ТЕОРЕМА 1. (Основная теорема арифметики) Для каждого натурального числа n>1 существует и единственно (с точностью до порядка сомножителей) его представление в виде $n=p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$, где p_1,\ldots,p_k — различные простые. Такое представление называется каноническим разложением n на простые множители.

Задача 1. (*Существование*) Докажите что для каждого натурального числа n > 1 найдутся такие простые числа p_1, \ldots, p_k , что $n = p_1 \cdot \ldots \cdot p_k$.

Задача 2. (Единственность: доказательство «от противного») Предположим, что n — минимальное натуральное число, большее 1, у которого есть два различных разложения в произведение простых: $n=p_1\cdot\ldots\cdot p_k$ и $n=q_1\cdot\ldots\cdot q_s$, где $p_1\leqslant\ldots\leqslant p_k,\,q_1\leqslant\ldots\leqslant q_s$ — простые числа. Докажите, что

- a) $n \geqslant p_1^2, n \geqslant q_1^2$; 6) $n > p_1 q_1$;
- в) $p_2 \cdot ... \cdot p_k$ делится на q_1 (Указание: рассмотрите число $n p_1 q_1$);
- г) пункт в) противоречит нашему предположению.

Есть два других доказательства теоремы, опирающиеся на такое свойство простых чисел:

Для любого простого числа p верно следующее утверждение: если m:p, то либо m:p, либо n:p. (*)

Задача 3. Докажите единственность разложения на простые, используя (*).

Задача 4. (Единственность: доказательство, использующее представление (a,b) в виде ax + by)

Пусть a, b — целые числа, причем (a, b) = 1. Тогда

- а) найдется такое целое x, что $ax \equiv 1 \pmod{b}$; б) если $ca \equiv 0 \pmod{b}$, где c целое, то $c \equiv 0 \pmod{b}$.
- в) Из пункта б) выведите свойство (*).

Определение 1. Назовём udeanom в множестве целых чисел $\mathbb Z$ любое подмножество I с такими свойствами:

- 1) если $i \in I$ и $j \in I$, то и $i + j \in I$ (сумма любых двух чисел из идеала также принадлежит этому идеалу);
- 2) если $i \in I$, $n \in \mathbb{Z}$, то $ni \in I$ (умножая число из идеала на *любое целое*, мы получаем число из этого идеала).

Задача 5. Верно ли, что разность любых двух чисел из идеала также принадлежит этому идеалу?

Задача 6. Какие из следующих множеств являются идеалами в \mathbb{Z} : а) \mathbb{Z} ; б) \mathbb{N} ; в) множество чётных целых чисел; г) множество нечётных целых чисел; д) $\{0\}$ (нулевой идеал); е) множество чисел, делящихся на целое число m (обозначение: $m\mathbb{Z}$); ж) сумма идеалов I_1 и I_2 — множество всевозможных сумм вида x_1+x_2 , где $x_1 \in I_1$, $x_2 \in I_2$; з) пересечение идеалов I_1 и I_2 — множество $\{x \mid x \in I_1, x \in I_2\}$.

Задача 7. (*Теорема об идеалах в* \mathbb{Z}) Пусть r — наименьшее положительное число, принадлежащее ненулевому идеалу I (оно называется *порожедающим элементом* идеала I). Докажите, что

а) любое число из I делится на r; б) I состоит из всех целых чисел, делящихся на r.

Задача 8. (Единственность: доказательство с идеалами) Пусть m и n — ненулевые целые числа, $mn \mid p$ и (m,p)=1. Рассмотрим множество J всех таких целых чисел j, что $mj \mid p$. Докажите, что **a)** J — идеал; **b)** $1 \notin J$; $p \in J$;

в) наименьшее положительное число в J равно p; \mathbf{r}) $n \mid p$, откуда следует свойство (*).

Задача 9. Числа a, b, c, n натуральные, $(a, b) = 1, ab = c^n$. Найдутся ли такие целые x и y, что $a = x^n, b = y^n$?

Задача 10. Решите в натуральных числах уравнение $x^{42} = y^{55}$.

Задача 11. Найдите каноническое разложение числа **а)** 2014; **б)** 1002001; **в)** 17!.

Определение 2. *Наименьшим общим кратным* ненулевых целых чисел a и b называется наименьшее натуральное число, которое делится на a и на b. Обозначение: [a,b] или HOK(a,b).

Задача 12. а) Как, зная канонические разложения чисел a и b, найти (a,b) и [a,b]? б) Найдите [192,270]. в) Докажите, что $ab = (a,b) \cdot [a,b]$. г) Верно ли, что числа [a,b]/a и [a,b]/b взаимно просты?

Задача 13. Докажите, что любое общее кратное целых чисел a и b делится на [a,b].

Задача 14. Про натуральные числа a и b известно, что (a,b)=15, [a,b]=840. Найдите a и b.

Определение 3. Пусть a_1, \ldots, a_k — натуральные. Назовём их наибольшим общим делителем порождающий элемент идеала $a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}$, наименьшим общим кратным — порождающий элемент идеала $a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z}$.

Задача 15. Докажите, что для положительных чисел a_1, \ldots, a_k

- a) наибольший общий делитель d является наибольшим числом, которое делит данные числа;
- б) наибольший общий делитель делится на все остальные общие делители;
- в) найдутся такие целые числа $x_1, ..., x_k$, что $d = a_1 x_1 + ... + a_k x_k$;
- г) наименьшее общее кратное является наименьшим натуральным числом, которое делится на данные числа;
- д) наименьшее общее кратное делит остальные общие кратные данных чисел.

1	8	2 a	2 б	2 B	2 Г	3	4 a	4 б	4 B	5	6 a	6 6	_	6 г	-		7 a	8 a	8 6	8 B	8 Г	9	10	11 a	11 б	11 B	12 a	12 б	12 B	12 Г	13	14	15 a	15 б	15 B	15 г	15 д