Глава 1

Целые, рациональные и действительные числа

1.1. Деление с остатком

1. Каждое из чисел ± 23, ± 4 разделите с остатком на каждое из чисел ± 5.

2. Найдите все положительные делители числа 42.

3. Сейчас 13 часов. Какое время суток будет через 64 часа?

4. Сегодня пятница. Какой день недели будет через 24 дня?

5. 1 января некоторого года приходится на понедельник. Какой день недели будет

1) 31 января этого года;
2) 28 февраля этого года;
3) 1 января следующего года?

6. Пусть k — целое число. Доказать, что каждое из следующих чисел делится на 6: $k(k+1)(2k+1)$, $k^3 - k$, $k^3 + 17k$.

7. Rata Die (RD) — это порядковый номер дня нашей эры по продленному в прошлое григорианскому календарю[1]. День первый — это 1 января 1 г. н. э.

1) Объясните, почему Rata Die можно вычислить по следующим формулам (удобным для программирования):

$$\mathrm{RD} = D + \left\lfloor \frac{153m+2}{5} \right\rfloor + 365y + \left\lfloor \frac{y}{4} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor + \left\lfloor \frac{y}{400} \right\rfloor - 306,$$

где

$$a = \left\lfloor \frac{14-M}{12} \right\rfloor, \qquad y = Y - a, \qquad m = M + 12a - 3,$$

Y — год нашей эры, M — номер месяца, D — порядковый номер дня в месяце;

[1]Rata Die — *от фиксированной даты* (лат.). Согласно григорианскому (т. е. современному) календарю, год y — високосный $\Leftrightarrow$ $y \bmod 4 = 0$, но при этом $y \bmod 100 = 0$ и $y \bmod 400 \neq 0$. Например, 2000 г. — високосный, а 1900 и 2100 — обычные (не високосные) года.

2) зная, что 1 января 1 г. был понедельник, объясните, как найти день недели для произвольной даты нашей эры; проверьте этот алгоритм на датах, для которых вы знаете, на какой день недели они приходились (например, для сегодняшней даты);
3) покажите, что обратный переход от RD к дате можно осуществить по следующим формулам:

$$Y = 100c + y + \left\lfloor \frac{m}{10} \right\rfloor, \quad M = m + 3 - 12 \left\lfloor \frac{m}{10} \right\rfloor, \quad D = d - \left\lfloor \frac{153m + 2}{5} \right\rfloor + 1,$$

где

$$c = \left\lfloor \frac{4\,\mathrm{RD} + 1223}{146097} \right\rfloor, \quad b = \mathrm{RD} + 305 - \left\lfloor \frac{146097c}{4} \right\rfloor, \quad y = \left\lfloor \frac{4b + 3}{1461} \right\rfloor,$$

$$d = b - \left\lfloor \frac{1461y}{4} \right\rfloor, \qquad m = \left\lfloor \frac{5d + 2}{153} \right\rfloor.$$

1.2. Наибольший общий делитель

8. Найдите НОД(42, 60), НОД(220, 273).

9. Алгоритмом Евклида найдите НОД и его линейное представление для чисел
1) 89, 24; 2) 156, 69; 3) 691, 103.

10. Доказать, что коэффициенты u, v в линейном представлении НОД $ua+vb = d$, где $d = \mathrm{НОД}(a, b)$, можно выбрать так, что

$$|u| < \frac{|b|}{d}, \qquad |v| < \frac{|a|}{d}.$$

11. Докажите, что
1) $\mathrm{НОК}(a, b) = \dfrac{ab}{\mathrm{НОД}(a, b)}$;
2) $\mathrm{НОК}(a, b, c) = \dfrac{abc\,\mathrm{НОД}(a, b, c)}{\mathrm{НОД}(a, b)\,\mathrm{НОД}(a, c)\,\mathrm{НОД}(b, c)}$.

12. Докажите, что
1) $\mathrm{НОД}(a_1, a_2, \ldots, a_s) = \mathrm{НОД}(a_1, \mathrm{НОД}(a_2, \ldots, a_s))$;
2) если $d = \mathrm{НОД}(a_1, a_2, \ldots, a_s)$, то найдутся целые $u_1, u_2, \ldots, u_s$, такие, что $d = u_1a_1 + u_2a_2 + \cdots + u_sa_s$.

13. (р) Уравнение, в котором неизвестные должны принимать только целые значения, называется *диофантовым*. Рассмотрим линейное диофантово уравнение от двух неизвестных $ax + by = c$, где $a, b, c \in \mathbb{Z}$. Обозначим $d = \mathrm{НОД}(a, b)$. Доказать, что
1) если уравнение $ax + by = c$ совместно (в целых числах), то $c \vdots d$;

2) если $c \vdots d$, то общее решение (в целых числах) этого уравнения имеет вид

$$x = \frac{uc}{d} + \frac{tb}{d}, \qquad y = \frac{vc}{d} - \frac{ta}{d} \qquad (t \in \mathbb{Z}),$$

где u, v — произвольные коэффициенты Безу для чисел a и b, т. е. произвольные целочисленные решения уравнения $au + bv = d$. Отсюда также следует, что прежде чем решать уравнение исходное уравнение, разумно его сократить на $d = \text{НОД}(a, b)$.

14. Найти общее решение в целых числах уравнения:

1) $7x - 5y = 19$; 2) $7x - 13y = 23$;

3) $9x - 15y = 57$; 4) $89x + 24y = 3$.

15. Найти общее решение системы диофантовых уравнений:

1) $\begin{cases} x + y - 3z = -1, \\ x + 2y + 2z = 0; \end{cases}$ 2) $\begin{cases} x + y + z = 10, \\ 8x + 3y + z = 13. \end{cases}$

16. Задача Алкуина из «Propositiones ad Acuendos Juvenes». Некто купил 100 свиней за 100 денариев, причем каждого хряка покупал по 10 денариев, свиноматку — по 5 денариев, а поросенка — по $\frac{1}{2}$ денария. Сколько было куплено хряков, свиноматок и поросят?

17. Задача из «Арифметики» Л. Ф. Магницкого. Купил некто на 80 алтын гусей, уток и чирков. Гуся покупал по 2 алтына, утку — по 1 алтыну, чирка же — по 3 деньги[2], а всех куплено 80 птиц. И ведательно есть, сколько которых птиц купил.

18. Задача из «Занимательной алгебры» Я. И. Перельмана. Требуется на 1 руб. купить 40 штук почтовых марок: копееченых, 4-копеечных и 12-копеечных. Сколько окажется марок каждого достоинства?

19. На плоскости дан угол в 13°. С помощью циркуля и линейки построить угол в 1°.

20. Пусть в результате применения алгоритма Евклида к числам a, b получается последовательность неполных частных $q_1, q_2, \ldots, q_{s+1}$. Докажите, что тогда

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_s + \cfrac{1}{q_{s+1}}}}}$$

Дробь такого вида называется *цепной* (или *непрерывной*) *дробью*. Если цепную

[2] 1 алтын = 3 копейки = 6 денег.

дробь оборвать на k-м шаге, получим k-ю *подходящую дробь* α_k к числу $\dfrac{a}{b}$:

$$\alpha_1 = q_1, \quad \dots, \quad \alpha_k = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}, \quad \dots, \quad \alpha_{s+1} = \frac{a}{b}.$$

21. Указанное рациональное число записать в виде цепной дроби и найти все подходящие дроби:

1) $\dfrac{89}{24}$; 2) $\dfrac{156}{69}$; 3) $\dfrac{691}{103}$; 4) $\dfrac{21}{13}$.

22. Записать иррациональное число, представимое в виде бесконечной периодической цепной дроби:

1) $1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{3 + \dots}}}}}$; 2) $1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \dots}}}}}$.

23. Разложить в бесконечную цепную дробь следующие иррациональные числа:

1) $\sqrt{2}$; 2) $\dfrac{1+\sqrt{5}}{2}$; 3) $\dfrac{1+\sqrt{2}}{2}$; 4) $\dfrac{1+\sqrt{3}}{2}$; 5) $\dfrac{2+\sqrt{10}}{2}$.

24. Разложить в бесконечную цепную дробь:

1) $\sqrt{n^2+1}$, $n \in \mathbb{N}$; 2) $\sqrt{n^2-1}$, $n \in \mathbb{N}$.

25. Число $\tau = \dfrac{1+\sqrt{5}}{2}$ называется *золотым сечением*. Доказать, что k-я подходящая дробь к нему равна F_{k+1}/F_k, где F_k — k-й элемент *последовательности чисел Фибоначчи*: $F_0 = 0$, $F_1 = 1$, $F_{k+2} = F_{k+1} + F_k$ $(k = 0, 1, 2, \dots)$. Вычислить первые шесть подходящих дробей с 5 знаками после десятичной запятой.

26. Вывести формулы для подходящих дробей к числу τ^{-1}, обратному золотому сечению.

27. Начальный фрагмент разложения числа π в цепную дробь имеет вид:

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \ldots}}}}}.$$

Вычислить первые 5 подходящих дробей к числу π.

28. Пусть $\psi(a, b)$ — количество операций деления в алгоритме Евклида, примененном к целым числам a, b. Доказать, что

1) $\psi(F_{k+2}, F_{k+1}) = k$, где F_k — k-й элемент последовательности Фибоначчи;
2) $F_k = \dfrac{1}{\sqrt{5}}\left(\tau^k - (-\tau)^{-k}\right)$, где $\tau = \dfrac{1+\sqrt{5}}{2}$ — золотое сечение;
3) если $\psi(a, b) = k$, $a > b > 0$, то $a \geq F_{k+2}$, $b \geq F_{k+1}$;
4) если $a > b > 0$, то $\psi(a, b) = 1 + \log_\tau b \approx 5 \lg b$ (*теорема Ламэ́*).

29. Алгоритм Евклида — не единственный быстрый алгоритм нахождения НОД. *Бинарный алгоритм* основан на следующих утверждениях. Пусть a, b натуральные числа. Докажите, что

1) если a, b четны, то $\text{НОД}(a, b) = 2\,\text{НОД}(a/2,\, b/2)$;
2) если a четно, а b нечетно, то $\text{НОД}(a, b) = 2\,\text{НОД}(a/2,\, b)$;
3) если a, b нечетны, то $\text{НОД}(a, b) = 2\,\text{НОД}\,((a-b)/2,\, b)$.

30. Докажите, что количество итераций в бинарном алгоритме нахождения НОД двух натуральных чисел a и b не превосходит $\log_2 a + \log_2 b$.

31. Применяя бинарный алгоритм, доказать: $\text{НОД}(2^m - 1,\, 2^n - 1) = 2^{\text{НОД}(m,n)} - 1$.

32. Докажите, что $\text{НОД}(a^m - 1,\, a^n - 1) = a^{\text{НОД}(m,n)} - 1$ для любого целого $a \neq 1$.

33. Пусть a, b, n — натуральные числа, $\text{НОД}(a, b) = 1$. Задача решения уравнения $ax + by = n$ в *неотрицательных* целых числах называется *задачей о размене*. Доказать, что

1) если $n \geq (a-1)(b-1)$, то уравнение совместно в неотрицательных целых числах;
2) если $n = (a-1)(b-1) - 1 = ab - a - b$, то уравнение не имеет неотрицательных целых решений.

Таким образом, число $ab - a - b$, называемое *числом Сильвестра*, — это максимальное значение n, для которого уравнение $ax + by = n$ не совместно в неотрицательных целых числах. Доказать, что

3) если $1 \leq n < ab$ и $n \not\vdots a$, $n \not\vdots b$, то из уравнений $ax+by = n$ и $ax+by = ab-n$ имеет целое неотрицательное решение ровно одно;
4) при $1 \leq n \leq (a-1)(b-1)$ уравнение $ax+by = n$ совместно в неотрицательных целых числах ровно для половины, т. е. $\dfrac{(a-1)(b-1)}{2}$, возможных

значений n.

Задача нахождения максимального натурального n, для которого уравнение $a_1x_1 + a_2x_2 + \cdots + a_mx_m = n$ несовместно в неотрицательных целых числах, называется *задачей Фробениуса*.

1.3. Основная теорема арифметики

34. Найти каноническое разложение чисел:
1) 561; 2) 51480; 3) 562275; 4) 1001; 5) 111111.

35. Найти каноническое разложение НОК чисел $1, 2, \ldots, n$.

36. *Теорема Лежандра.* Найти каноническое разложение для $n!$.

37. Не пользуясь комбинаторными соображениями доказать, что биномиальные коэффициенты

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1)}{1 \cdot 2 \cdot 3 \cdot \cdots \cdot k}$$

— целые числа.

38. Доказать, что при простом p и натуральном $k < p$ биномиальный коэффициент $\binom{p}{k}$ является кратным p. Вывести отсюда, что для любого простого p и любых целых a и b

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

В качестве обобщения получить, что для любых целых $a_1, a_2, \ldots, a_s$

$$(a_1 + a_2 + \cdots + a_k)^p \equiv a_1^p + a_2^p + \cdots + a_k^p \pmod{p}.$$

39. Из предыдущей задачи вывести *малую теорему Ферма*: для любого целого a и простого p

$$a^p \equiv a \pmod{p}.$$

В частности, если a не кратно p, то

$$a^{p-1} \equiv 1 \pmod{p}.$$

40. Можно проверить, что $2^{4171996} \equiv 1856113 \pmod{4171997}$. Может ли число 4171997 быть простым?

41. Докажите, что формула

$$f(p/q) = \frac{p^2q^2}{p_1p_2 \ldots p_s},$$

где p, q — взаимно простые натуральные числа, а $p_1, p_2, \ldots, p_s$ — все различные простые множители числа p, задает биекцию множества всех положительных рациональных чисел на множество всех натуральных.

42. Тройка натуральных чисел a, b, c называется *пифагоровой*, если $a^2 + b^2 = c^2$. Пифагорова тройка называется *примитивной*, если a, b, c взаимно просты. Проверить, что формулы

$$a = 2mn, \qquad b = m^2 - n^2, \qquad c = m^2 + n^2,$$

где m, n — произвольные взаимно простые натуральные числа разной четности, $m > n$, дают примитивную пифагорову тройку.

43. Цель этой задачи, доказать, что формулы из № 42 дают все примитивные пифагоровы тройки (с точностью до переименования a и b). Пусть a, b, c — примитивная пифагорова тройка. Доказать, что

1) числа a, b, c — *попарно* взаимно простые;
2) ровно одно из чисел a, b, c четно;
3) c нечетно.

Итак, в пифагоровой тройке одно из чисел a, b четно, а c нечетно. Пусть для определенности a четно. Доказать, что

4) $\dfrac{c-b}{2}$ и $\dfrac{c+b}{2}$ — целые и взаимно простые;
5) $m^2 = \dfrac{c-b}{2}$, $n^2 = \dfrac{c+b}{2}$ для некоторых целых m и n;
6) вывести отсюда формулы из № 42;
7) доказать, что m, n взаимно просты и имеют разную четность.

44. Пусть a, n — натуральные числа. Доказать, что если $a^n - 1$ — простое, то $a = 2$, а n — простое. Привести пример, когда $2^p - 1$ не является простым, если p — простое. Простые числа вида $2^p - 1$ называются *простыми числами Мерсенна*.

45. Докажите, что если $2^n + 1$ — простое, то 2 — степень двойки. Числа $2^{2^n} + 1$ при $n \geq 0$ называются *числами Ферма*. Ферма выдвинул гипотезу, что все такие числа — простые. Опроверг ее Эйлер, показав, что $2^{32} + 1 = 4294967297 = 641 \times 6700417$ простым не является. В настоящее время не известно ни одного простого числа Ферма, кроме чисел, получающихся при $n = 0, 1, 2, 3, 4$.

46. Доказать, что если p — простое число вида $4k - 1$, где $k \in \mathbb{N}$, то сравнение $x^2 \equiv -1 \pmod{p}$ не имеет решений (см. также № 68).

47. Доказать, что

1) существует бесконечно много простых чисел вида $4k - 1$, где $k \in \mathbb{N}$;
2) существует бесконечно много простых чисел вида $4k + 1$, где $k \in \mathbb{N}$.

1.4. Сравнения и классы вычетов

48. Какие наборы чисел образуют полную систему представителей (вычетов) по модулю 7:

1) $1, 2, 3, 4, 5, 6, 7$; 2) $0, 1, 2, 3, 4, 5, 6, 7$; 3) $0, 1, 2, 3, 4, 5, 6$;
4) $0, -1, 2, -3, 4, -5, 6$; 5) $14, -6, 2, 10, -3, 5, 13$?

49. Пусть $(a_n a_{n-1} \ldots a_1 a_0)_{10}$ — запись в десятичной системе счисления числа a, т. е. $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$. Доказать, что

1) остаток от деления a на 3 равен $(a_0 + a_1 + \ldots a_{n-1} + a_n) \bmod 3$;
2) остаток от деления a на 9 равен $(a_0 + a_1 + \ldots a_{n-1} + a_n) \bmod 9$;
3) остаток от деления a на 11 равен $\big(a_0 - a_1 + a_2 - \cdots + (-1)^n a_n\big) \bmod 11$.

50. Докажите, что остаток от деления числа на 99 равен остатку от деления на 99 суммы его цифр в системе счисления по основанию 100. Например, $123456789 \bmod 99 = (1 + 23 + 45 + 67 + 89) \bmod 99 = 225 \bmod 99 = 27$. Сформулируйте и докажите соответствующее свойство остатка при делении на 33.

51. Докажите, что остаток от деления числа на 37 равен остатку от деления на 37 суммы его цифр в системе счисления по основанию 1000. Например, $123456789 \bmod 37 = (123{+}456{+}789) \bmod 37 = 1368 \bmod 37 = (1{+}368) \bmod 37 = 369 \bmod 37 = 36$.

52. Докажите, что остаток от деления числа на 101 равен остатку от деления на 101 знакопеременной суммы его цифр в системе счисления по основанию 100, причем число единиц берется со знаком плюс. Например, $123456789 \bmod 101 = (1{-}23{+}45{-}67{+}89) \bmod 101 = 45 \bmod 101 = 45$. Сформулируйте и докажите соответствующее свойство для случая деления на 7 и 13.

53. 1 января 2000 г. была суббота. На какой день недели выпадает
1) (р) 1 января 2100 г.; 2) 1 января 2200 г.?

54. Найдите остаток от деления:
1) $16^{2019} \bmod 15$; 2) $14^{2019} \bmod 15$.

55. Найдите остаток от деления:
1) (р) $19^{1861} \bmod 23$; 2) $(12^{231}{+}22^{314}) \bmod 35$; 3) $(13^{31}{-}31^{13}) \bmod 45$.

56. На какую цифру заканчивается число 2017^{2018}?

57. Найдите две последние цифры числа 1234^{5678}.

58. Пусть a, b, n — натуральные числа. Покажите, как найти $a^b \bmod n$ без явного вычисления a^b с использованием не более $2\lfloor \log_2 b \rfloor$ умножений по модулю n.

59. Постройте таблицы сложения и умножения классов вычетов
2) по модулю 2; 3) по модулю 3; 4) по модулю 4; 5) по модулю 5.

60. Класс вычетов $\overline{b}$ по модулю n называется *обратным* к классу $\overline{a}$, если $\overline{a} \cdot \overline{b} = \overline{1}$, т. е. $ab \equiv 1 \pmod n$. Обозначение: $(\overline{a})^{-1} = \overline{b}$. Для каждого класса вычетов по указанному модулю найти обратный:
2) по модулю 2; 3) по модулю 3; 4) по модулю 4; 5) по модулю 5.

61. (р) Докажите, что если класс $\overline{a}$ имеет обратный по модулю n, то других обратных у $\overline{a}$ по модулю n нет.

62. (р) Докажите, что для того, чтобы класс $\overline{a}$ имел обратный по модулю $n > 1$ необходимо и достаточно, чтобы НОД$(a, n) = 1$.

63. Найти обратный к классу $\overline{18}$
1) по модулю 25; 2) по модулю 27; 3) по модулю 29; 4) по модулю 31.

64. Решить сравнения:
1) $3x + 1 \equiv 0 \pmod{17}$; 2) $5x \equiv 9 \pmod{18}$; 3) $7x \equiv 4 \pmod{19}$;
4) $8x \equiv 9 \pmod{21}$.

65. Решить сравнения:
1) $8x \equiv 12 \pmod{18}$; 2) $6x \equiv 12 \pmod{21}$; 3) $6x \equiv 21 \pmod{30}$.

66. Решить сравнения:
1) $x^2 \equiv -1 \pmod{13}$; 2) $x^2 \equiv -1 \pmod{19}$; 3) $x^2 \equiv 4 \pmod{13}$;
4) $x^2 \equiv 5 \pmod{13}$; 5) $x^2 \equiv 10 \pmod{13}$; 6) $x^2 \equiv 11 \pmod{19}$.

67. Решить сравнения:
1) $x^2+2x+13\equiv 0 \pmod{19}$; 2) $x^2+4x+4\equiv 0 \pmod{13}$;
3) $x^2+3x+13\equiv 0 \pmod{23}$; 4) $x^2+5x+5\equiv 0 \pmod{13}$.

68. Доказать, что уравнение $x^2\equiv -1 \pmod{p}$, где p — простое, имеет в классах вычетов единственное решение при $p=2$, два решения при $p=4k+1$, и не имеет решений при $p=4k-1$, где $k\in\mathbb{N}$ (ср.№ 46).

69. *Китайская теорема об остатках.*
1) (р) Пусть натуральные числа m и n взаимно просты, а a и b — произвольные целые числа. Докажите, что найдется, причем единственный, класс вычетов $\overline{x}$ по модулю mn, такой, что $x\equiv a \pmod{m}$, $x\equiv b \pmod{n}$.
2) Пусть числа $m_1, m_2, \ldots, m_s$ попарно взаимно просты, а $a_1, a_2, \ldots, a_s$ — произвольные целые числа. Докажите, что найдется, причем единственный, класс вычетов $\overline{x}$ по модулю $m_1m_2\ldots m_s$, такой, что $x\equiv a_1 \pmod{m_1}$, $x\equiv a_2 \pmod{m_2}$, $\ldots$, $x\equiv a_s \pmod{m_s}$.

70. Найдите x из условий:
1) $x\equiv 2 \pmod 5$, $x\equiv 1 \pmod 6$;
2) $x\equiv 2 \pmod 3$, $x\equiv 1 \pmod 4$, $x\equiv 4 \pmod 5$;
3) $x\equiv 2 \pmod 7$, $x\equiv 5 \pmod{11}$, $x\equiv 9 \pmod{13}$.

71. Докажите малую теорему Ферма (см.№ 39), перемножая произведения всех ненулевых вычетов по простому модулю на фиксированный вычет a.

72. Докажите, что
1) если p — простое, то $(p-1)!\equiv -1 \pmod{p}$ (*теорема Вильсона*);
2) если a — составное и $a\neq 4$, то $(a-1)!\equiv 0 \pmod{a}$.

73. *Протокол Диффи–Хеллмана генерации общего ключа.* Алиса и Боб для тайной переписки хотят придумать секретный ключ, который был бы известен только им. Однако в их распоряжении имеется лишь открытый канал связи. Кто-нибудь из них, например, Алиса придумывает два числа: большое простое p и натуральное[3] g — и передает их по открытому каналу Бобу. Также Алиса генерирует случайное число a, а Боб — большое число b (это будут «секретные части» их общего ключа), и держат их в тайне. Далее Алиса и Боб вычисляют соответственно числа $A=g^a \bmod p$ и $B=g^b \bmod p$ и передают их по открытому каналу друг другу. Получив друг у друга эти значения, Алиса находит $B^a \bmod p$, а Боб — $A^b \bmod p$.
1) Проверить, что в результате Алиса и Боб придут к одному и тому же числу K — это и есть их общий ключ.
2) Предположим, что Владимир перехватил p, g, A, B. Почему ему будет трудно восстановить K?

74. EAN (European Article Number) — это европейский стандарт штрих-кода товара. Наиболее распространенным является штрих-код, содержащий 13 цифр: $d_{13}d_{12}\ldots d_1$. Последняя цифра d_1 — контрольная — вычисляется так, чтобы

[3] g должен быть первообразном корнем по модулю p. Для повышения криптостойкости $(p-1)/2$ также должно быть случайным простым числом. Мы опускаем здесь эти детали.

остаток от деления на 10 взвешенной суммы всех цифр с чередующимися весами 1, 3 равнялся 0: $d_{13} + 3d_{12} + d_{11} + 3d_{10} + \cdots + d_3 + 3d_2 + d_1 \equiv 0 \pmod{10}$. Проверить правильность составления кодов:
1) 4606369020350;
2) 6941059602369.

75. Проверить, что стандарт EAN позволяет обнаружить одиночные ошибки замены (одиночная цифра меняется на другую). Привести пример, показывающий, что при этом могут не обнаруживаться перестановки соседних цифр.

76. ISBN (International Standard Book Number) — это уникальный номер книжного издания. Согласно стандарту 1970 г. этот номер содержит 10 цифр[4]: $d_{10}d_9 \ldots d_1$. Последняя цифра d_1 — контрольная. Она вычисляется так, чтобы $10d_{10} + 9d_9 + 8d_8 + \cdots + 2d_2 + d_1 \equiv 0 \pmod{11}$. Все цифры, кроме контрольной, — десятичные. Контрольная цифра может равняться X, что соответствует 10. Штрих-код издания получается приписыванием спереди ISBN префикса 978 и заменой последней цифры на контрольную цифру, вычисленную по стандарту EAN. С 2007 г. действует новый стандарт ISBN. Согласно ему ISBN издания совпадает с его штрих-кодом. Проверить корректность ISBN согласно старому стандарту и конвертировать его в новый:
1) 5-85746-837-X;
2) 5-93208-009-4.

77. Проверить, что старый стандарт ISBN обнаруживает не только одиночные ошибки замены, но и любые одиночные перестановки двух цифр (не обязательно соседних).

78. Согласно методу Луна контрольная цифра d_1 в номере банковской карты $d_n d_{n-1} \ldots d_2 d_1$ должна вычисляться так, чтобы для четного n

$$(2d_n \bmod 9) + d_{n-1} + (2d_{n-2} \bmod 9) + d_{n-3} + \cdots + (2d_2 \bmod 9) + d_1 \equiv 0 \pmod{10}$$

и для нечетного n

$$d_n + (2d_{n-1} \bmod 9) + d_{n-2} + (2d_{n-3} \bmod 9) + \cdots + (2d_2 \bmod 9) + d_1 \equiv 0 \pmod{10}.$$

Восстановите контрольную цифру номера:
1) 548633292137770_; 2) 288267993171138_.

79. Проверить, что метод Луна позволяет обнаружить одиночные ошибки замены. Все ли одиночные перестановки соседних цифр он обнаруживает? Привести соответствующие примеры.

1.5. Рациональные и иррациональные числа

80. Докажите, что если $p_1, p_2, \ldots, p_s$ — попарно различные простые числа, то $\sqrt{p_1 p_2 \ldots p_s}$ — иррациональное число. Вывести отсюда, что если натуральное

[4]Первая (старшая) цифра (или группа цифр) несет информацию о стране или группе стран, объединенных общим языком (для России это 5). Следующая группа — код издательства. Далее идет уникальный номер издания и контрольная цифра.

n не является точным квадратом, то $\sqrt{n}$ — иррационально.

81. Докажите, что $\log_2 3$ — иррациональное число.

82. Заданное рациональное число представить в виде десятичной периодической дроби:

1) $\frac{125}{100}$; 2) $\frac{1}{3}$; 3) $\frac{1}{7}$; 4) $\frac{1}{17}$; 5) $\frac{17}{42}$; 6) $\frac{321}{14}$.

83. Десятичную периодическую дробь записать в виде обыкновенной дроби:

1) 1,1(9); 2) 0,(123456789); 3) 123,456(789); 4) 1,25(173).

84. Является ли рациональным или иррациональным число $0{,}123456789101112\ldots$ (после запятой идут последовательно десятичные записи всех натуральных чисел)?

1.6. Числовые функции

85. Найти количество натуральных чисел, не превосходящих 1000, не кратных ни одному из чисел: 7, 11, 13.

86. *Функцией Эйлера* $\varphi(n)$ натурального аргумента n называется количество натуральных чисел, не превосходящих n и взаимно простых с ним. В частности, $\varphi(1) = 1$, $\varphi(p) = p - 1$, если p — простое. Доказать, что

1) если p — простое, то $\varphi(p^k) = p^k - p^{k-1}$;

2) если НОД$(m, n) = 1$, то $\varphi(mn) = \varphi(m)\varphi(n)$.

87. Доказать, что

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right),$$

где $p_1, p_2, \ldots, p_s$ — все различные простые делители числа n.

88. Доказать, что

$$n = \sum_{d|n} \varphi(d),$$

где суммирование идет по всем натуральным делителям d числа n.

89. *Функцией Мёбиуса* $\mu(n)$ натурального аргумента n называется

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^s, & \text{если } k_1 = k_2 = \cdots = k_s = 1, \\ 0 & \text{иначе,} \end{cases}$$

где $n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ — каноническое разложение числа n на простые множители, $p_i \neq p_j$ при $i \neq j$. Доказать, что

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \geq 2. \end{cases}$$

90. *Формула обращения Мёбиуса.* Пусть $f(n)$ и $g(n)$ — функции натурального аргумента n. Доказать, что если для любого натурального n

$$f(n) = \sum_{d|n} g(d), \quad \text{то} \quad g(n) = \sum_{d|n} \mu(d)\, f\Big(\frac{n}{d}\Big).$$

91. Доказать, что для произвольного натурального n

$$\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

Ответы, указания, решения

1. $23 \operatorname{div} 5 = 4$, $23 \bmod 5 = 3$; $(-23) \operatorname{div} 5 = -5$, $(-23) \bmod 5 = 2$; $4 \operatorname{div} 5 = 0$, $4 \bmod 5 = 4$; $(-4) \operatorname{div} 5 = -1$, $(-4) \bmod 5 = 1$; $23 \operatorname{div} (-5) = -4$, $23 \bmod (-5) = 3$; $(-23) \operatorname{div} (-5) = 5$, $(-23) \bmod (-5) = 2$; $4 \operatorname{div} (-5) = 0$, $4 \bmod (-5) = 4$; $(-4) \operatorname{div} (-5) = 1$, $(-4) \bmod (-5) = 1$.

2. 1, 2, 3, 6, 7, 14, 21, 42.

3. $(13 + 64) \bmod 24 = 5$ часов.

4. $(5 + 24) \bmod 7 = 1$, т. е. понедельник.

5. 1) Среда, так как $31 \bmod 7 = 3$;

2) среда, так как $(31 + 28) \bmod 7 = 3$;

3) вторник, если год обычный (день недели отстоит на $365 \bmod 7 = 1$ день), и среда, если год високосный (день недели отстоит на $366 \bmod 7 = 2$ дня).

7. 1) *Указание.* Нумеровать месяцы удобнее с 0, присваивая этот номер марту. Январь и февраль при этом считаются 10-м и 11-м месяцами предыдущего года. Функция $\lfloor (153m + 2)/5 \rfloor$ возвращает количество дней, прошедших в году к началу m-го месяца.

3) *Указание.* 146097 — количество дней в 400-летии; 1461 — количество дней за 4 года; формулу для c можно записать как $c = \left\lfloor \dfrac{4(\mathrm{RD} + 305) + 3}{146097} \right\rfloor$.

8. НОД(42, 60) = 6, НОД(220, 273) = 1.

9. 1) $1 = -7 \times 89 + 26 \times 24$;

2) $3 = 4 \times 156 - 9 \times 69$;

3) $1 = 24 \times 691 - 161 \times 103$.

13. 1) Пусть $c \not\vdots d$, тогда левая часть уравнения $ax + by = c$ делится на d, а правая не делится. Противоречие.

2) Непосредственной проверкой убеждаемся, что пара $x = \dfrac{uc}{d} + \dfrac{tb}{d}$, $y = \dfrac{vc}{d} - \dfrac{ta}{d}$ является решением уравнения $ax + by = c$. Теперь покажем, что каждое решение x, y удовлетворяет этим формулам. Вычтем из равенства $ax + by = c$ равенство $au + bv = d$, умноженное на c/d. Получим $a\left(x - \dfrac{uc}{d}\right) + b\left(y - \dfrac{vc}{d}\right) = 0$, откуда $y - \dfrac{vc}{d} = \dfrac{a(xd - uc)}{bd}$. Так как $\mathrm{НОД}\left(\dfrac{a}{d}, b\right) = 1$, то для того, чтобы y был целым необходимо и достаточно, чтобы $(xd - uc) \vdots b$, т. е. $xd - uc = bt$, где $t \in \mathbb{Z}$, откуда $x = \dfrac{uc}{d} + \dfrac{tb}{d}$. Подставляя это выражение в исходное уравнение, находим $y = \dfrac{vc}{d} - \dfrac{ta}{d}$.

14. Обращаем внимание, что возможны разные (эквивалентные) формы записи общего решения.

1) $x = 2 + 5t$, $y = -1 - 5t$, $t \in \mathbb{Z}$;
2) $x = 7 + 13t$, $y = 2 - 7t$, $t \in \mathbb{Z}$;
3) $x = 8 + 5t$, $y = 1 + 3t$, $t \in \mathbb{Z}$;
4) $x = -21 + 24t$, $y = 78 - 89t$, $t \in \mathbb{Z}$.

15. 1) $x = -2 + 8t$, $y = 1 - 5t$, $z = t$, $t \in \mathbb{Z}$;
2) $x = 1 + 2t$, $y = -2 - 7t$, $z = 11 + 5t$, $t \in \mathbb{Z}$.

16. Решение задачи сводится к поиску целых неотрицательных (не просто целых) решений системы уравнений

$$\begin{cases} x + y + z = 100, \\ 10x + 5y + \dfrac{1}{2}z = 100. \end{cases}$$

Общее решение в целых числах: $x = 1 - 9t$, $y = 9 + 19t$, $z = 90 - 10t$ ($t \in \mathbb{Z}$). Из условий $1 - 9t \geq 0$, $9 + 19t \geq 0$, $90 - 10t \geq 0$, получаем $-8/19 \leq t \leq 1/9$. Учитывая, что $t \in \mathbb{Z}$, получаем $t = 0$. Таким образом, решение в натуральных числах единственно: 1 хряк, 9 свиноматок, 90 поросят.

17. Решение задачи сводится к поиску целых неотрицательных решений системы уравнений

$$\begin{cases} x + y + z = 80, \\ 2x + y + \dfrac{1}{2}z = 80. \end{cases}$$

Общее решение в целых числах: $x = 15 + t$, $y = 35 - 3t$, $z = 30 + 2t$ ($t \in \mathbb{Z}$). Так как нас интересуют только целые неотрицательные решения, то $15 + t \geq 0$, $35 - 3t \geq 0$, $30 + 2t \geq 0$, откуда $-15 \leq t \leq \frac{35}{3}$. Учитывая, что $t \in \mathbb{Z}$, получаем $-15 \leq t \leq 11$. В целых неотрицательных числах задача имеет 27 решений. Заметим, что Магницкий приводит лишь одно: $x = 15$, $y = 35$, $z = 30$.

18. Решение задачи сводится к поиску целых неотрицательных решений системы уравнений

$$\begin{cases} x + 4y + 12z = 100, \\ x + y + z = 40. \end{cases}$$

Общее решение в целых числах: $x = 20 + 8t$, $y = 20 - 11t$, $z = 3t$ ($t \in \mathbb{Z}$). Так как нас интересуют только целые неотрицательные решения, то получаем границы для t: $0 \leq t \leq \frac{20}{11}$, т. е. возможны лишь 2 целых значения: $t = 0, 1$. Соответствующие значения x, y, z таковы:

t	x	y	z
0	20	20	0
1	28	9	3

Итак, покупка марок может быть произведена только двумя способами.

21. 1) $3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{3}}}}$, 3, 4, $\frac{11}{3}$, $\frac{26}{7}$, $\frac{89}{24}$;

2) $2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5}}}$, 2, $\frac{7}{3}$, $\frac{9}{4}$, $\frac{52}{23} = \frac{156}{69}$;

3) $6 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4}}}}}$, 6, 7, $\frac{20}{3}$, $\frac{47}{7}$, $\frac{161}{24}$, $\frac{691}{103}$;

4) $1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2}}}}}$, 1, 2, $\frac{3}{2}$, $\frac{5}{3}$, $\frac{8}{5}$, $\frac{13}{8}$, $\frac{21}{13}$.

22. 1) $\frac{3+\sqrt{21}}{6}$. *Указание.* искомая иррациональность является корнем уравнения $x=1+\cfrac{1}{3+\frac{1}{x}}$.

2) $\frac{4+\sqrt{37}}{7}$.

23. 1) $\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\dots}}}}$;

2) $\frac{1+\sqrt{5}}{2}=1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\dots}}}$;

3) $\frac{1+\sqrt{2}}{2}=1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{4+\dots}}}}}$;

4) $\frac{1+\sqrt{3}}{2}=1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\dots}}}}}$;

5) $\frac{2+\sqrt{10}}{2}=2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\dots}}}}}$.

24. 1) $\sqrt{n^2+1}=n+\cfrac{1}{2n+\cfrac{1}{2n+\cfrac{1}{2n+\dots}}}$;

2) $\sqrt{n^2-1} = n-1+\cfrac{1}{1+\cfrac{1}{2(n-1)+\cfrac{1}{1+\cfrac{1}{2(n-1)+\cfrac{1}{1+\dots}}}}}$ при $n>1$.

27. 3, $\frac{22}{7} = 3{,}142857\dots$, $\frac{333}{106} = 3{,}141509\dots$, $\frac{355}{113} = 3{,}14159292\dots$, $\frac{103993}{33102} = 3{,}14159265301\dots$.

33. 1) *1-й способ.* Согласно № 13 общее решение уравнения $ax+by=n$ в *целых* числах выражается формулами $x = x_0 + tb$, $y = y_0 - ta$ ($t \in \mathbb{Z}$), где x_0, y_0 — некоторое частное решение. Так как $a>0$, $b>0$, то существует частное решение, для которого $x_0 \geq 0$. Выберем частное решение с минимально возможным неотрицательным x_0. Тогда $x_0 \leq b-1$ (иначе при $t=-1$ имеем $0 \leq x < x_0$ и x_0 не минимальный). Так как $n \geq (a-1)(b-1)$, то $by_0 = n - ax_0 \geq (a-1)(b-1) - a(b-1) = 1-b > -b$, откуда $y_0 > -1$. Так как $y_0 \in \mathbb{Z}$, то $y_0 \geq 0$. Таким образом, $(x_0,\, y_0)$ — неотрицательное целочисленное решение.

2-й способ. Можно дать «геометрическое решение» задачи (В. И. Арнольд). Рассмотрим семейство параллельных прямых $ax+by=n$ при всевозможных натуральных значениях n. Расстояние между соседними целочисленными точками на каждой такой прямой равно $L = \sqrt{a^2+b^2}$. С другой стороны, расстояние между точками пересечения этой прямой с координатными осями равно $\sqrt{(n/a)^2 + (n/b)^2}$. При $n \geq ab$ это расстояние будет не меньше L, поэтому на этой прямой обязательно будет лежать по крайней мере одна целочисленная точка из первой четверти координатной плоскости (т. е. точка с неотрицательными целыми координатами). Тем самым мы установили разрешимость в неотрицательных целых числах уравнения $ax+by=n$ при $n \geq ab$.

Теперь рассмотрим случай $ab-a-b < n < ab$. На прямой $ax+by=n$ при $n=ab$ лежат две целочисленные точки из первой четверти: $\mathcal{A}(b,\,0)$, $\mathcal{B}(0,\,a)$ (см. рисунок; на нем $a=5$, $b=7$ и изображены две прямые $ax+by=n$ при $n=ab$ и $n=ab-a-b$). На прямой при $n=ab-a-b$ в первой четверти целочисленных точек нет. Действительно, целочисленные точки $\mathcal{A}'(b-1,\,-1)$, $\mathcal{B}'(-1,\,a-1)$ лежат на этой прямой по «разные стороны» от первой четверти. Так как $|\mathcal{A}'\mathcal{B}'| = L$, то между $\mathcal{A}'$ и $\mathcal{B}'$ нет других целочисленных точек (тем самым доказано утверждение из п. 2 задачи). Каждая прямая $ax+by=n$ при $ab-a-b < n < ab$ находится между двумя рассмотренными прямыми, следовательно, пересекает оба из заштрихованных квадратов на рисунке. В частности, каждая такая прямая пересекает диагонали $\mathcal{A}\mathcal{A}'$ и $\mathcal{B}\mathcal{B}'$ этих квадратов. Очевидно, что расстояние между точками пересечения с диагоналями равно L. Но квадраты не содержат внутренних целочисленных точек, следовательно, такие точки обязательно появятся в первом квадранте на каждой из прямой $ax+by=n$ при целых значениях n в рассматриваемом диапазоне.

34. 1) $3\cdot 11\cdot 17$; 2) $2^3\cdot 3^2\cdot 5\cdot 11\cdot 13$; 3) $3^3\cdot 5^2\cdot 7^2\cdot 17$; 4) $7\cdot 11\cdot 13$; 5) $3\cdot 7\cdot 11\cdot 13\cdot 37$.

35. $\prod p^{\lfloor \log_p n \rfloor}$.

36. $\prod p^{\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \dots}$.

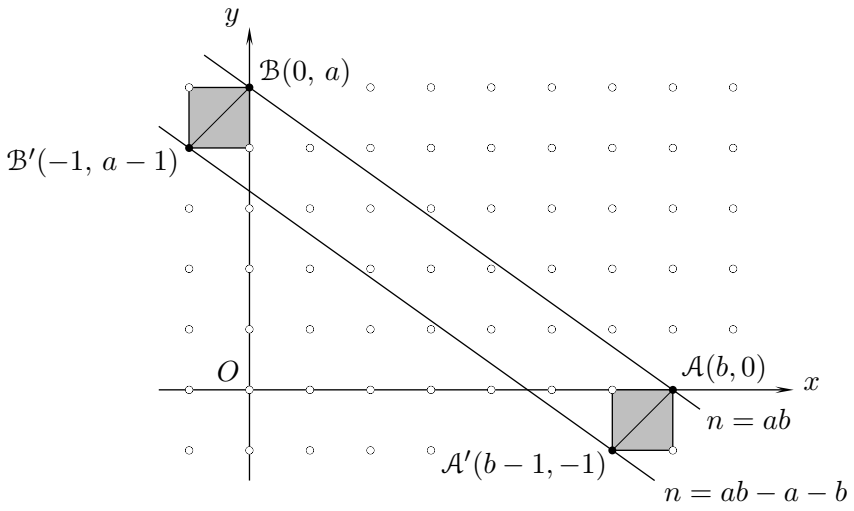
39. *Указание.* Рассмотреть $(1+1+\dots+1)^p$.

41. Пусть $p = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, $q = q_1^{\ell_1} q_2^{\ell_2} \dots q_t^{\ell_t}$ — разложения на простые множители чисел p и q. Тогда

$$\frac{p^2q^2}{p_1p_2\dots p_s} = p_1^{2k_1-1} p_2^{2k_2-1} \dots p_s^{2k_s-1} q_1^{2\ell_1} q_2^{2\ell_2} \dots q_t^{2\ell_t}.$$

В таком виде можно представить любое натуральное число, причем единственным образом.

43. 3) Пусть c четно, a, b нечетны, тогда $a = 2k+1$, откуда $a^2 = 4k^2+4k+1 \equiv 1 \pmod 4$, аналогично $b^2 \equiv 1 \pmod 4$, тогда $a^2+b^2 \equiv 2 \pmod 4$, что противоречит тому, что $c^2 \equiv 0 \pmod 4$.



4) Так как c и b нечетные, то $c-b$ и $c+b$ четные, поэтому $\frac{c-b}{2}$ и $\frac{c+b}{2}$ — целые. Если каждый из них делится на одно и то же простое p, то каждое из чисел $c=\frac{c+b}{2}+\frac{c-b}{2}$, $b=\frac{c+b}{2}-\frac{c-b}{2}$ также делится на это p, что противоречит взаимной простоте b и c.

5) Так как a четно, то $a=2\ell$ для некоторого целого ℓ. Тогда $a^2=4\ell^2=c^2-b^2=(c-b)(c+b)$, откуда

$$\ell^2=\frac{c-b}{2}\cdot\frac{c+b}{2}.$$

Пусть $\ell^2=p_1^{2k_1}p_2^{2k_2}\dots p_s^{2k_s}$ — каноническое разложение ℓ^2 на простые множители. Так как $\frac{c-b}{2}$ и $\frac{c+b}{2}$ взаимно простые, то для любого j имеем альтернативу: $\frac{c-b}{2}\,\vdots\,p_j^{2k_j}$ или $\frac{c+b}{2}\,\vdots\,p_j^{2k_j}$, откуда следует, что $\frac{c-b}{2}$ и $\frac{c+b}{2}$ являются квадратами целых чисел.

45. Если у $n=qd$ и q нечетно, то $2^n+1=(2^q+1)(2^{m-q}-2^{m-2q}+\dots-2^q+1)$.

46. Пусть $x^2\equiv-1\pmod p$, где $p=4k-1$. По малой теореме Ферма (см. № 39) $x^{p-1}\equiv1\pmod p$, поэтому $1\equiv x^{p-1}\equiv x^{4k-2}\equiv x^{2(2k-1)}\equiv(-1)^{2k-1}=-1\pmod p$. Получаем $1\equiv-1\pmod p$ — противоречие.

47. 1) *Указание.* Пусть $p_1,p_2,\dots,p_s$ — все простые числа вида $4k-1$. Рассмотреть число $a=4p_1p_2\dots p_s-1$. *Решение.* Число a является составным, так как имеет вид $4k-1$, но его нет в списке простых чисел такого вида. Так как a не делится ни на одно из простых чисел вида $4k-1$ и является нечетным, то оно должно раскладываться в произведение простых чисел вида $4k+1$. Но произведение чисел вида $4k+1$ само имеет такой вид. Противоречие.

2) *Указание.* Пусть $p_1,p_2,\dots,p_s$ — все простые числа вида $4k+1$. Рассмотреть число $a=4(p_1p_2\dots p_s)^2+1$. *Решение.* Число a является составным, так как имеет вид $4k+1$, но его нет в списке простых чисел такого вида. Так как a не делится ни на одно из простых чисел вида $4k+1$ и является нечетным, то оно должно раскладываться в произведение простых чисел вида $4k-1$. Пусть p — одно из таких чисел. Получаем $x^2+1\equiv0\pmod p$, где $x=2p_1p_2\dots p_s$, что противоречит № 46.

48. 1) Да; 2) нет; 3) да; 4) нет; 5) да.

53. 1) С 1 января 2000 г. по 1 января 2100 г. прошло 100 лет. Года 2000, 2004, 2008, 2012, …, 2092, 2096 — високосные. Всего $100/4=25$ високосных лет. Итак, в XXI столетии[5] $75\times365+25\times366$ дней. Так как $(75\times365+25\times366)\bmod7=(75\times1+25\times2)\bmod7=125\bmod7=6$,

[5]Точнее, не в XXI столетии, а с 2000-й по 2099-й год включительно. XXI век начался 1 января 2001 г. и закончится 31 декабря 2100 г.

то день недели 1 января 2100 г. будет отстоять от дня недели 1 января 2000 г. на 6 дней, т. е. так как 1 января 2000 г. была суббота, то 1 января 2100 г. будет пятница.

2) Среда (обратите внимание, что 2100 г. — обычный, не високосный, год).

54. 1) 1;

2) $-1 \equiv 14 \pmod{15}$.

55. 1) Приведем один из способов, как можно вычислить результат модулярного возведения в большую степень без явного вычисления самой степени. Вначале последовательно вычислим:

$$\begin{aligned}
19^2 &= 361 \equiv 16\\
19^4 &\equiv 16^2 = 256 \equiv 3\\
19^8 &\equiv 3^2 = 9 \equiv 9\\
19^{16} &\equiv 9^2 = 81 \equiv 12\\
19^{32} &\equiv 12^2 = 144 \equiv 6\\
19^{64} &\equiv 6^2 = 36 \equiv 13\\
19^{128} &\equiv 13^2 = 169 \equiv 8\\
19^{256} &\equiv 8^2 = 64 \equiv 18\\
19^{512} &\equiv 18^2 = 324 \equiv 2\\
19^{1024} &\equiv 2^2 = 4 \equiv 4
\end{aligned} \pmod{23}$$

Так как $1861 = 1 + 4 + 64 + 256 + 512 + 1024$, то получаем:

$$19^{1861} = 19 \times 19^4 \times 19^{64} \times 19^{256} \times 19^{512} \times 19^{1024} \equiv 19 \times 3 \times 13 \times 18 \times 2 \times 4 \equiv 7 \pmod{23}.$$

2) 7;

3) 36.

56. 9.

57. 96.

59. 2)

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

3)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

4)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

5)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{6}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

60. Ни для какого целого модуля $n > 1$ не существует $\overline{0}^{-1}$.
2) $\overline{1}^{-1} = \overline{1}$;
3) $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{2}$;
4) $\overline{1}^{-1} = \overline{1}$, $\overline{3}^{-1} = \overline{3}$; не существует $\overline{2}^{-1}$;
5) $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$.

61. От противного. Пусть для $\overline{a}$ нашлось два обратных: $\overline{b}$ и $\overline{c}$, тогда $ab \equiv ac \equiv 1 \pmod{n}$, откуда $b \equiv b \cdot 1 \equiv b(ac) \equiv (ba)c \equiv 1 \cdot c \equiv c \pmod{n}$, т. е. $\overline{b} = \overline{c}$.

62. Если $d = \text{НОД}(a, n) > 1$, то равенство $ab = 1 + kn$ невозможно ни при каких целых b и k, так как левая его часть делится нацело на d, а правая при делении на d дает остаток 1. Поэтому $ab \not\equiv 1 \pmod{n}$ ни при каких b. Если $d = \text{НОД}(a, n) = 1$, то найдутся такие u и v, что $ua + vn = 1$, откуда $au \equiv 1 \pmod{n}$, т. е. $\overline{a}^{-1} = \overline{u}$.

63. 1) $\overline{7}$; 2) не существует $\overline{18}^{-1}$; 3) $\overline{21}$; 4) $\overline{19}$.

64. 1) $x \equiv 11 \pmod{17}$; 2) $x \equiv 9 \pmod{18}$; 3) $x \equiv 6 \pmod{19}$; 4) $x \equiv 9 \pmod{21}$.

65. *Указание.* Линейное сравнение $ax \equiv b \pmod{n}$ сводится к диофантовому уравнению $ax = b + yn$.
1) $x_1 \equiv 6 \pmod{18}$, $x_2 \equiv 15 \pmod{18}$;
2) $x_1 \equiv 2 \pmod{21}$, $x_2 \equiv 9 \pmod{21}$, $x_3 \equiv 16 \pmod{21}$;
3) нет решений.

66. 1) $x_1 \equiv 5 \pmod{13}$, $x_2 \equiv 8 \pmod{13}$; 2) нет решений;
3) $x_1 \equiv 2 \pmod{13}$, $x_2 \equiv -2 \equiv 11 \pmod{13}$; 4) нет решений;
5) $x_1 \equiv 6 \pmod{13}$, $x_2 \equiv 7 \pmod{13}$; 6) $x_1 \equiv 7 \pmod{19}$, $x_2 \equiv 12 \pmod{19}$.

67. 1) $x_1 \equiv 7 \pmod{19}$, $x_2 \equiv 10 \pmod{19}$; 2) $x_{1,2} \equiv 11 \pmod{13}$;
3) $x_1 \equiv 2 \pmod{23}$, $x_2 \equiv 10 \pmod{23}$; 4) нет решений.

68. *Указание.* При $p > 2$ на множестве всех ненулевых вычетов по модулю p ввести отношение эквивалентности, отождествляя вычет с его противоположным (по сложению), обратным (по умножению) и противоположным обратному.
Решение. Каждый класс эквивалентности по введенному отношению будет содержать 4 вычета, кроме случаев: а) $x \equiv -x \pmod{p}$, что невозможно при $p > 2$; б) $x \equiv x^{-1} \pmod{p}$, что эквивалентно $x^2 \equiv 1 \pmod{p}$, откуда 2 решения: $\overline{\pm 1}$; в) $x \equiv -x^{-1} \pmod{p}$, что эквивалентно сравнению $x^2 \equiv -1 \pmod{p}$, которое либо не имеет решений, либо имеет два решения $\overline{\pm x_0}$. Если $p = 4k + 1$, то случай в) реализуется, а если $p = 4k - 1$ — нет.

69. 1) Представим x в виде $x = vm + u$, откуда $u \equiv a \pmod{m}$. Сравнение $vm + a \equiv b \pmod{n}$ имеет единственное решение v, откуда $x \equiv vm + a \pmod{mn}$. Таким образом, если искомый класс вычетов существует, то он единственен. С другой стороны, легко видеть, что $x \equiv vm + a \pmod{mn}$ действительно удовлетворяет каждому из двух заданных сравнений.

70. 1) $x \equiv 17 \pmod{30}$; 2) $x \equiv 29 \pmod{60}$; 3) $x \equiv 555 \pmod{1001}$.

71. Пусть a — ненулевой вычет по простому модулю p. Тогда множество $1a, 2a, \ldots, (p-1)a$ исчерпывает множество всех вычетов по этому модулю, поэтому

$$1a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}.$$

Сокращая обе части на $(p-1)!$, получаем $a^{p-1} \equiv 1 \pmod{p}$.

72. 1) *Указание.* Воспользоваться тем, что при $p > 2$ все вычеты, кроме 1 и $p-1$, разбиваются на пары взаимно обратных.
2) *Указание.* Воспользоваться теоремой Лежандра (см. № 36).

73. 2) Владимиру придется находить a и b из уравнений $A = g^a \bmod p$ и $B = g^b \bmod p$. Решение таких уравнений — это задача *дискретного логарифмирования*, которая, по-видимому, является сложной (хотя это не доказано).

74. 1) Код составлен верно; 2) код содержит ошибку.

76. 1) 978-5-85746-837-1; 2) 978-5-93208-009-2.

78. 1) 0; 2) 6.

82. 1) Допускает два представления: $1{,}250000\ldots = 1{,}25(0)$ и $1{,}249999\ldots = 1{,}24(9)$;
2) $0{,}3333\ldots = 0{,}(3)$; 3) $0{,}(142857)$; 4) $0{,}(0588235294117647)$; 5) $0{,}4(047619)$; 6) $22{,}9(285714)$.

83. 1) $\dfrac{6}{5}$; 2) $\dfrac{13717421}{111111111}$; 3) $\dfrac{41111111}{333000}$; 4) $\dfrac{31262}{24975}$.

85. 720. *Указание.* Воспользоваться формулой включений–исключений.

86. 2) Согласно китайской теореме об остатках (см. № 69), для любых a, b, таких, что $0 \leq a < m$, $0 \leq b < n$, найдется единственное c, такое, что $c \equiv a \pmod m$, $c \equiv b \pmod n$, $0 \leq c < mn$. Ясно, что НОД$(a, m) =$ НОД(c, mn) и НОД$(b, n) =$ НОД(c, mn). В частности, НОД$(a, m) = 1$ и НОД$(b, n) = 1$ тогда и только тогда, когда НОД$(, mn) = 1$.

87. *Указание.* Воспользоваться формулой включений-исключений или № 86.

88. В последовательности $\dfrac{1}{n}, \dfrac{2}{n}, \dfrac{3}{n}, \ldots, \dfrac{n}{n}$ заменим каждую дробь на равную ей несократимую. В результате получаются дроби, знаменатели которых являются делителями числа n. Количество дробей со знаменателем d равно $\varphi(d)$.

89. При $n \geq 2$

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 p_2 \ldots p_s} \mu(d) = 1 - \binom{s}{1} + \binom{s}{2} - \binom{s}{3} + \cdots + (-1)^s = 0$$

(число $p_1 p_2 \ldots p_s$ имеет $\binom{s}{k}$ делителей, составленных из k простых множителей).

90. Подставим в формулу для $g(n)$ выражение для $f(n)$ и поменяем порядок суммирования:

$$\sum_{d|n} \mu(d)\, f\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) \sum_{\delta|\frac{n}{d}} g(\delta) = \sum_{d|n} \sum_{\delta|\frac{n}{d}} \mu(d) g(\delta) = \sum_{\delta|n} \sum_{d|\frac{n}{\delta}} \mu(d) g(\delta) = \sum_{\delta|n} g(\delta) \sum_{d|\frac{n}{\delta}} \mu(d) = g(n).$$

Последнее равенство вытекает из № 89.