МАТЕМАТИКА

Вавилов В.В.

Многоликий алгоритм Евклида

Школа им. А.Н. Колмогорова
СУНЦ МГУ
2015

Вавилов В.В.

Многоликий алгоритм Евклида. –М.: Школа им. А.Н. Колмогорова СУНЦ МГУ, 2012. – 42с.

Книга представляет собой сборник задач, которые в разные годы использовались на занятиях по алгебре, в работе специальных курсов в школе им. А.Н. Колмогорова Специализированного учебно-научного центра (факультета) МГУ им. М.В. Ломоносова, при подготовке олимпиад и конкурсов различных уровней. Все задачи, так или иначе, связаны с понятием наибольшего общего делителя двух целых чисел и с алгоритмом Евклида.

Ко всем задачам даны их полные решения и некоторые из них довольно трудны. В приведенных решениях, и в комментариях к ним, содержатся точные литературные источники задач или указаны их авторы.

Критические замечания и предложения будут встречены с большой благодарностью.

Теоретические сведения

Для нахождения *наибольшего общего делителя* двух натуральных чисел a и b, $a>b$, часто применяют алгоритм Евклида, который состоит в последовательных делениях целых чисел, определенных следующей системой неравенств:

$$\begin{aligned}
a &= bq_1 + r_1, \quad \text{где} \quad 0 < r_1 < b,\\
b &= r_1q_2 + r_2, \quad \text{где} \quad 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, \quad \text{где} \quad 0 < r_3 < r_2,\\
&\dots\dots\dots\dots\dots\dots\\
r_{n-2} &= r_{n-1}q_n + r_n, \quad \text{где} \quad 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1} + r_{n+1}, \quad \text{где} \quad r_{n+1} = 0.
\end{aligned} \tag{1}$$

Теорема (Евклид). *Для любых натуральных чисел a и b, $a > b$, имеет место соотношение*

$$r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = \ldots = (r_2, r_1) = (r, b) = (a, b),$$

где r_n – последний отличный от нуля остаток в системе (1).

Кроме алгоритма Евклида в приведенной форме для нахождения (a, b) используется его эквивалентная форма, в основе которой лежат следующие равенства

$$(a, b) = (a - b, a) = (a + b, b), \tag{2}$$

которые являются следствием того, что любой общий делитель чисел a и b является общим делителем чисел $a \pm b$ и a и, наоборот, любой общий делитель чисел $a \pm b$ и a является делителем чисел a и b.

Для нахождения наибольшего общего делителя (a, b) используют также основную теорему арифметики о единственности разложения натурального числа на простые множители: если

$$a = \prod_k p_k^{\alpha_k}, \quad b = \prod_k p_k^{\beta_k}, \tag{3}$$

где $p_1, p_2, \ldots$ - упорядоченные по величине простые числа, а $\alpha_1, \alpha_2, \ldots$ и $\beta_1, \beta_2 \ldots$ – целые неотрицательные числа (некоторые из них могут быть нулями), то

$$(a, b) = \prod_k p_k^{\min(\alpha_k, \beta_k)} \tag{4}$$

Наименьшее общее кратное $[a, b]$ двух натуральных чисел вычисляется по формуле

$$[a, b] = \frac{ab}{(a,b)}. \tag{5}$$

Из (3), (4), (5) и очевидного, при любом k, равенства $\alpha_k + \beta_k = \max(\alpha_k\beta_k) + \min(\alpha_k\beta_k)$ замечаем, что

$$[a, b] = \prod_k p_k^{\max(\alpha_k, \beta_k)} \tag{6}$$

и, тем самым, наименьшее общее кратное $[a, b]$ является наименьшим из всех общих кратных чисел a и b.

Рекуррентные формулы

$$(a_1, a_2, \dots, a_{n-1}, a_n) = ((a_1, a_2, \dots, a_{n-1}), a_n),$$
$$[a_1, a_2, \dots, a_{n-1}, a_n] = [\,[a_1, a_2, \dots, a_{n-1}], a_n]$$

позволяют вычислить НОД и НОК нескольких чисел и свести эти вычисления к последовательному нахождению НОД и НОК двух чисел.

Процедура, известная как алгоритм Евклида, возникла не позднее III-го века до нашей эры (см. [1]) и встречается в седьмой книге Евклида (и, видимо, имеет более раннее происхождение). Предназначен был этот алгоритм для решения задачи о соизмеримости двух отрезков. Общей мерой отрезков с длинами a и b называется такой отрезок длины d, который можно уложить без остатка, как в первом отрезке, так и во втором; ясно, что $d = (a, b)$ – является одним из возможных решений (и единственным, если требуется найти наибольшую меру).

Алгоритм Евклида для двух натуральных чисел имеет еще одну интересную геометрическую интерпретацию: в прямоугольник размерами $a \times b$ $(a > b)$ укладываем q_1 квадратов (см. (1)) размерами $b \times b$, плотно прикладывая, их друг к другу и начиная от стороны исходного прямоугольника, затем в оставшийся прямоугольник размерами $b \times r_1$ укладываем q_2 раз аналогичным образом квадраты размерами $r_1 \times r_1$; в оставшийся прямоугольник размерами $r_1 \times r_2$ укладываем q_3 раз квадраты размерами $r_2 \times r_2$ и т.д., пока не покроем весь прямоугольник $a \times b$ квадратами n разных размеров в сумарном количестве $q_1 + q_2 + \dots + q_{n+1}$ штук.

Отметим также, что если имеется прямоугольник $a \times b$, стороны которого проходят по линиям клетчатой бумаги, то на его диагонали находится $(a, b) + 1$ узлов сетки.

Из системы равенств (1) следует (см. задачу 34 ниже), что для данных натуральных чисел a и b существуют такие целые числа x и y, что

$$(a, b) = xa + yb.$$

Это представление наибольшего общего делителя (a, b) позволяет довольно просто найти все решения в целых числах уравнения вида

$$ax + by = c.$$

Теорема. *Для того чтобы уравнение $ax + by = c$ имело решение в целых числах (x, y) необходимо и достаточно, чтобы c делилось на $(a, b) = d$. Если это выполнено и (x_0, y_0) одно из решений этого уравнения, то все его решения задаются формулами*

$$x = x_0 + b_1 t, \quad y = y_0 = a_1 t,$$

где $a_1 = a/d$, $b_1 = b/d$. (Доказательство см., например, в [34]).

ЗАДАЧИ

1. а) Найти

1) $(1517, 2257)$; 2) $(1411, 4641)$;

3) $[187, 533]$; 4) $[374, 1599, 9061]$.

б) Найти все натуральные числа a и b такие, что

1) $\begin{cases}(\mathrm{a}, b) = 24,\\ [a, b] = 2496;\end{cases}$ 2) $\begin{cases}(a, b) = 30,\\ a + b = 50;\end{cases}$

3) $\begin{cases}(a, b) = 20,\\ ab = 8400;\end{cases}$ 4) $\begin{cases}ab = 20,\\ [a, b] = 10.\end{cases}$

2. Доказать, что (n, m – натуральные числа):

1) $(n, n + 1) = 1$; 6) $(10n + 9, n + 1) = 1$;

2) $[n, n + 1] = n(n + 1)$; 7) $(3n + 1, 10n + 3) = 1$;

3) $(2n, 2n + 2) = 2$; 8) $(n, m) = (5n + 3m, 13n + 8m)$;

4) $(2\mathrm{n} + 1, 2\mathrm{n} + 3) = 1$; 9) $(12\mathrm{n} + 1, 30\mathrm{n} + 2) = 1$;

5) $(n, 2n + 1) = 1$; 10) $[2n + 13, n + 7]$;

11) $(n, n + 1, n + 2) = 1$; 12) $(n, m) \le |n - m|$, $n \ne m$.

13) $[n, n + 1, n + 2] = \frac{1}{2} n(n + 1)(n + 2)$ или $n(n + 1)(n + 2)$ в зависимости от четности n;

3. Доказать, что (a, b – натуральные числа)

1) Число (a, bc) делится на (a, b);

2) Если (a, c) делится на (a, b), то $(a, bc) = (a, b)$;

3) $(ac, bc) = c(a, b)$;

4) Если c делится на b, то $(a, b) = (a + c, b)$.

4. Доказать, что

1) $(a, a) = a$, $[a, a] = a$;

2) $(a, b) = (b, a)$, $[a, b] = [b, a]$;

3) $((a, b), c) = (a, (b, c))$, $[[a, b], c] = [a, [b, c]]$;

4) $(a, [a, b]) = a$, $[a, (a, b)] = a$;

5) $abc = (a, b, c) \cdot [ab, bc, ca]$, $abc = (ab, bc, ca)[a, b, c]$.

5. а) Доказать, что если $(a, b) = (c, d) = 1$, то

1) $(ac, bd) = (a, b)(c, d)$; 2) $[ac, bd] = [a, b]\,[c, d]$.

б) Доказать, что для любых натуральных чисел a и b имеем:

1) $((a, b), [a, b]) = 1$, 2) $(ab, [a, b]) = [a, b]$,

3) $(a + b, [a, b]) = (a, b)$.

6. Доказать, что если $(a, b) = 1$, то $(2a + b, a(a + b)) = 1$.

7. Пусть числа m и n взаимно просты. Найти наибольший общий делитель чисел $a = 2mn - m^2$, $b = n^2 - m^2$, $c = m^2 + n^2 - mn$.

8. Доказать, что если a, b, c – нечетные числа, то

$$(a, b, c) = \left(\frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}\right).$$

9. Доказать, что если $a = cq + r$ и $b = cq_1 + r_1$, где a, b, q, q_1, r, r_1 целые неотрицательные числа и c – натуральное число, то

$$(a, b, c) = (c, r, r_1).$$

10. Доказать, что если a и b – положительные целые числа, то число членов конечной арифметической прогрессии

$$a,\ 2a,\ \ldots,\ ba$$

делящихся на b, равно (a, b).

11. Доказать, что если a, b, a_1, b_1 натуральные числа и $a_1/b_1 = a_2/b_2$, то

$$\frac{a_1}{a_2} = \frac{b_1}{b_2} = \frac{[a_1, b_1]}{[a_2, b_2]}$$

12. а) Даны дроби $\frac{8}{15}$ и $\frac{18}{35}$. Найти наибольшее из всех рациональных чисел, при делении на которые каждой из данных дробей получаются целые числа.

б) Даны дроби $\frac{35}{396}$ и $\frac{28}{297}$. Найти наименьшее из всех рациональных положительных чисел, при делении которых на каждую из данных дробей получаются целые числа.

13. Пусть $K(x)$ равно числу несократимых дробей $\frac{a}{b}$ таких, что $a < x$ и $b < x$ (a и b – натуральные числа). Например, $K(5/2) = 3$ (дроби 1; 2; $5/2$). Вычислить сумму

$$K(100) + K\left(\tfrac{100}{2}\right) + K\left(\tfrac{100}{3}\right) + \ldots + K\left(\tfrac{100}{99}\right) + K\left(\tfrac{100}{100}\right).$$

14. Доказать, что ($m, n > 0$ – натуральные числа и $n < m$)

1) $(2^n - 1, 2^m - 1) = 2^{(n,\, m)} - 1$;

2) $(10^n - 1, 10^m - 1) = 10^{(n,\, m)} - 1$;

3) $(a^n - 1, a^m - 1) = a^{(n,\, m)} - 1$, $(a \in \mathbb{N},\ a > 1)$.

4) Используя 2), доказать, что существуют бесконечно много простых чисел.

5) Найти $(\underbrace{22\ldots2}_{m}, \underbrace{88\ldots8}_{n})$.

15. Доказать, что для натуральных чисел m и a имеет место равенство

$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m)$$

16. Пусть m и n – натуральные числа. Доказать, что

1) $(2^{2^m} + 1,\ 2^{2^n} + 1) = 1$;

2) $(a^{2^n}+1,\ a^{2^m}+1)=\begin{cases}1, \text{ если } a \text{ четно;}\\ 2, \text{ если } a \text{ нечетно.}\end{cases}$

3) $a^{2^n}+1 \mid a^{2^m}-1.$

17. Доказать, что

1) $(n,\ 2^{2^n}+1)=1,\ n=1,\ 2,\ \ldots;$

2) существует бесконечно много натуральных чисел n, для которых $(n, 2^n-1)>1$ и найти наименьшее из них.

18. Пусть $d=(a, b)$, $a=a'd,$ $b=b'd$ и n – натуральное число, $n\geq 2$. доказать, что если число b' нечетно, то общий множитель чисел n^a+1 и n^b-1 не может быть меньше 2.

19. Доказать, что

$$(\underbrace{11\ldots1}_{n},\ \underbrace{11\ldots1}_{m}) = \underbrace{11\ldots1}_{(n,\,m)}.$$

20. 1) От прямоугольника 324×144 мм отрезают несколько квадратов со стороной 141 мм, пока не останется прямоугольник, у которого длина одной стороны меньше 141 мм. От полученного прямоугольника отрезают квадраты, стороны которых равны по длине его меньшей стороне, до тех пор пока это возможно, и т.д. Какова длина стороны последнего квадрата?

2) Найти какие-нибудь два числа a и b, чтобы при таком разрезании прямоугольника $a\times b$ получились квадраты разных размеров.

21. Три автомата печатают на карточках пары целых чисел. Каждый автомат, прочитав некоторую карточку, выдает новую карточку; прочитав карточку с парой (m, n), первый автомат выдает карточку $(m-n, n)$, второй– $(m+n, n)$, третий карточку (n, m). Пусть первоначально имеется карточка с парой чисел $(19, 86)$. Можно ли, используя автомат в любом порядке, получить из нее карточку

1) $(31, 13)$; 2) $(12, 21)$?

3) Найти необходимое и достаточное условие того, чтобы из карточки (m, n) можно было получить карточку (a, b).

22. Натуральные числа a и b взаимно просты. Доказать, что наибольший общий делитель чисел $a+b$ и a^2+b^2 равен 1 или 2.

23. Произведение двух чисел равно 600. Какое наибольшее значение может иметь наибольший общий делитель таких чисел?

24. Сумма натуральных чисел $a_1,\ a_2,\ \ldots,\ a_{49}$ равно 999. Какое набольшее значение может принимать их наибольший делитель?

25. Сумма десяти натуральных чисел равна 1001. Какое набольшее значение может принимать их наибольший общий делитель?

26. Доказать, что

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

2) $(a, b)(a, c)(b, c)[a, b][a, c][b, c] = a^2b^2c^2$;

3) $(a, b, c) \cdot [(a, b), (a, c), (b, c)] \cdot [a, b, c] = abc$;

4) $(a, [b, c]) = [(a, b), (a, c)]$;

5) $[a, (b, c)] = ([a, b], [a, c])$;

6) $[(a, b), (a, c), (b, c)] = ([a, b], [a, c], [b, c])$

7) $\dfrac{[a,b,c]^2}{[a,b][b,c][c,a]} = \dfrac{(a,b,c)^2}{(a,b)(b,c)(c,a)}$;

8) $(ab, cd) = (a, c)(b, d)\left(\dfrac{a}{(a,c)}, \dfrac{d}{(b,d)}\right)\left(\dfrac{c}{(a,c)}, \dfrac{b}{(b,d)}\right)$;

9) $a_1a_2\ldots a_n = G_r \cdot L_{n-r}$, где G_r обозначает общий делитель всех произведений чисел a_i, взятых r раз и L_{n-r} обозначает наименьшее общее кратное всех произведений чисел a_i, взятых $n-r$ раз;

10) $[a_1a_2\ldots a_n] =$
$= a_1a_2\ldots a_n(a_1, a_2)^{-1}(a_2, a_3)^{-1}\ldots(a_{n-1}, a_n)^{-1}(a_1, a_2, a_3)\ldots(a_1a_2\ldots a_n)^{\pm 1}$.

27. Доказать, что для натуральных чисел k, m, и n справедливо неравенство

$$[k, m][m, n] \le [k, m, n]^2.$$

28. Даны натуральные числа a и b такие, что число

$$\frac{a+1}{b} + \frac{b+1}{a}$$

является целым. Доказать, что $(a, b) \le \sqrt{a+b}$.

29. Пусть n – натуральное число. Рассмотрим пары натуральных чисел (u, v), наименьшее общее кратное которых совпадает с числом k (если $u \ne v$, то пара (u, v) считается отличной от пары (v, u)). Доказать, что при заданном значении n таких пар существует столько же, сколько положительных делителей у числа n^2.

30. Пусть натуральные числа m и n таковы, что

$$(11k-1, m) = (11k-1, n),\ k = 1, 2, \ldots .$$

Доказать, что $m = 11^l n$ для некоторого целого числа l.

31. Пусть $A(n) = [n, n+1, \ldots, n+k]$, $n \in \mathbb{N}$ и k– заданное натуральное число. Доказать, что существует бесконечно много значений $n \in \mathbb{N}$, удовлетворяющих неравенству $A(n) > A(n+1)$.

32. Для положительных чисел n и k, $1 \le k \le n$, обозначим через $A(n, k)$ наименьшее общее кратное чисел n, $n-1$, …, $n-k+1$, т. е.

$$A(n, k) = [n, n-1, \ldots, n-k+1].$$

а) Доказать, что наибольшее число n, для которого существует целое $k \le n$, такое, что $A(n, 1) < A(n, 2) < \ldots < A(n, k) = A(n, n)$ равно 14.

б) Обозначим через $f(n)$ наибольшее значение k такое, что $A(n, 1) < A(n, 2) < \ldots < A(n, k)$. Доказать, что $f(n) < 3\sqrt{n}$.

в) Доказать, что если $n > k! + k$, то $f(n) > k$ (т. е. $f(n) \to \infty$ при $n \to \infty$).

33. Рассмотрим n натуральных чисел $a_1 < a_2 < \ldots < a_n \leq 2n$ таких, что наименьшее общее кратное любых двух из них больше $2n$. Доказать, что $a_1 < \left[2n/3\right]$.

34. Доказать, что $d = (a, b)$ и $(-d)$ единственные общие делители чисел a и b, которые можно представить в виде линейной комбинации чисел a и b с целыми коэффициентами, т. е. в виде $xa + yb$.

35. Пусть a, b, p – любые целые числа. Доказать, что найдутся такие взаимно простые k и l, что $ak + bl$ делится на p.

36. Представить число nab, где a, b, n – натуральные числа и $(a, b) = 1$ в виде $ax + by$, где x, y также натуральные числа.

37. Даны два натуральных взаимно простых числа p и q. Целое число n называется хорошим, если его можно представить в виде $n = px + qy$, где x и y – целые неотрицательные числа, и плохим – в противном случае.

1) Доказать, что существует такое число c, что из двух чисел c и $c - n$ всегда одно хорошее, а другое плохое.

2) Сколько всего плохих неотрицательных чисел.

38. Пусть a, b, c – неотрицательные числа. Доказать, что существуют целые числа p_1, q_1, r_1, p_2, q_2, r_2 такие, что

$$a = q_1r_2 - q_2r_1, \quad b = r_1p_2 - r_2p_1, \quad c = p_1q_2 - p_2q_1.$$

39. Найти какие-нибудь целые числа A и B такие, что

$$\frac{A}{999} + \frac{B}{1001} = \frac{1}{999999} .$$

40. Решить в целых числах уравнения:

1) $45x - 37y = 25$;	2) $43x + 37y = 21$;
3) $109x + 89y = 1$;	4) $249x + 181y = 1$;
5) $208x + 136y = 120$;	6) $1726x + 1229y = 3$;
7) $100x + 72y + 90z = 11$;	8) $100x + 72y + 90z = 6$.

41. Найти наименьшее положительное целое число, которое при делении на числа 1000 и 761 дает в остатке 1 и 8 соответственно.

42. Найти число положительных решений уравнения:

1) $10x + 28y = 1240$;	2) $33x + 41y = 1946$;
3) $31x - 7y = 2$;	4) $3x + 11y = 1000$;

5) Пусть a, b – натуральные числа, $(a, b) = 1$. Доказать, что существует $n_0 \in \mathbb{N}$ такое, что уравнение $ax + by = c$ имеет положительное решение (x, y) при любом $c > n_0$.

43. Доказать, что число шагов в алгоритме Евклида может быть сколь угодно велико.

44. Доказать, что если a и b – натуральные числа и $a<b<F_n$, где F_n – n-ое число Фибоначчи, то число шагов в алгоритме Евклида для нахождения наибольшего общего делителя (a, b) меньше n.

45. Доказать, что

$$(F_n, F_m) = F_{(n,\, m)},$$

где $\{F_k\}$ – последовательность чисел Фибоначчи:

$$F_1 = F_2 = 1, \quad F_{k+1} = F_k + F_{k-1}, \quad k \geq 2.$$

46. Числа $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$ называются числами Ферма. Доказать, что любая пара различных чисел Ферма взаимно проста.

47. Даны два натуральных числа a и b, где $a>b$. Найти максимальное число соотношений (последовательных делений) в алгоритме Евклида при нахождении наибольшего общего делителя чисел a и b. (*Теорема Ламе*).

48. 1) Доказать, что видоизмененный алгоритм Евклида для нахождения наибольшего общего делителя двух натуральных чисел a и b, $a>b$ (остатки t_i могут быть отрицательными, неполные частные p_i – положительны).

$$\begin{gathered}
a = bp_1 + t_1, \quad 0 < |\,t\,| < b \\
b = |\,t_1\,|\,p_2 + t_2, \quad 0 < |\,t_2\,| < |\,t_1\,| \\
|\,t_1\,| = |\,t_2\,|\,p_3 + t_3, \quad 0 < |\,t_3\,| < |\,t_2\,| \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
|\,t_{n-2}\,| = |\,t_{n-1}\,|\,p_n + t_n\,, \quad 0 < |\,t_{n-1}\,| < |\,t_n\,| \\
|\,t_{n-1}\,| = |\,t_n\,|\,p_{n+1}, \quad t_{n+1} = 0
\end{gathered}$$

приводит к тому же самому результату, т.е. $(a, b) = \pm\, t_n$.

Например, для $a = 76084$ и $b = 63020$ имеется две возможные схемы вычислений:

$76084 = 1 \cdot 63020 + 13064,$	$76084 = 1 \cdot 63020 + 13064,$
$63020 = 4 \cdot 13064 + 10764,$	$63020 = 5 \cdot 13064 - 2300,$
$13064 = 1 \cdot 10764 + 2300,$	$13064 = 6 \cdot 2300 - 736,$
$10764 = 4 \cdot 2300 + 1564,$	$2300 = 1 \cdot 1564 + 736,$
$2300 = 1 \cdot 1564 + 736,$	$736 = 8 \cdot 92.$
$1564 = 2 \cdot 736 + 92,$	
$736 = 8 \cdot 92.$	

2) Найти наибольшие общие делители а) $(139, 49)$; б) $(1124, 1472)$; в) $(17296, 18416)$, используя алгоритм Евклида и указанную его модификацию.

3) Доказать, что алгоритм Евклида не может быть короче, чем его модификация, т.е. если $N(a, b)$ и $\hat{N}(a, b)$ число делений, соответственно, в алгоритме Евклида и его модификации, то $N(a, b) \geq \hat{N}(a, b)$.

Решения. Указания. Ответы

1. а) 1) Приведем три возможных способа вычислений.

Раскладывая на простые множители, получим:

$$2257 = 61 \cdot 37,\ 1517 = 37 \cdot 41.$$

Следовательно, $(2257, 1517) = 37$.

Используя равенство (2), имеем:

$$(2257, 1517) = (740, 1517) = (740, 777) = (740, 37) =$$
$$= (20 \cdot 37, 37) = \ldots = 37 \cdot (20, 1) = 37.$$

Вычисления при помощи алгоритма Евклида таковы:

$$2257 = 1 \cdot 1517 + 740,$$
$$1517 = 2 \cdot 740 + 37,$$
$$740 = 20 \cdot 37.$$

2) $(1411, 4641, 5253) = (1411, (4641, 525)) = (1421, (4641, 612)) =$
$= (1421, (357, 612)) = (1421, (357, 255)) = (1421, (102, 255)) =$
$= (1421, (102, 51)) = (1421, (51, 51)) = (1421, 51) = \ldots = (44, 51) = (44, 7) = 1.$

3) $[187, 533] = \dfrac{187 \cdot 533}{(187,533)} = 187 \cdot 533 = 99671$, т.к.

$$(187, 533) = (87, 159) = = (28, 159) = (11, 28) = 1.$$

4) Заметим, что $(374, 1599) = (374, 103) = (65, 103) = (65, 48) = 1$, поэтому $[374, 1599] = 374 \cdot 1599 = 2 \cdot 3 \cdot 11 \cdot 13 \cdot 17 \cdot 41$. Так как $9061 = 13 \cdot 17 \cdot 41$, то $[374, 1599, 9061] = [[374, 159], 9061] = [2 \cdot 3 \cdot 11 \cdot 13 \cdot 17 \cdot 41, 13 \cdot 17 \cdot 41] =$
$= 2 \cdot 3 \cdot 11 \cdot 13 \cdot 17 \cdot 41$.

б) *Ответы:* 1) $a = 24$, $a = 242$; $b = 312$, $b = 2496$; 2) $a = 30$, 60, 90, 120 и, соответственно, $b = 120$, 90, 60, 30; 3) $a = 20$, 60, 140, 420 и, соответственно, $b = 420$, 140, 60, 20; 4) $a = 2{,}10$ и, соответственно, $b = 10$, 2;

1) Если $(a, b) = 24$, то $a = 24m$ и $b = 24n$, где $(m, n) = 1$; пусть $n < m$. Тогда из равенства $(a, b) = \frac{ab}{(a,b)}$ найдем, что $mn = 2^3 \cdot 13$. Так как $(m, n) = 1$, то

отсюда имеем две возможности: $mn = 1104$ или $mn = 8 \cdot 13$, т. е. $m = 1$ и $n = 4$ или $m = 8$ и $n = 13$.

2) Равенство $(a, b) = 30$ равносильно системе:

$$\begin{cases} a = 30m, \\ b = 30n, \\ (m, n) = 1, \end{cases}$$

поэтому первое уравнение данной системы дает, что $m+n=5$; откуда $m=1$, 2, 3, 4 и, соответственно, $a=30$, 60, 90, 120. Соответствующие значения b можно найти по формуле $b=150-a$.

Замечание. Аналогичные задачи встречаются и в словесной форме; например (см. [25], задача 2051): частные от деления двух целых чисел на их наибольший общий делитель равны, соответственно, 27 и 10. Найти эти числа, если известно, что сумма их наибольшего общего делителя и наименьшего общего кратного равна 1626.

(*Ответ:* 162 и 60).

2. Схема проверки всех равенств 1–12 использует соотношение (2) из введения к списку задач. Докажем, например, равенство 8. Имеем:

$$(5n+3m,\ 13n+8m)=(5n+3m,\ 8n+5m)=(5n+3m,\ 3n+2m)=$$
$$=(2n+m,\ 3n+2m)=(2n++m,\ n+m)=(n,\ n+m)=(n,\ m).$$

Для доказательства равенства 13 заметим, что если $m>n$, то $(n,m)=(n,m-n)$; следовательно, $(n,m)\le m-n$. Аналогично рассматривается случай $m<n$.

Отметим отдельно еще одно неравенство, которое мы использовали: $(n,m)\le \min(n,m)$.

3. В основе доказательства лежит следующая важная лемма о делимости, принадлежащая Евклиду:

Если произведение ac делится на число b и $(b,a)=1$, то множитель c также делится на b.

Так как $(b,a)=1$, то последний остаток r_n в алгоритме Евклида равен 1, т. е

$$\begin{cases} a=q_1b+r_1, \\ \dots\dots\dots\dots\dots \\ r_{n-2}=q_nr_{n-1}+1. \end{cases}$$

Умножая каждое соотношение на c, получим

$$\begin{cases} ac=q_1bc+r_1c, \\ \dots\dots\dots\dots\dots \\ r_{n-2}c=q_nr_{n-1}c+c. \end{cases}$$

Так как ac делится на b по предположению, то первое соотношение показывает, что r_1c делится на b. Из второго соотношения знаем, что r_2c делится на b; продолжая, найдем, что все r_ic делятся на b и, наконец, c делится на b, что и утверждает лемма.

Отметим следующее следствие: если число взаимно просто с каждым из нескольких чисел, то это число взаимно просто с произведением этих чисел.

Действительно, пусть $(a,b)=1$ и $(a,c)=1$, а числа a и bc имеют делителем число $d>1$. Но $(d,b)=1$. т. к. d делит a; следовательно, по лемме, d делит c, что противоречит тому, что $(d,c)=1$.

Для доказательства формулы 3 воспользуемся алгоритмом Евклида, умножая каждое уравнение на число c; получим:

$$\begin{cases} ac = q_1 bc + r_1 c, \\ \dots\dots\dots\dots\dots \\ r_{n-2}c = q_n r_{n-1} c + r_n c, \\ r_{n-1}c = q_{n+1} r_n c. \end{cases}$$

Ясно, что это алгоритм нахождения (ac, bc), т. е. $(ac, bc) = c(a, b)$.

Отметим, одно следствие: если $d=(a, b)$, то $a=a_1d$ и $b=b_1d$, где $(a_1, b_1)=1$. Действительно, $d=(a, b)=(a_1d, b_1d)=d(a_1, b_1)$.

4. Приведенные равенства являются, соответственно, следствиями следующих равенств (и основой теоремы арифметики):

1) $\min(\alpha, \alpha)=\alpha$, $\max(\alpha, \alpha)=\alpha$;

2) $\min(\alpha, \beta)=\min(\beta, \alpha)$, $\max(\alpha, \beta)=\max(\beta, \alpha)$;

3) $\min\{\min(\alpha, \beta), \gamma\}=\min\{\alpha, \min(\beta, \gamma)\}$, $\max\{\max(\alpha, \beta), \gamma\}=\max\{\alpha, \max(\beta, \gamma)\}$;

4) $\min\{\alpha, \max(\alpha, \beta)\}=\alpha$, $\max\{\alpha, \min(\alpha, \beta)\}=\alpha$.

Доказательство 5) типично. Пусть p^{α}, p^{β}, p^{γ} наивысшие степени простого числа p, которые входят в a, b, c, соответственно. Тогда числа справа и слева в доказываемых равенствах содержат p, соответственно, в степенях

$$\alpha+\beta+\gamma=\max(\alpha+\beta, \beta+\gamma, \alpha+\gamma)+\min(\alpha, \beta, \gamma),$$
$$\alpha+\beta+\gamma=\min(\alpha+\beta, \beta+\gamma, \alpha+\gamma)+\max(\alpha, \beta, \gamma).$$

См. также решение задачи 26 ниже.

Замечание 1. Отсюда видно, что операции нахождения НОД и НОК, max и min, а так же, как известно, в теории множеств операции $\cup$ и $\cap$, являются *дуальными*, т.е. любая из формул, в которой участвуют только эти пары операций, остается справедливой после взаимной замены этих операций в этой формуле.

Замечание 2. Пусть на множестве натуральных чисел $\mathbb{N}$ (точнее на $\mathbb{N}\times\mathbb{N}$) введена операция $\otimes$ такая, что

(1) $a\times b=b\times a$,

(2) $a\times a=a$,

(3) $a\times(a\times b)=a\times b$.

Тогда $a\times b=(a, b)$ и условия (1)–(3) ослабить нельзя.

Действительно, пусть $a+b=c$, т. е. $b=c-a$; тогда из (3) при $c>a$ получаем

(3′) $a\times c = a\times(c-a)$.

Далее, для выполнения $a\times c$ при $a\le c$ мы можем использовать (1). Если $a=c$, то $a\times c = a$ по (2).

Таким образом, при $a<c$, используя многократно (3′) и, если необходимо (1), мы придем к равенству $a'\times a' = a'$ (например, $5\times 15 = 5\times 5 = 5$). Так как свойствами (1)–(3) обладает операция $a\times b=(a,b)$, то мы замечаем, что (a,b) может быть вычислена при помощи того же процесса; отсюда, $a\times b=(a,b)$.

Условия (1) – (3) не могут быть ослаблены, т. к. для $a\times b=\min(a,b)$ выполняются (1), (2), но не (3). Затем, для $a\times b\equiv 1$ выполняются (1), (3), но не (2). Наконец, для $a\times b = a$ выполняются (2), (3), но не (1).

5. *Указание.* Использовать основную теорему арифметики и схему решения задачи 1.4.(См. также решение задачи 26 ниже).

6. Так как $(a,b)=1$, то $(a,2a+b)=1$. Предположим, что

$$(2a+b,\ a+b)=d>1;$$

тогда

$$2a+b=dm,\ a+b=dn, \text{ где } (m,n)=1.$$

Следовательно,

$$a=d(m-n),\ b=d(2n-m),$$

т.е. $d\,|\,a$ и $d\,|\,b$, что невозможно по условию задачи. Таким образом, $d=1$.

7. (*Математика в школе, 1961 г, № 3, задача 891*) НОД данных чисел $d=(a,b,c)$ совпадает с НОД чисел a, b, c, $a+b+c=3n^2$, $a-2b+2c=3m^2$. Так как $(m,n)=1$, то $d=3$ или $d=1$. Первая возможность реализуется, например, при $m=4$, $n=5$, а вторая – при $m=2$, $n=3$.

Замечание. Имеем:

$$a=2m(n+m)-3m^2,\ b=(n-m)(n+m),\ c=(n+m)^2-3mn.$$

Если $n+m$ делится на 3, то a, b, c делятся на 3; если $n+m$ не делится на 3, то c не делятся на 3. Следовательно, если $3\,|\,(n+m)$, то $d=3$, а если $3\nmid(n+m)$, то $d=1$.

8. Пусть $d=(a,b,c)$; тогда $a=md$, $b=nd$, $c=kd$, где d – нечетное число по условию. Имеем:

$$\frac{a+b}{2}=\frac{m+n}{2}d\,,\ \frac{a+c}{2}=\frac{m+k}{2}d\,,\ \frac{b+c}{2}=\frac{n+k}{2}d$$

и, тем самым, d – общий делитель чисел $\frac{a+b}{2}$, $\frac{a+c}{2}$, $\frac{b+c}{2}$. Докажем, что d будет и наибольшим делителем. Пусть $\left(\frac{a+b}{2},\frac{a+c}{2},\frac{b+c}{2}\right)=D$. По доказанному $d\,|\,D$ и

$$\frac{a+b}{2}=m_1D,\ \frac{a+c}{2}=n_1D,\ \frac{b+c}{2}=k_1D.$$

Отсюда, складывая и вычитая, найдем:
$a=(m_1+n_1-k_1)D,\ b=(m_1-n_1+k_1)D,\ b=(-m_1+n_1+k_1)D.$

Таким образом, числа a, b и c делятся на D и поэтому $d\,|\,D$. Из тех же равенств заключаем, что $D\,|\,a$ и $D\,|\,b$, т. е. $D\,|\,d$, что и требовалось доказать.

Замечание. Для n чисел будем иметь:

$$(a_1, a_2, \ldots, a_n) = (a_n, r_1, r_2, \ldots, r_n),$$

$r_1, r_2, \ldots, r_n$ – остатки от деления чисел $a_1, a_2, \ldots, a_{n-1}$ на a_n.

10. (*Венгерская олимпиада, 1901 г.* [2], *стр. 12, задача 24*). Пусть $d=(a,b)$, тогда $a=dr,\ b=ds,$ где $(r,s)=1$. Если разделить все данные числа на b, то частные можно записать в виде

$$\frac{r}{s},\ \frac{2r}{s},\ \frac{3r}{s},\ \ldots,\ \frac{(ds)r}{s}.$$

Но $(r,s)=1$, следовательно, целыми числами могут быть лишь те, у которых в числителе коэффициент при r, равный 1, 2, 3, …, ds делится на s, а число таких коэффициентов равно d.

11. Для того чтобы найти наименьшее общее кратное двух заданных чисел, необходимо найти два как можно меньших числа, таких, что, умножив одно из них на одно заданное число, а другое на другое заданное число, мы получим одно и тоже произведение. Следовательно, в силу самого выбора этих чисел они зависят только от отношения двух заданных чисел.

12. (*Московская олимпиада,* [3] *задачи 62, 63*)

а) Так как $[15,35]=105$ и $(8,18)=2$, то число $\frac{2}{105}$ – искомое.

б) Так как $[35,28]=140$ и $(396,297)=99$, то число $\frac{140}{99}$ – искомое.

Замечание. Назовем наименьшим общим кратным положительных рациональных чисел $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}$ такое наименьшее положительное число M, которое делится нацело на каждое из этих чисел. Тогда

$$M = \left[\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}\right] = \frac{[p_1, p_1, \ldots, p_k]}{(p_1, p_1, \ldots, p_k)}.$$

Действительно, найдем наименьшее число $\frac{P}{Q}$ такое, чтобы для каждой дроби $\frac{p_i}{q_i}$ $(i=1, 2, \ldots, k)$ выполнятся равенство

$$\frac{P/Q}{p_i/q_i} = \frac{P_{qi}}{Q_{pi}} = a_i, \qquad (*)$$

где a_i – натуральные числа. Если $P=[p_1, p_2, \ldots, p_k]$ и $Q=(p_1, p_2, \ldots, p_k)$, то все числа $\frac{q_i}{Q} = \frac{P}{p_i} = \frac{P_{qi}}{Q_{pi}} = a_i$ будут натуральными числами, т.к. каждый сомножитель является натуральным числом. Легко показать, что, выбрав так P и Q, мы получим наименьшее рациональное число $\frac{P}{Q}$, для которого имеет место соотношение $(*)$.

Доказанное выше равенство (*) имеет применение при исследованиях, связанных с суммой периодических функций одной и нескольких переменных; интересные примеры можно найти в [4, стр. 170-187].

13. (*Московская олимпиада 1972,* [5]*, с. 123*) Рассмотрим *все* дроби, сократимые и несократимые, у которых числитель и знаменатель не превосходят 100; общее их число равно 100^2.

Если $(a,b)=d$, то дробь $\frac{a}{b}$ сократима на d и полученная несократимая дробь $\frac{a_1}{b_1}$, $(a_1,b_1)=1$, такова, что $a_1 \le \frac{100}{d}$ и $b_1 \le \frac{100}{d}$, т. е. в количестве $K(\frac{100}{d})$ несократимых дробей мы учтем и эту дробь. Следовательно, искомая сумма равна количеству всех рассмотренных дробей, т.е. равно 10 000.

14. Докажем последнее равенство 3. Пусть $n>m$ и $n=q_1m+r_1$, тогда

$$a^n - 1 = a^{mq_1+r_1} - 1 = a^{r_1}(a^{mq_1} - 1) + (a^{r_1} - 1).$$

Но число

$$a^{mq_1} - 1 = (a^m)^{q_1} - 1$$

делится на число a^m-1; следовательно, любой общий делитель D чисел a^m-1 и a^n-1 делит число $a^{r_1}-1$. Точно так же доказывается, что число $a^{r_2}-1$, где r_2 – остаток от деления числа m на r_1, делится на D; что $a^{r_3}-1$, где r_3 – остаток от деления r_1 на r_2, делится на D и т. д. Этот процесс, по алгоритму Евклида, приведет к тому, что D делит $a^{(m,n)}-1$.

С другой стороны, если $d=(m,n)$, то $m=m_1d$ и $n=n_1d$, где $(n_1,m_1)=1$ и

$$a^n - 1 = (a^d)^{n_1} - 1,$$

$$a^m - 1 = (a^d)^{m_1} - 1;$$

тем самым, d делит a^n-1 и a^m-1. отсюда следует нужное утверждение.

Отметим одну важную формулу, которую мы использовали выше: $x^n - y^n = (x-y)(x^{n-1} + yx^{n-2} + \ldots + y^{n-2}x + y^{n-1})$.

Замечание 1. Чтобы не повторять анализ каждого соотношения в алгоритме Евклида в отдельности, можно воспользоваться его важным следствием (см. [7], а также задачу 36 ниже): если m, n натуральные числа и $d=(m,n)$, то найдутся такие целые числа x и y, что $nx = my + d$.

Тогда

$$a^{mx} - 1 = a^{ny+\alpha} - 1 = a^{\alpha}(a^{ny}-1) + (a^{\alpha} - 1)$$

откуда тоже легко получить все равенства 1 – 3.

Замечание 2. Отметим ряд полезных следствий.

(1) числа 2^m-1 и 2^n-1 $(m,n\in\mathbb{N})$ взаимно просты тогда и только тогда, когда $(m,n)=1$ (см. [12], задача 96).

Например, следующая запись предлагалась на олимпиаде в Испании (см. [9], задача 5.7): найти наибольший общий делитель чисел $A = 2^{97482} - 1$ и $B = 2^{29579} - 1$.

(2) Если числа $2^m - 1$ и $2^n - 1$ делятся на число b, то и число $a^{(m,\, n)} - 1$ делится на b.

15. (*См.* [13]*, задачи 12*) Пусть

$$d = \left(\frac{a^n - 1}{a - 1},\, a - 1 \right).$$

Так как

$$\frac{a^m - 1}{a - 1} = (a^{m-1} - 1) + (a^{m-2} - 1) + \ldots + (a - 1) - m,$$

то d делит m, т. к. при любом $k = 0, 1, 2, \ldots$ число $a^k - 1$ делится на $(a - 1)$.

Если бы числа $a - 1$ и m имели общий делитель $D > d$, то из этого же равенства мы замечаем, что $\frac{a^m - 1}{a - 1}$ делилось бы на D и, тем самым, числа $\frac{a^m - 1}{a - 1}$ и $a - 1$ имели бы общий делитель $D > d$,что невозможно.

Замечание. (*Из материалов жюри XXII Международной олимпиады, Польша*) Отсюда, в частности, следует, что $\left(\frac{a^m - 1}{a - 1}, \frac{a^m - 1}{a - 1} \right) = (n, m)$.

16. (*Венгерская олимпиада, 1940. См.* [2]*, задача 13*)

Решение 1. Пусть $f_k = 2^{2^k}$ и докажем, что $(f_k - 1) \,|\, (f_{k+1} - 1)$, $k = 1, 2, \ldots$. Действительно, так как

$$f_{k+1} - 1 = f_k^{\,2} - 1 = (f_k - 1)(f_k + 1),$$

то $f_{k+1} - 1$ делится на $f_k - 1$. Нетрудно видеть также, что $f_{k+1} - 1$ делится на $f_k + 1$, а значит и число $f_m - 1$ также делится на $f_k + 1$ при $m > n$.

Таким образом, если $m > n$, то

$$f_m + 1 = q(f_n + 1) + 2,$$

где q – целое число. Тем самым, наибольший общий делитель чисел $f_m + 1$ и $f_n + 1$ является делителем 2. Следовательно, числа $f_m + 1$ и $f_n + 1$ взаимно просты, так как являются нечетными числами.

Решение 2. Имеет место тождество (см. [2], стр. 194)

$$(1 + x)(1 + x^2)(1 + x^4)(1 + x^{2^k - 1}) = 1 + x + x^2 + \ldots + x^{2^k - 1}.$$

Положим здесь $x = 2$ и прибавим к правой и левой части по 2, получим равенство

$$F_1 F_2 \ldots F_k + 2 = F_k + 1, \text{ где } F_k = f_{k-1} + 1.$$

При $l < k$ число F_k входит сомножителем в левой части. Следовательно, (F_l, F_k) должен быть делителем числа 2, но поскольку два числа нечетные, то $(F_l, F_k) = 1$.

17. (*См.* [13], *задача 44*) Известно (это показал Эйлер см.[18]), что любой делитель, больший единицы, числа $F_n = 2^{2^n} + 1$ есть число вида $2^{n+2}k + 1$, где k – натуральное число. Так как два натуральных числа n и k
$2^{n+2}k + 1 \geq 2^{n+2} + 1 > n,$
то каждый делитель числа F_n является числом, большим n. Отсюда

$$(n, F_n) = 1,\ n = 1,\ 2,\ \dots .$$

2) Непосредственным вычислением устанавливаем, что $(n, 2^n - 1) = 1$, при $n = 1, 2, 3, 4, 5$, а $(6, 2^6 - 1) = 3$. Таким образом, наименьшее число, о котором идет речь, есть $n = 6$. Далее, т. к. $3 \mid 2^6 - 1$ и $2^6 - 1 \mid 2^{6k} - 1$ для $k = 1, 2, \dots$, то отсюда заключаем, что $(6k, 2^{6k} - 1) \geq 3$ для $k = 1, 2, \dots$.

18. (*См.* [14], *задача 306*). Пусть $a > b$. Любой общий делитель чисел $n^a + 1$ и $n^b + 1$ должен быть делителем их суммы $n^a + n^b = n^b(n^{a-b} + 1)$, т. е. Общим делителем чисел $n^b - 1$ и $n^{a-b} + 1$. Продолжая этот процесс дальше (используя свойство: $(a, b) = (a - b, b)$), заключаем, что общий делитель чисел $n^a + 1$ и $n^b - 1$ должен быть делителем числа $n^d + 1$.

Пусть $x = n^d$, так что $n^b - 1 = x^{b'} - 1$, b' – нечетное число. Тогда разделить $n^b - 1$ означает то же самое, что разделить $x^{b'} - 1$ на $x + 1$. Остаток от деления $x^{b'} - 1$ на $x + 1$ равен (–2). Следовательно, числа $n^a + 1$ и $n^b - 1$ не могут иметь общий множитель, который был бы больше 2.

Замечание 1. На аналогичной идее может быть построено решение следующей задачи (*сборы команды Испании в 1988 году для участия в XXIX ММО, см.* [20]): Пусть a, b, m, n – натуральные числа, $a > 1$ и $(a, b) = 1$. Доказать, что $a^n + b^n$ делит $a^m - b^m$ тогда и только тогда, когда число m кратно числу n.

Замечание 2. В статье из журнала [23] указано, что задача из замечания 1 была придумана русскими школьниками. В этой связи приведем задачу, которая была на VI Всесоюзной олимпиаде школьников в 1972 году (*см.* [24], *задача 162*):

Пусть a, b, m, n – натуральные числа, $a > 1$ и $(a, b) = 1$. Доказать, что если $a^m + b^m$ делится на $a^n + b^n$, то m делится на n.

Решение. Из того, что $(a, b) = 1$ и тождеств

$$a^k + b^k = a^{k-n}(a^n + b^n) - b^n(a^{k-n} - b^{k-n}),$$
$$a^l - b^l = a^{l-n}(a^n + b^n) - b^n(a^{l-n} + b^{l-n})$$

следует, что

(1) если $a^k + b^k$ делится на $a^n + b^n$, то $a^{k-n} - b^{k-n}$ делится на $a^n + b^n$;

(2) если $a^l - b^l$ делится на $a^n + b^n$, то $a^{l-n} + b^{l-n}$ делится на $a^n + b^n$.

Теперь, если $m = qn - r$, где $0 \leq r < n$, то из (1), (2) следует, что $a^r + (-1)^q b^r$ делится на $a^n + b^n$.

Но

$$0 \le | a^r + (-1)^q b^r | < a^n + b^n.$$

Отсюда следует, что $r = 0$ (а число q – нечетно; ср. с решением задачи 18).

19. Найдем (n, m), используя алгоритм Евклида:

$$\begin{array}{ll} n = mq_1 + r_1, & 0 < r_1 < m, \\ m = r_1 q_2 + r_2, & 0 < r_2 < r_1, \\ \dots\dots\dots\dots & \dots\dots\dots \\ r_{k-2} = r_{k-1} q_k + r_k, & 0 < r_k < r_{k-1}, \\ r_{k-1} = r_k q_{k+1}, & (r_{k+1} = 0). \end{array}$$

Тогда $(n, m) = r_k$, где r_k – последний отличный от нуля остаток.

В соответствии с этой системой равенств, применим алгоритм Евклида и для нахождения наибольшего общего делителя данных чисел. Получим:

$$\underbrace{11\ldots1}_{n} = \underbrace{11\ldots1}_{m} \cdot 10^{q_1} + \underbrace{11\ldots1}_{r_1};$$

$$\underbrace{11\ldots1}_{m} = \underbrace{11\ldots1}_{r_1} \cdot 10^{q_2} + \underbrace{11\ldots1}_{r_2};$$

$$\dots\dots\dots\dots\dots\dots$$

$$\underbrace{11\ldots1}_{r_{k-2}} = \underbrace{11\ldots1}_{r_{k-1}} \cdot \underbrace{11\ldots1}_{q_k} + \underbrace{11\ldots1}_{r_k};$$

$$\underbrace{11\ldots1}_{r_{k-1}} = \underbrace{11\ldots1}_{r_k} \cdot \underbrace{11\ldots1}_{q_k},$$

что и доказывает нужное утверждение.

Замечание. Частные случаи этой задачи встречаются во многих источниках (см., например, [2], [3], [7], [12]).

20. (См. [22], задача 2.4, а также [15])

1) *Ответ:* 3мм.

Используя алгоритм Евклида, найдем:

$324 = 141 \cdot 2 + 42$ (*2 квадрата со стороной 141 мм*);

$141 = 42 \cdot 3 + 15$ (*3 квадрата со стороной 42 мм*);

$42 = 15 \cdot 2 + 12$ (*2 квадрата со стороной 15 мм*);

$15 = 12 \cdot 1 + 3$ (*1 квадрат со стороной 12 мм*);

$12 = 3 \cdot 4$ (*4 квадрата со стороной 3 мм*).

Замечание. Для произвольного прямоугольника $a \times b$ длина стороны последнего квадрата равна (a, b).

2) *Ответ,* например, $a = 12$, $b = 13$.

Имеем:

$$21 = 1 \cdot 13 + 8;$$
$$13 = 1 \cdot 8 + 5;$$
$$8 = 1 \cdot 5 + 3;$$
$$5 = 1 \cdot 3 + 2;$$

$$3 = 1 \cdot 2 + 1;$$
$$2 = 2 \cdot 1.$$

Замечание. Для произвольного натурального числа n существуют такие числа a и b, чтобы при разрезании получилось ровно n различных квадратов (см. задачи и ниже).

21. (См.[22], задача 2.5, а также статью [23]).

1) *Ответ:* можно.

Будем операции автоматов соответственно обозначать через L, R, S и условимся n сделанных подряд операций L или R записывать через L^n или R^n. Тогда карточку $(31, 13)$ можно получить из карточки $(19, 86)$ следующим образом:

$$(19, 86) \xrightarrow{S} (86, 19) \xrightarrow{R^4} (10, 19) \xrightarrow{S} (19, 10) \xrightarrow{L}$$
$$(9, 10) \xrightarrow{S} (10, 9) \xrightarrow{L} (1, 9) \xrightarrow{S} (9, 1) \xrightarrow{L^7}$$
$$(2, 1) \xrightarrow{S} (1, 2) \xrightarrow{L} (3, 2) \xrightarrow{S} (2, 3) \xrightarrow{R}$$
$$(5, 3) \xrightarrow{S} (3, 5) \xrightarrow{R^2} (13, 5) \xrightarrow{S} (5, 13) \xrightarrow{R^2} (31, 13).$$

2) *Ответ:* нельзя.

Так как операции L, R, S сохраняют наибольший общий делитель (m, n), а $(19, 86) = 1 \neq (12, 21) = 3$, то из карточки $(19, 86)$ нельзя получить карточку $(12, 21)$.

3) Необходимое и достаточное условие того, чтобы из карточки (m, n) можно было получить карточку (a, b), состоит в том, что

$$\text{НОД}(m, n) = \text{НОД}(a, b).$$

Необходимость следует из того, что все три операции сохраняют наибольший общий делитель пары чисел на карточки.

Если это условие выполнено, то обе карточки при помощи алгоритма Евклида можно привести к карточке (d, d), где $d = \text{НОД}(a, b) = \text{НОД}(m, n)$. Действительно, каждый шаг алгоритма Евклида – это деление с остатком числа a на число b: $a = b \cdot q + r, \cdot 0 \le r < \text{b}$. Этот шаг можно провести так:

$$(a, b) \xrightarrow{L^q} (r, b).$$

Затем, после операции $(r, b) \xrightarrow{S} (b, r)$, можно аналогично сделать следующий шаг алгоритма и т. д. до тех пор, пока не получится карточка (d, d).

Идя по цепочке $(a, b) \longrightarrow \dots \longrightarrow (d, d)$ в обратном порядке с заменой операции L на операцию R, мы из карточки (d, d) получим карточку (a, b).

Итак, проделав «спуск» от (m, n) к (d, d), а затем «подъем» от (d, d) к (a, b), мы пройдем от карточки (m, n) к карточке (a, b), что и требовалось.

Замечание 1. Приведем здесь одно интересное обобщение этой задачи из статьи [23].

С матрицей $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ разрешается проводить следующие операции:

$$L\colon \begin{pmatrix} a & c \\ b & d \end{pmatrix} \longrightarrow \begin{pmatrix} a-b & c-d \\ b & d \end{pmatrix},$$

$$R\colon \begin{pmatrix} a & c \\ b & d \end{pmatrix} \longrightarrow \begin{pmatrix} a+b & c+d \\ b & d \end{pmatrix},$$

$$L\colon \begin{pmatrix} a & c \\ b & d \end{pmatrix} \longrightarrow \begin{pmatrix} b & d \\ a & c \end{pmatrix}.$$

Можно ли этими операциями из матрицы $\begin{pmatrix} 1 & 5 \\ 2 & 7 \end{pmatrix}$ получить следующие матрицы:

а) $\begin{pmatrix} 1 & 3 \\ 2 & a \end{pmatrix}$, б) $\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$, в) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, г) $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$, д) $\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}$?

Какие вообще матрицы можно получить из данной матрицы $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$?

Будем называть две матрицы эквивалентными, если одну из них операциями L, R, S можно перевести в другую. Матрица $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ называется сокращенной, если числа каждого столбца разделены на их наибольший общий делитель. Величина $\Delta = |ad - bc|$ называется определителем матрицы $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ и она сохраняется при операциях L, R, S.

Лемма ([23]). Любую сокращенную матрицу операциями L, R, и S можно преобразовать к каноническому виду

$$\begin{pmatrix} 1 & r \\ 0 & \Delta \end{pmatrix}, \quad \text{где} \quad 0 \le r < \Delta \quad \text{и} \quad \text{НОД}(r, \Delta) = 1$$

или

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad \text{если} \quad \Delta = 0.$$

Теперь мы можем сформулировать ответ к задаче:

Две матрицы $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ и $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$ эквиваленты тогда и только тогда, когда

$$\text{НОД}(a, b) = \text{НОД}(p, q),$$
$$\text{НОД}(c, d) = \text{НОД}(r, s)$$

и соответствующие сокращенные матрицы имеют один и тот же канонический вид. (См. [23]).

Замечание 2. Еще одна, близкая по духу, задача предлагалась в 1978 году на XII Всесоюзной математической олимпиаде (см. [24, задача260]).

22. (*Всероссийская математическая олимпиада 1963 г. См. [24], задача 30*) Если a^2+b^2 и $a+b$ делятся на d, то и $(a+b)^2-(a^2+b^2)=2ab$ делятся на d. Следовательно, $2a^2=2a(a+b)-2ab$ и $2b^2=2b(a+b)-2ab$ делятся на d.

Но если $(a,b)=1$, то $(a^2,b^2)=1$; следовательно, числа $2a^2$ и $2b^2$ не могут делиться ни на какие $d>2$.

23. (*См. [15]*) *Ответ:* 10.

Пусть $ab=600$, $d=(a,b)$, т.е. $a=nd$ и $b=md$, где $(n,m)=1$. Тогда $nmd^2=600$. Наибольший квадрат, на который делится число 600, равен 100; поэтому $d\le 10$.

Пример: $a=60$, $b=10$.

24. (*Киевская олимпиада 1979 г. См. [26], стр. 66*) *Ответ:* 9.

Пусть $d=(a_1, a_2, \ldots, a_{49})$. Так как $a_1+a_2+\ldots+a_{49}=999$, то d делитель числа $999=3^3\cdot 37$. По определению, $a_k\ge d$, $k=1, 2, \ldots 49$, то

$$999 = a_1 + a_2 + \ldots + a_k \ge 49$$

и, тем самым, $d\le \frac{999}{49}<21$.

Итак, имеется три возможности: $d=1$, $d=3$, $d=9$. Наибольшее значение $d=9$ достигается, так как
$999 = 9 + 9 + \ldots + 567$.

25. (*Российская олимпиада 1985 г. См. [27], с. 19*) *Ответ:* 91.

Пусть $k=\text{НОД}(a_1, a_2, \ldots, a_{10})$; тогда $a_1=kb_1$, $a_2=kb_2, \ldots$ $a_{10}=kb_{10}$, причем $b_1+b_2+\ldots+b_{10}\ge 10$, и

$$k=\frac{a_1+a_2+\ldots+a_{10}}{b_1+b_2+\ldots+b_{10}}\le\frac{1001}{10}<101.$$

Т.к. $1001=7\cdot 11\cdot 13$ и k – делитель числа 1001, не превосходит 100, то $k\le 91=7\cdot 13$. Поскольку для чисел $a_1=a_2=\ldots=a_9=91$ и $a_{10}=182$ имеем $k=91$, то, что и есть ответ задачи.

26. Доказательство проводится по одной схеме, которую мы покажем на примере равенства 7 (эта задача предлагалась на Американской олимпиаде в 1972 году; см. [28]).

Пусть
$$a=\prod p_i^{\alpha_i},\ b=\prod p_i^{\beta_i},\ c=\prod p_i^{\gamma_i},$$
где p_i обозначают простые делители чисел a, b, c (некоторые из показателей могут быть равны). Так как
$$[a, b]=\prod p_i^{\max(\alpha_i,\beta_i)},\ (a, b)=\prod p_i^{\min(\alpha_i,\beta_i)}$$
и т.д. мы должны показать, что
$$2\max\{\alpha_i, \beta_i, \gamma_i\}-\max\{\alpha_i, \beta_i\}-\max\{\beta_i, \gamma_i\}-\max\{\alpha_i, \gamma_i\}=$$
$$=2\min\{\alpha_i, \beta_i, \gamma_i\}-\min\{\alpha_i, \beta_i\}-\min\{\beta_i, \gamma_i\}-\min\{\alpha_i, \gamma_i\}$$
для каждого индекса i. Без ограничения общности мы можем предположить, что $\alpha_i \ge \beta_i \ge \gamma_i$ для любого частного значения i. Нужное равенство следует из равенства
$$2\alpha_i-\alpha_i-\beta_i-\alpha_i=2\gamma_i-\beta_i-\gamma_i-\gamma_i.$$

Два последних тождества носят общий характер (последняя задача заимствована из книги [29], отдел 8, гл. 1, §4). Их решение основано на одной теореме формальной логики, применение которой к нашему случаю дает: Если $\alpha_1, \alpha_2,\ldots, \alpha_n$ произвольные целые числа, то
$$\begin{gathered}\max(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n)=\\ =\alpha_1+\alpha_2+\ldots+\alpha_{n-1}+\alpha_n-\\ -\min(\alpha_1, \alpha_2)-\min(\alpha_2, \alpha_3)-\ldots-\min(\alpha_{n-1}, \alpha_n)+\\ +\min(\alpha_1, \alpha_2, \alpha_3)-\ldots\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \pm\min(\alpha_1, \alpha_2,\ldots, \alpha_{n-1}, \alpha_n).\end{gathered}$$

27. (*Российская олимпиада 1994 г., предложена А. Головановым*).

См. решение предыдущей задачи и задачи 4.

28. (*Российская олимпиада 1994 г., предложена А. Головановым и Е. Малинниковой; ср. с задачей 30 из [24] и задачей [15]*).

Пусть $d=(a, b)$. Так как
$$\frac{a+1}{b}+\frac{b+1}{a}=\frac{a^2+b^2+a+b}{ab},$$
по условию целое число и d^2 делит ab, то d^2 делит также a^2+b^2+a+b и, тем самым, $a+b$ (т. к. d^2 делит и a^2+b^2). Таким образом, число $a+b$ делится на d^2 и, следовательно,
$$d \le \sqrt{a+b}.$$

29. (*Венгерская олимпиада 1962 г., см. [2], задача 184)*. Пусть
$$n=p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}$$
– каноническое разложение числа n на простые множители ($p_1, p_2,\ldots, p_s$ – простые и $a_1, a_2,\ldots, a_s$ – натуральные числа). По условию,
$$[u, v]=p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}, \qquad (*)$$

и, тем самым, разложение чисел u и v в произведение простых чисел могут содержать лишь числа $p_1, p_2, \ldots, p_s$. Из равенства (*) следует, что каждое p_k входит в разложение для u и v в степени не больше a_k. Рассмотрим отдельно три возможности:

1) в разложения u и v число p_k входит в степени a_k (одна возможность для данного k);

2) в разложение числа u простое число p_k входит в степени a_k, а в разложение v – в меньшей степени, т. е. в одной из степеней 0, 1, 2, … , a_k-1 (a_k возможных случаев);

3) в разложение числа v простое число p_k входит в степени a_k, а в разложение числа u – в меньшей степени (снова a_k возможных случаев).

Таким образом, всего возможно $(2a_k+1)$ различных вариантов распределения степеней простого числа p_k между разложениями чисел u и v.

Поскольку, фиксируя любое из возможных распределений степени одного простого числа, мы можем комбинировать его с любым допустимым распределением степеней любого другого простого числа, то общее число возможных распределений простых чисел $p_1, p_2, \ldots, p_s$ между разложениями чисел u и v равен

$$(2a_1 + 1)(2a_2 + 1)\ldots(2a_s + 1).$$

Так как

$$n^2 = p_1^{2a_1} p_2^{2a_2} \ldots p_s^{2a_s},$$

то делители числа n^2 могут содержать простое число p_k в степени 0, 1, 2, … , $2a_k$, т. е. простое число p_k может входить в различные делители числа n^2 всего $(2a_k+1)$ способами. Поскольку каждое простое число p_1, $p_2, \ldots, p_s$ можно выбрать независимо от другого, то общее число делителей числа n^2 равно:

$$(2a_1 + 1)(2a_2 + 1)\ldots(2a_s + 1),$$

что и требовалось доказать.

Замечание. В [2] на стр. 325 имеется другое решение, основанное на существовании взаимно однозначного соответствия между упорядоченными парами (u, v) такими, что $[u, v] = n$ и делителями числа n^2: каждой паре (u, v) ставится в соответствие число d такое, что $\frac{u}{v} = \frac{d}{n}$.

31. (*Венгерская олимпиада 1982 г., см. [30],задача 1.20*). Докажем, что неравенству $A(n) > A(n+1)$ удовлетворяет любое число $n = r \cdot k! - 1$, $r \in \mathbb{N}$, $r > 3$.

Обозначим

$$m = [n + 1, \ldots, n + k].$$

При $j = 1, \ldots, k$ имеем $n \equiv -1 (\mathrm{mod}\, j)$ откуда $(n, j) = 1$ и $(n, n + j) = 1$.

Следовательно,

$$(n, m) = 1 \text{ и } A(n) = [n + 1, \ldots, n + k] = [n, m] = nm.$$

С другой стороны число $n+k+1=r\cdot k!$, а значит, и на k. Поэтому число $\frac{m(n+k+1)}{k}$ делится как на m, так и на $n+k+1$. Значит

$$A(n+1)=[n+1,\ \dots,\ n+k]=[m,\ n+k+1]\le\frac{m(n+k+1)}{k}.$$

Отсюда, учитывая оценки $k\ge 2$ и $r\ge 3$, получаем

$$A(n+1)\le\frac{m(n+k+1)}{2}=$$

$$=\frac{mn}{2}\left(1+\frac{k+1}{n}\right)\le\frac{mn}{2}\left(1+\frac{k+1}{3k-1}\right)<\frac{mn}{2}\cdot 2=mn=A(n),$$

что и требовалось доказать.

32. (*American Mathematical Monthly, 1991 г. т. 98, №6, стр. 555, задача E3350 П. Эрдеша*).

б) Заметим, что

$$A(n,\ k+1)=[n-k,\ A(n,\ k)],\ 1\le k<n. \qquad (*)$$

Поэтому

$$A(n,\ k)\le A(n,\ k+1)$$

и равенство имеет место тогда и только тогда, когда $(n-k)$ делит $A(n,k)$ (см. решение задачи). Отметим, что $f(1)=1$.

При $m>1$ имеем

$$A(m^2,\ 2)=m^2(m^2-1)=(m^2-m)(m^2+m).$$

Таким образом, $(m^2-m)\,|\,A(m^2,2)$ и, тем самым, $(m^2-m)\,|\,A(m^2,m)$, т.к.

$$A(m^2,\ m)=[A(m^2,\ 2),\ m^2-2,\ \dots,\ m^2-m+1].$$

Отсюда и из (*) заключаем, что

$$A(m^2,\ m+1)=A(m^2,\ m).$$

Тогда по определению функции f, имеем:

$$f(m^2)\le m,\quad m=1,\ 2,\ \dots.$$

Заметим, что из соотношения (*) следует, что если $A(n,k)=A(n,k+1)$, то

$$A(n+j,\ k+j)=A(n+j,\ k+j+1)\quad j=1,\ 2,\ \dots.$$

Таким образом

$$f(n+j)\le f(n)+j\quad (n,\ j=1,\ 2,\ \dots).$$

Теперь, если $m^2\le n<(m+1)^2$, то $n=m^2+j$, где $0\le j\le 2m$. Следовательно,

$$f(n)\le f(m^2+j)\le 3m\le 3\sqrt{n},$$

где, по крайней мере, одно из последних неравенств должно быть строгим.

33. (*Задача П. Эрдеша из книги [14]*).

Предположим, что $a_1\le[2n/3]$;тогда $3a_1\le 2n$. Рассмотрим множество целых чисел $2a_1$, $3a_1$, a_2, $\dots$, a_n. Оно содержит $n+1$ целых чисел, из которых ни одно не делит другое. Поскольку это невозможно, то полученное противоречие доказывает утверждение задачи.

Замечание. Приведем еще две задачи П. Эрдеша из книги [14], решение которых неизвестно.

1) Пусть $a_1 < a_2 < \ldots a_n \le 2n$ – конечная последовательность целых положительных чисел.

Доказать, что

$$\min[a_i, a_j] < 6\left(\left[\frac{n}{2}\right] - 1\right)$$

и эту оценку для $\min[a_i, a_j]$ улучшить нельзя.

2) Пусть $a_1 < a_2 < \ldots a_n \le 2n$ – конечная последовательность целых положительных чисел.

Доказать, что

$$\max(a_i, a_j) > \tfrac{38n}{147} - c,$$

где c не зависит от n, и эту оценку для $\max(a_i, a_j)$ нельзя улучшить.

34. Пусть m какой-либо делитель чисел a и b и

$$m = ax + by.$$

Если $d = (a, b)$, то отсюда следует, что d делит m. С другой стороны

$$d = ax' + by'$$

и, тем самым, m делит d. Таким образом, $m = kd$ и $d = lm$, где k и l некоторые целые числа. Следовательно, $kl = 1$ и, тем самым, $k = l = 1$ или $k = l = -1$.

Замечание 1. Если

$$\begin{array}{ll} a = bq_1 + r_1, & \text{где} \quad 0 < r_1 < b, \\ b = r_1q_2 + r_2, & \text{где} \quad 0 < r_2 < r_1, \\ r_1 = r_2q_3 + r_3, & \text{где} \quad 0 < r_3 < r_2, \\ \ldots\ldots\ldots\ldots & \\ r_{n-2} = r_{n-1}q_n + r_n, & \text{где} \quad 0 < r_n < r_{n-1}, \\ r_{n-1} = r_nq_{n+1} + r_{n+1}, & \end{array}$$

то $r_n = (a, b)$. Остаток r_1 записывается в виде $ax_1 + by_1$, т. к. $r_1 = a - bq_1$. Следующий остаток r_2 также, т.к.

$r_2 = a - r_1q_2 = b - (ax_1 + by_1)q_2 =$

$= a(-x_1q_2) + b(1 - y_1q_2) = ax_2 + by_2$

и т.д. до $r_n = (a, b)$.

Поэтому наибольший общий делитель представим в виде линейной комбинации чисел a и b с целыми коэффициентами. Утверждение задачи показывает только два общих делителя чисел a и b (среди всех общих делителей) обладают этим свойством.

Замечание 2. Легко проверить, что ($r_0 = b$, $r_{-1} = a$)

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix},$$

$i = n-1,\ n-2,\ \ldots,\ 2,\ 1,\ 0.$

Таким образом,

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Если произведение квадратных матриц в этом равенстве обозначить через

$$\begin{pmatrix} u & v \\ x & y \end{pmatrix},$$

то имеем равенство

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} u & v \\ x & y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

откуда

$$(a, b) = r_n = xa + yb.$$

Замечание 3. A. Newhouse в [31] получил интересные формулы для x и y:

$$x = (-1)^n \begin{vmatrix} q_2 & 1 & 0 & & & & \ldots & & 0 \\ -1 & q_3 & 1 & 0 & & & \ldots & & 0 \\ 0 & -1 & q_4 & 1 & 0 & & \ldots & & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & & & \ldots & & & 0 & -1 & q_{n+1} \end{vmatrix},$$

$$y = (-1)^{n+1} \begin{vmatrix} q_1 & 1 & 0 & & & & \ldots & & 0 \\ -1 & q_2 & 1 & 0 & & & \ldots & & 0 \\ 0 & -1 & q_3 & 1 & 0 & & \ldots & & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & & & \ldots & & & 0 & -1 & q_{n+1} \end{vmatrix}.$$

Замечание 4. Leo Moser (см. [14], задача 392) предложил следующую форму, представляющую интерес,

$$(a, b) = \sum_{m=0}^{a-1} \sum_{n=0}^{a-1} \tfrac{1}{a} e^{2\pi i bmn/a}\ .$$

В основе доказательства лежит формула для сумм конечного числа членов геометрической прогрессии (подробности в [14]).

35. (*Всероссийская олимпиада 1961 г., см. [24, задача 29]*). Пусть $d = (b, p-a)$; тогда $b = kd$ и $p - a = ld$, где $(k, l) = 1$. Таким образом,

$$ak + bl = \frac{ab}{d} + \frac{(p-a)b}{d} = pk,$$

что и утверждалось.

36. *Ответ:* такое представление возможно $(n-1)$ способами:

$$x = bk,\ y = a(n-k) \text{ где } k = 1,\ 2,\ \ldots,\ n-1$$

(ср. с предыдущей задачей).

Если $nab = ax + by$, то $x = bk$ (т. к. $(a, b) = 1$), где $k = 1, 2, \ldots$. Отсюда $nab = abx + by$, т. е. $y = a(n-k)$ и $k = 1, 2, \ldots, n-1$.

Так как $abk + ba(n-k) = nab$, то требуемое представление осуществимо, причем $(n-1)$ способами при $k = 1, 2, \ldots, n-1$.

37. (*Всероссийская олимпиада 1965 г., см. [24], задача 68, а также статью[32]*).

Ответ: 2) $\frac{(p-1)(q-1)}{2}$.

Если $(p, q) = 1$, то любое целое число z можно представить в виде $z = px + qy$. Всякое представление такого вида получается из некоторого фиксированного $ap + bq = z$ по одной общей формуле

$$z = p(a - qt) + q(b + bt), \text{ где } t \in \mathbb{Z},$$

причем такое представление единственно, если $0 \le x \le q-1$.

Каждому числу z мы поставим в соответствие пару (x, y) чисел такую, что $0 \le x \le q-1$, $z = px + qy$. Разным числам соответствуют разные пары, причем z будет хорошим только при $y \le 0$. (Если $z = px + qy$ – хорошее число, то при $x = qt + r \ge 0$, $0 \le r \le q-1$, имеется представление $z = pr + q(y+t)$).

Теперь заметим, что если число $z = px + qy$, $0 \le x \le q-1$ – хорошее, то число $z' = (p-1-x)p + (1-y)q$ – плохое и, наоборот, если z – плохое, то z' – хорошее. Точки (x, y) и $(p-1-x, -1-y)$ симметричны относительно точки $(x_0, y_0) = \left(\frac{q-1}{2}, -\frac{1}{2}\right)$, а сами числа z и z' симметричны относительно точки

$$z_0 = px_0 + qy_0 = \frac{pq - p - q}{2},$$

т.к. $z + z' = pq - p - q = 2z_0 + c$.

Тем самым доказано а): хорошему числу z соответствует плохое число (симметричное ему) $c - z = z'$ и наоборот.

Так как наименьшее хорошее число 0, то наибольшим плохим будет c, а всего плохих чисел будет

$$\frac{c+1}{2} = \frac{(p-1)(q-1)}{2}.$$

Замечание. В статье [32] имеется решение, основанное на следующей геометрической интерпретации: пары (x, y) – точки плоской решетки, а $px + qy = z$ – проходящие через них прямые.

38. (*Материалы жюри международной олимпиады 1991 г.; предложена Ирландией*). Без ограничения общности можно считать, что $(a, b, c) = 1$; заметим, что $(a, b, c) = ((a, b), c)$.

Пусть $r = (a, b)$, тогда существуют целые α и β такие, что $a\alpha + b\beta = r$ и целые x и y такие, что $xr + yc = 1$. Так как $(\alpha, \beta) = 1$, то существуют такие γ и δ, что $y = \beta\gamma - \alpha\delta$.

Таким образом,

$$a = a(xr + yc) = axr + ac(\beta\gamma - \alpha\delta) =$$
$$= axr + ac\beta\gamma - c\delta(r - \beta\delta) = (ax - \delta c)r + \beta c(\alpha\gamma - b\delta);$$
$$b = b(xr + yc) = bxr + bc(\beta\gamma - \alpha\delta) =$$
$$= bxr + c\delta(r - a\alpha) - bc\alpha\delta = r(bx + \gamma c) - \alpha c(a\gamma + b\alpha);$$
$$c = c(xr + yc) = c(xr + c\beta\gamma - \alpha\delta c) =$$
$$= c[(a\alpha + b\beta)x + c\beta\gamma - \alpha\delta c] = c[(bx + \gamma c)\beta + \alpha(ax - \delta c)] =$$
$$= \beta c(bx + \gamma c) + \alpha c(ax - \delta c).$$

Полагая

$$p_1 = -(bx + \gamma c), \quad q_1 = ax - \delta c, \quad r_1 = \alpha\gamma - b\delta;$$
$$p_2 = \alpha c, \quad q_2 = -\beta c, \quad r_2 = \mathrm{r}$$

получаем нужные представления чисел a, b, c.

Пример. Если $a = 1$, $b = 9$, $c = 95$, то

$$1 = 191 \cdot 1 - 95 \cdot 2,$$
$$9 = 2 \cdot (-950) - 1 \cdot (-1909),$$
$$95 = (-1909) \cdot 95 - (-950) \cdot 191.$$

39. (*Ленинградская олимпиада 1986 года, см. [33]*)

1) *Ответ:* $A = -499$, $B = 500$ (одно из возможных решений).

Данное равенство изменяем в виде:

$$1001A + 999B = 1. \qquad (*)$$

Число 1001 и 999 взаимно просты; применяя алгоритм Евклида, имеем

$$1001 = 1 \cdot 999 + 2,$$
$$999 = 499 \cdot 2 + 1.$$

Поэтому

$$999 = 499(1001 - 999) + 1$$

или

$$(-499) \cdot 1001 + 500 \cdot 999 = 1. \qquad (**)$$

Замечание. Все целочисленные решения уравнения $(*)$ задается формулами

$$A = -499 + 999n,$$
$$B = 500 - 1001n,$$

где n – целое число.

Во-первых, нетрудно проверить, что такие A и B при любом фиксированном n, удовлетворяют уравнению (*). Чтобы доказать, что это все решения, вычтем из (*) равенство (**); получим

$$1001(A + 499) = 999(500 - \mathrm{B}),$$

откуда $999 \mid (A + 499)$ и $1001 \mid (500 - B)$, т. к. $(999, 10001)$.

Справедлива следующая

Теорема. *Для того, чтобы уравнение $ax + bx = c$ имело решение в целых числах (x, y) необходимо и достаточно, чтобы $d =$ НОД$(a, b) \mid c$, если это выполнено и (x_0, y_0) одно из решений этого уравнения, то все его решения задаются формулами*

$$x = x_0 + b_1 t, \quad y = y_0 - a_1 t_1,$$

$$\text{где } a_1 = a / d,\ b_1 = b / d.$$

Отметим, что для отыскания частного решения (x_0, y_0) можно использовать теорему о линейном представлении наибольшего общего делителя (a, b) (см. решение задачи 34).

2) *Ответ:* $A = -499$, $B = -1$, $C = 501$.

Данное уравнение имеет вид:

$$1000 \cdot 1001 \cdot A + 999 \cdot 1001 \cdot B + 999 \cdot 1000 \cdot C = 1$$

$$1000 \cdot (1001 \cdot A + 999 \cdot (B + C) + 999 \cdot B = 1$$

Используя уравнение (*), имеем:

$$A = -499, \quad C + \mathrm{B} = 500, \quad B = -1.$$

Данный набор чисел удовлетворяет условию задачи.

Замечание. Общая теория решения уравнений в целых числах вида

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n + \ldots = b \qquad \textbf{(*)}$$

изложена в [34], [35], [19], [16], основу которой составляет возможность сведения к отысканию решений линейных уравнений с двумя неизвестными. Много задач с решениями содержатся в [42].

Теорема. *Пусть $d = (a_1, a_2, \ldots, a_n)$. Уравнение (*) имеет решение тогда и только тогда, когда $d \mid b$. Уравнение (*) либо не имеет решений, либо имеет бесконечно много решений.*

Отыскание частного решения уравнение (*) связано с возможностью представления наибольшего общего делителя $d = (a_1, a_2, \ldots, a_n)$ в виде (*).

Отметим также, что если x_1', x_2', … , x_k' – решение (*), то

$$x_1' + a_2 n, \quad x_2' - a_1 n, \quad x_3', \quad \ldots, \quad x_k'$$

при любом целом n также является решением уравнения (*).

40. 1) $x = 17 + 37n$, $y = 20 + 45n$ $(n \in \mathbb{Z})$;

2) $x = 22 + 37n$, $y = -25 + 43n$ $(n \in \mathbb{Z})$;

3) $x = -40 + 81n$, $y = 49 - 109n$ $(n \in \mathbb{Z})$;

4) $x = 8 + 181n$, $y = -11 - 249n$ $(n \in \mathbb{Z})$;

5) Данное уравнение имеет решение, т.к. $(208, 136) = 8$ и число 8 делит 120. Имеем:

$$26x + 17y = 15.$$

Найдем сначала, т. к. $(26, 17) = 1$, решение уравнения

$$26x + 17y = 1.$$

Используя алгоритм Евклида для чисел 26 и 17, имеем:

$$26 = 17 \cdot 1 + 9,$$
$$17 = 9 \cdot 1 + 8,$$
$$9 = 8 \cdot 1 + 1,$$
$$1 = 1 \cdot 1.$$

Найдем отсюда линейную комбинацию чисел 26 и 17, для представления их $(26, 17) = 1$. Получим:

$$26 \cdot 2 - 17 \cdot 3 = 1.$$

Умножая на 15, получим одно из решений: $x = 30$, $y = -45$.

Таким образом, общее решение исходного уравнения дается равенствами:

$$x = 30 + 17n, \quad y = -45 - 27n \quad (n \in \mathbb{Z}).$$

6) Используя алгоритм Евклида, можно найти частное решение уравнения $1726x + 1229y = 1$, т. к. $(1726, 1229) = 1$; получим: $x = -445$, $y = 639$.

Умножая на 3, получим частное решение данного уравнения: $x = -1335$, $y = 1917$. Общее решение дается формулами: $x = -1335 + 1335n$, $y = 1917 - 1726n$ $(n \in \mathbb{Z})$.

7) Решений нет, т. к. $(100, 72, 90) = 2$ и $(2, 11) = 1$.

8) Так как $(100, 72, 90) = 2$, то имеем:

$$50x + 36y + 75z = 3.$$

Найдем частное решение уравнения $50x + 36y + 75z = 1$. Для этого рассмотрим сначала уравнение $50x + 36y = 2$, т. к. $(50, 36) = 2$. Для отыскания решения последнего уравнения рассмотрим уравнение $25x + 18y = 1$, которое имеет решение $x = -5$, $y = 7$ (его можно найти при помощи алгоритма Евклида).

Итак, уравнение $50x + 36y = 2$ имеет решение $x = -10$, $y = 14$.

Следующим шагом мы решим уравнение

$$2n + 45z = 1,$$

которому удовлетворяют, например, $z = 1$, $n = -22$.

Таким образом, числа $x = 110$, $y = -154$, $z = 1$ удовлетворяют уравнению

$$50x + 36y + 75z = 1.$$

Наконец, числа $x = 330$, $y = -462$ и $z = 3$ является частным решением данного уравнения.

Замечание. В случае двух неизвестных, зная частное решение линейного уравнения, легко найти общее решение, т.е. все решения. Для случая трех переменных ситуация сложнее. Возможный способ получения общего решения мы покажем на примере уравнения $50x + 36y + 75z = 3$ (Применение теории уравнений см. [34], [51]).

Имеем:

$$y = \frac{3-50x-45z}{36} = -x - z + \frac{3-14x-9z}{36}.$$

Таким образом, $h = \dfrac{3-14x-9z}{36}$ – целое число. Выражая z из последнего равенства, найдем, что

$$z = -4h - 2x + \frac{3+4x}{9}$$

Таким образом, $m = \dfrac{3+4x}{9}$ – целое число и

$$x = 2m + \frac{m-3}{4}.$$

Следовательно, $n = \dfrac{m-3}{4}$ – целое число и $m = 4n + 3$.

Подставляя, найдем общее решение исходного уравнения:

$$\begin{cases} x = 9n+6, \\ y = 5l+5n+3, \quad (l,\ n \in \mathbb{Z}). \\ z = -4l-14n \end{cases}$$

41

41. (*См. [1]*) *Ответ:* 86001.

Искомое число имеет вид:

$$n = 1000x + 1 = 761y + 8,$$

откуда

$$1000x - 761y = 7.$$

Частное решение этого уравнения можно найти, используя алгоритм Евклида, $x = 847$ и $y = 1113$. Тогда общее решение дается формулами:

$$x = 847 - 761n, \quad y = 1113 - 1000n \quad (n \in \mathbb{Z}).$$

Наименьшее положительное решение получаем при $n = 1$.

42. (*См. [1]*) *Ответ:* 8 решений.

Так как (10, 28) = 2, то

$$5x + 14y = 620.$$

Используя алгоритм Евклида, найдем частное решение уравнения $5x + 14y = 1$; получим $x = 3$, $y = -1$. Таким образом, общее решение данного уравнения: $x = 1860 - 14n$, $y = -620 + 5n$ ($n \in \mathbb{Z}$).

Чтобы получить положительное решение, нужно, чтобы

$$n < \frac{1860}{14} = 132\frac{6}{7}, \quad n < 124.$$

или $125 \le n \le 132$.

43. Рассмотрим последовательность чисел Фибоначчи:
$F_1 = F_2 = 1, \quad F_{n+1} = F_n + F_{n-1}, \quad n \ge 2.$

Тогда для нахождения (F_{n+1}, F_n), $n > 2$ – фиксировано, при помощи алгоритма Евклида имеем:

$$\begin{gathered} F_{n+1} = 1 \cdot F_n + F_{n-1}, \\ F_n = 1 \cdot F_{n-1} + F_{n-2}, \\ \dots\dots\dots\dots\dots\dots \\ F_3 = 1 \cdot F_2 + F_1, \\ F_2 = 1 \cdot F_1 \end{gathered}$$

Таким образом, $(F_{n+1}, F_n) = 1$ при всех $n = 1, 2, \dots$ и алгоритм Евклида имеет n шагов.

Замечание. См. также задачу из §3, а также книгу [9], где имеется много арифметических свойств последовательности чисел Фибоначчи. Приведем без доказательства некоторые из них:

1) $F_{p+q} = F_{p-1}F_q + F_pF_{q+1}, \quad p, q \in \mathbb{N}$;

2) Если $q \mid p$, то $F_q \mid F_p, \quad p, q \in \mathbb{N}$.

44. См. решение задачи 3 ниже, а также книгу [9].

45. Пусть $d = (n, m)$, тогда существует такие числа x и y, что

$$d = nx + my.$$

Из известного равенства (см. замечание к решению задачи 43, а также книгу [9])

$$F_{r+s} = F_{s-1}F_r + F_sF_{r+1}.$$

Получим тогда, что

$$F_{(n,m)} = F_d = F_{nx-1}F_{my} + F_{nx}F_{my+1}.$$

Пусть k – любой общий делитель чисел F_n и F_m. Так как F_{nx} делится на F_k (см. [9]), то F_{nx} делится на k, аналогично F_{my} делится на k. Поэтому число F_d делится на любой общий делитель чисел F_n и F_m, что и требовалось доказать.

Замечание. 1) Другие доказательства см. в [9].

2) Частные случаи этой задачи встречаются во многих источниках (см., например, [12] для $m = 1000$ и $n = 770$ и др).

Мы укажем на статью Глена Микаэля в «The Fibonacci Quarterly», 1964, pp. 57–58, а также книгу [37], где имеются и другие арифметические свойства последовательности чисел Фибоначчи и других более общих последовательностей.

46. См., в частности, [57] и [13], [40], [43].

Последовательность чисел Ферма начинается с чисел 3, 5, 17, 257, 65537, … . Они удовлетворяют рекуррентному соотношению

$$F_n = F_0 F_1 \dots F_{n-1} + 2,$$

что легко устанавливается по индукции (другой способ доказательства см. в [57]).

Из этого соотношения следует, что если $m < n$, то

$$F_n = F_0 F_1 \dots F_m \dots F_{n-1} + 2.$$

Следовательно, любой общий делитель чисел F_n и F_m должен быть делителем числа 2. Такой общий делитель равен 1 или 2. Но он не может быть равен 2, так как все числа Ферма нечетны.

47. См. [58], с. 324, а также [54]. Пусть

$$\begin{cases} a = bq_1 + r_1, & 0 < r_1 < b \\ b = r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 = r_2 q_3 + r_3, & 0 < r_3 < r_2 \\ \dots\dots\dots\dots & \dots\dots\dots\dots \\ r_{n-2} = r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1}, & r_{n+1} = 0 \end{cases}$$

Наибольшее число операций будет в том случае, если
$q_1 = q_2 = \dots = q_n = q_{n+1} = 1$.
Пусть $\{F_k\}$ – последовательность чисел Фибоначчи: $F_0 = 0$, $F_1 = F_2 = 1$, $F_k = F_{k-1} + F_{k-2}$, $k > 2$. Тогда в алгоритме Евклида будем иметь:

$$r_{n+1} = F_0, \quad r_n \ge F_1,$$
$$r_{n-1} \ge F_2, \quad r_{n-2} \ge F_3, \quad \dots ,$$
$$r_2 \ge F_{n-1}, \quad r_1 \ge F_n, \quad b \ge F_{n+1}.$$

Имеем (см. [9], формула Бинэ):

$$F_k = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right], \quad k = 0, 1, 2, \dots .$$

Так как

$$\left|\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right| < 2, \quad n = 0, 1, 2, \dots ,$$

а числа F_n – целые, то из формулы видно, что F_{n+1} является ближайшим целым числом к числу

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}.$$

Также ясно, что

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}$$

отстоит меньше, чем на $\frac{1}{2}$ от ближайшего целого числа; поэтому не может быть справедливо равенство

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} = b + \frac{1}{2}, \quad n = 0, 1, 2, \dots .$$

Тогда мы имеем неравенство:

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} < b + \frac{1}{2}$$

(чтобы ближайшее целое число не превосходило b).

И наоборот ясно, что если

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} < \mathrm{b} + \frac{1}{2},$$

то ближайшее целое будет меньше либо равно b.

Поэтому неравенство $F_{n+1} \le b$ выполняется тогда и только тогда, когда

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} < b + \frac{1}{2}$$

или

$$(n+1)\lg\left(\frac{1+\sqrt{5}}{2}\right) < \lg\left\{\left(b+\frac{1}{2}\right)\sqrt{5}\right\},$$

т.е. при

$$n + 1 < \frac{\lg\left\{\left(b+\frac{1}{2}\right)\frac{1}{\sqrt{5}}\right\}}{\lg\left(\frac{1+\sqrt{5}}{2}\right)}$$

отношение логарифмов справа не может быть целым числом. Действительно, если предположить, что оно равно k, $k \in \mathbb{Z}$, то мы получили бы, что

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k = b + \frac{1}{2},$$

что противоречит полученным выше результатам.

Таким образом, максимальное число шагов $(n + 1)$ в алгоритме Евклида равно

$$\left[\frac{\lg\left\{\left(b+\frac{1}{2}\right)\sqrt{5}\right\}}{\lg\left(\frac{1+\sqrt{5}}{2}\right)}\right],$$

где $[x]$ – целая часть числа x, т. е. наибольшее целое число, не превосходящее x.

Замечание 1. Заметим, что одновременно мы нашли число различных чисел Фибоначчи, не превосходящих данного натурального числа N. Оно равно $n – 1$, где

$$n = \left[\frac{\lg\left\{\left(b+\frac{1}{2}\right)\sqrt{5}\right\}}{\lg\left(\frac{1+\sqrt{5}}{2}\right)}\right];$$

подробности см. в [57].

Замечание 2. Из проведенного анализа не трудно получить теорему Ламе: число операций последовательных делений в алгоритме Евклида для нахождения (a, b), $a > b$, меньше $5p$, где p – число цифр в десятичной записи числа b, т. е. имеет место следующее неравенство Ламе: $m + 1 < 5p$. (См. [58]).

Замечание 3. Обозначим через $N(a, b)$ число шагов алгоритма Евклида, примененного к натуральным числам a и b. Нами показано, что

$$N(a, b) \le \left[\lg_{\varphi}\sqrt{5}\left(\min(a,b)+\frac{1}{2}\right)\right],$$

где $\varphi = \frac{1+\sqrt{5}}{2}$ – так называемое «золотое сечение». Эта оценка достижима (см. решение задачи 43 для числа $a = F_{n+1}$, $b = F_n$).

По поводу оценок для $N(a, b)$ и другой величины $M(a, b)$ – суммы всех неполных частных в алгоритме Евклида см. задачу 3 ниже, а также статью С.Б. Гашкова [61].

Отметим здесь неравенство из [61]

$$M(a,\ b) \geq \left[\lg_{\varphi} \sqrt{5} \left(\max(a,b) - \frac{1}{2} \right) \right] - 1$$

и подчеркнем, что с геометрической точки зрения сумма всех неполных частных в алгоритме Евклида является числом квадратов, которым накрывается без наложений прямоугольник $a \times b$.

Замечание 4. Данной проблематике уделяется много внимания: см., например, [54], [59], [60], [62].

48. 1) Этим вопросом впервые заинтересовался немецкий математик Кронекер; использованные здесь примеры заимствованы из книги [1], с. 42–44.

Доказательство нужного утверждения проводится «слово в слово» как и при доказательстве теоремы Евклида.

2) а)

$139 = 2 \cdot 49 + 41$
$49 = 1 \cdot 41 + 8$
$41 = 5 \cdot 8 - 1$
$8 = 1 \cdot 8$

$139 = 3 \cdot 49 - 8$
$49 = 49 \cdot 1$

б)

$1472 = 1 \cdot 1124 + 348$
$1124 = 3 \cdot 348 + 80$
$348 = 4 \cdot 80 + 28$
$80 = 2 \cdot 28 + 16$
$28 = 1 \cdot 16 + 12$
$16 = 1 \cdot 12 + 4$
$12 = 3 \cdot 4$

$1472 = 1 \cdot 1124 + 348$
$1124 = 3 \cdot 348 + 80$
$348 = 4 \cdot 80 + 28$
$80 = 3 \cdot 28 - 4$
$28 = 7 \cdot 4$

в)

$18416 = 1 \cdot 17296 + 1120$
$17296 = 15 \cdot 1120 + 496$
$1120 = 2 \cdot 496 + 128$
$496 = 3 \cdot 128 + 112$
$128 = 1 \cdot 112 + 16$
$112 = 7 \cdot 16$

$18416 = 1 \cdot 17296 + 1120$
$17296 = 15 \cdot 1120 + 496$
$1120 = 2 \cdot 496 + 128$
$496 = 4 \cdot 128 - 16$
$128 = 8 \cdot 16$

3) См. примеры из п. 2 этой задачи.

ЛИТЕРАТУРНЫЕ ИСТОЧНИКИ

[1] ORE O. *Number theory and its history.* – McGrow-Hill Book Company, Inc., New York, 1948.

[2] *Венгерские математические олимпиады.* Под редакцией Алексеева В.М. –М.: Мир, 1976.

[3] Зубулевич Г. И. *Сборник задач московских математических олимпиад (V-VIII классы)*. –М.: Просвещение, 1967.

[4] В мире математики, выпуск 18, Киев, 1987 (статья И.Г. Габовича, на украинском языке).

[5] Гальперин Г.А., Толпыго Л.К. *Московские математические олимпиады*. Под ред. Колмогорова А.Н. –М.: Просвещение, 1986.

[6] Сборник задач московских математических олимпиад. Составитель Леман Л.Л., под ред. Болтянского В.Г. –М.: Просвещение, 1965.

[7] Калужнин Л.А. Основы теории арифметики. –М.: Наука, 1969.

[8] Francisco Belld Rosado, Ma Victoria Davan Miguel, Felix Lopez Fernandes-Asenjo. Olimpiada matematica Uratola; problemas propuestas en el districto universitario de Valladdid, – Valladdid: Instituto de Crenctas de la Educacion, Universidad, 1992.

[9] Воробьев Н.Н. Числа Фибоначчи, –М.: Наука, 1983.

[10] Оре О. Приглашение в теорию чисел, –М.: Наука, 1980.

[11] Бельский Л.А., Калужнин Л.А. Деление с остатком, –Киев: Вища школа, 1977.

[12] Дынкин Е.Б., Молчанов С.А., Розенталь А.Л., Толпыго А.К. Математические задачи. –М.: Наука, 1971.

[13] Серпинский В. 250 задач по элементарной теории чисел. –М.: Просвещение, 1968.

[14] Избранные задачи (из журнала American Mathematical Mouthly). –М.: Мир, 1988.

[15] Вагутен В.Н. Алгоритм Евклида и основная теорема арифметики. –Журнал «Квант», 1972, №2, стр. 30-35.

[16] Воробьев Н.Н. Признаки делимости. –М.: Наука, 1963.

[17] Башмаков М.Н. Нравится ли вам возиться с целыми числами. – Журнал «Квант», 1971, №3. Гельфанд А.О. Решение уравнений в целых числах. –М.: Наука, 1983.

[18] Радемахер Г., Теплиц О., Числа и фигуры. –М.: Физматгиз, 1962.

[19] Уфнаровский В.А. Математический аквариум. –Кишинев: Штиница, 1987.

[20] Reviste Gaceta Matematica, Real Sociedad Matematice Espanola, 2[a] Serie, v.1, №2, 1985.

[21] Reviste Gaceta Matematica, Real Sociedad Matematice Espanola, 2[a] Serie, v.1, №1, 1988.
[22] Васильев Н.Б., Гутенмахер В.Л., Раббот Ж.М., Тоом А.Л. Заочные математические олимпиады. –М.: Наука, 1986.
[23] Вагутен Н. Арифметические препятствия. –Журнал «Квант», 1979, №3, стр. 22-31.
[24] Васильев Н.Б., Егоров А.А. Задачи всесоюзных математических олимпиад. –М.: Наука, 1988.
[25] 260 problemas de Matematicas, Departamento de Matematicas de la Universidad Nacional de San Luis, Argentina, 1992.
[26] Вышинский В.А., Карташов Н.В., Михайловский В.И., Ядренко М.И. Сборник задач киевских математических олимпиад. –Киев: Вища школа, 1984.
[27] Яковлев Г.Н., Купцов Л.П., Резниченко С.В., Гусятников П.Б. Всероссийские математические олимпиады школьников. –М.: Просвещение, 1992.
[28] USA Mathematical Olimpiads 1972-1986. Compiled and with solutions by Murray S.Klamkin, Neir Mathematical library, Math. Association of Amtrica. –Washington, 1988.
[29] Полиа Г., Сеге Г. Задачи и теоремы из анализа, т.2. –М.: Наука, 1978.
[30] Зарубежные математические олимпиады. Кол. Авторов под ред. И.Н.Сергеева. –М.: Наука, 1987.
[31] American Mathematical Moutly, 1955, v.62, p.657.
[32] Журнал «Квант», 1973, №11, решение задачи М194.
[33] Фомин Д.Д. Задачи ленинградских математических олимпиад. –Ленинград, 1990.
[34] Сергиенский В. О решении уравнений в целых числах. –М.: Физматгиз, 1961.
[35] Бухштаб А.А. Теория чисел. –М.: Учпедгиз, 1960.
[36] Арнольд И.В. Теория чисел. –М.: Учпедгиз, 1939.
[37] Honsberger R. Mathematical Gems III, the Mathematical Association of America, 1985.
[38] Кудреватов Г.А. Сборник задач по теории чисел. –М.: Просвещение, 1970.
[39] Грибанов В.Ч., Титов П.И. Сборник упражнений по теории чисел. –М.: Просвещение, 1964.
[40] Серпинский В. Что мы знаем и чего мы не знаем о простых числах. –М.-Л.: Физматгиз, 1963.
[41] Нивен А. Числа рациональные и иррациональные. –М.: Мир, 1966.

[42] Диксон Л.Е. Введение в теорию чисел. –Тбилиси: Изд. АН Груз.ССР, , 1941.
[43] Шнирельман Л.Г. Простые числа. –М.-Л.: Гостехиздат, 1940.
[44] Дэвэнпорт Г. Высшая арифметика. –М.: Наука, 1965.
[45] Трост Э. Простые числа. –М.: Физматгиз, 1959.
[46] Крамер В.А. Задачник по алгебре. –М.-Л.: Гостехиздат, 1950.
[47] Берман Г.Н. Число и наука о нем. –М.: Физматгиз, 1960.
[48] Шклярский Д.О. и др. Избранные задачи и теоремы элементарной математики, часть I. –М.: Гостехиздат, 1954.
[49] Хинчин А.Я. Элементы теории чисел. –М.-Л.: Гостехиздат, 1951.
[50] Хинчин А.Я. Цепные дроби. –М.: Наука, 1978.
[51] Виноградов И.М. Основы теории чисел. –М.: Наука, 1972.
[52] Лежен-Дирихле П.Г. Лекции по теории чисел. –М.-Л.: Гостехиздат, 1936.
[53] Башмакова И.Г. Диофант и диофантовы уравнения. –М.: Наука, 1972.
[54] Кнут Д. Искусство программирования для ЭВМ, т.1-3. –М.: Мир, 1976-1978.
[55] Курант Р., Роббинс Г. Что такое математика. –М.: Просвещение, 1968.
[56] Клейн Ф. Элементарная математика с точки зрения высшей: в 2-х томах, т.1. Арифметика. Алгебра. Анализ. –М.: Наука, 1987.
[57] Хансбергер Р. Математические изюминки. –М.: Наука, 1992.
[58] Гельфонд А.О. Исчисления конечных разностей. –М.: Наука, 1967.
[59] Felix Lopez Fernandez-Asenjo, Juan Tena Aynso. Introduccion a la teoria de numeras primos: Cospectos algebraicos oy analiticos. –Valladolidi Instituto de Cicucras de la Educacion, Universidad, 1998.
[60] Hardy G.H., Wright E.M. An introduction to the Theory of Numbers, Oxford, 1971.
[61] Журнал «Квант», №2, 1994.
[62] Uspensky J.V., Heasalet M.A. Elementary Number Theory, McGraw – Hill Book Company, Inc., New York, 1939.
[63] Дьюдени Г.Э. 520 головоломок. –М.: Мир, 1975.
[64] Гашков С.Б. Журнал «Квант», 6(1998).
[65] American Mathematical Mouthly, 1962, v.69, N5, p.454.
[66] Mathematics Magazine, 1962, v.35, p.311.
[67] Тригг Ч. Задачи с изюминкой. –М.: Мир, 1975.
[68] Mathematics and Informatics Quarterly, v.3, N4, 1993.
[69] Журнал «Квант», 1991, №9; задача М1280.
[70] Mathematics Magazine, 1956, v.29, p.173.

[71] Болл У., Коксетер Г. *Математические эссе и резвлечения.* –М.: Мир, 1986.
[72] American Mathematical Mouthly, 1921, v.28, а также этот же журнал за 1922 г, v.29.
[73] Математика в школе, 1948, №3.
[74] Башмаков М.И., Беккер Б.М., Гольховой В.М. Задачи по математике. Алгебра и анализ. –М.: Наука, 1982.
[75] Mathematics Magazine, 1970, v.43, N1 p.56.
[76] The Wohascum Country Problem Book, George T.Gilbert, Mark I. Krusemeyer, Loren C.Larson, Dolsiani Mathematical Expositions, The Matematical Association of America, 1993.
[77] В.А. Колосов, Теоремы и задачи алгебры, теории чисел и комбинаторики. –М.: Гелиос АРВ, 2001.-256с.
[78] С.Б. Гашков, Современная элементарная алгебра в задачах и упражнениях. –М.: МЦНМО, 2006-328с.
[79] Н.Б. Алфутова, А.В. Устинов, Алгебра и теория чисел. Сборник задач. – М. МЦНМО: 2002.
[80] С.Б. Гашков, В.Н. Чубариков, Арифметика. Алгоритмы. Сложность вычислений. –М. Высшая школа, 2002.
[81] В.В. Вавилов, А.В. Устинов, Многоугольники на решетках. _ М.: МЦНМО, 2006, -72с.

Валерий Васильевич ВАВИЛОВ

Многоликий алгоритм Евклида

Специализированный учебно-научный центр (факультет)
Московского государственного университета имени М.В. Ломоносова
Школа имени академика А.Н. Колмогорова

Кафедра математики
127357 Москва, ул. Кременчугская, 11
тел. 445 –4054
электронный адрес: vvavilov1@yandex.ru