**Порядок проведения экзамена**

На экзамене каждый студент получит 6-7 вопросов разной сложности (сложность зависит от рейтинга студента).

Критерии оценки:

для получения оценки удовл. (3-4) надо знать вопросы на удовл. и основные определения и формулировки утверждений курса. В ходе экзамена необходимо будет ответить на 6 или 7 вопросов на удовл. или больше. Если вы не знаете хотя бы двух вопросов из списка на удовл., вам ставится неуд.(2). Разница между 3 и 4 определяется скоростью ответа на эти вопросы, и в спорных случаях дополнительным вопросом преподавателя.

Оценка хор. (5-6) : знать вопросы на удовл. и хор., а также основные определения и формулировки утверждений курса. В ходе экзамена необходимо будет ответить на 4 вопроса на хор. или больше. Если вы не знаете одного вопроса из списка на хор., ставится не больше хор(5). Если вы не знаете трёх вопросов на хор., ставится не больше удовл. (4). Разница между хор.(5) и хор.(6) определяется скоростью ответа на вопросы на хор. и дополнительным вопросом преподавателя. Хор.(7) ставится, если вы знаете вопросы на хор., и можете рассказать половину вопросов на отл.

Оценка отл. (8-9) : знать все вопросы, а также основные определения и формулировки утверждений курса. В ходе экзамена необходимо ответить на 3 вопроса на отл. Если вы не знаете двух вопросов на отл., то ставится хор.(7)

На отл(10) может быть задана дополнительная задача.

**Итоговая оценка**

Если $S$ — оценка в семестре, а $E$ — оценка за экзамен, то итоговая оценка $I$ равна

$$I = \begin{cases} 2, & E = 2 \\ \max(3, \min(4, [0.5 \cdot E + 0.5 \cdot S + 0.5])), & E = 3, 4 \\ \max(5, \min(7, [0.5 \cdot E + 0.5 \cdot S + 0.5])), & E = 5, 6, 7 \\ \max(8, \min(10, [0.5 \cdot E + 0.5 \cdot S + 0.5])), & E = 8, 9, 10 \end{cases},$$

где $[x]$ — целая часть $x$.

**Вопросы на удовл.**

**1.** Простые числа. Основная теорема арифметики (формулировка, существование).

**2.** Основы теории делимости: наибольший общий делитель, наименьшее общее кратное, алгоритм Евклида (доказательство того, что алгоритм остановится, и последний ненулевой член — это НОД).

**3.** Представимость наибольшего общего делителя $(a, b)$ в виде линейной целочисленной комбинации $a$ и $b$.

**4.** Лемма Евклида: формулировка, любое из доказательств, не использующее основную теорему арифметики.

**5.** Вывод единственности в основной теореме арифметики через лемму Евклида.

**6.** Основы теории сравнений. Системы вычетов. Определение сложения и умножения. Обратимые элементы. Делители нуля. Связь между ними.

**7.** Системы вычетов. Малая теорема Ферма (любое доказательство).

**8.** Системы вычетов. Теорема Эйлера.

**9.** Теорема Лагранжа о числе корней многочлена по простому модулю(б/д). Теорема Вильсона (с использованием теоремы Лагранжа).

**10.** Доказательство теоремы Вильсона с использованием первообразных корней.

**11.** Бесконечность количество простых вида $3k + 2$, $4k + 3$, $4k + 1$.

**12.** Сравнения второй степени. Квадратичные вычеты и невычеты. Количество вычетов и невычетов по простому нечётному модулю $p$.

**13.** Квадратичные вычеты и невычеты. Символ Лежандра. Формулы $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$,

$\left(\frac{a_1 \dots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \dots \left(\frac{a_n}{p}\right)$.

**14.** Умение вычислить символ Лежандра.

**15.** Матрицы Адамара. Определение. Равносильность попарной ортогональности строчек и попарной ортогональности столбцов. Канонический вид (нормальная форма). Достижение верхней оценки в неравенстве Адамара.

**16.** Существование матриц Адамара при $n = 1$ и 2. Необходимость делимости на 4 при $n > 3$. Гипотеза Адамара. Комбинаторная переформулировка гипотезы (через систему подмножеств мощности $\frac{n}{2}$ в множестве из $n-1$ элемента). Утверждение о плотности матриц Адамара в натуральном ряде (б/д).
**17.** Попытка построить матрицу для $n = 2^k$ путем наложения единиц на минус единицы (получается только $k$ строчек). Решение для $n = 2^k$ через кронекеровское произведение.
**18.** Разброс (уклонение, дискрепанс) системы подмножеств относительно раскраски. Теорема о верхней оценке (б/д).
**19.** Коды, исправляющие ошибки. Расстояние Хэмминга. Понятие $(n, M, d)$-кода. Число ошибок, исправляемых кодом. Граница Хэмминга.
**20.** Распределение простых чисел в натуральном ряде. Функции $\pi(x)$, $\theta(x)$, $\psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_1 \geqslant \lambda_2$. Постулат Бертрана (б/д). Теорема Адамара, Валле-Пуссена (б/д). «Дырки» между соседними простыми числами (б/д).
**21.** Степень вхождения простого числа в факториал и центральный биномиальный коэффициент. Неравенство

$$C_{2n}^{n} \leqslant \prod_{p \leqslant 2n} p^{\left[\log_p(2n)\right]}.$$

**22.** Показатель. Показатель элемента из множества $\mathbb{Z}_m$ делит $\varphi(m)$. Первообразный корень (определение и значения при $m \leqslant 7$). Пример модуля, по которому не существует первообразного корня. Теорема о существовании первообразного корня (б/д).
**23.** Индексы. Корректность определения в случае первообразного корня. Таблицы индексов. Решение степенных сравнений (умение).
**24.** Теорема Дирихле о диофантовых приближениях (формулировка и доказательство любым способом).
**25.** Конечные цепные дроби. Каноническая запись. Подходящие дроби. Рекуррентные соотношения для числителей и знаменателей подходящих дробей (б/д). Следствия: несократимость подходящих дробей, возрастание подходящих дробей с четными номерами и убывание подходящих дробей с нечетными номерами.
**26.** Рекуррентные соотношения для числителей и знаменателей подходящих дробей.
**27.** Определение бесконечной цепной дроби. Доказательство сходимости соответствующих подходящих цепных дробей (можно пользоваться без доказательства соотношениями на их коэффициенты).
**28.** Бесконечные периодические цепные дроби. Теорема о периодичности дроби для квадратичной иррациональности (доказательство в одну сторону). Умение находить периодическую цепную дробь по её значению, и наоборот, нахождение значения дроби по её периоду.
**29.** Квадратичные иррациональности. Множество $\mathbb{Z}[\sqrt{m}]$: сопряжение, замкнутость сложения, умножения. Согласованность сопряжения и умножения. Норма и её свойства.
**30.** Пара $(a, b)$, где $a + b\sqrt{2} = (1 + \sqrt{2})^n$ является решением уравнения Пелля $a^2 - 2b^2 = \pm 1$.
**31.** Связь между решениями уравнения Пелля $a^2 - 2b^2 = \pm 1$ и элементами $\mathbb{Z}[\sqrt{2}]$ нормой 1.
**32.** Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Степень алгебраического числа. Теорема Лиувилля (б/д).
**33.** Определение решётки (эквивалентность двух определений) и дискретного подмножества. Определитель решётки. Независимость значения определителя от выбора базиса.
**34.** Определение решётки и его определителя. Решётка $\Lambda_{\overline{a}}$ и её определитель.
**35.** Определение равномерной распределённой последовательности по модулю 1. Является ли $\sqrt{n}$ р.р. (mod 1) последовательностью?
**36.** Определение равномерной распределённой последовательности по модулю 1. Является ли р.р. (mod 1) последовательность $a^n$ при $a < 1$?
**37.** Определение всюду плотности. Последовательность $\ln n$ всюду плотна на $[0, 1]$.
**38.** Определение всюду плотности. Если последовательность равномерно распределена по модулю 1, то она и всюду плотна.
**39.** Тригонометрические суммы. Критерий Вейля для р.р. (mod 1) (формулировка). Последовательность $\alpha n$ при иррациональном $\alpha$ является р.р. (mod 1). Что происходит при рациональном $\alpha$?
**40.** Определение равномерной распределённой последовательности по модулю 1. Являются ли р.р. (mod 1) последовательности **а)** $1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \ldots$; **б)** $\frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{3}{8}, \frac{5}{8}, \frac{7}{8}, \frac{1}{16}, \frac{3}{16}, \frac{5}{16}, \frac{7}{16}, \frac{9}{16}, \frac{11}{16}, \frac{13}{16}, \frac{15}{16}, \ldots$.

**41.** Определение равномерной распределённой последовательности по модулю 1. Пусть последовательность $x_n$ р.р. $(\mathrm{mod}\ 1)$ и $m$ — фиксированное целое число, не равное нулю. Докажите, что последовательность $mx_n$ также р.р. $(\mathrm{mod}\ 1)$. Верно ли, что если $m$ — не целое, то это не верно?
**42.** Описание алгоритма AKS (6 шагов). Лемма об оценке $r$ (б/д). Оценка сложности алгоритма. Тождество $(X+a)^p = X^p + a\ (\mathrm{mod}\ p)$.

**Вопросы на хор.**

**1.** Линейная выразимость НОДа (б/д). Доказательство леммы Евклида при помощи алгоритма Евклида.
**2.** Доказательство леммы Евклида через «идеалы».
**3.** Доказательство единственности в основной теореме арифметики «от противного».
**4.** Системы вычетов. Малая теорема Ферма (4 доказательства).
**5.** Мультипликативность функции Эйлера. Формула с произведением по простым числам: вывод из свойства мультипликативности.
**6.** Теорема Лагранжа о числе корней многочлена по простому модулю.
**7.** Китайская теорема об остатках.
**8.** (умение) Решение линейных сравнений и систем линейных сравнений.
**9.** Сравнения второй степени. Квадратичные вычеты и невычеты. Тождество $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$.
**10.** Сравнения второй степени. Квадратичные вычеты и невычеты. Формула для $\left(\frac{2}{p}\right)$ (тождеством с суммой по $\left[\frac{2ax}{p}\right]$ можно пользоваться без доказательства).
**11.** Матрицы Адамара. Кронекеровское произведение и общая формулировка про $A \cdot B$.
**12.** Матрицы Адамара. (Первая) конструкция Пэли с квадратичными вычетами при $n = p{+}1$, $p = 4m{+}3$.
**13.** Матрицы Адамара. (Вторая) конструкция Пэли с квадратичными вычетами при $n = 2p+2$, $p = 4m+1$.
**14.** $(n, M, d)$-коды. Граница Плоткина.
**15.** Распределение простых чисел в натуральном ряде. Функции $\pi(x)$, $\theta(x)$, $\psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_2 \geqslant \lambda_3$.
**16.** Распределение простых чисел в натуральном ряде. Функции $\pi(x)$, $\theta(x)$, $\psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_3 \geqslant \lambda_1$.
**17.** Порядки(показатели) элементов в системах вычетов. Равенство $\mathrm{ord}(g^l) = \frac{\mathrm{ord}\, g}{(l, \mathrm{ord}\, g)}$. Следствие: если есть порядок $k$, то есть порядки и всех делителей $k$.
**18.** Порядки(показатели) элементов в системах вычетов. Если $\mathrm{ord}\, g = k$, $\mathrm{ord}\, h = l$, и $(k,l) = 1$, то $\mathrm{ord}(gh) = kl$.
**19.** Пусть $\varphi(m) = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ — каноническое разложение числа $\varphi(m)$ на простые сомножители, $(g,m) = 1$. В этом случае $g$ — первообразный корень в $\mathbb{Z}_m$ тогда и только тогда, когда $g$ не является решением ни одного из сравнений $g^{\frac{\varphi(m)}{p_k}} \equiv 1\ (\mathrm{mod}\ m)$ при $k = 1, \ldots, s$.
**20.** (умение) Решение степенных сравнений по простому модулю.
**21.** Теорема Дирихле о диофантовых приближениях (формулировка и доказательство с использованием принципа Дирихле).
**22.** Уточнение теоремы Дирихле в случае рациональных дробей.
**23.** Бесконечные цепные дроби. Утверждение о том, что значение бесконечной цепной дроби является иррациональным числом.
**24.** Бесконечные цепные дроби. Представление иррационального числа в виде бесконечной цепной дроби.
**25.** Бесконечные цепные дроби. Единственность представления иррационального числа в виде бесконечной цепной дроби.
**26.** Передоказательство теоремы Дирихле при помощи цепных дробей. Уточнение теоремы Дирихле (б/д). Зависимость качества аппроксимации от скорости роста неполных частных: существование чисел с заданным наперед качеством аппроксимации; золотое сечение как самое плохо приближаемое число (б/д).

**27.** Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Теорема Лиувилля (б/д). Конструкция трансцендентного числа с помощью цепной дроби и теоремы Лиувилля. Сводка результатов о трансцендентности: $e$, $\pi$, $e+\pi$, $\pi+e^\pi$, $\alpha^\beta$ (теорема Гельфонда), вывод про $e^\pi$ из теоремы Гельфонда.
**28.** Умение: решать уравнения Пелля.
**29.** Иррациональность числа $e$.
**30.** Определение решётки и дискретного подмножества. Любая дискретная подгруппа $\mathbb{R}^n$ является решёткой.
**31.** Двумерная теорема Минковского. Ее уточнение для замкнутых множеств (б/д).
**32.** Применение двумерной теоремы Минковского для передоказательства теоремы Дирихле. Теорема Дирихле о совместном диофантовом приближении (б/д)
**33.** Критический определитель решётки. Переформулировка теоремы Минковского через критический определитель. Теорема Минковского–Главки и история ее улучшений (б/д). Многомерный октаэдр, его объём.
**34.** Равномерно распределенные последовательности $\pmod 1$: три эквивалентные формулировки.
**35.** Является ли $\ln n$ р.р. $\pmod 1$ последовательностью?
**36.** Определение р.р. $\pmod 1$ последовательности. Вывод интегрального признака из того, что последовательность р.р. $\pmod 1$. Формулировка интегрального признака через комплекснозначную функцию (б/д).
**37.** Определение р.р. $\pmod 1$ последовательности. Вывод р.р. $\pmod 1$ последовательности из интегрального признака. Формулировка интегрального признака через комплекснозначную функцию (б/д).
**38.** Теорема Вейерштрасса про приближение непрерывной функции тригонометрическим многочленом(б/д). Равносильность критерия Вейля и интегрального признака.
**39.** Суммы Гаусса.
**40.** Асимптотическая оценка $[1, 2, \dots, n]$ снизу. Более грубая оценка, верная для $n \geqslant 7$. (б/д)
**41.** Алгоритм AKS. Определение и неравенства, связывающие числа $p, r, \log_2 n$ (б/д). Определение множеств $I, P$. Определение группы $G$, неравенство $|G| > \log_2^2 n$. Утверждения о делителе $h(X)$ многочлена $X^r - 1$ (б/д). Группа $\mathcal{G}$.
**42.** Алгоритм AKS. Верхняя оценка на $r$ (б/д). Обоснование неравенства $p > r > \log_2^2 n$ для подходящего делителя $p$ числа $n$. Вывод тождества $(X + a)^{n/p} = X^{n/p} + a \pmod{X^r - 1, p}$. Определение перестановочности многочлена и числа. Утверждения о свойствах перестановочности.

**Вопросы на отл.**

**1.** Сравнения второй степени. Квадратичные вычеты и невычеты. Тождество $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]}$ для нечётного $a$. (тождеством с суммой по $\left[\frac{2ax}{p}\right]$ можно пользоваться без доказательства).
**2.** Сравнения второй степени. Квадратичные вычеты и невычеты. Квадратичный закон взаимности (тождеством с суммой по $\left[\frac{ax}{p}\right]$ для нечётного $a$ можно пользоваться без доказательства).
**3.** Нижняя оценка разброса (уклонения) величиной $\sqrt{n}/2$ с помощью матриц Адамара.
**4.** Распределение простых чисел в натуральном ряде. Функции $\pi(x)$, $\theta(x)$, $\psi(x)$. Теорема Чебышёва (нижняя оценка — с док-вом, верхняя — формулировка).
**5.** Распределение простых чисел в натуральном ряде. Функции $\pi(x)$, $\theta(x)$, $\psi(x)$. Теорема Чебышёва (верхняя оценка — с док-вом, нижняя — формулировка).
**6.** Постулат Бертрана для $n >> 0$.
**7.** Показатели. Первообразные корни. Существование по модулю $p$.
**8.** Показатели. Первообразные корни. Существование по модулю $p^\alpha, \alpha \geqslant 2$: формулировка и доказательство леммы. Существование по модулю $2p^\alpha$.
**9.** Показатели. Первообразные корни. Существование по модулю $p^\alpha, \alpha \geqslant 2$: формулировка леммы (б/д) и вывод существования из неё. Существование по модулю $2p^\alpha$.
**10.** Показатели. Первообразные корни. Несуществование по модулю $2^n$, $n \geqslant 3$.
**11.** Показатели. Первообразные корни. Несуществование по модулям, отличным от $2^\alpha$, $p^\alpha$, $2p^\alpha$.
**12.** Теорема Лиувилля.

**13.** Доказательство трансцендентности $e$. Тождество Эрмита. Следствие из тождества Эрмита с использованием $a_k$ (коэффициентов многочлена $f(x)$ в предположении алгебраичности числа $e$). Определение многочлена $f(t)$. Неравенство

$$\left|\sum_{x=0}^{m} a_x e^x \int_0^x f(t)e^{-t}dt\right| < 1$$

при $n >> 0$.

**14.** Доказательство трансцендентности $e$. Тождество Эрмита (б/д). Определение многочлена $f(t)$, определение $F(x)$, свойства значений $F(k)$, $f(k)$, $f^{(l)}(k)$ при $k = 1, \ldots, m$, $l = 0, 1, \ldots, n-1$. Неравенство

$$|-\sum_{x=0}^{m} a_x F(x)| \geqslant 1$$

при $n >> 0$. Приведение к противоречию алгебраичности числа $e$.

**15.** Решетки в пространствах. Базис и определитель. Многомерная теорема Минковского (для произвольной решетки).

**16.** Доказательство теоремы Минковского-Главки для октаэдра: переформулировка условия теоремы через $\Lambda_{\overline{a}}$ и неравенства на $p$ и $n$. Сведение теоремы к неравенству

$$\frac{1}{p^n}\sum_{\overline{a}} |\Lambda_{\overline{a}} \cap \mathcal{O}^n \setminus \{0\}| < 1.$$

**17.** Теорема Минковского-Главки для октаэдра (формулировка). Доказательство неравенства

$$\frac{1}{p^n}\sum_{\overline{a}} |\Lambda_{\overline{a}} \cap \mathcal{O}^n \setminus \{0\}| < 1.$$

**18.** Доказательство теоремы Минковского-Главки для октаэдра. Определение октаэдра, решётки $\Lambda_{\overline{a}}$, числа $S_{\overline{a}}$. Лемма для $S_{\overline{a}}$ (формулировка). Вывод из леммы неравенства $\frac{1}{(p-1)^n}\sum_{\overline{a}} S_{\overline{a}} < 1$.

**19.** Алгоритм AKS. Верхняя оценка на $r$: вывод из утверждения о нижней оценке $[1, 2, \ldots, n]$.

**20.** Алгоритм AKS. Определение и неравенства, связывающие параметры $p, r, \log_2 n, t$, группы $G, \mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $|\mathcal{G}| \geqslant C_{t+l}^{t-1}$.

**21.** Алгоритм AKS. Определение и неравенства, связывающие $p, r, \log_2 n, t$, группы $G, \mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $|\mathcal{G}| \leqslant n^{\sqrt{t}}$ при $n \neq p^k$.

**22.** Алгоритм AKS. Определение и неравенства, связывающие $p, r, \log_2 n, t$, группы $G, \mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $C_{t+l}^{t-1} > n^{\sqrt{t}}$.