МГУ им. М.В. Ломоносова
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра теории чисел
Содержание курса “Теория чисел” (1 курс)

Лекции до 17 октября 2022 г.

Теоремы о делении с остатком: обычная, деление с отрицательным остатком, деление с наименьшим по модулю остатком. НОК и НОД теорему что НОК делит любое общее кратное и соответствующие теорема про НОД.

Алгоритм Евклида. Оценка количества шагов в обычном алгоритме Евклида и алгоритме, связанном с деление с минимальным по модулю остатком.

Представление рациональных чисел ценными дробями. Рекуррентные соотношения для подходящих дробей. Теорема о разности между соседними подходящими дробями.

Формула Перрона для приближения (рационального) числа его подходящей дробью.

Линейное представление НОД.

Сравнения и их простейшие свойства. Необходимое и достаточное условие существования обратного элемента.

Функция Эйлера: определение. Теорема Эйлера.

Показатель числа по модулю m. Теорема от том, что показатель делит любое , таке что $a^x \equiv 1 \pmod m$.

Классы вычетов, полная и приведённая системы вычетов.

Теорема о том, как построить полную/приведенную систему вычетов по модулю mn для взаимно простых m и n, если дай полные/приведенные системы вычетов по модулям m и n. Следствие: мультипликативность функции Эйлера.

Лекция 17 октября 2022 г.

Определение простого числа. Теорема о том, что наименьший делитель натурального числа $n > 1$, отличный от единицы, есть число простое. Теорема Евклида о бесконечности множества простых чисел. Теорема о том, что если простое p делит произведение ab двух целых чисел, то p делит хотя бы одно из чисел a и b (два доказательства: через линейное представление Н.О.Д. и индукцией по простым числам). Основная теорема арифметики. Теорема о том, что наименьший простой делитель составного числа n не превосходит $\sqrt{n}$. Решето Эратосфена.

Доказательство неравенства

$$\sum_{p \leqslant x} \frac{1}{p} \geqslant \ln\ln x - 1, \qquad x \geqslant 3$$

(p пробегает подряд идущие простые числа). Замечание об оценке снизу суммы

$$\sum_{n \leqslant x} \frac{1}{n}$$

с помощью неравенства $\ln\bigl(1 + 1/n\bigr) \leqslant 1/n$.

Лекция 25 октября 2022 г.

Определение функции $\pi(x)$. Определение функции Мёбиуса $\mu(n)$. Теорема об основном свойстве функции Мёбиуса. Доказательство неравенства

$$\pi(x) \leqslant \frac{2x}{\ln\ln x},$$

справедливого при всех $x \geqslant x_0$.

Теорема о решении системы линейных сравнений вида $x \equiv a_j \pmod{m_j}$, $j = 1, \ldots, s$, где модули m_j попарно взаимно просты (китайская теорема об остатках). Пример на применение этой теоремы. Следствие китайской теоремы об остатках: если $f(x)$ - полином с целыми коэффициентами, и $J(f; m)$ - число решений полиномиального сравнения $f(x) \equiv 0 \pmod{m}$, то функция $J(f; m)$ (при фиксированном f) - мультипликативная функция аргумента m.

Лекция 1 ноября 2022 г.

Пример решения полиномиального сравнения по составному модулю (пояснение к китайской теореме об остатках). Отыскание решений сравнения $ax \equiv b \pmod{m}$ (при условии взаимной простоты m и a) через неполные частные разложения m/a в цепную дробь. Отыскание решения того же сравнения через малую теоремы Ферма.

Теорема о том, что полиномиальное сравнение степени n по простому модулю p равносильно некоторому сравнению степени не выше $p - 1$. Теорема Лагранжа о числе решений полиномиального сравнения по простому модулю (два доказательства: первое - через формулы Крамера, второе - через представление полинома $f(x)$ в виде суммы слагаемых вида $(x-x_1)\ldots(x-x_j)$, $j = 1, 2, \ldots, n$, где x_j - решения исходного сравнения). Теорема Вильсона (критерий простоты числа).

Лекция 7 ноября 2022 г.

Процедура «подъёма» решения $x \equiv x_1 \pmod{p}$ полиномиального сравнения $f(x) \equiv 0 \pmod{p}$ до решения сравнения $f(x) \equiv 0 \pmod{p^\alpha}$, $\alpha \geqslant 2$ (рассматривается лишь случай нечётного простого p и $f'(x_1) \not\equiv 0 \pmod{p}$). Примеры, относящиеся к случаям, когда условие $f'(x_1) \not\equiv 0 \pmod{p}$ нарушается.

Определение вычетов и невычетов n-й степени по модулю m ($m, n \geqslant 2$). Теорема о том, что в случае простого $m = p \geqslant 3$ сравнение $x^2 \equiv a \pmod{p}$ (a - квадратичный вычет) имеет два решения. Теорема о том, что приведённая системы вычетов про нечётному простому модулю p из $\dfrac{p-1}{2}$ квадратичных невычетов и $\dfrac{p-1}{2}$ квадратичных вычетов, сравнимых с числами $1^2, 2^2, \ldots, \left(\dfrac{p-1}{2}\right)^2$. Критерий Эйлера.

Лекция 15 ноября 2022 г.

Определение символа Лежандра $\left(\dfrac{a}{p}\right)$. Переформулировка критерия Эйлера в терминах символа Лежандра. Теорема о простейших свойствах символа Лежандра (периодичность, значение при $a = -1$, мультипликативность, равенство нулю суммы значений символа Лежандра по полной системе вычетов по простому модулю и пр.). Разрешимость сравнения $x^2 + 1 \equiv 0 \pmod{p}$.

Вспомогательные утверждения для доказательства закона взаимности квадратичных вычетов: лемма о выражении символа Лежандра через произведение величин ε_x, $x = 1, 2, \ldots, p_1 = \dfrac{p-1}{2}$, где $a \cdot x \equiv \varepsilon_x \cdot r_x \pmod{p}$, $1 \leqslant r_x \leqslant p_1$, $\varepsilon_x = \pm 1$; две формулы:

$$\left(\frac{a}{p}\right) = (-1)^{\delta}, \quad \delta = \sum_{x=1}^{p_1} \left[\frac{2ax}{p}\right]; \qquad \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\delta_1}, \quad \delta_1 = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}.$$

Значение символа Лежандра при $a = 2$. Простые числа, для которых 2 является квадратичным вычетом (невычетом). Закон взаимности квадратичных вычетов (через подсчёт целых точек в прямоугольнике $0 < x < p/2$, $0 < y < q/2$).

Лекция 22 ноября 2022 г.

Теорема о том, что множества простых чисел вида $4n+1$ и $4n+3$ бесконечны. Теорема о том, что всякое простое число p вида $4n + 1$ представимо суммою двух квадратов натуральных чисел.

Две вспомогательные леммы (для доказательства теоремы Лагранжа о четырёх квадратах): тождество: произведение двух сумм 4-х квадратов есть сумма 4-х квадратов; если p - нечётное простое число, то существуют целые числа x, y и m такие, что $x^2 + y^2 + 1 = pm$, причём $1 \leqslant m < p$. Теорема Лагранжа о четырёх квадратах.

Лекция 29 ноября 2022 г.

Завершение доказательства теоремы Лагранжа. Понятие о проблема Варинга, её современная формулировка. Теорема о том, что всякое натуральное число есть сумма не более чем 53 биквадратов натуральных чисел. Определение показателя числа a по заданному модулю m ($m \geqslant 2$, $(a, m) = 1$). Численные примеры: нахождение всех показателей по модулям $2, 3, 4$ и 5. Лемма о том, что если a принадлежит по модулю m показателю δ, то числа a^k, $k = 0, 1, \ldots, \delta - 1$ различны по модулю m. Лемма о том, что сравнение $a^{\gamma} \equiv a^{\gamma'} \pmod{m}$ равносильно сравнению $\gamma \equiv \gamma' \pmod{\delta}$. Вывод следствия: все показатели, которым принадлежат числа приведённой системы вычетов по модулю m, являются делителями $\varphi(m)$. Доказательство тождества

$$\sum_{d|m} \varphi(d) = m.$$

Лекция 06 декабря 2022 г.

Теорема о том, что при нечётном простом p для всякого δ, делящего $p - 1$, в приведённой системе вычетов по модулю p имеется ровно $\varphi(\delta)$ чисел, принадлежащих по модулю p показателю δ. Следствие: существование первообразных корней по простому модулю. Пример с $p = 7$. Теорема о том, что если g - первообразный корень по нечётному простому модулю p, то можно подобрать целое число t так, что $g_1 = q + pt$ будет первообразным корнем по всякому модулю p^{α}, $\alpha \geqslant 2$. Теорема о том, что если g_1 - первообразный корень по модулю p^{α} ($p \geqslant 3$ - простое), то нечётное из чисел g_1, $g_1 + p^{\alpha}$ будет первообразным корнем по модулю $2p^{\alpha}$.

Лекция 13 декабря 2022 г. (план)

Критерий первообразного корня. Понятие индекса и его простейшие свойства. Индексы по модулю 2^{α}. Теорема о том, что первообразные корни по модулю m существуют лишь в случаях, когда $m = 2, 4$, p^{α}, $2p^{\alpha}$, где p - нечётное простое, $\alpha \geqslant 1$.