Ликбез по теории чисел: Ферма, Эйлер и многое другое.

Системы вычетов.

Определение. Полной системой вычетов (ПСВ) по модулю n называется множество чисел $\{a_1, a_2, ..., a_n\}$, в котором все числа дают разные остатки по модулю n.

Основное свойство ПСВ.
Если $(n; m) = 1$, то $\{b, m+b, 2m+b, 3m+b, ..., (n-1)m+b\}$ – ПСВ по модулю n.

Определение. Приведенной системой вычетов (ПрСВ) по модулю n называется множество чисел $\{a_1, a_2, ..., a_{\phi(n)}\}$, в котором все числа дают разные остатки по модулю n, взаимно простые с n.

Основное свойство ПрСВ.
Пусть $\{a_1, a_2, ..., a_{\phi(n)}\}$ – ПрСВ $mod\ n$, $(n; m) = 1$. Тогда $\{ma_1, ma_2, ..., ma_{\phi(n)}\}$ – тоже ПрСВ.

Функция Эйлера.

Определение. Будем обозначать $\phi(n)$ - количество чисел, меньших n, и взаимно простых с n. $\phi(n)$ называют функцией Эйлера числа n.

Определение. Функция $f(x) : \mathbb{N} \to \mathbb{N}$ называется мультипликативной, если для любых взаимно простых m, n выполняется $f(mn) = f(m) \cdot f(n)$.

Составим таблицу $n \times m$, в которой в клетке с координатой $(x; y)$ стоит число $x + ym$.
(а) Сколько в этой таблице чисел, взаимно простых с m?
(б) Сколько в каждом столбце таблицы чисел, взаимно простых с n?
(в) С помощью этой таблицы докажите мультипликативность функции Эйлера.

Выведем формулу функции Эйлера. Нетрудно убедиться, что $\phi(p^k) = p^k - p^{k-1}$. Отсюда и из мультипликативности следует, что если $n = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$, то

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot ... \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = n \left(1 - \frac{1}{p_1}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right).$$

Альтернатива. Можно вывести эту формулу из формулы включений-исключений.

Малая теорема Ферма и теорема Эйлера.

Малая теорема Ферма. Пусть p – простое число и a не делится на p. Тогда $a^{p-1} \equiv 1 \ mod \ p$.

Для доказательства этой теоремы следует рассмотреть числа $a, 2a, 3a, \ldots, (p-1)a$, понять, что они образуют ПрСВ, и после рассмотреть их произведение.

У малой теоремы Ферма существует комбинаторное доказательство. Чтобы его придумать, нужно решить задачу: сколько существует раскрасок правильного p-угольника в a цветов, если раскраски, получающиеся друг из друга поворотом, считаются одинаковыми.

Следствие из МТФ. Если p — простое число, то $a^p - a \vdots p$.

Определение. Порядком числа a по модулю p называется такое число k, что k – наименьшее натуральное число, для которого $a^k \equiv 1 \ mod \ p$. Обозначается $ord_p a = k$.

Верен следующий факт: для простого p и a, не кратного p, $p - 1 \vdots ord_p a$.

Теорема Эйлера. Если $(a, n) = 1$, то $a^{\phi(n)} \equiv 1 \ mod \ n$.

Проверьте, что МТФ – частный случай теоремы Эйлера. Доказательство теоремы Эйлера почти полностью совпадает с доказательством МТФ. Нужно рассмотреть числа $r_1 \cdot a, r_2 \cdot a, \ldots, r_{\phi(n)} \cdot a$, где $r_1, r_2, \ldots, r_{\phi(n)}$ —- взаимно простые с n остатки. Для этих чисел выполнить те же шаги, что и в МТФ.

Конструктивный факт. Если $(a; n) = 1$, то существует такое натуральное число k, что $a^k \equiv 1 \ mod \ n$. И мы даже умеем находить такое k.

Обратные и дробные остатки.

Определение. Остаток b называется обратным остатку a по модулю m, если $ab \equiv 1 \ mod \ m$. Можно обозначать $b \equiv a^{-1} \ mod \ m$.

В случае если $(a; m) = 1$, то у остатка a существует обратный по модулю m. Если $(a; m) \neq 1$, то обратного остатка a по модулю m нет.

Конструктивный факт. Обратный остаток (если он вообще существует) можно находить по формуле $b \equiv a^{\phi(m)-1} \ mod \ m$.

Определение. Будем говорить, что несократимая дробь $\frac{a}{b}$ имеет остаток x при делении на простое число p, если $a \equiv bx \ mod \ p$.

Свойства дробных остатков.
(а) $\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{ac}{bd} \ mod \ p$;
(б) $\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd} \ mod \ p$.

Теорема Вильсона. p — простое число тогда и только тогда, когда $(p-1)! \equiv -1 \ mod \ p$.

Решение линейных сравнений и систем сравнений.

Рассмотрим линейное сравнение $ax \equiv b \ mod \ m$.
(а) Докажите, что при $(a; m) = 1$ сравнение имеет единственное решение $mod \, m$;
(б) В каких случаях есть решения у сравнения, если $(a; m) \neq 1$? Сколько будет решений, если они есть?

Конструктивный факт. Решение линейного сравнения можно записать в виде $x \equiv b \cdot a^{\phi(m)-1}$.

Исходя из этого, придумайте, как находить частное решение диофантова уравнения.

Китайская теорема об остатках. Если числа $m_1, m_2, ..., m_k$ попарно взаимно просты, то для произвольных целых чисел $a_1, a_2, ..., a_k$ существует единственное по модулю $m_1 \cdot m_2 \cdot ... \cdot m_k$ решение системы

$$\begin{cases} x \equiv a_1 \ mod \ m_1, \\ x \equiv a_2 \ mod \ m_2, \\ ... \\ x \equiv a_k \ mod \ m_k. \end{cases}$$

Базовое доказательство КТО — применение индукции и свойства ПСВ.

У КТО существует комбинаторное доказательство: нужно установить биекцию между наборами $(a_1, a_2, ..., a_k)$, где $0 \leqslant a_i \leqslant m_i$ и остатками $m_1 \cdot m_2 \cdot ... \cdot m_k$.

Конструктивный факт. Докажите, что число $x = (m_2...m_k)^{\phi(m_1)}$ — решение системы

$$\begin{cases} x \equiv 1 \ mod \ m_1, \\ x \equiv 0 \ mod \ m_2, \\ ... \\ x \equiv 0 \ mod \ m_k. \end{cases}$$

Тогда число $x = \sum_{i=1}^{k} (m_1...m_{i-1}m_{i+1}...m_k)^{\phi(m_i)}$ — решение системы из КТО.

Немного о квадратичных вычетах.

Определение. Если $(a; m) = 1$ и сравнение $x^2 \equiv a \ mod \ m$ имеет решение, то число a называют квадратичным вычетом по модулю m. Если решений нет, то квадратичным невычетом.

По каждому простому модулю существует ровно $\frac{p-1}{2}$ вычетов и столько же невычетов. Для произвольного модуля используется крайне громоздкая формула Стангла.

Правила квадратичной арифметики: $вычет \cdot вычет = вычет$, $вычет \cdot невычет = невычет$, $невычет \cdot невычет = вычет$.

Критерий Эйлера. Если есть простое $p > 2$, $(a; p) = 1$, то число a является квадратичным вычетом по модулю p тогда и только тогда, когда $a^{(p-1)/2} \equiv 1 \ mod \ p$.