Многочлены деления круга

В. СЕНДЕРОВ, А. СПИВАК

Известны формулы сокращенного умножения

$$x^2-1=(x-1)(x+1),$$
$$x^3-1=(x-1)(x^2+x+1),$$
$$x^4-1=(x^2-1)(x^2+1)=(x-1)(x+1)(x^2+1),$$
$$x^5-1=(x-1)(x^4+x^3+x^2+x+1).$$

Раскрыв скобки, легко проверить и общую формулу

$$x^n-1=(x-1)(x^{n-1}+x^{n-2}+\ldots+x+1), \qquad (1)$$

которая изучается в школе как формула суммы геометрической прогрессии.

Мы расскажем о разложениях на множители многочленов вида x^n-1. Оказывается, они тесно связаны с задачей о делении окружности на n равных частей. Именно изучение этих многочленов позволило К.Ф.Гауссу в 1796 году решить задачу о том, при каких n правильный n-угольник может быть построен циркулем и линейкой. (Например, можно построить правильный 17-угольник и даже 65537-угольник. Подробно это объяснено в статье А.Кириллова в «Кванте» №6 за 1994 год и в книге С.Гиндикина «Рассказы о физиках и математиках» — Библиотечка «Квант», вып. 14.) Не обойтись без них и в теории Галуа, позволяющей по алгебраическому уравнению сказать, решается оно в радикалах или нет. Важнейшие объекты алгебры и арифметики — *корни из единицы, функция Эйлера* $\varphi(n)$ и функция $\tau(n)$ (количество натуральных делителей числа n) — встретятся нам на первых же шагах изучения многочленов деления круга.

* * *

На Московской олимпиаде 1997 года девятиклассники решали задачу, вошедшую в «Задачник «Кванта»:

М1598. *Пусть $1+x+x^2+\ldots+x^{n-1}=F(x)G(x)$, $n>1$, $F(x)$ и $G(x)$ — многочлены с неотрицательными коэффициентами.*

а) Докажите, что все коэффициенты этих многочленов — нули и единицы.

б) Докажите, что один из многочленов $F(x)$, $G(x)$ представим в виде $(1+x+\ldots+x^{k-1})T(x)$, где $k>1$, а коэффициенты полинома $T(x)$ — нули и единицы.

Точнее говоря, на олимпиаде было предложено решить пункт б) для многочленов F и G, коэффициенты которых суть нули и единицы. Решил задачу только один школьник, а большинство из остальных 509 участвовавших в олимпиаде девятиклассников вообще не поняли, о чем речь. Дело в том, что М1598 — лишь частичка теории разложений многочленов $f_n(x)=1+x+x^2+\ldots+x^{n-1}$ на множители. Поэтому она выглядит естественной (и красивой, и не очень трудной!) лишь для того, кто интересовался этими разложениями.

Рассказать обо всем сразу невозможно. Начнем с примеров. Они вполне доступны семикласснику, изучившему формулы сокращенного умножения (особенно если он не станет задумываться над вопросами неприводимости [1]).

Разложения с целыми коэффициентами

> Когда не знаешь, что именно делаешь, делай это особенно тщательно.
>
> *Правило для лаборантов*

Начнем копить «экспериментальный материал». Не ленитесь выписывать разложения и решать упражнения — только в этом случае вы всё поймете и правильно оцените.

$n=2$, $x^2-1=(x-1)(x+1)$. Обозначим $\Phi_1(x)=x-1$, $\Phi_2(x)=x+1$.

$n=3$, $x^3-1=(x-1)(x^2+x+1)$. Обозначим $\Phi_3(x)=x^2+x+1$. Многочлен Φ_3 нельзя разложить на множители с целыми коэффициентами.

Упражнение 1. Докажите это.

$n=4$, $x^4-1=(x-1)(x+1)(x^2+1)$. Обозначим $\Phi_4(x)=x^2+1$.

$n=5$, $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$. Обозначим $\Phi_5=x^4+x^3+x^2+x+1$. Неразложимость многочлена Φ_5 на множители с целыми коэффициентами уже не вполне очевидна. Можно рассуждать, например, так. Делителей первой степени нет, поскольку в противном случае многочлен Φ_5 имел бы рациональный корень, который заодно был бы корнем многочлена x^5-1, т.е. должен был бы равняться числу 1. Значит, надо привести к противоречию возможность разложения вида

$$x^4+x^3+x^2+x+1=(ax^2+bx+c)(dx^2+ex+f).$$

Разумеется, $ad=1$ и $cf=1$. Следовательно, коэффициенты a, c, d, f могут равняться лишь ±1.

Упражнение 2. Доведите рассуждение до конца.

$n=6$, $x^6-1=(x^3-1)(x^3+1)=(x-1)(x^2+x+1)\times(x+1)(x^2-x+1)$. Как и раньше, возник один новый неприводимый делитель $\Phi_6(x)=x^2-x+1$.

$n=7$, $x^7-1=(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$. Второй множитель, как обычно, обозначим Φ_7. Неразложимость многочлена Φ_7, как и любого многочлена $f_p(x)=x^{p-1}+\ldots+x+1$, где p — простое число, можно установить при помощи признака Эйзенштейна (формулировка и доказательство — в *Приложении*).

$n=8$, $x^8-1=(x^4-1)(x^4+1)=(x-1)(x+1)\times(x^2+1)(x^4+1)$.

$n=9$, $x^9-1=(x^3-1)(x^6+x^3+1)=(x-1)(x^2+x+1)\times(x^6+x^3+1)$.

[1] Слова *неразложимый* и *неприводимый* — синонимы, как и слова *многочлен* и *полином*.

Иллюстрация П. Чернуского

Упражнение 3. Проверьте неразложимость многочленов $\Phi_8(x) = x^4 + 1$ и $\Phi_9(x) = x^6 + x^3 + 1$.

Указание. Можно рассуждать как при $n = 5$, т.е. применять так называемый метод неопределенных коэффициентов, а можно использовать признак Эйзенштейна.

Упражнение 4. Разложите на неприводимые множители многочлены $x^n - 1$ при $n = 10, \ldots, 14$.

Заметьте, что для каждого из изученных значений n многочлен $x^n - 1$ разлагается на неприводимые множители, только один из которых ни разу не встречался в разложениях многочленов $x^m - 1$ при $m < n$. Именно этот множитель следует обозначить через Φ_n.

$\boldsymbol{n = 15}$. Применим формулу для разности кубов:

$$x^{15} - 1 = (x^5 - 1)(x^{10} + x^5 + 1) = (x - 1)(x^4 + x^3 + x^2 + x + 1)(x^{10} + x^5 + 1).$$

С другой стороны, как разность пятых степеней,

$$x^{15} - 1 = (x^3 - 1)(x^{12} + x^9 + x^6 + x^3 + 1) = (x - 1)(x^2 + x + 1)(x^{12} + x^9 + x^6 + x^3 + 1).$$

Мы получили два разложения на множители. Как «объединить» их в одно? Оказывается, $x^{10} + x^5 + 1$ делится на $x^2 + x + 1$. Поделим в столбик:

$$\begin{array}{l|l}
x^{10} + x^5 + 1 & x^2 + x + 1 \\ \hline
-\;x^{10} + x^9 + x^8 & x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\
\quad -x^9 - x^8 + x^5 + 1 & \\
\quad -\;-x^9 - x^8 - x^7 & \\
\qquad x^7 + x^5 + 1 & \\
\qquad -\;x^7 + x^6 + x^5 & \\
\qquad\quad -x^6 + 1 & \\
\qquad\quad -\;-x^6 - x^5 - x^4 & \\
\qquad\qquad x^5 + x^4 + 1 & \\
\qquad\qquad -\;x^5 + x^4 + x^3 & \\
\qquad\qquad\quad -x^3 + 1 & \\
\qquad\qquad\quad -\;-x^3 - x^2 - x & \\
\qquad\qquad\qquad x^2 + x + 1 & \\
\qquad\qquad\qquad -\;x^2 + x + 1 & \\
\qquad\qquad\qquad\qquad 0 &
\end{array}$$

и получим

$$x^{15} - 1 = (x - 1)(x^2 + x + 1) \times (x^4 + x^3 + x^2 + x + 1)(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1).$$

Замечание. Неразложимость последнего множителя не очевидна. Она доказана в *Приложении*. Там же показано, почему неприводимы полиномы Φ_{20} и Φ_{60}, которые вскоре потребуются нам. Но при первом чтении лучше об этом не задумываться.

Общий закон вполне очевиден из таблицы, в которой под каждым из исследованных значений n выписано, на сколько неразложимых множителей можно разложить многочлен $x^n - 1$. Множителей оказывается в точности столько, сколько делителей у числа n.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4

Проверим этот закон для $\boldsymbol{n = 60}$. Число 60 имеет 12 делителей. Значит, мы должны разложить $x^{60} - 1$ на 12 множителей с целыми коэффициентами. Начнем:

$$x^{60} - 1 = (x^{30} - 1)(x^{30} + 1) = (x^{15} - 1)(x^{15} + 1)(x^{10} + 1)(x^{20} - x^{10} + 1).$$

Упражнение 5. Завершите это разложение, представив $x^{60} - 1$ в виде произведения 12 многочленов с целыми коэффициентами: Φ_1, Φ_2, Φ_3, Φ_4, Φ_5, Φ_6, Φ_{10}, Φ_{12}, Φ_{15}, Φ_{20}, Φ_{30}, Φ_{60}.

В учебниках арифметики и алгебры доказывается, что всякий многочлен с целыми коэффициентами единственным с точностью до порядка сомножителей образом разлагается в произведение неприводимых многочленов с целыми коэффициентами. (Ситуация здесь такая же, как и для чисел: как известно, натуральные числа единственным с точностью до порядка сомножителей образом разлагаются в произведение простых чисел.) Для многочлена $x^n - 1$ разложение на неприводимые множители таково:

$$x^n - 1 = \prod_{n \vdots k} \Phi_k(x), \tag{2}$$

где произведение берется по всем делителям k числа n (знак $\vdots$ читается «делится нацело»). Доказательство, к сожалению, далеко выходит за рамки школьной программы.

Но все-таки в следующем разделе мы объясним, почему степень многочлена Φ_n деления круга равна $\varphi(n)$, где $\varphi(n)$ — *функция Эйлера*. (Функция Эйлера, по определению, — это количество натуральных чисел, не превосходящих n и взаимно простых с числом n.)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Покажем, как можно использовать формулу (2) для нахождения Φ_n. Например, чтобы посчитать Φ_{81}, выпишем два разложения:

$$x^{81} - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x)\Phi_{27}(x)\Phi_{81}(x),$$

$$x^{27} - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x)\Phi_{27}(x).$$

Поделив одно на другое, получим

$$\Phi_{81}(x) = (x^{81} - 1)/(x^{27} - 1) = x^{54} + x^{27} + 1.$$

Таким же образом доказывается общая формула $\Phi_{p^\alpha}(x) = (x^{p^\alpha} - 1)/(x^{p^{\alpha-1}} - 1)$, где p — простое число, α — натуральное.

Упражнение 6. а) Докажите равенство $\Phi_{pq}(x) = ((x^{pq} - 1)(x - 1))/((x^p - 1)(x^q - 1))$, где p, q — различные простые числа.

б) Выведите аналогичную формулу для Φ_{pqr}, где p, q, r — различные простые числа.

Упражнение 7. а) Выпишите $\Phi_{2p}(x)$, где $p > 2$ — простое число.

б)* Докажите равенство $\Phi_{2n}(x) = \Phi_n(-x)$ при любом нечетном $n > 1$.

Упражнение 8. Докажите, что если p — нечетное простое число, то $\Phi_{4p}(x) = f_p(-x^2)$.

Упражнение 9. Разложите на множители а) $x^4 + x^2 + 1$; б) $f_p(x^2) = x^{2p-2} + x^{2p-4} + \ldots + x^2 + 1$, где p — простое число.

Разложения с комплексными коэффициентами

...Всякое объяснение неизвестно откуда начинать, оно же тянется от дальних-дальних азов. Вот сейчас из-под лавки вылезет пещерный человек и попросит объяснить ему за пять минут, как электричеством ходят поезда. Ну как ему объяснить? Сперва вообще пойди научись грамоте. Потом — арифметике, алгебре, черчению, электротехнике... Чему там еще?

— Ну, не знаю... магнетизму...

— Вот, и ты не знаешь; а на последнем курсе! А потом, мол, приходи, через пятнадцать лет, я тебе все за пять минут и объясню, да ты и сам уже будешь знать.

А.И.Солженицын. «В круге первом»

Чтобы понять, как устроены многочлены Φ_n и почему их степень есть функция Эйлера, потребуется, как это ни странно для новичка, разлагать $x^n - 1$ на множители с комплексными коэффициентами.

Тем, кто не знаком с комплексными числами, достаточно пока знать, что операции над ними выполняются по обычным правилам алгебры, к которым добавлено только одно дополнительное правило: $i^2 = -1$. (Подробности — в статье Ю.Соловьева «Комплексные числа» в Приложении к журналу «Квант» №2 за 1994 год.) Комплексное число $a + bi$, где a и b — «обычные» (т.е. более привычные) вещественные числа, изображается точкой (a,b) координатной плоскости (рис. 1).

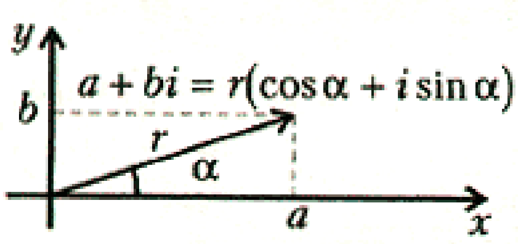


Рис. 1

Приведем несколько примеров.

$n = 3$. Уравнение $x^3 - 1 = 0$ имеет корень $x = 1$ и еще два комплексных корня, которые легко найти, решив по обычной формуле квадратное уравнение $x^2 + x + 1 = 0$:

$$x = \frac{-1 \pm \sqrt{1^2 - 4\cdot 1}}{2} = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm i\sqrt{3}}{2}.$$

Итак,

$$x^3 - 1 = (x-1)\left(x + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\left(x + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right).$$

Числа 1, $-\frac{1}{2} + \frac{i\sqrt{3}}{2}$, $-\frac{1}{2} - \frac{i\sqrt{3}}{2}$ — вершины правильного треугольника (рис. 2,*а*).

$n = 4$, $x^4 - 1 = (x-1)(x+1)(x+i)(x-i)$. Числа 1, i, -1, $-i$ — вершины квадрата (рис. 2,*б*).

Отложим на время случай $n = 5$ и разберем более простой (ибо само число составное) случай

$n = 6$. Очевидно, $x^6 - 1 = (x^3-1)(x^3+1) = (x-1) \times (x^2+x+1)(x+1)(x^2-x+1)$, так что

$$x^6 - 1 = (x-1)\left(x + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\left(x + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right) \times$$
$$\times (x+1)\left(x - \frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\left(x - \frac{1}{2} - \frac{i\sqrt{3}}{2}\right).$$

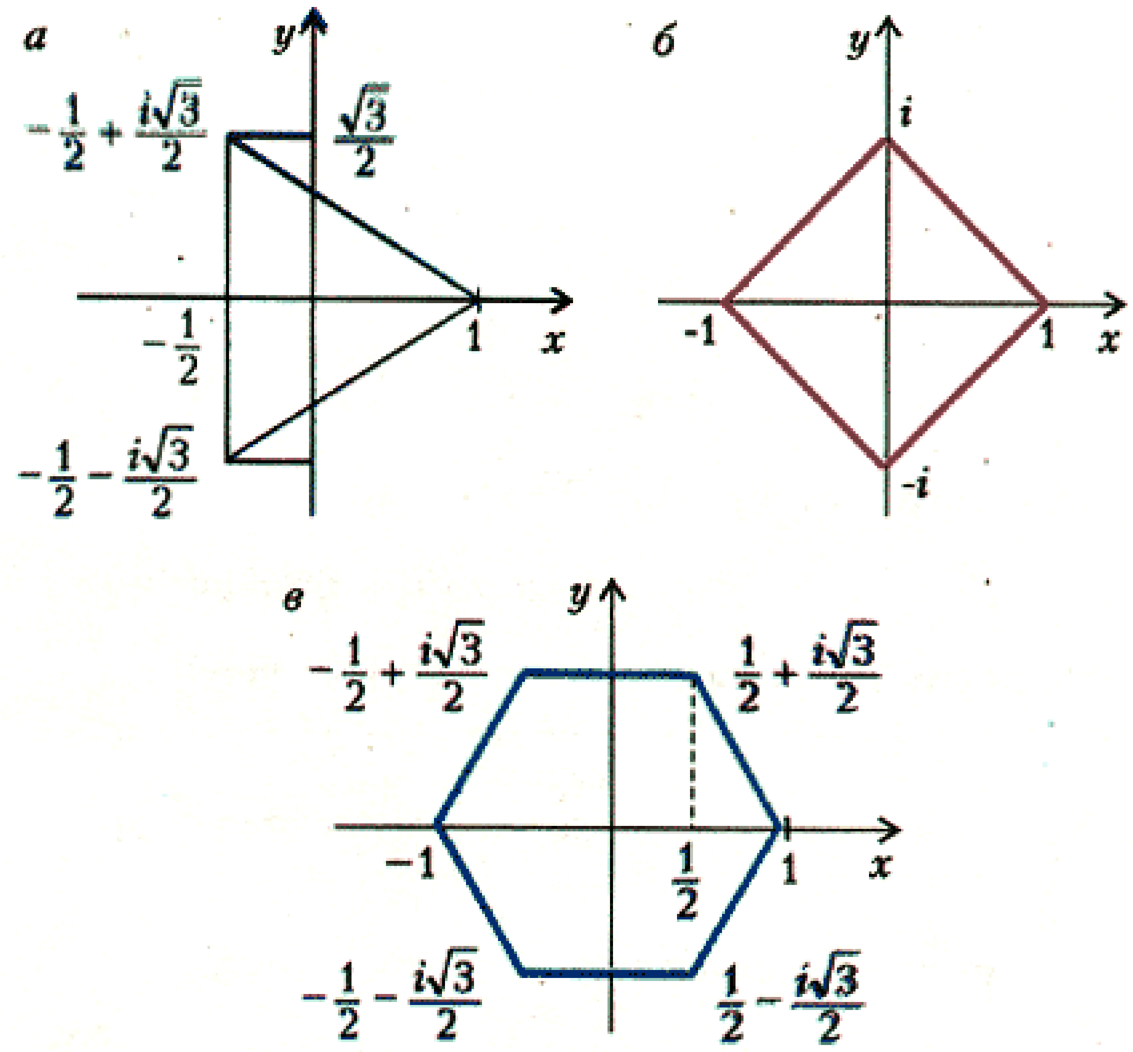


Рис. 2

Числа 1, $\frac{1}{2} + \frac{i\sqrt{3}}{2}$, $-\frac{1}{2} + \frac{i\sqrt{3}}{2}$, -1, $-\frac{1}{2} - \frac{i\sqrt{3}}{2}$, $\frac{1}{2} - \frac{i\sqrt{3}}{2}$ — вершины правильного шестиугольника (рис. 2,*в*). Это, как мы установили, корни шестой степени из единицы.

Теперь рассмотрим случай $n = 5$. Чтобы решить уравнение

$$x^4 + x^3 + x^2 + x + 1 = 0,$$

разделим на x^2 и сгруппируем:

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0,$$

$$x^2 + \frac{1}{x^2} + x + \frac{1}{x} + 1 = 0,$$

$$\left(x + \frac{1}{x}\right)^2 - 2 + \left(x + \frac{1}{x}\right) + 1 = 0.$$

Сделав замену $x + \frac{1}{x} = y$, получим квадратное уравнение $y^2 + y - 1 = 0$, откуда $y = \frac{-1 \pm \sqrt{5}}{2}$. Осталось решить уравнения $x + \frac{1}{x} = \frac{-1 \pm \sqrt{5}}{2}$. Это легко сделать, но получаются громоздкие ответы. И по ним не очевидно, что полученные корни (вместе с числом 1) делят единичную окружность на 5 равных частей.

Оказывается, гораздо проще воспользоваться тригонометрической формой записи комплексных чисел: точку (a,b) (отличную от начала координат) представим в виде

$$a + bi = r\cos\alpha + ir\sin\alpha, \qquad (3)$$

где $r = \sqrt{a^2 + b^2}$ — расстояние от начала координат до точки (a,b) (так называемый *модуль* числа $a + bi$), а угол α (*аргумент* числа $a + bi$) — угол между положительным направлением оси абсцисс и лучом, выходящим из начала координат и проходящим через точку (a,b) (углы, как обычно, отсчитываем против часовой стрелки). Возможность представления (3) вытекает из определений синуса и косинуса.

Интереснейшее свойство комплексных чисел — то, что закон умножения можно просто записать не только в алгебраической форме:

$$(a + bi)(c + di) = ac + adi + bic + bidi =$$
$$= (ac - bd) + i(ad + bc),$$

но и в тригонометрической:

$$r(\cos\alpha + i\sin\alpha)\cdot R(\cos\beta + i\sin\beta) =$$
$$= rR(\cos(\alpha+\beta) + i\sin(\alpha+\beta)),$$

так что модуль произведения комплексных чисел равен произведению их модулей, а аргумент равен сумме аргументов (как водится, с точностью до 360°).

Теперь, пользуясь тригонометрической формой, легко записать операцию возведения в степень:

$$\left(r\cdot(\cos\alpha + i\sin\alpha)\right)^n = r^n\cdot(\cos n\alpha + i\sin n\alpha).$$

Последняя формула называется *формулой Муавра*. Из нее следует, что все решения уравнения $x^n = 1$ имеют модуль, равный 1, а их аргументы удовлетворяют условию $n\alpha = 360°k$, где k — целое число. Следовательно, корни степени n из 1 — это в точности числа вида $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$, где $k = 1, \ldots, n$. Они являются вершинами правильного n-угольника, вписанного в окружность единичного радиуса.

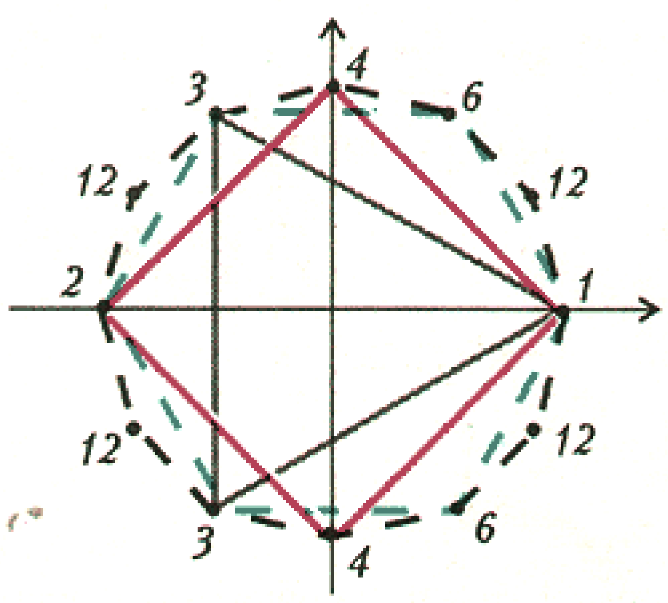


Рис. 3

Заметим, что корни n-й степени из единицы, т.е. решения уравнения $x^n = 1$, заодно являются и корнями mn-й степени: $x^{mn} = 1$. Например, всякий корень 3-й степени является и корнем 12-й степени. Поэтому естественно ввести следующее определение: корень называется *первообразным степени n*, если он не удовлетворяет никакому уравнению $x^k = 1$ при натуральном $k < n$. (Например, 1 — единственный первообразный корень степени 1, −1 — первообразный корень степени 2, $-\frac{1}{2} \pm \frac{i\sqrt{3}}{2}$ — первообразные корни степени 3.)

Упражнение 10. а) Для правильного 12-угольника, вписанного в единичную окружность, на рисунке 3 отмечено, первообразными корнями какой степени являются его вершины. На заставке (с.10) буквы расположены в вершинах 24-угольника. Определите, какие буквы первообразным корням какой степени соответствуют.

б) Нарисуйте часы и расставьте около 60 минутных делений числа, показывающие, первообразными корнями какой степени являются соответствующие корни 60-й степени из 1.

в) Как по натуральным числам k и n узнать, корнем какой наименьшей степени является число $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$?

Внимательному читателю уже ясно, что корни многочлена Φ_n — это в точности первообразные корни n-й степени из 1. Другими словами, корни многочлена Φ_n — это числа вида $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$, где k — взаимно простое с n число, $1 \le k \le n$. Таким образом, степень многочлена Φ_n действительно равна $\varphi(n)$.

Упражнение 11. Какой остаток дает x^{100} при делении на $x^2 + x + 1$?

Упражнение 12. а) Разложите на множители с целыми коэффициентами многочлен $x^5 + x + 1$.

б) Делится ли $x^{11} + x^7 + 1$ на $x^2 + x + 1$?

в) Докажите, что если натуральные числа m и n не делятся на 3 и их разность $m - n$ не делится на 3, то многочлен $x^m + x^n + 1$ делится на $x^2 + x + 1$.

г) При каких n число

$$1\underbrace{0\ldots0}_{n}1\underbrace{0\ldots0}_{n}1$$

делится на 37?

Подсказка. $37 \cdot 3 = 111 = 10^2 + 10 + 1$.

Упражнение 13. а) Убедитесь, что если модуль числа x равен 1, а аргумент равен α, т.е. если $x = \cos\alpha + i\sin\alpha$, то $x + \frac{1}{x} = 2\cos\alpha$.

б) Верно ли, что если $x + \frac{1}{x} = 2\cos\alpha$, то модуль числа x равен 1, а аргумент равен α?

Упражнение 14. Вычислите а) $\cos 72°$; б) $\sin 72°$.

Упражнение 15. Докажите, что если $x + \frac{1}{x} = 2\cos\alpha$, то $x^n + \frac{1}{x^n} = 2\cos n\alpha$.

Упражнение 16*. При каких n многочлен $x^{2n} + x^n + 1$ делится на а) $x^2 + x + 1$; б) $x^2 - x + 1$; в) $x^4 - x^2 + 1$; г) $x^4 + x^2 + 1$?

Упражнение 17*. При каких n многочлен $x^{2n} - x^n + 1$ делится на а) $x^2 + x + 1$; б) $x^2 - x + 1$; в) $x^4 - x^2 + 1$; г) $x^4 + x^2 + 1$?

Упражнение 18. Проверьте, что $\Phi_{60}(x) = \Phi_{15}(-x^2)$. Вообще, $\Phi_{4n}(x) = \Phi_n(-x^2)$ при нечетных $n > 1$.

Упражнение 19*. Докажите формулы а) $\Phi_{p^\alpha}(x) = \Phi_p\left(x^{p^{\alpha-1}}\right)$, где p — простое число, α — натуральное число;

б) $\Phi_{p^\alpha q^\beta r^\gamma}(x) = \Phi_{pqr}\left(x^{p^{\alpha-1}q^{\beta-1}r^{\gamma-1}}\right)$, где α, β, γ — натуральные числа, p, q, r — различные простые числа.

Разложения с вещественными коэффициентами

Имея формулу

$$x^n - 1 = \prod_{k=1}^{n}\left(x - \cos\frac{2\pi k}{n} - i\sin\frac{2\pi k}{n}\right),$$

легко разложить $x^n - 1$ на множители с вещественными коэффициентами.

Ясно, что любой множитель-многочлен с вещественными коэффициентами, имеющий некоторый комплексный корень $a + bi$, имеет и сопряженный корень $a - bi$. Значит, мы должны «объединить» сопряженные множители.

При нечетном n на вещественной оси лежит лишь один корень n-й степени из единицы (а именно, само число

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 $P(x) = x^n \cdot P\left(\dfrac{1}{x}\right)$.

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.

Доказательство леммы 2. Предположив противное, обозначим через i наименьший из таких номеров, что хотя бы одно из чисел a_i, b_i отлично от 0 и 1. Пусть, для определенности, a_i не равно ни 0, ни 1. По лемме 1 имеем $a_{m-i} = a_i$. Значит, $a_{m-i} > 0$.

Если $b_i > 0$, то коэффициент при x^m после раскрытия скобок произведения $g(x)h(x)$ получается больше 1 (сообразите, почему!). Если же $b_i = 0$, то первое слагаемое выражения $a_ib_0 + a_{i-1}b_1 + \ldots + a_0b_i = 1$ не равно ни 0, ни 1, а каждое из остальных слагаемых равно 0 или 1.

Третий способ

Этот способ не использует комплексных чисел. Оказывается, верны следующие леммы.

Лемма 1'. *Если возвратный многочлен $f(x)$ разложен в произведение многочленов $g(x)$ и $h(x)$ с неотрицательными коэффициентами, причем все коэффициенты многочлена f не превосходят величины его свободного члена, то полиномы g и h — тоже возвратные. (Разумеется, мы считаем, что многочлен f отличен от тождественного нуля.)*

Лемма 2'. *Если возвратный многочлен $f(x)$, все коэффициенты которого суть 0 и 1, разложен в произведение полиномов $g(x)$ и $h(x)$ с неотрицательными коэффициентами, то и все коэффициенты многочленов $g(x)$, $h(x)$ равны 0 или 1.*

Они сильнее, чем леммы 1 и 2, поэтому вывод теоремы 1 из лемм остается прежним. Доказательство леммы 2' по сути не отличается от доказательства леммы 2, поэтому нам осталось только доказать лемму 1'.

Как обычно, можно считать, что $a_0 = b_0 = b_n = a_m = 1$. Пусть хотя бы один из полиномов g, h не является возвратным. Рассмотрим *наименьшее* i, для которого хотя бы одно из равенств $a_i = a_{m-i}$, $b_i = b_{n-i}$ не выполнено.

Коэффициент при x^i произведения вычисляется по формуле

$$a_0b_i + a_1b_{i-1} + \ldots + a_ib_0 . \qquad (5)$$

Он должен равняться коэффициенту при x^{m+n-i}, т.е. сумме

$$a_{m-i}b_n + \ldots + a_mb_{n-i} . \qquad (6)$$

Поскольку при всех $j < i$ выполнены равенства $a_j = a_{m-j}$, $b_j = b_{n-j}$, в суммах (5) и (6) все слагаемые, кроме крайних, совпадают. Значит,

$$a_0b_i + a_ib_0 = a_{m-i}b_n + a_mb_{n-i} ,$$

т.е. $b_i + a_i = a_{m-i} + b_{n-i}$.

Осталось решить два упражнения.

Упражнение 23. Докажите, что $b_ia_{m-i} = 0$ и $a_ib_{n-i} = 0$.

Указание. Рассмотрите, соответственно, коэффициенты при x^m и x^n.

Упражнение 24. Завершите доказательство леммы 1'.

Разложения f_n при составном n

Перейдем теперь к описанию разложений с неотрицательными коэффициентами полиномов $f_n(x)$, где n — *произвольное* натуральное число.

Упражнение 25. Завершите разложения

а) $f_4(x) = x^3 + x^2 + x + 1 = (x+1)(\ldots)$;

б) $f_6(x) = x^5 + x^4 + x^3 + x^2 + x + 1 = \left(x^2 + x + 1\right)(\ldots)$;

в) $f_{15}(x) = \left(x^2 + x + 1\right)(\ldots)$.

Упражнение 26. Докажите, что при любом составном $n = ab$ полином $f_n(x)$ представим в виде $f_{ab}(x) = f_a(x)f_b\left(x^a\right)$.

Упражнение 27. Если $n = abc$ — некоторое разложение в произведение натуральных чисел, то

$$f_n(x) = f_a(x)f_b\left(x^a\right)f_c\left(x^{ab}\right). \qquad (7)$$

Аналогичное разложение можно выписать, если число n разложено не на два или три, а на большее число множителей. Более того, никаких других разложений полиномов $f_n(x)$ на множители с неотрицательными коэффициентами, по существу, не бывает (см. теорему 2). Ключ к доказательству этого — задача М1598. Мы сейчас изложим ее решение.

а) При доказательстве лемм 1 и 2 простота p не использовалась. Поэтому можно считать, что коэффициенты a_i и b_i равны только 0 или 1.

б) Теперь — сюрприз. М1598,б) — это геометрическая задача. Понять ее условие и решение проще всего, если рисовать отрезки и смотреть, что происходит при сдвигах.

В самом деле, давайте изображать многочлен $x^\alpha + x^\beta + \ldots$ системой отрезков $[\alpha, \alpha+1] \cup [\beta, \beta+1] \cup \ldots$ Умножение на x^t будем представлять как параллельный перенос на t единиц. Тогда, например, разложению

$$1 + x + x^2 + \ldots + x^{11} = \left(1 + x + x^6 + x^7\right)\left(1 + x^2 + x^4\right)$$

будет соответствовать система отрезков $[0,2] \cup [6,8]$, сдвиги которой на 0, 2 и 4 единицы покрывают в точности отрезок $[0,12]$ (рис.4). (Один множитель задает систему отрезков, другой — величины сдвигов. Не удивляйтесь их неравноправию. Скоро все станет ясно.)

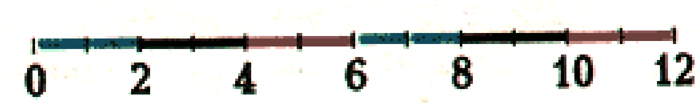


Рис. 4

Итак, для геометра задача М1598 может быть сформулирована следующим образом:

На отрезке задана некоторая система S не пересекающихся друг с другом отрезочков. Докажите, что если отрезок можно составить из параллельных сдвигов системы S, то длины всех отрезочков системы S одинаковы. (Отрезочки не имеют никаких общих точек, в частности, не имеют общих концов. При параллельных сдвигах все точки большого отрезка должны быть покрыты; отрезочки не должны накладываться друг на друга внутренними точками, а должны «стыковаться» в концах.)

Решение очень простое. Можно считать, что все сдвиги выполняются только направо. (Если есть и сдвиги налево, то возьмем наибольший из них. Вместо системы S можно рассматривать этот ее сдвиг.)

Рассмотрим самый левый отрезочек. Очевидно, среди сдвигов должен быть сдвиг на длину k этого отрезочка. Из этого следует, что длины всех отрезочков системы не превосходят k (иначе длинный отрезочек накладывался бы на себя при сдвиге).

Если же среди отрезочков системы найдется отрезочек, длина которого меньше k, рассмотрим самый левый из всех таких отрезочков. Противоречие очевидно.

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 $a_0 \cdot b_m x^m$, а также $a_m \cdot b_0 x^m$. 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, $a_1, \ldots$ 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 $a_u, \ldots, a_{u+k-1}$. (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 $u, \ldots, u + k - 1$.

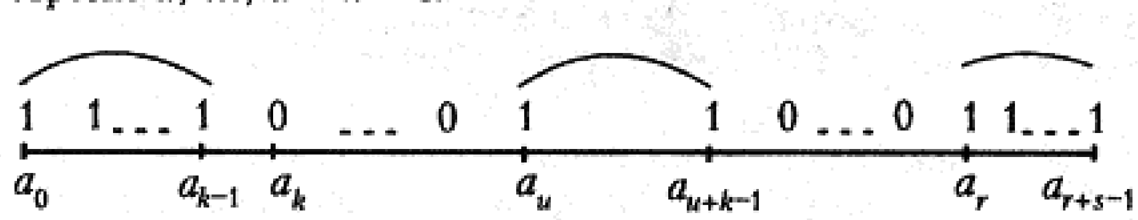


Рис. 5

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

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

можно доказать, что все коэффициенты многочлена Φ_{pq}, где p и q — различные нечетные простые числа, равны ± 1 или 0. Из этого с помощью упражнений 19 и 7 легко следует, что при $n < 105$ все коэффициенты полиномов Φ_n равны 0 или ± 1 (поскольку $105 = 3 \cdot 5 \cdot 7$, любое $n < 105$ имеет не более двух нечетных простых делителей).

В 1941 году В.Иванов доказал эти факты и вычислил:

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^{9} - x^{8} - 2x^{7} - x^{6} - x^{5} + x^{2} + x + 1.$$

Среди коэффициентов этого многочлена деления круга есть -2.

Упражнение 34. При каких n в разложении многочлена $f_n(x) = x^{n-1} + \ldots + x + 1$ на неприводимые множители все коэффициенты всех многочленов-сомножителей неотрицательны?

Подсказка. Если $n = p^\alpha$, то все коэффициенты многочлена $\Phi_{p^\alpha} = f_p\left(x^{p^{\alpha-1}}\right)$ неотрицательны. Если же n делится на различные простые числа p и q, то $x^n - 1$ делится на Φ_{pq}, среди коэффициентов которого есть отрицательные (например, коэффициент при первой степени x полинома Φ_{pq} равен, как легко посчитать, -1).

Упражнение 35. При каких натуральных a и b многочлен $f_a\left(x^b\right)$ неприводим?

* * *

Мы говорили, что многочлены разлагаются на множители «так же, как числа». Ниже сформулированы некоторые факты, придающие этим словам точный математический смысл.

• Многочлены можно делить с остатком: для любых двух многочленов $f(x)$ и $g(x) \neq 0$ с рациональными коэффициентами существуют (и определены единственным образом!) такие многочлены $q(x)$ и $r(x)$, что

$$f(x) = q(x)g(x) + r(x), \qquad (8)$$

где степень многочлена r меньше степени многочлена g или $r = 0$. (Равенство (8) можно записать и в виде $\dfrac{f(x)}{g(x)} = g(x) + \dfrac{r(x)}{g(x)}$.)

• Для любых двух ненулевых многочленов $A(x)$ и $B(x)$ многочлен (отличный от нуля) минимальной степени, представимый в виде

$$A(x) \cdot K(x) + B(x) \cdot L(x),$$

где K и L — многочлены, является наибольшим общим делителем многочленов A и B.

Упражнение 36. Любой многочлен, имеющий общий корень с неприводимым полиномом, делится на этот полином.

• *(Основная теорема арифметики для многочленов)* Любой многочлен с рациональными коэффициентами единственным способом разлагается в произведение неразложимых многочленов с рациональными коэффициентами.

• *(Лемма Гаусса)* Если многочлен с целыми коэффициентами разложим на множители с рациональными коэффициентами, то он разложим и на множители с целыми коэффициентами.

Упражнение 37. а) Если многочлен с целыми коэффициентами имеет рациональный корень x и если старший коэффициент этого многочлена равен 1, то x — целое число.

б) Если многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ с целыми коэффициентами имеет рациональный корень p/q, где дробь p/q записана в несократимом виде (т.е. НОД$(p,q)=1$), то числитель p — делитель свободного члена a_0, а знаменатель q — делитель старшего коэффициента a_n.

* * *

Мы пользовались неразложимостью некоторых многочленов. Объясним напоследок, как можно «кустарно», т.е. не используя общую теорию, доказать неразложимость Φ_{15}, Φ_{20} и Φ_{60}.

Упражнение 38. Если $f_n(x)$ разложен в произведение многочленов с вещественными коэффициентами, то каждый из множителей-многочленов возрастает на луче $[1, +\infty)$.

Указание. Все сомножители $x^2 - 2x\cos\varphi + 1$ разложения (4) возрастают при $x \geq 1$.

Упражнение 39. Докажите непосредственно, т.е. не пользуясь формулой (2), неразложимость многочлена $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ на множители с целыми коэффициентами.

Из неразложимости Φ_{15} сразу следует неразложимость многочлена $\Phi_{30}(x) = \Phi_{15}(-x)$. Поскольку $\Phi_{20}(x) = \Phi_{10}(x^2)$ и $\Phi_{60}(x) = \Phi_{30}(x^2)$, то для доказательства неприводимости Φ_{20} и Φ_{60} можно использовать неприводимость Φ_{10} и Φ_{30}. К сожалению, мы не можем попросту сказать, что если многочлен $f(x)$ неприводим, то и $f(x^2)$ неприводим (контрпримеры: $x^2 - 1 = (x-1)(x+1)$, $x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1)$, $x^6 - 4 = (x^3 - 2)(x^3 + 2)$).

Упражнение 40. Докажите, что если $f(x)$ неприводим, то $f(x^2)$ или неприводим, или разлагается на неприводимые множители следующим образом: $f(x^2) = \pm P(x)P(-x)$ (выясните, в каком случае какой знак).

Упражнение 41. Докажите непосредственно, т.е. не пользуясь формулой (2), неразложимость многочленов а) $\Phi_{20}(x) = (x^{10} + 1)/(x^2 + 1)$; б) $\Phi_{60}(x) = (x^{20} - x^{10} + 1)/(x^4 - x^2 + 1)$ на множители с целыми коэффициентами.

НАМ ПИШУТ

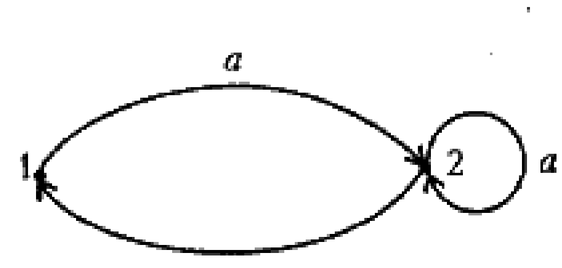
ГЕНЕРАТОР СЛОВ И ЧИСЛА ФИБОНАЧЧИ

В 1992 году я предложил на лингвистической олимпиаде следующую задачу:

«С помощью схемы, изображенной на рисунке, строятся слова некоторого искусственного языка. Слова получаются движением из точки 1 в направлении стрелок и записью букв, написанных около проходимых стрелок. Слово может заканчиваться как в точке 1, так и в точке 2.

Таким образом может быть получено лишь одно слово длиной 1 — «*a*», два слова длиной 2 — «*aa*» и «*ab*», три слова длиной 3, пять слов длиной 4 и т.д.

Обозначим через $N(n)$ число слов длиной n. Докажите, что $N(n)$ делится на 5 тогда и только тогда, когда $n + 1$ делится на 5».



Решение этой задачи основано на свойстве чисел $N(n)$: $N(0) = N(1) = 1$, $N(n+1) = N(n) + N(n-1)$. Но именно этими условиями определяется последовательность Фибоначчи! Значит, числа $N(n)$ являются n-ми числами ряда Фибоначчи.

Таким образом, получен еще один механизм возникновения чисел ряда Фибоначчи.

А.Серебряный