Арифметика II: Алгоритм Евклида и его следствия

Соглашение. Все числа в этом листке предполагаются целыми.

▷ **Определение 1.** Пусть a и b — целые числа. Наибольший элемент множества $\{x \in \mathbb{Z} : x \mid a, x \mid b\}$ называется *наибольшим общим делителем*, а наименьший положительный элемент множества $\{x \in \mathbb{Z} : a \mid x, b \mid x\}$ — *наименьшим общим кратным* чисел a и b.

Задача 1. Найдите а) НОД$(n, n+1)$; б) НОД$(n, n+2)$; в) НОД$(n+1, n^2)$.

Задача 2 (алгоритм Евклида). а) НОД не меняется при замене пары (a, b) на пару $(a, b+ka)$ (для любого целого числа k).
б) Последовательностью преобразований вида $(a, b) \mapsto (a, b+ka)$ и $(a, b) \mapsto (b, a)$ любую пару целых чисел можно перевести в пару вида $(c, 0)$.
в) Сформулируйте алгоритм нахождения наибольшего общего делителя двух чисел.

Задача 3. а) Чему может быть равен НОД$(x+y, x-y)$, если НОД$(x, y) = 1$?
б*) Как может измениться НОД при замене пары (x, y) на пару $(ax+by, cx+dy)$?

Задача 4. Найдите а) НОД$(6188, 4709)$; б) НОД$(1597, 2584)$;
в) НОД$([n], [m])$; г) НОД$(x^n - 1, x^m - 1)$.

Задача 5*. а) Для какого наименьшего целого числа a существует такое целое число b $(0 < b < a)$, что алгоритм Евклида для них не завершается за $n-1$ шаг?
б*) Оцените время работы алгоритма Евклида для чисел a и b.

Задача 6. От прямоугольника $a \times b$ $(a < b)$ отрезают квадрат со стороной a. С оставшимся прямоугольником операцию повторяют и т. д. На какие квадраты будет в результате таких действий порезан прямоугольник 6188×4709?

Задача 7. а) Множество $(a) + (b) := \{ak + bl : k, l \in \mathbb{Z}\}$ равно множеству (c) для некоторого целого числа c. б) Чему равно это c?

Задача 8. Какие суммы можно заплатить, используя монеты по a и b рублей (возможно со сдачей)?

▷ **Определение 2.** Два числа называются *взаимно простыми*, если их НОД равен 1.

Задача 9. Если числа a и b взаимно просты, то "a обратимо по модулю b": существует такое целое число a', что $aa' - 1$ кратно b.

Задача 10. а) Решите уравнение $ax + by = 0$.
б) Пусть (x_0, y_0) — одно решение уравнения $ax + by = c$. Опишите все его решения.

Задача 11. Решите уравнения
а) $7x + 11y = 1$; б) $1023x + 15y = 2010$; в) $1023x + 15y = 11$.

Задача 12. а) Если ab делится на простое число p, то либо a делится на p, либо b делится на p.
б) Разложение целого числа на простые множители единственно (с точностью до перестановки сомножителей и смен знаков).

▷ **Определение 3.** Степень, в которой простое число p входит в разложение на простые множители числа a называется *p-показателем* числа a. Обозначение: $\mathrm{ord}_p(a)$.

Задача 13. а) $\operatorname{ord}_p(ab) = \operatorname{ord}_p(a) + \operatorname{ord}_p(b)$; б) $a \mid b \iff \forall p\ \operatorname{ord}_p(a) \leqslant \operatorname{ord}_p(b)$.

Задача 14. а) $\operatorname{ord}_p(n!) = \sum\limits_{\alpha \geqslant 1} \left\lfloor \dfrac{n}{p^\alpha} \right\rfloor$ (где $\lfloor a/b \rfloor$ — неполное частное при делении a на b); выясните, на сколько нулей оканчивается десятичная запись числа $10^4!$.
б*) Найдите формулу для $\operatorname{ord}_p \binom{n}{k}$; проверьте, что получается неотрицательное число.
в*) Если число p простое, то все числа в p^n-й строке треугольника Паскаля, кроме первого и последнего, делятся на p.

Задача 15. а) $ab = \text{НОД}(a, b) \cdot \text{НОК}(a, b)$; б*) сформулируйте и докажите обобщение последнего утверждения для трех сомножителей.

Задача 16. Решите в целых числах уравнения а) $(x - 7)(x - 11) = 2^n$; б*) $x^2 - 1 = y^3$.

Задача 17. а) Опишите все пифагоровы тройки: решите в целых числах уравнение $a^2 + b^2 = c^2$. (Указание: докажите, что $a + c$ — либо полный квадрат, либо удвоенный полный квадрат.)
б*) Решите уравнение $x^4 + y^4 = z^4$.
в*) Решите уравнение $x^3 + y^3 = z^3$.