Студент: Тимур Хабибуллин
Группа: 1
Дата: 5 мая 2022 г.

---

1. Алгоритм Евклида работает по следующей формуле:

$$\texttt{gcd(a, b) = gcd(b, a\%b)}$$

На каждом шаге одно из чисел уменьшается не менее чем в 2 раза. Пусть $a \geqslant 2b$, тогда $a\%b < b \leqslant a/2$. Или же если $2b > a > b$, тогда $a\%b = a - b < a - a/2 = a/2$.
Тогда в худшем случае за $O(\log(\min(a,b)+1))$ (зедсь $+1$ нужно для того, если $\min(a,b) = 0$) операции мы дойдем до того, что второй агрумент `gcd` станет единицей:

$$\texttt{gcd(a, b)} = \texttt{gcd(b, a\%b)} = \cdots \texttt{= gcd(x, 1)}$$

и еще за одну доп операцию мы поймем, что x — наибольший общий делитель Итого в худшем случае асимптотика алгоритма $O(\log(\min(a,b)+1)+1)$.

2. (a) Пусть $n = O(\log_2(a))$, $m = O(\log_2(b))$. На каждом шаге мы проводим деление по модулю, значит, каждый раз оно работает за $O(nm)$ (грубая оценка). При этом в предыдущей задаче показали, что надо сделать $O(\log(\min(a,b)+1)$ шагов, чтобы получить результат работы алгоритма Евклида. На каждом шаге одно из чисел уменьшается хотя бы в 2 раза, поэтому длина этого числа в двоичной системе исчисления уменьшается на 1. Тогда, учитывая то, что $a, b > 0$ и что $\log(x)$ — монотонная функция, всего шагов будет

$$O(\log(\min(a,b)+1)) = O(\min(\log(a), \log(b))) = O(\min(m,n))$$

Тогда асимптотика алгоритма $O(nm\min(n,m)))$.

(b)
- Проверим равенство

$$\texttt{gcd(2a, 2b)} = 2\texttt{gcd(a, b)}$$

Пусть $x = \texttt{gcd(a, b)}$, $y = \texttt{gcd(2a, 2b)}$ Если $2a, 2b \sim y$, то тогда $a, b \sim \frac{1}{2}y \leqslant x$
В другу сторону: если $a, b \sim x$, то $2a, 2b \sim 2x \leqslant y$. Получаем

$$y \leqslant 2x,\ 2x \leqslant y,$$

значит, выполняется равенство.

- Проверим равенство

$$\texttt{gcd(a, 2b)} = \texttt{gcd(a, b)}$$

Пусть $x = \texttt{gcd(a, b)}$, $y = \texttt{gcd(a, 2b)}$ Если $a, b \sim x$, то $a, 2b \sim x \leqslant y$.
С другой стороны $a, 2b \sim y$, тогда $a \sim y \leqslant x$.
Как и в прошлом пункте, получаем равенство.

- Воспользуемся этими фактами. Пусть хотим посчитать `gcd(a,b)`. На каждом шаге проверяем текущие числа на четность за $O(max(a,b))$. Если одно число четное, то делим его пополам, если оба, то делим оба и запоминаем, что ответ надо будет умножить на 2, это тоже все дается за $O(max(a,b))$. Если оба числа нечетные, то вместо деления с отстатком, как в обычном алгоритме Евклида, вычтем из большего меньшее, тогда полученное число окажется четным и можно будет его сразу же разделить пополам. Т.е.

$$\texttt{gcd(2k+1, 2m+1)} = \texttt{gcd(2k+1, 2(k-m))} = \texttt{gcd(2k+1, k-m)}$$

Такую ситуацию мы обработаем тоже за $O(max(a,b))$. Получается, что на каждом шаге мы уменьшаем одно из чисел хотя бы 2 раза, поэтому всего шагов будет не более чем $O(max(a,b))$. В итоге, получаем асимптотику алгоритма $O((max(a,b))^2)$.

3. Отличие этого алгоритма в том, что мы помечаем числа составными не начиная с $2i$, а с i^2. Покажем по индукции, что на i-шаге среди $2 * i, \ldots, i^2 - 1$ все числа, кратные i уже помечены составными.
   Очевидно верно для $i = 1, 2$. Предположим, что верно для $i = k$. Рассмотрим $i = k+1$. Тогда для любого $i \leqslant k$ мы пометили составными числа, вида $m{*}i,\ m \in \mathbb{Z}$. Среди чисел $2(k{+}1), \ldots, (k{+}1)^2{-}1$ числа, кратные $k+1$ имеют вид $\alpha(k+1)$, где $\alpha = 2, \ldots, k$. Но все эти числа кратны $i = \alpha = 2, \ldots, k$, поэтому мы должны были пометить их составными на предыдущих шагах. Значит, можно помечать числа составными сразу с $(k+1)^2$.

4.