Теоретические задачи по курсу «Алгоритмы алгебры и теории чисел»

Длинная арифметика

1. Придумать алгоритм сложения длинных чисел слева направо. Есть два числа из n десятичных цифр каждое. Числа подаются на вход слева направо (сначала подаются на вход наиболее значящие цифры). Требуется вывести их сумму. Время работы: $O(n)$. Памяти: $O(1)$.
2. Факториальная система счисления. Доказательство существования и единственности записи любого натурального числа в следующем виде: $n = \sum_{k=0}^{m} b_k \cdot k!$, где $0 \le b_k \le k$.
3. Доказать формулу Бине для чисел Фибоначчи:

$$f_n = \frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}$$

4. Доказать, что если $n, m \le f_k$, то число шагов в алгоритме Евклида для чисел n и m равно $k + O(1)$.
5. Доказать, что если числа n и m записаны в b-ичной системе счисления из L цифр, то время работы алгоритма Евклида равно $O(L^2)$.
6. Придумать алгоритм извлечения квадратного корня из длинного числа.
   a) Время работы: $O(n^3)$
   b) Время работы: $O(n^2)$

Теоремы о простых числах

1. Доказать бесконечность простых чисел вида $4k + 3$.
2. Доказать, что в ряде простых чисел существуют сколь угодно большие пробелы: для любого K существует M такое, что числа $M, M + 1, \ldots, M + K - 1$ не являются простыми.
3. Доказать, что среди чисел, представляемых данным многочленом $p(n)$ с целыми коэффициентами, существует бесконечно много составных.
4. Пусть $p = 4k + 3$ — простое число. Доказать, что если $a^2 + b^2$ делится на p, то и a и b оба делятся на p.
5. Доказать бесконечность простых чисел вида $4k + 1$.

Пифагоровы тройки

1. Каждой примитивной пифагоровой тройке соответсвует рациональная точка на единичной окружности. Каждой рациональной точке на единичной окружности соответствует рациональная прямая, проходящая через $(1, 0)$. Вывести из этого формулу для примитивных пифагоровых троек: $a^2 + b^2 = c^2$ тогда и только тогда, когда $a = n^2 - m^2, b = 2nm, c = n^2 + m^2$ (при четном b).

Ряд Фарея

1. Пусть $\frac{a}{b}$ и $\frac{c}{d}$ — две соседние дроби в ряду Фарея N-ого порядка. И пусть $\frac{x}{y}$ — несократимая дробь, не лежащая в ряду Фарея N-ого порядка и такая что $\frac{a}{b} < \frac{x}{y} < \frac{c}{d}$. Доказать, что существуют натуральные числа α и β такие, что $x = a\alpha + c\beta$ и $y = b\alpha + d\beta$.
2. Пусть $\frac{a}{b}$ и $\frac{c}{d}$ — две соседние дроби в ряду Фарея N-ого порядка. Доказать, что $bc - ad = 1$.

Сумма ряда из обратных квадратов

1. Доказать, что $\operatorname{ctg}^2 \alpha < \frac{1}{\alpha^2} < \frac{1}{\sin^2 \alpha}$ при $0 < \alpha < \frac{\pi}{2}$.
2. Используя формулу Муавра Доказать, что числа $\operatorname{ctg}^2(\frac{k\pi}{2n+1})$ при $1 \le k \le n$ являются корнями многочлена $\binom{2n+1}{1}x^n - \binom{2n+1}{3}x^{n-1} + \binom{2n+1}{5}x^{n-2} - \ldots + (-1)^n$.
3. Доказать, что $\operatorname{ctg}^2(\frac{\pi}{2n+1}) + \operatorname{ctg}^2(\frac{2\pi}{2n+1}) + \ldots + \operatorname{ctg}^2(\frac{n\pi}{2n+1}) = \frac{n(2n-1)}{3}$.
4. Доказать, что $\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$.

Вероятность того, что два случайных натуральных числа взаимнопросты

1. Пусть q_n — количество упорядоченных пар чисел (u, v), принадлежащих интервалу $[1..n]$, таких что $gcd(u, v) = 1$.
   a) Доказать, что $q_n = \sum_{k=1}^{n} \mu(k)[\frac{n}{k}]^2$
   b) Доказать, что $\lim_{n\to+\infty} \frac{q_n}{n^2} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2}$
   c) Доказать, что $\lim_{n\to+\infty} \frac{q_n}{n^2} = \frac{6}{\pi^2}$

Разные задачи

1. Рассмотрим число $S_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$. Представим это число в виде несократимой дроби $S_n = \frac{a_n}{b_n}$. Доказать, что b_n четно при $n > 1$. Таким образом, S_n не целое при $n > 1$.
2. Как решать систему из КТО если модули не обязательно попарно взаимно просты?
3. Доказать, что если $2^n - 1$ простое, то n тоже простое (простые числе Мерсенна).
4. Доказать, что если $2^n + 1$ простое, то $n = 2^k$ (простые числа Ферма).
5. Доказать, что для любого натурального n существует натуральное m такое, что f_m делится на n.
6. Найти в какой степени простое число p входит в $n!$.
7. Дано N чисел $a_1, \ldots, a_n$ по модулю M. Требуется за одно использование gcd найти обратные ко всем числам по модулю M или сказать что не для всех чисел обратные есть.
8. Доказать, что число $\sqrt{2}$ — иррациональное.
9. (*) Доказать, что число $\sqrt{2} + \sqrt{3} + \sqrt{5}$ — иррациональное.
10. Доказать, что если сравнение $x^n \equiv a \pmod p$ имеет решение при простом p, то сравнение $x^n \equiv a \pmod p^r$ тоже имеет решение.
11. Доказать, что если $2^p - 1$ — простое число, то $n = 2^{p-1}(2^p - 1)$ — совершенное.
12. Доказать, что если $n\phi(n) = m\phi(m)$, то $n = m$.
13. Найти все простые числа p и q такие, что $2^p + 1$ делится на q и $2^q + 1$ делится на p.
14. Найти все натуральные числа n такие, что $n^2 + 1$ делится на $n - 1$.
15. Доказать, что $(n + 1)^n - 1$ делится на n^2.
16. Доказать, что существует бесконечно много натуральных n таких что $2^n + 1$ делится на n.
17. Доказать, что если a и b различные натуральные числа, то существует бесконечно много натуральных n таких что $gcd(a + n, b + n) = 1$.

Численные задачи

1. Доказать, что $2^{70} + 3^{70}$ делится на 13.
2. Решить уравнение $\phi(n) = 239$.
3. Решить уравнение $\phi(n) = 566$.
4. Решить уравнение $364x + 277y = 1$ в целых числах.
5. Решить систему уравнений: $x \equiv 3 \pmod 8$, $x \equiv 11 \pmod{20}$, $x \equiv 1 \pmod{15}$.