AMB-6

Волынцев Дмитрий 676 гр.

18 марта 2018

Задача 1

1) (идея взята у Т.Бабушкиной) $(A^n)_{ij}$ - число путей длины n из i в j. Для $n = 1$ верно по определению A. Для остальных верен переход $(A^n)_{ij} = \sum_{k=1}^{4}(A^{n-1})_{ik}A_{kj}$, где элемент суммы - число путей длины n из i в j и их предпоследняя вершина - k. Тогда $g(n) = \sum_{i=1}^{4}(A)_{1i}$
$g(2) = 4 + 2 + 2 + 4 = 12$

Задача 2

1) НОД$(a, N) = 1$, $a^{N-1} \neq 1 \bmod N$. Тогда если $x_i^{N-1} = 1 \bmod N$, то, перемножив с a^{N-1}, получим $a^{N-1} \neq 1 \bmod N$, значит хотя бы половина таких b существует

2) Рассмотрим приведенный алгоритм и оценим его время работы: мы будем получать рандомное число (1 операция), прогонять алгоритм Евклида (полином) и производить деление по модулю (также полином - возведение в степени и вычисление остатков по mod N). Значит, тест Ферма работает за полином операций.

3) Тест Ферма выдает верный результат на составных числах и может ошибаться на простых. Аналогично примеру в комментариях к задаче: $k = \frac{1}{2}$, N независимых прогонов, тогда вероятность равна $1 - \frac{1}{2^N}$

Задача 3

1) Бобу нужно возвести число в степень секретного ключа, который равен $25^{-1} \bmod \varphi(2021)$. $\varphi(2021) = 42 * 46 = 1932$, т.к. $2021 = 43 * 47$. Таким образом получаем уравнение $25x = 1 \bmod 1932$, которое можно решить с помощью алгоритма Евклида:
$1932 = 77 * 25 + 7$
$25 = 3 * 7 + 4$
$7 = 1 * 4 + 3$
$4 = 1 * 3 + 1$
$3 = 3 * 1 + 0$
Тогда $1 = 1*1+0*0 = 1*1+0*(3-3*1) = 0*3+1*1 = 0*3+1*(4-1*3) = 1*4-1*3 = 1*4-1*(7-1*4) = -1*7+2*4 = -1*7+2*(25-3*7) = 2*25-7*7 = 2*25-7*(1932-77*25) = -7*1932+541*25$
Это значит, что $25^{-1} = 541 \bmod 1932$ и ответ: 541

2)

Задача 4

Составим систему $a^{\delta} = 1 \bmod n_1$ и $a^{\delta} = 1 \bmod n_2$, где δ_1 и δ_2 - делители δ. НОД$(n_1, n_2) = 1$, значит по китайской теореме об остатках $\exists!$ решение по $\bmod n_1 n_2$, причем $a^{\delta} = 1 \bmod n_1 n_2$ (т.к. любое $a^{\delta} = x * n_1 n_2 + 1$ подходит). Показателем будет наименьшее такое δ, а значит $\delta =$ НОК(δ_1, δ_2)

Задача 5

$\varphi(n) = 6$
1) Пусть $n = p_1^{\alpha_1} * .. * p_k^{\alpha_k}$ - разложение n на простые множители, тогда $6 = \varphi(p_1^{\alpha_1}) * .. * \varphi(p_k^{\alpha_k})$
$\varphi(x)$ - четно при $x > 2$, значит нет x такого, что $\varphi(x) = 3$, а значит каждый множитель п.ч. равен либо 1, либо 6. Если 1, то ее дает только 2^1. Если 6: при $\alpha = 1$ $\varphi(p) = p - 1 = 6$ и $p = 7$; при $\alpha > 1$ $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = 6$, т.е. p - делитель 6. 2 не подходит (нет решений), 3 подходит: $\alpha = 2$, $p^{\alpha} = 9$
$\varphi(2) = 1$, $\varphi(7) = 6$, $\varphi(9) = 6$; НОД(2,7)=1=НОД(2,9), значит $\varphi(14) = \varphi(18) = 6$ Таким образом все возможные решения: 7,9,14,18

2)

3) Количество первообразных корней по mod 19 равно $\varphi(\varphi(19)) = \varphi(18) =$

6. a - первообразный корень тогда и только тогда, когда $a^{\varphi(p)} = 1 \bmod p$ и для любого делителя d p (не равны) $a^d \neq 1 \bmod p$
$\varphi(19) = 18$, делители: 1,2,3,6,9. Проверим 2:(все по mod 19)
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^6 = 64 = 7$
$2^9 = 7 * 8 = 18$
2 - первообразный корень. Тогда получим все первообразные, возводя 2 в степени, взаимнопростые с 18:(все по mod 19)
$2^1 = 2$
$2^5 = 13$
$2^7 = 14$
$2^{11} = 15$
$2^{13} = 3$
$2^{17} = 10$
Первообразные корни: 2,3,10,13,14,15

Задача 6