ДАУГАВПИЛССКИЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

ВОПРОСЫ ПРЕПОДАВАНИЯ МАТЕМАТИКИ

Выпуск 2

СБОРНИК СТАТЕЙ

XXIV

ИЗДАТЕЛЬСТВО «ЗВАЙГЗНЕ»
РИГА 1975

М $\frac{6\text{-}5\text{-}115}{\text{М}802(11)\text{-}75}$ 309—75

Ш. Х. МИХЕЛОВИЧ

ОБ ИСПОЛЬЗОВАНИИ ТЕОРИИ МНОЖЕСТВ В ДОПОЛНИТЕЛЬНЫХ ВОПРОСАХ АРИФМЕТИКИ (НА ФАКУЛЬТАТИВНЫХ ЗАНЯТИЯХ В VII КЛАССЕ)

I. При изучении теории делимости натуральных чисел в школьном курсе теорией множеств до сих пор пользовались мало. И в новом учебном пособии для пятого класса [1] теоретико-множественный аппарат применяется весьма ограниченно.

На с. 100 указывается, что множество общих кратных чисел 4 и 6 есть пересечение множества A (чисел, кратных 4) и B (чисел, кратных 6), т. е.

$$A \cap B = \{12, 24, 36, 48, \ldots\},$$

откуда следует, что наименьшее общее кратное этих чисел равно 12:

$$K(4, 6) = 12.$$

На с. 96 записаны множества A — делителей числа 48 и B — делителей числа 36:

$$A = \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\};$$

$$B = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}.$$

По образцу на с. 100 следовало бы и здесь отметить, что

$$A \cap B = \{1, 2, 3, 4, 6, 12\}.$$

Однако в данном случае авторы ограничиваются словесным указанием, что общими делителями чисел 48 и 36 являются числа: 1, 2, 3, 4, 6, 12, и заключают, что

$$D\ (48, 36) = 12.$$

Таким образом, операция объединения множеств вообще не получает применения в теории делимости, хотя именно во второй главе о делимости натуральных чисел она и вводится.

В дальнейшем, на с. 110, отмечается, что всякое натуральное число, кроме 1, можно разложить на простые множители и что такое разложение является единственным, если не учитывать порядка расположения множителей, а на с. 112 — что в разложение НОД двух чисел должны войти простые множители, которые содержатся в разложении как одного, так и второго числа, причем если они входят в эти разложения с разными показателями, то берется множитель с меньшим показателем.

Чтобы факультативные занятия не были формальными и оторванными от этого изложения и вызвали бо́льший интерес, следовало бы обратить внимание учащихся на то, что последнее утверждение и другие базируются на упомянутой выше теореме единственности.

В качестве первого шага рассматриваем важное следствие основной теоремы арифметики, а именно: любой простой делитель p числа a обязательно входит в его разложение на простые множители.

В самом деле, если a делится на p, то $a=p\cdot a_1$. Поэтому разложение a можно получить из разложения a_1, добавив к нему простой множитель p. Так как по предположению других разложений числа a на простые множители не существует, то p в указанное разложение входит.

С другой стороны, в системе чисел $E=\{1, 2, 4, 6, 8, \ldots\}$, в которой однозначная разложимость на неразложимые множители не имеет места, из делимости числа a на «простое» число p еще не следует, что оно входит в разложение a. Так, например, 108 делится на 2 $(108=2\cdot 54)$, но 2 не входит в разложение $108=6\cdot 18$.

Согласно указанному следствию, которое, как видно, тесно связано с однозначной разложимостью на простые множители, легко получить каноническую форму произведения двух чисел a и b, заданных в такой же форме: она будет содержать те и только те простые множители, которые входят в a и b, и каждый из них войдет в нее столько раз, сколько в a и b вместе.

Так, например, из

$$60=2^2\cdot 3\cdot 5, \qquad 42=2\cdot 3\cdot 7 \Longrightarrow 60\cdot 42=2^3\cdot 3^2\cdot 5\cdot 7.$$

II. В дальнейшем целесообразно шире использовать теоретико-множественные операции. Трудности в этом отношении связаны с тем, что при разложении числа на простые множители они могут повторяться. Возникает как будто бы противо-

речие с основным положением Г. Кантора, что элементы множества должны быть различимыми. Однако, по нашему мнению, эти трудности можно преодолеть, если развить замысел, изложенный в заметке К. Н. (по-видимому, Korczowski Henryk), [2].

Исходя из разложения числа a на простые множители, будем рассматривать и множество P_a его простых делителей, например, $P_{60}=\{2, 2, 3, 5\}$, включая в это множество каждый простой делитель столько раз, сколько раз он входит в a как множитель (мы считаем, таким образом, одинаковые простые множители различимыми).

В общем случае, когда $a=p_1^{\alpha_1}, p_2^{\alpha_2} \ldots p_k^{\alpha_k}$,

$$P_a=\{\underbrace{p_1, p_1, \ldots, p_1}_{\alpha_1}, \underbrace{p_2, p_2, \ldots p_2}_{\alpha_2} \ldots, \underbrace{p_k, p_k, \ldots, p_k}_{\alpha_k}\}.$$

Для сокращения записи будем впредь пользоваться обозначением:

$$P_a=\{\underset{(\alpha_1)}{p_1}, \underset{(\alpha_2)}{p_2}, \ldots, \underset{(\alpha_k)}{p_k}\}.$$

Если $a=1$, то множество простых делителей этого числа пусто, так что

$$P_1=\varnothing.$$

Вернемся к исходной позиции: из теоремы единственности вытекает, что каждый простой множитель p, на который a делится, входит в его разложение. Ее можно теперь выразить иначе: p входит в множество P_a простых делителей a. Если через Т. Е. обозначим теорему единственности, а символом $a|p$ — то, что a делится на p ($a\nmid p$ означает — a не делится на p), то последнее утверждение можно записать кратко следующим образом:

$$\text{Т. Е.} \Longrightarrow (\forall p, a|p \Longrightarrow p\in P_a). \qquad \text{(I)}$$

Если числа a и b заданы в канонической форме, то легко указать общий критерий их делимости: a делится на b в том и только в том случае, если все простые множители b входят и в a, притом с не меньшим показателем степени, чем в b. Пользуясь множествами P_a и P_b, указанный критерий можно выразить и так:

$a|b$ тогда и только тогда, когда $P_a\supset P_b$, т. е.

$$a|b \Longleftrightarrow P_a\supset P_b.$$

П р и м е р ы.

1) $a=2520=2^3\cdot3^2\cdot5\cdot7$; $\quad P_a=\left\{\begin{matrix}2, & 3, & 5, & 7\\ (3) & (2) & & \end{matrix}\right\}$;

$b=\ 630=2\cdot3^2\cdot5\cdot7$; $\quad P_b=\left\{\begin{matrix}2, & 3, & 5, & 7\\ & (2) & & \end{matrix}\right\}$;

$a|b$, так как $P_a\supset P_b$.

2) $a=1890=2\cdot3^3\cdot5\cdot7$; $\quad P_a=\left\{\begin{matrix}2, & 3, & 5, & 7\\ & (3) & & \end{matrix}\right\}$;

$b=\ 168=2^3\cdot3\cdot7$; $\quad P_b=\left\{\begin{matrix}2, & 3, & 7\\ (3) & & \end{matrix}\right\}$;

$a \nmid b$, так как $P_a\not\supset P_b$.

Согласно введенным обозначениям из

$$\underset{(\alpha)}{p}\in P_a;\quad \underset{(\beta)}{p}\in P_b,\ \text{где}\ 1\leqslant\alpha\leqslant\beta,$$

вытекает:

$$\underset{(\alpha)}{p}\in P_a\cap P_b;\quad \underset{(\beta)}{p}\in P_a\cup P_b,$$

т. е. $\underset{(\alpha)}{p}$ принадлежат пересечению этих множеств, а $\underset{(\beta)}{p}$ — объединению (рис. 1 и 2).

Для сохранения этих соотношений в случае, когда $p\notin P_a$, этот факт будем записывать в форме $\underset{(0)}{p}\in P_a$.

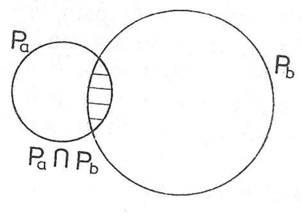

Рис. 1

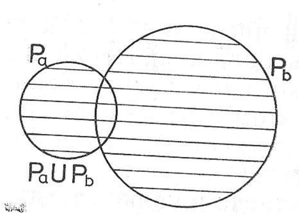

Рис. 2

Введем для множеств P_a и P_b простых делителей двух чисел операции их сложения и вычитания.

Множество, получаемое при сложении, будем называть суммой множеств и обозначать его P_a+P_b, считая, что

$$\underset{(\alpha)}{p}\in P_a,\ \underset{(\beta)}{p}\in P_b \Longrightarrow \underset{(\alpha+\beta)}{p}\in P_a+P_b.$$

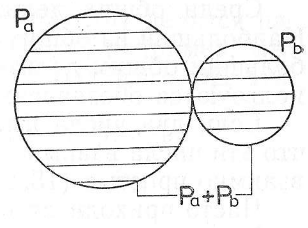

Рис. 3

Таким образом, все встречающиеся в отдельных множествах одинаковые простые множители будем считать различимыми в их сумме.

Соответствующий график можно представить в виде рис. 3.

Операцию вычитания множеств P_a и P_b будем рассматривать только в том случае, когда $P_a\supset P_b$. Множество, получаемое при вычитании, будем называть разностью данных множеств и обозначать его P_a-P_b. Положим по определению:

$$\underset{(\alpha)}{p}\in P_a;\quad \underset{(\beta)}{p}\in P_b \Longrightarrow \underset{(\alpha-\beta)}{p}\in P_a-P_b.$$

При этом, согласно принятому условию, $\alpha\geqslant\beta$.

Итак, при образовании разности множеств P_a и P_b каждый простой множитель из P_b сопоставляется равному множителю из P_a и исключается.

Для наглядного изображения разности P_a-P_b можно воспользоваться рис. 4.

Если $P_a-P_b=P_c$,

то понятно, что

$$P_a=P_b+P_c.$$

Введенные операции сложения и вычитания двух множеств имеют тесное отношение к множествам простых множителей произведения и частного двух натуральных чисел a и b (для частного — в том случае, когда a делится на b), а именно:

$$P_{ab}=P_a+P_b;$$

$$P_{a:b}=P_a-P_b.$$

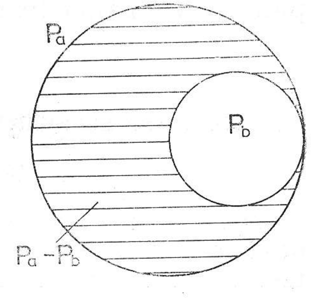

Рис. 4

III. Среди делителей двух чисел бывают общие (ОД). Запишем, например, в возрастающем порядке все делители чисел 24 и 30:

делители 24: 1, 2, 3, 4, 6, 8, 12, 24;

„ 30: 1, 2, 3, 5, 6, 10, 15, 30.

$$\frac{1620}{108}=\frac{2^2\cdot 3^4\cdot 5}{2^2\cdot 3^3}=3\cdot 5,$$

так что

$$\left(\frac{1512}{108}, \frac{1620}{108}\right)=(2\cdot 7,\ 3\cdot 5)=1.$$

3. Если $(a, b)=d$, то $(am, bm)=dm$.

Действительно, в числах am и bm, по сравнению с числами a и b, появляется новый общий множитель m.

Переходя к соответствующим множествам простых сомножителей, мы имели бы:

$$P_d=P_{(a,b)}=P_a \cap P_b;$$

$$P_{am}=P_a+P_m, \quad P_{bm}=P_b+P_m;$$

$$P_{(am,bm)}=(P_a+P_m) \cap (P_b+P_m).$$

Обращаясь к иллюстрации (рис. 6), убеждаемся в том, что

$$(P_a+P_m) \cap (P_b+P_m)=$$
$$=(P_a \cap P_b)+P_m=P_d+P_m=P_{dm}.$$

Таким образом:

$$P_{(am,bm)}=P_{dm}, \quad \text{откуда} \quad (am,\ bm)=dm.$$

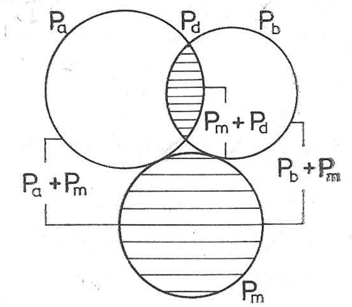

Рис. 6

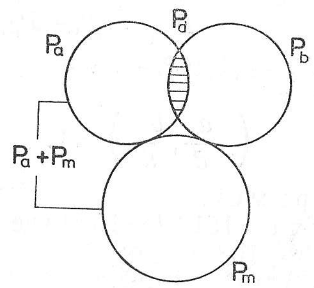

Рис. 7

4. НОД двух чисел не изменяется от умножения (или деления, если это возможно) одного из них на число, взаимно простое со вторым, т. е.

$$(a,\ b)=d, \quad (m,\ b)=1 \Rightarrow (am,\ b)=d;$$

$$(a,\ b)=d, \quad (m,\ b)=1,\ a|m \Rightarrow \left(\frac{a}{m},\ b\right)=d.$$

Дело в том, что в связи с указанным умножением числа am и b не приобретают новых ОД, по сравнению с теми, которые были у a и b (аналогично и при делении).

Проиллюстрируем этот факт, обращаясь также к множествам простых сомножителей (рис. 7).

$$P_{(am,b)}=P_{am} \cap P_b=(P_a+P_m) \cap P_b=P_a \cap P_b=P_d,$$

так как $P_m \cap P_b=\varnothing$.

5. Если $ab|c$ и $(a, c)=1$, то $b|c$.

Пример. $72=8\cdot 9$, $72|4$, $(9, 4)=1 \Rightarrow 8|4$, что, конечно, хорошо известно.

Для обоснования этого свойства обратимся к соответствующим множествам простых сомножителей.

1) $ab|c \Rightarrow P_{ab} \supset P_c$ или $P_a+P_b \supset P_c$; (1)

2) $(a,\ c)=1 \Rightarrow P_a \cap P_c=\varnothing$; (2)

3) Из (1) и (2) следует, что $P_b \supset P_c$, откуда $b|c$.

Приводим соответствующую иллюстрацию (рис. 8).

Данное свойство можно также получить из свойства 4.

В самом деле, если $ab|c$, то $(ab, c)=c$. Но поскольку $(a, c)=1$, то (по свойству 4) $\left(\frac{ab}{a}, c\right)=(b, c)=c$, а это значит, что $b|c$.

6. Если произведение нескольких чисел делится на простое число p, то по меньшей мере один из этих сомножителей делится на p.

Это свойство вытекает из предыдущего.

Если, например, $abc|p$, но $c \nmid p$, т. е. $(c, p)=1$, то $ab|p$; если, далее, $b \nmid p$, то $a|p$.

7. Если $(a, m)=1$, $(b, m)=1$, то и $(ab, m)=1$. Это свойство непосредственно следует из свойства 4;

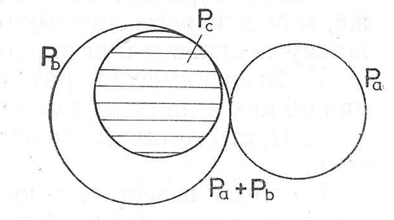

Рис. 8

его можно обобщить: если $(a, m)=1$, $(b, m)=1$ и $(c, m)=1$, то $(abc, m)=1$.

8. Пусть (a, b, c) — НОД натуральных чисел a, b и c. Так же, как и в случае двух чисел, должно быть:

$$P_{(a,b,c)}=P_a\cap P_b\cap P_c.$$

Но по самому определению — пересечение множеств ассоциативно, т. е.

$$P_a\cap P_b\cap P_c=(P_a\cap P_b)\cap P_c=$$
$$=P_a\cap(P_b\cap P_c).$$

Поэтому имеем также

$$P_{(a,b,c)}=R_{((a,b),c)}=R_{(a,(b,c))},$$

откуда

$$(a,\ b,\ c)=((a,\ b),\ c)=(a,\ (b,\ c)).$$

Так, например,

$$(88,\ 24,\ 132)=\begin{cases}((88,\ 24),\ 132)=(8,\ 132)=4;\\(88,\ (24,\ 132))=(88,\ 12)=4.\end{cases}$$

9. В заключение отметим следующие следствия свойств пересечения множеств:

$$A\cap A=A\Longrightarrow (a,\ a)=a;$$
$$A\cap B=B\cap A\Longrightarrow (a,\ b)=(b,\ a),$$

которые и сами по себе вполне очевидны.

Таким образом, действие нахождения НОД обладает (так же, как и пересечение множеств) свойствами идемпотентности, коммутативности и ассоциативности.

V. Введенный аппарат можно также использовать для изучения общих и наименьших общих кратных данных чисел.

1. Пусть даны разложения чисел a и b на простые множители.

Как нам известно, c кратно a (т. е. c делится на a) тогда и только тогда, когда $P_c\supset P_a$, аналогично $c|b \Longleftrightarrow P_c\supset P_b$. Таким образом, общим кратным чисел a и b может быть только

такое число c, множество простых сомножителей которого содержит объединение множеств P_a и P_b, так что

$$P_c\supset P_a\cup P_b.$$

Для чисел $a=120=2^3\cdot 3\cdot 5$ и $b=126=2\cdot 3^2\cdot 7$ имеем, например,

$$P_a=\left\{\begin{matrix}2, & 3, & 5\\ (3) & & \end{matrix}\right\};\quad P_b=\left\{\begin{matrix}2, & 3, & 7\\ & (2) & \end{matrix}\right\};$$

$$P_a\cup P_b=\left\{\begin{matrix}2, & 3, & 5, & 7\\ (3) & (2) & & \end{matrix}\right\},$$

поэтому для любого ОК c чисел a и b

$$P_c\supset\left\{\begin{matrix}2, & 3, & 5, & 7\\ (3) & (2) & & \end{matrix}\right\}.$$

С другой стороны, множество простых сомножителей НОК a и b, т. е. для $[a, b]$, должно быть наименьшим множеством простых чисел, содержащим P_a и P_b, и должно поэтому совпадать с их объединением, т. е.

$$P_{[a,b]}=P_a\cup P_b$$

Для вышеуказанных a и b имеем

$$[a,\ b]=2^3\cdot 3^2\cdot 5\cdot 7=2520.$$

Итак, для нахождения НОК двух чисел a и b надо перемножить их простые сомножители, встречающиеся хотя бы в одном из них, и взять каждый из этих сомножителей с наибольшим показателем степени, с которым он входит в a или в b.

2. Если одно из данных чисел a делится на другое число b, то a является НОК a и b. Действительно, a делится на каждое из данных чисел, поэтому оно является ОК, но поскольку число, делящееся на a, не может быть меньше a, то a является также НОК.

Формально имеем

$$a|b\Longrightarrow P_a\supset P_b\Longrightarrow$$
$$P_a\cup P_b=P_a\Longrightarrow P_{[a,b]}=P_a\Longrightarrow [a,\ b]=a.$$

Пример: $[36, 12]=36$.

3. Разделим $[a, b]$ на a и на b.

Для вышеупомянутых значений получаем:

$$\frac{[a,\ b]}{a}=\frac{2^3\cdot 3^2\cdot 5\cdot 7}{2^3\cdot 3\cdot 5}=3\cdot 7;$$

$$\frac{[a,\ b]}{b}=\frac{2^3\cdot 3^2\cdot 5\cdot 7}{2\cdot 3^2\cdot 7}=2\cdot 5;$$

имеем $(3\cdot 7, 2\cdot 5)=1$.

Покажем, что всегда

$$\left(\frac{[a,\ b]}{a},\ \frac{[a,\ b]}{b}\right)=1. \qquad (1)$$

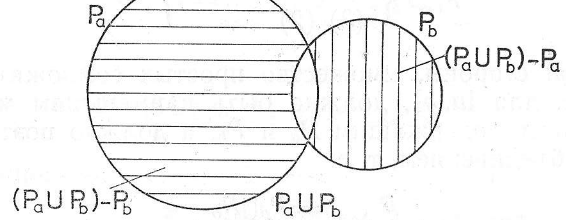

Рис. 9

Рассмотрим для этого соответствующие множества простых множителей (рис. 9)

$$P_{\frac{[a,b]}{a}}=P_{[a,b]}-P_a=(P_a\cup P_b)-P_a;$$

$$P_{\frac{[a,b]}{b}}=P_{[a,b]}-P_b=(P_a\cup P_b)-P_b.$$

Но

$$[(P_a\cup P_b)-P_a]\cap[(P_a\cup P_b)-P_b]=\varnothing,$$

поэтому справедливо (1).

4. Между $[a, b]$ и (a, b) существует важная связь. Чтобы легче ее разглядеть, воспользуемся в разложениях чисел a и b нулевыми показателями; это дает нам возможность утверждать, что данные числа содержат одинаковые простые множители.

Пример:

Числа	Их разложения на одни и те же простые множители			
a	2^3	3^1	5^1	7^0
b	2^1	3^2	5^0	7^1
$[a, b]$	2^3	3^2	5^1	7^1
(a, b)	2^1	3^1	5^0	7^0
ab	2^4	3^3	5^1	7^1

Рассматривая степени p^α и p^β разложений a и b, замечаем, что не бо́льшая всегда входит в (a, b), а не меньшая — в $[a, b]$, между тем $p^{\alpha+\beta}$ всегда принадлежит ab. Поэтому имеем соотношение

$$ab=[a,\ b]\,(a,\ b).$$

К этому результату приводит нас также рассмотрение соответствующих множеств простых сомножителей.

С одной стороны,

$$P_{ab}=P_a+P_b,$$

поэтому следует общую часть областей P_a и P_b (если P_a и P_b представлены пересекающимися) считать дважды (рис. 10).

С другой стороны,

$$P_{[a,b]}=P_a\cup P_b; \qquad P_{(a,b)}=P_a\cap P_b,$$

так что

$$P_{[a,b]\cdot(a,b)}=(P_a\cup P_b)+(P_a\cap P_b),$$

но и это означает, что общая часть P_a и P_b в их объединении следует учитывать дважды.

Таким образом,

$$P_{ab}=P_{[a,b]\cdot(a,b)}\ ,$$

откуда $ab=[a, b]\cdot(a, b)$.

Из этого свойства следует:

1) $[a,\ b]=\dfrac{ab}{(a,\ b)}$;

2) В случае, когда $(a, b)=1$, $[a, b]=ab$.

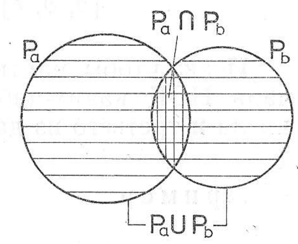

Рис. 10

Пример. $a=120$, $b=126$, $(a, b)=6 \Longrightarrow [a, b]=\frac{120\cdot 126}{6}=2520.$

5. Из предыдущего свойства следует, что при умножении данных чисел a и b на одно и то же натуральное число m их НОК увеличивается в m раз.

В самом деле, пусть $(a, b)=d$, так что $(am, bm)=dm$. Тогда

$$[am, bm]=\frac{abm^2}{dm}=\frac{abm}{d}=[a,b]\cdot m.$$

6. Наоборот, если $a|m$, $a|n$ и $(m, n)=1$, то $a|m\cdot n$.

В самом деле, по условию a является ОК m и n, поэтому $a|[m, n]$. Но в данном случае $[m, n]=mn$, поэтому $a|mn$.

Пример.

Если число делится на 2 и на 3, то оно делится на 6.

7. Чтобы найти $[a, b, c]$ — НОК трех (и более) данных натуральных чисел a, b и c, заметим, что так же, как и для двух чисел, должно быть

$$P_{[a,b,c]}=P_a\cup P_b\cup P_c.$$

Но по самому определению — объединение множеств ассоциативно, т. е.

$$P_a\cup P_b\cup P_c=(P_a\cup P_b)\cup P_c=P_a\cup(P_b\cup P_c).$$

Поэтому имеем также

$$P_{[a,b,c]}=P_{[[a,b],c]}=P_{[a,[b,c]]},$$

откуда следует

$$[a, b, c]=[[a, b], c]=[a, [b,c]].$$

Итак, чтобы найти НОК трех данных чисел, находим сначала НОК каких-нибудь двух из них, затем — полученного числа и третьего из данных.

Пример.

$$[24, 16, 15]=\begin{cases} [[24, 16], 15]=[48, 15]=240; \\ [24, [16, 15]]=[24, 240]=240. \end{cases}$$

Отметим также, что из свойств объединения множеств вытекают следующие следствия:

$$A\cup A=A \Longrightarrow [a, a]=a;$$

$$A\cup B=B\cup A \Longrightarrow [a, b]=[b, a].$$

Таким образом, действие нахождения НОК обладает (так же как и объединение множеств) свойствами идемпотентности, коммутативности и ассоциативности.

VI. В рамках данного изложения следует в заключение вернуться к соотношению (I) и показать, что и наоборот:

$$(\forall p,\ a|p \Longrightarrow p\in P_a) \Longrightarrow \text{Т. Е.} \qquad (11)$$

Поэтому интересно доказать, что $a|p \Longrightarrow p\in P_a$. Это можно сделать различными способами: исходя из алгоритма Евклида, при помощи теоремы Безу или следуя идеям Э. Цермело.

ЛИТЕРАТУРА

1. Математика. V класс. Учебное пособие под редакцией А. И. Маркушевича. М., «Просвещение», 1971. 239 с.

2. *K. H. W* sprawie N W W i N W P — «Matematyka», 1965, rok XVIII, № 1 (85), s. 46—48.