6 Алгебра и криптография

6.1 Практика

1. Дано число n, a и b. Известно, что $a^2 = b^2 (\bmod n)$, но $a \neq \pm b \pmod n$. Найдите нетривиальное разложение n на множители.

2. (a) Заметим, что $gcd(2x, 2y) = 2gcd(x, y)$ и, если x — нечетное число, то $gcd(x, 2y) = gcd(x, y)$. Придумайте `gcd` за $\mathcal{O}(n^2)$.

   (b) Придумайте нерекурсивную версию расширенного Евклида.

   (c) Докажите, что для тождества Безу $Ax + By = gcd(x, y)$, которое вернет расширенный Евклид, если $x, y > 0$, то $|A| \leq y$ и $|B| \leq x$.

3. Дано множество натуральных чисел A и параметр b. Известно, что каждое число из A раскладывается в произведение степеней первых b простых чисел (т.е. $\forall a \in A \ a = \prod_{i=1}^{b} p_i^{\alpha_i}$). Требуется найти непустое подмножество A, числа из которого которые в произведении дадут квадрат некоторого натурального числа. Придумайте полиномиальный от b и $|A|$ алгоритм, для поиска такого подмножества.

4. Дана матрица A размера $n \times m$ над конечным полем, $n \geq m$. Найдите матрицу B размера $m \times n$ такую, что $BA = I_{m \times m}$, или установите, что такой не существует.

5. Перед нами стоит задача: получить случайное простое число в диапазоне от 1 до n. Решать ее будем так: выбираем случайное число равновероятно из диапазона и запускаем тест Миллера-Рабина k раз. Если все k тестов прошли, то возвращаем число, иначе — повторяем весь процесс сначала. Этот метод не так плох как кажется, т.к. простые числа достаточно часты (среди чисел от 1 до n примерно $\frac{n}{\ln n}$ простых чисел). Известно, что любое составное число проваливает тест Миллера-Рабина с вероятностью $\frac{3}{4}$, и повторные запуски теста независимы друг от друга. Какое минимальное k нужно выбрать, чтобы получить простое число с вероятностью $\geq 90\%$?

6. Вам дана система линейных уравнений по модулю n. Решите данную систему при условии, что

   (a) $n = pq$, p, q — разные простые.

   (b) $n = p^k$, p — простое.

   (c) для произвольного n.

7. Есть множество $A \subseteq [n]$ и k ячеек, каждая из которых умеет хранить $\mathcal{O}(\log n)$ бит информации. В каждый момент времени максимум t из k ячеек могут оказаться недоступны (мы можем узнать про ячейку, доступна ли она, и, если доступна, прочитать данные). Требуется организовать такой способ хранения информации, чтобы в любой момент времени можно было востановить множество A.

   (a) $k = (t + 1) \cdot |A|$.

   (b) $k = t + |A|$.

8. Допустим, случайно оказалось, что сообщение, шифруемое RSA, не взаимно просто с n. Сломается ли процедура шифрования/дешифрования? Чем плохо такое сообщение?

9. Аня решила послать приглашение на секретную вечеринку Боре, Ване и Гоше. Аня разослала им одинаковый текст приглашения M закодированный с помощью RSA. У Вани, Бори и Гоши выбраны различные n, но ключ e у всех одинаковый: $e = 3$. Придумайте, как Дима сможет узнать, где будет происходить секретная вечеринка, если ему доступны все три шифрованных приглашения и открытые ключи.

10. В d-мерном пространстве над $\mathbb{Q}$ даны точка и набор из k векторов — базис подпространства. Найдите расстояние от точки до подпространства.

11. Для заданных n, k и простого p посчитайте за линейное время $\binom{n}{k} \bmod p$. Учтите, что p может быть меньше, чем n. Можно считать, что все операции в $\mathbb{Z}_p$ выполняются за $\mathcal{O}(1)$.

12. Дан набор векторов с весами, оболочка векторов совпадает со всем пространством. Выбрать из данных векторов базис минимального суммарного веса.

13. Дана матрица A размера 2×2 над кольцом целых чисел. Придумайте алгоритм, представляющий A в виде $A = LDR$, где D — диагональная матрица, а L и R — обратимые.

Дополнительные задачи

1. Известно, что последовательность $1, 1, 2, 3, 5, 8, 13, \ldots$ образована линейным рекуррентным соотношением с коэффициентами $1, 1$: $a_i = a_{i-1} + a_{i-2}$. Решите обратную задачу: дана последовательность длины n, найти минимальное k и k коэффициентов, задающих данную последовательность, как линейную рекурренту.

2. Рассмотрим матрицу $A \in \{0,1\}^{n \times m}$. Для произвольных i и j ($1 \le i \le n$, $1 \le j \le m$) разрешается поменять все значения в строке i и столбце j на противоположные (значение на пересечении строки и столбца меняется). Требуется получить нулевую или единичную матрицу. Придумайте алгоритм за $o((nm)^3)$.

3. Дан набор векторов с весами, оболочка векторов совпадает со всем пространством. Выбрать из данных векторов базис минимального суммарного веса.

4. Найдите базис ядра матрицы над полем.