Доклады Академии Наук СССР
1953. Том XCIII, № 5

МАТЕМАТИКА

М. В. ЯКОВКИН

ОБ ОДНОМ МЕТОДЕ ОТЫСКАНИЯ НЕПРИВОДИМЫХ МНОЖИТЕЛЕЙ

(Представлено академиком И. М. Виноградовым 8 X 1953)

В настоящей статье излагается новый метод отыскания неприводимых множителей полиномов в поле рациональных чисел. Главное из преимуществ излагаемого нами метода по сравнению хотя бы с самым распространенным в математической литературе ([1-3]) методом Кронекера состоит в том, что если методом Кронекера ([1], стр. 82) по $[n/2]+1$ парам значений аргумента и функции n-й степени находятся непосредственно лишь делители степени не выше $[n/2]$, то методом, предлагаемым нами, лишь по о д н о й паре значений аргумента и функции находятся делители этой функции л ю б о й степени.

Для того чтобы методом Кронекера найти непосредственно делители любой степени, понадобилось бы ([3], стр. 19) выбрать уже не $[n/2]+1$, а $n+1$ пар значений функции и аргумента. Кроме того в нашем методе совершенно исключается построение испытуемых функциональных делителей при помощи интерполяционных формул, а также и их проверка путем непосредственного умножения (или деления).

Прежде всего приведем одно замечание и теорему, на которых основано построение излагаемого метода.

З а м е ч а н и е. Пусть

$$f(x)=\sum_{k=0}^{n} a_k x^{n-k}, \quad \varphi(x)=\sum_{k=0}^{p} b_k x^{p-k}, \quad \psi(x)=\sum_{k=0}^{q} c_k x^{q-k} \tag{1}$$

целочисленные полиномы с неотрицательными коэффициентами и если $f(x)=\varphi(x)\psi(x)$, то наибольшая из абсолютных величин коэффициентов функции $f(x)$ не меньше абсолютных величин всех коэффициентов $\varphi(x)$ и $\psi(x)$.

Т е о р е м а. *Для справедливости тождества*

$$f(x)=\varphi(x)\psi(x) \tag{2}$$

необходима и достаточна справедливость равенств

$$f(1)=\varphi(1)\psi(1), \quad f(t)=\varphi(t)\psi(t) \tag{3}$$

хотя бы при одном целом значении t, превышающем все коэффициенты функций (1).

Краткое доказательство этой теоремы дано в моей статье ([5]).

По поводу этой теоремы уместно также отметить, что она дает весьма простые необходимые и достаточные условия приводимости или неприводимости многочленов в поле рациональных чисел.

В частном случае, когда t равно некоторой целой положительной степени 10, использование этой теоремы значительно упрощается, так как в этом случае мы получаем уже готовые числовые разложения по степеням 10 благодаря обиходной десятичной системе счисления.

Хотя все рассуждения метода будут справедливы для функций со знакопостоянными или со знакочередующимися коэффициентами, мы для простоты будем полагать рассматриваемые целочисленные полиномы и их сомножители лишь с неотрицательными коэффициентами.

Итак, допустим, что функции (1) удовлетворяют тождеству (3). Положим далее, что каждый из коэффициентов $f(x)$ состоит не более чем из m цифр; тогда, согласно сделанному выше замечанию, коэффициенты $\varphi(x)$ и $\psi(x)$ состоят также не более чем из m цифр.

Положив в тождестве (2) $x = 10^m$, мы получим слева число, составленное припиской друг к другу всех коэффициентов данной функции, взятых по m цифр каждый, а справа разложение этого числа на два сомножителя и притом такое, что если в каждом из сомножителей отсчитывать справа налево по m цифр, то мы получим коэффициенты сомножителей $\varphi(x)$ и $\psi(x)$ рассматриваемой функции.

Обратно, если мы найдем указанное числовое разложение, то мы можем написать разложение многочлена, взяв за коэффициенты многочленов-сомножителей числа из граней по m цифр справа налево найденного числового разложения.

Выбор такого числового разложения существенно упрощается благодаря простым условиям, необходимым и достаточным для приводимости многочленов, вытекающим из приведенной выше теоремы.

При этом удобно использовать иногда также и другие весьма простые условия, например $a_0 = b_0c_0$ и $a_n = b_pc_q$, являющиеся уже только необходимыми, но не достаточными.

Здесь важно заметить также, что комбинирование простых делителей числа $f(t)$ в попарные сомножители и проверка для этих комбинаций необходимого условия $a_0 = b_0c_0$ существенно упрощается, если предварительно привести эти простые делители к наименьшим вычетам по модулю t.

Приведем пример, рассмотренный Н. Г. Чеботаревым ([3], стр. 67). Требуется разложить на множители функцию

$$f(x) = x^5 - 5x^4 + 13x^3 - 22x^2 + 27x - 20.$$

Попытка найти разложение этой функции при помощи метода Кронекера привела Н. Г. Чеботарева к 2654208 гипотезам, каждая из которых состоит в построении соответствующей функции при помощи интерполяционной формулы Лагранжа, а затем в проверке делимости данной функции на найденную.

Применим к этой функции только что изложенный метод. Для простоты заменой $x = -y$ преобразуем эту функцию со знакопеременными коэффициентами в функцию со знакопостоянными коэффициентами

$$f(-y) = -(y^5 + 5y^4 + 13y^3 + 22y^2 + 27y + 20).$$

Здесь $m = 2$, поэтому, полагая $y = 10^m = 10^2$, мы получим число -10513222720, составленное припиской друг к другу коэффициентов данной функции.

В тех случаях, когда удается найти простые делители численного значения заданной функции, комбинированием этих простых делителей можно найти искомое разложение. В тех же случаях, когда не удается находить все простые делители числового значения заданной функции, приходится находить другое значение этой функции при

другом значении аргумента и такое, простые делители которого возможно найти.

Для данного числа находим разложение

$$-10513222720 = 1020305 \cdot 10304,$$

удовлетворяющее необходимым и достаточным условиям приводимости функции:

$$-(20 + 27 + 22 + 13 + 05 + 01) = -(05 + 03 + 02 + 01)\cdot(04 + 03 + 01),$$
$$-88 = -11 \cdot 8.$$

Следовательно, мы вправе написать соответствующее функциональное разложение

$$(-y^3 - 2y^2 - 3y - 5)(y^2 + 3y + 4).$$

Заменив, обратно, $-y$ через x, мы получим

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

Мы изложили метод, полагая, для простоты, t равным некоторой степени 10, но ясно, что этот метод остается в силе при любом значении t, превышающем коэффициенты заданной функции $f(x)$ (а не голько при $t = 10^m$).

В нашем примере можно было t положить равным не 100, а 28, 29, 30 и т. д.

Для того чтобы применить метод к целочисленным полиномам с произвольными (в смысле знаков) коэффициентами согласно теореме 1 работы ([4]), достаточно воспользоваться одним линейным преобразованием.

Однако заметим, что в общем случае можно обойтись и без линейного преобразования, но изложение этого второго метода уже выходит за рамки настоящей статьи.

Поступило
27 V 1953

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Ван-дер-Варден, Современная алгебра, ч. 1, 1934. [2] Л. Я. Окунев, Высшая алгебра, 1937. [3] Н. Г. Чеботарев, Основы теории Галуа, ч. I, 1934. [4] М. В. Яковкин, ДАН, 28, № 9 (1940). [5] М. В. Яковкин, ДАН, 92, № 4 (1953).