Основная теорема арифметики, связь между НОК и НОД, теорема о «превышениях», алгоритм Евклида. Простые доказательства для школы

Спасский Станислав

В одной из своих лекций для преподавателей известный математик А. В. Савватеев (https://www.youtube.com/watch?v=uTI10rjbPSM, с 26 мин.) рассказал об **основной теореме арифметики** (автором считается Евклид). Ролик понравился, смотрел его много раз. Согласно Основной теореме, целое число можно разложить на простые множители только одним способом. Большинство учеников и не подозревает о ее существовании, считая факт однозначности разложения очевидным и не зная, что проблема не такая уж простая. Поразило то, что, по словам Алексея Владимировича, все гимназисты в дореволюционной России обязаны были знать ее доказательство. «Со школьниками это полгода упорной работы!».

Мне захотелось найти простой вывод этой теоремы, наглядный, не использующий искусственных «хитроумных» приемов, доступный нашим школьникам (скажем, 8-9-го класса). Я начал разбираться с проблемой, хотя по жизни это тема не моя. Но, наверное, это было и к лучшему, т.к. удалось увидеть простой наглядный подход, мимо которого почему-то прошли.

Кроме **общепринятого** доказательства Основной теоремы, данного в ролике, оказалось, что существует **еще два** подхода, использующие **метод индукции**. Но они тоже явно мало подъемны для учеников (довольно сложные логические построения).

В ролике дается традиционное доказательство, состоящее из 3 пунктов.

В 1-м пункте ролика доказывается (3 непростых логических звена), что для натурального числа **a** и простого **p**, таких, что **a** не делится на **p**, всегда имеется целочисленное решение (**m,n**) уравнения $\mathbf{a \cdot m + p \cdot n = 1}$. Это один из вариантов записи «**Соотношения Безу**». Обычно при доказательстве его используется «**алгоритм Евклида**» («**взаимного вычитания**»). В ролике этот пункт доказывается проще (но тоже не просто).

Во 2-м пункте ролика доказывается, что для целых **a** и **b**, если каждое из них **не делится** на простое **p**, то и ($\mathbf{a \cdot b}$) **не делится** на **p**. Это т.н. «**лемма Эвклида**». Доказательство ее тоже непростое, «искусственное», хотя красивое. Фактически, все 3 звена 1-го пункта строятся, только чтобы подвести ко 2-му пункту. Вместе 1-й и 2-й пункты составляют «хитрое» логическое сооружение. С каждым логическим звеном вы вынуждены согласиться, а вся конструкция вызывает сложные ощущения. Об этих пунктах Алексей Владимирович говорит: «Вы видите, как хитро всё, очень хитро. Как Евклид додумался до этого я не знаю… Но это Евклид!»

3-й пункт в ролике простой для понимания. На основании 2-го пункта доказывается главное утверждение основной теоремы арифметики - единственность разложения целого числа на простые множители. Его, конечно, для школьников надо оставить тем же, что и в ролике, стандартным.

Материал далее дан в том виде, как, по-моему, он должен излагаться ученикам: подробно, с параллельными числовыми примерами.

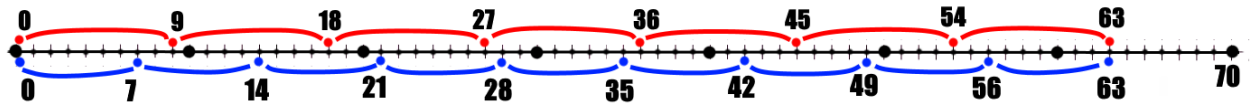
Урок 1. Введение в целочисленную арифметику на основе числовой оси

Вспомним материал 5-го класса, как ученики ищут общий знаменатель двух дробей с разными знаменателями. Вспомним понятия **НОД** (наибольший общий делитель) и **НОК** (наименьшее общее кратное). Если знаменатели **a** и **b** - взаимно простые числа (у них нет общих множителей, 1 не в счет), то их общий знаменатель – просто произведение (**a·b**). Например, у знаменателей **9** и **7** (**НОД(9,7)=1**) он **9·7=63**.

Если **a,b** имеют общий множитель (1 не в счет), например, **a=10=5·2**, **b=8=4·2, НОД(10,8)=2**, то учат в качестве общего знаменателя брать **5·4·2**, так как **5·4·2** делится и на **10,** и на **8**. Объяснение: у чисел 10 и 8 есть независимые части 5 и 4, и одинаковая часть, множитель **2 (НОД).** Поэтому, если мы перемножим **a** и **b** (10 и 8), то общая часть 2 будет повторена дважды, а достаточно и одного раза. Поэтому, чтобы убрать повтор, произведение **a·b нужно разделить на НОД,** (**10·8/2=40**). Т.е. их **НОК(10·8)** - это произведение обоих чисел, но сокращенное в **НОД раз**.

Продемонстрируем всё сказанное на числовой оси, визуализируем.

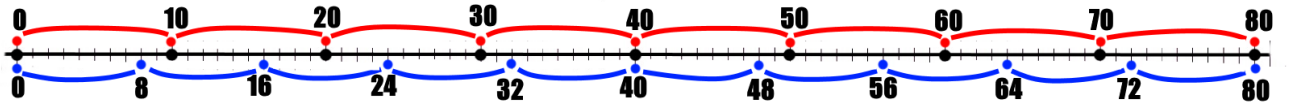
Сначала для двух рядов чисел, с шагами **a,b** (**9** и **7**) с **НОД=1**. Числа с шагом **9** отмечены красными точками: **9·i, i=0,1,2,…,7**. Все эти числа делятся на **9** (кратны **9**).



Числа ряда **7·j, j=0,1,2,…9** отмеченные синими точками. Все они делятся на **7**.

А какие из чисел делятся одновременно и на **9**, и на **7**? Это «точки совпадения» в двух рядах. На схеме **0** и **63**. Точку **63 (a·b)** можно считать уже началом следующего цикла, подобного предыдущему по взаимному расположению точек обоих рядов (на схеме 2-й цикл не показан). 1-й цикл длиной **63 (a·b)** (это интервал **[0,63]**) будем называть «**базовым**». Число **a·b** - «железный» общий знаменатель для всех случаев, **a·b** всегда является точкой совпадения. Отметим, что для рядов **9·i** и **7·j** на интервале **[0,63]** кроме **0** и **63** точек совпадения нет!

Теперь смотрим два ряда точек: красные с шагом **10**: **10·i, i=0,1,…8,** и синие с шагом **8**: **8·j, j=0,1,2,…10**. **НОД(10,8)=2**. Базовый цикл – это **[0,10·8],** (**[0,a·b]**).



Видим появление **3-й** точки совпадения в середине: **0,40,80**.
НОК(10,8)=40=10·8/2.

Обратите внимание на то, что на «базовом цикле» **[0,10·8]** укладывается ровно **2** «внутренних цикла» (**НОД(a,b)=2**). А также на то, что рисунок взаимных расположений красных и синих точек от числа **40** точно повторяет рисунок от **0.**

Важное замечание. Обычно о рассматриваемых числах (у нас a и b) говорится, что они целые. Чтобы не усложнять материал, мы будем всегда считать, что они натуральные (целые положительные). Или оговаривать особо. Практически всегда этого достаточно.

Урок 2. Основная теорема арифметики. Вывод

Формулировка. Натуральное число раскладывается на простые множители однозначно.

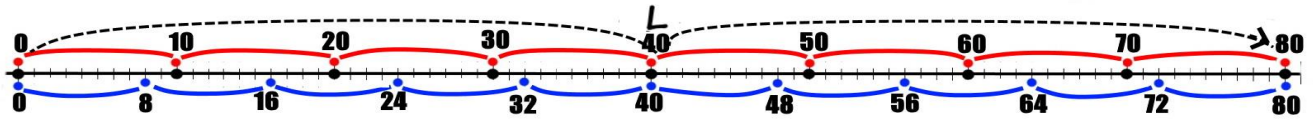
Доказательство строим на понятии **НОК(a,b)** (наименьшее общее кратное), известное школьникам с 5-го класса.

Шаг1. Формулировка. Для двух натуральных взаимно простых **a** и **b внутри** интервала **[0,a·b]** нет чисел, общих кратных **a** и **b** (точек «совпадения»), **только 2 крайние.** Далее цикл **[0,a·b]** повторяется. Числа - общие кратные **a,b: 0, ab, 2ab,** …

Доказательство:

Идем от **0** вправо по **i, j** и ищем **ближайшую** точку «**совпадения**» двух рядов на интервале **[0,a·b].** Эта точка существует. Либо **внутри** интервала **[0,a·b],** либо это сама точка **a·b**. По самому определению найденная точка - это **НОК(a,b).** Обозначим длину этого «внутреннего интервала» **L**. В нашем 2-м примере мы бы дошли до точки **L=40**. Ясно, что **внутри** интервала **[0,L]** точек совпадения нет, только **0** и **L**.

Далее **за** интервалом **[0,L]** (**[0,40]**) картина взаимных расположений точек обоих рядов должна точно повторять их картину на интервале **[0,L]**, т.е. **«внутренний цикл» [0,L]** идет повторами. Идем по этим повторам, пока не дойдем до конечной точки базового цикла **a·b** (**80**)**.** Этот повтор должен попасть своей крайней точкой в **ab**.



Почему? Потому что **внутри [0,L]** и внутри его повторов точек совпадений нет, только на краях. А сама точка **a·b** является точкой совпадения. Поэтому цикл **[0,L]** на интервале **[0,a·b] должен** уложиться **кратно**, точно целое число раз! Обозначим это число повторов **k.** Вычисляем **k** делением: **k=ab/L** (в примере **k=10·8/40=2**).

Перепишем соотношение **k=ab/L** в таком виде: **L=ab/k.** Или: **L=a(b/k)=b(a/k).**

Точка **L** является точкой совпадения, т.е. кратной **a** и **b**. Значит, **(b/k)** и **(a/k) –** это целые числа. Если **k** не равно **1,** то является общим делителем **a** и **b.** Но **a** и **b** по условию взаимно простые. Значит, **k** равно **1**, **L=a·b**, и на **[0,a·b]** точек совпадения нет!

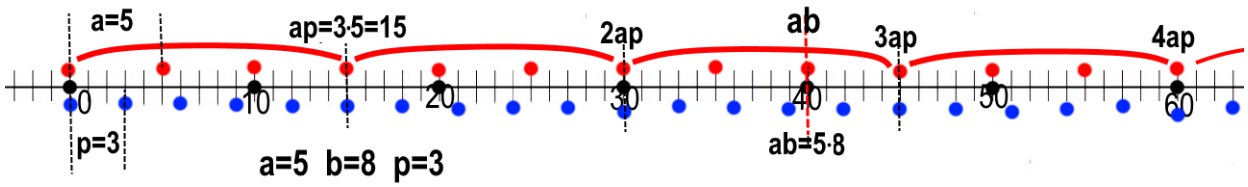
Далее цикл **[0,a·b]** повторяется. Общие кратные **a, b** только**: 0, ab, 2ab, 3ab**…

Урок 3. Шаг 2. Лемма Евклида. (Докажем 2-й пункт ролика , но по-иному.)

Формулировка. Даны два натуральных числа **a** и **b**, таких, что каждое из них **не делится** на простое **p**. У них нет с **p** общих делителей, т.к. у **p** делители только **1** и **p**. Докажем, что и число **a·b** тоже **не** делится на **p**.

Замечание. Для предлагаемого доказательства вполне достаточно, чтобы каждое из чисел **a** и **b** были с **p** попарно взаимно простыми.

Мы рассмотрим всё это параллельно с частным случаем: **a=5, b=8, p=3**. **5** и **8** не делятся на простое число **3**. Покажем, что **a·b=5·8** тоже не может делиться на **3**.



В качестве «**основы**» возьмем ряд точек с шагом **a**: **a·i, i=0,1,2….** В нашем примере – это (**5·i**). (**Замечание**: можно было выбрать в качестве «основы» и ряд **b·i**).

Зачем нам ряд **a·i** в качестве основы?

Во-первых, по предыдущему пункту мы уже знаем, что для взаимно простых **a,p** по ряду чисел **a·i** делятся на **p** только числа **0, ap, 2ap, 3ap**…. То есть, по ряду **a·i** у **этих чисел** номера **i** кратны **p**: **i=0, p, 2p, 3p**…(в примере это **i**=0,3,6…) Других нет! И на рисунке видно, что **совпадения** идут через 3 (**p**) интервала красных точек.

Во-вторых, точка **a·b** (у нас **5·8**) тоже является одой из точек ряда **a·i,** с **i=b** (8)**.**

Но по условию **b** (8) не делится на **p** (3). Поэтому точка **ab**, принадлежа ряду **ai**, **не** попадает в семейство точек из ряда **a·i**, делящихся на **3** (**p**). На рисунке это видно.

Доказан 2-й пункт ролика (лемма Евклида). Число **ab** не делится на **p** тоже!

Урок 4. 3-й шаг (и 3-й пункт ролика) простой и понятный для школьников. Конечный шаг основной теоремы арифметики

Берётся два разных (по предположению) возможных разложения целого числа **m** на простые множители. Убирая одинаковые множители в обоих вариантах, получаем число **a** с разными наборами простых p и q: $\mathbf{a=(p_1\cdot p_2\cdot p_3\cdot\ldots\cdot p_s)=(q_1\cdot q_2\cdot q_3\cdot\ldots\cdot q_t)}$. Степени в разложениях $\mathbf{p^\alpha}$ и $\mathbf{q^\beta}$ (т.е. повторы **p** и **q**) разлагаем в общие ряды. Множители **p** и **q** ставятся по возрастанию. Мы вправе выбрать вторым вариантом тот, у которого 1-й множитель меньше (только для удобства). Т.е. имеем: $\mathbf{a = p_1\cdot p_2\cdot\ldots = q_1\cdot q_2\cdot\ldots,\quad p_1 > q_1}$**.** Например (**условно!**): $\mathbf{a = 5\cdot 7\cdot 11\cdot 19 = 2\cdot 2\cdot 3\cdot 3\cdot 13\cdot 17,\ \ 5>2.}$

Сначала берутся множители $\mathbf{p_1}$ и $\mathbf{p_2}$ (5,7), каждое из них не делится на $\mathbf{q_1}$ (2)**.** По условию. Значит, и $\mathbf{p_1\cdot p_2}$ не делится на $\mathbf{q_1}$. Мы доказали это в пункте 2. Затем берётся пара чисел $\mathbf{(p_1\cdot p_2)}$ и $\mathbf{p_3}$. На том же основании и число $\mathbf{p_1\cdot p_2\cdot p_3}$ не делится на $\mathbf{q_1}$. Идем так до конца всего числа, показывая, что всё число **a** не делится на $\mathbf{q_1}$. Это является противоречием, так как $\mathbf{q_1}$ (2) входит в число сомножителей **a** по предположению.

Теорема единственности разложения чисел на простые множители доказана.

Урок 5. Вывод связи НОК и НОД

Для натуральных чисел **a,b НОК(a,b)=a·b/НОД(a,b)**. Если **НОД(a,b)= 1**, то **НОК(a,b)= a·b** (внутренний цикл совпадает с базовым, точек совпадения внутри интервала **[0,a·b]** нет.

Вообще, доказав Основную теорему, мы имеем право вывести эту связь просто, как ее выводят в школе, раскладывая числа на простые множители и выделяя в них часть из общих множителей.

Но можно вывести соотношение как базовое, «с нуля». И не формально логически, школьники так не воспримут, а наглядно.

Начало совпадает с началом доказательства предыдущей теоремы:

Шаг 1. Идем от **0** до 1-й точки совпадения: Получаем **НОК(a,b)=L**. Опираясь на обязательную кратность интервала **[0,L]** на интервале **[0,a·b]** получаем число повторов **k** делением: **k=ab/L.** Переписываем это выражение в виде **L=ab/k.** Или так: **L=a(b/k)=b(a/k).** Т.к. **L** кратна **a,b**, то значит, **(b/k)** и **(a/k) –** это целые числа, а **k** является общим делителем **a**,**b**. Далее вывод соотношения идет по-своему.

Итак, **k** является общим делителем **a**,**b**. Но наибольший ли он, т.е. **НОД**?

Шаг 2. **Покажем, что на [0,ab] не может быть общего делителя для a,b больше полученного k. Т.е. k – это наибольший делитель, НОД(a,b)=k.**

В примере с **a=10,8** идя от **0** мы бы дошли до 1-й точки совпадения **L=40.** Затем делением **ab** на **L** мы бы определили, что интервал **[0, L]** на интервале **[0,ab] ([0,80])** укладывается дважды **(k=2)** и доказали, что число **k** (2) должно быть общим делителем и 10 и 8. Но является ли этот делитель 2 **наибольшим** общим делителем?

Покажем, что полученная нами формула **L=ab/k** работает и в другую сторону.

Допустим, нам сообщили, что у чисел **a,b** есть некий общий делитель k_1. Смотрим число $L_1=ab/k_1$ (или $L_1=a(b/k_1)=b(a/k_1)$).Т.к. (b/k_1) и (a/k_1) – это целые числа, то наше число $L=ab/k_1$ на **[0,ab]** является точкой **совпадения** (кратна и **a,** и **b**).

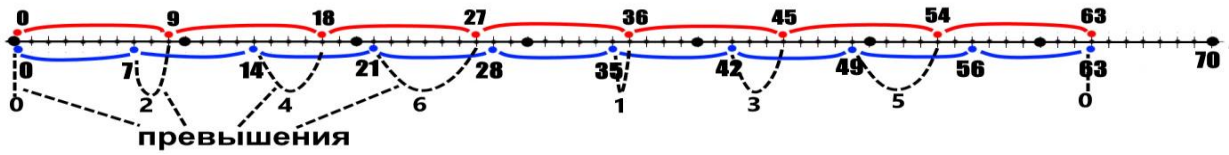
Мы не знали, является ли **k,** полученное нами из **(ab)/L,** наибольшим делителем **a** и **b**, и допускали, что может быть делитель $k_1>k$. Но тогда должна быть точка совпадения $L_1=ab/k_1$ **.** И L_1 должно быть меньше **L=ab/k,** т.к. $k_1>k$. **Но L** мы получили, как **самое маленькое значение** совпадения**. Пришли к противоречию.**

Т.е. полученное нами **k=ab/L** является **НОД(a,b)**.

Вывод: теорема о связи НОК и НОД доказана. НОК(a,b) = ab/НОД(a,b).

Урок 6. Теорема о превышениях

В качестве введения рассмотрим знакомую шкалу с рядами **9i** и**7j**, с **НОД(9,7)=1**.



Введем понятие «**превышения** по точкам ряда **9i**»: на сколько каждая точка **9i** (красная) превышает ближайшую слева точку ряда **7j** (синюю). Можно это понятие определить формально, как остаток от деления числа **ai** на **b:** (**r=ai mod b**). Но термин «превышение» нагляднее. Эти **превышения** отмечены на рисунке пунктирными дугами и указаны их числовые значения. «Превышение» 0 означает «совпадение».

Обратите внимание, что на базовом интервале **[0,ab)** (**ab=63**) число точек ряда **ai** равно **b** (**7**), если не считать точку **63**, которую следует отнести к началу другого цикла. Число возможных **значений** превышения тоже равно числу **b** (**7**): **0,1,…6**. Обратите внимание, что на базовом интервале **[0,63)** есть все значения превышений.

Докажем это свойство для любой пары взаимно простых **a,b**, (**НОД(a,b)=1**).

Теорема о превышениях. На базовом интервале **[0,ab)** при условии **НОД(a,b)=1** по ряду **ai** имеются все возможные значения «превышений» **0,1,2,…(b-1) по разу**.

Доказательство. Число точек ряда **ai** на интервале **[0,ab)** равно **b**. Принципиально число разных значений превышений тоже равно **b**: **0,1,2,…(b-1)**. Если никакое значение превышения не повторяется, то обязаны быть все возможные превышения! Надо только доказать, что внутри интервала **[0,ab) нет** точек **ai с одинаковым** превышением.

Напомним, что внутри интервала **[0,ab)** при **НОД(a,b)=1** нет точек «совпадения» (**превышения** равного **0**). Но допустим, что при этом внутри интервала **[0,ab)** есть 2 точки ряда **ai с одинаковым превышением**, т.е. с одинаковым взаимоположением точек **i** и ближайшего слева **j**. Т.е. имеет место цикл. И в нем, как доказано, нет точек **совпадений**. Повторы этого цикла должны идти бесконечно, и на всем этом пространстве должны отсутствовать точки совпадения. Но они есть: например, точка **ab**. Мы пришли к противоречию. Значит, внутри интервала **[0,ab)** точек **повторов превышений** по ряду **ai** нет. (То же по ряду **bj**).

Теорема о «превышениях» доказана. Честно говоря, ее результат удивляет.

Следствие: для **a,b** с **НОД(a,b)=1** по ряду **ai** на интервале **[0,ab)** есть все превышения от **0** до **b-1.** Значит, есть и превышение **1**. Т.е. $\mathbf{a \cdot i_0 - b \cdot j_0 = 1}$. Это решение уравнения $\mathbf{a \cdot m + b \cdot n = 1}$ с $\mathbf{m = i_0}$ и $\mathbf{n = -j_0}$. Факт наличия решения для такого уравнения называется **«соотношением Безу»**, оно доказывается в 1-м пункте ролика.

Урок 7. Некоторые простые соотношения

Деление пары чисел a,b на их НОД

Введение. Пример. Имеем числа **a=10** и **b=8**. **НОД(a,b)=2**. Разделим **a,b** на их **НОД(a,b)=2**. Получаем $\mathbf{a_1=5}$ и $\mathbf{b_1=4}$, взаимно простые числа. Это работает всегда?

Доказав **основную теорему арифметики,** мы вправе разложить числа **a** и **b** на простые множители **однозначно**. Выделяем у них максимально общую группу простых множителей. Их произведение – это **НОД(a,b)**. Поделив **a** и **b** на **НОД(a,b)** получаем числа $\mathbf{a_1}$ и $\mathbf{b_1}$. Они не должны иметь общих множителей, т.е. $\mathbf{a_1}$ и $\mathbf{b_1}$ – взаимно простые числа, $\mathbf{НОД(a_1,b_1)=1}$.

Обратно. Если мы имеем 2 взаимно простых числа **a,b, НОД(a,b)=1**, и умножим их на одно и то же число **d**, получив числа $\mathbf{a_1}$ и $\mathbf{b_1}$, то $\mathbf{НОД(a_1,b_1)=d}$.

Еще 2 свойства

Утверждение. Имеем **a+b=c** (**a,b,c** натуральные). Пусть **a** и **b** делятся на число **d**. Тогда и число **c** должно делиться на **d**.

Запишем **a+b** в виде: $\mathbf{a+b=d \cdot a_1+d \cdot b_1=d(a_1+b_1)=c.}$ Значит и **c** должно делиться на **d**.

Утверждение. Пусть **a** и **b** – взаимно простые числа и **a+b=c.** Тогда и **b,c** – взаимно простые числа.

Запишем **a+b=c** в виде **a=c -b**. Допустим, что **b** и **c** не взаимно простые числа. Но тогда **b** и **c** имеют общий множитель **d**, не равный **1**.

Можно записать: $\mathbf{a=d\cdot c_1-d\cdot b_1=d(b_1-c_1)}$**.** Значит, и число **a** содержит множитель **d**. Получается, что **a** и **b** имеют общий множитель **d**. Но **a** и **b** по условию взаимно простые числа. Пришли к противоречию. Значит, **b** и **c** – взаимно простые числа.

Урок 8. Алгоритм Евклида, поиск НОД(a,b) методом взаимного вычитания, (метод остатков)

Важное место в теме **НОД** занимает метод **нахождения НОД(a,b)** (**алгоритм Евклида**).

Сначала покажем на примерах в чем он состоит.

Пример 1. Имеем 2 натуральных числа **a** и **b**. Например, **9** и **7**. Надо найти **НОД(9,7)**. Начинаем с того, что ищем остаток **r** от деления большего числа на меньшее: **9/7**, остаток **2**. Переходим от пары **9,7** к паре **7,2**. Далее делим **7/2,** получая остаток **1**. Переходим к паре **2** и **1**. Далее остатка не будет. Последний делитель **1,** от которого остатка не будет**,** он-то и является **НОД(9,7)=1**.

Пример 2. Даны числа **16** и **12**. Делим **16/12, остаток 4.** 2-я пара **12 и 4**. Эта пара делится на **4** без остатка. Последний делитель **4** и является **НОД(16,12)=4**.

Запомните**: НОД(a,b)** – это **делитель последнего деления (без остатка).**

Но возникает важный вопрос. При переходе от пары **a** и **b** к паре **b** и **r** (**r** - остаток от деления **a/b**) сохраняет ли **НОД(b,r)** значение **НОД(a,b)?** Не может ли он измениться при переходе от одной пары чисел к другой?

Итак, исходная пара чисел **a,b**. 1-м числом (**a**) берем **большее** из чисел.

Запишем уравнение, связывающее **a,b,r**: **a=k·b+r**, **a**-делимое, **b**-делитель, **k**-частное, **r-**остаток. Например, для **a=16** и **b=12: 16=1·12+4**. Соотношение **a=k·b+r** можно записать и в виде **a-k·b=r**. Нам пригодятся оба варианта.

Шаг 1. Рассмотрим только самый 1-й переход. В остальных будет то же самое. **Первое утверждение**: если **НОД(a,b)=d**, то остаток **r делится** на **d**.

Действительно, в выражении **a-k·b=r** вынесем общий множитель **d** в левой части за скобки, запишем соотношение в виде $\mathbf{a-k\cdot b=d(a_1)-k\cdot d(b_1)=d(a_1-k\cdot b_1)=r.}$ $\mathbf{d(a_1-k\cdot b_1)}$ делится на **d**. Значит, и остаток **r** должен делиться на **d**. Итак, **остаток r от a/b делится на НОД(a,b)**.

Шаг 2. Разделим левую и правую части **a-k·b=r** на **d**. Получаем $\mathbf{a_1-k\cdot b_1=r_1}$. $\mathbf{a_1}$ и $\mathbf{b_1}$ у нас после деления на **НОД(a,b)=d** должны стать **взаимно простыми** числами (нет общих множителей). Вопрос: а в новой паре $\mathbf{b_1}$ и $\mathbf{r_1}$ – станут ли они после деления на **d взаимно простыми** числами? Если да, то **НОД(b,r)** тоже равен **d, сохраняется.**

Шаг 3. Запишем наше равенство в виде $\mathbf{a_1=k\cdot b_1+r_1.}$ Допустим противное, что $\mathbf{b_1}$ и $\mathbf{r_1}$ не взаимно простые, т.е. существует их общий делитель. Обозначим его **m** и вынесем за скобки: $\mathbf{a_1=k\cdot b_2\cdot m+r_2\cdot m=m(k\cdot b_2+ r_2).}$ Но тогда из $\mathbf{a_1=m(k\cdot b_2+r_2)}$ следует**,** что и число $\mathbf{a_1}$ должно делиться на **m** (как и $\mathbf{b_1}$). Но $\mathbf{a_1}$ и $\mathbf{b_1}$ взаимно простые числа.

Пришли к противоречию. Значит, b_1 и r_1 **взаимно простые** числа. А значит, до деления чисел **a**,**b**,**r** на **НОД(a,b)=d НОД(b,r)** тоже был равен **d.** Т.е. при соотношении **a=k·b+r НОД(b,r)** повторяет значение **НОД(a,b)**.

Значит, при переходе от пары a,b к паре b,r НОД сохраняется.

Понятно, что всё это же выполняется при переходе к следующим парам, составленным из делителя и остатка от предыдущего шага**.**

Урок 9. Сокращение количества ходов (улучшенный алгоритм Евклида)

Понятно, что цель шагов постоянно уменьшать числа в новых парах. Остаток **r** от деления **a/b** всегда меньше **b**. Но часто бывает, что **r** ненамного меньше **b**.

Например, пусть на каком-то шаге имеем пару **a=41**, **b=22**, т.е. **k=1** и **r =19**. Второе число **b** (22), не уложившееся целиком в число **a** (41), выходит за пределы **a** «хвостом», равным **b-r** (3). Так вот, вместо **r** (19) в следующую пару можно брать «хвост» $r_{хв}$ (3), который в конкретных случаях бывает намного меньше **r.** Это часто сильно сокращает весь процесс.

Почему это можно делать? Если в рассмотренном нами связи **a=k·b+r** выразить остаток **r** через его «хвост» $r_{хв}$ ($r = b - r_{хв}$), то вместо выражения **a=k·b+r** получим $a = k \cdot b + (b - r_{хв})$, или $a = (k+1) \cdot b - r_{хв}$. Такая замена **r** на $r_{хв}$ никак не влияет на предыдущий проведенный анализ по сохранению НОД в паре **b** и **r.**

На практике это выглядит так: смотрим остаток **r** от деления **a/b**, если полученный остаток **r** по величине получается близким к **b**, то для следующей пары вместо **b,r** выгодней взять пару **b,(b-r).**

Пример использования алгоритма Евклида и его улучшенного варианта:

a	b	r
100	61	39
61	39	22
39	22	17
22	17	5
17	5	2
5	2	1

a	b	r или $r_{хв}$	
100	61	22	$r_{хв}$
61	22	5	$r_{хв}$
22	5	2	r
5	2	1	

Урок 10. Уравнение Диофанта

Уравнение Диофанта — это уравнение, в котором все числа, удовлетворяющие уравнению, должны быть целыми числами. Например, для целочисленного уравнения **6m+4n=14** подойдет решение **m=1**, **n=2**. Приведенный пример – это самый простой тип уравнения Диофанта, т.н. «линейное уравнение Диофанта с двумя переменными». Подробнее разберем этот тип уравнения дальше.

Тема целочисленных задач идет от древнегреческого математика Диофанта Александрийского, жившего 2000 лет тому назад.

Вспомним теорему Пифагора для прямоугольного треугольника $\mathbf{c^2=a^2+b^2}$.

Зададимся вопросом, можно ли найти целочисленное решение $\mathbf{c^2=a^2+b^2}$? Это тоже один из многих вариантов уравнения Диофанта. Вспомните, что есть т.н. «**египетский треугольник**» со сторонами **5,4,3**. Есть и другие целочисленные решения. Например, **13,12,5**. Все эти целочисленные решения называются «**пифагоровы тройки**». Находить их не сложно, используя вариант записи $\mathbf{a^2=c^2-b^2=(c-b)(c+b)}$ и разбив число $\mathbf{a^2}$ на 2 подходящих множителя.

Пример. Допустим, возьмем $\mathbf{a=3,\ a^2=9}$. Раскладываем число **9** на 2 множителя: $\mathbf{a^2=9=1\cdot 9=M\cdot N}$. Т.е. получаем систему: **c-b=1, c+b=9**, которая имеет простое решение: **c=(1+9)/2=5, b=(9-1)/2=4.** Получили числа египетского треугольника.

Числа **M** и **N** должны быть одной четности из-за делителя **2** в выражениях.

Замечание. В 1630 г. французский математик Пьер Ферма (1601 — 1665) сформулировал гипотезу, которую называют «**великой (или большой) теоремой Ферма**»: «Уравнение $\mathbf{x^n+y^n=z^n}$ для натурального $\mathbf{n \geq 3}$ не имеет решений в натуральных числах». Доказали гипотезу только недавно.

Урок 11. Решение уравнение Диофанта типа a·m+b·n=c

Обратимся к **«линейному уравнению Диофанта с двумя переменными»** типа **6m+4n=14**. **6** и **4** – это наши натуральные **a** и **b**. **m** и **n** – искомые целые числа.

Прежде всего следует определить **НОД(6,4)** (НОД(a,b)). В нашем примере он равен 2.

Если бы правая часть (**14**) не делилась на **НОД(6,4),** то решения у этого уравнения не было бы в принципе. Это легко понять, вынеся в левой части **НОД(6,4)** за скобки.

Если правая часть делится на **НОД(a,b),** то делим на него и левую, и правую части уравнения, получая новое уравнение, равносильное исходному. В нашем случае от уравнения **6m+4n=14** переходим к равносильному **3m+2n=7.** Но теперь наши новые **a** и **b** (3 и 2) – взаимно простые числа.

Если найдено какое-то **частное решение**, то **общее решение** составляется из двух частей: любого **частного решения** (скажем, **m=2, n=1**) и **другой** части, которая равна **0,** она берется с целым параметром-множителем **t**.

В нашем случае уравнения **3m+2n=7,** его частное решение **3·2+2·1=7, m=2,n=1.** Выражение **3·2+2·(-3)=0, т.е. a·b+b·(-a)=0.** И с любым целым **t**: **t·(3·2+2·(-3))=0.**

Складываем оба решения: 3·2+2·1 + t·(3·2+2·(-3)) = 7.

Общее решение отдельно по **m** и **n**: **m=2+t·2, n=1+t·(-3), t**-любое целое.

Урок 12. Решение уравнения Диофанта типа a·m+b·n=1

Особое место в случае **НОД(a,b)=1** занимает уравнение с **1** в правой части: **a·m+b·n=1**. Умея находить его решение, можно получить частное решение с любой правой частью **c**, умножив полученные **m,n** нашего решения и **1** справа на величину **c**: **a·(cm)+b·(cn)=c**.

Итак, учимся решать уравнение типа **a·m+b·n=1** при условии **НОД(a,b)=1.**

При взаимно простых **a,b** было показано, что на интервале **[0,ab]** для превышений **a·i-b·j** существует весь набор возможных «превышений», обязательно есть превышение равное **1**. Т.е. решение **a·m - b·n=1** существует. Это утверждение соответствует т.н. «лемме Безу». Но надо еще уметь находить само решение **m,n**.

В ролике показано, как найти решение уравнения **100m+61n=1** с помощью **цепных дробей**. Мы разберем, как отыскать решение с помощью алгоритма Евклида.

Прежде всего не следует забывать об элементарной сообразительности. Например, в уравнении **100m+61n=1** (из ролика)**, a=100, b=61** видим, что **a-b=39**. Далее, что **10b-6a=610-600=10**. Значит, **40b-24a=40**. А **40-39=1**. Т.е. **(40b-24a)-(a-b)=1**.

В результате: **-25a+41b=1**. Проверяем: **-25·100+41·61=1.**

Вот стандартное решение с помощью алгоритма Евклида.

a=100	b=61	100-61=39	=a-b
b=61	(a-b)=39	61-39=22	=b-(a-b)=2b-a
(a-b)=39	2b-a=22	39-22=17	=(a-b)-(2b-a)=2a-3b
2b-a=22	2a-3b=17	22-17=5	=(2b-a)-(2a-3b)=5b-3a
2a-3b=17	5b-3a=5	17-3·5=2	=(2a-3b)-3(5b-3a)=11a -18b
5b-3a=5	11a-18b=2	5-2·2=1	=(5b-3a)-2(11a-18b)=41b-25a

41·**61**-25·**100**= 2501-2500=**1**

А теперь решение улучшенным алгоритмом Евклида.

a=100	b=61	2·61-100=22	=2b-a $r_{хв}$
b=61	2b-a=22	3·22-61=5	=3(2b-a)-b=5b-3a $r_{хв}$
2b-a =22	5b-3a=5	22-4·5=2	=(2b-a)-4(5b-3a)=11a-18b
5b-3a=5	11a-18b=2	5-2·2=1	=(5b-3a)-2(11a-18b)=41b-25a

Думаю, этот материал стоит включить в программу школы или по крайней мере в программу факультатива по математике.