УДК 519.115.1

01.00.00 Физико-математические науки

О ГИПОТЕЗЕ ВОРОНОГО

Сергеев Александр Эдуардович
к. ф.-м. н., доцент
Кубанский государственный аграрный Университет, Краснодар, Россия

Задача установления факторизации непроизводимых полиномов с целыми коэффициентами по простым модулям p давно интересуют математиков. Квадратичный и кубический законы взаимности решают эту задачу для квадратных полиномов и биномов вида x3-a. Более общие законы взаимности решают сформированную задачу для некоторых классов полиномов, например с абелевой группы Галуа, но для полиномов с неабелевой группой Галуа задача далека от полного решения. В данной работе показано как с помощью результатов Вороного Г.Ф., Хассе Х. и Штилькебергера можно находить условия которым должно удовлетворять простое число p, чтобы получать для неприводимого кубического полинома определенный тип факторизации по модулю p, Гаусс получил подобный результат для бинома x3-2. Приводятся конкретные примеры, например для полинома x3-x+1, формулируются также условия при которых квадратичное поле погружается в неабелево расширение Галуа 6-ой степени. Также приводятся условия при которых диофантово уравнение a12a22-4a22-4a13a3-27a32+18a1a2a3=D имеет решение для целых значений D

Ключевые слова: НЕПРИВОДИМЫЙ МНОГОЧЛЕН, ГРУППА ГАЛУА, ФАКТОРИЗАЦИЯ

Doi: 10.21515/1990-4665-134-075

UDC 519.115.1

Physical-Mathematical sciences

TO THE HYPOTHESIS OF VORONOI

Sergeev Alexandr Eduardovich
Cand. Phys.-Math. Sci., associate Professor
Kuban State Agrarian University, Krasnodar, Russia

The problem of establishing of the factorization of irreducible polynomials with integer coefficients on prime modules p has been long of interest to mathematicians. The quadratic and cubic reciprocity laws solve this problem for quadratic polynomials and binomials of the form x3-a . More general reciprocity laws solve the formulated problem for some classes of polynomials, for example, with Abelian Galois group, but for polynomials with non-Abelian Galois group, the problem is far from its complete solution. Our study shows how using the results of Voronov G.F., Hasse H. and Stickelberger L., one can find conditions that must satisfy prime number p. Gauss received a similar result for binomial x3-2. Specific examples are given, for instance, for the polynomial x3-x - I, also conditions arc formulated for which a quadratic field is immersed in non-Abelian Galois extension of degree 6. Also, conditions are given under which a Diophantine equation: a12a22-4a22-4a13a3-27a32+18a1a2a3=D has a solution for integer values of D

Keywords: IRREDUCIBLE POLYNOMIAL, GALOIS GROUP, FACTORIZATION

О гипотезе Вороного

Пусть $q(x)$ - неприводимый полином n-ой степени над полем рациональных чисел Q с целыми коэффициентами и дискриминантом D и p - простое число не делящее D. Одной из важных задач теории чисел является изучение факторизации полинома $q(x)$ в произведение неприводимых по модулю p полиномов над полем вычетов Z_p.

Пусть

$$q(x) \equiv \varphi_1(x)\varphi_2(x)\dots\varphi_r(x)(mod p) \quad (1)$$

где неприводимые полиномы $q_j(x), (J = 1,2\dots,r)$, имеют соответственно степени $n_1, n_2, \dots, n_r, n_1 + n_2 + \cdots n_r = n$, тогда будем считать, что по модулю p полином $q(x)$ имеет факторизованный тип $(n_1, n_2, \dots, n_r)$.

В связи с этим возникают две проблемы :

1. Описать для конкретного неприводимого полинома $q(x)$ степени n его возможные факторизационные типы по всевозможным простым модулям.
2. Для данного неприводимого полинома $q(x)$ и данного его факторизационного типа $n_1, n_2, \dots, n_r)$ описать все простые числа p для которых по модулю p реализуется данный факторизационный тип в представлении (1).

На первую проблему отвечает группа Галуа G(φ) полинома $q(x)$, рассматриваемая над полем рациональных чисел Q: если группа Галуа G(φ) представлена подстановками, т.е. G(φ) подгруппа симметрической группы S_n, то цикленные типы подстановок из группы G(φ) определяет факторизационные типы полинома (неприводимые над Q) $q(x)$ по всевозможных простым модулем.

Например, если полином $q(x)$ третий степени целыми коэффициентами имеет группу Галуа знакопеременную A_3, то его возможные цикленные типы по модулю p будут или (1,1,1), или (3), т.е. полином $q(x)$ неприводим по модулю p, причем все случаи реализуются.

Если же группа Галуа полинома третьей степени с целыми коэффициентами изоморфна симметрической группы S_3, то его возможные цикленные типы по модулю p будет или (1,1,1), или (3), или (1,2), причем

все цикленные типы реализуются при некоторых простых числах p.

В самом простом случае, когда $q(x)$ есть полином 2-ой степени, обе проблемы полностью решаются с помощью квадратичного закона взаимности. Например, полином $q(x) = x^2 + 4x + 5$ факторизуется на линейные множители по модулю p, если $p = 4k + 1$ и остается неприводимым, если p=4k+3.

В принципе вторая проблема может быть решена, если группа Галуа полинома $q(x)$ абелева, в этом случае используют теорию полей классов. В частности, если $q(x) = \varphi_n(x) - n - й$ круговой полином, то сравнительно элементарными методами доказывается следующая замечательная теорема о том, что n-й круговой полином $\varphi_n(x)$ имеющий степень φ_n, *где* φ_n – функция Эйлера, расщепляется по модулю простого числа p в произведение неприводимых полиномов по такому правилу: если t - наименьшее натуральное число для которого $p^t \equiv 1(mod n)$, то тогда $\varphi_n(x) \equiv g_1 \cdot (x) g_2(x) \dots g_r(x)(mod\, p)$, где $g_j(x), (j = 1,2,\dots,r)$ – неприводимые по модулю p полином степени t, а $r = g\frac{n}{t}$. Например, так как $\varphi_5(x) = x^4 + x^3 + x^2 + x + 1$, то для простых p вида $p = 5k + 1$ для $\varphi_5(x)$ по mod p имеем факторизационный тип (1,1,1,1); для $p = 5k + 4$ факторизационный тип (2,2); для $p = 5k + 2$ *или* $p = 5k + 3$ имеем факторизационный тип (4).

Случай неприводимого полинома третьей степени гораздо сложнее. Перед тем как его рассмотреть, сформулируем замечательную теорему Штекельберга – Вороного: пусть $q(x)$ – неприводимый над Q полином n-ой степени с целыми коэффициентами, тогда если простое число p не делит дискриминант D полинома $q(x)$, то число r - неприводимых по модулю p множителей полинома $q(x)$ удовлетворяет равенству

$$\left(\frac{D}{p}\right) = (-1)^{n-r},$$

где $\left(\frac{D}{p}\right)$ – символ Лежандра.

Таким образом, если $q(x)$ – неприводимый над Q полином 3-ей степени с целыми коэффициентами и дискриминантом D, а p-простое число не делящее D, то факторизационный тип полинома $q(x)$ по модулю p будет (1,2) только если выполняется равенство $\left(\frac{D}{p}\right) = -1$.

Это позволяет охарактеризовать такие простые числа p с помощью соответствующих арифметических прогрессий. Если при этом группа Галуа полинома $q(x)$ - циклическая, т.е. дискриминант D - квадрат целого числа, то типы факторизаций полинома $q(x)$ будет или (1,1,1), или (3).

Пример1. Рассмотрим полином $q(x) = x^3 - 2$, он неприводим над Q, его дискриминант -108=-4,27.

Имеем:

$$\left(\frac{D}{p}\right) = \left(-\frac{108}{p}\right) = \left(-\frac{1}{p}\right)\left(\frac{4}{p}\right)\left(\frac{27}{p}\right) = (-1)^{p-\frac{1}{2}}\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1, p = 3k+1 \\ -1, p = 3k+2 \end{cases}.$$

Следовательно, для простых чисел P вида p=3k+2 полиномом $x^3 - 2$ расщепляется по модулю p на линейный и неприводимый квадратный множитель. Например, при p=5 имеем

$$x^3 - 2 \equiv (x-3)(x^2+3x+4)(mod5)$$

Если простое p имеет вид 3k+1, то К.Ф. Гаусс доказал, что полином

$x^3 - 2$ расщепляется на линейные множители по модулю p, только если существуют такие целые числа C и D, что $p = c^2 + 27D^2$. Другими словами простое число p можно представить квадратичной формой $x^2 + 27y^2$ дискриминанта -108 при некоторых целых x и y. Простые числа p, представимые формой $4x^2 + 2xy + 7y^2$ дают для $x^3 - 2$ тип расщепления

(3), т.е. этот полином неприводим.

Аналогичный результат справедлив для полинома $g(x) = x^3 + 2$.

В 1898 году выдающийся русский математик Г.Ф. Вороной сформулировал следующую гипотезу:

1. Для того, чтобы сравнение 3-ей степени при простом модуле имело только один корень, необходимо и достаточно, чтобы дискриминант сравнения был не квадратичным вычетом по этому модулю.
2. В том случае, когда дискриминант – квадратичный вычет по рассматриваемому модулю, сравнение имеет три корня, или не имеет ни одного.
3. При всех простых модулях, представляемых в какой-нибудь квадратичной бинарной форме с определителем равным дискриминанту сравнения 3-ей степени, это сравнение всегда одинаковое число корней.

Принимая во внимание теорему Штекельберга – Вороного, мы видим, что в доказательстве нуждается только последний третий пункт.

Для полиномов вида $q(x) = x^3 - k$ справедливость пункта 3 гипотезы Вороного была в 1900 году доказана Р. Дедекином [5]. А в 1950 году Х. Хассе доказал справедливость пункта 3 для любого неприводимого полинома 3ей степени с целыми коэффициентами [3].

Отметим, что и после доказательства гипотезы Вороного, вопрос связанный с проблемой 2 не решен еще полностью, так как ответ дается в терминах представимости простых чисел классами квадратичных форм, но пока не найдены критерии такой представимости простых чисел, если число классов в роде больше единицы.

Полиномы $q(x) = x^3 - a$ и $g = x^3 + a$, $a \ni Z$, имеют один и тот же дискриминант D=-27a^2 и $\left(\frac{p}{p}\right) = -1$ только если простое число p имеет вид

p=3k+2, поэтому, если q и g - неприводимые над полем рациональных чисел Q полиномы, то для простых чисел p вида p=3k+2 (и только для них) оба полинома q и g – неприводимые над полем рациональных чисел Q полиномы, то для простых чисел p имеют тип факторизации (1,2). Так как если полином q(mod p) расщепляется на линейные множители , то и полином g(mod p) также расщепляется на линейные множители, ввиду того, что если полином $x_0^3 - a \equiv 0(mod p)$, то и $(-x_0)^3 + a \equiv \equiv (mod p)$. Следовательно, если полином q = $x^3 - a$ по модулю p имеет какой-нибудь тип расщепления, то и полином g = $x^3 - a$ по модулю p имеет тот же тип расщепления.

В дальнейшем мы будем рассматривать полиномы 3-ей степени вида $q = x^3 + px + q$ с целыми коэффициентами, неприводимые над полем рациональных чисел Q и имеющие не абелеву группу Галуа S_3 шестого порядка. Это означает, что дискриминант $D(q) = -4p^3 - 27q^2$ не есть квадрат целого числа. Так как в этом случае полином q(x) имеет один вещественный корень и два мнимых сопряженный корня, то $r_1 = 1, r_2 = 1$ и тогда, как известно знак у D(q) будет:

$$Sign\, D(q) = (-1)^{r_2} = (1)^1 = -1,$$

таким образом в рассматриваемом случае D(q) < 0.

Пусть a_1, a_2, a_3 – корни кубического неприводимого полинома q(x), поле $K_i = Q(\alpha_i)$, i=1,2,3, поле N=Q(a_1, a_2, a_3) – поле расщепления над Q полинома q(x), L=Q ($\sqrt{D(q)}$) – квадратичное подполе, содержащееся в N, пусть

$$D(q) = d \cdot \varphi^2, \qquad (2)$$

где d – дискриминант квадратичного поля.

Рассмотрим пример. Пусть p= -1, q=1, тогда

$$q(x) = x^3 - x + 1, \qquad D(q) = -23, \qquad Gal(q) = S_3$$

Квадратичное поле L=Q($\sqrt{-23}$) имеет число классов идеалов, равное 3.

Если символ Лежандра $\left(-\frac{23}{p}\right) = -1$, только если простое число p имеет вид:

p=92k+5,7,11,15,17,19,21,33,37,43,45,51,53,57,61,63,65,67,79,83,89,91,

где k пробегает некоторые натуральные числа.

Например $x^3 - x + 1 \equiv (x+2)(x^2 - 2x + 3)(mod5)$.

Если $\left(-\frac{23}{p}\right) = -1$, то для таких простых чисел p имеем $\left(-\frac{23}{p}\right) = +1$ и для них факторизационные типы для полинома $x^3 - x + 1$ будет (1,1,1) и (3). Распознать какой тип факторизации будет у данного полинома по модулю p можно с помощью приведённых положительно определённых квадратичных форм дискриминанта -23. Имеется три приведённые бинарные положительно определенные квадратичные формы дискриминанта -23, которые неэквивалентны относительно унимодулярных преобразований :

$$g(x,y) = 2x^2 + xy + 3y^2, n(x,y) = x^2 + xy + 6y^2, t(x,y) = x^2 - xy + 6y^2.$$

Простые числа p, представимые формой g(x,y) дают факторизационный тип (3), т.е. полином $x^3 - x + 1$ для таких p неприводим по модулю p. Простые числа p, представимые формами h(x,y) и t(x,y) дают тип расщепления (1,1,1), т.е. полином $x^3 - x + 1$ расщепляется в произведение трёх линейных множителей по модулю p. Например: g(0,1)=3, g(1,0)=2, g(2,1)=13, g(2,3)=41 и т.д; h(1,-2)=23, h(1,4)=101 и т.д. Заметим, что если x, y – целые числа, то области значений форм h(x,y) и t(x,y) совпадают, если x, y – принимают только натуральные числа, то области значений этих форм различны.

Если p – данное простое и $\left(-\frac{23}{p}\right) = -1$, то нет критериев, обеспечивающих представление p одной из этих форм.

Заметим, что число классов идеалов квадратичного поля L=Q($\sqrt{-23}$) равно 3, и это не случайное значение для рассматриваемого случая, как мы увидим в дальнейшем.

Аналогичное исследование можно провести для других кубических неприводимых полиномов с целыми коэффициентами, например для $q(x) =$

$= x^3 + x + 1$ с дискриминантом D(q)=-31. В этом случае имеем $\left(-\frac{31}{p}\right) = -1$ для простых чисел p, имеющих вид:

p= 124k + 3, 11, 13, 15, 17, 21, 23, 27, 29, 37, 43, 53, 55, 57, 61, 65, 73, 75, 77, 79, 83, 85, 89, 91, 99, 105, 115, 117, 119,

где k – пробегает натуральные числа, для которых p=124k+a есть простое число и a-одно из указанных 30 значений. Для этих простых чисел p полином $x^3 + +x + 1$ по модулю p имеет факторизационный тип (1,2). Другие простые числа доставляющие другие факторизационные типы (1,1,1) и (3) для полинома $x^3 + +x + 1$ характеризуется тремя квадратичными приведёнными формами дискриминанта -31:

$$y_1(x,y) = x^2 + xy + 8y^2, \quad h_1(x,y) = 2x^2 + xy + 4y^2,$$
$$t_1(x,y) = 2x^2 - xy + 4y^2$$

Простые числа представимые формой $g_1(x,y)$ дают факторизационный тип (3), т.е. полином $x^3 + x + 1$ неприводим по модулю этих простых чисел; а простые числа представимые квадратичными формами $h_1(x,y)$ и $t_1(x,y)$ дают для полинома $x^3 + x + 1$ факторизационный тип (1,1,1). Заметим, что число классов идеалов в поле $Q(\sqrt{-31})$ равно 3.

Сформируем один из основных результатов упомянутой работы Х. Хассе. Пусть $\alpha_1, \alpha_2, \alpha_3$ – корни неприводимого полинома q(x) с целыми коэффициентами, поле K=Q(α), где α – один из корней α_i. Дискриминант

D(q) не является квадратом целого числа. В этом случае поле N=Q ($\alpha_1, \alpha_2, \alpha_3$) содержит единственное квадратичное подполе L=Q($\sqrt{d}$), где d – арифметический дискриминант поля L, т.е. целое число свободное от квадратов.

Обозначим через D- арифметический дискриминант поля K, т.е. дискриминант фундаментального базиса целых алгебраических чисел поля K, тогда, как известно, выполняются соотношения:

$$D(q) = D \cdot t^2, \quad D = d \cdot q^2,$$ где t, q – целые числа

В этой ситуации Хассе доказал, что для q и d выполняются следующие условия:

a) $q = p_1 \cdot p_2 \dots p_n$

b) $q = p_1 \cdot p_2 \dots p_n 3^w$, где w=1 или 2,

при этом p_i (i=1,…, n; $n \geq 0$)- простые числа отличные от 3 и выполняются сравнения

$$p_i \equiv \left(\frac{d}{p_i}\right) (mod 3)$$

В случае b) имеем:

для $d \not\equiv 0\ (mod 3), w = 2$,

для $d \equiv +3\ (mod 9), w = 1$,

для $d \equiv -3 (mod 9), w = 1$ *или* 2.

И это необходимое условие для существования кубического поля с арифметическим дискриминантом D, если при этом поле L=Q($\sqrt{d}$) имеет число классов идеалов, делящееся на 3, то приведённые условия являются необходимыми и достаточными для существования кубических расширений с дискриминантом D, погружаемых в нормальное расширение с дискриминантом D, погружаемых в нормальное расширение поля Q степени 6.

Приведённое утверждение имеет интересные следствия.

Пусть $q(x) = x^3 + a_1x^2 + a_2x + a_3$ – полином 3-ей степени и D(q) его дискриминант, тогда, как известно,

$$D(q)=a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3.$$

Рассмотрим диофантово уравнение

$$D(q)=D \qquad (3)$$

где D - некоторое целое число, удовлетворяющее условию $D \equiv 0(mod4)$ *или* $D \equiv 1(mod4)$, если при этом $D \neq t^2$, t- некоторое целое число D не делится на квадраты целых чисел и поле $L=Q(\sqrt{D})$ имеет число классов идеалов не делящееся на 3, то уравнение (3) не имеет решений в целых числах. Например, при D = 5, 13, 17, 21, 29, 37, 41, 61, 69 диофантово уравнение (3) не имеет решений в целых числах, это означает, что не существует полиномов 3-ей степени с целыми коэффициентами, имеющие данные дискриминанты.

Литература

1. Боревич З.И. Шафревич И.Р. Тоерия чисел, М. Наука, 1973
2. Вандер Варден, Алгебра, М., Наука, 1976.
3. Hasse H., Arithmetiche Theirie der Kubischer Zahlorper auq Klassenkorpertheoretischer Grundlage. Math. Zeitchr., Bd.31 (1930), N4, S. 565-582.
4. Чеботарев Н.Г., Основы теории Галуа, М.1934
5. Алгебраическая теория чисел, сб. под ред. Дж. Кассельса и А. Фрёлиха, М. Мир, 1969.
6. С. Ленг, Алгебраические числа, М. Мир, 1966.
7. Сергеев А.Э., Сергеев Э.А., Основы теории Галуа, Краснодар 2014.
8. Чебышев П.Л., Полное собрание сочинений, Том 1, м., 1944.
9. Айрленд К., Роузен М., Классическое введение в современную теорию чисел, М. Мир, 1987.
10. Манин Ю.И., Панчиникин А.А., Введение в современную теорию чисел, М., МЦНМО, 2009.

References

1. Borevich Z.I. Shafrevich I.R. Toerija chisel, M. Nauka, 1973
2. Vander Varden, Algebra, M., Nauka, 1976.
3. Hasse H., Arithmetiche Theirie der Kubischer Zahlorper auq Klassenkorpertheoretischer Grundlage. Math. Zeitchr., Bd.31 (1930), N4, S. 565-582.

4. Chebotarev N.G., Osnovy teorii Galua, M.1934
5. Algebraicheskaja teorija chisel, sb. pod red. Dzh. Kassel'sa i A. Frjoliha, M. Mir, 1969.
6. S. Leng, Algebraicheskie chisla, M. Mir, 1966.
7. Sergeev A.Je., Sergeev Je.A., Osnovy teorii Galua, Krasnodar 2014.
8. Chebyshev P.L., Polnoe sobranie sochinenij, Tom 1, m., 1944.
9. Ajrlend K., Rouzen M., Klassicheskoe vvedenie v sovremennuju teoriju chisel, M. Mir, 1987.
10. Manin Ju.I., Panchinikin A.A., Vvedenie v sovremennuju teoriju chisel, M., MCNMO, 2009.