ПЕРВООБРАЗНЫЕ КОРНИ: ПРОДОЛЖЕНИЕ

ПОСТРОЕНИЕ ПЕРВООБРАЗНОГО КОРНЯ

На прошлом уроке мы получили, что $\forall\, i\ \exists\, a_i$ — остаток по модулю p такой, что $Ord\ a_i = q_1^{\beta_1} q_i^{\alpha_i} \dots q_s^{\beta_s}$.

Сконструируем на их основе элементы, порядки которых будут равны в точности $q_i^{\alpha_i}$.

ЛЕММА

Если $Ord\ a = k = l \cdot m$, то $Ord\ (a^l) = m$.
Очевидно, ведь a^l не может стать сравнимо с 1 по модулю p не раньше и не позже, чем через m шагов.

Для каждого $i = 1, 2, \dots, s$ рассмотрим элемент $b_i = a_i^{\frac{Ord\ a_i}{q_i^{\alpha_i}}}$.
По лемме (при $m = q_i^{\alpha_i}$) его порядок будет равен $q_i^{\alpha_i}$.

Далее мы докажем лемму о взаимно простых порядках и на ее основе выведем, что как раз произведение $b_1 b_2 \dots b_s$ и будет являться первообразным корнем.

ЛЕММА О ПОРЯДКАХ

ЛЕММА

Пусть $Ord\ a = t$, $Ord\ b = s$, и $НОД(t, s) = 1$. Тогда $Ord\ (ab) = ts$.

ДОКАЗАТЕЛЬСТВО

$(ab)^{ts} = (a^t)^s (b^s)^t \equiv 1 \bmod p$.

Пусть $(ab)^k \equiv 1 \bmod p$. Тогда $a^k = b^{-k}$ по модулю p.

Обозначим $c = a^k = b^{-k}$. Имеем: $Ord\ c \mid t$, а также $Ord\ c \mid s$. Но по условию $НОД(t, s) = 1$, а значит $Ord\ c = 1$. Это возможно только если $c \equiv 1 \bmod p$. Значит, $a^k \equiv 1 \bmod p$, $b^k \equiv 1 \bmod p$. Значит, число k должно делиться и на t, и на s, а т. к. $НОД(t, s) = 1$, число k кратно произведению ts.

Что и требовалось доказать.

По сути это завершает доказательство теоремы о существовании первообразного корня, который мы сконструировали. Ведь по индукции порядок произведения $b_1 b_2 \dots b_s$ будет равен $q_1^{\alpha_1} q_i^{\alpha_2} \dots q_s^{\alpha_s}$, что как раз равно $p - 1$.

ТЕОРЕМА О КОРНЯХ ОСТАТКОВ

На прошлом уроке нами установлен критерий:
a — первообразный корень по модулю $p \Leftrightarrow a^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p$ ни при каком i, где $p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$.

ТЕОРЕМА

Пусть $p - 1 = rt$, где r, $t > 1$ — натуральные числа.
Тогда $\exists \sqrt[r]{a}$ по модулю $p \Leftrightarrow a^t \equiv 1 \bmod p$.

Мы уже доказали, что $\exists \sqrt{a}$ по модулю $p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Теперь докажем для корня любой степени, являющейся делителем числа $p - 1$.

Пример: $p = 13 \Rightarrow p - 1 = 12 = 3 \cdot 4$. Согласно этому утверждению, $\exists \sqrt[3]{a}$ по модулю $13 \Leftrightarrow a^4 \equiv 1 \bmod 13$.

Докажем мы эту теорему чуть позже, а пока получим следствие из нее.

СЛЕДСТВИЕ

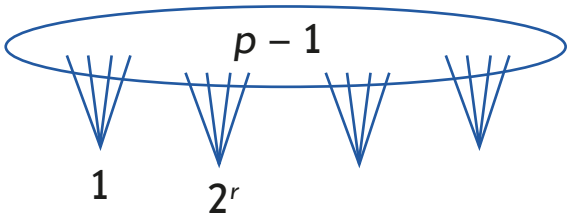
a — первообразный корень по модулю $p \Leftrightarrow$ не существует корней из a ни одной из степеней $q_1, q_2, \ldots q_s$, где $p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$.

В результате вопрос о поиске первообразного корня сводится к вопросу о существовании таких корней. Это отдельная интереснейшая область арифметики, которой первым занялся Гаусс — законы взаимности. Гаусс установил, как можно понять, существует ли квадратный корень из данного остатка по простому модулю.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ О КОРНЯХ ОСТАТКОВ

Итак, $p - 1 = rt$. Выпишем подряд все r-тые степени остатков: $1^r, 2^r, \ldots (p-1)^r$. Вопрос: сколько их различных? Не более, чем t, ибо $(b^r)^t = b^{p-1} \equiv 1 \bmod p$, а значит, все они — корни многочлена $x^t - 1$.

Имеем такую картину: все $p - 1$ остатков некоторым образом группируются в r-тые степени:



Должно получиться не более, чем t групп. Если же групп получится меньше, чем t, то в какой-то группе $b^r = c$ должно больше, чем r элементов. Но это невозможно, т. к. многочлен $x^r - c$ не может иметь более, чем r корней. То есть будет ровно t групп ровно по r элементов.

Таким образом, мы получаем, что $\exists \sqrt[r]{a}$ по модулю $p \Leftrightarrow a^t \equiv 1 \bmod p$. Теорема доказана.

КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ

(I) $\exists \sqrt{-1}$ по модулю $p \Leftrightarrow p = 4k + 1$ для некоторого целого k;

(II) $\exists \sqrt{2}$ по модулю $p \Leftrightarrow p = 8k \pm 1$ для некоторого целого k;

(III) При простых p и q вида $4k + 3$: $\exists \sqrt{p}$ по модулю $q \Leftrightarrow \nexists \sqrt{q}$ по модулю p;

(IV) При простых p и q таких, что одно из них или оба имеют вид $4k + 1$: $\exists \sqrt{p}$ по модулю $q \Leftrightarrow \exists \sqrt{q}$ по модулю p.

Пример: хотим узнать, существует ли $\sqrt{41}$ по модулю 73. Должен существовать $\sqrt{73}$ по модулю $41 \Leftrightarrow \exists\sqrt{32}$ по модулю $41 \Leftrightarrow \exists\sqrt{2}$ по модулю $41 \Leftrightarrow 41 \equiv \pm 1 \bmod 8$ по пункту (II), а это так и есть. Значит, $\sqrt{41}$ по модулю 73 существует!

Этот метод можно использовать, когда нужно выяснить, существует ли $\sqrt{ab}$. Должно быть выполнено $(ab)^{\frac{p-1}{2}} \equiv 1 \bmod p$. А это выполнено либо когда a и b одновременно являются квадратичными вычетами, либо когда они одновременно являются квадратичными невычетами.

Подробнее о законах взаимности можно прочитать в книге: Аэрленд, Роузен «Классическое введение в современную теорию чисел».