Скорая помощь комбинаторике

1. Можно ли познакомить между собой n человек так, чтобы каждый был знаком ровно с четырьмя другими и среди любых трёх по крайней мере двое были незнакомы?

2. Должен состояться круговой турнир на $2n$ команд – каждая должна сыграть с каждой ровно одну партию. В день каждая команда может участвовать не более чем в одной встрече. За какое наименьшее количество дней можно провести турнир?

3. Штат охранного предприятия насчитывает $2n+1$ человека. Каждую ночь дежурит группа из троих охранников. Может ли через некоторое количество ночей оказаться, что любые двое ровно трижды дежурили вместе?

4. На Марсе несколько стран, в каждой живет несколько мужчин и столько же женщин. Они собираются переехать каждый в другую страну так, чтобы никакие два человека разного пола из одной страны не переехали в одну и ту же другую страну и чтобы в каждой стране после переезда жило столько же мужчин и столько же женщин, сколько и до. Докажите, что это возможно, если количество жителей каждой страны не превосходит четверти общего населения Марса.

5. В городе N разрешены только парные обмены квартир (А меняется с Б, Б меняется с А). За один день с любой квартирой можно производить не более одного обмена. Докажите, что любой сложный обмен квартирами можно осуществить за два дня.

6. $\#\mathcal{M} = 16$. Докажите, что существуют 16 подмножеств из 6 элементов каждое, такие что любые два подмножества имеют ровно два общих элемента.

7. Дано множество $\mathcal{M}$ из 133 элементов. Докажите, что для некоторого p можно выбрать подмножества $L_1, L_2, ..., L_{133} \subset \mathcal{M}$ так, что будут выполняться следующие условия:

   - любые L_i и L_j $(i \neq j)$ пересекаются ровно по одному элементу;
   - любые $m_i, m_j \in \mathcal{M}$ принадлежат ровно одному подмножеству;
   - любое L_k содержит ровно p элементов;
   - любой $m \in \mathcal{M}$ принадлежит ровно p подмножествам.

Функция Эйлера

! *Функция Эйлера* $\varphi(m)$ равна количеству натуральных чисел, не превосходящих m и взаимно простых с ним.

1. Найдите $\varphi\left(p^k\right)$, где $p \in \mathbb{P}$.
2. При каких m число $\varphi(m)$ чётно?
3. Докажите, что $\sum\limits_{m \vdots d} \varphi(d) = m$.
4. Докажите, что если $m_1 \perp m_2$, то $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.
5. Пусть $m = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot ... \cdot p_k^{\gamma_k}$ — разложение числа n на простые множители. Докажите, что
$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right) .$$

Приведённая система вычетов

! Набор остатков, взаимно простых с m, называется *приведённой системой вычетов* по модулю m.

1. Сколько элементов содержит приведённая система вычетов?

!! **Китайская теорема об остатках.**
Пусть $m_1 \perp m_2$ и $m = m_1 m_2$. Поставим каждому вычету a по модулю m в соответствие пару вычетов (a_1, a_2), где $a \equiv_{m_1} a_1$ и $a \equiv_{m_2} a_2$. Докажите, что это биекция.

2. Пусть $a \perp m$. Поставим каждому вычету b в соответствие вычет ab по модулю m. Докажите, что это биекция.

!! **Теорема Эйлера.**
Если $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $a \perp m$, то $a^{\varphi(m)} \equiv_m 1$.
(*Обобщение малой теоремы Ферма.*)

3. а) Найдите остаток от деления 7^{120} на 143.
   б) Найдите три последние цифры числа $17^{1000001}$.
4. Докажите, что для любого натурального n, взаимно простого с 10, найдётся натуральное k такое, что $nk = 11...1$.

Примитивные вычеты

! Пусть $a \perp m$. Говорят, что вычет a *имеет порядок* d по модулю m (при этом пишут $\mathrm{ord}_m a = d$), если d — наименьшее натуральное число такое, что $a^d \equiv_m 1$. Далее $\psi(d)$ обозначает количество вычетов порядка d.

1. Докажите, что если $a \perp m$ и a имеет порядок d по модулю m, то $\varphi(m) \vdots d$.
2. Пусть $m_1 \perp m_2$ и $a \perp m_1 m_2$. Пусть $\mathrm{ord}_{m_1} a = d_1$ и $\mathrm{ord}_{m_2} a = d_2$.
   Докажите, что $\mathrm{ord}_{m_1 m_2} a = [d_1, d_2]$.
3. Докажите, что $\sum\limits_{d \,|\, \varphi(m)} \psi(d) = \varphi(m)$.

! Вычет g называется *примитивным* по модулю m, если $\mathrm{ord}_m g = \varphi(m)$.
Таким образом, то, что g — примитивный вычет по модулю m, означает, что вычеты $g, g^2, ..., g^{\varphi(m)} \equiv_m 1$ образуют приведённую систему вычетов по модулю m.

4. Пусть $m = p \in \mathbb{P}$.
   а) Рассмотрим вычет a порядка d. Докажите, что...
      i. ... для всякого k справедливо $\mathrm{ord}_p(a^k) = \dfrac{d}{(d,k)}$;
      ii. ... все решения сравнения $x^d \equiv_m 1$ — это вычеты $1, a, a^2, ..., a^{d-1}$.
   б) Докажите, что либо $\psi(d) = 0$, либо $\psi(d) = \varphi(d)$.
   в) Докажите, что для любого d, делящего $p-1$, существует ровно $\varphi(d)$ вычетов порядка d. (В частности, существует ровно $\varphi(p-1)$ примитивных вычетов.)

!! Примитивные вычеты существуют по этим и только этим модулям: 2, 4, p^γ и $2p^\gamma$ (где p — нечетное простое, а γ — произвольное натуральное число).

5. Можно ли записать по кругу числа 1, 2, ..., 12 так, чтобы для любых трех подряд стоящих чисел a, b, c число $b^2 - ac$ делилось на 13?
6. Запишите в таблицу 4×4 числа 1,2, ..., 16 так, чтобы всевозможные произведения всех чисел, стоящих в одной строке, и всевозможные произведения чисел, стоящих в одном столбце, (т.е. всего 8 чисел) давали один и тот же остаток при делении на 17.