Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Теория чисел

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности

ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля: контрольная работа (ИОПК-3.1);

Пример.

1. Решите сравнение 8 x ≡ 13 (19).

2. Решить систему сравнений $\begin{cases} x \equiv 1(3) \\ x \equiv 2(5) \\ x \equiv 1(7) \end{cases}$

3. Найдите каноническое разложение числа 20! на простые множители.

4 Пусть n = 225.

Найти: а) число делителей б) сумму делителей в) функцию Эйлера.

5. Представить рациональное число 43/30 в виде цепной дроби, затем с помощью подходящих дробей восстановить исходное число.

6. Найти иррациональное число, представленное данной периодической цепной дробью: [(2,1)]

7. Найти остаток от деления $208^{362}+17^{184}$ на 19

8. Решить сравнение методом понижения степени: $x^8+x^6+4x^5+2x^3-4x+1\equiv 0(5)$.

9. Решить сравнение по составному модулю: $x^3+x^2+3x+2\equiv 0(35)$.

10. Выяснить с помощью символа Лежандра, разрешимо ли сравнение $x^2\equiv 31(43)$.

11. Найти количество первообразных корней по модулю 97.

Ответы.

1. {4+19k} 2. {22+105k} 3. $2^{18}\cdot 3^8\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19$

4. а) 9 б) 403 в) 120 5. [1,2,3,4] 6. $1+\sqrt{3}$ 7. 17

8. {1+5k} и {3+5k}. 9. {22+35k} 10. Да (символ Лежандра равен 1) 11. 32.

Критерии оценивания: суммарно за всю работу в семестре студент можно получить 3,5 балла из 5,0, то есть 70% от итоговой оценки. Ещё 30% - за ответ по теории на экзамене.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзамен проводится по билетам, билет состоит из 2 теоретических вопросов. За верный ответ по теории студент получает 1,5 балла из 5 баллов оценки. При сложении с семестровым рейтингом за практику (3,5 балла из итоговой оценки) студент получает 5,0 баллов. В случае получения дробной оценки, итоговая оценка определяется по правилам округления.

Вопросы к экзамену на доказательства (ИОПК-3.2, ИОПК-3.3).

1. Докажите, что остаток r_k, полученный при алгоритме Евклида, является общим делителем для a,b

2. Докажите, что остаток r_k, полученный при алгоритме Евклида, является аибольшим среди общих делителей.

3. Доказать рекурсивные формулы для коэффициентов Безу: $u_k = u_{k-2} - q_k u_{k-1}$,

$v_k = v_{k-2} - q_k v_{k-1}$

4. Любое из доказательств теоремы Евклида о бесконечности множества простых чисел.

5. Докажите, что для любого $k \geq 1$ найдётся k составных чисел подряд.

6. Доказать, что если $n \in N$ не делится ни на одно простое число, меньшее или равное [$\sqrt{n}$], то оно простое.

7. Основная теорема арифметики: Каждое натуральное число $n > 1$ может быть представлено в виде произведения простых чисел: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, две таких записи могут отличаться лишь порядком следования сомножителей.

8. Доказать, что если p простое, то $\sqrt{p}$ иррационально.

9. Пусть $a = p_1^{s_1} \cdot \ldots \cdot p_m^{s_m}$, $b = p_1^{t_1} \cdot \ldots \cdot p_m^{t_m}$, доказать, что

НОД (a,b) = $p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$, где $k_i = \min(s_i, t_i)$,

10. Доказать, что $[a,b](a,b) = ab$.

11. Доказать, что для всякого чётного n ≥ 4, число $2^n - 1$ составное.

12. Доказать, что для всякого нечётного составного числа n ϵ N, $2^n - 1$ составное.

13. Доказать, что число вида $2^n + 1$ может быть простым лишь при $n = 2^k$.

14. Доказать, что всякий многочлен с целыми коэффициентами, при некотором натуральном значении x = n принимает значение, равное составному числу.

15. Доказать, что показатель простого числа p в разложении n! равен

$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots + \left[\frac{n}{p^m}\right]$, где p^m последнее число, не превосходящее n.

16. Доказать формулу числа натуральных делителей: если $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$, то

$\tau(n) = (k_1 + 1) \cdot (k_2 + 1) \cdot \ldots \cdot (k_s + 1)$.

17. Доказать формулу суммы всех натуральных делителей.

Если $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$, то $\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{k_s+1} - 1}{p_s - 1}$.

18. Доказать теорему о сумме f(d) по всем натуральным делителям).

Пусть $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$. Тогда

$$\sum_{d|n} f(d) = (1 + f(p_1) + f(p_1^2) \ldots + f(p_1^{k_1})) \cdot \ldots \cdot (1 + f(p_s) + f(p_s^2) + \ldots + f(p_s^{k_s}))$$

19. Доказать, что если $n = 2^{k-1}(2^k - 1)$ то n является совершенным

20. Доказать, что если чётное число совершенно, то оно имеет вид $n = 2^{k-1}(2^k - 1)$, где $k \geq 2$, $p = 2^k - 1$ - простое.

21. Доказать свойство суммы функции Мёбиуса по всем делителям: $\sum_{d|n} \mu(d) = \begin{cases} 1 & (n = 1) \\ 0 & (n > 1) \end{cases}$

22. Доказать, что $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

23. Доказать $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$ (p, q простые).

24. Доказать $\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$.

25. Доказать, что $\varphi(n^k) = n^{k-1}\varphi(n)$.

26. Если $(m, n) = d$, то $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$.

27. Доказать формулу Гаусса $\sum_{d|n} \varphi(d) = n$

28. Доказать, что число n простое $\Leftrightarrow$ $\varphi(n) = n \cdot \tau(n) - \sigma(n)$.

29. Доказать, что $\tau(n)$ нечётно $\Leftrightarrow n = k^2$.

30. Доказать, что среднее гармоническое по всем делителям = $\tau(n)\frac{n}{\sigma(n)}$.

31. Доказать, что всякое чётное совершенное число является числом Оре.

32. Вывести рекурсивные формулы вычисления числителя и знаменателя подходящих дробей:

$\frac{P_n}{Q_n} = \frac{P_{n-1}q_n + P_{n-2}}{Q_{n-1}q_n + Q_{n-2}}$.

33. Доказать, что для подходящих дробей верно равенство: $P_nQ_{n-1} - P_{n-1}Q_n = (-1)^n$.

34. Доказать, что для подходящих дробей верно равенство:

$P_nQ_{n-2} - P_{n-2}Q_n = (-1)^{n-1}q_n$

35. Вывести формулы вычисления подходящих дробей через определители.

36. Доказать, что если цепная дробь периодическая, то соответствующее ей число есть квадратичная иррациональность.

37. Доказать, что $A\alpha^2 + B\alpha + C = 0$, то при замене $\alpha = \frac{Px + R}{Qx + S}$, при условии $|PS - QR| = 1$ получится квадратичное уравнение с тем же дискриминантом.

38. (Теорема Лагранжа). Доказать, что любая квадратичная иррациональность разлагается в периодическую цепную дробь.

39. Z_n - кольцо вычетов. Доказать: $(k, n)=1 \Leftrightarrow \bar{k}$ обратимый.

40. Z_n - кольцо вычетов. Доказать: $(k, n)=1 \Leftrightarrow \bar{k}$ не делитель нуля.

41. Если $(a,m) = 1$, $\{x_1,..., x_m\}$ - полная система вычетов по модулю m, то числа вида $\{ax_1 + b,..., ax_m + b\}$ тоже есть полная система вычетов по модулю m.

41. Если $(a,m) = 1$, $\{x_1,..., x_{\varphi(m)}\}$ - приведённая система вычетов по модулю m, то $\{ax_1,..., ax_{\varphi(m)}\}$ тоже образуют приведённую систему вычетов по модулю m.

43. Доказать, что:

1) Если $(a,m) = 1$, то $ax \equiv b(m)$ имеет единственное решение.

2) Если $(a,m) = d \neq 1$, b не делится на d, то $ax \equiv b(m)$ неразрешимо.

3) Если $(a,m) = d \neq 1$, и $b \vdots d$, то $ax \equiv b(m)$ имеет d решений.

44. Теорема Эйлера. $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1(m)$.

45. Докажите, что для любого простого числа p и $a \in Z$, $a^{p-1} \equiv 1(p)$.

(малая теорема Ферма).

46. Пусть $n = p_1 \cdot p_2 \cdot ... \cdot p_k$, и $(n-1) \vdots (p_i - 1)$ $\forall i = 1,...,k$. Докажите, что n есть число Кармайкла (абсолютно псевдопростое).

47. Пусть $p_1,..., p_k$ - простые числа, тогда существует число x, такое что: $x \equiv r_1(p_1),..., x \equiv r_k(p_k)$ (китайская теорема об остатках).

48. Докажите, что всякое сравнение $f(x) = \alpha_n x^n + ... + \alpha_1 x + \alpha_0 \equiv 0(p)$ степени $n \geq p$ равносильно некоторому сравнению степени не выше $p-1$.

49. Докажите, что если x_1 - решение сравнения $f(x) \equiv 0(p)$, то это сравнение равносильно $(x - x_1)q(x) \equiv 0(p)$, где $q(x)$ - неполное частное от деления $f(x)$ на $(x - x_1)$.

50. Докажите, что p является простым $\Leftrightarrow$ $((p-1)!+1) \equiv 0(p)$ (теорема Вильсона).

51. Докажите, что если $f(a) \equiv 0(p^k)$ и $f'(a)$ не делится на p, то существует такое t, что $f(a + p^k t) \equiv 0(p^{k+1})$.

52. Докажите, что если p - простое нечётное число, то либо $d^{\frac{p-1}{2}} \equiv 1(p)$, либо $d^{\frac{p-1}{2}} \equiv -1(p)$.

53. Докажите, что существует ровно $\frac{p-1}{2}$ квадратичных вычетов по простому нечётному модулю p.

54. Докажите, что d является квадратичным вычетом по простому нечётному модулю p $\Leftrightarrow$ $d^{\frac{p-1}{2}} \equiv 1(p)$, и не является квадратичным вычетом $\Leftrightarrow$ $d^{\frac{p-1}{2}} \equiv -1(p)$ (критерий Эйлера).

55. Докажите, что $p-1$ является квадратичным вычетом по модулю p тогда и только тогда, когда $p = 4k+1$.

56. Критерий Гаусса. Докажите, что $\left(\frac{a}{p}\right) = (-1)^t$, где t - количество чисел $\left\{a, 2a, ..., \frac{p-1}{2}a\right\}$, для которых наименьший по модулю вычет отрицателен.

57. Докажите, что $x^2 \equiv a(p)$ разрешимо $\Leftrightarrow \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]$ чётно.

58. Доказать $\left(\frac{2}{p}\right) = \begin{cases} 1 & если \quad p \equiv \pm 1(8) \\ -1 & если \quad p \equiv \pm 3(8) \end{cases}$

59. Доказать $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

60. Доказать, что для нечётного a, $x^2 \equiv a(p)$ разрешимо $\Leftrightarrow \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]$ чётно.

61. Критерий квадратичной взаимности.

Для двух простых нечётных чисел p,q: $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

62. Докажите, что для составного числа вида $n = pq$, где p,q нечётны, количество квадратичных вычетов по модулю n равно $\frac{p+1}{2} \cdot \frac{q+1}{2}$, а в общем случае $\prod_{i=1}^{k} \frac{p_i+1}{2}$.

63. Докажите, что если $\frac{pq+1}{2} > \frac{p+1}{2} \cdot \frac{q+1}{2}$, то найдутся такие x,y что $x^2 - y^2 \vdots pq$.

64. Докажите, что если a нечётно, то решениями сравнения $x^2 \equiv a(2^k)$ могут быть только числа вида 8k+1.

65. Доказать свойство символа Якоби: $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

66. Доказать, что $a^n \equiv 1(m) \Rightarrow n \vdots P_m(a)$ и следствие: $\varphi(m) \vdots P_m(a)$.

67. Доказать, что если $P_m(a) = k$, то во множестве $\{a^0, a^1, ..., a^{k-1}\}$ все элементы попарно не сравнимы.

67. Доказать, что если $P_m(a) = k$, то $a^s \equiv a^t(m) \Leftrightarrow s \equiv t(k)$.

68. Доказать, что если (a,m)=1, то $a^{L(m)} \equiv 1(m)$.

69. Доказать, что если p простое число, и $\varphi(p) = p - 1 = q_1^{b_1} \cdot ... \cdot q_s^{b_s}$, то:

a первообразный $\Leftrightarrow$ $a^{\frac{\varphi(p)}{q_1}}, ..., a^{\frac{\varphi(p)}{q_s}}$ все не сравнимы с 1 по модулю p.

70. Доказать, что показатель $P_{2^n}(a) \le 2^{n-2}$ при нечётном a и $n \ge 3$.

71. Пусть p простое. Доказать, что первообразный корень по модулю p^2 является также первообразным по модулю p.

72. Доказать, что если a первообразный по модулю p, и a^{p-1} не сравнимо с 1 по модулю p^2, то a первообразный и по модулю p^2.

73. Доказать, что если a первообразный по модулю p, то a или $a + p$ первообразный по модулю p^2.

74. Доказать свойства индексов. $ind_a bc = ind_a b + ind_a c$, $ind_a(b^n) = n \cdot ind_a b$

75. Доказать, что если простое нечётное число имеет вид $p = 4k + 1$, то существует $q \in N$, такое, что $q^2 \equiv -1(\text{mod } p)$.

76. Теорема Эйлера-Ферма. Если простое нечётное число имеет вид $4k + 1$, то оно представимо в виде суммы квадратов $x^2 + y^2$.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

В качестве материалов для проверки остаточных знаний можно использовать те же самые контрольные задачи, которые студенты решают на контрольных работах в течение семестра.

Информация о разработчиках

Приходовский Михаил Анатольевич, к.ф.м.н., доцент кафедры компьютерной безопасности ИПМКН ТГУ.