Пример 19. Вот типичное соотношение Безу: $12 \cdot 1 + 8 \cdot (-1) = 4$.

Польза от этого самого соотношения Безу следующая: предположим, плохой начальник заставляет вас найти наибольший общий делитель чисел 1234567 и 89101112. Вы приносите ему 1. «Ну хорошо», говорит начальник, «эти числа действительно делятся на 1, но какие ваши доказательства, что они больше ни на что не делятся»? А если вы принесете ему

$$1234567 \cdot 76257319 + 89101112 \cdot (-1056606) = 1,$$

то сделав два умножения и одно вычитание, начальник убеждается, что равенство верно, и автоматически получает доказательство того, что

$$\text{НОД}(1234567, 89101112) = 1.$$

Ибо если бы эти числа делились на другое число, на это другое число делилось бы и число $1234567 \cdot 76257319$, число $89101112 \cdot (-1056606)$ и число

$$1234567 \cdot 76257319 + 89101112 \cdot (-1056606),$$

а оно равно 1 и на другие числа не делится.

На всякий случай запомните: соотношение Безу находится неоднозначно. Т.е. если начальник даст одинаковые числа разным людям, то они могут найти разные, но правильные соотношения Безу.

Пример 20. Вот два разных но правильных соотношения Безу: $3 \cdot (-1) + 4 \cdot (1) = 1$ и $3 \cdot (3) + 4 \cdot (-2) = 1$.

Перейти от одного соотношения Безу к другому можно с помощью следующего приёма:

Утверждение 6. *Если* $A \cdot (u) + B \cdot (v) = N$ *то* $A \cdot (u - B) + B \cdot (v + A) = N$ *и* $A \cdot (u + B) + B \cdot (v - A) = N$.

Для доказательства достаточно раскрыть скобки.

Пример 21. Берем вот такое $3 \cdot (-1) + 4 \cdot (1) = 1$ соотношение Безу, прибавляем и вычитаем: $3 \cdot (-1 + 4) + 4 \cdot (1 - 3) = 1$, и получаем $3 \cdot (3) + 4 \cdot (-2) = 1$.

Кстати, таким методом можно переставить минус в соотношении Безу, иногда (в примере 16 (стр. 4)) это важно.

Итак, у вас остались два вопроса:

1. Как искать НОД быстрее чем методом перебора?
2. Как находить числа в равенстве Безу?

2.3 Алгоритм Евклида для нахождения наибольшего общего делителя

Заметим, что если некие числа делятся на x, то их суммы, разности и произведения тоже будут делиться на x. Например, 12, 9 и 15 делятся на 3. Легко проверить на калькуляторе, что $12 + 9$, $12 - 9$, $15 \cdot 12 + 9$ тоже делятся на 3, И даже $12 \cdot 7$ и $15 \cdot 5 - 9$ делятся на 3, хотя 7 и 5 на 3 не делятся.

Основываясь на этом наблюдении, проделаем следующее странное действие: поделим одно число на другое с остатком: $A = B \cdot C + R$ (A — делимое, C — делитель R — остаток). Следовательно, делители R и B будут делителями A. Это же равенство можно записать через разность: $R = A - B \cdot C$. И, следовательно, делители A и B будут делителями R. Таким образом, мы нечаянно доказали

Утверждение 7 (Теорема Евклида о НОД)**.** *Если* $A\%B = R$*, то* $\text{НОД}(A, B) = \text{НОД}(B, R)$.

Которое позволяет свести сложную задачу поиска НОД для больших чисел A и B к чуть менее сложной задаче поиска НОД для чуть меньших чисел B и R (напомним, что $R = A\%B$). Потом, аналогично, свести эту чуть менее сложную задачу к ещё менее сложной, и так далее.

Практически это означает, что если начальник вас заставляет искать $\text{НОД}(A, B)$, нужно поделить с остатком, подозвать подчиненного и дать ему задание найти $\text{НОД}(B, R)$. Подчиненный сделает то же самое, т.е. даст аналогичное задание своему подчиненному. Где-то там, на дне иерархии подчиненных, очередной подчиненный получит задание с маленькими числами и сможет найти НОД перебором. (В программировании это называется *рекурсивная функция*).

Кстати, этот подчиненный из глубин иерархии может и сам прибежать к вашему начальнику и принести готовый ответ[6].

Пример 22. Найдем $\text{НОД}(29, 12)$. Находим остаток: $29\%12 = 5$. Даем задание подчиненному: «А ну ка братец, найди мне $\text{НОД}(12, 5)$». Подчиненный находит остаток $12\%5 = 2$ и дает задание подподчиненному: «А ну ка братец, найди мне $\text{НОД}(5, 2)$». Числа 5 и 2 достаточно маленькие, чтобы найти НОД. Он равен 1. Итого: $\text{НОД}(29, 12) = 1$.

2.4 Алгоритм Евклида для нахождения равенства Безу

Основан на такой же рекурсии как и алгоритм нахождения наибольшего общего делителя[7].

Предположим, начальник дал нам A, B и велел найти u, v в равенстве

$$A \cdot (u) + B \cdot (v) = \text{НОД}(A, B).$$

Вычисляем остаток $A = B \cdot C + R$ и даем задание своему подчинённому пойти и найти числа в равенстве

$$B \cdot (u_1) + R \cdot (v_1) = \text{НОД}(B, R).$$

Когда подчиненный принесет нам НОД и свои u_1, v_1, выражаем

$$R = A - B \cdot C,$$

подставляем в предыдущее равенство

$$B \cdot (u_1) + (A - B \cdot C) \cdot (v_1) = \text{НОД}(B, R)$$

и преобразуем в

$$A \cdot (v_1) + B \cdot (u_1 - C \cdot v_1) = \text{НОД}. \tag{3}$$

Таким образом, наше u равно v_1 нашего подчиненного и наше $v = u_1 - C \cdot v_1$.

Как же подчиненный находит свои u_1 и v_1? Да понятно как, он подзывает своего подчиненного и даёт ему аналогичное задание. На дне иерархии подчиненных некий совсем уже низкопоставленный подчинённый получит совсем маленькие A, B и найдет НОД, u и v просто перебором.

[6] В программировании это называется *хвостовая рекурсия*

[7] Если вы еще не читали раздел 2.3, то сейчас самое время это сделать.

Утверждение 3 (Китайская теорема об остатках в облегченной формулировке). *Если на левой звездочке A зубчиков, на правой B и эти числа взаимно просты* (*т.е.* НОД$(A,B)=1$), *то операция «плюс один» переведет звездочки через всевозможные комбинации, и комбинаций этих будет $A\cdot B$ штук.*

Более того, верно

Утверждение 4 (Продолжение Китайской теоремы). *Если пронумеровать эти комбинации пар чисел в том порядке, в котором они появляются, то этот велосипедик будет работать так же, как и обыкновенное кольцо вычетов*[4] $Z_{A\cdot B}$.

Про «будет работать так же» следует пояснить: вот представьте, что у нас на стеклянной стене карточки, у которых с одной стороны написаны пары чисел от «велосипедика», а с другой их номер, т.е. числа из большого кольца вычетов (посмотрите на пример 12). Если теперь производить всякие там арифметические действия с числами из большого кольца вычетов, то люди с другой стороны стеклянной стены будут думать, что эти действия производятся с парами чисел «покоординатно».

Пример 13. Вычислим $2+3$ в Z_{12} и вычислим покоординатно $(2,2)+(0,3)$ в велосипедике (см. пример 12). На одной стороне стеклянной стены будет $2+3=5$, на другой $(2,2)+(0,3)=(2+0,2+3)=(2,1)$. Но у карточки с парой чисел $(2,1)$ на другой стороне как раз и написано 5.

Пример 14. Вычислим 3^2 в Z_{12} и вычислим покоординатно $(0,3)\cdot(0,3)$ в велосипедике (и опять см. пример 12). На одной стороне доски будет $3\cdot 3=9$, на другой $(0,3)\cdot(0,3)=$ $=(0\cdot 0,3\cdot 3)=(0,1)$. Но у карточки с парой чисел $(0,1)$ на другой стороне как раз и написано 9.

Благодаря этому вот наблюдению, алгоритм извлечения корня из раздела 1.5 (стр. 3) можно применять в кольцах вычетов $Z_{p\cdot q}$, где p и q простые числа. И сейчас вы узнаете

1.6.1 Как извлекать корни в $Z_{p\cdot q}$

1. Мысленно строим таблицу соответствий между $Z_{p\cdot q}$ и «велосипедиком» со звездочками Z_p и Z_q.

2. Ищем в этой таблице пару, соответствующую нашему числу.

3. Вместо извлечения корня из числа в большом кольце вычетов, будем два раза извлекать корень из двух чисел в двух маленьких кольцах вычетов. Это можно и нужно делать по алгоритму из раздела 1.5.1 (стр. 3) так как p и q простые числа.

4. Потом опять посмотрим в таблицу и найдем число, соответствующее паре этих самых корней. Это и будет ответ.

Пример 15. Числа 11 и 5 простые. Возьмите большой-пребольшой лист бумаги и запишите на него таблицу с $11\cdot 5=$ $=55$ числами. У вас должно получиться как-то так: $0-$ $-(0,0)$, $1-(1,1)$, $2-(2,2)$, $\ldots$ $5-(5,0)$, $6-(6,1)$, $\ldots$ $11-(0,1)$, $12-(1,2)$, $\ldots$ $54-(10,4)$.

Число 3 взаимно просто с $10=11-1$ и $4=5-1$, так что извлечь корень 3 степени у нас получится. Возьмем первое попавшееся число, например, 53. Посмотрев в большую таблицу, увидим, что числу 53 соответствует пара $(9,3)$.

Теперь будем два раза извлекать корень, так, как это сделано в примере 11 (стр. 3). Если вы все сделаете правильно, то у вас получится: $\sqrt[3]{9}=4$ в Z_{11} и $\sqrt[3]{3}=2$ в Z_5. (В этом месте желательно сделать проверку: $4^3=16\cdot 4=$ $=5\cdot 4=20=9$ в Z_{11} и $2^3=8=3$ в Z_5).

И опять посмотрев в таблицу, увидим, что паре $(4,2)$ соответствует число 37. На всякий случай сделаем проверку (см. упр. 6 (стр. 5)): сосчитав на калькуляторе $(37\cdot 37\cdot 37-53)/55$, обнаружим, что получилось целое число. Значит, все правильно.

Вероятно, вам не понравилось рисование гигантских таблиц, и сейчас вы узнаете,

1.6.2 Как обойтись без таблицы

Итак, у нас есть «велосипедик» из Z_A и Z_B. Заметим, что выписывание пар чисел по порядку есть не что иное, как наматывание двух веревочек на два бревна. Так что пара (a,b), соответствующая большому числу D, есть просто остатки от деления.

$$\left\{\begin{array}{lcl} a & = & D\%A \\ b & = & D\%B. \end{array}\right.$$

И действительно, 53%11=9 и 53%5=3. В обратную сторону несколько сложнее.

Предположим, у нас есть пара чисел (a,b) в «велосипедике» из Z_A и Z_B, и нам нужно найти число x из большого кольца вычетов, которое соответствует этой паре, т.е. нужно решить систему уравнений

$$\left\{\begin{array}{lcl} a & = & x\%A \\ b & = & x\%B. \end{array}\right.$$

Вспомним, что такое остаток от деления

$$\left\{\begin{array}{lcl} x & = & A\cdot\alpha+a \\ x & = & B\cdot\beta+b \end{array}\right.$$

и приравняем правые части уравнений

$$A\cdot\alpha+a=B\cdot\beta+b.$$

Ясно, что если мы найдем α или β, то найдем и x. Перенесем неизвестные влево и известные вправо

$$A\cdot\alpha+B\cdot(-\beta)=b-a.$$

Ой, это же почти что соотношение Безу! (см. раздел 2.2 (стр. 5)). Ну теперь уравнение легко решить.

Пример 16. Пусть у нашего велосипедика звездочки с 11 и 5 зубчиками, и нам надо найти соответствие паре $(9,3)$. Система уравнений будет такая

$$\left\{\begin{array}{lcl} 9 & = & x\%11 \\ 3 & = & x\%5, \end{array}\right.$$

потом такая

$$\left\{\begin{array}{lcl} x & = & 11\cdot\alpha+9 \\ x & = & 5\cdot\beta+3 \end{array}\right. \tag{1}$$

и уравнение получится такое

$$11\cdot\alpha+5\cdot(-\beta)=3-9=-6. \tag{2}$$

Найдем соотношение Безу (см. раздел 2.4 (стр. 6))

$$11\cdot(1)+5\cdot(-2)=1.$$

[4] По научному это называется *«изоморфизм»*.

Присмотревшись к циферблатику, можно заметить, что противоположные числа находятся на противоположных (относительно вертикали) сторонах. Напротив 2 находится 10, и действительно, $2 + 10 = 0$ (в Z_{12}).

Операция вычитания как бы лишняя, потому что её можно заменить на прибавление противоположного, для демонстрации чего и приведен

Пример 5. В нормальных числах -3 противоположно 3, и это значит, что вычитание $x - 3$ можно заменить на сложение $x + (-3)$. Аналогично в ненормальных числах: так как $7 + 5 = 0$ (в Z_{12}), вычитание можно заменить на сложение: $3 - 7 = 3 + 5 = 8$. Проверяем сложением: $8 + 7 = 15 = 12 + 3 = 3$.

Упражнение 1. Решить уравнение $x + 3 = 2$ в Z_5.

1.3 Деление

Деление — это операция, обратная к умножению. Поскольку в Z_{12} верно равенство $4 \cdot 5 = 8$, то $8/5 = 4$. Делить числа так, как мы раньше умножали и складывали, т.е. «поделить на веревочке и намотать», (как в примере 4 (стр. 1)), к сожалению, невозможно. $8/5 = 1.6$ и на 4 совершенно не похоже.

Так же как и в случае с «черточкой», у математиков есть три вида «поделить»:

1. Обычное деление, на калькуляторе это кнопочка справа.
2. Нахождение обратного. Обозначается x^{-1}. На калькуляторе обозначается $1/x$ или x^{-1}.
3. «Запятая» на индикаторе калькулятора, что, как вы, наверное, помните, означает несколько раз поделить на 10.

Напомним на всякий случай, что одно число называется обратным к другому, если их произведение равно 1, и вместо деления можно использовать умножение на обратное число.

Пример 6. В обычных числах $2 \cdot 0.5 = 1$, т.е. 2 обратно к 0.5 и 0.5 обратно к 2. И теперь можно делить умножением: $a/2 = a \cdot 0.5$ и $a/0.5 = a \cdot 2$.

Примерно так мы и будем делить в кольце вычетов.

Пример 7. Произведение $3 \cdot 4 = 12 = 11 + 1$ т.е. $3 \cdot 4 = 1$ в Z_{11}. Следовательно, мы внезапно научились делить на 3 и на 4 в Z_{11}: $2/3 = 2 \cdot 4 = 8$, $2/4 = 2 \cdot 3 = 6$, $5/3 = 5 \cdot 4 = 20 = 9$ и т.д.

С обратными числами в кольцах вычетов всё не просто.

Пример 8. Проведем исследование в Z_6, для этого перемножим всевозможные числа (кроме 1 и 0): $2 \cdot 2 = 4$, $2 \cdot 3 = 6 = 0$, $2 \cdot 4 = 8 = 6 + 2 = 2$, $2 \cdot 5 = 10 = 6 + 4 = 4$, $3 \cdot 3 = 9 = 6 + 3 = 3$, $3 \cdot 4 = 12 = 6 \cdot 2 + 0 = 0$, $3 \cdot 5 = 15 = 6 \cdot 2 + 3 = 3$, $4 \cdot 4 = 16 = 6 \cdot 2 + 4 = 4$, $4 \cdot 5 = 20 = 6 \cdot 3 + 2 = 2$, $\mathbf{5 \cdot 5 = 25 = 6 \cdot 4 + 1 = 1}$.

Как видите, не у всех чисел есть обратное (5 обратно 5, но у других чисел обратного нет), да и у тех, у которых есть, совершенно не ясно, как это самое обратное находить.

Понятно, что находить обратное тупым перебором можно в маленьких кольцах вычетов, но нельзя в больших. В популярном в криптографических кругах Zстозначное число, перебор всех вариантов (как показано в разделе 3.2 (стр. 7)) вообще никогда не не закончится. Сейчас вы узнаете достаточно быстрый

1.3.1 Алгоритм нахождения обратного в кольце вычетов

Он основан на соотношении Безу, про которое можно (и нужно) почитать в разделе 2.2 (стр. 5).

Предположим, некто заставляет нас найти A^{-1} в кольце вычетов Z_N. Заставим кого-нибудь (кто уже прочитал раздел 2.2 (стр. 5)) найти для нас числа u и v в соотношении Безу

$$A \cdot u + N \cdot v = \text{НОД}(A, N).$$

Нам нужно то соотношение, в котором число u положительное и v отрицательное (см. утверждение 6 (стр. 6)). Если НОД получился не 1, то это хорошо, обратного не существует. Так этому Некту и говорим, и идем отдыхать.

Если НОД равен 1, то это плохо, придется считать дальше. Преобразуем это соотношение Безу

$$A \cdot u + N \cdot v = 1$$

в равенство

$$A \cdot u = N \cdot (-v) + 1.$$

Отчетливо видно, что слева умножение двух чисел, а справа формула деления с остатком. Вот мы и нашли обратное, это будет u.

Пример 9. Найдем 3^{-1} в Z_{11}. Нам принесут $3 \cdot 4 + 11 \cdot (-1) = 1$. Делаем вывод: $3^{-1} = 4$. Делаем проверку: $3 \cdot 4 = 12 = 11 + 1$.

Ах да, если тот самый кто-нибудь принес нам соотношение Безу со слишком большими числами, (например $3 \cdot 15 + 11 \cdot (-4) = 1$), то придется это обратное «намотать на бревно» ($15 = 11 + 4 = 4$ в Z_{11}), чтобы оно помещалось в кольцо вычетов.

Упражнение 2. Решить уравнение $33 \cdot x + 25 = 0$ в кольце вычетов Z_{41}.

1.4 Возведение в степень

Возведение в степень — это многократное умножение, как все знают. Также все знают, что возводить в большую степень нет смысла, получается очень большое число, которое ни в какой компьютер не поместится. Но в кольце вычетов слишком больших чисел не бывает. Ибо даже стозначное число в стозначной степени в стозначном кольце вычетов — всего лишь стозначное число, и оно почти в любом компьютере помещается. Проблема в том, что проделать стозначное число умножений невозможно. (Про это написано в разделе 3.2 (стр. 7)). Оказывается, есть более

1.4.1 Быстрый алгоритм возведения в степень

Проиллюстрируем его идею на примере: $x^6 = x \cdot x \cdot x \cdot x \cdot x \cdot x$, т.е. пять умножений. Но если схитрить: $x^6 = (x^3)^2 = (((x^2) \cdot x)^2)$, то понадобится только три умножения. Может показаться, что три не намного лучше чем пять, но при больших степенях разница становится впечатляющей, x^{1024} можно сосчитать за 1023 умножения, а можно вспомнить, что $1024 = 2^{10}$, и сосчитать за десять возведений в квадрат.

Погуглив в Википедии[1], можно узнать, что количество умножений при этом быстром возведении в степень не более чем в два раза больше, чем длина двоичной записи степени. Стозначное десятичное число — это не более чем 400

[1] Алгоритмы быстрого возведения в степень.
goo.gl/yae8h9