7. Алгоритм Евклида: следствия

С помощью алгоритма Евклида можно доказать критерий разрешимости линейных уравнений в целых числах. Мы сейчас это объясним, но начнём с примеров.

7.1 В стране в ходу только две монеты: 8 флоринов и 15 флоринов. И у вас, и у кассира есть неограниченный запас монет обоих видов (для оплаты и для сдачи). Как заплатить 30 флоринов? 40 флоринов? 10 флоринов? 1 флорин? 13 флоринов? любое целое число флоринов?

▷ Заплатить 30 и 40 флоринов просто: два раза по 15 и пять раз по 8. Теперь можно заплатить 10, заплатив 40 ($=5\cdot 8$) и получив сдачи 30 ($=2\cdot 15$). Другими словами, $10 = 5\cdot 8 - 2\cdot 15$. Чтобы заплатить 1 флорин, можно заплатить 16 флоринов двумя монетами по 8 и получить сдачи 15. Другими словами, $1 = 2\cdot 8 - 1\cdot 15$. Теперь безо всяких вычислений можно понять, как заплатить любое целое число флоринов: надо просто много раз платить один флорин. Другими словами, можно умножить последнее равенство на любое число: $13 = (13\cdot 2)\cdot 8 - (13\cdot 1)\cdot 15 = 26\cdot 8 - 13\cdot 15$. ◁

7.2* Покажите, что можно заплатить кассиру любое число флоринов и в том случае, когда у вас есть только монеты в 15 флоринов, а у него только в 8 флоринов.

▷ Можно заметить, что $7\cdot 15 - 13\cdot 8 = 105 - 104 = 1$, и дальше можно повторять платежи. Но можно и заранее поменять 15-флориновые монеты на 8-флориновые у того же кассира (по курсу 8 за 15) в любом нужном количестве и свести задачу к предыдущей. ◁

7.3 Пусть теперь в ходу только две монеты: в 25 и 15 флоринов. Как заплатить 80 флоринов? 5 флоринов? 2005 флоринов? 7 флоринов? Какие суммы можно заплатить, а какие нет?

▷ Заплатить 80 можно как $50 + 30 = 2\cdot 25 + 2\cdot 15$. Чтобы заплатить 5, можно заплатить 50 и получить 45 сдачи: $5 = 2\cdot 25 - 3\cdot 15$. Теперь можно заплатить любое кратное 5 (заплатив 5 несколько раз), в том числе и 2005. А заплатить 7 нельзя, потому что все уплачиваемые суммы кратны 5 (поскольку обе монеты кратны 5, любая уплачиваемая сумма будет кратна 5, а 7 не делится на 5). Так что можно заплатить суммы, кратные 5, а не кратные — нельзя. ◁

В общем виде можно сказать так. Пусть даны два числа a и b. Мы рассматриваем числа вида $ma + nb$ при всевозможных целых m и n (суммы,

которые можно уплатить, если есть только монеты a и b). Будем коротко называть такие числа «выразимыми» через a и b (полностью было бы «выразимыми в виде целочисленной линейной комбинации чисел a и b»). В предыдущих задачах мы установили, что

- любые целые числа выразимы через 8 и 15;
- целые числа, кратные 5, и только они, выразимы через 25 и 15.

Возникает общий вопрос: какие числа выразимы через данные два числа a и b? Ответ на него такой: *те* (*и только те*), *которые кратны* НОД (a, b). Мы вскоре увидим, почему это так.

7.4 Фиксируем a и b и будем рассматривать выразимость через них. Покажите, что любое кратное выразимого числа выразимо. Покажите, что сумма и разность двух выразимых чисел выразими.

▷ Математики сформулировали бы утверждение этой задачи, сказав, что *выразимые числа образуют идеал*. (Терминология странная, но так получилось исторически.) ◁

▷ На языке монет: если можно уплатить u, то можно уплатить и любое кратное u (повторяя уплату). Если можно уплатить u и v, то можно уплатить $u + v$, сначала уплатив u, а потом уплатив v. Чтобы уплатить $u - v$, надо уплатить u, а потом получить сдачу v (уплата «в другую сторону»). ◁

7.5 Докажите, что число c выразимо через a и b в том и только том случае, когда c делится на $d = $ НОД (a, b).

• Эта формулировка означает, что надо доказать две вещи: (1) если c выразимо, то оно делится на d; (2) если c делится на d, то оно выразимо через a и b.

▷ Первая часть совсем простая: если обе монеты кратны какому-то d (наибольшему общему делителю, или даже просто общему делителю), то всё, что можно ими уплатить, тоже будет кратно d. Другими словами, поскольку a и b кратны $d = $ НОД (a, b), то и любая уплачиваемая сумма $ma + nb$ будет кратна d (как сумма или разность нескольких кратных d).

Вторая часть главная: почему d и любое кратное d выразимы (можно уплатить монетами a и b)? Достаточно доказать про d (потому что если можно один раз уплатить d, то можно и повторять). Тут как раз и нужен алгоритм Евклида. В нём мы много раз вычитаем одно число пары

из другого (деление с остатком можно считать многократным вычитанием). Начинаем мы с выразимых чисел a и b, и разность выразимых чисел всегда выразима, поэтому всё, что получится в ходе алгоритма, будет выразимо. В том числе и результат (то, что будет на последнем шаге), то есть наибольший общий делитель d. $\triangleleft$

• Как это выглядит для нашего примера с 15 и 8? Алгоритм Евклида даёт последовательно $(15, 8) \to (7, 8) \to (7, 1)$, дальше 7 делится без остатка, так что мы останавливаемся и получаем НОД $(15, 8) = 1$.

Оба числа 15 и 8 выразимы через 15 и 8 (естественно), поэтому выразима их разность $7 = 15 - 8$. Раз числа 8 и 7 выразимы, то выразима их разность $1 = 8 - 7 = 8 - (15 - 8) = 2 \cdot 8 - 15$.

Утверждение предыдущей задачи формулируют ещё и так. Пусть a и b — произвольные целые числа (не равные оба нулю), и c — произвольное целое число.

Уравнение

$$ax + by = c$$

разрешимо в целых числах x, y тогда и только тогда, когда число c делится на НОД (a, b).

7.6 Имеет ли уравнение $23x + 89y = 5$ решения в целых числах? Найдите одно из них.

$\triangleright$ Применяем алгоритм Евклида:

$(89, 23)$	$89 \bmod 23 = 20$	$20 = 89 - 3 \cdot 23$	$(23, 20)$
$(23, 20)$	$23 \bmod 20 = 3$	$3 = 23 - 1 \cdot 20$	$(20, 3)$
$(20, 3)$	$20 \bmod 3 = 2$	$2 = 20 - 6 \cdot 3$	$(3, 2)$
$(3, 2)$	$30 \bmod 2 = 1$	$1 = 3 - 1 \cdot 2$	$(2, 1)$

Теперь последовательно выражаем числа $20, 3, 2, 1$ в виде целочисленных линейных комбинаций 89 и 23 (и напоследок умножаем на 5):

$$20 = 1 \cdot 89 - 3 \cdot 23$$

$$3 = 1 \cdot 23 - 1 \cdot 20 = 1 \cdot 23 - 1 \cdot (89 - 3 \cdot 23) = 4 \cdot 23 - 1 \cdot 89$$

$$2 = 1 \cdot 20 - 6 \cdot 3 = 1 \cdot (1 \cdot 89 - 3 \cdot 23) - 6 \cdot (4 \cdot 23 - 1 \cdot 89) = 7 \cdot 89 - 27 \cdot 23$$

$$1 = 1 \cdot 3 - 1 \cdot 2 = 1 \cdot (4 \cdot 23 - 1 \cdot 89) - 1 \cdot (7 \cdot 89 - 27 \cdot 23) = 31 \cdot 23 - 8 \cdot 89$$

$$5 = (5 \cdot 31) \cdot 23 - (5 \cdot 8) \cdot 89 = 155 \cdot 23 - 40 \cdot 89.$$

Конечно, это не единственное решение — например, можно было бы сложить выражения для 3 и 2 и получить $4 \cdot 23 - 1 \cdot 89 + 7 \cdot 89 - 27 \cdot 23 = 6 \cdot 89 - 23 \cdot 23$. Но мы следовали общей схеме: сначала выразить наибольший общий делитель, а потом любое его кратное. ◁

• В этой задаче требуется найти одно решение — но можно и найти общую формулу для всех решений. Мы вскоре вернёмся к этому вопросу.

7.7 Докажите, что для любых двух целых чисел a, b (не равных одновременно нулю) их наибольший общий делитель не просто *больше* любого другого делителя, но и *делится* на него.

▷ Пусть d — этот наибольший общий делитель, а d' — какой-то другой делитель. Мы доказали (как следствие алгоритма Евклида), что можно найти x, y, для которых $ax + by = d$. Раз x и y делятся на d', то и ax, by, и, наконец, $ax + by$ (то есть d) делятся на d'. ◁

• Посмотрим снова на уравнение $ax + by = c$. Там две переменные x и y, значения которых мы ищем, и они входят симметрично. Но можно посмотреть на дело иначе: мы сначала подбираем x, а потом y. На первом шаге нужны такие x, при которых y найдётся, то есть для которых $c - ax$ делится на b (потому что $y = (c - ax)/b$ должно быть целым). Таким образом, мы ищем x, при котором $ax \equiv c \pmod{b}$. И это возможно (как мы теперь знаем), когда c делится на НОД (a, b).

Важный частный случай, когда a и b взаимно просты, разбирается в следующей задаче.

7.8 Пусть числа a и b взаимно просты. Тогда число a *обратимо по модулю* b, то есть найдётся такое x, что $ax \equiv 1 \pmod{b}$. (Это число x — мы скоро увидим, что оно единственно по модулю b — называют *обратным к* a *по модулю* b.)

▷ Поскольку a и b взаимно просты (их наибольший общий делитель равен 1), найдутся целые x и y, для которых $ax + by = 1$, и $ax - 1 = by$ делится на b, то есть $ax \equiv 1 \pmod{b}$, что и требовалось доказать. ◁

7.9 Пусть $b = 10$. Найдите все взаимно простые с b среди остатков по модулю 10, и укажите для них обратные.

▷ Ответ можно посмотреть в таблице умножения по модулю 10, которая у нас была: взаимно просты 1[1], 3[7], 7[3], 9[9] (в квадратных скобках указаны обратные). ◁

7.10 Пусть a и b взаимно просты. Докажите, что для любого c существует x, при котором $ax \equiv c \pmod{b}$, и что такое x единственно (по модулю b).

• Эта задача говорит о решении линейных уравнений по модулю b, если коэффициент при неизвестной взаимно прост с b.

▷ Условие $ax \equiv c \pmod{b}$, означает, что $ax - c$ делится на b, то есть найдётся такое y, что $ax - c = by$, то есть $ax + by = c$. А это мы уже знаем.

Можно было объяснить и иначе: мы знаем, что есть обратный элемент z, при котором $az \equiv 1 \pmod{b}$. Теперь это сравнение можно умножить на c, и получится $azc \equiv c \pmod{b}$, то есть можно положить $x = zc$.

Теперь единственность: пусть $ax \equiv ax' \pmod{b}$. Мы знаем, что a имеет обратный элемент z по модулю b, и можно умножить на него. Получится $zax \equiv zax' \pmod{b}$, то есть $x \equiv x' \pmod{b}$ (ведь $za \equiv 1 \pmod{b}$). ◁

Простое число взаимно просто со всеми числами, не делящимися на него. Для этого случая получаем такие утверждения:

7.11 Пусть p — простое число. Докажите, что любой ненулевой остаток a по модулю p обратим: существует такое x, что $ax \equiv 1 \pmod{p}$. Докажите, что уравнение (сравнение) $ax \equiv c \pmod{p}$ при $a \not\equiv 0 \pmod{p}$ имеет решение при любом c, и это решение единственно по модулю p.

• В частности, и обратный элемент единствен (как решение сравнения $ax \equiv 1 \pmod{p}$).

▷ Это мы уже делали для произвольного модуля, взаимно простого с a (в частности, годится любое простое p, которое не делит a). ◁

7.12 Покажите, что если p — простое число, и $ab \equiv 0 \pmod{p}$ для каких-то целых чисел a и b, то или $a \equiv 0 \pmod{p}$, или $b \equiv 0 \pmod{p}$ (или оба).

• Это утверждение можно переформулировать так: *если произведение двух целых чисел (ab) делится на p, то хотя бы одно из этих чисел (a или b) делится на p*. Или так: *если два целых числа не делятся на простое p, то их произведение не делится на p*. Или даже так: *если произведение ab делится на p, и при этом a не делится на p, то b делится на p*. Все эти формулировки запрещают одно и то же: сомножители не делятся, а произведение делится.

▷ Пусть ab делится на p, то есть сравнимо с 0 по модулю p, а первый сомножитель a не делится на p. Тогда a, как мы видели в предыдущей

задаче, имеет обратный элемент по модулю p: есть такое x, что $ax \equiv 1 \pmod p$. Теперь перемножим три числа a, x, b и рассмотрим их произведение по модулю p. Если перемножать сначала ax, а потом умножить на b, то получится b. Но если перемножить сначала ab, а потом полученный 0 (по модулю p) умножить на x, то получится 0. Значит, $b \equiv 0 \pmod p$. ◁

• Рассуждения по модулю с непривычки могут казаться странными, поэтому можно изложить решение без сравнений по модулю. Покажем, что если p просто, a не делится на p, и ab делится на p, то b делится на p. Раз p просто и a не делится на p, то a взаимно просто с p. Поэтому (следствие из алгоритма Евклида) можно найти такие x и y, что $ax + py = 1$. Умножим это равенство на b, получим $abx + pby = b$. В левой части оба слагаемых делятся на p (в первом ab делится на p, во втором p есть в явном виде), поэтому их сумма b делится на p.

7.13 Куда надо смотреть в таблицах умножения по модулю p и что проверять, чтобы убедиться, что действительно — в соответствии с доказанным нами — каждый ненулевой элемент имеет единственный обратный? А как проверить, что при $a \not\equiv 0 \pmod p$ уравнение $ax \equiv b \pmod p$ имеет единственное (по модулю p) решение*

▷ Надо убедится, что во всех строках (и столбцах, но это одно и то же), кроме первой (где умножают на 0) остаток 1 встречается ровно один раз.

Во втором случае надо проверить, что в каждой из строк, кроме нулевой первой, *все* остатки по модулю p встречаются ровно один раз. (Другими словами, все строки получаются из $0, 1, 2, \ldots, p-1$ некоторой перестановкой.) ◁

7.14 Найдите обратное к числу 23 по модулю 89.

▷ Мы уже искали решения уравнения $23x + 89y = 1$, и нашли $x = 31$ и $y = 8$. Так что по модулю 89 обратным к 23 будет 31 (и обратное, как мы уже видели, единственно). ◁

7.15 Решите уравнение $23x \equiv 5 \pmod{89}$ (найдите все его целые решения и объясните, почему других нет).

▷ И это мы уже делали в форме решения $23x + 89y = 5$, и тогда нашли $x = 155$. Поскольку мы решаем уравнение по модулю 89, то годится любое число, которое сравнимо с 155 по этому модулю, например $66 = 155 - 89$. Общий вид таких чисел $155 + 89k$ (или $66 + 89l$, если начать с 66). Есть ли другие? мы уже знаем, что уравнение $ax \equiv c \pmod p$

имеет единственное решение по модулю p, если модуль p простой (а 89 — простое число). Так что других решений (кроме чисел вида $155 + 89k$) нет. ◁

Мы уже говорили, что уравнение $ax + by = c$ (при целых коэффициентах a, b, c) имеет решение в целых числах x, y тогда и только тогда, когда c делится на $d = \text{НОД}(a, b)$. Как найти все его решения? Разделим уравнение на d. Тогда получится уравнение $a'x + b'y = c'$, где $a' = a/d$, $b' = b/d$ и $c' = c/d$. Коэффициенты a' и b' в левой части — целые взаимно простые числа (почему?). Если число c' справа нецелое, то решений нет. Если целое, то есть, и одно решение x_0, y_0 можно найти с помощью алгоритма Евклида. Мы уже видели, что значение x' единственно по модулю b', так что все решения можно найти как $x_k = x_0 + kb'$, и соответственно $y_k = y_0 - ka'$.

Напишем какое-то целое число и будем прибавлять к нему какое-то другое целое число много раз (скажем, $3, 8, 13, 18, \ldots$). Получится *арифметическая прогрессия*, а то число, которое прибавляют, называют её *разностью* (потому что такова разность двух соседних членов).

• На числовой оси арифметическую прогрессию можно представлять себе так: мы начинаем с некоторого числа и откладываем много раз какое-то другое число (разность).

7.16 Даны две арифметические прогрессии из целых чисел. Первые члены их могут быть любыми, а разности — положительные взаимно простые целые числа. Покажите, что найдётся целое число, которое входит в обе прогрессии.

▷ Арифметическая прогрессия, которая начинается с a_1, а потом увеличение на b_1, содержит члены вида $a_1 + b_1x$. Вторая прогрессия содержит члены $a_2 + b_2y$. Мы ищем *неотрицательные* x и y, для которых $a_1 + b_1x = a_2 + b_2y$, или $b_1x - b_2y = a_2 - a_1$. Мы уже знаем, что в силу взаимной простоты b_1 и b_2 такие числа x и y найдутся, но как их сделать неотрицательными? Если добавить к x число b_1, а к y число b_2, то решение останется решением (изменения сократятся). Будем так делать, пока x и y не станут неотрицательными. ◁

7.17 Путник начинает движение у столба 0 на кольцевом шоссе длиной в a километров и каждый день проходит b километров. У всех ли километровых столбов ему придётся заночевать — и если не у всех, то у каких именно?

▷ Вопрос можно переформулировать так: какие остатки при делении на b могут давать числа, кратные a? Другими словами, при каких r от 0 до $b-1$ уравнение $ax \equiv r \pmod{b}$ имеет решение? Это бывает, когда найдутся x и y, при которых $ax+by=r$, а на этот вопрос мы ответ знаем: когда r кратно НОД(a,b).

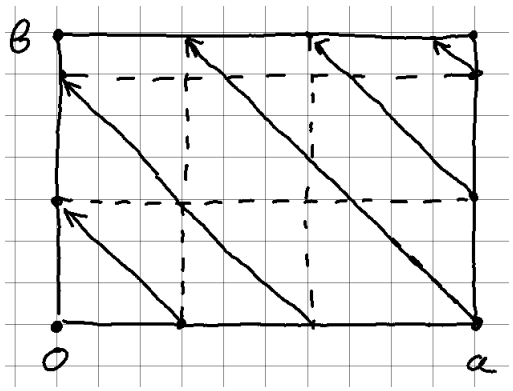
Так что при взаимно простых a и b все столбы будут использованы для ночёвки, а если НОД$(a,b)=rf>1$, то будет каждый r-й столб (все столбы с номерами, кратными r). ◁

7.18 Есть две бочки с большим запасом воды и два ведра, в a литров и b литров, причём a и b — взаимно простые целые числа. Как перелить из одной бочки в другую один литр?

▷ Одно ведро позволяет перелить ax литров, если переливать x раз (отрицательные x соответствуют переливанию в другом направлении). Второе даёт by литров, всего $ax+by$ литров, так что нам надо решить уравнение $ax+by=1$. А это, как мы знаем, возможно, поскольку НОД$(x,y)=1$. ◁

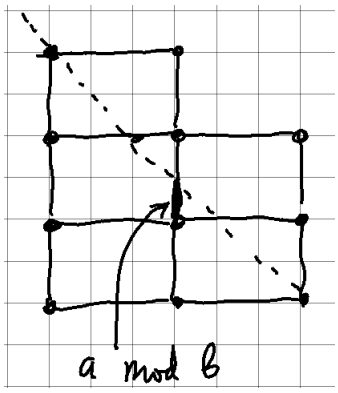
7.19* Пусть теперь имеется одна бочка (из которой можно черпать и куда можно сливать воду) и два ведра в a и b литров, причём a и b — взаимно простые целые числа, и $a>b$. Покажите, что можно отмерить (получить в ведре b) любое целое число литров от 0 до b. (Использовать какие-то другие ёмкости, кроме этих двух вёдер и бочки, нельзя.)

▷ Тут полезно нарисовать, как говорят, *фазовое пространство* нашей системы. В каждый момент ситуация описывается двумя числами: сколько воды в одном ведре (обозначим это количество x) и в другом (y). При этом $0 \leqslant x \leqslant a$ и $0 \leqslant y \leqslant b$. Как в этих терминах описываются наши возможные действия? Если ведро пустое, то его можно наполнить, а если полное — вылить. Это значит, что мы можем с края прямоугольника перейти на другой край (перпендикулярно краю и параллельно другой стороне). Кроме того, мы можем переливать из одного ведра в другое (это соответствует движению под углом 45° к осям).



Начав с $(0, 0)$, мы перепрыгиваем в $(a, 0)$ (наливаем воду в большое ведро), затем двигаемся вверх–налево до $(a - b, b)$, потом перепрыгиваем вниз (выливаем воду из малого ведра), потом снова вверх–налево (в нашем случае вода в большом ведре кончается, а в малом $a - b$), наливаем воду в большое ведро и так далее. Нам надо показать, что продолжая двигаться по этой линии (с пунктирными перепрыгиваниями), мы побываем во всех целых точках на вертикальной оси (от 0 до b).

Чтобы это понять, удобно заменить прыжки переходом в другую копию прямоугольника (топологи сказали бы, что отождествление точек левого и правого края превращает прямоугольник в цилиндр, а после этого отождествление верхнего и нижнего — в тор, а затем мы накрываем этот тор плоскостью).



На рисунке это показано для прямоугольника поменьше и его разложенных по всей плоскости копий. Теперь можно сказать так: когда линия пересекает прямоугольник справа налево, мы смещаемся влево на a и вверх на a, то есть попадаем в точки $a \bmod b$, $2a \bmod b$ и так далее (сдвиг на кратное b соответствует переходу в другую копию, так что можно вычитать). А мы уже знаем, что среди

$ax \mod b$ при НОД $(a, b) = 1$ есть все остатки (потому что a обратимо в остатках по модулю b). ◁

• Если это рассуждение кажется непонятным, полезно проследить, что будет в примере с нашего первого рисунка ($a = 10$, $b = 7$), что в каком порядке будет переливаться, наливаться, выливаться и что будет оставаться в малом ведре, когда большое пустое.

7.20* Будем откладывать на окружности, начав с некоторой точки, одну и ту же (по величине) дугу много раз, и отмечать полученные точки. (Начав с какой-то точки круга, мы делаем равные шаги и никогда не останавливаемся.) Покажите, что возможно одно из двух: либо мы через несколько шагов вернёмся в исходную точку, либо наши отметки будут, как говорят, *плотны на окружности* — это значит, что на любой дуге (ненулевой длины) будут наши отметки.

▷ Будем откладывать и откладывать точки. Если в какой-то момент мы придём в уже посещённую точку, то между ними будет целое число оборотов, так что дальше всё будет повторяться (первый случай). Если же нет, то точек будет становиться всё больше и больше, а расстояние между ближайшими точками всё меньше и меньше: если точек n, то одна из дуг между ними будет меньше $1/n$. Посмотрим на переход по этой дуге: ещё через столько же шагов мы снова сдвинемся на то же расстояние, меньшее $1/n$. Значит, мы будем двигаться шагами, равными этой малой дуге, и таким образом рано или поздно попадём в любую дугу длины больше $1/n$. Поскольку n произвольно, то в любую дугу мы рано или поздно попадём. ◁

• На самом деле можно показать, что не только наши отметки будут плотны на окружности, но ещё они равномерно распределены: это означает, грубо говоря, что средняя доля отметок, попадающих в некоторую дугу, пропорциональна длине этой дуги. Но это уже доказать сложнее (наиболее естественное доказательство использует разложение непрерывных функций в ряд Фурье, точнее, их приближение тригонометрическими многочленами).

7.21* Возьмём произвольное положительное число α (не обязательно целое) и будем смотреть на числа α, 2α, 3α, ... Покажите, что возможно только два варианта: либо какое-то из них будет целым (и тогда α — отношение двух целых чисел, то есть рациональное число), либо среди них будет число, которое в десятичной записи будет иметь после запятой сто нулей.

• В этой задаче сто нулей можно заменить на любую группу цифр.

▷ Эта задача сводится к предыдущей: мы двигаемся по окружности длины 1 шагами в α. Либо мы вернёмся в исходную точку (и тогда α рационально), либо нет. Во втором случае мы попадём в любую дугу, то есть, в частности, в отрезок от 0 до 0,000 ... 01 (сто нулей), что и означает, что у некоторого целого кратного α будет 100 нулей после запятой.

По тем же причинам (отрезок такой же длины, но с другого места) можно получить любую группу цифр после запятой. ◁

• В этой главе мы извлекали следствия из такого факта (который, в свою очередь, получается как результат алгоритма Евклида): уравнение $ax + by =$ НОД (a, b) имеет решение в целых числах x и y. Его можно доказать и неконструктивно. Вот как это делается. Рассмотрим числа, выразимые через a и b. Возьмём среди них наименьшее положительное число d. Покажем, что это будет общий делитель a и b, который делится на любой другой общий делитель. Второе понятно: если d' делит a и b, то оно делит и любое выразимое число, в частности, наименьшее выразимое d. Теперь первое: почему a, скажем, делится на d? Разделим a на d с остатком: $a = qd + r$, где $0 \leqslant r < d$. Здесь числа a и qd выразимы, поэтому $r = a - qd$ выразимо, что невозможно при $r \neq 0$, так как d было *наименьшим* выразимым положительным числом (а остаток при делении на d всегда меньше d). Значит, d будет наибольшим общим делителем, то есть НОД $(a, b) = d$ выразим.

7.22* Пусть a, b — положительные целые числа. Рассмотрим их *общие кратные*, то есть числа, делящиеся и на a, и на b. (Таково, например, ab.) Пусть m — их *наименьшее* общее кратное. Покажите, что оно будет делителем любого общего кратного a и b.

• Это легко будет следовать из теоремы о единственности разложения на множители, как мы увидим, но и без неё это доказывается довольно просто.

▷ Пусть m' — какое-то другое общее кратное (будем считать, что положительное, иначе изменим знак). Поскольку m было наименьшим, то $m < m'$. Поделим m' с остатком на m: пусть $m' = qm + r$, где $0 \leqslant r < m$. Тогда $r = m' - qm$ будет общим кратным a и b (как разность двух общих кратных), но $r < m$, а m было наименьшим. Значит, $r = 0$, что и требовалось доказать. ◁

7.23 Докажите, что если a делится на b и на c, причём b и c взаимно просты, то a делится на bc.

▷ Мы увидим скоро, что это сразу видно, если воспользоваться единственностью разложения на простые множители. Но можно доказать и так: раз b и c взаимно просты, можно найти такие x и y, что $bx + cy = 1$. Тогда $a = a(bx + cy) = abx + acy$. Оба сладаемых делятся на bc. Скажем,

abx делится на bc, потому что ax делится на c (а это потому, что a делится на c). Аналогично и для acy. Значит, и сумма, равная a, делится на bc. $\triangleleft$

7.24 Мы хотим найти целое число, которое даёт остаток 3 при делении на 4 и остаток 6 при делении на 9. Какое уравнение в целых числах надо для этого решать и есть ли у него решения?

$\triangleright$ Числа, которые дают остаток 3 при делении на 4, имеют вид $4k+3$, а числа, которые дают остаток 6 при делении на 9, имеют вид $9l+6$. Поэтому, чтобы найти общее число, мы должны решить уравнение $4k+3 = 9l+6$, или $4k - 9l = 3$. Мы уже знаем, что оно имеет решение, поскольку 4 и 9 взаимно просты. Впрочем, тут оно сразу видно: $k = 3$, $l = 1$, $4k+3 = 9l+6 = 15$, так что искомое число 15. $\triangleleft$

7.25 Пусть a и b — взаимно простые целые числа, а m и n — произвольные (тоже целые) числа. Докажите, что можно найти число u, для которого

$$u \equiv m \pmod{a} \quad \text{и} \quad u \equiv n \pmod{b}.$$

$\triangleright$ Как и в прошлой задаче, здесь надо решать уравнение $m+ak = n+bl$ (считая переменными k и l: при данных a, b, m, n мы ищем подходящие k и l). Это уравнение можно переписать как $ak - bl = n - m$, и оно имеет решение, так как a и b взаимно просты. (Точнее, a и $-b$ взаимно просты.) $\triangleleft$

На это утверждение можно посмотреть иначе. Пусть b и c взаимно просты. Если мы знаем остаток от деления какого-то числа x на bc, то можно восстановить (даже не зная x) остатки от деления на b и c, надо просто поделить остаток $x \bmod bc$ на b и на c.

Предыдущая задача показывает, что *при этом может получиться любая пара остатков* (всего таких пар bc, как и остатков по модулю bc). При этом разные остатки (не сравнимые по модулю bc) дадут разные пары: если x и x' сравнимы по модулям b и c одновременно, то $x - x'$ делится на b и на c. А раз b и c взаимно просты, то $x - x'$ делится и на bc (задача 23).

Математики говорят, что *возникает взаимно-однозначное соответствие*

$$x \bmod bc \leftrightarrow (x \bmod b, x \bmod c)$$

между остатками по модулю bc и парами остатков по взаимно простым модулям b и c, и называют это утверждение *китайской теоремой об остатках*).

▷ История этого названия, как всегда довольно запутанная. Если верить википедии, то ещё в третьем веке новой эры китайский математик Сунь цзы разобрал в своём сочинении один из примеров такого рода (см. следующую задачу 26), и потом это много раз переоткрывалось, обобщалось, доказывалось и т.п. ◁

7.26* Есть неизвестное число предметов. Если считать их тройками, останутся два, если пятёрками, останутся три, и если семёрками, то останутся два. Сколько всего предметов?

• В этой задаче модуля не два, а три (3, 5, 7), но они попарно взаимно просты, и утверждение обобщается и на этот случай.

▷ Тут надо найти x, для которого $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$. Раз уж совпали остатки по модулям 3 и 7, удобно начать с них: $x - 2$ делится на 21, то есть $x = 21k + 2$. Теперь по модулю 5 получаем $21k + 2 \equiv 3 \pmod 5$, или $k + 2 \equiv 3 \pmod 5$, так что $k \equiv 1 \pmod 5$. Минимальный ответ $k = 1$, то есть число 23, дальше $128 = 6 \cdot 21 + 2$, и так далее. ◁

7.27* Докажите такое обобщение китайской теоремы об остатках (на несколько модулей): если $b_1, \ldots, b_n$ — попарно взаимно простые целые числа, а $c_1, \ldots, c_n$ — произвольные остатки по модулям $b_1, \ldots, b_n$ соответственно, то система сравнений

$$x \equiv c_1 \pmod{b_1}, \quad x \equiv c_2 \pmod{b_2}, \ \ldots, \quad x \equiv c_n \pmod{b_n}$$

имеет решение x, и притом это x ровно одно по модулю $b_1 \cdot \ldots \cdot b_n$.

▷ Уже доказанное (про два остатка) позволяет заменить «$x \equiv c_1 \pmod{b_1}$ и $x \equiv c_2 \pmod{b_2}$» на $x \equiv c_{12} \pmod{b_1 b_2}$, и уменьшить число сравнений. Надо только отметить, что $b_1 b_2$ взаимно просто с любым b_k из остальных, потому что это произведение двух взаимно простых с ним чисел. После этого повторяем рассуждение, пока не останется одно сравнение. ◁

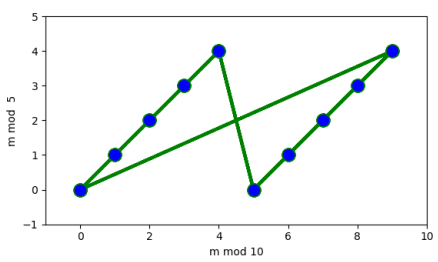
7.28* Иногда шахматную доску «сворачивают в тор»: если фигура выходит за границу, то её возвращают с другой стороны (сдвигая по горизонтали на ширину доски и/или по вертикали на высоту доски).

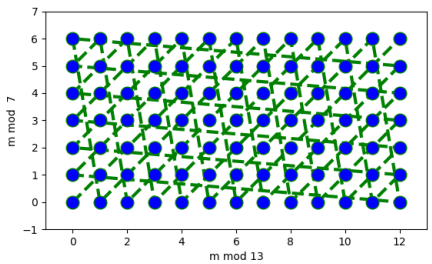
Докажите, что на свёрнутой в тор доске $a \times b$ со взаимно простыми a и b шахматный король, который начинает с какой-то клетки и всё время идёт вправо-вверх по диагонали, побывает во всех клетках по разу и вернётся в исходную клетку.

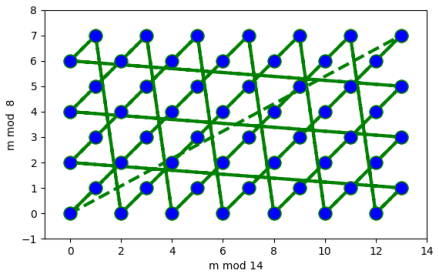
• На одном из следующих рисунков как раз и показан путь короля. (На каком?)

▷ Шахматный король ведёт себя в точности как остатки $(x \bmod a, x \bmod b)$ при увеличении x на 1, так что достаточно сослаться на китайскую теорему об остатках. ◁

Китайскую теорему об остатках (и условие взаимной простоты) можно проиллюстрировать картинками, на которых изображены возможные пары остатков $(x \bmod a, x \bmod b)$ для трёх пар модулей: (10, 5), (13, 7) и (14, 8). Линии соединяют пары остатков для соседних значений x.







В первом случае остаток при делении на 5 однозначно определяется остатком при делении на 10 (является *функцией* от него). Во втором случае — как и положено для взаимно простых модулей — возможны все пары остатков. Третий случай промежуточный: в нём модули не кратны друг другу, но и не взаимно просты, поэтому возможны многие пары остатков, но не все.

7.29* Какая доля всех пар остатков реализуется на последней картинке? Общий вопрос: если мы рассмотрим все пары остатков по модулям a, b, то какая их доля реализуется как $(x \bmod a, x \bmod b)$?

▷ На картинке они идут в шахматном порядке, так что реализуется половина. В общем случае ответ будет $1/\text{НОД}(a,b)$. В самом деле, появление пары (u,v) означает, что уравнение $u + ax = v + by$ имеет решение. Его можно переписать как $ax - by = v - u$, так что $v - u$ должно делиться на $\text{НОД}(a,b)$, и в каждой вертикали (или горизонтали) будет как раз доля $1/\text{НОД}(a,b)$. ◁

7.30* Покажите, что уравнение $ax+by+cz = 1$ с целыми коэффициентами a, b, c имеет решение (с целыми значениями переменных x, y, z) тогда и только тогда, когда у a, b, c нет общего делителя, кроме 1.

• В терминах платежей: монетами в a, b и c флоринов можно уплатить 1 флорин (и потому любое целое число) в том и только том случае, когда нет (целого положительного) числа, которому кратны все три монеты.

▷ Если общий делитель $d > 1$ есть, то левая часть в $ax + by + cz$ кратна d, а правая нет. Обратное чуть сложнее. Прежде всего заметим, что в виде $ax + by$ можно представить все числа, кратные $\text{НОД}(a,b)$, поэтому достаточно решить уравнение $\text{НОД}(a,b)t + cz = 1$ относительно t и z. Если его нельзя решить, то у $\text{НОД}(a,b)$ и c есть общий делитель, который будет делителем всех трёх чисел a, b, c. ◁

7.31* Игрок тасует колоду из 52 карт (рубашкой вверх) так: он берёт стопку из 10 верхних карт и меняет её местами с оставшимися картами (так что теперь сверху 42 другие карты, внизу снятые 10, по-прежнему все карты рубашкой вверх). Затем он делает то же самое ещё раз, потом ещё раз и так до бесконечности. Сколько карт побывают в низу колоды (будут в какой-то момент на последнем месте в колоде)?

▷ Описанное преобразование — сдвиг на 10 в цикле из 52 карт, поэтому получатся все сдвиги, кратные $\text{НОД}(10, 52) = 2$. Значит, в низу колоды побывает ровно половина всех карт. ◁