05) Оценка на собственные числа ограничения. Оценка на след.
1. С.ч. операторов A и B. По КФ, мин/макс для μ_i берется по подпр. внутри соотв. подпр. для λ. 2. Это след: взять матрицу A в ортонорм. базисе u_i. $v_i = (0, \dots, 1, \dots, 0)^T$ $A_{i,i} = v_i^T A v_i = q(u_i)$. Оценка: почленные нер-ва из 1.

07) Сингулярные значения и SVD-разложение.
$X^* = X^\top, \langle X^* e_i, e_j \rangle = \langle e_i, X e_j \rangle, \sigma_i = \sqrt{d_i} > 0$ с.ч. $A^* A$. SVD $A\colon U \to V$ $\exists$ о/н $u_i, v_j\colon$ матр $A = \Sigma(\sigma_{1..r}$ на диаг) $(X = L\Sigma R)$. e_i – о/н с.в. $\langle Ae_i, Ae_j \rangle = \langle A^* A e_i, e_j \rangle = \langle d_i e_i, e_j \rangle, f_i = \frac{Ae_i}{\sqrt{d_i}}$ доп до базиса. $R = C^{-1} = C^\top, C$ столбцы e_i.

08) Приближение матрицей указанного ранга и SVD-разложение. Возможность применения к сжатию изображения.
pr из Б6 $\Leftrightarrow$ ближ по $||X||_F = \sqrt{\operatorname{Tr} X^\top X}$. $X = L\Sigma R$. pr на $\langle v_1^\top .. v_k^\top \rangle$. v_i базис $X^\top X$ и строки R. pr a на $V^{(k)} = \sum a v_i v_i^\top$. $X^{(k)} = L\Sigma(\sum R v_i v_i^\top) = L\Sigma R^{(k)} = L\Sigma^{(k)} R$. Сж $L^{(k)}\Sigma^{(k)} R^{(k)}$. $2kn + k \to 2kn$ при $k < \frac{n}{2}$. Минор $k^2 + 2k(n-k) + 2k$.

09) Положительные матрицы. Теорема Перрона.
Док-во Перрона: положительность ($A|x| \geq |x| \Rightarrow A|x| < \frac{A^n}{(1+\varepsilon)^n} A|x| \to 0$ противореч.), единственность (сонапр. коорд. $v \Leftarrow \sum\limits_j A_{kj}|v_j| = |\sum\limits_j A_{kj} v_j|$) и некратность (Жорд. клетки; либо $\exists c, i : |x_1 - cx_2|_i = 0$, либо $Ax_2 = x_2 + x_1$)

10) Единственность положительного собственного вектора. Применение к случайному блужданию.
Знаем предел $\lim\limits_{k\to\infty} A^k v$, если у A макс по модулю с. ч. $\lambda = 1$ кратности 1. $A = P(G)$ нам не походит, замена $P(G)$: $P_\alpha(G) = (1-\alpha)P(G) + \alpha\frac{1}{n}J,\ \alpha \in (0,1),\ \forall i, j\ J_{ij} = 1$ – а это норм, Перрон гарантирует.

13) Две оценки на размер максимального независимого множества.
Натянуть подпространство на множество, следствие из Куранта-Фишера, нулевая квадратичная форма
Характеристический вектор множества, разложить по ортонорм. базису регулярного(!) графа с $u_1 = (1, \cdots, 1)\frac{1}{\sqrt{n}}$

17) Тензорное произведение линейных отображений. Кронекерово произведение. Тензорное произведение операторов и его собственные числа. Категорное произведение графов.
Единств: определено на тензорятах; $\exists$: отобразить $U_1 \times \cdots \times U_k$ в $V_1 \otimes \cdots \otimes V_K$ полилин. (композ полилин.) $\Rightarrow$ (опр. тенз.) $\exists!$. Наше правило подходит. Матрица: расписать $(\sum\limits_k A_{k,i} f_k) \otimes (\sum\limits_l B_{l,j} f'_l)$. С.ч. $A \otimes B$: жорданов базис.

27) Лемма Гаусса. Содержание многочлена. Делимость в $Q(R)[x]$ и в $R[x]$.
Лемма: Пусть нет, возьмём $\min a_i, b_j \not\vdots\, p$, тогда $c_{i+j} \not\vdots\, p$. Следствие: поделим на $\operatorname{cont} g, h$, убедимся что $\operatorname{cont} f = 1$. Лемма про $Q(R)[x]$: d_1, d_2 — НОК знаменателей, $c = \frac{d_1}{d_2}$.

28) Факториальность кольца многочленов над факториальным кольцом.
$R[x]$ факториально и простые в нём: $f = p \in R,\ f : \operatorname{cont}(f) = 1$ — непр. в $Q(R)[x]$. Док-во: 1) они и правда простые 2) в них раскладывается (посмотрим в $Q(R)$) 3) единственность $\Rightarrow$ других нет

29) Редукционный признак неприводимости. Примеры. Признак Эйзенштейна.
$a_n \not\vdots\, p$, f - неприводим в $R/p[x] \Rightarrow$ неприводим над $Q(R)$. $cont = 1$ и неприводимость над $Q(R) \Rightarrow$ неприводимость над R.
$a_n \not\vdots\, p$, все $a_i \vdots\, p$ $i < n$, но $a_0 \not\vdots\, p^2$, то многочлен $f(x)$ неприводим. Пусть $b_0 \not\vdots\, p$.

30) Алгоритм Кронекера. Сведение для многочленов от нескольких переменных.
1) Перебираем наборы делителей $f(i), 0 \leq i \leq \frac{degf}{2}$, интерполируем, проверяем. 2) Различным разложениям $f(x_1, \dots, x_n)$ соответствуют различные разложения $f(x, \dots, x^{d^{n-1}})$ для d больших $\max_{i=1}^n \{\deg_{x_i} f\}$. Рассмотреть образ x^α.

31) Лемма Гензеля. Разложение на множители при помощи леммы Гензеля.
Доказательство леммы: Индукция по k. Строим для k + 1. Помним, что $\forall f :\ p^k f \equiv p^k \overline{f} \pmod{p^{k+1}}$.
$\overline{h} \equiv \hat{h} + p^k a(x) \Rightarrow \overline{h}\overline{g} \equiv \hat{g}\hat{h} + p^k(a(x)g + b(x)h)$. С другой стороны $f - \hat{g}\hat{h} = p^k c(x) \Rightarrow a,\ b$ берем из лп НОДа g и h

32) Степенные суммы. Тождество Ньютона.
$0 = (-1)^n n\sigma_n + \sum_{k=0}^{n-1}(-1)^k \sigma_k s_{n-k}$, в многочлен подставим корни, просуммируем по всем корням, отдельно случаи $k < n$ - добавим нулевые переменные, $k > n$ - занулим не входящие в моном переменные

33) Целые алгебраические элементы. Замкнутость относительно операций.
а алгебраический $==$ $\exists f \in \mathbb{Z}[x] : f(a) = 0$. Замкнуто: $\prod(x - (a_i + b_j))$ симметрично по $_i$, тогда коэффициенты выражаются через симметрические, симметрический по b_i - все коэффициенты целые.

39) Конечные поля. Число элементов. Основное уравнение. Эндоморфизм Фробениуса. Корни $x^{p^n} - x$ образуют подполе.
Хорошо смотреть на мультипл. группу. Теорема Ферма для групп. Биномиальный коэф. делится на p почти всегда.

49) Циклические коды. Эквивалентное описание. Коды БЧХ. Пример.

$q = p^s$, m, n такие, что $q^m - 1 \vdots n$, $2 \leq d \leq n$, $l_0 \leq n$. α – образующая ${\mathbb{F}_{q^m}}^*$, $\beta = \alpha^{(q^m-1)/n}$

50) Основная теорема про коды БЧХ.
Делится $\Leftrightarrow$ обнуляется на корнях. Пусть плохо $\mathbb{F}_q$, тогда плохо в $\mathbb{F}_{q^m}$, определитель.