Теория делимости

М. И. Магин, Б.А. Золотов

1. Делимость целых чисел. Определение, базовые свойства делимости. Свойства четных и нечетных чисел.
2. Простые числа. Теорема Евклида. Теорема о k последовательных составных в натуральном ряде.
3. Деление с остатком. Существование и единственность остатка.
4. Сравнения по модулю. Определение, основные свойства: арифметика остатков, сокращение на взаимнопростой множитель, сравнимость по модулю — отношение эквивалентности.
5. Десятичная запись числа и признаки делимости. Признак делимости на 3 (9), признак делимости на 11.
6. Признак делимости на $2^n(5^n)$.
7. Аксиомы кольца. Примеры и антипримеры колец. Кольцо классов вычетов $\mathbb{Z}/p\mathbb{Z}$ (определение).
8. Наименьшее общее кратное. Свойства НОК: любое общее кратное набора чисел делится на НОК, $\operatorname{lcm}(a_1, \ldots, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{n-1}), a_n)$.
9. Наибольший общий делитель. Свойства НОД: НОД набора чисел делится на любой общий делитель, $\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$.
10. Свойства НОД: $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$, $\gcd(a, b) = \gcd(a, a + b) = \gcd(a, a - b)$.
11. Алгоритм Евклида.
12. Обобщенный алгоритм Евклида. Линейное представление НОД.
13. Линейные диофантовы уравнения: критерий разрешимости, общий вид решений.
14. Методы решений диофантовых уравнений: перебор с отсечениями, метод спуска, разложение на множители.
15. Лемма Евклида. Основная теорема арифметики.
16. НОД и НОК в терминах основной теоремы арифметики. Формула для функции τ количества делителей.
17. Формула для функции суммы делителей σ, степень вхождения простого в факториал.
18. Число сочетаний $\binom{n}{k}$. Бином Ньютона, доказательство по индукции.
19. Лемма о $(a + b)^p \equiv a^p + b^p \pmod{p}$. Малая теорема Ферма, доказательство через лемму.
20. Китайская теорема об остатках.
21. Пример применения КТО.
22. Коэффициенты разложения по исходным числам в алгоритме Евклида: метод “сверху вниз”.
23. Определение функции Эйлера. Четность. Значения для простого числа и степени простого числа.
24. Мультипликативность функции Эйлера. Явная формула для функции Эйлера.
25. В случае конечного G сократимость равносильна существованию обратного в определении группы.
26. Группа $V(n)$ остатков, взаимно простых с n. Теорема Эйлера.
27. Длина цикла остатков при возведении в степень, когда основание не взаимно просто с модулем.
28. $\sum_{d|n} \varphi(d) = n$.