^{t+1} - \sum_{\ell}^- z_{\ell,t} s_{k,t} b^{t+1})$$

$$r_\ell - r_{\ell,0} = b r_\ell + b \sum_{\ell}^+ s_k - b \sum_{\ell}^- (z_\ell \& s_k)$$

Новые значения регистров

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad r_\ell = \sum_{t=0}^q r_{\ell,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$\sum_{t=0}^{q-1} r_{\ell,t+1} b^{t+1} = \sum_{t=0}^{q-1} (r_{\ell,t} b^{t+1} + \sum_{\ell}^+ s_{k,t} b^{t+1} - \sum_{\ell}^- z_{\ell,t} s_{k,t} b^{t+1})$$

$$r_\ell - r_{\ell,0} = b r_\ell + b \sum_{\ell}^+ s_k - b \sum_{\ell}^- (z_\ell \& s_k)$$

$$r_1 - a = b r_1 + b \sum_{\ell}^+ s_k - b \sum_{\ell}^- (z_\ell \& s_k)$$

$$r_\ell = b r_\ell + b \sum_{\ell}^+ s_k - b \sum_{\ell}^- (z_\ell \& s_k), \quad \ell = 2, \dots, n$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$s_{d,t+1} =$$

$$= \sum_d^+ s_{k,t} + \sum_d^- z_{\ell,t} s_{k,t} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t}$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$s_{d,t+1} =$$

$$= \sum_d^+ s_{k,t} + \sum_d^- z_{\ell,t} s_{k,t} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t}$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$s_{d,t+1} =$$

$$= \sum_d^+ s_{k,t} + \sum_d^- z_{\ell,t} s_{k,t} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t}$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$s_{d,t+1} =$$

$$= \sum_d^+ s_{k,t} + \sum_d^- z_{\ell,t} s_{k,t} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t}$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$s_{d,t+1} b^{t+1} =$$

$$= \sum_d^+ s_{k,t} b^{t+1} + \sum_d^- z_{\ell,t} s_{k,t} b^{t+1} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t} b^{t+1}$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$\begin{aligned} & \sum_{t=0}^{q-1} s_{d,t+1} b^{t+1} = \\ &= \sum_{t=0}^{q-1} \left(\sum_d^+ s_{k,t} b^{t+1} + \sum_d^- z_{\ell,t} s_{k,t} b^{t+1} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t} b^{t+1} \right) \end{aligned}$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$\begin{aligned} & \sum_{t=0}^{q-1} s_{d,t+1} b^{t+1} = \\ &= \sum_{t=0}^{q-1} \left(\sum_d^+ s_{k,t} b^{t+1} + \sum_d^- z_{\ell,t} s_{k,t} b^{t+1} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t} b^{t+1} \right) \end{aligned}$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$\begin{aligned} & \sum_{t=0}^{q-1} s_{d,t+1} b^{t+1} = \\ &= \sum_{t=0}^{q-1} \left(\sum_d^+ s_{k,t} b^{t+1} + \sum_d^- z_{\ell,t} s_{k,t} b^{t+1} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t} b^{t+1} \right) \end{aligned}$$

$$s_d - s_{d,0} = b \sum_d^+ s_k + b \sum_d^+ (z_\ell \& s_k) + b \sum_d^0 ((e - z_\ell) \& s_k)$$

Новые состояния

$$s_k = \sum_{t=0}^q s_{k,t} b^t \quad z_\ell = \sum_{t=0}^q z_{\ell,t} b^t$$

$$\begin{aligned} & \sum_{t=0}^{q-1} s_{d,t+1} b^{t+1} = \\ &= \sum_{t=0}^{q-1} \left(\sum_d^+ s_{k,t} b^{t+1} + \sum_d^- z_{\ell,t} s_{k,t} b^{t+1} + \sum_d^0 (1 - z_{\ell,t}) s_{k,t} b^{t+1} \right) \end{aligned}$$

$$s_d - s_{d,0} = b \sum_d^+ s_k + b \sum_d^+ (z_\ell \& s_k) + b \sum_d^0 ((e - z_\ell) \& s_k)$$

$$e = \sum_{t=0}^{q-1} 1 \cdot b^{t+1} = \frac{b^q - 1}{b - 1}$$

Индикаторы нуля

$$z_{\ell,t} = \begin{cases} 0, & \text{если } r_{\ell,t} = 0 \\ 1 & \text{в противном случае} \end{cases}$$

Индикаторы нуля

$$z_{\ell,t} = \begin{cases} 0, & \text{если } r_{\ell,t} = 0 \\ 1 & \text{в противном случае} \end{cases}$$

$$b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1$$

Индикаторы нуля

$$z_{\ell,t} = \begin{cases} 0, & \text{если } r_{\ell,t} = 0 \\ 1 & \text{в противном случае} \end{cases}$$

$$b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

Индикаторы нуля

$$z_{\ell,t} = \begin{cases} 0, & \text{если } r_{\ell,t} = 0 \\ 1 & \text{в противном случае} \end{cases}$$

$$b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} =$$

Индикаторы нуля

$$z_{\ell,t} = \begin{cases} 0, & \text{если } r_{\ell,t} = 0 \\ 1 & \text{в противном случае} \end{cases}$$

$$b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

Индикаторы нуля

$$z_{\ell,t} = \begin{cases} 0, & \text{если } r_{\ell,t} = 0 \\ 1 & \text{в противном случае} \end{cases}$$

$$b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

$$2^c \& (2^c - 1 + r_{\ell,t}) = 2^c z_{\ell,t}$$

Индикаторы нуля

$$z_{\ell,t} = \begin{cases} 0, & \text{если } r_{\ell,t} = 0 \\ 1 & \text{в противном случае} \end{cases}$$

$$b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

$$2^c \& (2^c - 1 + r_{\ell,t}) = 2^c z_{\ell,t}$$

$$\sum_{t=0}^q (2^c \& (2^c - 1 + r_{\ell,t})) b^t = \sum_{t=0}^q 2^c z_{\ell,t} b^t$$

Индикаторы нуля

$$z_{\ell,t} = \begin{cases} 0, & \text{если } r_{\ell,t} = 0 \\ 1 & \text{в противном случае} \end{cases}$$

$$b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

$$2^c \& (2^c - 1 + r_{\ell,t}) = 2^c z_{\ell,t}$$

$$\sum_{t=0}^q (2^c \& (2^c - 1 + r_{\ell,t})) b^t = \sum_{t=0}^q 2^c z_{\ell,t} b^t$$

$$2^c f \& ((2^c - 1)f + r_{\ell}) = 2^c z_{\ell} \quad f = \sum_{t=0}^q 1 \cdot b^{t+1} = \frac{b^{q+1} - 1}{b - 1}$$

Выбор c

$$r_{\ell,t} < b$$

Выбор c

$$r_{\ell,t} < b = 2^{c+1}$$

Выбор c

$$r_{\ell,t} < b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

Выбор c

$$r_{\ell,t} < b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

Выбор c

$$r_{\ell,t} < b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

$$2^c \& r_{\ell,t} = 0$$

Выбор c

$$r_{\ell,t} < b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

$$2^c \& r_{\ell,t} = 0$$

Выбор c

$$r_{\ell,t} < b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

$$2^c \& r_{\ell,t} = 0$$

Выбор c

$$r_{\ell,t} < b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

$$\sum_{t=0}^q (2^c \& r_{\ell,t}) b^t = 0$$

Выбор c

$$r_{\ell,t} < b = 2^{c+1} \quad r_{\ell,t} \leq 2^c - 1 = 01 \dots 1$$

$$2^c - 1 + r_{\ell,t} = \begin{cases} 01 \dots 1, & \text{если } r_{\ell,t} = 0 \\ 1 * \dots * & \text{в противном случае} \end{cases}$$

$$\sum_{t=0}^q (2^c \& r_{\ell,t}) b^t = 0$$

$$2^c f \& r_{\ell} = 0 \quad f = \sum_{t=0}^q 1 \cdot b^{t+1} = \frac{b^{q+1} - 1}{b - 1}$$

Все условия

Все условия

$$b = 2^{c+1}$$

Все условия

$$b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} = br_\ell + b\sum_\ell^+ s_k - b\sum_\ell^-(z_\ell \& s_k)$$

Все условия

$$b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} = br_\ell + b\sum_\ell^+ s_k - b\sum_\ell^-(z_\ell \& s_k)$$

$$s_d - s_{d,0} = b\sum_d^+ s_k + b\sum_d^+(z_\ell \& s_k) + b\sum_d^0((e - z_\ell) \& s_k)$$

Все условия

$$b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} = br_\ell + b\sum_\ell^+ s_k - b\sum_\ell^-(z_\ell \& s_k)$$

$$s_d - s_{d,0} = b\sum_d^+ s_k + b\sum_d^+(z_\ell \& s_k) + b\sum_d^0((e - z_\ell) \& s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

Все условия

$$b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} = br_\ell + b\sum_\ell^+ s_k - b\sum_\ell^-(z_\ell \& s_k)$$

$$s_d - s_{d,0} = b\sum_d^+ s_k + b\sum_d^+(z_\ell \& s_k) + b\sum_d^0((e - z_\ell) \& s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

$$2^c f \& ((2^c - 1)f + r_\ell) = 2^c z_\ell \quad f = \frac{b^{q+1} - 1}{b - 1}$$

Все условия

$$b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} = br_\ell + b\sum_\ell^+ s_k - b\sum_\ell^-(z_\ell \& s_k)$$

$$s_d - s_{d,0} = b\sum_d^+ s_k + b\sum_d^+(z_\ell \& s_k) + b\sum_d^0((e - z_\ell) \& s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

$$2^c f \& ((2^c - 1)f + r_\ell) = 2^c z_\ell \quad f = \frac{b^{q+1} - 1}{b - 1}$$

$$2^c f \& r_\ell = 0$$

Все условия

$$b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} = br_\ell + b\sum_\ell^+ s_k - b\sum_\ell^-(z_\ell \& s_k)$$

$$s_d - s_{d,0} = b\sum_d^+ s_k + b\sum_d^+(z_\ell \& s_k) + b\sum_d^0((e - z_\ell) \& s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

$$2^cf \& ((2^c - 1)f + r_\ell) = 2^cz_\ell \quad f = \frac{b^{q+1} - 1}{b - 1}$$

$$2^cf \& r_\ell = 0 \qquad s_m = b^q$$

Теорема Куммера

$$\binom{m+n}{m} = C_{m+n}^m$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C_{m+n}^m \\ &= \frac{(m+n)!}{m!n!}\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C_{m+n}^m \\ &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C_{m+n}^m \\ &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

Теорема (Ernst Eduard Kummer [1852]). *Запишем числа m и n в позиционной системе счисления с основанием p и сложим их «в столбик»;*

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C_{m+n}^m \\ &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

Теорема (Ernst Eduard Kummer [1852]). Запишем числа m и n в позиционной системе счисления с основанием p и сложим их «в столбик»; $\alpha_p(m, n)$ равно количеству переносов из разряда в разряд при этом сложении.

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

$$\alpha_p(m, n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n)$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \cdots p^{\beta_p(k)} \cdots$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \cdots p^{\beta_p(k)} \cdots$$

$$p, 2p, 3p, \dots,$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \cdots p^{\beta_p(k)} \cdots$$

$$p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \cdots p^{\beta_p(k)} \cdots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p : $p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \cdots p^{\beta_p(k)} \cdots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p : $p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2 : $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \cdots p^{\beta_p(k)} \cdots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p : $p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2 : $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \frac{k}{p^3} \right\rfloor$ чисел кратных p^3 : $p^3, 2p^3, 3p^3, \dots, \left\lfloor \frac{k}{p^3} \right\rfloor p^3$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \cdots p^{\beta_p(k)} \cdots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p : $p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2 : $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \frac{k}{p^3} \right\rfloor$ чисел кратных p^3 : $p^3, 2p^3, 3p^3, \dots, \left\lfloor \frac{k}{p^3} \right\rfloor p^3$

$\vdots$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \cdots p^{\beta_p(k)} \cdots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p : $p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2 : $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \frac{k}{p^3} \right\rfloor$ чисел кратных p^3 : $p^3, 2p^3, 3p^3, \dots, \left\lfloor \frac{k}{p^3} \right\rfloor p^3$

$\vdots$

$$\beta_p(k) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

$$\alpha_p(m, n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n)$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

$$\begin{aligned}\alpha_p(m, n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\ &= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\ &\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\ &\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\alpha_p(m, n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\ &= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\ &\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\ &\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\alpha_p(m, n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\&= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\&\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\&\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots \\&= \left(\left\lfloor \frac{m+n}{p} \right\rfloor - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{n}{p} \right\rfloor \right) + \left(\left\lfloor \frac{m+n}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + \\&\quad + \left(\left\lfloor \frac{m+n}{p^3} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + \dots\end{aligned}$$

Теорема Куммера

$$\left\lfloor \frac{m+n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor = \begin{cases} 1, & \text{если есть перенос} \\ 0, & \text{если нет переноса} \end{cases}$$

Теорема Куммера

$$\left\lfloor \frac{m+n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor = \begin{cases} 1, & \text{если есть перенос} \\ 0, & \text{если нет переноса} \end{cases}$$

$$\begin{aligned} m &= \sum_{j=0}^r m_j p^j = \\ n &= \sum_{j=0}^r n_j p^j = \\ m+n &= \sum_{j=0}^r \ell_j p^j = \end{aligned}$$

m_r	$\dots$	m_k	m_{k-1}	$\dots$	m_0
n_r	$\dots$	n_k	n_{k-1}	$\dots$	n_0
ℓ_r	$\dots$	ℓ_k	ℓ_{k-1}	$\dots$	ℓ_0

$$\begin{aligned} \left\lfloor m/p^k \right\rfloor &= \\ \left\lfloor n/p^k \right\rfloor &= \\ \left\lfloor (m+n)/p^k \right\rfloor &= \end{aligned}$$

m_r	$\dots$	m_k
n_r	$\dots$	n_k
ℓ_r	$\dots$	ℓ_k

Теорема Куммера

$$\begin{aligned}\alpha_p(m, n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\&= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\&\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\&\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\alpha_p(m, n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\&= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\&\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\&\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots \\&= \left(\left\lfloor \frac{m+n}{p} \right\rfloor - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{n}{p} \right\rfloor \right) + \left(\left\lfloor \frac{m+n}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + \\&\quad + \left(\left\lfloor \frac{m+n}{p^3} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + \dots\end{aligned}$$

Следствие теоремы Куммера

Следствие теоремы Куммера

Лемма. При сложении чисел a и b в двоичной системе счисления не происходит ни одного переноса из разряд в разряд в том и только том случае, когда биномиальный коэффициент $\binom{a+b}{a}$ является нечетным

Следствие теоремы Куммера

Лемма. При сложении чисел a и b в двоичной системе счисления не происходит ни одного переноса из разряд в разряд в том и только том случае, когда биномиальный коэффициент $\binom{a+b}{a}$ является нечетным, то есть существует натуральное число d такое, что

$$\binom{a+b}{a} = 2d + 1.$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

<i>a</i>	...	0	...	0	...	1	...	1	...
<i>b</i>	...	0	...	1	...	0	...	1	...
<i>c</i>	...	0	...	0	...	0	...	1	...

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \& b \implies \binom{a}{c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \& b \implies \binom{a}{c} \text{ нечетн.} \wedge \binom{b}{c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \& b \implies \binom{a}{c} \text{ нечетн.} \wedge \binom{b}{c} \text{ нечетн.} \wedge \\ \wedge \binom{(a-c) + (b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \& b \implies \binom{a}{c} \text{ нечетн.} \wedge \binom{b}{c} \text{ нечетн.} \wedge$$

$$\wedge \binom{(a-c) + (b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \& b \iff \binom{a}{c} \text{ нечетн.} \wedge \binom{b}{c} \text{ нечетн.} \wedge$$

$$\wedge \binom{(a-c) + (b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \& b \iff \binom{a}{c} \text{ нечетн.} \wedge \binom{b}{c} \text{ нечетн.} \wedge \\ \wedge \binom{(a-c) + (b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \& b \iff \binom{a}{c} \text{ нечетн.} \wedge \binom{b}{c} \text{ нечетн.} \wedge \\ \wedge \binom{(a-c) + (b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \quad b = \sum_{k=0}^{\infty} b_k 2^k \quad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \& b \iff \binom{a}{c} \text{ нечетн.} \wedge \binom{b}{c} \text{ нечетн.} \wedge \\ \wedge \binom{(a-c) + (b-c)}{a-c} \text{ нечетн.}$$

Биномиальные коэффициенты

Биномиальные коэффициенты

$$(1 + u)^m = \binom{m}{m} u^m + \binom{m}{m-1} u^{m-1} + \binom{m}{m-2} u^{m-2} + \\ + \dots + \binom{m}{n} u^n + \dots + \binom{m}{1} u + \binom{m}{0}$$

Биномиальные коэффициенты

$$(1+u)^m = \binom{m}{m} u^m + \binom{m}{m-1} u^{m-1} + \binom{m}{m-2} u^{m-2} + \\ + \cdots + \binom{m}{n} u^n + \cdots + \binom{m}{1} u + \binom{m}{0}$$

$$2^m = \binom{m}{0} + \cdots + \binom{m}{n} + \cdots + \binom{m}{m}$$

Биномиальные коэффициенты

$$(1+u)^m = \binom{m}{m}u^m + \binom{m}{m-1}u^{m-1} + \binom{m}{m-2}u^{m-2} + \\ + \dots + \binom{m}{n}u^n + \dots + \binom{m}{1}u + \binom{m}{0}$$

$$2^m = \binom{m}{0} + \dots + \binom{m}{n} + \dots + \binom{m}{m}$$

$$c = \binom{m}{n} \iff \exists upq \{ (1+u)^m = pu^{n+1} + cu^n + q \wedge \\ c < u \wedge q < u^{n-1} \wedge u > 2^m \}$$