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

Лекция № 1 (07 сентября 2023 г.)

Интуитивно ясные понятия: натуральные числа, целые числа, сумма и разность целых чисел. Аксиома индукции и три её следствия (формулировки). Делимость целых чисел: определение, простейшие свойства делимости, теорема о делении с остатком. Общее кратное набора натуральных чисел. Наименьшее общее кратное (Н.О.К.): определение Н.О.К. набора натуральных чисел, теорема о том, что каждое общее кратное набора натуральных чисел делится на их Н.О.К. Общий делитель набора натуральных чисел. Наибольший общий делитель (Н.О.Д.) набора натуральных чисел. Взаимно простые числа. Равенство Н.О.К.(a, b) · Н.О.Д.$(a, b) = ab$. Теорема о том, что если a, b, c - натуральные числа, a делит произведение bc, причём a и b взаимно просты, то тогда a делит c.

Лекция № 2 (14 сентября 2023 г.)

Лемма о том, что если b делит a, то Н.О.Д.$(a, b) = b$. Лемма о том, что если $a = bq+r$, где $0 < r < q$, то Н.О.Д.(a, b) = Н.О.Д.(b, r). Алгоритм Евклида. Теорема о том, что Н.О.Д.(a, b) равен последнему ненулевому остатку в алгоритме Евклида. Линейные диофантовы уравнения. Критерий разрешимости уравнения $ax+by = c$ в переменных x, y. Формулы, выражающие общее решение такого уравнения через его частное решение.

Лекция № 3 (21 сентября 2023 г.)

Простые и составные числа: определение, примеры. Лемма о том, что всякое целое число, большее единицы, имеет простой делитель. Теорема Евклида о бесконечности множества простых чисел. Решето Эратосфена. Основная теорема арифметики. Простейшие свойства величины $\nu_p(n)$ - показателя, с которым простое p входит в каноническое разложение числа n.

Лекция № 4 (25 сентября 2023 г.)

Формула для величины $\nu_p(n!)$ - показателя, с которым простое p входит в каноническое разложение факториала числа n:

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

Лемма о том, что последовательность $a_n = (1+1/n)^n$ монотонно возрастает и ограничена сверху. Определение числа «e», определение натурального логарифма положительного числа. Неравенство $\ln(1 + 1/n) < 1/n$. Доказательство неравенства

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \geqslant \ln n + \frac{1}{n}, \quad n \geqslant 1.$$

Доказательство неравенства

$$\prod_{p\leqslant n}\left(1-\frac{1}{p}\right)<\frac{1}{\ln n},\quad n\geqslant 2$$

(слева - произведение по всем простым числам, не превосходящим n). Доказательство неравенства

$$\sum_{p\leqslant n}\frac{1}{p}\geqslant \ln\ln n-1.$$

Лекция № 5 (05 октября 2023 г.)

Функция Мёбиуса $\mu(n)$: определение, мультикликативность и её основное свойство. Функция $\pi(x)$ (количество простых чисел, не превосходящих x). Доказательство неравенства

$$\pi(x)\leqslant\frac{2x}{\ln\ln x},\quad x\geqslant x_0.$$

Определение мультипликативной функции. Простейшие свойства мультипликативных функций: (a) если $f\not\equiv 0$, то $f(1)=1$; (b) если $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$, то $f(n)=f\big(p_1^{\alpha_1}\big)\ldots f\big(p_k^{\alpha_k}\big)$; (c) если f,g мультипликативны, то $h(n)=f(n)\cdot g(n)$ также мультипликативна.

Лекция № 6 (12 октября 2023 г.)

Теорема о том, что функция F, определенная при любом $n\geqslant 1$ равенством $F(n)=\sum\limits_{d|n}f(d)$, где f - заданная мультипликативная функция, также является мультипликативной. Следствия этой теоремы: (a) если $f\not\equiv 0$ и $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$, то

$$F(n)=\prod_{i=1}^{k}\big(1+f(p_i)+f(p_i^2)+\ldots+f(p_i^{\alpha_i})\big);$$

(b) ещё один вывод основного свойства функции Мёбиуса; (c) мультипликативность функций: числа делителей $\tau(n)$ и суммы делителей $\sigma(n)$, формулы для их вычисления. Определение функции Эйлера $\varphi(n)$, её мультипликативность; формула для вычисления $\varphi(n)$. Формула (первая) обращения Мёбиуса:

$$g(n)=\sum_{d|n}f(d),\quad n=1,2,3,\ldots\quad\Leftrightarrow\quad f(n)=\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right).$$

Лекция № 7 (19 октября 2023 г.)

Примеры на применение (первой) формулы обращения Мёбиуса: доказательства тождеств

$$\sum_{d|n}\varphi(d)=n,\quad \sum_{d|n}\mu(d)\tau\left(\frac{n}{d}\right)=1.$$

Формулировки теорем о поведении при $x \to +\infty$ сумм значений функций Эйлера и делителей

$$\sum_{n\leqslant x}\tau(n) = x(\ln x + 2\gamma - 1) + r_1(x), \quad |r_1(x)| \leqslant c_1\sqrt{x},$$

$$\sum_{n\leqslant x}\varphi(n) = \frac{3}{\pi^2}\,x^2 + r_2(x), \quad |r_2(x)| \leqslant c_2 x\ln x,$$

где γ - константа Эйлера, $c_1, c_2 > 0$ - некоторые постоянные. Разложение вещественного числа α в непрерывную дробь. Неполные частные, подходящие дроби. Связь разложения несократимой рациональной дроби $\alpha = a/b$ в непрерывную дробь и алгоритма Евклида. Теорема о свойствах числителей и знаменателей P_s, Q_s подходящих дробей $\delta_s = P_s/Q_s$ (формулировка, начало доказательства).

Лекция № 8 (26 октября 2023 г.)

Теорема о свойствах числителей и знаменателей P_s, Q_s подходящих дробей $\delta_s = P_s/Q_s$ (завершение доказательства). Разбор численного примера на нахождение значений P_s, Q_s по рекуррентным формулам. Следствия: равенства

$$aQ_{s-1} - bP_{s-1} = (-1)^s, \qquad \delta_s - \delta_{s-1} = \frac{(-1)^s}{Q_sQ_{s-1}}.$$

Знак разности $\delta_s - \alpha$, неравенство

$$|\alpha - \delta_{s-1}| \leqslant \frac{1}{Q_sQ_{s-1}}.$$

Разложение в цепную дробь числа $\sqrt{2}$, связь подходящей дроби δ_6 с форматом бумаги A_4. Выражение общего решения уравнения $ax - by = 1$ (Н.О.Д. $(a, b) = 1$) через частное решение (x_0, y_0). Нахождение частного решения.

Лекция № 9 (02 ноября 2023 г.)

Теорема о разрешимости в целых числах уравнения $ax - by = c$. Формулы, дающие решения этого уравнения в случае его разрешимости. Понятие сравнимости двух целых чисел по модулю m, $m \geqslant 2$. Простейшие свойства сравнений (в частности, если $ac \equiv bc \pmod{m}$, и Н.О.Д.$(c, m) = 1$), то $a \equiv b \pmod{m}$; если $a \equiv b \pmod{m}$, то Н.О.Д.$(a, m) =$ Н.О.Д.(b, m) и пр. Определение классов вычетов по модулю m. Полная система вычетов по модулю m. Наименьшая неотрицательная и наименьшая по модулю системы вычетов по модулю m.

Лекция № 10 (09 ноября 2023 г.)

Теорема о том, что если Н.О.Д.$(a, m) = 1$, b - произвольное целое, а x пробегает полную систему вычетов по модулю m, то $ax + b$ также пробегает полную систему вычетов по модулю m. Обратный вычет. Приведённая система вычетов по модулю m, число элементов в ней. Теорема о том, что если Н.О.Д.$(a, m) = 1$, а x пробегает приведённую систему вычетов по модулю m, то ax также пробегает приведённую систему вычетов по модулю m. Теорема Эйлера: если Н.О.Д.$(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod m$. Малая теорема Ферма: если p - простое число, то $a^p \equiv a \pmod p$ для любого a. Полиномиальное сравнение; его степень. Решение линейного сравнения $ax \equiv b \pmod m$ в случае Н.О.Д.$(a, m) = 1$: с помощью теоремы Эйлера и с помощью разложения числа m/a в цепную дробь.

Лекция № 11 (16 ноября 2023 г.)

Теорема о разрешимости сравнения $ax \equiv b \pmod m$ в случае Н.О.Д.$(a, m) = d > 1$. Китайская теорема об остатках: если модули m_s, $s = 1, \ldots, k$ попарно взаимно просты, $M = m_1 \ldots m_k = m_s M_s$, $M_s N_s \equiv 1 \pmod{m_s}$, то при любых целых a_s решение системы сравнений $x \equiv a_s \pmod{m_s}$, $s = 1, \ldots, k$, имеет вид $x \equiv x_0 \pmod M$, где

$$x_0 = a_1 M_1 N_1 + \ldots + a_k M_k N_k.$$

Сведение решения полиномиального сравнения $f(x) \equiv 0 \pmod m$ по составному модулю $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ к решению системы сравнений вида $f(x) \equiv 0 \pmod{p_s^{\alpha_s}}$, $s = 1, \ldots, k$. Теорема о том, что всякое полиномиальное сравнение по простому модулю $m = p$ равносильно некоторому полиномиальному сравнению степени не выше $p - 1$. Теорема Лагранжа: если сравнение степени n $(n < p)$ имеет по простому модулю p более чем n решений, то все коэффициенты полинома $f(x)$ кратны p. Следствие (теорема Вильсона): $(p-1)! + 1 \equiv 0 \pmod p$ для любого простого p. Критерий простоты числа, основанный на теореме Вильсона. Производная многочлена (формальное определение). Формула Тейлора для многочлена (без доказательства). Процедура поднятия решения $x \equiv x_1 \pmod p$ полиномиального сравнения $f(x) \equiv 0 \pmod p$ в случае $f'(x_1) \not\equiv 0 \pmod p$ до решения $x \equiv x_2 \pmod{p^2}$ аналогичного сравнения по модулю p^2.

Лекция № 12 (23 ноября 2023 г.)

Определение вычета n-й степени по модулю m. Квадратичные вычеты и невычеты по нечётному простому модулю p. Теорема о том, что если a - квадратичный вычет, то сравнение $x^2 \equiv a \pmod p$ имеет два решения. Теорема о том, что приведённая система вычетов по модулю p содержит $(p-1)/2$ квадратичных вычетов (сравнимых с числами $1^2, 2^2, \ldots, ((p-1)/2)^2$ по модулю p), и $(p-1)/2$ квадратичных невычетов. Критерий Эйлера. Определение символа Лежандра (a/p). Теорема о том, что $a^{(p-1)/2} \equiv (a/p) \pmod p$. Простейшие свойства символа Лежандра. Теорема о том, что (-1) является квадратичным вычетом по простому нечётному модулю p Тогда, и только тогда, когда $p \equiv 1 \pmod 4$. Квадратичный закон взаимности (формулировка).

Лекция № 13 (30 ноября 2023 г.)

Доказательство формулы ($p \geqslant 3$ - простое, $(a, p) = 1$):

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

Доказательство формулы ($p \geqslant 3$ - простое, $(a, p) = 1$, a - нечетное):

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

Следствие: значение символа Лежандра $(2/p)$; простые p, для которых число 2 будет квадратичным вычетом (невычетом). Доказательство закона взаимности квадратичных вычетов. Теорема о том, что множества простых чисел вида $4n+1$ и $4n+3$ бесконечны. Теорема о том, что всякое простое p вида $4n+1$ представимо суммою квадратов двух натуральных чисел: $p = a^2 + b^2$.

Лекция № 14 (7 декабря 2023 г.)

Определение показателя, которому принадлежит по модулю m число a с условием: Н.О.Д.$(a, m) = 1$. Лемма: если a принадлежит по модулю m показателю δ, то числа $a^0 = 1, a, a^2, \ldots a^{\delta-1}$ различны по модулю m. Лемма: если Н.О.Д.$(a, m) = 1$, то сравнение $a^\gamma \equiv a^{\gamma'} \pmod{m}$ имеет место тогда, и только тогда, когда $\gamma \equiv \gamma' \pmod{\delta}$, где δ - показатель, которому принадлежит a. Следствие: все показатели, которым принадлежат числа по модулю m, являются делителями $\varphi(m)$. Определение первообразного корня. Теорема о том, что при простом $p \geqslant 3$ и произвольном $\delta|(p-1)$ в приведённой системе вычетов по модулю p существует ровно $\varphi(\delta)$ вычетов, принадлежащих показателю δ. Следствие: существование первообразных корней по простому модулю. Теорема о существовании первообразных корней по модулю вида p^α, где $p \geqslant 3$ - простое, $\alpha \geqslant 2$ - произвольное целое число.

Лекция № 15 (14 декабря 2023 г.)

Теорема о существовании первообразного корня по модулю $2p^\alpha$, где $p \geqslant 3$ - простое, $\alpha \geqslant 1$ - произвольное целое. Критерий первообразного корня. Теорема об отсутствии первообразных корней по модулю вида 2^α, $\alpha \geqslant 3$. Теорема о том, что первообразные корни существуют только по модулям вида $2, 4, p^\alpha, 2p^\alpha$, где $p \geqslant 3$ - простое, $\alpha \geqslant 1$ - произвольное целое.