Упражнение 28. Почему?

Задача решена. Для поклонника индексов и формул мы сейчас переведем это красивое геометрическое решение на язык алгебры.

Для этого обозначим

$$F(x)=a_0+a_1x+a_2x^2+\ldots,\quad G(x)=b_0+b_1x+b_2x^2+\ldots.$$

Тогда

$$(a_0+a_1x+a_2x^2+\ldots)(b_0+b_1x+b_2x^2+\ldots)=1+x+x^2+\ldots+x^{n-1}.$$

Свободный член произведения равен произведению свободных членов, т. е. $a_0\cdot b_0=1$. Значит, $a_0=1$ и $b_0=1$. Коэффициент при первой степени x произведения $F(x)\cdot G(x)$ вычисляется по формуле $a_0b_1+a_1b_0$. Поскольку он равен 1, то либо $a_1=1$, $b_1=0$, либо $a_1=0$, $b_1=1$. Для определенности предположим, что $a_1=1$ и $b_1=0$.

Если все коэффициенты a_i многочлена $F(x)$ равны 1, то утверждение задачи выполнено. Если же среди них присутствует 0, то рассмотрим наименьшее k, для которого $a_k=0$. Тогда

$$a_0=a_1=\ldots=a_{k-1}=1,\ a_k=0.$$

Если какой-нибудь коэффициент b_m, где $1\le m<k$, равен 1, то сразу видим, что коэффициент при x^m больше 1: член x^m произведения можно получить, умножая $a_0\cdot b_mx^m$, а также $a_m\cdot b_0x^m$. Значит, $b_m=0$ при $1\le m<k$. Теперь ясно, что $b_k=1$: в противном случае коэффициент при x^k был бы равен 0.

Последовательность коэффициентов a_0, a_1,... можно представлять себе как последовательность чередующихся отрезков: сначала отрезок из единиц, потом отрезок из нулей, потом снова из единиц и т.д.

Рассмотрим один из таких отрезков: $a_r=\ldots=a_{r+s-1}=1$, причем $a_{r-1}=0$, $a_{r+s}=0$. Длина s этого отрезка (длиной отрезка натурального ряда будем называть количество натуральных чисел этого отрезка: например, длина отрезка 1, 2, 3 равна 3) не может быть больше k: в противном случае член x^{r+k} произведения можно получить, умножая $a_rx^r\cdot b_kx^k$, а также $a_{r+k}x^{r+k}\cdot b_0$.

Докажем, что эта длина не может быть меньше k. Предположим противное. Рассмотрим самый левый (окаймленный нулями) отрезок из единиц $a_r,\ldots,a_{r+s-1}$, длина s которого меньше k.

Член x^{r+s} произведения $F(x)\cdot G(x)$ должен получаться при умножении какого-то члена вида a_ux^u на некоторый член b_vx^v. (Разумеется, $u+v=r+s$. Поскольку $a_{r+s}=0$, случай $v=0$ невозможен.)

Нетрудно понять, что в таком случае $a_{u-1}=0$ (в противном случае можно получить x^{r+s-1} двумя способами: $a_{u-1}x^{u-1}\cdot b_vx^v$ и $a_{r+s-1}x^{r+s-1}\cdot 1$). Значит, должен существовать отрезок из единиц $a_u,..,a_{u+k-1}$. (Длина его равна k, поскольку он расположен левее отрезка $a_r,\ldots,a_{r+s-1}$: так как $v\ge k$, то $u\le r+s-k<r$.) Далее, $a_rx^r\cdot b_kx^k=a_{r+k-v}x^{r+k-v}\cdot b_vx^v$, где величина $r+k-v$ лежит на отрезке $u,\ \ldots,\ u+k-1$.

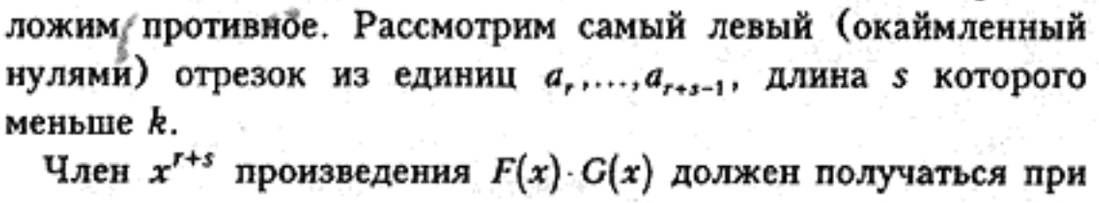

Рис. 5

Чтобы получить противоречие, осталось доказать, что $k\ne v$. Действительно, $r>u+k$ (рис.5), откуда $r+s>u+k+s$. Значит, $v=r+s-u>k+s>k$. Следовательно, все отрезки из единиц имеют одну и ту же длину k. Отсюда ясно, что многочлен F представим в виде произведения многочлена $1+x+\ldots+x^{k-1}$ на многочлен, коэффициенты которого — нули и единицы.

Итак, мы решили задачу М1598. Она позволяет легко получить полное описание всех «неотрицательных» разложений полиномов f_n:

Теорема 2. *Всякое разложение полинома $f_n(x)$ в произведение отличных от константы полиномов с неотрицательными коэффициентами можно получить из равенства типа (7) некоторой группировкой сомножителей.*

Упражнение 29. Докажите, что всякий неразложимый на множители с неотрицательными коэффициентами делитель многочлена $f_n(x)$ имеет вид $f_p(x^m)$, где p — простой делитель числа n, m — делитель числа n/p.

Для разложений с неотрицательными коэффициентами не выполняется основная теорема арифметики, например:

$$f_6(x)=(x+1)(x^4+x^2+1)=(x^2+x+1)(x^3+1),$$

причем многочлены $(x+1)$, (x^4+x^2+1), (x^2+x+1), (x^3+1) не разлагаются на множители с неотрицательными коэффициентами.

Упражнение 30. Разложение $f_n(x)$, где $n>1$, на не разложимые далее множители с неотрицательными коэффициентами единственно тогда и только тогда, когда n — степень простого числа.

Приложение

В первом разделе сказано, что неприводимость f_p следует из признака неразложимости Эйзенштейна. Объясним, что это значит. Сначала сделаем замену $x=y+1$.

Упражнение 31. Вычислите а) $\Phi_3(y+1)$; б) $\Phi_5(y+1)$; в) $\Phi_7(y+1)$.

Убедитесь, что все коэффициенты, кроме старшего, будут делиться на 3 в пункте а), на 5 — в пункте б) и на 7 — в пункте в).

При любом p имеем

$$f_p(y+1)=\frac{(y+1)^p-1}{(y+1)-1}=y^{p-1}+C_p^1y^{p-2}+\ldots+C_p^2y+C_p^1.$$

Упражнение 32. Пусть p — простое. Докажите, что все, кроме старшего, коэффициенты полученного многочлена делятся на p. (Заметьте, что свободный член $C_p^1=p$ не делится на p^2.)

Упражнение 33 (*признак Эйзенштейна*). Если все коэффициенты многочлена $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$, кроме старшего коэффициента a_n, делятся на простое число p, а свободный член a_0 не делится на p^2 (но делится, как уже было сказано, на p), то f неразложим на множители с целыми коэффициентами.

(Подробнее о признаке Эйзенштейна рассказано в «Кванте» №4 за 1994 г. в решении задачи М1419.)

* * *

Все встречавшиеся нам полиномы деления круга имели коэффициентами лишь числа ±1 и 0. В 1938 году Н.Г.Чеботарев задал вопрос, всегда ли это так.

Используя равенство

$$\Phi_{pq}=\frac{x^{pq}-1}{x^p-1}\cdot(1-x)\frac{1}{1-x^q}=\left(x^{p(q-1)}+x^{p(q-2)}+\ldots+x^p+1\right)\times$$
$$\times(1-x)\left(1+x^q+x^{2q}+x^{3q}+\ldots\right),$$

можно доказать, что все коэффициенты многочлена Φ_{pq}, где p и q — различные нечетные простые числа, равны ±1 или 0. Из