14. Основная теорема арифметики

Основная теорема арифметики. Для каждого целого 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.

Лемма Евклида.[1] Если p простое и $p \mid ab$, то $p \mid a$ или $p \mid b$.

В этом листке мы будем доказывать эти утверждения. Вот примеры вопросов, которые, если задуматься, не так уж очевидны.
1) 71, 73, 89, 101 — простые числа. Вдруг $71 \cdot 101 = 73 \cdot 89$?
2) $96577 = 221 \cdot 437 = 323 \cdot 299$. Вдруг это — два различных разложения на простые множители? Даже если нет, разложим множители в обоих произведениях на простые множители. Обязательно ли таким образом мы получим одно и то же разложения на простые множители?

☐ **1°** Забудем про существование нечётных чисел. *Чётнопростым* будем называть число, которое нельзя представить как произведение двух чётных чисел. Единственно ли разложение чётного числа на чётнопростые множители?

☐ **2°** Попробуйте рассказать принимающему, почему основная теорема арифметики очевидна. Поймите, где возникает проблема.

3 ☐ **а)°** Выведите из леммы Евклида основную теорему арифметики,
☐ **б)°** Выведите из основной теоремы арифметики лемму Евклида.

☐ **4°** Составьте таблицы сложения и умножения остатков по модулям 5 и 6. В чем принципиальная разница между полученными таблицами умножения? Откуда она взялась?

☐ **5** Какие длины можно отложить на прямой от данной точки, имея шаблоны 6 см и 15 см?

☐ **6** Синим на числовой оси отметили числа, дающие при делении на 24 остаток 17, белым — дающие при делении на 40 остаток 7. Найдите наименьшее расстояние между белой и синей точками.

Определение 1. *Наибольший общий делитель* (a, b) целых чисел a и b — это наибольшее целое число, делящее и a, и b. Обозначение: (a, b). Если $(a, b) = 1$, то a и b называют *взаимно простыми*.

☐ **7°** Докажите, что (a, b) существует и единственен, если a и b не равны одновременно 0.

☐ **8°** Докажите, что $(a, b) = (a - b, b) = (r, b)$, где r — остаток от деления a на b.

9 Найдите возможные значения:
☐ **а)** $(n, 12)$; ☐ **б)** $(n, n+1)$; ☐ **в)** $(2n+3, 7n+6)$; ☐ **г)** $(n^2, n+1)$.

Ниже мы докажем лемму Евклида и, тем самым, основную теорему арифметики. Здесь предлагается три варианта, как это сделать. Эти пути независимые, по каждому из них можно пройти, не пользуясь результатами другого. Можно начать с любого из них. Обязательно доказать основную теорему арифметики хотя бы одним способом, советуем в итоге разобраться со всеми.

- Можно решить задачу 10, а затем вывести из неё задачи 12–19.
- Можно решить задачу 11, а затем вывести из неё задачи 12–19.
- Можно решить задачу 20, а затем вывести из неё предыдущие задачи.

10 От прямоугольника с целыми сторонами $a \times b$ отрезают квадраты со стороной, равной меньшей стороне прямоугольника, пока это возможно. С оставшимся прямоугольником делают то же, и т. д.
☐ **а)** Сколько и каких квадратов получится, если $a = 324$, $b = 141$?
Докажите, что:
☐ **б)** прямоугольник разрежут на конечное число квадратов;
☐ **в)** сторона d самого маленького квадрата — общий делитель сторон прямоугольника;
☐ **г)** любой общий делитель сторон прямоугольника укладывается в d целое число раз;
☐ **д)** d — наибольший общий делитель сторон прямоугольника.

[1] Это не такое общепризнанное название, как «основная теорема арифметики», но в этом листке оно будет удобно.

11 **а)**° *(Алгоритм Евклида)* Даны два натуральных числа a и b. С ними проделывают такую операцию: наибольшее число заменяет на модуль разности двух чисел. Её повторяют, пока не получится 0. Докажите, что последнее ненулевое число будет наибольшим общим делителем a и b.

б)° То же самое, но заменяют на остаток от деления большего числа на меньшее.

12° Кузнечик прыгает по целым точкам числовой прямой. Он начинает в нуле и умеет прыгать на m и на n. Обозначим множество точек, куда он может допрыгать, через I. Докажите, что

а) если $a \in I$, то $ka \in I$;

б) если $a, b \in I$, то $a - b \in I$.

в) Пусть d — минимальное положительное число в I. Докажите, что $I = \{dk \mid k \in \mathbb{Z}\}$.

г) Докажите, что d — общий делитель n и m.

д) Докажите, что $(m, n) \mid d$.

е) Докажите, что d — наибольший общий делитель m и n. *Подсказка. Тобшбмб еплбзйуё, шуп ОПЕ нёоэщё ймй сбгёо d, б рпупн — шуп впмэщё.*

13° Докажите, что для любых целых a и b найдутся целые x и y такие, что $ax+by = (a, b)$.

14° Докажите, что уравнение $ax+by = c$ (*линейное диофантово уравнение*) имеет решение относительно x и y тогда и только тогда, когда $(a, b) \mid c$.

15° Докажите, что сравнение $mx \equiv 1 \pmod{n}$ имеет решение относительно x тогда и только тогда, когда m и n взаимно просты.

16° У ненулевого остатка по простому модулю есть обратный по умножению. Что это значит? Почему это верно?

17° Пункты этой задачи можно решать в любом порядке (и вывести из одного другой).

а) Докажите, что нули в таблице умножения по простому модулю встречаются только в нулевом столбце и нулевой строке. (Нумерация строк и столбцов начинается с нуля.)

б) Докажите, что в таблице умножения по простому модулю в любой ненулевой строке встречаются все остатки, причём по одному разу.

18° Докажите для простого p: если $a \not\equiv 0 \pmod{p}$ и $b \not\equiv 0 \pmod{p}$, то $ab \not\equiv 0 \pmod{p}$.

19 **а)**° Докажите лемму Евклида.

б)° Докажите основную теорему арифметики.

20 Эта задача — ещё один способ сформулировать доказательство леммы Евклида. Попробуйте решить её, не используя задачи 10–19.

а) Пусть в строке таблицы умножения по простому модулю есть два нуля на расстоянии $x > 1$. Докажите, что в ней есть два нуля на большем расстоянии.

б) Докажите, что нули в таблице умножения по простому модулю встречаются только в первом столбце и первой строке.

в) Выведите отсюда 17, лемму Евклида, основную теорему арифметики, другие задачи.

21° Докажите, что если $c \mid ab$ и $(a, c) = 1$, то $c \mid b$.

22° Докажите, что следующие утверждения эквивалентны:

1. числа n и a взаимно просты;
2. найдётся x такой, что $ax \equiv 1 \pmod{n}$;
3. если $ax \equiv 0 \pmod{n}$, то $x \equiv 0 \pmod{n}$;
4. если $ax \equiv ay \pmod{n}$, то $x \equiv y \pmod{n}$.

23 Найдите все решения линейного диофантова уравнения с двумя переменными.

24 Рассмотрим множество чисел $M = \{a + b\sqrt{-5} \text{ для } a, b \in \mathbb{Z}\}$. Определим сложение и умножение:
$(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5}$,
$(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}$.
Простым назовём число из M, которое нельзя представить как произведение двух чисел из M, отличных от ± 1. Простое ли число **а)** 5; **б)** 2?

в) Разложите 6 на простые множители двумя способами (отличающиеся только знаками способы считаем одинаковыми).

г***)** Единственно ли разложение на простые множители в числах вида $a + b\sqrt{-1}, a, b \in \mathbb{Z}$ (*гауссовых целых числах*)?