Шифрование и задача дискретного логарифмирования

Предположим, что Алиса и Боб хотят обменяться секретной информацией (например, паролем). При этом все сообщения, которые они друг другу передают, становится видны постороннему наблюдателю Еве. Могут ли Алиса и Боб осуществить задуманное?

Для решения этой задачи можно использовать следующий трюк. Сначала Алиса и Боб находят большое простое число p и первообразный корень g по модулю p. После этого Алиса загадывает большое число A и сообщает Бобу g^A, а Боб загадывает большое число B и сообщает Алисе g^B.

После этого Алиса, имея A и g^B, может получить $(g^B)^A = g^{A\cdot B}$. Боб, имея B и g^A, также может получить $(g^A)^B = g^{A\cdot B}$. Используя $g^{A\cdot B}$, они могут кодировать сообщения по модулю $g^{A\cdot B}$.

А что делать Еве? Она знает p, g, $g^A = x$, $g^B = y$. Но для вычисления $g^{A\cdot B}$ этих данных недостаточно, нужно найти A, то есть дискретный логарифм числа x по основанию g. Так как на данный момент нет алгоритмов, которые бы позволили быстро решить данную задачу, Ева не сможет найти число A, а значит, и $g^{A\cdot B}$.

Дискретный логарифм нельзя быстро найти перебором из-за того, что g имеет очень большой порядок по модулю p. Поэтому в данном случае вместо простых чисел можно рассматривать также числа, по модулю которых есть элементы достаточно большого порядка. Например, произведение двух простых или квадрат простого числа также будут годиться.

Чтобы использовать данный метод, надо уметь находить достаточно большие простые или почти простые числа. И тут часто используют так называемый вероятностный тест на простоту. Это означает, что мы берём число и проводим несколько тестов. Чем больше тестов мы проведём, тем с большей вероятностью число простое. Мы не можем быть уверены, что найденное нами число простое, но число с небольшим количеством делителей нас тоже устроит.

Листок состоит из трёх частей. В первой мы обсудим, какие максимальные порядки могут быть у элементов $\mathbb{Z}/m\mathbb{Z}$. Вторая и третья посвящена двум различным вероятностным методам на простоту. При желании можно пропустить первую часть, при этом можно использовать теорему из задачи 6.

Задача 1. Дайте определение порядка $d_m(a)$ элемента $a \in (\mathbb{Z}/m\mathbb{Z})^*$, покажите, что $d_m(a)$ делит $\varphi(m)$.

Задача 2. Пусть $k = d_m(a)$, $l = d_m(b)$. Верно ли, что
а) если $(k, l) = 1$, то $d_m(a \cdot b) = kl$;
б) если $(k, l) \neq 1$, то $d_m(a \cdot b) = [k, l]$?
в) Пусть теперь $(n, k) = 1$, $a \in (\mathbb{Z}/nk\mathbb{Z})^*$, a_n и a_k — остатки при делении a на n и k соответственно. Докажите, что $d_{nk}(a) = [d_n(a_n), d_k(a_k)]$.

Задача 3. **а)** Используя задачу 2в), найдите максимальный порядок элемента по модулю 14; 15.
б) Докажите, что первообразный корень может существовать только по модулю чисел вида 2^k, p^m, $2p^m$, где p — простое число, k, m — произвольные положительные степени.

Задача 4. **а)** Докажите, что для любого $l \geqslant 0$ выполняется равенство $5^{2^l} = 1 + 2^{l+2} \cdot u$ для некоторого нечётного числа u, зависящего от l.
б) Найдите $d_{2^l}(5)$.
в) Докажите, что первообразный корень существует по модулям 2 и 4 и не существует по модулю 2^k, $k \geqslant 3$.

Задача 5. Зафиксируем простое число p, и первообразный корень g по модулю p. Будем рассматривать g как натуральное число.
а) Докажите, что если $g^{p-1} \equiv 1 \pmod{p^2}$, то $(g + p)^{p-1} \not\equiv 1 \pmod{p^2}$. Выведите отсюда, что можно считать, заменив g на $g + p$ при необходимости, что $g^{p-1} \not\equiv 1 \pmod{p^2}$.

Положим $g^{p-1} = 1 + pu$, где u не делится на p.
б) Докажите, что $g^{(p-1)p^k} = 1 + p^{k+1}u_k$ для некоторого u_k, не делящегося на p.
в) Докажите, что g — первообразный корень по модулю p^n для любого n.

Задача 6. (*Теорема о существовании первообразного корня*) Докажите, что первообразный корень по модулю n существует тогда и только тогда, когда $n \in \{2, 4, p^\alpha, 2p^\alpha\}$, где p — нечётное простое, α — положительное целое.

Тест Ферма на простоту

Тест Ферма устроен так. Берём любой остаток a по модулю n. Проверяем, что $(a, n) = 1$. Если $a^{n-1} \not\equiv 1$, то n — не простое. Если $a^{n-1} \equiv 1$ (то есть, *a прошёл тест Ферма по модулю n*), берём любой новый остаток по модулю n, и т.д.
Обозначение 1. Пусть $B_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{n-1} = 1\}$ — множество остатков по модулю n, которые проходят тест Ферма.

Задача 7. Докажите, что **а)** либо $B_n = (\mathbb{Z}/n\mathbb{Z})^*$, либо $|B_n| \leqslant \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^*|$;
б) если n — простое, то все остатки проходят тест Ферма. **в)** Найдите $|B_n|$ для $n \leqslant 10$.

Задача 8. Докажите, что если мы провели тест Ферма для числа n ровно k раз, и каждый раз остаток проходил тест Ферма, то с вероятностью $1 - \frac{1}{2^k}$ все остатки проходят тест Ферма по модулю n (мы считаем, что каждый раз мы независимо выбираем новый остаток).

Тем самым мы довольно быстро с большой вероятностью можем заключить, что $B_n = (\mathbb{Z}/n\mathbb{Z})^*$. Это хорошая новость. Плохая новость — есть составные числа, для которых это тоже верно.

Определение 1. *Числом Кармайкла* называется такое составное число $n > 1$, что $B_n = (\mathbb{Z}/n\mathbb{Z})^*$.

Теорема 1. *Составное число n является числом Кармайкла тогда и только тогда, когда выполнено два условия:*
(1) n свободно от квадратов, то есть n не делится на p^2 для любого простого p;
(2) для любого простого делителя $p \mid n$ верно, что $n - 1$ делится на $p - 1$.

Задача 9. (*Доказательство Теоремы 1 «в обратную сторону»*) Докажите, что если для составного числа n выполнены свойства (1) и (2), то n — число Кармайкла.

Задача 10. Докажите, что $3 \cdot 11 \cdot 17$ и $5 \cdot 13 \cdot 17$ — числа Кармайкла.

Задача 11. Пусть $n = p^k \cdot d$, где $(d, p) = 1$, p — простое и $k \geqslant 2$. Докажите, что
а) найдётся такое число a, что $a \equiv 1 + p \pmod{p^k}$ и $a \equiv 1 \pmod{d}$; **б)** n — не число Кармайкла.

Задача 12. Докажите Теорему 1 «в прямую сторону».

Вывод из Теоремы 1: числа Кармайкла существуют, но их не очень много, что позволяет использовать тест Ферма.

Задача 13. Докажите, что n — число Кармайкла, если и только если $a^n \equiv a \pmod{n}$ для всех $a \in \mathbb{Z}$.

Задача 14. Докажите, что все числа Кармайкла нечётные.

Задача 15. Пусть для натурального k числа $6k + 1$, $12k + 1$, $18k + 1$ — простые. Докажите, что тогда $(6k + 1) \cdot (12k + 1) \cdot (18k + 1)$ — число Кармайкла.

Тест Миллера-Рабина на простоту

Обозначение 2. Пусть n нечётно, $n - 1 = 2^l \cdot m$ для некоторой степени l и нечётного числа m.

Попробуем улучшить наш тест. Как мы знаем, простые числа n отличаются от составных тем, что многочлен $x^{n-1} - 1$ имеет ровно $n - 1$ корней в $\mathbb{Z}/n\mathbb{Z}$. Если n — нечётное простое, то данный многочлен можно разложить как $(x^{\frac{n-1}{2}} - 1)(x^{\frac{n-1}{2}} + 1)$, и каждая скобка будет иметь ровно $\frac{n-1}{2}$ корней. Если $\frac{n-1}{2}$ снова чётно, то многочлен можно разложить на три скобки, и.т.д. Пользуясь этой идеей, опишем тест Миллера-Рабина на простоту.

Для каждого остатка a по модулю n сначала вычислим a^m. Если оно равно 1 или -1, то a *прошёл тест Миллера-Рабина.* Иначе будем возводить a^m в квадрат k раз подряд, вычисляя a^{2m}, a^{4m}, …, $a^{2^{l-1}m}$. Если в какой-то момент получим -1, то a прошёл тест Миллера-Рабина. Если не получим, то a не прошёл тест Миллера-Рабина.

Обозначение 3. Положим $B_{MR}(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^m = 1 \text{ или } a^{m2^k} = -1 \text{ для некоторого } 0 \leqslant k < l\}$.

Теорема 2. (Миллер-Рабин) *Если $n > 9$ — нечётное составное число, то $|B_{MR}(n)| \leqslant \frac{1}{4}|(\mathbb{Z}/n\mathbb{Z})^*|$.*

Задача 16. **а)** Докажите, что элементы $B_{MR}(n)$ проходят тест Ферма.
б) Опишите $B_{MR}(n)$ для $n \leqslant 15$. Проверьте теорему Миллера-Рабина для данных n.

Обозначение 4. Пусть M_0 — множество остатков $a \in \mathbb{Z}/n\mathbb{Z}$, для которых $a^m \equiv 1 \pmod{n}$, и пусть M'_k — множество остатков $a \in \mathbb{Z}/n\mathbb{Z}$, для которых $a^{m \cdot 2^k} \equiv -1 \pmod{n}$, $k = 0, \ldots, l - 1$.

Задача 17. **а)** Докажите, что $|M_0| = |M'_0|$, $B_{MR} = M_0 \sqcup M'_0 \sqcup M'_1 \sqcup \ldots \sqcup M'_k$.
б) Пусть $p_1, \ldots p_s$ — простые делители числа n. Обозначим через N_k множество остатков $a \in \mathbb{Z}/n\mathbb{Z}$, для которых $a^{m \cdot 2^k} \equiv \pm 1 \pmod{p_i}$ для всех $i = 1, \ldots, s$, причём хотя бы по одному модулю в равенстве будет 1, и хотя бы по одному модулю будет -1. Докажите, что $|N_k| = 2^s |M'_k|$, $N_k \cap M'_k = \emptyset$.
в) Докажите, что в случае $s \geqslant 3$ выполнено неравенство $|B_{MR}| \leqslant \frac{1}{6}|(\mathbb{Z}/n\mathbb{Z})^*|$.
г) Докажите, что в случае $s = 2$ выполнено неравенство $|B_{MR}| \leqslant \frac{1}{4}|(\mathbb{Z}/n\mathbb{Z})^*|$.
д) Закончите доказательство теоремы Миллера-Рабина, разобрав оставшийся случай $s = 1$.

1	2 а	2 б	2 в	3 а	3 б	4 а	4 б	4 в	5 а	5 б	5 в	6	7 а	7 б	7 в	8	9	10	11 а	11 б	12	13	14	15	16 а	16 б	17 а	17 б	17 в	17 г	17 д