Лекция 3 по курсу

Математические основы криптологии

Университет ИТМО

Преподаватель: Петтай Павел Пээтерович

6. Наибольший общий делитель: существование и основные свойства.

Опр.6.1. Если $\forall i \in \{1,2,...,n\}$ $a_i \vdots d$, то d называют *общим делителем чисел* $a_1, a_2, ..., a_n$.

Из монотонности умножения следует, что любое ненулевое число имеет конечное число делителей. Также 1 является общим делителем любого набора чисел. Отсюда следует, что *любой набор чисел, не все из которых нули, имеет конечное не пустое множество общих делителей*.

Опр.6.2. Положительный общий делитель d чисел $a_1, a_2, ..., a_n$, кратный всем общим делителям данных чисел, называют их *наибольшим общим делителем* и обозначают $НОД(a_1, a_2, ..., a_n)$.

$$\boxed{d = НОД(a_1,a_2,...,a_n) \Leftrightarrow d > 0 \wedge \forall i \in \{1,2,...,n\}\ a_i \vdots d \wedge (\forall i \in \{1,2,...,n\}\ a_i \vdots d \rightarrow d \vdots d)}$$

Замечание 6.1. Не сложно понять, что *у набора* $\{0,0,...,0\}$ *нет наибольшего общего делителя*. В самом деле, предположим, что $НОД(0,0,...,0) = d > 0$, но тогда ясно, что $0 \vdots 2d$, тогда, по определению, $d \vdots 2d$ и при этом $d < 2d$, тогда по Свойству 1.7. $d = 0$ - противоречие.

Утверждение 6.1. *Если* $d = НОД(a_1, a_2, ..., a_n)$, *то* d - *максимальный элемент множества всех общих делителей чисел* $\{a_1, a_2, ..., a_n\}$.

$$\boxed{НОД(a_1,a_2,...,a_n) = \max\{d \mid \forall i\ a_i \vdots d\}}$$

Доказательство. Очевидно, что $d \in \{d \mid \forall i\ a_i \vdots d\}$. Предположим, что $d_1 \in \{d \mid \forall i\ a_i \vdots d\}$ и $d_1 > d > 0$. Тогда и $|d_1| > |d|$, при этом, по определению, $d \vdots d_1 \overset{Св-во\,1.7}{\Rightarrow} d = 0$ - противоречие. **Ч.т.д.**

Замечание 6.2. Если среди чисел $\{a_1, a_2, ..., a_n\}$ есть хоть одно ненулевое, то множество всех их общих делителей конечно. Существование максимального элемента конечного числового множества (по отношению $\le$) очевидно. Однако мы пока что *не доказали*, что максимальный элемент множества всех общих делителей является наибольшим общим делителем этих чисел, а доказали обратное утверждение. Конкретно, не доказано существование наибольшего общего делителя, но, если докажем, то, в силу Утверждения 6.1., сможем искать его, как максимальный элемент множества всех делителей. В «школьных» курсах часто Утверждение 6.1. предлагается в качестве определения наибольшего общего делителя. В этом случае с существованием не будет никаких проблем, однако возникнут определённые сложности с доказательством (важного!) свойства, состоящего в том, что наибольший общий делитель кратен всем остальным делителям данного набора чисел.

Пример 6.1. Рассмотрим набор чисел $\{66,-24,54\}$.

Делители 66: $\{\pm1,\pm2,\pm3,\pm6,\pm11,\pm22,\pm33,\pm66\}$

Делители -24: $\{\pm1,\pm2,\pm3,\pm4,\pm6,\pm8,\pm12,\pm24\}$

Делители 54: $\{\pm1,\pm2,\pm3,\pm6,\pm9,\pm18,\pm27,\pm54\}$

Тогда множество всех общих делителей чисел $\{66,-24,54\}$ будет пересечением данных множеств: $\{\pm1,\pm2,\pm3,\pm6\}$. $\max\{\pm1,\pm2,\pm3,\pm6\}=6$. Не сложно проверить, что *6 делится на любой элемент данного множества*, следовательно, $НОД(66,-24,54)=6$.

<u>Теорема 6.1</u>.(о существовании и линейном представлении НОД).

Если среди чисел $\{a_1,a_2,...,a_n\}$ *есть хоть одно ненулевое, то:*

1.) $\boxed{\exists d = НОД(a_1,a_2,...,a_n)}$

2.) $\boxed{\exists c_1,c_2,...,c_n \in \mathbb{Z}\ d=\sum_{i=1}^{n} c_i a_i}$

Доказательство. Пусть $A=\left\{\sum_{i=1}^{n} c_i a_i \mid c_1,c_2,...,c_n \in \mathbb{Z}\right\}$ - множество всевозможных линейных комбинаций аргументов НОД с целыми коэффициентами.

Возьмём любой элемент $a_j \neq 0$. Очевидно, $a_j \in A$ (возьмём $c_j=1$ и $\forall i \neq j\ c_i=0$). Также $-a_j \in A$ (возьмём $c_j=-1$ и $\forall i \neq j\ c_i=0$). Таким образом, в множестве A есть, как положительные, так и отрицательные элементы. При этом очевидно, что все элементы A являются целыми числами. Поэтому в множестве A есть *наименьший положительный элемент. Обозначим его* d, дальше будем доказывать, что именно он и является наибольшим общим делителем чисел $\{a_1,a_2,...,a_n\}$. $d=\min\{x \mid x\in A \wedge x>0\}$.

Пусть $B=\{kd \mid k\in\mathbb{Z}\}$. Покажем, что $B=A$.

$d\in A$, т.е. при некоторых $c_1,c_2,...,c_n\in\mathbb{Z}$ $d=\sum_{i=1}^{n} c_i a_i$, тогда $\forall b\in B\ \ \exists k\in\mathbb{Z}$

$$b=kd=k\sum_{i=1}^{n} c_i a_i=\sum_{i=1}^{n}(kc_i)a_i\in A \Rightarrow \underline{B\subseteq A}.$$

Обратно, выберем $a \in A$, тогда $a = \sum_{i=1}^{n} c_i a_i$. Разделим a на d с остатком: $a = dk + r$, где $0 \le r < d$. Тогда $r = a - dk = \sum_{i=1}^{n} c_i a_i - \sum_{i=1}^{n} c_i a_i \cdot k = \sum_{i=1}^{n} (c_i - c_i \cdot k) a_i \in A$. Если $r \neq 0$, то $r > 0 \wedge r < d \wedge r \in A$, что противоречит тому, что d - минимальный положительный элемент A. Следовательно, $r = 0$, а тогда $a = dk \in B \Rightarrow \underline{A \subseteq B}$. Таким образом, заключаем, что $A = B$.

Получается, что все элементы множества A (в частности, элементы $a_1, a_2, ..., a_n$) кратны d, следовательно, d - общий делитель чисел $a_1, a_2, ..., a_n$.

Наконец, пусть d_1 - ещё какой-нибудь общий делитель чисел $a_1, a_2, ..., a_n$. Тогда $d = \sum_{i=1}^{n} c_i a_i \vdots d_1$. Тем самым доказано, что $d = НОД(a_1, a_2, ..., a_n)$. Представление d в виде $d = \sum_{i=1}^{n} c_i a_i$ получено выше. **Ч.т.д.**

В частности, доказано, что $\boxed{\forall a, b\ НОД(a,b) = d \Rightarrow \exists x, y \in \mathbb{Z}\ ax + by = d}$.

Пример 6.2. Легко проверить, что $НОД(4,6,10) = 2$. При этом $3 \cdot 4 + 0 \cdot 6 + (-1) \cdot 10 = 2$. Также верно, что $0 \cdot 4 + 2 \cdot 6 + (-1) \cdot 10 = 2$, а также, что $7 \cdot 4 + (-1) \cdot 6 + (-2) \cdot 10 = 2$.

Вывод: представление $d = НОД(a_1, a_2, ..., a_n)$ в виде $d = \sum_{i=1}^{n} c_i a_i$ не единственно.

Следствие 6.1. НОД набора чисел, среди которых не все нули, существует и единственен.

Доказательство. Существование доказано в Теореме 6.1. тогда, в силу Утверждения 6.1, НОД является максимальным элементом множества всех делителей, единственность максимального элемента очевидна. **Ч.т.д.**

<u>Свойство 6.1</u>. *НОД не меняется при перестановке аргументов*.

Доказательство. Очевидно, так как в определении НОД никак не учитывается порядок чисел. **Ч.т.д.**

В частности, $\boxed{НОД(a,b) = НОД(b,a)}$.

Свойство 6.2. *Если среди чисел* $a_1, a_2, ..., a_n$ есть 1 или -1, то $НОД(a_1, a_2, ..., a_n) = 1$.

Доказательство. Т.к мы перечисляем общие делители всех чисел, то они должны быть и делителями 1 или -1. Такими делителями являются только 1 или -1 (например, в силу Свойств 1.1. и 1.7). Таким образом, множеством всех общих делителей будет $\{1; -1\}$, а значит $НОД(a_1, a_2, ..., a_n) = 1$. **Ч.т.д.**

Опр.6.3. Если $НОД(a, b) = 1$, то числа a и b называют *взаимно простыми*.

Опр.6.4. Если $НОД(a_1, a_2, ..., a_n) = 1$, то числа $a_1, a_2, ..., a_n$ называют *взаимно простыми в совокупности*.

Опр.6.5. Если $\forall i \neq j \; НОД(a_i, a_j) = 1$, то числа $a_1, a_2, ..., a_n$ называют *попарно взаимно простыми*.

Пример 6.3. Не сложно проверить, что $НОД(18,9) = 9$, $НОД(18,16) = 2$, но при этом $НОД(18,9,16) = 1$, следовательно, числа 18,9,16 являются взаимно простыми в совокупности, но не являются попарно взаимно простыми.

Замечание 6.3. В литературе по теории чисел $НОД(a_1, a_2, ..., a_n)$ не редко обозначают, как $(a_1, a_2, ..., a_n)$, однако такое обозначение двусмысленно (надо стараться понимать из контекста о чём идёт речь: о наибольшем общем делителе или об упорядоченном наборе чисел). В случаях неоднозначной интерпретации будем использовать стандартное обозначение. В новых обозначениях факт *взаимной простоты* чисел a и b записывается, как $\boxed{(a,b) = 1}$, факт *взаимной простоты в совокупности* чисел $a_1, a_2, ..., a_n$ будет обозначаться, как $\boxed{(a_1, a_2, ..., a_n) = 1}$. Т.к. никакой упорядоченный набор чисел, очевидно, не равен одному целому числу (исключаем изоморфизмы, вроде $(6,3) = 6/3 = 2$), такая запись уже воспринимается всегда однозначно и потому будет использоваться в дальнейшем.

Далее мы сначала обсудим свойства НОД и некоторые связанные с НОД свойства делимости для двух чисел.

Свойство 6.3. *Если существует* $НОД(a, b)$, *то для любого* c *существует* $НОД(a - bc, b)$ *и* $\boxed{НОД(a, b) = НОД(a - bc, b)}$.

Доказательство. Пусть d - какой-нибудь общий делитель чисел a и b, тогда $a \vdots d \wedge b \vdots d \overset{Св-во 1.5}{\Rightarrow} a - bc \vdots d$, т.е. d - общий делитель чисел $a - bc$ и b. Обратно, если d - какой-нибудь общий делитель чисел $a - bc$ и b, тогда

$a-bc \vdots d \wedge b \vdots d \overset{Св-во 1.5}{\Rightarrow} a \vdots d$, т.е. d - общий делитель чисел a и b. Таким образом, множество всех делителей чисел a и b совпадает с множеством всех делителей чисел $a-bc$ и b. Тогда, если в одном множестве существует положительный элемент, кратный всем остальным, то такой же элемент существует и в другом множестве, при этом данные элементы совпадают. **Ч.т.д.**

Пример 6.4. Множество всех общих делителей чисел 20 и 12 это $\{1,-1,2,-2,4,-4\}$. Не сложно увидеть, что $НОД(20,12)=4$. Если вычислить $20-12=8$, то множество всех общих делителей чисел 20 и 8 это $\{1,-1,2,-2,4,-4\}$. Множества общих делителей совпали, отсюда сразу следует, что $НОД(20,8)=4$.

<u>Свойство 6.4</u>. *Если* $n \geq 3$ *и среди чисел* $a_1, a_2, ..., a_n$ есть 0, то его можно исключить из аргументов $НОД(a_1, a_2, ..., a_n)$, т.е.

$\boxed{НОД(a_1,a_2,...,0)=НОД(a_1,a_2,...,a_{n-1})}$. Если $a \neq 0$, то $\boxed{НОД(a,0)=|a|}$.

Доказательство. Т.к. 0 кратен любому числу, кроме 0, то множество его делителей это $\mathbb{Z}\setminus\{0\}$, множество делителей любого другого числа – подмножество данного множества. Следовательно, общими делителями нуля и остальных чисел будут все общие делители нуля и остальных чисел, а значит, ноль можно исключить из числа аргументов. Если аргументов два, то очевидно, что $|a|>0$, является делителем a и кратен любому другому делителю a (множество делителей a совпадает с множеством делителей $|a|$ и является подмножеством множества делителей нуля). Поэтому $НОД(a,0)=|a|$ **Ч.т.д.**

Пример 6.5. Найти $НОД(102,340)$.

Решение. $НОД(102,340) \overset{Св-во 6.3.}{=} НОД(102,340-3\cdot 102)=НОД(102,34) \overset{Св-во 6.3.}{=}$
$=НОД(102-3\cdot 34,34)=НОД(0,34) \overset{Св-во 6.4.}{=} 34$.

Если $ab \vdots c$, то вовсе не обязательно, что $a \vdots c$ или $b \vdots c$. Например, $(6\cdot 8) \vdots 24$, однако $6 \not\vdots 24$ и $8 \not\vdots 24$. Значит необходимо дополнительное условие.

<u>Свойство 6.5</u>. *Если* $ab \vdots c$*, при этом* a *и* c *взаимно простые, то* $b \vdots c$ $\boxed{ab \vdots c \wedge (a,c)=1 \Rightarrow b \vdots c}$.

Доказательство. $(a,c)=1 \overset{Т.6.2}{\Rightarrow} \exists x\, \exists y\; ax+cy=1 \Rightarrow \underset{\vdots c}{\underline{ab}}\,x+\underset{\vdots c}{\underline{c}}\,by=b \overset{Св-во.1.5.}{\Rightarrow} b \vdots c$ **Ч.т.д.**

<u>Свойство 6.6</u>. *Если a взаимно просто с числами b и c, то a взаимно просто и с их произведением* $\boxed{(a,b)=1 \wedge (a,c)=1 \Rightarrow (a,bc)=1}$.

Доказательство. Пусть $НОД(a,bc)=d$,

$(a,c)=1 \overset{T.6.1}{\Rightarrow} \exists x\, \exists y\; ax+cy=1 \Rightarrow \underset{\vdots d}{\underline{a}}bx+\underset{\vdots d}{\underline{bc}}y=b \Rightarrow b \vdots d$, таким образом, d - общий делитель a и b, следовательно, $НОД(a,b) \vdots d$, т.е. $1 \vdots d \wedge d>0$, а значит $d=1$. **Ч.т.д.**

Пример 6.6. $НОД(26,9)=1$, $НОД(26,77)=1$, следовательно, мы сразу можем утверждать, что $НОД(26,9\cdot 77)=НОД(26,693)=1$.

Если одно число делится на два других, то вовсе не обязательно оно делится и на их произведение. Например, $36 \vdots 12$ и $36 \vdots 6$, но $36 \not\vdots 72$, где $72=12\cdot 6$. И дело здесь не только в том, что результат произведения оказался больше по модулю. Например, $36 \vdots 2$ и $36 \vdots 4$, но $36 \not\vdots 8$, где $8=2\cdot 4$.

<u>Свойство 6.7</u>. *Если $a \vdots b$, $a \vdots c$ при этом числа b и c взаимно просты, то $a \vdots (bc)$*

$\boxed{a \vdots b \wedge a \vdots c \wedge (b,c)=1 \Rightarrow a \vdots (bc)}$.

Доказательство. $a \vdots b \Rightarrow a=b\cdot a_1$, $a \vdots c \Leftrightarrow ba_1 \vdots c$, *т.к.* $НОД(b,c)=1$, то по Свойству 6.5., $a_1 \vdots c$ т.е., $a_1=c\cdot a_2$. Таким образом,
$a=ba_1=b(ca_2)=(bc)a_2 \vdots (bc)$. **Ч.т.д.**

Например, т.к. $НОД(2,3)=1$, то, если число кратно 2 и кратно 3, то оно кратно и 6. Аналогично, т.к. $НОД(4,9)=1$, то, если число кратно 4 и кратно 9, то оно кратно и 36. Однако, если число кратно 4 и кратно 10, то отсюда вовсе не следует, что оно кратно 40. В качестве контрпримера подойдёт число 60.

<u>Свойство 6.8</u>. $\boxed{НОД(a,b)=НОД(a,-b)=НОД(-a,b)=НОД(-a,b)}$.

Доказательство. Ясно, что любой делитель b будет делителем и $-b$ ($b=c\cdot b_1 \Rightarrow -b=-(c\cdot b_1)=c\cdot(-b_1)$). Таким образом, множество общих делителей чисел a и b совпадает с множеством общих делителей чисел a и $-b$, следовательно, совпадают и наибольшие элементы этих множеств. Остальные равенства доказываются аналогично. **Ч.т.д.**

<u>Свойство 6.9</u>. $\boxed{НОД(ca,cb)=|c|\cdot НОД(a,b)}$.

Доказательство. Пусть $НОД(a,b)=d$, $НОД(ca,cb)=d_1$. По Следствию 1.2. нам достаточно доказать, что $d_1 \vdots (|c|d)$ и $(|c|d) \vdots d_1$.

$a\vdots d \wedge b\vdots d \Rightarrow ca\vdots cd \wedge cb\vdots cd$, т.е. cd - общий делитель ca и cb, следовательно, $d_1\vdots cd \Rightarrow d_1\vdots |cd| \Leftrightarrow d_1\vdots |c|d$.

Обратно, по Теореме 6.1.
$\exists x\, \exists y\; ax+by=d \Rightarrow \underset{\vdots d_1}{\underline{ca}}\,x+\underset{\vdots d_1}{\underline{cb}}\,y=cd \Rightarrow cd\vdots d_1 \Rightarrow |c|d\vdots d_1$. **Ч.т.д.**

<u>Свойство 6.10</u>. $\boxed{НОД(a,b)=d \Rightarrow НОД(\frac{a}{d},\frac{b}{d})=1}$.

Доказательство.

$$d=НОД(a,b)=НОД(d\cdot\frac{a}{d},d\cdot\frac{b}{d})\overset{Св-во\ 6.9}{=}d\cdot НОД(\frac{a}{d},\frac{b}{d}) \Leftrightarrow НОД(\frac{a}{d},\frac{b}{d})=1$$ **Ч.т.д.**

<u>Свойство 6.11</u>. $\boxed{(b,c)=1 \Rightarrow НОД(ac,b)=НОД(a,b)}$.

Доказательство. Пусть $НОД(a,b)=d$, $НОД(ac,b)=d_1$. Т.к. $a\vdots d$, то $ac\vdots d$ также $b\vdots d$, таким образом, d - общий делитель ac и b, следовательно, $d_1\vdots d$. По Следствию 1.2. для доказательства равенства $d=d_1$ нам достаточно доказать, что $d\vdots d_1$.

$НОД(b,c)=1\overset{T.6.1}{\Rightarrow}\exists x\,\exists y\; bx+cy=1 \Rightarrow a\underset{\vdots d_1}{\underline{b}}\,x+\underset{\vdots d_1}{\underline{ac}}\,y=a \Rightarrow a\vdots d_1$ Т.к. $a\vdots d_1$ и $b\vdots d_1$, то $d=НОД(a,b)\vdots d_1$. **Ч.т.д.**

<u>Свойство 6.12</u>. $\boxed{НОД(b,c)=d \Rightarrow НОД(ac,b)=d\cdot НОД(a,\frac{b}{d})}$.

Доказательство. $НОД(ac,b)=НОД(d\cdot a\cdot\frac{c}{d},d\cdot\frac{b}{d})\overset{Св-во\ 6.9}{=}d\cdot НОД(a\cdot\frac{c}{d},\frac{b}{d})$.

Т.к. по Свойству 6.10 $НОД(\frac{c}{d},\frac{b}{d})=1$, то по Свойству 6.11

$d\cdot НОД(a\cdot\frac{c}{d},\frac{b}{d})=d\cdot НОД(a,\frac{b}{d})$. **Ч.т.д.**

Пример 6.7.

$$НОД(108\cdot 88,24)\overset{НОД(88,24)=8}{=}8\cdot НОД(108,24/8)=8\cdot НОД(108,3)=8\cdot 3=24$$

Замечание 6.4. Разумеется, Свойство 6.11 – частный случай Свойства 6.12, но Свойство 6.11 мы использовали в доказательстве Свойства 6.12, поэтому выводить Свойство 6.11 из свойства 6.12 мы не можем.

Доказанные свойства НОД двух чисел в том числе позволяют нам быстрее находить НОД.

Пример 6.8. Вычислим $НОД(65444,2560)$.

$$НОД(65444,2560)=НОД(2\cdot 32722,2\cdot 1280)\overset{6.9}{=}2\cdot НОД(32722,1280)=$$

$$=2\cdot НОД(2\cdot 16361,2\cdot 640)\overset{6.9}{=}4\cdot НОД(16361,640)=4\cdot НОД(16361,64\cdot 10)=$$

$$(НОД(16361,10)\overset{6.3}{=}НОД(16361-1636\cdot 10,10)=НОД(1,10)\overset{6.2}{=}1)$$

$$\overset{6.11}{=}4\cdot НОД(16361,64)=4\cdot НОД(16361,2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2)=$$

$$(т.к. 16361\not\vdots\, 2, то\ НОД(16361,2)=1)$$

$$\overset{6.11}{=}4\cdot НОД(16361,2)=4\cdot 1=4$$

Вспомним, что, в силу Свойства 3.6., $a\equiv b\ (\mathrm{mod}\ m)\Rightarrow a\cdot c\equiv b\cdot c\ (\mathrm{mod}\ m)$, однако, в силу Замечания 3.2., обратное не верно (нельзя просто так сокращать на общий множитель в сравнении). Однако, при некотором дополнительном условии (и таковым снова станет взаимная простота) сокращать уже можно.

Свойство 6.13. $\boxed{a\cdot c\equiv b\cdot c\ (\mathrm{mod}\ m)\wedge(c,m)=1\Rightarrow a\equiv b\ (\mathrm{mod}\ m)}$.

Доказательство. $a\cdot c\equiv b\cdot c\ (\mathrm{mod}\ m)\Leftrightarrow(a-b)c\,\vdots\, m$, т.к. $(c,m)=1$, то по Свойству 6.5. $a-b\,\vdots\, m\Leftrightarrow a\equiv b\ (\mathrm{mod}\ m)$. **Ч.т.д.**

Мы определяли НОД для любого количества чисел, но большинство свойств доказали именно для НОД 2-х чисел, возникает вопрос, что делать, если аргументов НОД больше? Ответить на эти вопросы помогает следующая теорема, позволяющая рекуррентно выразить НОД большего количества чисел через НОД меньшего количества чисел.

Теорема 6.2 *Если среди чисел* $a_1,a_2,...,a_n$ не все равны 0*, то*

$\boxed{НОД(a_1,a_2,...,a_n)=НОД(НОД(a_1,a_2,...,a_{n-1}),a_n)}$ *(если* $a_1=a_2=...=a_{n-1}=0$, то $\boxed{a_1=a_2=...=a_{n-1}=0\Rightarrow НОД(a_1,a_2,...,a_n)=|a_n|}$*).*

Например, $НОД(a,b,c)=НОД(НОД(a,b),c)$,
$НОД(a,b,c,d)=НОД(НОД(a,b,c),d)=НОД(НОД(НОД(a,b),c),d)$.

Доказательство. *Если* $a_1=a_2=...=a_{n-1}=0$, то множество их общих делителей это $\mathbb{Z}\setminus\{0\}$, множество делителей числа $a_n\neq 0$ - подмножество данного множества, следовательно, его наибольший элемент, очевидно равный $|a_n|$ и будет $НОД(a_1,a_2,...,a_n)$. В остальных случаях пусть $НОД(a_1,a_2,...,a_n)=d$,

$НОД(a_1,a_2,...,a_{n-1})=d_1$, $НОД(d_1,a_n)=d_2$. Хотим доказать, что $d=d_2$. По Следствию 1.2 для этого нам достаточно доказать, что $d \vdots d_2$ и $d_2 \vdots d$.

$$НОД(a_1,a_2,...,a_n)=d \Rightarrow \begin{cases} a_1 \vdots d \wedge a_2 \vdots d \wedge ... \wedge a_{n-1} \vdots d \\ a_n \vdots d \end{cases} \overset{НОД(a_1,a_2,...,a_{n-1})=d_1}{\Rightarrow} \begin{cases} d_1 \vdots d \\ a_n \vdots d \end{cases} \overset{НОД(d_1,a_n)=d_2}{\Rightarrow}$$

$\Rightarrow \underline{d_2 \vdots d}$

$$НОД(d_1,a_n)=d_2 \Rightarrow \begin{cases} d_1 \vdots d_2 \\ a_n \vdots d_2 \end{cases}$$

$НОД(a_1,a_2,...,a_{n-1})=d_1 \Rightarrow a_1 \vdots d_1 \wedge a_2 \vdots d_1 \wedge ... \wedge a_{n-1} \vdots d_1$, т.к. $d_1 \vdots d_2$, то $a_1 \vdots d_2 \wedge a_2 \vdots d_2 \wedge ... \wedge a_{n-1} \vdots d_2$. Т.к. вдобавок $a_n \vdots d_2$, то d_2 - общий делитель $a_1,a_2,...,a_n$, следовательно, $НОД(a_1,a_2,...,a_n)=\underline{d \vdots d_2}$. **Ч.т.д.**

Пример 6.9. Найдём $НОД(455,560,1280)$.

Решение.

$$НОД(455,560)=5\cdot НОД(91,112)=5\cdot НОД(91,112-91)=5\cdot НОД(91,21)=$$
$$=5\cdot НОД(91-4\cdot 21,21)=5\cdot НОД(7,21)=5\cdot 7=35$$

Теперь

$$НОД(35,1280)=5\cdot НОД(7,256)=5\cdot НОД(7,256-36\cdot 7)=5\cdot НОД(7,4)=5\cdot 1=5$$

Таким образом, $НОД(455,560,1280)=5$.

Опираясь на формулу из Теоремы 6.2, мы сможем обобщить некоторые свойства НОД на большее количество аргументов. Обобщим, например, Свойство 6.9.

<u>Свойство 6.14</u>. $\boxed{НОД(ca_1,ca_2,...,ca_n)=|c|\cdot НОД(a_1,a_2,...,a_n)}$ **.**

Доказательство. Для краткости записи ограничимся доказательством для $n=3$, общий случай легко доказывается индукцией по n и остаётся читателю в качестве несложного упражнения (идея перехода от $n+1$ к n точно такая же, как идея перехода от $n=3$ к $n=2$).

$$НОД(ca_1,ca_2,ca_3)\overset{T.6.3}{=}НОД(НОД(ca_1,ca_2),ca_3)\overset{Св-во\ 6.9}{=}НОД(|c|\,НОД(a_1,a_2),ca_3)=$$
$$\overset{Св-во\ 6.8}{=}НОД(|c|\,НОД(a_1,a_2),|c|\,a_3)\overset{Св-во\ 6.9}{=}|c|\,НОД(НОД(a_1,a_2),a_3)\overset{T.6.2}{=}$$
$$=|c|\cdot НОД(a_1,a_2,a_3).$$ **Ч.т.д.**

Пример 6.10.

$$НОД(645,510,420)=5\cdot НОД(129,102,84)=5\cdot 3\cdot НОД(43,34,28)=15$$

Обобщение Свойства 6.3. будет выглядеть так:

<u>Свойство 6.15</u>. $\boxed{НОД(a_1,a_2,...,a_{n-1},a_n)=НОД(a_1,a_2,...,a_{n-1},a_n-c\cdot a_k)}$ *(при* $k\neq n$*) - НОД не изменится, если из одного аргумента вычесть несколько других***.**

Доказательство. Будем доказывать индукцией по n. Для $n=2$ утверждение верно в силу Свойства 6.3., тем самым, доказана база индукции.

Предположим, что для *некоторого* n НОД не меняется, если из любого одного аргумента вычесть любое количество любых других аргументов (предположение индукции). Т.к. по Свойству 6.1. НОД не меняется при перестановке аргументов, не умаляя общности мы можем считать, что нам нужно из первого аргумента вычесть сколько-то вторых. Тогда:

$$НОД(a_1,a_2,...,a_n,a_{n+1})\overset{T6.2}{=}НОД(НОД(a_1,a_2,...,a_n),a_{n+1})\overset{П.И.}{=}$$
$$\overset{П.И.}{=}НОД(НОД(a_1-ka_2,a_2,...,a_n),a_{n+1})\overset{T.6.2}{=}НОД(a_1-ka_2,a_2,...,a_n,a_{n+1}).$$ **Ч.т.д.**

Пример 6.11. $НОД(15424,7988,15422)\overset{6.15}{=}НОД(15424-15422,7988,15422)=$
$=НОД(2,7988,15422)\overset{6.14}{=}2\cdot НОД(1,3994,7711)\overset{6.2}{=}2\cdot 1=2$.

Обобщим Свойство 6.10

<u>Свойство 6.16</u>. $\boxed{НОД(a_1,a_2,...,a_n)=d\Rightarrow НОД(\frac{a_1}{d},\frac{a_2}{d},...,\frac{a_n}{d})=1}$**.**

Доказательство. Полностью аналогично доказательству обобщаемого Свойства 6.10, только аргументов больше и вместо Свойства 6.9. нужно сослаться на Свойство 6.14. **Ч.т.д.**

<u>Утверждение 6.2</u>. *Числа* $a_1,a_2,...,a_n$ *взаимно просты в совокупности в том и только том случае, когда найдутся такие* $c_1,c_2,...,c_n\in\mathbb{Z}$*, что* $\sum_{i=1}^{n}c_ia_i=1$.

Доказательство. Если $a_1,a_2,...,a_n$ взаимно просты в совокупности, т.е. $НОД(a_1,a_2,...,a_n)=1$, то по Теореме 6.1. $\exists c_1,c_2,...,c_n\in\mathbb{Z}\ \sum_{i=1}^{n}c_ia_i=1$.

Обратно, если $\exists c_1, c_2, ..., c_n \in \mathbb{Z} \sum_{i=1}^{n} c_i a_i = 1$ и $НОД(a_1, a_2, ..., a_n) = d$, то $\forall i \; a_i \vdots d$, следовательно, $1 = \sum_{i=1}^{n} c_i a_i \vdots d \Rightarrow d = 1$, т.е. $a_1, a_2, ..., a_n$ взаимно просты в совокупности. **Ч.т.д.**

<u>Утверждение 6.3</u>. *Если среди чисел некоторого набора есть пара взаимно простых чисел, то числа набора взаимно просты в совокупности. В частности, попарно взаимно простые числа взаимно просты в совокупности. Обратное не верно.*

Доказательство. Не умаляя общности можем считать, что $НОД(a_1, a_2) = 1$, тогда, применяя нужное количество раз Теорему 6.2, получаем

$$НОД(a_1, a_2, ..., a_n) \overset{T.6.2}{=} НОД(....НОД(НОД(a_1, a_2), a_3)..., a_n) =$$
$$= НОД(....НОД(1, a_3)..., a_n) \overset{T.6.2}{=} НОД(1, a_3, ..., a_n) \overset{Св.6.2}{=} 1.$$

Если рассмотреть набор чисел $\{10, 6, 15\}$, то не сложно проверить, что $НОД(10, 6, 15) = 1$, т.е. эти числа взаимно просты в совокупности. При этом $НОД(10, 6) = 2$, $НОД(10, 15) = 5$, $НОД(6, 15) = 3$, т.е. среди этих чисел нет пар взаимно простых. **Ч.т.д.**