257-, 65537-УГОЛЬНИКИ И «РАЗОБЛАЧЕНИЕ ЧЕРНОЙ МАГИИ»

ПОСТРОЕНИЕ p-УГОЛЬНИКА ДЛЯ p — ПРОСТОГО ЧИСЛА ФЕРМА

При построении правильного 17-угольника мы разбили 8 вспомогательных чисел $v_1, v_2, \dots, v_8$ на две группы:

$A = v_1 + v_2 + v_3 + v_4 + v_8$, $B = v_3 + v_5 + v_6 + v_7$.

На этом уроке с помощью теории первообразных корней мы разберемся, почему именно такое разбиение привело нас к успеху, и как нужно действовать при построении циркулем и линейкой правильных 257- и 65537-угольника.

На уроке 86 мы доказали, что только для простого числа вида $p = 2^r + 1$ возможно построение правильного p-угольника, где, в свою очередь, $r = 2^l$. Построение сводится к тому, чтобы описать алгоритм для квадратичного калькулятора, с помощью которого может быть получено число $v_1 = \xi + \xi^{-1} = 2\cos\frac{2\pi}{p}$, где $\xi = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ — вершина правильного p-угольника на комплексной плоскости (корень p-й степени из 1).

При этом выполнено $\xi + \xi^2 + \dots + \xi^{p-1} = -1$.

Вспомним определение первообразного корня:

ОПРЕДЕЛЕНИЕ

Первообразный корень — такой остаток η при делении на p, что $\eta^0 = 1, \eta^1, \eta^2, \dots, \eta^{p-2}$ — есть все различные ненулевые остатки по модулю p, а $\eta^{p-1} \equiv 0 \ mod\ p$.

То есть если η — первообразный корень, то $Ord\ \eta = p - 1$.

С помощью такого остатка мы и проделаем разбиение группы слагаемых $\xi + \xi^2 + \dots + \xi^{p-1}$ на две части, затем каждую из них еще на две и т.д. так, что в конечном счете получится вычислимое на квадратичном калькуляторе число.

РАЗБИЕНИЕ НА ГРУППЫ СТЕПЕНЕЙ $1, 2, \dots, p-1$

Пусть η — первообразный корень по модулю p. Тогда, переставив слагаемые, мы можем переписать указанную сумму в таком виде:

$\xi^{\eta^0} + \xi^{\eta^1} + \dots + \xi^{\eta^{p-1}} = \xi^{\eta^0} + \xi^{\eta^1} + \dots + \xi^{\eta^{p-1}}$, где $p - 1 = 2^{2^l}$.

Представим это в виде суммы $A + B$, где в группу A соберем все четные степени , а в группу B — все нечетные степени.

Дальше мы разбиваем:

$A = A_1 + A_2$, где в A_1 входят степени η, кратные 4, в A_2 входят степени η, сравнимые с 2 по модулю 4;

$B = B_1 + B_2$, где в B_1 и B_2 входят степени , сравнимые с 1 и 3 по модулю 4, соответственно.

Далее идет разбиение с учетом остатков по модулю 8.

Этот можно продолжать, сколько потребуется, т.к. $p - 1 = 2^{2^l}$. В книге Скопенков и др. «Элементы математики в задачах» доказывается, что такая процедура приведет к нужному алгоритму для квадратичного калькулятора.

Оказывается, для простых чисел вида Ферма в качестве такого числа можно брать число 3. Далее мы это докажем с помощью квадратичного закона взаимности Гаусса.

3 — ПЕРВООБРАЗНЫЙ КОРЕНЬ ДЛЯ ПРОСТОГО ЧИСЛА ФЕРМА

ТЕОРЕМА

Число 3 является первообразным корнем по модулю любого простого числа Ферма $p = 2^{2^l} + 1$, $l > 0$.

ДОКАЗАТЕЛЬСТВО

Нужно доказать, что $\{1, 3, 3^2, \ldots, 3^{p-2}\}$ — все ненулевые остатки по модулю числа Ферма $p = 2^{2^l} + 1$.

Нам достаточно будет того, что $p = 2^r + 1$.
Пусть есть некоторый остаток β. По доказанному нами в уроках, посвященных МТФ, $Ord\ \beta$ делит $p - 1 = 2^r$.
Тогда $Ord\ \beta = 2^s$ для какого-то $s \leqslant r$.

β — первообразный корень $\Leftrightarrow s = r \Leftrightarrow Ord\ \beta$ не делит 2^{r-1}.

Но $2^{r-1} = \frac{p-1}{2}$, и мы доказывали теорему о том, что $\alpha^{\frac{p-1}{2}} \equiv 1\ mod\ p \Leftrightarrow \exists \sqrt{\alpha}\ mod\ p$ (α — квадратичный вычет по модулю p). Значит, β — первообразный корень $\Leftrightarrow \beta$ не является квадратичным вычетом.

Докажем, что 3 не является квадратичным вычетом по модулю простого числа вида Ферма.

КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ

Основное утверждение звучит так:

1-й случай. Пусть p, q — простые числа вида $4k + 3$.
Тогда $\exists \sqrt{p}\ mod\ q \Leftrightarrow \nexists \sqrt{q}\ mod\ p$.

2-й случай. p, q — нечетные простые числа, хотя бы одно из них вида $4k + 3$. Тогда $\exists \sqrt{p}\ mod\ q \Leftrightarrow \exists \sqrt{q}\ mod\ p$.

В конце урока мы наметим доказательство этого утверждения.

3 — первообразный корень по модулю $p \Leftrightarrow \nexists \sqrt{3}\ mod\ p$.
По квадратичному закону взаимности это означает, что $\nexists \sqrt{p}\ mod\ 3$. Значит, должно быть $p = 3k + 2$, а это то же самое, что $2^{2^l} = 3k + 1$. Это всегда выполнено. Тем самым, 3 — действительно первообразный корень.

Теорема доказана.

ПУТЬ ДОКАЗАТЕЛЬСТВА КЗВ

ЛЕММА ЗОЛОТАРЕВА

Рассмотрим перестановку

$$\begin{pmatrix} 0\ 1\ 2 & \ldots & p-1 \\ 0\ q\ 2\ q & \ldots & (p-1)q \end{pmatrix}$$

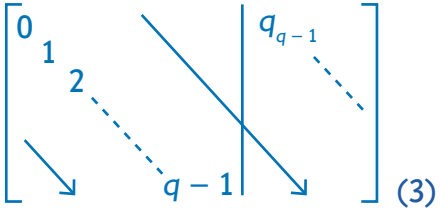
Ее знак равен знаку символа Лежандра $\left(\frac{q}{p}\right)$, т.е. «+» (чет), если $\exists \sqrt{q}\ mod\ p$ и «–» (нечет), если $\nexists \sqrt{q}\ mod\ p$.

3 Рассмотрим также следующие способы перечисления всех остатков по модулю pq от 0 до $pq-1$:

$$\begin{pmatrix} 0\ 1 & \dots & p-1 \\ p\ p+1 & \dots & 2p-1 \\ & \dots & \\ (q-1)p & \dots & qp-1 \end{pmatrix} \quad (1)$$

$$\begin{pmatrix} 0\ q & \dots & (p-1)q \\ 1\ q+1 & \dots & \\ & \dots & \\ q-1 & \dots & qp-1 \end{pmatrix} \quad (2)$$

а также вот такую таблицу:

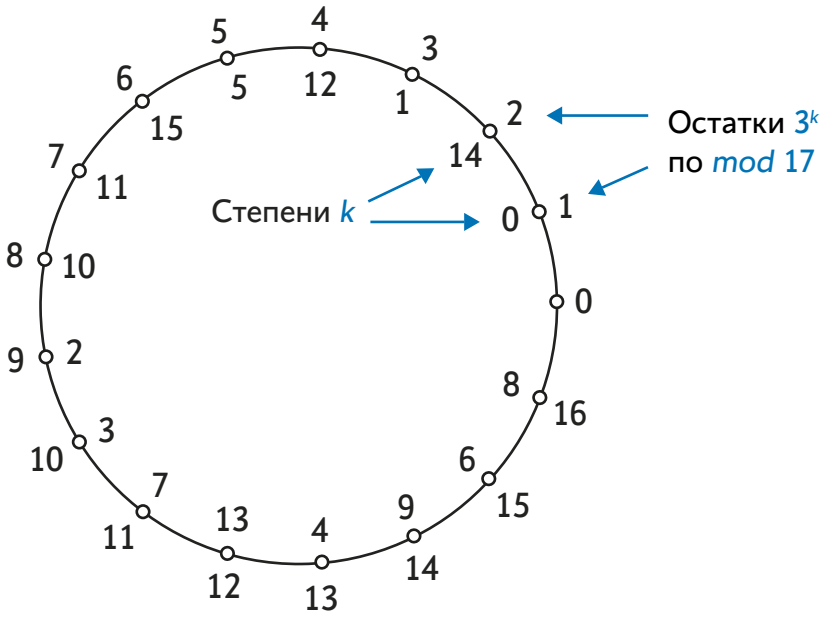


(3)

Количество транспозиций (перемен знака) при переходе от (1) к (2) равно $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, что как раз будет равно 1, если хотя бы одно из чисел p,q имеет вид $4k+1$ и будет равно -1, если оба они имеют вид $4k+3$. Но эта перестановка, на самом деле, есть композиция перестановок перехода от (1) к (3) и от (3) к (2), причем знак одной из них равен $\left(\frac{q}{p}\right)$, а другой — $\left(\frac{p}{q}\right)$.

СЛУЧАЙ 17-УГОЛЬНИК

Так как 3 — первообразный корень по *mod* 17, все степени в тождестве $\eta^1+\eta^2+\eta^3+\dots+\eta^{16}=-1$ соответствуют различным степеням числа 3 по *mod* 17.



В сумму A вошли все такие η^k, которые являются остатками четных степеней 3 по *mod* 17:

$$\eta^1+\eta^2+\eta^4+\eta^8+\eta^9+\eta^{13}+\eta^{15}+\eta^{16}=$$
$$=(\eta^1+\eta^{-1})+(\eta^2+\eta^{-2})+(\eta^4+\eta^{-4})+(\eta^8+\eta^{-8})=A.$$

Соответственно, в сумму B вошли все остатки нечетных степеней 3 по *mod* 17.

При таком разбиении получается, что A и B являются корнями квадратного уравнения с целочисленными коэффициентами.

Далее, мы объединили

$\alpha = v_1 + v_4$;

$\beta = v_2 + v_8$;

$\gamma = v_3 + v_5$;

$\delta = v_6 + v_7$ по принципу, что η^k вв каждой из этих сумм соответствуют степеням 3, имеющим одинаковые остатки при делении на 4. И снова получили, что α и β (а также, γ и δ) являются корнями квадратного уравнения с целочисленными коэффициентами!

Для случаев 257- и 65537-угольников этот же алгоритм можно повторять нужное количество раз.

На этом мы завершаем знакомство с задачами на построение циркулем и линейкой.