8ВМ, спецкурс, занятие 8

7 октября 2022

Обратный алгоритм Евклида

Запишем алгоритм Евклида для чисел a и b, причем деление с остатком будем писать в развернутом виде.

$$\begin{array}{rll}
a \text{ делим с остатком на } b: & a = q_1 b + r_1 & r_1 < |b| \\
b \text{ делим с остатком на } r_1: & b = q_2 r_1 + r_2 & r_2 < r_1 \\
r_1 \text{ делим с остатком на } r_2: & r_1 = q_3 r_2 + r_3 & r_3 < r_2 \\
 & \dots & \\
r_{n-1} \text{ делим с остатком на } r_n: & r_{n-1} = q_{n+1} r_n + r_{n+1} & r_{n+1} < r_n \\
r_n \text{ разделилось нацело на } r_{n+1}: & r_n = q_{n+2} r_{n+1} &
\end{array}$$

$$(a,\, b) = (b,\, r_1) = (r_1,\, r_2) = \dots = (r_{n-1},\, r_n) = (r_n,\, r_{n+1}) = (r_{n+1},\, 0) = r_{n+1}$$

Остатки $r_1, r_2, \dots, r_{n+1}$ убывают, поэтому рано или поздно остаток станет нулевым и алгоритм закончит действие.

Теперь можно последовательно выражать остатки $r_1, r_2, \dots, r_{n+1}$ через a и b:

$$r_1 = a - q_1 b$$

$$r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = -q_2 a + (1 + q_1 q_2) b$$

$$r_3 = r_1 - q_3 r_2,$$

а r_1 и r_2 мы уже выразили через a и b. И так далее. В итоге получится, что

$$\text{НОД}(a,\, b) = r_{n+1} = xa + yb,$$

где x и y — какие-то целые числа.

> *Обратный алгоритм Евклида* позволяет находить такие целые x и y, что $xa + yb = (a,\, b)$.

Определение. Уравнения, которые нужно решить в целых (или натуральных) числах, называются *диофантовыми уравнениями.*

Уравнения вида $ax + by = c$, где a, b, c — какие-то целые числа, у которых нужно искать целые решения $(x,\, y)$ называются *линейными диофантовыми уравнениями* с двумя переменными.

Для решения линейных диофантовых уравнений используется следующая идея. Для простоты предположим, что a и b — взаимно простые числа.

Сначала нужно каким-то образом найти какое-то *частное решение* $(x_0,\, y_0)$ этого уравнения. Его можно угадать или воспользоваться обратным алгоритмом Евклида. Тогда $ax + by = c$ и $ax_0 + by_0 = c$, а значит

$$a(x - x_0) + b(y - y_0) = 0$$

Получается, что $x - x_0$ делится на b, то есть $x - x_0 = kb$. Тогда $y - y_0 = -ka$. Так мы находим *общий вид решения* уравнения: $x = kb + x_0$, $y = -ka + y_0$, где k — произвольное целое число.

1 Кузнечик умеет прыгать вдоль прямой на 6 см и 10 см.

a Сможет ли он попасть в точку отстоящую от исходной на 7 см? А на 14 см?

b Опишите все точки, в которые он сможет попасть.

2 Примените обратный алгоритм Евклида к числам a 28 и 11; b 189 и 97; c 605 и 44; d 162 и 546.

3 Даны углы 32° и 25°. Как построить угол в 1°?

4 Решите уравнения в целых числах:

a $3x + 5y = 1$;

b $525x + 231y = 43$;

c $15x + 43y = 3$;

d $162x + 46y = 2000$.

5 На площади стоят дяди и тети. У каждого дяди в кармане было 13 рублей, у каждой тети — 23 рубля. По площади прошел вор и незаметно украл все деньги. Какое наибольшее количество людей могло стоять на площади, если вор украл всего 1543 рубля?

6 На складе 3003 шкафа. Розовый шлюбзик умеет переносить 7 шкафов за раз, а лысый шпегльморгер — 20 шкафов за раз. Сколькими способами можно отрядить на склад отряд шлюбзиков и шпегльморгеров, чтобы они за раз вытащили со склада все шкафы, и каждый из них был загружен полностью?

7* Найдите все решения уравнения $2x + 3y + 5z = 13$ в целых числах.

8 У скупого рыцаря есть 5 сундуков с золотом: в первом сундуке 1001 золотая монета, во втором — 2002, в третьем — 3003, в четвертом — 4004, в пятом — 5005. Каждый день скупой рыцарь выбирает 4 сундука, забирает из них по 1 монете и перекладывает в оставшийся сундук. Спустя какое-то время в первом сундуке не осталось монет, а еще в одном сундуке было ровно 2022 монеты. В каком?