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?

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.

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?

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.) ◁

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

• 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.

• 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 $\text{НОД}(15, 8) = 1$.

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 $\text{НОД}(a, b)$.

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

• 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.

• 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 $\text{НОД}(a, b)$.

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.)

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

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 $ax \equiv 1 \pmod{p}$).

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.

• 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*

7.14 Найдите обратное к числу 23 по модулю 89.

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

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?

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?

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.)

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.

• 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.

• В этой главе мы извлекали следствия из такого факта (который, в свою очередь, получается как результат алгоритма Евклида): уравнение $ax + by = \text{НОД}(a, b)$ 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.

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

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?

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

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

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.

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

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

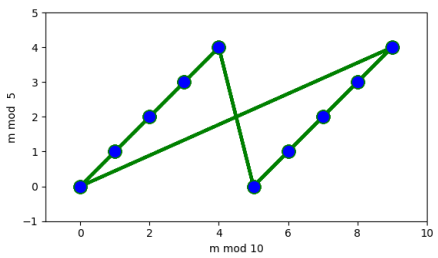
имеет решение x, и притом это x ровно одно по модулю $b_1 \cdot \ldots \cdot b_n$.

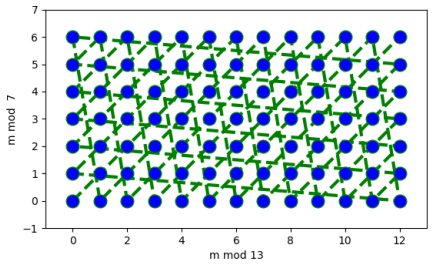
7.28* Иногда шахматную доску «сворачивают в тор»: если фигура выходит за границу, то её возвращают с другой стороны (сдвигая по горизонтали на ширину доски и/или по вертикали на высоту доски).

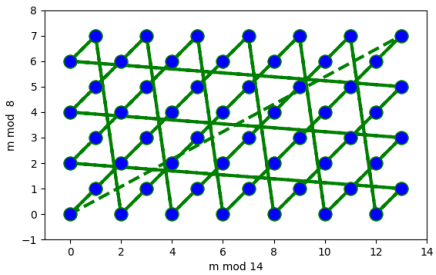
Докажите, что на свёрнутой в тор доске $a \times b$ со взаимно простыми a и b шахматный король, который начинает с какой-то клетки и всё время идёт вправо-вверх по диагонали, побывает во всех клетках по разу и вернётся в исходную клетку.

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

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 $(x \bmod a, x \bmod b)$?

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.

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)?