1), а остальные разбиваются на пары сопряженных (т.е. симметричных относительно оси абсцисс) корней $\cos\varphi + i\sin\varphi$, $\cos\varphi - i\sin\varphi$, где $\varphi = 2\pi k/n$, $k = 1, \ldots, (n-1)/2$.

Поскольку

$$(x-\cos\varphi - i\sin\varphi)(x-\cos\varphi + i\sin\varphi) = \\ = (x-\cos\varphi)^2 - (i\sin\varphi)^2 = x^2 - 2x\cos\varphi + 1,$$

то разложение $x^n - 1$ на неприводимые множители с вещественными коэффициентами легко выписать:

$$x^n - 1 = (x-1)\prod_{k=1}^{(n-1)/2}\left(x^2 - 2x\cos\frac{2\pi k}{n} + 1\right) \qquad (4)$$

при нечетном n.

Упражнение 20. Разберите случай, когда n четно.

Разложения с неотрицательными коэффициентами

Неразложимость f_p при простом p

В 1937 году в знаменитом парижском журнале «Comptes Rendus» была высказана гипотеза: *ни при каком простом p полином $f_p(x) = x^{p-1} + x^{p-2} + \ldots + 1$ не представим в виде произведения отличных от константы полиномов с вещественными неотрицательными коэффициентами.*

Эта гипотеза вскоре была доказана московским математиком Д.А.Райковым. Мы дадим три доказательства, первое из которых использует комплексные числа и неразложимость f_p на множители с целыми коэффициентами (заметьте — на первый взгляд, не было никакой связи между этими частями статьи, а выясняется, что все едино!), второе опирается на разложение (4) с вещественными коэффициентами, а третье «ничего не использует», но зато требует от читателя сосредоточенности и аккуратности. Итак,

Теорема 1. *Если p — простое число, то в любом разложении многочлена f_p в произведение отличных от константы множителей с вещественными коэффициентами встретится хотя бы один отрицательный коэффициент.*

Начало всех трех способов доказательства одинаково. Предположим, что $f_p(x)$ разложен в произведение многочленов $g(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$ и $h(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$, все коэффициенты которых неотрицательны. Поскольку любой из многочленов g и h можно разделить на положительное число, умножив одновременно другой на это же число, мы будем считать, что $a_m = 1$. Тогда, поскольку старший коэффициент произведения есть произведение старших коэффициентов, обязательно $b_n = 1$.

Если теперь какой-нибудь коэффициент a_k окажется больше 1, сразу возникнет противоречие: при перемножении g и h члены $a_k x^k$ и x^n дадут $a_k x^{n+k}$. Коэффициент при x^{n+k} окажется больше 1.

Поэтому все $a_k \le 1$. Разумеется, и все $b_j \le 1$. В частности, $a_0 \le 1$, $b_0 \le 1$. Поскольку свободный член произведения равен $a_0 b_0 = 1$, то $a_0 = b_0 = 1$.

Первый способ

Разложение $f_p(x) = g(x)h(x)$ имеет вид

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = \\ = \left(x^m + a_{m-1}x^{m-1}\ldots + a_1 x + 1\right)\left(x^n + b_{n-1}x^{n-1}\ldots + b_1 x + 1\right).$$

Коэффициент при первой степени x равен $1 = a_1 + b_1$. Значит, хотя бы одно из чисел a_1, b_1 отлично от 0. Пусть $a_1 \ne 0$. Обратим внимание на произведения $1\cdot x^n$ и $a_1 x \cdot b_{n-1}x^{n-1}$. Если $b_{n-1} > 0$, то коэффициент при x^n в правой части благодаря им оказывается больше 1.

Если же $b_{n-1} = 0$, то противоречие получается по-другому. Вспомним, что многочлен $h(x)$ разлагается на множители вида

$$h(x) = \left(x-\varepsilon^{k_1}\right)\left(x-\varepsilon^{k_2}\right)\ldots\left(x-\varepsilon^{k_n}\right),$$

где $k_1, \ldots, k_n$ — натуральные числа (меньшие p), $\varepsilon = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p}$. Вычисляя коэффициент при x^{n-1}, получим

$$b_{n-1} = -\varepsilon^{k_1} - \varepsilon^{k_2} - \ldots - \varepsilon^{k_n}.$$

Поскольку $b_{n-1} = 0$, многочлен $x^{k_1} + x^{k_2} + \ldots + x^{k_n}$ (заметьте — многочлен с целыми коэффициентами!) имеет общий корень ε с многочленом $f_p(x)$. Последний, как мы знаем, неприводим. Известно (см. упражнение 36 в *Приложении*), что всякий многочлен с целыми коэффициентами, имеющий общий корень с неприводимым многочленом, делится на него. Значит, $x^{k_1} + x^{k_2} + \ldots + x^{k_n}$, степень которого не превосходит $p-1$, делится на многочлен $f_p(x)$ степени $p-1$. Следовательно, $x^{k_1} + x^{k_2} + \ldots + x^{k_n} = f_p(x)$, что невозможно, поскольку левая часть обращается в нуль при $x = 0$.

Второй способ

Начнем с определения. *Полином $P(x) = \sum_{i=0}^{n} a_i x^i$ называется возвратным, если для любого $0 \le i \le n$ справедливо равенство $a_{n-i} = a_i$.*

Упражнение 21. Полином $P(x)$ степени n возвратный тогда и только тогда, когда $P(x) = x^n \cdot P\left(\frac{1}{x}\right)$.

Упражнение 22. Произведение любых двух возвратных многочленов — возвратно.

Теперь сформулируем два вспомогательных утверждения.

Лемма 1. *Многочлены $g(x)$ и $h(x)$ — возвратные.*

Лемма 2. *Все коэффициенты полиномов g, h равны 0 или 1.*

Очевидно, теорема из них следует: подставляя $x = 1$ в разложение $f_p(x) = g(x)h(x)$, получим противоречие с простотой числа $p = f_p(1)$.

Доказательство леммы 1. При $p = 2$ утверждение очевидно. При нечетных p все множители правой части разложения

$$f_p(x) = \prod_{k=1}^{(p-1)/2}\left(x^2 - 2x\cos\frac{2\pi k}{p} + 1\right),$$

полученного из (4), являются возвратными. Значит, в силу упражнения 22, $g(x)$ и $h(x)$ — возвратные.