Задание 3

Коновалов Андрей, 074

1	2	3	4	5	6	7	8	9	10	Σ

Введем обозначения: P - множество простых чисел, $a \ \% \ b$ - остаток от деления a на b.

Задача 1

(i) Вычисление g_n самым "тупым" способом дает асимтотику $\Theta(n)$, т.к. необходимо сделать $n-2$ шагов, вычисляя последовательно $g_3, g_4, ..., g_n$, при условии, что $g_1 = 3$ и $g_2 = 7$ (естественно, считая все по mod 19).

(ii) Докажем, что последовательность $\{g_n\}$ периодична по любому модулю. Пусть последовательность $\{f_n = g_n \ \% \ 19\}$. Каждое следующее число в f_n определяется только двумя предыдущими. Заметим, что $\forall n \ 0 \leq f_n < 19$. Поскольку f_n бесконечна, а число возможных пар ее элементов конечно, то в какой-то момент f_n зациклится.

Рассчитаем период для mod 19. Для f_n получим $3, 7, 17, 3, 4, 11, 7, 6, 0, 6, 12, 11, 15, 3, 2, 7, 16, 1, 18, 18, 16, 12, 2, 16, 15, 8, 12, 13, 0, 13, 7, 8, 4, 16, 17, 12, 3, 18, 1, 1, 3, 7$. Последние 2 элемента f_n совпали с первыми двумя, дальше все будет циклически повторяться. Итого, период f_n равен 40.

Для вычисления f_n в этом случае необходимо рассчитать период, который имеет размер $r = O(p^2)$, а затем за $\Theta(1)$ можно найти и f_n взяв элемент $n \ \% \ r$ периода. Итоговая асимптотика получается $O(p^2)$, или, если считать $p = const$, $\Theta(1)$.

(iii) Явная формула для g_n (была получена в предыдущем задании):

$$g_n = \frac{1}{2}\left(1+\sqrt{2}\right)^{n+1} + \frac{1}{2}\left(1-\sqrt{2}\right)^{n+1}$$

Заметим, что 2 является квадратичным вычетом по mod 23, поскольку $x^2 \equiv 2 \pmod{23}$ при $x = 5$. Из корректности выражения для g_n следует, что все слагаемые, содержащие $\sqrt{2}$ уйдут, а значит, при подсчете g_n по mod 23 можно заменить $\sqrt{2}$ на 5, так как $2 \equiv 5^2 \pmod{23}$. Получим

$$g_n = \frac{6^{n+1}}{2} + \frac{(-4)^{n+1}}{2}$$

Теперь можно считать g_n считая числа вида a^n за $\Theta(\log n)$.

Посчитаем ответ для $n = 10000$. Заметим, что по малой теореме Ферма $a^{22} \equiv 1 \pmod{23}$. Поскольку $10001 \equiv 13 \pmod{22}$, то $a^{10001} \equiv a^{13} \pmod{23}$. Получаем, что $g_{10000} \equiv \frac{6^{13}-4^{13}}{2} \equiv 10 \pmod{23}$.

Задача 2

(i) Допустим, что больше чем для половины чисел из промежутка $1 \leq b < N$ выполнено $b^{N-1} \equiv 1 \pmod{N}$. Поскольку $a^{N-1} \neq 1 \pmod{N}$, то для всех тех b выполнено $(ab)^{N-1} \neq 1 \pmod{N}$.

Заметим, что все эти b различны. Иначе пусть $ab_1 \equiv ab_2 \pmod{N}$. Вопользовавшись тем, что НОД$(a, N) = 1$ получаем, что $b_1 \equiv b_2 \pmod{N}$, а числа b_1 и b_2 были различны изначально.

Получаем, что каждому $b^{N-1} \equiv 1 \pmod{N}$ соответствует число $(ab)^{N-1} \neq 1 \pmod{N}$. Посколько чисел b больше, чем половина промежутка $1 \leq b < N$, то и чисел ab будет больше, чем половина, что невозможно.

(ii) В тесте Ферма используются две ассимптотически "сложные" операции: подсчет НОД(a, N) и $a^{N-1} \pmod{N}$. Возведение в степень N, как известно, выполняется за $\Theta(\log N)$.

Алгоритм Евклида "дольше" всего выполняется на двух последовательных числах Фибоначчи. Если $a = F_n$, $b = F_{n-1}$, то будет выполнено $n-2$ шагов алгоритма. Учитвая, что числа Фибоначчи растут экспоненциально (как константа в степени n), получаем, что алгоритм Евклида выполняется за $O(\log min(a, b))$ шагов. В нашем случае это $O(\log N)$.

Получаем, что тест Ферма выполняется за $O(\log N)$, а значит за полиномиальное по входу число операций.

(iii) Тест Ферма не ошибается, если число составное, то есть, если он выдает ответ "нет". Количество ответов "нет" не увеличится, если не делать проверку на НОД, но тогда, в соответствии с пунктом *(i)*, по крайней мере для половины чисел a из промежутка $[0, N)$ выполнено $a^{N-1} \neq 1 \pmod{N}$, а значит ответ для них будет "нет". В итоге, по крайней мере для половины чисел ответ будет "нет", а значит правильный.

Задача 3

Что бы алгоритм был полиномиальным, необходимо, что бы его сложность была $O(polynom(\log N))$. При выполнении решета Эратосфена нам необходимо "посетить" каждый элемент списка от 1 до N по крайней мере 1 раз. Значит сложность алгоритма будет $\Omega(N)$.

При проходе по списку мы находим очередное невычеркнутое число и вычеркиваем кратные ему. Понятно, что каждое найденное невычеркнутое число будет простым. Получаем, что

$$complexity = \Theta\left(\frac{N}{2} + \frac{N}{3} + \frac{N}{5} + \frac{N}{7} + ...\right)$$

Оценим сложность сверху

$$complexity = O\left(\frac{N}{2} + \frac{N}{3} + \frac{N}{4} + \frac{N}{5} + ...\right) = O(N \log N)$$

Получаем, что сложность решета Эратосфена $O(N \log N)$.

Задача 5

Пусть открытый ключ Боба $(e, N) = (10, 899)$. Тогда

$$N = pq \quad \wedge \quad p, q \in P \quad \Rightarrow \quad p = 29,\ q = 31$$

Когда Боб вычислял e он воспользовался неким числом d, таким, что

$$e \equiv d^{-1} \pmod{(p-1)(q-1)}$$

или

$$10d \equiv 1 \pmod{28 \cdot 30 = 840}$$

Верно, что

$$10d \equiv 1 \pmod{840} \quad \Rightarrow \quad 10d \equiv 1 \pmod{10}$$

но

$$10d \equiv 0 \pmod{10}$$

Значит такого числа d не могло существовать и задача некорректна.

Задача 7

Воспользуемся тем, что если n факторизовано как

$$n = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$$

то

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot ... \cdot (p_k^{\alpha_k} - p_k^{\alpha_k})$$

Есть четыре "различных" способа "факторизовать" число 6:

$$6 = 6 \cdot 1^t = 2 \cdot 3 = 2 \cdot 3 \cdot 1^t$$

где каждый сомножитель соответствует одной скобке в разложении $\phi(n)$.

Решим уравнения

$$(p^k - p^{k-1}) = v, \quad p \in P,\ v \in \{1, 2, 3, 6\}$$

Получим решения

$$v = 1,\ k = 1,\ p = 2$$
$$v = 2,\ \{k = 1,\ p = 3\},\ \{k = 2,\ p = 2\}$$
$$v = 3,\ \varnothing$$
$$v = 6,\ \{k = 1,\ p = 7\},\ \{k = 2,\ p = 3\}$$

Получаем, что существует 2 решения (7 и 3^2), соответствующие первому способу факторизации и 2 решения($7 \cdot 2$ и $3^2 \cdot 2$), соответствующие второму. Итого, $n \in \{7, 9, 14, 18\}$.

Задача 8

Посчитаем показатель для каждого из чисел $(0, 19)$. Получим

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2

(i) Распределие по вычетов по показателям:

1	2	3	6	9	18
1	18	7, 11	8, 12	4, 5, 6, 9, 16, 17	2, 3, 10, 13, 14, 15

(ii) Первообразные корни: $2, 3, 10, 13, 14, 15$.