Гомологии групп

Михаил Иванов

13 июля 2019 г.

1. Дискретное логарифмирование по модулю

Наша задача — найти логарифм числа n по основанию a и по модулю p (p — необязательно простое), то есть наименьшее $k \in \mathbb{N}_0$, чтобы было выполнено $a^k \equiv n \pmod p$.

Для начала, если $(a, p) = 1$, то такое наименьшее k строго меньше $\varphi(p)$ (поскольку если для $k \geqslant \varphi(p)$ условие $a^k \equiv n \pmod p$ выполнено, то по теореме Эйлера $a^k = a^{k-\varphi(p)}a^{\varphi(p)} \equiv a^{k-\varphi(p)} \cdot 1 \equiv n \pmod p$, то есть для числа $k-\varphi(p)$ тоже логарифмическое тождество выполнено, и k не является наименьшим). Тогда мы берём любое T, такое что $T^2 \geqslant \varphi(p)$, и рассматриваем два набора чисел:

$$n, n \cdot a^{-1}, n \cdot a^{-2}, \ldots, n \cdot a^{-(T-1)}$$

и

$$1, a^T, a^{2T}, \ldots, a^{(T-1)T}.$$

Предположим, что они пересекаются, то есть $n \cdot a^{-\ell}$ совпало с каким-то a^{mT}. Тогда утверждается, что мы нашли дискретный логарифм (или по крайней мере один из дискретных логарифмов, не наименьший): действительно, из того, что $n \cdot a^{-\ell} \equiv a^{mT}$, следует, что $n \equiv a^{mT+\ell}$, то есть $k = mT + \ell$ подходит.

Обратно, если k — дискретный логарифм, поделим его с остатком на T: $k = mT + \ell$. Тогда $n \equiv a^{mT+\ell}$, откуда $n \cdot a^{-\ell} \equiv a^{mT}$. При этом $\ell < T$, так как это остаток, а $m < T$, поскольку $k < T^2$, так как $k < \varphi(p)$.

Чтобы найти не любой дискретный логарифм, а именно наименьший, надо искать пересечение тех множеств не как угодно. Надо по очереди перебирать $1, a^T, a^{2T}, \ldots$ и искать их среди $n, n \cdot a^{-1}, n \cdot a^{-2}, \ldots, n \cdot a^{-(T-1)}$, а если наше a^{mT} там встретилось несколько раз, то надо найти не какое попало, а наименьшее ℓ, что $a^{mT} \equiv n \cdot a^{-\ell}$. Хэш-таблица вполне позволяет всё это делать за $\mathcal{O}(T)$.

Как же быть в случае $(a, p) \neq 1$? Надо применить приёмчик с разбиением на случаи. Возьмём небольшое натуральное M такое, что в p каждый простой множитель входит в степени, не превосходящей M (например, можно просто взять $M = 64$). Явно переберём $a^0, a^1, \ldots, a^{M-1}$ на предмет того, сравнимы ли они с n (если сравнимы, то первый такой показатель — и есть логарифм). Если нет, то тогда наш искомый логарифм имеет вид $k + M$, где $k \in \mathbb{N}_0$:

$$a^{k+M} \equiv n \pmod p.$$

Разложим на множители:

$$a^k a^M \equiv n \pmod p.$$

Найдём НОД модуля и множителя в левой части: пусть $\left(a^M, p\right) = c$, $p = qc$, $a^M = xc$, а числа q и x уже взаимно простые. Тогда наше условие преобразуется:

$$a^k xc \equiv n \pmod{cq}.$$

Если n не кратно c, то это сравнение не может быть выполнено. Если же кратно, то есть $n = mc$, то сократим:

$$a^k x \equiv m \pmod{q}.$$

Поскольку x взаимно просто с q, можно домножить на обратный к x:

$$a^k \equiv x^{-1} m \pmod{q}.$$

Утверждение: a взаимно просто с q. Действительно, если a и q оба делятся на какое-то простое r, то тогда a^M делится на r^M. При этом $a^M = xc$, где x взаимно просто с q и поэтому не может делиться на r. Значит, c кратно r^M. Следовательно, $p = qc$ кратно r^{M+1}, а мы предполагали, что в p все простые входят в степенях, не превосходящей M.

Итак, $(a, q) \equiv 1$, теперь можно решать задачу дискретного логарифмирования для случая взаимно простого основания и модуля.

2. Извлечение корня по модулю

Мы постараемся научиться извлекать корень любой натуральной степени из любого числа по любому модулю: то есть для данных $a \in \{0, 1, \ldots, p-1\}$ и $m \in \mathbb{N}$ находить такое $t \in \{0, 1, \ldots, p-1\}$, что $t^m \equiv a \pmod{p}$. Вообще говоря, корней может и не быть, а может быть более одного; мы для модуля, некратного 8, покажем, как перечислить их все в каком-то порядке. В этом деле у нас будет два друга: КТО (китайская теорема об остатках) и дискретное логарифмирование.

Для начала сведём все наши размышления к случаю, когда p — степень простого.

Теорема 1. *Пусть вместо того, чтобы найти* $\sqrt[m]{a} \pmod{p}$, *мы нашли* $b \equiv \sqrt[m]{a} \pmod{q}$ *и* $c \equiv \sqrt[m]{a} \pmod{r}$, *где* $p = qr$, $(q, r) = 1$. *Рассмотрим по китайской теореме об остатках такой вычет* $t \pmod{p}$, *что* $t \equiv b \pmod{q}$ *и* $t \equiv c \pmod{r}$. *Тогда он является корнем* m*-й степени из* a *по модулю* p: $t^m \equiv c \pmod{p}$.

Обратно, любое $t \equiv \sqrt[m]{a} \pmod{p}$ *является корнем* m*-й степени из* a *по модулям* q *и* r: $t^m \equiv c \pmod{q}$, $t^m \equiv c \pmod{r}$.

Доказательство. В одну сторону, так как $t \equiv b \pmod{q}$ и $t \equiv c \pmod{r}$, получается, что $t^m \equiv b^m \equiv a \pmod{q}$ и $t^m \equiv c^m \equiv a \pmod{r}$. Поскольку t^m сравнимо с a и по модулю q, и по модулю r, по КТО оно сравнимо с a по модулю $qr = p$.

Обратно, если $t^m \equiv c \pmod{p}$, то это сравнение верно по модулю любого делителя p, в частности, по модулям q и r. □

Следствие. *Корни* m*-й степени из* a *по модулю* p *находятся в биекции (взаимно однозначном соответствии) с парами корней* m*-й степени из* a *по модулям* q *и* r. *В частности, если всего* x *корней* m*-й степени из* a *по модулю* q *и* y *корней* m*-й степени из* a *по модулю* r, *то по модулю* p *корней* xy.

Теорема даёт нам такой рецепт корня m-й степени из a по модулю p:

1. Разложим p на простые множители: $p = \prod_{i=1}^{k} p_i^{\alpha_i}$.

2. Извлечём корни m-й степени из a по модулю $p_i^{\alpha_i}$, получим k вычетов $t_1, \ldots, t_k$. Если хоть какого-то из t_i не существует (то есть если хотя бы один из корней не извлёкся), то и корня по модулю p не существует.

3. С помощью КТО склеим все сравнимости $\sqrt[m]{a} \equiv t_i \pmod{p_i^{\alpha_i}}$ в одну сравнимость $\sqrt[m]{a} \equiv t \pmod{p}$. t — это и есть искомый корень.

Рецепт для поиска *всех* корней аналогичен.

1. Разложим p на простые множители: $p = \prod_{i=1}^{k} p_i^{\alpha_i}$.

2. Извлечём корни m-й степени из a по модулю $p_i^{\alpha_i}$, получим для $p_1^{\alpha_1}$ сколько-то корней: $t_{1,1}, t_{1,2}, \ldots, t_{1,\ell_1}$; для $p_2^{\alpha_2}$ сколько-то корней: $t_{2,1}, t_{2,2}, \ldots, t_{2,\ell_2}$, и так далее.

3. Тогда по модулю p всего $\prod_{i=1}^{k} \ell_i$ корней. Чтобы их все получить, надо всеми способами выбрать по одному корню по каждому из модулей $p_i^{\alpha_i}$ и с помощью КТО склеить все сравнимости $\sqrt[m]{a} \equiv t_{i_1} \pmod{p_1^{\alpha_1}}$, $\sqrt[m]{a} \equiv t_{i_2} \pmod{p_2^{\alpha_2}}$, …, $\sqrt[m]{a} \equiv t_{i_k} \pmod{p_k^{\alpha_k}}$ в одну сравнимость $\sqrt[m]{a} \equiv t_{i_1,i_2,\ldots,i_k} \pmod{p}$. Нужные нам корни — это и есть все возможные $t_{i_1,i_2,\ldots,i_k}$.

Здорово, осталось всего лишь научиться делать всё по модулю степени простого. Как же извлечь корень из a степени m по модулю p^α? Сейчас мы постараемся свести всё к случаю, когда $(a, p) = 1$, то есть a не делится на p.

1. Если $a \equiv 0$ (a делится на p^α), то нам подойдёт в качестве корня t, делящееся на достаточно большую степень p: а именно, если t делится ровно на p^k, то его m-я степень будет делиться ровно на p^{km}, то есть просто должно быть выполнено $km \geqslant \alpha$. Таким образом, корни — ровно те вычеты, которые делятся на $p^{\lceil \frac{\alpha}{m} \rceil}$.

2. Если a делится степень p, меньшую, чем α (возможно, нулевую). Показатель этой степени должен делиться на m, то есть иметь вид km для какого-то $k \in \mathbb{N}_0$, иначе a не будет ничьей m-й степенью. Ну, получается такая задача: нам дали какой-то вычет $a_1 \cdot p^{km} \pmod{p^\alpha}$, надо извлечь из него корень m-й степени. Для этого мы сократим на p^{mk} и будем вместо этого извлекать корень m-й степени из a_1 по модулю $p^{\alpha-mk}$, где a_1 взаимно просто с $p^{\alpha-mk}$. Предположим, что мы справились и нашли корень: ${t_1}^m \equiv a_1 \pmod{p^{\alpha-mk}}$. Тогда можно взять любое $t \pmod{p^{\alpha-k}}$, которое сравнимо с $t_1 p^k$ по модулю $p^{\alpha-(m-1)k}$ (например, просто взять в качестве t число $t_1 p^k$, однако на самом деле вариантов тут $p^{(m-2)k}$ вариантов), и оно будет искомым корнем m-й степени:

$$t^m \equiv \left(t_1 p^k\right)^m \equiv {t_1}^m p^{km} \equiv a_1 p^{km} \equiv a \pmod{p^\alpha}.$$

Здесь сомнения может вызывать только первое сравнение. Мы знаем, что $t - t_1 p^k$ кратно $p^{\alpha-(m-1)k}$, и хотим понять, почему $t^m - \left(t_1 p^k\right)^m$ кратно p^α. Ну, так как $t - t_1 p^k$ кратно $p^{\alpha-(m-1)k}$, оно кратно даже p^k, поэтому t кратно p^k, поэтому $t = t_2 p^k$, тогда $t_2 - t_1$ кратно $p^{\alpha-mk}$, тогда $t_1 \equiv t_2 \pmod{p^{\alpha-mk}}$, тогда ${t_1}^m \equiv {t_2}^m$

$(\mathrm{mod}\ p^{\alpha-mk})$, поэтому $t^m - \left(t_1 p^k\right)^m = {t_2}^m p^{km} - {t_1}^m p^{km} = \left(t_2 - t_1\right) p^{km}$ делится на $p^{\alpha-km} \cdot p^{km} = p^\alpha$. Можно понять, что мы на самом деле доказали, что это все возможные корни m-й степени из a.

Теперь осталось рассмотреть случай, когда a взаимно просто с p^α, то есть a не делится на p. Положим пока, что p — нечётное простое, а случай двойки оставим на потом. Вспомним, что у нас есть первообразный корень по модулю p^α (это g, чьи степени — это вся приведённая система вычетов по модулю p^α; оно же такой вычет, который впервые объединичивается в степени $\varphi\left(p^\alpha\right) = p^\alpha - p^{\alpha-1}$: то есть $g^i \equiv 1 \pmod{p^\alpha}$ при $i = p^\alpha - p^{\alpha-1}$, а $g^i \not\equiv 1 \pmod{p^\alpha}$ при $i \in \{0, 1, \ldots, p^\alpha - p^{\alpha-1} - 1\}$). Найдём дискретный логарифм a по основанию g по модулю p^α (поскольку $(g, p^\alpha) = 1$, приятным бонусом будет, что основание логарифма взаимно просто с модулем, то есть достаточно простой версии дискретного логарифма), получим, что $a \equiv g^k \pmod{p^\alpha}$. То есть извлечь корень m-й степени надо из g^k. Мы его будем искать тоже в виде степени g^ℓ. Он является корнем, если $g^{\ell m} \equiv g^k$, а это равносильно тому, что $g^{\ell m - k} \equiv 1$, то есть $\ell m - k$ кратно $\varphi\left(p^k\right)$.

Что же? Нам дали числа m и k и просят найти все такие $\ell \pmod{\varphi\left(p^k\right)}$, чтобы было выполнено сравнение $\ell m \equiv k \pmod{\varphi\left(p^k\right)}$. Такие сравнения решаются стандартным образом: найти c, то есть НОД m и $\varphi\left(p^k\right)$, если k на него не делится, то решений нет, иначе надо сократить всё на c, получится $\ell m' \equiv k' \pmod{\frac{\varphi\left(p^k\right)}{c}}$. Теперь уже m' взаимно просто с модулем, так что можно на него сократить: $\ell \equiv \frac{k'}{m'} \pmod{\frac{\varphi\left(p^k\right)}{c}}$, ну вот мы и задали остаток ℓ при делении на $\frac{\varphi\left(p^k\right)}{c}$ (который соответствует ровно c различным вычетам ℓ по модулю $\varphi\left(p^k\right)$.

Ну хорошо, а что же с двойкой? По модулю 2^α нет первообразного корня при $\alpha \geqslant 3$ (то есть, если $\alpha \leqslant 2$, то всё предыдущее рассуждение прекрасно работает, либо же при $\alpha \leqslant 2$ можно всё там разобрать вручную). Проблема в том, что все квадраты сравнимы с единицей по модулю восемь, поэтому, если взять нечётный вычет d, то по модулю восемь его степени выглядят так: $d, 1, d, 1, d, 1, \ldots$. Это означает, что нельзя одним и тем же генератором породить все остатки, и сравнимые с 3, и сравнимые с 5, и сравнимые с 7 по модулю 8, можно вложиться максимум в один из них. Поэтому задача перечисления всех корней довольно сложная. Однако задача нахождения *одного* корня *чётной* степени всё ещё поддаётся решению.

А именно, заметим, что, поскольку m чётно, a должно быть сравнимо с 1 по модулю 8, ведь если корень равен r, то $r^{\frac{m}{2}}$ является квадратным корнем из a, а он бывает только для $a \equiv 1 \pmod 8$. Поэтому на самом деле нам не требуется первообразный корень, порождающий всю приведённую систему вычетов по модулю 2^α; нам достаточно породить лишь те остатки, из которых возможно извлечь квадратный корень. Такой недопервообразный корень существует!

Лемма. *Число 5 всегда является недопервообразным корнем по модулю 2^α при $\alpha \geqslant 3$. А именно, среди чисел 5^0, 5^2, 5^4, …, $5^{2^{\alpha-2}-2}$ встречаются все $2^{\alpha-3}$ остатков, сравнимых с 1 по модулю 8, по одному разу каждый.*

Доказательство. Все эти остатки действительно сравнимы с 1 по модулю 8, поэтому достаточно понять, что все они различны. Если среди них есть два одинаковых, то их частное сравнимо с 1 по модулю 2^α. То есть нашлось число t, что $5^t - 1$ кратно 2^α, где $t < 2^{\alpha-2}$.

Докажем очевидный факт (являющихся частным случаем утверждения, называемого *леммой об уточнении показателя*), из которого следует, что так не бывает.

Теорема 2. *Пусть x и y — нечётные целые числа. Пусть в число $x-y$ двойка входит ровно в k-й степени, $k \geqslant 2$. Тогда в x^2-y^2 двойка входит ровно в $(k+1)$-й степени. Если d — нечётное натуральное число, то в x^d-y^d двойка входит ровно в k-й степени.*

Доказательство. $x^2-y^2=(x+y)(x-y)$. Во второй множитель двойка входит ровно в k-й степени, поэтому нужно доказать, что в первый она входит ровно в первой степени. Первый множитель чётный, так как это сумма двух нечётных чисел. Почему же он не делится на четыре? Ну, если он делится, то сумма $x+y$ и $x-y$ тоже делится на 4. Однако их сумма равна $2x$, которое делится ровно на первую степень двойки.

Посмотрим теперь на x^d-y^d. Из несложной алгебры следует, что это выражение равно $(x-y)\left(x^{d-1}+x^{d-2}y+x^{d-3}y^2+\ldots+y^{d-1}\right)$. Первый множитель делится на двойку ровно в k-й степени, а второй нечётен, ведь он состоит ровно из d нечётных слагаемых, где d нечётно. Значит, в x^d-y^d двойка входит в k-й степени. □

Теперь всё ясно. Нам интересно, в какой степени двойка входит в 5^t-1. Пусть $t=2^\ell d$, где d нечётно; легко видеть, $\ell \leqslant \alpha-3$, ведь $t<2^{\alpha-2}$. Так как $5-1$ делится ровно на 4, 5^2-1 делится ровно на 8, 5^4-1 делится ровно на 16, …, $5^{2^\ell}-1$ делится ровно на $(2+\ell)$-ю степень двойки. Тогда $5^{2^\ell d}-1=5^t-1$ тоже делится ровно на $(2+\ell)$-ю степень двойки, что меньше, чем α. □

Итак, для извлечения такого корня можно логарифмировать не по первообразному корню, а по недопервообразному.