КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

Н.А. Корешков, М.Ф. Насрутдинов

СБОРНИК ЗАДАЧ ПО ТЕОРИИ ЧИСЕЛ

Казань — 2016

Казанский (Приволжский) федеральный университет

Н.А. Корешков, М.Ф. Насрутдинов

СБОРНИК ЗАДАЧ ПО ТЕОРИИ ЧИСЕЛ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Казань
2016

УДК 512

Печатается по решению учебно-методической комиссии Института математики и механики им. Н.И. Лобачевского от 10 декабря 2015 г. (протокол №3).

Научный редактор
кандидат физико-математических наук, доцент Абызов А.Н.

Корешков Н.А., Насрутдинов М.Ф.

Сборник задач по теории чисел. Учебно-методическое пособие /Корешков Н.А., Насрутдинов М.Ф. – Казань: Казанский университет, 2016. — 24 с.

Учебно-методическое пособие предназначено для студентов младших курсов Института математики и механики им. Н.И. Лобачевского для проведения практических занятий дисциплины "Теория чисел".

Оглавление

1 Деление с остатком

1.1. Найти наибольшее число, дающее при делении на 13 частное 17.

1.2. Доказать, что остаток при делении квадрата нечетного натурального числа на 8 равен 1.

1.3. Доказать, что сумма квадратов двух последовательных натуральных чисел при делении на 4 дает остаток 1.

1.4. Доказать, что если $a \equiv 1 \mod n$ и $b \equiv 1 \mod n$, то $ab \equiv 1 \mod n$.

1.5. Доказать, что $3n + 2$ не может быть квадратом целого числа.

1.6. Доказать, что среди 5 последовательных натуральных чисел одно делится на 5.

1.7. Доказать, что сумма $2n+1$ последовательных чисел делится на $2n+1$.

1.8. Доказать, что $5|m^5 - m$.

1.9. Доказать, что $6|m^3 + 5m$.

1.10. Доказать, что $6|m(m + 1)(2m + 1)$.

1.11. Доказать, что $9|4^n + 15n - 1$ для любых положительных целых n.

1.12. Доказать, что если $m - p|mn + pq$, то $m - p|mq + np$.

1.13. Найти все натуральные n, для которых $n + 1|n^2 + 1$.

1.14. Найти все целые $n \neq 3$, для которых $n - 3|n^3 - 3$.

1.15. Доказать, что если $7|m^2 + n^2$, то $7|m$ и $7|n$.

1.16. Доказать, что в пифагоровой тройке[1] один из катетов делится на 3.

1.17. Доказать, что в пифагоровой тройке одна из сторон делится на 5.

1.18. Доказать, что простое число $p > 5$ при делении на 6 дает остаток 1 или 5.

1.19. Доказать, что квадрат простого числа $p > 3$ при делении на 24 дает остаток 1.

1.20. Если трехзначное число делится на 37, то все числа полученные круговой перестановкой тоже делится на 37.

1.21. Доказать, что сумма квадратов двух нечетных чисел не может быть квадратом целого числа.

1.22. Доказать, что сумма четных степеней двух нечетных чисел не может быть кубом целого числа.

1.23. Доказать, что 5-я степень любого натурального числа оканчивается на ту же самую цифру, что и само число.

[1] Тройка положительных целых чисел a, b, c называется пифагоровой, если $a^2 + b^2 = c^2$

1.24. Доказать, что

а) $a^{10} - 9a + 8$ делится на 2,

б) $a^5 + 3a^3 - 12$ делится на 4,

в) $a^3 - 7a + 18$ делится на 6,

г) $a^7 - a - 56$ делится на 7,

д) $a^5 - 17a^3 + 24$ делится на 8,

е) $a^9 + 17a^3 - 18$ делится на 9.

1.25. Доказать, что

а) разность четных степеней двух нечетных чисел делится на 4,

б) сумма кубов двух последовательных нечетных чисел делится на 6,

в) разность квадратов двух нечетных чисел делится на 8,

г) сумма кубов трех последовательных целых чисел делится на 3.

1.26. Доказать, что

а) $5ab$ делится на 45, если $a^6 + b^6$ делится на 3,

б) $4ab$ делится на 100, если $a^8 + b^8$ делится на 5,

в) $2ab$ делится на 98, если $a^4 + b^4$ делится на 7,

г) $3ab$ делится на 363, если $a^2 + b^2$ делится на 11.

1.27. Доказать, что $n(n^2 + 1)(n^2 + 4)$ делится на 5 при любом целом n.

1.28. Доказать, что целое число a не может быть квадратом целого числа, если число $a - 5$ делится на 9.

1.29. Доказать, что $\dfrac{n-5}{15}$ и $\dfrac{n-6}{24}$ не могут быть одновременно целыми числами.

1.30. Доказать, что abc делится на 3, если $a^3 + b^3 + c^3$ делится на 9.

1.31. Доказать, что $7^{n+2} + 8^{2n+1}$ делится на 3 при любом целом неотрицательном n.

1.32. Доказать, что $5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}$ делится на 19 при любом целом неотрицательном n.

1.33. Доказать, что при любом натуральном n

а) $2^{n+2} + 2^{n+1} + 2^n$ делится на 14,

б) $7^{2n} - 4^{2n}$ делится на 33,

в) $5^{2n+1} + 3^{n+2} \cdot 2^{n-1}$ делится на 19,

г) $12^{2n+1} + 11^{n+1}$ делится на 133.

1.34. Найти все простые числа p, для которых числа $p + 10$ и $p + 14$ также простые.

1.35. Доказать, что сумма квадратов трех простых чисел, бóльших трех, есть число составное.

1.36. Найти все натуральные n, для которых $8^n - 1$ — простое число.

1.37. Доказать, что для любого натурального n число $32^n + 1$ является составным.

1.38. Найти все наборы из пяти последовательных целых чисел, сумма которых есть число простое.

1.39. Доказать, что натуральное число вида $6k - 1$ имеет простой делитель того же вида.

1.40. Доказать, что существует бесконечно много простых чисел вида $6k - 1$, $k \in \mathbb{N}$.

1.41. Найти все простые числа p, для которых числа $p+5$ и $p+11$ также простые.

1.42. Доказать, что сумма квадратов двух нечетных простых чисел есть число составное.

1.43. Найти все натуральные n, для которых

а) $3^n - 1 \in P$,

б) $6^n - 1 \in P$,

в) $12^n - 1 \in P$,

г) $18^n - 1 \in P$,

где P — множество простых чисел.

1.44. При каких натуральных n число $n^4 + n^2 + 1$ является простым?

1.45. Найти все тройки p, $p+2$, $p+4$ последовательных нечетных простых чисел.

1.46. Найти все простые p, для которых $7p^2 + 8$ — простое число.

1.47. Для каких простых p число $p+4$ является квадратом целого числа?

1.48. Найти все простые числа p, для которых $2p + 1$ является кубом целого числа.

2 Функции [ ] и { }

Целой частью вещественного числа называется наибольшее целое число, не превосходящее x. Обозначение $[x]$ (читается "антье от x"). Дробной частью числа x называется число $\{x\} = x - [x]$.

Примеры. $[3.14] = 3$, $[-3.14] = -4$, $\{-3.14\} = 0.86$.

Теорема 2.1 *Показатель, с которым простое число p входит в разложение $n!$ равен*

$$[\frac{n}{p}] + [\frac{n}{p^2}] + \dots [\frac{n}{p^k}] + \dots$$

При этом лишь конечное число слагаемых в сумме не равно нулю.

2.1. Найти целые и дробные части следующих чисел:
а) 3.14, б) -4.1,
в) $\sqrt{35}$, г) $\sqrt{30} + \sqrt[3]{10}$

2.2. Построить графики функций $y = [x]$, $y = \{x\}$

2.3. Выразить $[x + y]$ через целые и дробные части x, y

2.4. Показать, что количество чисел кратных d, лежащих на отрезке $[1, x]$ равно $[\frac{x}{d}]$

2.5. Сколькими нулями оканчивается число 2016!

2.6. Сколькими нулями оканчивается число 191!

2.7. С каким показателем число 6 входит в произведение 100!

2.8. С каким показателем степени простое число p входит в $(p^n)!$

2.9. Найти НОК всех натуральных чисел, не превышающих m.

2.10. . Сколько натуральных n, не превосходящих 1000, не делится ни на 5, ни на 7?

2.11. Решить уравнение $[x] = 1 + 2\{x\}$.

2.12. Построить графики функций $f(x) = [2x - 1]$, $f(x) = \{2x - 1\}$.

2.13. Сколько натуральных чисел, не превосходящих 100, не делится ни на 2, ни на 3, ни на 5.

2.14. Запишите каноническое разложение чисел
а) 14!, б) 16!, в) 18!, г) 20!, д) 26!
е) $\frac{20!}{10!10!}$, ж) $\frac{16!}{8!8!}$, з) $\frac{16!}{10!6!}$, и) $\frac{20!}{16!4!}$.

2.15. Решите уравнения
а) $[x] = -3$, б) $[2x] = 2$,
в) $[x^2 - 4x + 7] = 3$, г) $[3x^2 - x] = x - 1$,
д) $\{x\} = [x + 15]$, е) $[x] + 5 = 2\{x\}$,
ж) $\frac{x-1}{3} = \{x\}$.

2.16. Построить графики функций

а) $f(x) = [\sin x]$, $f(x) = \{\sin x\}$,

б) $f(x) = [2\cos x - 3]$, $f(x) = \{2\cos x - 3\}$,

в) $f(x) = [x^3 - 1]$, $f(x) = \{x^3 - 1\}$.

2.17. Решить неравенства

а) $[1 - x^2] > -4$, г) $\{1 - x^2\} > 0,5$,

б) $[\sin 2x - 4] \leq 3,5$, д) $\{\sin 2x - 4\} \leq 0,5$,

в) $[\log_5 x] \geq 0$, е) $\{\log_5 x\} \geq 0,2$.

2.18. Докажите

а) $[x] + [x + \frac{1}{k}] + [x + \frac{2}{k}] + \cdots + [x + \frac{k-1}{k}] = [kx]$, где $x \in \mathbb{R}$, $k \in \mathbb{N}$,

б) $[\frac{m}{n}] + [2\frac{m}{n}] + \cdots + [(n-1)\frac{m}{n}] = \frac{(m-1)(n-1)}{2}$, где $m, n \in \mathbb{N}$, $(m, n) = 1$,

в) $\sum\limits_{n=1}^{q/2} [\frac{np}{q}] + \sum\limits_{m=1}^{p/2} [\frac{mq}{p}] = \frac{p-1}{2} \cdot \frac{q-1}{2}$, где $m, n \in \mathbb{N}$, $p, q \in P \setminus 2$, $p \neq q$.

3 Некоторые теоретико-числовые функции

Функция $\theta : \mathbb{N} \to \mathbb{C}$ называется мультипликативной, если (1) $\theta(a) \neq 0$ хотя бы для одного натурального a (2) для любых взаимно простых чисел a и b имеем $\theta(ab) = \theta(a)\theta(b)$.

Функцией Мебиуса называется функция $\mu : \mathbb{N} \to \{-1, 0, 1\}$, определяемая условиями

$$\mu(a) = \begin{cases} 1, & \text{если } a = 1 \\ (-1)^n, & \text{если } a = p_1 p_2 \dots p_n, \text{где все } p_i \text{ различные простые числа} \\ 0, & \text{если } a \text{ делится на квадрат простого числа} \end{cases}$$

Функция Эйлера $\varphi(a)$ определяется для положительных чисел и равна количеству чисел ряда $0, 1, \dots, a-1$ взаимно простых с a. По определению $\varphi(1) = 1$.

Для целого числа a будем обозначать также через $\tau(a)$ число делителей a, через $S(a)$ сумму делителей a.

3.1. Какие из следующих функций $f(x)$ мультипликативны:

1. $f(x) = x^s$, где s любое вещественное (или комплексное) число;
2. $f(x) = \sin(x)$;
3. $f(x) = \lg(x)$.

В следующих задачах a – целое положительное число и $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ его каноническое разложение на простые множители.

3.2. Пусть $\theta(x)$ – мультипликативная функция. Доказать, что

$$\sum_{d|a} \theta(d) = (1 + \theta(p_1) + \dots + \theta(p_1^{\alpha_1})) \dots (1 + \theta(p_n) + \dots + \theta(p_n^{\alpha_n}))$$

3.3. Пусть $\theta(a)$ мультипликативная функция. Доказать, что $\theta_1(a) = \sum\limits_{d|a} \theta(d)$ – мультипликативная функция.

3.4. Доказать, что $\sum\limits_{d|a} d^s = (1 + p_1^s + \dots + p_1^{s\alpha_1}) \dots (1 + p_n^s + \dots + p_n^{s\alpha_n})$.

3.5. Доказать, что число делителей a равно $\tau(a) = (1 + \alpha_1) \dots (1 + \alpha_n)$.

3.6. Найти сумму делителей $S(a)$ числа a.

3.7. Найти сумму и число делителей числа 500.

3.8. Пусть θ мультипликативная функция. Доказать, что $\sum\limits_{d|a} \mu(d)\theta(d) = (1 - \theta(p_1)) \dots (1 - \theta(p_n))$

3.9. Найти $\varphi(a)$ и $\mu(a)$ для чисел от 1 до 15.

3.10. Найти $\sum\limits_{d|a} \mu(d)\varphi(d)$.

3.11. Найти $\sum\limits_{d|n} \mu(d)$.

3.12. Найти $\sum\limits_{d|n} \dfrac{\mu(d)}{d}$. (Применить теорему к мультипликативной функции $1/d$)

3.13. Решить уравнения (S и τ – функции из примеров 3.6 и 3.5)

а) $\tau(x) = 2$, д) $\tau(5x) = \tau(7x)$, и) $S(x) = x$,
б) $\tau(x) = 11$, е) $\tau(2x) = \tau(11x)$, к) $S(x) = x + 1$,
в) $\tau(x) = 13$, ж) $\tau(13x) = \tau(17x)$, л) $S(x) = x + 2$,
г) $\tau(x) = 17$, з) $\tau(3x) = \tau(37x)$, м) $S(x) = x + 4$.

3.14. Найти натуральное число n, если $n = p^\alpha q^\beta$, $r(n) = 6$, $S(n) = 28$, p, q — простые.

3.15. Найти натуральное число n, если $n = 32pq$ и $S(n) = 3n$, p, q — простые.

3.16. Найти наименьшее натуральное число n такое, что

а) $\tau(n) = 11$, б) $\tau(n) = 22$, в) $\tau(n) = 13$, г) $\tau(n) = 39$.

3.17. Найти все натуральные n, для которых $\tau(n) = 9$, $S(n) = 91$.

3.18. Доказать, что

а) $\tau(1)+\tau(2)+\cdots+\tau(n)=[\frac{n}{1}]+[\frac{n}{2}]+\cdots+[\frac{n}{n}]$,

б) $S(1)+S(2)+\cdots+S(n)=1\cdot[\frac{n}{1}]+2[\frac{n}{2}]+\cdots+n[\frac{n}{n}]$.

4 Умножение Дирихле и функция Эйлера

Пусть $f,g:\mathbb{N}\to\mathbb{C}$. Произведение Дирихле функций f и g определяется формулой

$$(f\circ g)(n)=\sum_{d|n}f(d)g(\frac{n}{d}).$$

4.1. Доказать, что произведение Дирихле ассоциативно.

4.2. Определим функцию α равенствами $\alpha(1)=1$ и $\alpha(n)=0$ для $n>1$. Пусть $f:\mathbb{N}\to\mathbb{C}$ произвольная функция. Доказать $f\circ\alpha=\alpha\circ f=f$.

4.3. Определим функцию β равенствами $\beta(n)=1$ для всех $n\geq 1$. Пусть $f:\mathbb{N}\to\mathbb{C}$ произвольная функция. Доказать $f\circ\beta=\beta\circ f=\sum\limits_{d|n}f(d)$.

4.4. Доказать, что $\beta\circ\mu=\mu\circ\beta=\alpha$.

4.5. Формула обращения Мебиуса. Пусть $f:\mathbb{N}\to\mathbb{C}$ произвольная функция. Определим $F(n)=\sum\limits_{d|n}f(d)$. Доказать, что

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

4.6. Доказать, что $\sum\limits_{d|n}\varphi(d)=n$ (Гаусс).

(Рассмотреть числа $1/n,2/n,\ldots,n/n$, сократив числители и знаменатели, выяснить что означает количество чисел со знаменателем d.)

4.7. Пусть $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_l^{\alpha_l}$ каноническое разложение числа n. Доказать, что

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

4.8. Доказать, что $\varphi(mn)=\varphi(m)\varphi(n)\dfrac{d}{\varphi(d)}$, где $d=(m,n)$.

4.9. Найти все m, для которых $\varphi(m)=4$.

4.10. Вычислить а) $\varphi(\varphi(12))$, б) $\varphi(\varphi(20))$, в) $\varphi(\varphi(14))$.

4.11. Решить уравнения

а) $\varphi(x) = \dfrac{2x}{3}$, г) $\varphi(2x) = \varphi(5x)$, ж) $\varphi(x) = 3$,

б) $\varphi(x) = \dfrac{4x}{11}$, д) $\varphi(3x) = \varphi(5x)$, з) $\varphi(x) = 6$,

в) $\varphi(x) = \dfrac{x}{6}$, е) $\varphi(13x) = \varphi(17x)$, и) $\varphi(x) = 10$.

4.12. Найти количество натуральных чисел, не превосходящих 1000, и взаимно простых с 77.

4.13. Найти количество натуральных чисел, не превосходящих 875, и взаимно простых с 175.

4.14. Найти количество простых чисел, не превосходящих $2^{30} - 1$, и взаимно простых с $2^{10} - 1$.

4.15. Решить уравнения

а) $\varphi(x) = r(x)$, в) $\varphi(3x + 1) = \varphi(6x + 2)$,

б) $\varphi(6x - 3) = \varphi(2x - 1)$, г) $\varphi(3x - 1) = \varphi(9x - 3)$.

4.16. Вычислить $\sum\limits_{k=0}^{\infty} \dfrac{\varphi(p^k)}{p^{ks}}$, $s \in \mathbb{R}$, $s > 1$.

4.17. Доказать, что

а) $\varphi(4n) = 2\varphi(2n)$, г) $\varphi(n) + \tau(n) = S(n) \Leftrightarrow n \in P$,

б) $\varphi(4n + 2) = \varphi(2n + 1)$, д) $\varphi(n) + S(n) = nr(n) \Leftrightarrow n \in P$,

в) $a \mid b \Rightarrow \varphi(a) \mid \varphi(b)$, е) $p, 2p + 1 \in P \Rightarrow \varphi(4p + 2) = \varphi(4p) + 2$.

4.18. Доказать, что

а) $\sum\limits_{k=1}^{n} \varphi(k)[\dfrac{n}{k}] = \dfrac{n(n+1)}{2}$, в) $\sum\limits_{k=1}^{n} [\dfrac{1}{(n,k)}] = \varphi(n)$,

б) $\sum\limits_{d|n} \tau(d)\varphi(\dfrac{n}{d}) = S(n)$, г) $\sum\limits_{k=1}^{n} (n,k) = \sum\limits_{d|n} d\varphi(\dfrac{n}{d})$.

Здесь τ и S –функции из задач 3.5 и 3.6.

4.19. Решить уравнения

а) $\mu(5x) = \mu(3x)$, $x \in [5, 25]$,

б) $\mu(2x) = \mu(7x)$, $x \in [10, 30]$.

4.20. Вычислить

а) $\sum\limits_{d|n} \mu(d)d^k$, б) $\sum\limits_{d|n} \dfrac{\mu(d)}{\varphi(d)}$, в) $\sum\limits_{d|n} \dfrac{\mu^2(d)}{\varphi^2(d)}$,

г) $\sum\limits_{d|n} \mu(d)r(d)$, д) $\sum\limits_{d|n} \mu(d)r^3(d)$, е) $\sum\limits_{d|n} \dfrac{\mu(\dfrac{n}{d})d}{\varphi(d)}$.

5 Цепные дроби

Конечной цепной дробью называется выражение

$$\delta_n = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}},$$

где $q_1 \geq 0$, $q_i > 0$ при $i > 0$ и $q_n > 1$. Будем сокращенно записывать цепную дробь в виде $< q_1, q_2, \ldots, q_n >$

Теорема 5.1 *Всякое рациональное число* $\frac{a}{b} > 0$ *разлагается в конечную цепную дробь. При этом* q_i *неполные частные в алгоритме Евклида вычисления* (a, b).

Пусть $a = bq_1 + r_2$, $b = r_2q_2 + r_3, \ldots, r_{n-1} = r_nq_n$. Тогда $\frac{a}{b} = \delta_n$.

Приводя к общему знаменателю можно записать δ_s в виде обычной дроби. Обозначим $\delta_s = \frac{P_s}{Q_s}$, где $P_0 = 1$, $Q_0 = 0$, $P_1 = q_1$, $Q_1 = 1$. Тогда $P_s = q_sP_{s-1} + P_{s-2}$ и $Q_s = q_sQ_{s-1} + Q_{s-2}$; $(P_s, Q_s) = 1$.

Значения P_s и Q_s удобно вычислять с помощью таблицы

q_s		q_1	q_2	$\ldots$	q_{n-1}	q_n
P_s	1	q_1	P_2	$\ldots$	P_{n-1}	a
Q_s	0	1	Q_2	$\ldots$	Q_{n-1}	b

Если $\alpha =< q_1, q_2, \ldots, q_n >$, то $|\alpha - \frac{P_s}{Q_s}| < \frac{1}{Q_s^2}$, при $s \leq n$.

Для любой бесконечной последовательности натуральных чисел $q_0, q_1, \ldots$ существует $\alpha = \lim\limits_{n\to\infty} \frac{P_n}{Q_n}$, причем α — иррациональное число. Данная последовательность $q_0, q_1, \ldots = q_0, \ldots, q_{s-1}, (q_s, \ldots, q_r)$ периодична тогда и только тогда, когда α — квадратичная иррациональность.

5.1. Разложить в цепные дроби:

(a) $\dfrac{125}{92}$; (b) $\dfrac{127}{52}$, (c) $1,23$.

5.2. Свернуть непрерывные дроби:

(a) $<1,1,2,1,2,1,2>$, (b) $<0,1,2,3,4,5>$.

5.3. Следующие числа заменить дробями с возможно меньшими знаменателями так, чтобы погрешность не превосходила 10^{-4}:

(a) $\dfrac{1261}{881}$; (b) $\dfrac{587}{103}$.

5.4. Разложить в цепную дробь числа

а) $\sqrt{11}$, г) $\dfrac{1+\sqrt{5}}{2}$,

б) $1-2\sqrt{6}$, д) $\dfrac{7+2\sqrt{3}}{4}$,

в) $\dfrac{2+\sqrt{13}}{5}$, е) $\dfrac{2+\sqrt{11}}{2}$.

5.5. Найти значение цепной дроби

а) $\langle 2,(1)\rangle$, г) $\langle 1,5,2,(3)\rangle$,

б) $\langle 1,(1,2)\rangle$, д) $\langle -4,(1,3,1)\rangle$,

в) $\langle (2,1,1,4)\rangle$, е) $\langle -5,1,4,(10,5)\rangle$.

Теорема 5.2 *Пусть d — натуральное число, не равное квадрату целого и*

$$\sqrt{d}=\langle a_0;(a_1,\ldots,a_k,2a_0)\rangle$$

— разложение в цепную дробь с наименьшим периодом. Тогда множество решений уравнения Пелля

$$x^2-dy^2=1$$

в натуральных числах состоит из пар (P_n,Q_n) числителей и знаменателей подходящих дробей к $\sqrt{d}$ с условием, что $n+1$ четно и делится на $k+1$. Определим целые положительные числа x_1, y_1 равенствами

$$x_1+y_1\sqrt{d}=\begin{cases}P_k+Q_k\sqrt{d}, & \text{если } k \text{ нечетно},\\ (P_k+Q_k\sqrt{d})^2, & \text{если } k \text{ четно}.\end{cases}$$

Все решения уравнения Пелля в натуральных числах образуют последовательность (x_m,y_m) и получаются по формуле

$$x_m+y_m\sqrt{d}=(x_1+y_1\sqrt{d})^m,\quad m=1,2\ldots$$

5.6. Найти все целочисленные решения уравнений

а) $x^2 - 5y^2 = 1$, в) $x^2 - 41y^1 = 1$,

б) $x^2 - 19y^2 = 1$, г) $x^2 - 13y^2 = 1$.

6 Теорема Эйлера и ее применение

Теорема 6.1 *Чтобы* $a^{\varphi(m)} \equiv 1 \mod m$, *необходимо и достаточно, чтобы* $(a, m) = 1$.

6.1. Доказать, что любое нечетное целое число не кратное 5, в 12-той степени оканчивается на 1.

6.2. Доказать, что если $(a, 7) = 1$, то $7|a^{12} - 1$.

6.3. Доказать, что если $(a, 65) = (b, 65) = 1$, то $65|a^{12} - b^{12}$.

6.4. Пусть p – простое число. Доказать, что число вида $a^{p-1} + p - 1$, где $a \not\equiv 0 \mod p$, является составным.

6.5. Пусть p – простое число. Доказать, что $(a + b)^p \equiv a^p + b^p \mod p$.

6.6. Доказать, что наименьшее целое положительное x, удовлетворяющее сравнению $a^x \equiv 1 \mod m$, где $(a, m) = 1$, является делителем числа $\varphi(m)$.

6.7. Доказать, что натуральное число m не делящееся ни на 2, ни на 3, ни на 5 является делителем $\varphi(m)$-значного числа вида $11\ldots1$.

6.8. Доказать, что если $\sum\limits_{i=1}^{n} a_i \equiv 0 \mod 30$, то $\sum\limits_{i=1}^{n} a_i^5 \equiv 0 \mod 30$.

6.9. Доказать, что $p_1^{p_2-1} + p_2^{p_1-1} \equiv 1 \mod p_1 p_2$, где p_1, p_2–различные простые числа.

6.10. Доказать, что если $(a, m) = 1$ и $\alpha_1 \equiv \alpha_2 \mod \varphi(m)$, то $a^{\alpha_1} \equiv a^{\alpha_2} \mod m$.

6.11. Найти остаток от деления

а) 5^{14} на 7, в) 5^{100} на 11, д) 15^{175} на 11,

б) 24^{16} на 7, г) 3^{100} на 16, е) 3^{20} на 28.

6.12. Найти две последние цифры десятичной записи числа

а) 2^{999}, в) 123^{2010}, д) 200^{100},

б) 5^{2011}, г) 557^{2012}, е) 55^{150}.

6.13. Для любого натурального n найти остаток от деления 5^{21^n} на 37.

6.14. Найти две последние цифры десятичной записи числа $7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}$, если в конструкции участвует 1001 семерка.

7 Решение сравнений первой степени

7.1. Пусть $m > 0$ фиксированное целое число, $a, b \in \mathbb{Z}$. Будем говорить, что a эквивалентно b ($a \sim b$), если $m|a - b$. Показать, что это действительно отношение эквивалентности.

7.2. Пусть $m > 0$ фиксированное целое число. Обозначим через $[a] = \{x \in \mathbb{Z} | m|(a - x)\}$ класс эквивалентных элементов относительно введенного выше порядка. Показать, что

1. $[a] + [b] := \{x + y | x \in [a], y \in [b]\} = [a + b]$.
2. $[a] \cdot [b] := \{xy | x \in [a], y \in [b]\} = [ab]$.
3. Показать, что $Z_m = \{[0], [1], \ldots, [m - 1]\}$ кольцо относительно введенных операций.

Сравнение первой степени с одним неизвестным это сравнение вида

$$ax \equiv b \mod m. \tag{1}$$

Теорема 7.1 *(1) Если $(a, m) = 1$, то сравнение имеет единственное решение, которое находится по формуле*

$$x \equiv a^{\varphi(m)-1} b \mod m$$

или по формуле

$$x \equiv (-1)^{n-1} P_{n-1} b \mod m,$$

где P_{n-1} числитель предпоследней подходящей дроби в разложении $\dfrac{m}{a}$ в цепную дробь.

(2) Если $(a, m) = d$, то сравнение имеет решение, только если $d|b$. При этом сравнение имеет d решений, которые находятся по формулам

$$x_k \equiv x_0 + k\frac{m}{d} \mod m,$$

$k = 1, 2, \ldots, d - 1$, а x_0 решение сравнения

$$\frac{a}{d} x_0 \equiv \frac{b}{d} \mod \frac{m}{d}.$$

7.3. Решить сравнения первой степени:
(a) $29x \equiv 1 \mod 17$; (b) $21x + 5 \equiv 0 \mod 29$;
(c) $6x \equiv 27 \mod 12$; (d) $8x \equiv 20 \mod 12$;
(e) $(a^2 + b^2)x \equiv a - b \mod ab$, $(a, b) = 1$; (f) $ax \equiv 1 \mod p$, p-простое и $p \nmid a$.
7.4. Решить в целых числах уравнения:
(a) $5x + 4y = 3$ (сводится к системе $5x \equiv 3 \mod 4$ и $4y \equiv 3 \mod 5$);
(b) $17x + 13y = 1$.
7.5. На прямой $8x - 13y + 6 = 0$ найти число целых точек, лежащих между прямыми $x = -100$ и $x = 100$.
7.6. Доказать, что внутри прямоугольника, ограниченного прямыми $x = -2$, $x = 5$ и $y = -1$, $y = 2$, на прямой $3x - 7y - 1 = 0$ не лежит ни одной целой точки.
7.7. Решить сравнение

а) $3x \equiv 1 \pmod 7$, д) $78x \equiv 102 \pmod{273}$,
б) $100x \equiv 21 \pmod{23}$, е) $315x \equiv -10 \pmod{275}$,
в) $42x \equiv 33 \pmod{90}$, ж) $76x \equiv 232 \pmod{220}$,
г) $20x \equiv 12 \pmod{48}$.

8 Китайская теорема об остатках и системы сравнений первой степени

Пусть $m_1, m_2, \ldots, m_k$ – попарно взаимные простые числа, то система

$$\begin{cases} x \equiv c_1 \mod m_1 \\ x \equiv c_2 \mod m_2 \\ \qquad \ldots \\ x \equiv c_k \mod m_k \end{cases} \tag{2}$$

имеет решение, которое единственно по модулю $m = m_1 m_2 \ldots m_k$.

Для решения системы необходимо найти $y_1, y_2, \ldots, y_k$, удовлетворяющие сравнениям $\dfrac{m}{m_j} y_j \equiv 1 \mod m_j$. Тогда решение имеет вид

$$x = \sum_{j=1}^{k} \frac{m}{m_j} y_j c_j.$$

8.1. Решить следующие системы сравнений

(1) $\begin{cases} x \equiv 2 \mod 5 \\ x \equiv 8 \mod 11 \end{cases}$; (2) $\begin{cases} 4x \equiv 3 \mod 7 \\ 5x \equiv 4 \mod 6 \end{cases}$;

(3) $\begin{cases} 17x \equiv 7 \mod 2 \\ 2x \equiv 1 \mod 3 \\ 2x \equiv 2 \mod 5 \end{cases}$; (4) $\begin{cases} 3x \equiv 5 \mod 7 \\ 2x \equiv 3 \mod 5 \\ 3x \equiv 3 \mod 9 \end{cases}$.

8.2. Найти все натуральные числа, делящиеся на 5 и дающие при делении на 2, 3, 4 в остатке 1.

8.3. (Старинная французская задача). Женщина несла на рынок корзину яиц. Прохожий нечаянно толкнул корзину и разбил яйца. Желая возместить ущерб, он спросил сколько было яиц в корзине. "Точно не помню, – ответила женщина, – но когда я раскладывала яйца по 2,3,4,5,6 яиц, то в корзине оставалось 1 яйцо, а когда по 7, то ничего не оставалось". Сколько было яиц?

8.4. Найти все значения a, при которых имеет решение система

$\begin{cases} 2x \equiv a \mod 4 \\ 3x \equiv 4 \mod 10 \end{cases}$

8.5. Найти хотя бы одно значение m, при котором не имеет решение система

$\begin{cases} x \equiv 3 \mod 6 \\ x \equiv 7 \mod m \end{cases}$

8.6. Найти целые точки прямых $4x-7y=9$, $2x+9y=15$ и $5x-13y=12$, лежащие на одном перпендикуляре к оси абсцисс.

8.7. Решить сравнение с двумя неизвестными (a) $x+2y \equiv 1 \mod 3$; (b) $2x-y \equiv 1 \mod 4$.

8.8. Решить системы сравнений

(a) $\begin{cases} x+3y \equiv 5 \mod 7 \\ 4x \equiv 5 \mod 7 \end{cases}$; (b) $\begin{cases} 9y \equiv 15 \mod 12 \\ 7x-3y \equiv 1 \mod 12 \end{cases}$.

8.9. Решить систему сравнений

а) $\begin{cases} x \equiv 3 \pmod 8, \\ x \equiv 11 \pmod{20}, \\ x \equiv 1 \pmod 5, \end{cases}$ б) $\begin{cases} 5x \equiv 11 \pmod{18}, \\ 3x \equiv 9 \pmod{16}, \\ 8x \equiv 4 \pmod{25}, \end{cases}$

в) $\begin{cases} 6x \equiv 2 \pmod{20}, \\ x \equiv -2 \pmod 5, \\ 4x \equiv 11 \pmod{29}, \end{cases}$ г) $\begin{cases} 6x \equiv -8 \pmod{15}, \\ 8x \equiv -4 \pmod{12}, \\ 4x \equiv 5 \pmod 7. \end{cases}$

8.10. Для нечетного простого числа p решить систему сравнений первой степени

а) $\begin{cases} x \equiv 1 \pmod{(p-1)}, \\ x \equiv 2 \pmod{p}, \\ x \equiv 3 \pmod{(p+1)}, \end{cases}$ б) $\begin{cases} x \equiv p-2 \pmod{(p+1)}, \\ x \equiv p+2 \pmod{(p-1)}. \end{cases}$

8.11. При каких целых a совместна система сравнений первой степени

а) $\begin{cases} x \equiv a \pmod{42}, \\ x \equiv 11 \pmod{70}, \end{cases}$ б) $\begin{cases} x \equiv a \pmod{28}, \\ x \equiv a^2 \pmod{77}. \end{cases}$

9 Решение сравнений. Сравнения по примарному модулю.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ многочлен с целыми коэффициентами. Рассмотрим сравнение

$$f(x) \equiv 0 \mod m.$$

Если $m = p$ – простое число, то сравнение равносильно сравнению $r(x) \equiv 0 \mod p$ степени не выше чем $p-1$, где $r(x)$ остаток от деления многочлена $f(x)$ на $x^p - x$.

Если $m = m_1m_2 \ldots m_n$, где m_i взаимно просты, то сравнение равносильно системе $f(x) \equiv 0 \mod m_i$, $i = 1, \ldots, n$.

Если $m = p^n$. То решение сводится к решению сравнений вида $f(x) \equiv 0 \mod p$.

Последовательно находим $x_1, x_2, \ldots, x_n$ следующим образом:
x_1 – решение сравнения $f(x) \equiv 0 \mod p$, при $f'(x_1) \neq 0$ находим $x_{i+1} = x_i + p^it$, где t решение сравнения $\dfrac{f(x_i)}{p^i} + tf'(x_i) \equiv 0 \mod p$.

Искомое x равно x_n.

9.1. Решить сравнения:
(a) $x^2 + 2x + 2 \equiv 0 \mod 9$;
(b) $9x^2 + 29x + 62 \equiv 0 \mod 64$;
(c) $6x^3 + 27x^2 + 17x + 20 \equiv 0 \mod 30$;
(d) $x^3 + 2x + 2 \equiv 0 \mod 125$;
(e) $x^2 \equiv p \mod p^2$.

9.2. Доказать, что сравнение $x^2 \equiv a \mod 4$, где $(a,2)=1$, имеет решение тогда и только тогда, когда $a \equiv 1 \mod 4$. Найти все решения сравнения при $a \equiv 1 \mod 4$.

9.3. Доказать, что сравнение $x^2 \equiv a \mod 8$, где $(a,2)=1$, имеет решение тогда и только тогда, когда $a \equiv 1 \mod 8$. Найти все решения сравнения при $a \equiv 1 \mod 8$.

9.4. Доказать, что сравнение $x^2 \equiv a \mod 2^k$, где $(a,2)=1$ и $k>2$, имеет решение тогда и только тогда, когда $a \equiv 1 \mod 8$. Доказать, что в этом случае существует ровно 4 решения.

9.5. Решить сравнение

а) $x^4+2x^3+8x+9 \equiv 0 \pmod{35}$,

б) $103x^{103}+88x^{73}+210x^{13}+100 \equiv 0 \pmod{105}$,

в) $725x^{603}-507x^{407}-311x^{126}+85 \equiv 0 \pmod{77}$,

г) $x^{p-1}+x^{p-2}+\cdots+x+1 \equiv 0 \pmod{p}$, где $p \in P$,

д) $x^{p-2}+x^{p-3}+\cdots+x+1 \equiv 0 \pmod{p}$, где $p \in P$,

е) $(p-1)x^{p-2}-(p-2)x^{p-3}+\cdots+3x^2+2x-1 \equiv 0 \ (p)$, где $p \in P$.

9.6. Решить сравнение

а) $x^3+2x+2 \equiv 0 \pmod{125}$,

б) $4x^3+6x^2+7x \equiv 0 \pmod{125}$,

в) $3x^4-8x^3+8x^2-3x+3 \equiv 0 \pmod{27}$,

г) $x^3+6x+7 \equiv 0 \pmod{27}$.

10 Дополнительные задачи

10.1. Доказать, что следующие области не являются факториальными: $\mathbb{Z}\left[\sqrt{-5}\right]$; $\mathbb{Z}\left[\sqrt{-10}\right]$.

10.2. Показать, что следующие области являются евклидовыми:
(a) $\mathbb{Z}[i]$; (b) $\mathbb{Z}\left[\sqrt{-2}\right]$; (c) $\mathbb{Z}\left[\sqrt{3}\right]$; (d) $\mathbb{Z}\left[\sqrt{6}\right]$.

10.3. Решить уравнения в целых числах.
(a) $y^2+1=x^3$;
(b) $y^2+4=x^3$;
(c) $y^2=x^3+1$.

10.4. (Криптографический алгоритм шифрования с открытым ключом RSA) Пусть p,q – простые числа, $n=pq$ их произведение, d – целое число взаимно простое с $\varphi(n)$. Доказать, что если $cd \equiv 1 \mod \varphi(n)$, то

для любого целого x $(0 \le x < n)$

$$x^{cd} \equiv x(\mod n).$$

10.5. Пусть $p = 3$, $q = 11$, $d = 3$. Вычислить c – взаимно обратное к d по модулю $\varphi(pq) = 20$. "Зашифровать" сообщение 5, то есть найти $5^3(\mod 33)$. Вычислить для проверки $(5^3)^c(\mod 33)$.

10.6. Доказать, что в системе шифрования RSA с модулем $n = 35$ все ключи шифрования совпадут с ключами дешифрования (то есть для любого d взаимно простого с $\varphi(n)$ выполнено $dd = 1(\mod n)$).

10.7. При шифровании в системе RSA с модулем n ключ шифрования совпал с ключом дешифрования. Объяснить причину.

11 Квадратичные вычеты

Число a называется квадратичным вычетом по модулю простого нечетного числа p, если сравнение $x^2 \equiv a \mod p$ имеет решение. В противном случае a называется квадратичным невычетом.

Символ Лежандра

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ квадратичный вычет} \\ -1, & \text{если } a \text{ квадратичный невычет} \end{cases}$$

Свойства символа Лежандра.

1. Если $a \equiv b \mod p$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; в частности, если $p \not| b$ то $\left(\frac{b^2}{p}\right) = 1$.
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;
4. $\left(\frac{1}{p}\right) = 1$;
5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

6. $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$, здесь q простое нечетное число (*закон взаимности квадратичных вычетов*)

11.1. Вычислить символ Лежандра:
(a) $\left(\frac{13}{7}\right)$; (b) $\left(\frac{22}{13}\right)$; (c) $\left(\frac{426}{491}\right)$.

11.2. При помощи символа Лежандра выяснить, какие из следующих сравнений разрешимы:
1) $x^2 \equiv 5 \mod 13$; 2) $x^2 \equiv 5 \mod 29$
3) $x^2 \equiv 2 \mod 97$; 4) $x^2 \equiv 151 \mod 587$.

11.3. При помощи критерия Эйлера выяснить, какие из следующих сравнений разрешимы и найти соответствующие решения:
1) $x^2 \equiv -3 \mod 7$; 2) $x^2 \equiv 3 \mod 11$
3) $x^2 \equiv 6 \mod 7$.

11.4. Найти значения a, при которых имеют решения сравнения:
1) $x^2 \equiv a \mod 3$; 2)$x^2 \equiv a \mod 5$;
3) $x^2 \equiv a \mod 7$; 4) $x^2 \equiv a \mod 11$;.

11.5. Доказать, что сравнение $x^2 + 1 \equiv 0 \mod p$ имеет решение тогда и только тогда, когда $p = 4n + 1$ $(n = 1, 2, 3, \ldots)$.

11.6. Доказать, что каноническое разложение чисел вида $a^2 + b^2$, где $(a, b) = 1$, содержит простые числа вида $p = 4n + 1$ $(n = 1, 2, 3, \ldots)$ и только такие простые числа.

11.7. Доказать, что произведение двух последовательных натуральных чисел при делении на 13 не может давать в остатке 1.

11.8. Доказать, что следующие сравнения разрешимы при любом простом $p > 2$:
(1) $(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \mod p$;
(2) $(x^2 - 3)(x^2 - 5)(x^2 - 7)(x^2 - 11)(x^2 - 1155) \equiv 0 \mod p$.

11.9. Решить уравнения в целых числах (найти целые точки, через которые проходят кривые):
(1) $4x^2 - 5y = 6$; (2) $11y = 5x^2 - 7$; (3) $13y = x^2 - 21x + 110$.

11.10. Найти все таки простые числа p, что разрешимы сравнения:
1) $x^2 \equiv 5 \mod p$; 2) $x^2 \equiv 2 \mod p$
3) $x^2 \equiv -7 \mod p$.

11.11. Вычислить $\sum\limits_{x=2}^{p-1}\left(\frac{x}{p}\right)$

11.12. Существует ли такое n, что число $1+2+\ldots+n$ оканчивается на 7.

11.13. Указать число решений сравнения

а) $2x^2+7x+5\equiv 0 \pmod{37}$,

б) $3x^2+5x+70\equiv 0 \pmod{87}$,

в) $5x^2+2x-5\equiv 0 \pmod{71}$,

г) $5x^2+x+8\equiv 0 \pmod{289}$.

11.14. Для каких простых p число 3 является квадратичным невычетом?

11.15. Для каких простых p число 7 является квадратичным вычетом?

11.16. Указать все простые делители квадратичной формы

а) $2y^2+10$, б) $3x^2+15$, x^2+10y^2.

11.17. Найти наименьшее натуральное число a, для которого сравнение $x^2\equiv a \pmod{101}$ неразрешимо.

12 Первообразные корни и индексы

Пусть n положительное целое число, $\mathbb{Z}_n$ кольцо вычетов по модулю n, $U=U(\mathbb{Z}_n)$ группа обратимых элементов кольца $\mathbb{Z}_n$.

Если $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, то $\mathbb{Z}_n\cong\mathbb{Z}_{p_1^{\alpha_1}}\bigoplus\mathbb{Z}_{p_2^{\alpha_2}}\bigoplus\ldots\bigoplus\mathbb{Z}_{p_k^{\alpha_k}}$ и $U(\mathbb{Z}_n)\cong U(\mathbb{Z}_{p_1^{\alpha_1}})\times U(\mathbb{Z}_{p_2^{\alpha_2}})\times\ldots\times U(\mathbb{Z}_{p_k^{\alpha_k}})$.

Порядок группы U равен $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$.

Теорема 12.1 *Пусть n целое положительное число. Группа $U(\mathbb{Z}_n)$ циклическая группа при n равном $n=2,4,p^\alpha$ или $2p^\alpha$, где p простое нечетное число. В остальных случаях группа $U(\mathbb{Z}_n)$ не является циклической.*

Число a, порождающее $U(\mathbb{Z}_n)$, называется первообразным корнем по модулю n.

Пусть $(a,n)=1$. Говорят, что m порядок элемента a по модулю n, если m порядок элемента $\overline{a}=a+n\mathbb{Z}$ в группе $U(\mathbb{Z}_n)$. Будем писать в этом случае $o(\overline{a})=m$.

Элемент a первообразный корень по модулю n тогда и только тогда, когда $o(\overline{a}) = \varphi(n)$.

12.1. Найти первообразные корни по модулю 11, 13, 17.

12.2. Показать, что 2 первообразный корень по модулю 29.

12.3. Показать, что если $p = 2^n + 1$ простое число Ферма, то 3 первообразный корень по модулю p.

12.4. Пусть a первообразный корень по модулю числа p^n (p простое). Доказать, что a первообразный корень по модулю p.

Первообразные корни по модулю p^k и $2p^k$.

Далее p простое нечетное число, $n = p^k$ или $n = 2p^k$. В этом случае $U(\mathbb{Z}_n)$ циклическая группа. Пусть g примитивный корень по модулю n и $(a, n) = 1$.

В этом случае $a = g^l$ для некоторого $1 \leq l \leq \varphi(n) - 1$. Число l называется индексом a по модулю n и обозначается $l = \mathrm{ind}a = \mathrm{ind}_g a$. Индекс аналогичен понятию логарифма, при этом первообразный корень играет роль аналогичную основанию логарифма.

$$\mathrm{ind}ab = \mathrm{ind}a + \mathrm{ind}b$$

Для небольших p составлены таблицы индексов.

Теорема 12.2 *Пусть $(m, \varphi(n)) = d$. Сравнение*

$$x^m = a \mod n$$

разрешимо тогда и только тогда, когда ind$a$ *делится на d. В случае разрешимости сравнение имеет d решений.*

Отметим, что сравнение $x^m \equiv a \mod n$ эквивалентно $m\mathrm{ind}x \equiv \mathrm{ind}a \mod \varphi(n)$.

12.5. По таблице индексов найти индексы по модулю 41 следующих чисел: 27, 21, 2.

12.6. Составить таблицу индексов по модулю 11.

12.7. Пользуясь таблицей индексов решить сравнения:

(a) $x^{60} \equiv 79 \mod 97$;

(b) $x^{55} \equiv 17 \mod 97$;

(c) $x^{15} \equiv 46 \mod 97$;

(d) $x^7 \equiv 7 \mod 11$.

12.8. Решить сравнения

а) $12x^{18} \equiv 54 \pmod{13}$, в) $x^{18} \equiv 1 \pmod{77}$,

б) $x^6 \equiv 23 \pmod{13}$, г) $x^{12} \equiv 1 \pmod{77}$.

12.9. Используя свойства индексов, найти остаток от деления

а) 100^{300} на 13, в) 200^{400} на 17,

б) 300^{500} на 19, г) 100^{200} на 11.

12.10. Через какие точки (x, y) с целыми координатами x и y проходит кривая

а) $19y = 3x^4 + 22$, б) $13y = 3x^2 + 20$.

Литература

[1] Виноградов И.М. *Основы теории чисел* – М.:Наука – 1981. – 172 с

[2] Айерленд К., Роузен М. *Классическое введение в современную теорию чисел.* – М.:Мир – 1987. – 428 с

[3] Кудреватов Г.А. *Сборник задач по теориии чисел.* – М.:Просвещение – 1970. – 128 с

[4] *Задачи и упражнения по теории чисел. Часть 1* – Н. Новгород.:ННГУ – 1995. – 29 с

[5] *Задачи и упражнения по теории чисел. Часть 2* – Н. Новгород.:ННГУ – 1995. – 32 с

[6] Корешков Н.А. *Теория чисел: учебно-методическое пособие* – Казань:Издательство Казанский университет – 2010. – 44 с