Теория чисел

Задача 1. Научитесь делать алгоритм Евклида для длинных чисел за $O(n^2)$, где n — длина числа.

Задача 2. Оцените время нахождения НОД набора из n чисел, не больших чем C.

Задача 3. Пусть a, b, c — целые числа. Рассмотрим уравнение $ax + by = c$ относительно целых x, y.
а) Покажите, что, если c не делится на $gcd(a, b)$, решений нет.
б) Покажите, что при $c = gcd(a, b)$, решение есть.
в) Покажите, что, решение есть тогда и только тогда, когда c делится на $gcd(a, b)$.
г) Покажите, что, если существует хотя бы одно решение, существует бесконечно много решений. Опишите их все.

Определение. Числа a, b называются взаимно обратными по модулю m, если $a \cdot b \equiv 1 \pmod m$.

Задача 4. Дано число a. Надо найти за $O(\log m)$ обратное ему по **не обязательно простому** модулю m или определить, что такого не существует.

— — —

Задача 5. Докажите, что $\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{n} = O(\log n)$.

Задача 6. Пусть $\tau(n)$ — количество натуральных делителей n. Докажите, что $\sum\limits_{i=1}^{n} \tau(i) = O(n \log n)$.

Определение. Функция f называется мультипликативной, если $f(n \cdot m) = f(n) \cdot f(m)$ для любых взаимно простых чисел n, m.

Задача 7. Пусть f, g —мультипликативные функции. Докажите, что функция $h(n) = f(n) \cdot g(n)$ мультипликативна.

Задача 8. Пусть f —мультипликативная функция. Докажите, что для любого k функция $g(n) = \sum\limits_{d|n} d^k \cdot f(d)$ мультипликативна. ($d|n$ — d *делит* n)

Задача 9. Докажите, что следующие функции мультипликативны:
а) $\tau(n)$ — количество натуральных делителей n.
б) $\sigma(n)$ — сумма натуральных делителей n.

— — —

Задача 10. За $O(n)$ для всех чисел от 1 до n найдите:
а) В какой степени минимальный простой делитель входит в его разложение.
б) Количество его простых делителей.
в) Количество его делителей.
г) Сумму его делителей.
д) Функцию Эйлера от него.

Задача 11. Научитесь вычислять $a \cdot b$ для натуральных a, b, используя только сложение, деление на 2 (в том числе с остатком), а также проверку на равенство 1 за $O(\log a)$ операций сложения.

Задача 12. (*Дискретное логарифмирование*) $a^x \equiv b \pmod m$, a и m взаимнопросты. Найти решение или определить, что его не существует, за время $O(\sqrt{m} \log m)$.
Подсказка. Представьте x в виде $ky - r$ для $k = \lfloor \sqrt{m} \rfloor$.

— — —

Задача 13. Найти сумму gcd по всем подотрезкам массива натуральных чисел, не больших C, за $O(n \log C)$.

Задача 14. Найти сумму gcd по всем непустым подмножествам массива из n натуральных чисел, не больших C, за $O(n + C \log C)$. Ответ найдите по модулю $10^9 + 7$.

Задача 15. Дан массив из n натуральных чисел, не больших C. Выпишем gcd по всем непустым подмножествам этого массива. Найдите медиану выписанных чисел за $O(n \cdot C \log C)$.

Задача 16. Назовём натуральное число кубастым, если его можно представить в виде $a^3 \cdot b$ для каких-то натуральных $a > 1, b \geq 1$. Найти количество кубастых чисел, не больших n. n до 10^{18}.