Алгоритм Евклида

На двух теоремах, доказанных в предыдущем листке, основан способ быстрого нахождения наибольшего общего делителя двух чисел, который носит название алгоритма Евклида. Для начала отметим следующее:

1. Если одно из двух чисел равно нулю, то их наибольший общий делитель равен наибольшему делителю второго числа.
2. Множество делителей отрицательного целого числа совпадает с множеством делителей противоположного ему по знаку положительного числа.

Благодаря этому задача о нахождении наибольшего общего делителя двух чисел сводится к нахождению наибольшего общего делителя двух натуральных чисел. Предположим, что требуется найти наибольший общий делитель двух натуральных чисел a и b, причем $a > b$. Пусть остаток от деления a на b равен r, это означает, что при некотором q верно равенство $a = bq+r$, а значит на основании теоремы 2 предыдущего листка имеем равенство $(a; b) = (b; r)$. Поскольку $r < b < a$, то нахождение наибольшего общего делителя двух чисел свелось к нахождению наибольшего общего делителя двух чисел, одно из которых стало меньше. Теперь можно повторить эту операцию снова, и, разделив b на r с остатком, заменить $(b; r)$ на следующую пару чисел: r и вновь получившийся остаток. Так продолжается до тех пор, пока в какой-то вновь полученной паре одно из чисел не будет делиться на другое без остатка. Тогда, согласно теореме 1 предыдущего листка, наибольший общий делитель этой пары чисел будет равен одному из чисел этой пары.

Пример 8.1. Найти $(7462, 6279)$.

Решение. Пользуясь алгоритмом Евклида, имеем

$$\begin{aligned} &(7462, 6279) = & \qquad & 7462 = 6279 \cdot 1 + 1183 \\ &= (6279, 1183) = & & 6279 = 1183 \cdot 5 + 364 \\ &= (1183, 364) = & & 1183 = 364 \cdot 3 + 91 \\ &= (364, 91) = 91 & & 364 = 91 \cdot 4 \end{aligned}$$

Ответ: 91.

Заметим, что благодаря алгоритму Евклида при нахождении наибольшего общего делителя нам не потребовалось искать разложение чисел на простые множители. В данном случае найти его не очень просто, поскольку исходные числа содержат такие простые делители, как 7, 13, 23, 41. К сожалению алгоритмы разложения чисел на простые множители работают довольно долго, ведь иногда приходится перебрать много вариантов, прежде чем удастся найти очередной простой делитель. В этом отношении алгоритм Евклида оказывается намного быстрее, и именно он обычно используется для нахождения наибольшего общего делителя с помощью компьютера. Скорость его работы позволяет понять следующая теорема, доказанная в 1845 году французским математиком Г. Ламе.

Теорема 8.1. Количество делений, необходимое для вычисления наибольшего общего делителя двух положительных чисел с помощью алгоритма Евклида, не превышает пятикратного количества цифр в десятичной записи меньшего из этих двух чисел.

Так, согласно теореме, если нужно найти наибольший общий делитель двух десятизначных чисел, то потребуется не более пятидесяти делений. Доказательство данной теоремы достаточно сложное, поэтому приводить его здесь мы не будем.

Пример 8.2. Определите на сколько и при каких натуральных значениях n может быть сократима дробь $\dfrac{4n+1}{11n+2}$.

Решение. Дробь будет сократима, если числитель и знаменатель имеют какой-либо общий делитель. Выясним, какой может быть наибольший общий делитель у числителя и знаменателя. Пользуясь теоремой 2 предыдущего листка можно записать серию равенств

$$\begin{aligned} &(11n+2, 4n+1) = && 11n+2 = (4n+1)\cdot 2 + 3n \\ &= (4n+1, 3n) = && 4n+1 = 3n\cdot 1 + n + 1 \\ &= (3n, n+1) = && \\ &= (n+1, -3) && 3n = (n+1)\cdot 3 - 3 \end{aligned}$$

Данную серию равенств мы сознательно здесь не назвали алгоритмом Евклида, хотя она на него и очень похожа. Дело в том, что в алгоритме Евклида на каждом этапе происходит деление с остатком, поэтому число -3 там возникнуть не может.

Поскольку у числа -3 есть только два положительных делителя, 1 и 3, то $(n+1, -3)$ может принимать значения только 1 или 3. Кстати, можно предварительно с помощью равенства $(n+1, -3) = (n+1, 3)$ вообще избавиться от отрицательных чисел. Если n дает остаток 2 при делении на 3, т.е. $n = 3k+2$, то $n+1 = 3k+3$ делится на 3, а значит $(n+1, -3) = 3$ и исходная дробь сократима на 3. Если же $n+1$ при делении на 3 дает остаток 0 или 1, то $n+1$ не делится на 3, тогда $(n+1, -3) = 1$, что означает, что исходная дробь несократима.

Ответ: если n при делении на 3 дает остаток 2, то дробь сократима на 3, если n при делении на 3 дает остаток 0 или 1, то дробь несократима.

Заметим еще одно важное свойство, которое следует из алгоритма Евклида. Пусть требуется найти наибольший общий делитель чисел a и b, при этом число k является одним из делителей чисел a и b. Тогда, действуя по алгоритму Евклида, на каждом шаге имеющаяся пара чисел заменяется на другую пару чисел, которая имеет такой же набор делителей, что и имевшаяся пара, это следует из теоремы 2 предыдущего листка. Поэтому число k будет являться общим делителем каждой следующей пары чисел. В частности, k будет являться делителем последней пары чисел в алгоритме. Однако наибольший общий делитель чисел a и b равен одному из чисел в этой последней паре. Но это означает, что k делит наибольший общий делитель a и b. Тем самым мы доказали следующую теорему:

Теорема 8.2. Любой общий делитель двух чисел делит их наибольший общий делитель.

С ее помощью можно получить одно важное свойство:

Теорема 8.3. Для любого натурального числа m верно равенство $(ma, mb) = m(a, b)$.

Обозначим $(a, b) = d$, $(ma, mb) = D$, тогда необходимо доказать, что $D = md$. Поскольку числа ma и mb делятся на m, то согласно предыдущей теореме $m|D$ и можно записать $D = md'$. Тогда получаем, что $md'|ma$, $md'|mb$, откуда $d'|a$, $d'|b$ (почему?). Но тогда d' — один из делителей чисел a и b, который не может быть больше наибольшего общего делителя этих чисел, поэтому $d' \leqslant d$, а значит $D = md' \leqslant md$.

С другой стороны $d|a$, $d|b$, следовательно $md|ma$, $md|mb$, поэтому md один из делителей чисел ma и mb, значит $md \leqslant D$. Но из неравенств $D \leqslant md$ и $md \leqslant D$ можно сделать вывод, что $D = md$, а это и требовалось доказать.

Задачи

Задача 8.1. Найдите с помощью алгоритма Евклида
а) $(198, 72)$; **б)** $(2337, 2109)$; **в)** $(2448, 1513)$; **г)** $(12345, 6789)$.

Задача 8.2. Определите на сколько и при каких натуральных значениях n сократимы дроби
а) $\dfrac{2n+5}{7n+17}$; **б)** $\dfrac{3n+2}{5n+2}$; **в)** $\dfrac{3n+4}{4n+3}$.

Задача 8.3. Какие значения могут принимать наибольшие общие делители следующих пар чисел в зависимости от натуральных значений n:
а) $(25, 5n+3)$; **в)** $(n^3+5n, 6)$;
б) $(6n^2+5n, 3n+1)$; **г)** $(n^4+2n^3+2n^2+3n, n^3+2n)$.

Задача 8.4. Найдите число, при делении на которое числа 908389, 734171 и 441168 дают одинаковые отличные от нуля остатки.

Задача 8.5. Найдите $(\underbrace{222\ldots22}_{448\text{ раз}}, \underbrace{222\ldots22}_{42\text{ раза}})$.

Задача 8.6. Укажите наименьшее натуральное значение n, при котором каждая из дробей $\dfrac{12}{n+15}, \dfrac{13}{n+16}, \ldots, \dfrac{27}{n+30}$ является несократимой.

Задача 8.7. **а)** Вычислите $(2^6-1, 2^{15}-1)$. **б)** Докажите, что $(2^m-1, 2^n-1) = 2^{(m,n)}-1$.

Задача 8.8. **а)** Докажите, что $(16a+7b, 7a+3b) = (a, b)$. **б)** Пусть $kn - ml = 1$. Докажите, что тогда $(ka+lb, ma+nb) = (a, b)$.

Задача 8.9(у). При использовании алгоритма Евклида пара натуральных чисел заменяется на следующую пару натуральных чисел с таким же наибольшим общим делителем, потом на следующую пару чисел и т.д., пока одно из чисел не разделится на другое. Докажите, что процесс отыскания наибольшего общего делителя с помощью алгоритма Евклида не может продолжаться бесконечно долго, т.е. в какой-то момент получится пара чисел, одно из которых делится на другое.

Задача 8.10. Положим, что для нахождения наибольшего общего делителя двух чисел воспользовались алгоритмом Евклида. В результате получилась последовательность равенств $(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = (r_3, r_4) = r_4$, где r_1, r_2, r_3, r_4 — остатки от деления, получаемые на каждом следующем шаге алгоритма. Докажите, что в этой последовательности $a \geqslant 13$, $b \geqslant 8$.

Задача 8.11. Докажите, что в случае применения алгоритма Евклида к двум двузначным числам потребуется не более девяти шагов (делений с остатком). Приведите пример таких двузначных чисел, для которых необходимо девять шагов.

Задача 8.12(у). Докажите равенства:
а) $(a, b, c) = (a, (b, c))$; **б)** $(a_1, a_2, \ldots, a_k) = (a_1, (a_2, \ldots, a_k))$.
в) Докажите, что нахождение наибольшего общего делителя нескольких чисел может быть сведено к последовательному нахождению с помощью алгоитма Евклида наибольших общих делителей нескольких пар чисел.

Задача 8.13(у). Докажите, что наибольший общий делитель нескольких чисел делится на любой их общий делитель.

Задача 8.14. Найдите с помощью алгоритма Евклида
а) $(78, 28, 12)$; **б)** $(5916, 4386, 2652)$.

Критерии оценок

«5»	«4»	«3»	«2»
11 задач	9 задач	7 задач	5 задач