Алгоритм Евклида и теория целых чисел: 1

Введение. Данные листки посвящены другому изложению теории целых чисел, основанному на алгоритме Евклида. Они не используют листки "Целые числа" и содержат некоторые новые доказательства многих теорем из "Целых чисел". Кроме того, здесь излагается метод , пригодный для нахождения наибольшего общего делителя двух чисел и для некоторых других целей. Мы повторяем многие определения листка "Целые числа" с тем, чтобы этот листок был полностью независим.

§1. Напоминания.

Определение. a делится на b ($a:b$), если существует такое k, что $a = b \cdot k$

Задачи.
1. Верно ли, что если $a:c$ и $b:c$, то ab/c делится на a и b?
2. Верно ли, что если $a, b, c, d \neq 0, ab = cd$ и $a:c$, то $d:b$?

Деление с остатком. Если a -целое число, $b > 0$, то существуют и единственны такие числа q /частное/ и r /остаток/, что
1/ $a = b \cdot q + r$ 2/ $0 \leq r < b$

Задачи.
3. Нарисуйте на числовой оси все числа отрезка $[-20, 20]$, дающие при делении на 4 остаток 1.
4. Докажите, что остатки чисел n и $100n$ при делении на 3 одинаковы. /Указание: $100n = 99n + n$/

Наибольший общий делитель.
Определение. Число c называется наибольшим общим делителем чисел a и b, если выполнены два условия:
1/ c -общий делитель a и b : $a:c$ и $b:c$
2/ Если c' -любой другой общий делитель a и b, то c' - делитель c : $a:c'$ и $b:c' \Rightarrow c:c'$

§2. Теорема о существовании НОД.

В листке "Целые числа" была доказана т е о р е м а о том, что любые два целых числа имеют НОД. /Задача № 16 из Ц.Ч./ Там предлагается два разных доказательства. В этих листках мы предложим еще одно доказательство, основанное на так называемом алгоритме Евклида. Поэтому мы пока считаем этот факт неизвестным и будем его доказывать.

Задачи.
5. Докажите, что множество общих делителей чисел a и b равно множеству общих делителей чисел a и $a-b$:
$$\{x \mid a:x \text{ и } b:x\} = \{x \mid a:x \text{ и } a-b:x\}$$
/Предположите, как обычно, что число x принадлежит одной из частей доказываемого равенства, затем докажите, что оно принадлежит другой части равенства/.
6. Получите из результата задачи 5, что если c -НОД a и b, то c есть НОД a и $a-b$. Отсюда будет следовать, что если у чисел a и b есть НОД /мы пока притворяемся, что не знаем, всегда ли он есть/, то и у a и $a-b$ есть НОД /а именно, тот же, что у a и b/. Напоминаем, что доказательство должно начинаться словами: "Пусть c -наибольший общий делитель a и b. Докажем, что c -НОД чисел a и $a-b$. Проверим условия 1/ и 2/. В самом деле,...
7. Пусть число b положительно. Тогда a можно разделить на b с остатком: $a = bq + r$. Докажите, что множество общих делителей чисел a, b, совпадает с множеством общих делителей чисел b, r. /Аналогично 5/.
8. Докажите, что если у a, b есть НОД, равный c, то

это же число c будет и НОД чисел b, r.
Докажите, что верно также и обратное: если у b и r есть НОД, равный d, то это число d будет и НОД a и b.
/Аналогично задаче 6/

Таким образом, поиск НОД для пары a, b и для пары b, r -одна и та же задача: найдя НОД одной из этих пар, мы найдем одновременно и НОД другой пары. Это обстоятельство может применяться при вычислении НОД.

Пример. Пусть надо найти НОД (30,42).
$42 = 30 \cdot 1 + 12$. Поэтому НОД (42,30) = НОД (30,12) /см. задачу 8, $a = 42$, $b = 30$, $q = 1$, $r = 12$/. Теперь ищем НОД (30,12).
$30 = 12 \cdot 2 + 6$, поэтому НОД(30,12) = НОД (12, 6). Ну, а НОД (12, 6) = 6; это следует из следующей задачи:

(9) Докажите, что если $a : b$, то b есть НОД (a, b).
/Как обычно, надо проверить соиства 1,2 из определения НОД/.

Рассмотрим наш пример внимательнее. Предполагали ли мы при этих вычислениях, что НОД существует, или, напротив, доказали это? Доказали ли мы, что 6 есть НОД (42,30)? Оказывается, доказали! В самом деле, мы доказали, что НОД (12,6) =6 /задача 9/. Раз это так, то по задаче 8 мы можем доказать, что НОД (30, 12) = 6, а затем доказать, что НОД (42, 30) = 6! Таким путем можно доказать, что у любой пары целых положительных чисел есть НОД.

(10) Докажите, что у чисел 273 и 1014 есть НОД, и найдите его.
(11) То же для чисел 16484 и 42282.

Этот процесс называется алгоритмом Евклида нахождения наибольшего общего делителя двух целых чисел. /Между прочим, он годится и для вычисления НОД двух многочленов, если Вы знаете, что это такое, и там он незаменим : прямой подбор и проверка невозможны!/

В общем виде схему действии можно записать так: даны числа a и b : $a > b > 0$, делим a на b с остатком:

$a = bq_1 + r_1$ НОД(a, b) = НОД(b, r_1) (задача 8)
$b = r_1 q_2 + r_2$ НОД(b, r_1) = НОД(r_1, r_2) (задача 8)
$r_1 = r_2 q_3 + r_3$ НОД(r_1, r_2) = НОД(r_2, r_3) (задача 8)
— — — — — — — — — — — —

(12) Что должно стоять в четвертой строчке ?

А не может ли быть так, что этот процесс никогда не кончится? Для того, чтобы ответить на этот вопрос, надо прежде всего понять, когда мы его кончаем. Мы кончаем его тогда, когда можно применить задачу 9, то есть когда очередной остаток равен 0. Может ли это никогда не случиться ? Нет, не может, так как остатки убывают.

(13) Докажите это: $r_1 > r_2 > r_3 > r_4 > \ldots$

Итак, теперь мы знаем, что верна теорема:

ТЕОРЕМА. У любых двух целых чисел a и b существует НОД.

(14) Мы в алгоритме Евклида предполагали, что $a > b > 0$ а в теореме об этом умалчиваем. Как восполнить этот пробел ?

Интересно, что идеи алгоритма Евклида позволяют решить задачу:
НОД$(2^m - 1, 2^n - 1) = 2^{\text{НОД}(m,n)} - 1$. (Указание: используйте то, что НОД(a, b) = НОД$(a, b - a)$ и правила действий со степенями)

§3. Следствия.

Теперь , вооруженные этой теоремой, мы получим разные следствия.

(15) /Эта задача нам в дальнейшем не потребуется , так что если она не будет получаться , ее можно смело пропустить/. общее
У любых двух чисел a и b существует наименьшее кратное.
/НОК чисел a и b называется число c , такое, что:
1/ $c:a$, $c:b$ 2/ $c':a$ и $c':b \Rightarrow c':c$ /
Указание. Пусть d -НОД (a,b). Докажите, что ab/d -НОК (a,b)

Напомним определение взаимной простоты.
Числа a и b взаимно просты, если у них нет общих делителей, кроме 1 и -1.

(16) Докажите, что a и b взаимно просты тогда и только тогда , когда $НОД(a,b)=$(или -1
(17) Даны числа a и b . Докажите, что если существуют такие x и y , что $ax+by=1$, то a и b взаимно просты.

Те, кто внимательно решали"Целые числа", знают, что верно и обратное : если a и b взаимно просты, то существуют такие x и y , что $ax+by=1$. Мы сейчас докажем это снова, причем наше доказательство даст способ находить эти x и y , более эффективный , чем слепой перебор.

Итак, пусть a и b взаимно просты. Пусть $a>b>0$. /Как свести любой случай к этому , понятно ?/ Тогда НОД $(a,b)=1$. Представим себе, что этот самый НОД вычисляется по алгоритму Евклида; a делят на b , затем b -на полученный остаток и т.п. Тогда мы получаем последовательность остатков, причем
$$НОД(a,b)=НОД(b,r_1)=НОД(r_1,r_2)=\ldots=НОД(r_k,r_{k+1})$$
Что будет на последнем месте ?. Раз мы прекратили процесс, то r_k делится на r_{k+1} и ответом будет r_{k+1}. Но мы этот ответ знаем : он равен 1. Итак, $r_{k+1}=1$. Для любой пары из этой последовательности НОД равен 1.

Здесь я хочу прервать изложение доказательства , чтобы сообщить, что те , кому нижеследующий текст покажется малосъедобным, могут пропустить его и попробовать прочесть другое доказательство (Начало на /Однако уже изложенная часть нужна и в нем/. след. стр.)

Если мы поверим на минуту в [redacted] тот факт, который нам надо доказать, то мы узнаем, что для всякой пары r_i, r_{i+1} из последовательности существуют такие x и y, что $r_ix+r_{i+1}y=1$. Впрочем, для последней пары это ясно и без всяких предположений: там $r_{k+1}=0$ и при $x=0, y=1$ $r_kx+r_{k+1}y=1$. А теперь /тоже без всяких предположений/ докажем, что если такие x и y можно подобрать для некоторой пары, то их можно подобрать и для предыдущей! Тогда получится, что и для a и b такие x и y подобрать можно. Итак, пусть для пары r_i, r_{i+1} удалось подобрать x и y так, чтобы $r_ix+r_{i+1}y=1$. А доказать надо то, что для пары r_{i-1}, r_i можно подобрать z и w так, чтобы $r_{i-1}z+r_iw=1$. Как связаны r_{i-1}, r_i, r_{i+1}? Известно как: r_{i+1} -остаток от деления r_{i-1} на r_i . Тогда имеем:
$$r_{i-1}=qr_i+r_{i+1};\ r_{i+1}=r_{i-1}-qr_i;\ 1=r_ix+r_{i+1}y=$$
$$=r_ix+(r_{i-1}-qr_i)y=r_i(x-qy)+r_{i-1}\cdot y$$
Отсюда ясно, что в качестве z и w годятся такие числа:
$z=y$, $w=x-qy$: $r_{i-1}z+r_iw=1$
Теперь мы можем [redacted] выразить 1 через числа последней пары, затем через числа предпоследней пары, затем -через числа предпредпоследней и т.д. Так мы выразим 1 через a и b, к чему мы и стремились. Утверждение доказано.

Другое доказательство. Пусть a и b взаимно просты; назовем число m х о р о ш и м , если оно может быть представлено в виде $ax+by=m$ при некоторых x и y. Нам надобно доказать, что 1 -хорошее. Рассмотрим алгоритм Евклида.

$$a = bq_1 + r_1 \qquad r_1 = a - bq_1$$
$$b = r_1 q_2 + r_2 \qquad r_2 = b - r_1 q_2$$
$$r_1 = r_2 q_3 + r_3 \qquad r_3 = r_1 - r_2 q_3$$

Глядя на эти формулы, мы находим из 1-ой формулы справа , что r_1 -хорошее.Зная это , из второй формулы справа получаем, что r_2 -хорошее , из третьей - что r_3 -хорошее. И так далее.

18. Докажите , что $r_1, r_2, r_3, \ldots$ -хорошие.

Отсюда мы получаем, что r_{k+1} /последний остаток/ -хороший. Но он равен 1 ! Итак , 1 -хорошее число, то есть представляется в нужном виде.

Итак , мы имеем два /правда, похожих/ доказательства того, что если a и b взаимно просты, то существуют такие x и y , что $ax+by=1$. Применим эти методы на практике.

Пример. Пользуясь этой наукой , найдем x и y такие, что $23x+19y=1$

Решение. Алгоритм Евклида дает:

$23 = 19\cdot 1 + 4$; $19 = 4\cdot 4 + 3$; $4 = 3\cdot 1 + \textcircled{1}$ ← н.о.д.

$a \quad b \quad q_1 \; r_1 \qquad b \quad r_1 \; q_2 \; r_2 \qquad r_1 \quad r_2 \; q_3 \; r_3$

Первый метод . /Сначала выражаем 1 через 4 и 3 , затем через 19 и 4 , затем через 23 и 19./

$1 = \boxed{4-3\cdot 1} = 4-(19-4\cdot 4)\cdot 1 = 4(1+4)-19\cdot 1 = \boxed{4\cdot 5 - 19\cdot 1} = (23-19\cdot 1)\cdot 5 - 19\cdot 1 =$

$= 23\cdot 5 - 19\cdot(5+1) = \boxed{23\cdot 5 - 19\cdot 6}$

Второй метод. /Сначала выражаем через 19 и 23 число 4 , затем числа 3 и 1 ./ : $4 = 23 - 19\cdot 1$; $3 = 19 - 4\cdot 4 = 19 - (23-19\cdot 1)\cdot 4 =$

$= 19\cdot 5 - 23\cdot 4$; $1 = 4 - 3 = (23-19\cdot 1) - (19\cdot 5 - 23\cdot 4) =$

$= 23\cdot 5 - 19\cdot 6$

Теперь , следуя предложенным образцам, найдите такие x и y , что:

19. $15x+4y=1$ 20. $7x+26y=1$

Таким образом, для любых взаимно простых целых чисел a и b мы можем найти решение в целых числах уравнения $ax+by=1$.

21. Наши методы годятся при $a>b>0$. А как надо решать в других случаях ?

22. Докажите, что если $d=HOД(a,b)$, то a/d и b/d взаимно просты.

23. Докажите, что уравнение $ax+by=c$ можно решить в целых числах тогда и только тогда, когда $c : HOД(a,b)$

24. Найти в целых числах решение уравнения $75x-39y=1$

25. То же для уравнения $43x+250y=77$.

§4. Продукты и плоды.

Итак , мы знаем еще одно эквивалентное определение взаимной простоты: a и b взаимно просты, если существуют такие x и y , что $ax+by=1$ Это определение очень удобно.

26. Докажите, что если a взаимно просто с bc , то a взаимно просто с b и a взаимно просто с c .

27. Докажите, что если a взаимно просто с b и c, то a взаимно просто с bc .

28.Докажите, что если p -простое , то есть не делится ни на что, кроме ± 1 и $\pm p$, и a не делится на p , то a взаимно просто с p.

29. Докажите, что если a и b не делятся на p, то ab не делится на p .

30. Докажите, что если ab делится на p , то a делится на p или b делится на p .

ДАЛЕЕ РЕКОМЕНДУЕТСЯ ПРОСМОТРЕТЬ ЗАДАЧИ "Ц.Ч" и РЕШИТЬ ИХ /особенно §5 и др./