Математики — люди ленивые и не любят много раз доказывать один и тот же факт в разных случаях. Поэтому встретив что-то полезное, они стремятся доказать его в максимальной общности, чтобы одним махом объять как можно больше случаев. Для этого иногда приходится анализировать множество примеров, когда факт «работает», искать общее в них и откидывать несущественное. В данном листке мы будем заниматься теорией делимости в евклидовых кольцах. Наиболее известными примерами евклидовых колец являются целые числа и многочлены от одной переменной. Есть и другие примеры. Если говорить коротко, то евклидово кольцо — это произвольное множество «чисел», которые можно складывать, умножать и делить с остатком. Впрочем, тут есть тонкости, о которых будет речь ниже.

Определение 1. «Число» x называется *обратимым,* если найдётся такое число y, что $xy = 1$.

Задача 1. Найдите все обратимые числа в кольцах
а) целых чисел; **б)** рациональных чисел; **в)** многочленов вещественной переменной.

Определение 2. Необратимое «число» p называется *простым,* если оно не может быть представлено в виде $p = ab$, где a и b — необратимые элементы.

Основной целью листка является доказательство достаточно общей теоремы:

Теорема 1. (Основная теорема арифметики) *В евклидовом кольце любой необратимый ненулевой элемент может быть разложен на простые множители, причём это разложение единственно с точностью до перестановки множителей и умножения их на обратимые элементы.*

Оказывается, бывают такие «числа», что в них разложение на простые множители совсем не единственно, а в особенно клинических случаях некоторые ненулевые необратимые элементы вообще не могут быть разложены на простые множители.

Приведём пример «чисел», в которых разложение на простые не единственно. Для этого рассмотрим всевозможные выражения вида $\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Такие числа обозначаются через $\mathbb{Z}[i\sqrt{5}]$. Их можно складывать (покомпонентно) и умножать (при этом $\sqrt{-5} \cdot \sqrt{-5} = -5$). Оказывается, число 6 в них имеет два разложения: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Можно показать (упражнение), что каждое из чисел 2, 3, $1 + \sqrt{-5}$ и $1 - \sqrt{-5}$ является простым. Кроме того, число 6 делится и на 2, и на $1 + \sqrt{-5}$, но совершенно не делится на $2 + 2\sqrt{-5}$ (упражнение). На этой прискорбной ноте начнём разбираться с тем, что же такое евклидово кольцо, и почему там такого не бывает.

Определение 3. *Кольцом*[1] называется множество K с операциями сложения и умножения, обладающими следующими свойствами:

1. $a + b = b + a$ для любых $a, b \in K$ (*коммутативность сложения*);
2. $a + (b + c) = (a + b) + c$ для любых $a, b, c \in K$ (*ассоциативность сложения*);
3. в K существует такой элемент 0 (*нуль*), что $a + 0 = a$ для любого $a \in K$;
4. для всех $a \in K$ существует такой элемент $-a \in K$, что $a + (-a) = 0$ (*противоположный*);
5. $a(b + c) = ab + ac$ для любых $a, b, c \in K$ (*дистрибутивность*);
6. $ab = ba$ для любых $a, b \in K$ (*коммутативность умножения*);
7. $a(bc) = (ab)c$ для любых $a, b, c \in K$ (*ассоциативность умножения*);
8. в K существует такой элемент 1 (*единица*), что $a \cdot 1 = a$ для любого $a \in K$;

Оказывается, мы уже много раз встречались с кольцами. Например, числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ являются коммутативными ассоциативными кольцами с единицей относительно обычных операций сложения и умножения. Множество $2\mathbb{Z}$ чётных целых чисел тоже является кольцом, однако уже без единицы. Множество многочленов, множество всех функций на числовой прямой, множество функций на любом подмножестве прямой тоже являются кольцами относительно обычных операций сложения и умножения функций. Кольца могут быть конечными, например множество остатков по модулю n также является кольцом.

Задача 2. **а)** Докажите, что в любом кольце нуль и единица единственны;
б) Докажите, что если в кольце хотя бы два элемента, то $0 \neq 1$;

Определение 4. Говорят, что элемент a кольца K *делится* на элемент $b \in K$ (или что b *делит* a), если существует такой элемент $q \in K$, что $a = qb$.

Задача 3. Докажите, что $a \,\vdots\, b$ и $b \,\vdots\, a$ одновременно тогда и только тогда, когда $a = bc$, где элемент c обратим. Элементы a и b в этом случае называют *ассоциированными.*

Определение 5. Ненулевой элемент a кольца K называется *делителем нуля,* если найдётся такой ненулевой элемент $b \in K$, что $ab = 0$.

Задача 4. Докажите, что в кольце без делителей нуля возможно сокращение: из того, что $ac = bc$ и $c \neq 0$, следует, что $a = b$.

Задача 5. Приведите пример кольца с делителями нуля.

[1] Если быть точным, то кольцо должно обладать только первыми пятью свойствами. В данном листке мы рассматриваем только коммутативные ассоциативные кольца с единицей.

Задача 6. Рассмотрим кольцо функций на множестве X. В каких случаях в нём есть делители нуля?

Определение 6. Функция $N : K \setminus \{0\} \to \mathbb{Z}_+$, которая каждому ненулевому элементу кольца ставит в соответствие неотрицательное число, называется *нормой,* если

1. $N(ab) = N(a)$, если b обратим, и $N(ab) > N(a)$ иначе;
2. для любых $a, b \in K$, где $b \neq 0$ существуют такие $q, r \in K$, что $a = bq + r$ и либо $r = 0$, либо $N(r) < N(b)$. То есть в кольце возможно деление с остатком. Его единственности не требуется.

Задача 7. **а)** Докажите, что модуль целого числа определяет норму на целых числах;
б) Докажите, что степень многочлена определяет норму на многочленах от одной переменной;

Определение 7. Кольцо без делителей нуля, для которого существует норма, называется *евклидовым.*

Соглашение 1. Далее говоря «число» мы имеем в виду элементы некоторого евклидового кольца K.

Определение 8. Если число d делит числа a и b, то d называется *общим делителем* чисел a и b. Любой из общих делителей чисел a и b с наибольшей нормой называется *наибольшим общим делителем* a и b (обозначение: (a, b)). В том случае, когда $(a, b) = 1$, говорят, что числа a и b *взаимно простые.*

Соглашение 2. Пусть a и b — два фиксированных числа. В данном листке через I будем обозначать множество всех чисел, представимых в виде $ax + by$ (где x и y — любые числа).

Задача 11°. (*о сумме идеалов*) Пусть d — число с наименьшей нормой в I. Докажите, что
а) каждое число из I делится на любой общий делитель чисел a и b (а значит, и на (a, b));
б) каждое число из I делится на d;
в) $d = (a, b)$;
г) число $d = (a, b)$ является числом с наименьшей нормой, делящимся на любой общий делитель a и b.

Задача 12°. (*Алгоритм Евклида*) Пусть a и b — два фиксированных числа. Будем последовательно заменять число с большей нормой на остаток от деления на число с меньшей. Докажите, что:
а) все числа, которые мы будем получать, лежат в множестве I;
б) в некоторый момент мы получим пару $(d, 0)$, $d \neq 0$;
в) d является наибольшим общим делителем a и b;
г) Как именно для данных чисел a и b при помощи алгоритма Евклида искать такие числа x и y, что $ax + by = (a, b)$?

Задача 13. **а)** Докажите, что для любого числа k выполнено $(ka, kb) = k \cdot (a, b)$.
б) Докажите, что если m — общий делитель чисел a и b, то $(a/m, b/m) = (a, b)/m$.

Задача 14. Докажите, что числа a и b взаимно просты тогда и только тогда, когда существуют такие числа x и y, что $ax + by = 1$.

Задача 15. Даны числа a, b и c, причём $(a, b) = 1$. Докажите, что
а) если $ac \vdots b$, то $c \vdots b$; **б)** если $c \vdots a$ и $c \vdots b$, то $c \vdots ab$.

Задача 16°. (*Основная теорема арифметики*) Докажите следующие утверждения:
а) для каждого необратимого ненулевого числа n найдутся такие простые числа $p_1, \ldots, p_k$, что $n = p_1 \cdot \cdots \cdot p_k$;
б) (*каноническое разложение*) Для каждого необратимого ненулевого числа n найдутся такие различные простые $p_1, \ldots, p_k$ и натуральные $\alpha_1, \ldots, \alpha_k$, что $n = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$;
в) разложения из пунктов а) и б) единственны с точностью до порядка сомножителей и домножения на обратимые элементы.

Задача 17. Даны числа $a, b, c \in K$, $n \in \mathbb{N}$, $(a, b) = 1$, $ab = c^n$. Найдётся ли такое число x, что $a = x^n$?

Задача 18. Решите уравнение $x^{42} = y^{55}$.

Задача 19. Найдите каноническое разложение целого числа **а)** 2013, **б)** 1002001, **в)** 17!, **г)** C_{20}^{10}.

Определение 9. *Общим кратным* ненулевых чисел a и b называется ненулевое число, которое делится как на a, так и на b. Любое общее кратное с наименьшей нормой называется *наименьшим общим кратным* чисел a и b. Обозначение: $[a, b]$.

Задача 20°. Пусть $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$, причём α_i, $\beta_i \geqslant 0$.
а) Найдите (a, b) и $[a, b]$. **б)** Докажите, что $ab = (a, b) \cdot [a, b]$.

Задача 21°. Докажите, что любое общее кратное чисел a и b делится на $[a, b]$.

Задача 22. Верно ли, что **а)** $[ca, cb] = c \cdot [a, b]$, если ненулевое число c необратимо; **б)** числа $[a, b]/a$ и $[a, b]/b$ взаимно просты?

Задача 23. Про натуральные числа a и b известно, что $(a, b) = 15$, $[a, b] = 840$. Найдите a и b.

1 а	1 б	1 в	2 а	2 б	3	4	5	6	7 а	7 б	11 а	11 б	11 в	11 г	12 а	12 б	12 в	12 г	13 а	13 б	14	15 а	15 б	16 а	16 б	16 в	17	18	19 а	19 б	19 в	19 г	20 а	20 б	21	22 а	22 б	23