Алгоритм Евклида

1 Определение

Алгоритм Евклида позволяет найти наибольший общий делитель двух чисел (НОД). Подробно про НОД вы узнаете на лекциях, сейчас предлагается попробовать это понятие на примерах. Например, НОД 15 и 10 равен 5, обозначим это так: $(15, 10) = 5$. Действительно, и 15, и 10 делятся на 5, но оба они ни на какое большее число не делятся.

Другие примеры:

$$(6, 8) = 2$$
$$(100, 60) = 20$$
$$(123, 321) = 3$$
$$(5, 7) = 1$$
$$(42, 0) = 42$$
$$(20, 30) = 10$$

Заметим, что НОД всегда хотя бы 1, потому что любые числа делятся на 1.

2 Алгоритм Евклида

Оказывается, что если у вас есть два числа a и b, для которых вы считаете НОД, можно уменьшить одно из чисел, не меняя НОД. Если точнее, то $(a, b) = (a, b \bmod a)$. Здесь $x \bmod y$ это остаток от деления. Остатки изучались в школе, на лекции мы их вспомним, если не помните до лекции, спросите в Discord.

Например, $(6, 20) = (6, 20 \bmod 6) = (6, 2)$. Можете убедиться, что действительно, $(6, 20) = 2$ и $(6, 2) = 2$.

Теперь мы можем писать алгоритм Евклида. Например, если нужно вычислить $(46, 20)$, можно написать следующий ряд чисел:

$$46, 20, 6, 2, 0$$

Здесь первые два числа взяты из условия. Каждое следующее число — это остаток от деления предпредпоследнего на предпоследнее. Здесь $6 = 46 \bmod 2$, $2 = 20 \bmod 6$, $0 = 6 \bmod 2$.

Этот ряд чисел говорит, что $(46, 20) = (20, 6) = (6, 2) = (2, 0) = 2$. Т.е. НОД всегда равен предпоследнему числу, перед нулём. Ответ в задаче: $(46, 20) = 2$.

Соответственно, чтобы выполнить алгоритм Евклида, нужно выписать ряд чисел, вычисляя остатки.

3 Расширенный алгоритм Евклида

Оказывается, что НОД двух чисел всегда «линейно выражается» через эти числа. Другими словами, если у вас есть два числа a и b, их НОД $d = (a, b)$, то можно подобрать целые x и y, такие, что $d = ax + by$.

Вспомним, что $2 = (46, 20)$. Для этого примера подберем $2 = 46 \cdot (-3) + 20 \cdot 7$, т.е. $x = -3$, $y = 7$.

Чтобы уметь находить такие x и y, нужно расширить алгоритм Евклида, т.е. проделывать дополнительные вычисления. Сначала давайте добавим в вычисления не только остатки от деления, а еще неполные частные. Например, при делении 46 на 20 получается $\frac{46}{20} = 2,3$, т.е. неполное частное равно 2, это округление вниз результата деления, и остаток 6. Можно записать это так: $46 - 2 \cdot 20 = 6$. В этом выражении видно и неполное частное, и остаток.

Получается вот такая запись вычисления НОД 46 и 20

$$
\begin{array}{l}
46 \\
20 \\
6 \quad {\scriptstyle 46-2\cdot 20} \\
2 \quad {\scriptstyle 20-3\cdot 6} \\
0 \quad {\scriptstyle 6-3\cdot 2}
\end{array}
$$

Повторю, что это повторение вычислений из обычной версии алгоритма Евклида, но записано больше информации о том, как именно получались остатки.

Последнее, что остается сделать, чтобы получить расширенный алгоритм Евклида — это добавить вычисления линейных комбинаций на каждом шаге. Исходные числа 46 и 20 выражаются через себя всегда одним и тем же способом: $46 = 1 \cdot 46 + 0 \cdot 20$ и $46 = 0 \cdot 46 + 1 \cdot 20$. Вы во всех задачах будете писать эти 1, 0 и 0, 1.

Каждое следующее число в списке получается вычитанием линейных комбинаций друг из друга:

$$
\begin{aligned}
46 &= 1 \cdot 46 + 0 \cdot 20 \\
20 &= 0 \cdot 46 + 1 \cdot 20 \\
6 &= 1 \cdot 46 + (-2) \cdot 20 \quad {}^{46-2\cdot 20} \\
2 &= (-3) \cdot 46 + 5 \cdot 20 \quad {}^{20-3\cdot 6} \\
0 &= \text{неважно} \quad {}^{6-3\cdot 2}
\end{aligned}
$$

Надо один раз понять, как делаются эти вычисления, больше ничего сложного в алгоритме нет. Имеется в виду, например, что раз $6 = 46 - 2 \cdot 20$, то, заменив 46 и 20 на их линейные комбинации, получится, что $6 = (1 \cdot 46 + 0 \cdot 20) - 2 \cdot (0 \cdot 46 + 1 \cdot 20) = (1 - 2 \cdot 0) \cdot 46 + (0 - 2 \cdot 0) \cdot 20 = 1 \cdot 46 + (-2) \cdot 20$.

Дальше аналогично. Самая частая проблема при решении — это запутаться в знаках, часто приходится *вычитать отрицательные* числа.

Ответ в задаче:

1. НОД $(46, 20) = 2$
2. линейное представление $2 = (-3) \cdot 46 + 5 \cdot 20$.

Если вы найдете этот алгоритм в другом месте, там будут те же вычисления, но записанные иначе. Посмотрите, например, учебник Рыбина и Позднякова, он выложен на сайте. Обычно многое из того, что написано в последнем решении, опускается. Нет смысла постоянно повторять 46 и 20, например.