Катехизис к экзамену: всё, что вы хотели знать, но боялись спросить.

Вопрос: Как будет выглядеть экзамен?

Ответ: Вы получите два теретических вопроса и две задачи (упражнение и «на подумать»); всё это надо будет сдать устно принимающему. Менять билет нельзя. Досдавать вопрос / задачу в случае, если ваш ответ показался принимающему неполным, можно. Тройка ставится за теорию — но только в том случае, если она сдана без существенных недочётов. Четвёрка — за теорию и одну задачу, пятёрка — за теорию и две задачи.

Вопрос: Что надо говорить про индукцию?

Ответ: Надо объяснить, в чём заключается принцип и из каких частей состоит доказательство по индукции, и привести пример задачи, которая таким способом решается.

Вопрос: Что такое соотношение Безу и зачем оно нужно?

Ответ: Соотношение Безу говорит, что для целых a и b, не равных одновременно нулю, существуют целые же x, y, такие что $ax+by=(a,b)$.

Доказательство основано на идее рассмотрения наименьшего положительного числа, представимого в виде $ax+by$ (оно существует, потому что в этом виде представимы по крайней мере $|a|$ и $|b|$). Назовём это число q, $q=ax_0+by_0$. Ясно, что $q\leqslant min(|a|,|b|)$, иначе оно не было бы наименьшим. Разделим a с остатком на q: $a=lq+r$, $0\leqslant r<q$. Тогда $r=a-lq=a-l(ax_0+by_0)=a(1-lx_0)-ly_0b$, т. е. r тоже представим в виде $ax+by$ и, в силу минимальности q среди положительных чисел, представимых в таком виде, равно 0. То есть $a=lq$ и (по аналогичным соображениям) $b=mq$, значит, q — их общий делитель. Осталось заметить, что он наибольший, потому что левая часть равенства $ax+by=c$ всегда делится на (a,b).

Коэффициенты Безу (они, разумеется, не единственны) находятся с помощью обратного алгоритма Евклида. Соотношение Безу позволяет решать диофантовы уравнения и системы сравнений, а ещё на нём основано довольно симпатичное доказательство леммы Евклида: если $ab\,\vdots\,p$ и $(a,p)=1$, то существуют x и y такие, что $ax+py=1$. Умножив это равенство на b, получим $abx+bpy=b$. $ab\,\vdots\,p$, значит, на p делится левая часть, откуда $b\,\vdots\,p$.

Вопрос: Что такое обратимые остатки и делители нуля?

Ответ: Обратимый остаток — тот, который имеет обратный. a обратимо по модулю n, если $\exists b: ab\equiv 1 \pmod n$. a — делитель нуля по модулю n, если $\exists b\neq 0: ab\equiv 0 \pmod n$.

Вопрос: Как находить решения систем сравнений?

Ответ: Для маленьких случаев это делается перебором остатков. Если $x\equiv r_1 \pmod{a_1}$ и $x\equiv r_2 \pmod{a_2}$ (причём $(a_1,a_2)=1$), то работает следующая идея. Соотношение Безу говорит нам, что $\exists x,y: a_1x+a_2y=1$. Найдём какое-нибудь решение этого уравнения. Тогда нам подходит взятое по модулю a_1a_2 $r_2a_1x+r_1a_2y$. Действительно, $r_2a_1x+r_1a_2y=r_2(1-a_2y)+r_1a_2y=r_2-r_2a_2y+r_1a_2y\equiv r_2 \pmod{a_2}$. Аналогично получаем, что $r_2a_1x+r_1a_2y=r_1(1-a_1x)+r_2a_1x=r_1-r_1a_1x+r_2a_1x\equiv r_1 \pmod{a_1}$.

Вопрос: Что такое формула полной вероятности?

Ответ: Если есть *полная система событий* $B_1,\ldots B_n$ (никакие два не пересекаются, а их объединение имеет вероятность 1), то $P(A)=\sum\limits_{i=1}^{n} P(A|B_i)P(B_i)$. Это правда потому, что по формуле Байеса $P(A|B_i)=P(A\cap B_i)/P(B_i)$, т. е. наша сумма имеет вид $P(A)=\sum\limits_{i=1}^{n} P(A\cap B_i)$, что верно, т. к. любой элемент A принадлежит какому-нибудь из B_i и притом лишь одному.

Вопрос: Как доказывать теорему Холла?

Ответ: Теорема Холла (она же теорема о свадьбах) говорит, что свадьбу n юношей можно организовать в том и только в том случае, когда для любого k $(1\leqslant k\leqslant n)$ любые k юношей симпатизируют хотя бы k девушкам (симпатии взаимны). В одну сторону это утверждение очевидно, в другую доказывается индукцией по числу юношей. База 1 (если каждому юноше нравится какая-нибудь девушка, то одного совершенно точно можно женить). Пусть для любого числа юношей, меньшего n, теорема верна. Тогда может быть два случая. Если любые $k<n$ юношей симпатизируют хотя бы $k+1$ девушке, то, взяв любых n юношей, мы поженим одного и получим компанию из $n-1$, на которых приходится хотя бы $n-1$ девушка. Если же есть такая компания из $k<n$ юношей, которой симпатичны в точности k девушек, переженим их. Среди оставшихся $n-k$ любым $r<n-k$ нравятся ещё хотя бы r свободных девушек (потому что иначе для компании в $r+k$ юношей не выполнено исходное предположение), значит, по предположению индукции их судьбу тоже можно устроить.