Math-Net.Ru

Общероссийский математический портал

С. И. Адян, В. М. Бухштабер, Е. И. Зельманов,
С. В. Кисляков, В. В. Козлов, Ю. В. Матиясевич,
С. П. Новиков, Д. О. Орлов, А. Н. Паршин, В. Л. Попов,
Д. В. Трещев, Владимир Петрович Платонов (к вось-
мидесятилетию со дня рождения), *УМН*, 2020, том 75,
выпуск 2, 197–200

DOI: <https://doi.org/10.4213/rm9938>

Использование Общероссийского математического портала Math-Net.Ru под-
разумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.91.87.62

26 апреля 2023 г., 16:20:03

МАТЕМАТИЧЕСКАЯ ЖИЗНЬ

Владимир Петрович Платонов

(к восьмидесятилетию со дня рождения)

1 декабря 2019 г. исполнилось восемьдесят лет выдающемуся ученому Владимиру Петровичу Платонову, академику Российской академии наук и Национальной академии наук Беларуси, главному научному сотруднику Научно-исследовательского института системных исследований РАН и Математического института имени В. А. Стеклова РАН.

В. П. Платонов – всемирно известный математик, специалист в области алгебры, алгебраической геометрии и теории чисел. Его математическое творчество отличается оригинальностью и самобытностью. Им решен ряд крупных математических проблем, среди которых проблема сильной аппроксимации в алгебраических группах, проблема Кнезера–Титса, проблема Таннаки–Артина, проблема рода для арифметических групп и целочисленных представлений конечных групп, проблема Гротендика о проконечных пополнениях, проблема рациональности групповых алгебраических многообразий. В. П. Платоновым написано более 180 научных работ, в том числе совместная с А. С. Рапинчуком монография “Алгебраические группы и теория чисел”, ставшая в мировой математической литературе основным источником сведений об арифметических группах и строении алгебраических групп над локальными и глобальными полями.

Многие научные результаты В. П. Платонова, а также основные этапы его преподавательской и научно-организационной деятельности освещены в статьях, посвященных его семидесятилетию (*УМН*, 65:3(393) (2010), 203–206) и семидесятипятилетию (*УМН*, 70:1(421) (2015), 204–207). В настоящей статье мы сосредоточиваемся на результатах, полученных в работах [1]–[18] последних лет. В них развита теория нахождения фундаментальных единиц в гиперэллиптических полях и на ее основе построены новые высокоэффективные алгоритмы их вычисления. Эти результаты имеют высокую практическую важность ввиду приложений в современной криптографии. Другие их важные приложения относятся к направлению, исследующему возможность обобщить классические результаты о группах кручения эллиптических кривых над полем рациональных чисел на случай абелевых многообразий размерности больше 1.

Принципиально новый подход В. П. Платонова к проблеме кручения в якобианах гиперэллиптических кривых получил дальнейшее развитие. Были построены четыре новые гиперэллиптические кривые рода 2, якобианы которых содержат $\mathbb{Q}$ -точку порядка 28, а также другие кривые рода 2, якобианы которых содержат $\mathbb{Q}$ -точки порядков 30, 36, 39. Была доказана абсолютная простота якобианов вышеуказанных кривых, что показывает невозможность их получения методом факторизации прямого произведения двух эллиптических кривых. В. П. Платоновым совместно с Г. В. Федоровым впервые для конечных нормирований была обнаружена связь между проблемой существования нетривиальных S -единиц в поле и периодичностью разложения в непрерывную дробь некоторых ключевых элементов этого поля. Полученные результаты позволили сформулировать быстрые алгоритмы для поиска S -единиц в полях функций гиперэллиптических кривых с одной точкой на бесконечности.

Получены новые существенные результаты о достаточных условиях периодичности и квазипериодичности разложения элементов гиперэллиптического поля L с полем констант k , определенного гиперэллиптической кривой X , заданной уравнением $y^2 = f$, где $f \in k[x]$. А именно, показано, что наличие периодических и квазипериодических элементов в L равносильно наличию нетривиальной S -единицы. В терминах решения уравнения типа Пелля получен критерий квазипериодичности произвольного элемента для произвольного поля констант k . Построены примеры как периодических разложений элемента $\sqrt{f}$, так и непериодических. Для гиперэллиптических полей L , обладающих фундаментальной S -единицей нечетной степени, было доказано, что свойство периодичности элемента $\sqrt{f}$ равносильно квазипериодичности. Для этого случая установлена симметрия разложения элемента $\sqrt{f}$ в непрерывную дробь. Обнаружено принципиальное различие между случаями наличия в гиперэллиптическом поле L нетривиальной S -единицы нечетной степени и наличия в нем только нетривиальных S -единиц четных степеней. В этих исследованиях использовались нетривиальные высокопроизводительные компьютерные вычисления.

Получены новые существенные продвижения в исследовании проблемы существования и построения фундаментальных S -единиц в гиперэллиптических полях для различных множеств нормирований S . А именно, доказан общий критерий квазипериодичности функциональных непрерывных дробей квадратичных иррациональностей поля формальных степенных рядов $k((h))$. Для гиперэллиптического поля L окончательно решен вопрос о периодичности ключевых элементов вида $\sqrt{f}/h^s$: для произвольного поля констант k характеристики, отличной от 2, доказано, что квазипериодичность разложения элемента $\sqrt{f}/h^s$ в функциональную непрерывную дробь равносильна его периодичности.

К числу наиболее значительных результатов относится доказательство следующего неожиданного утверждения: если степень многочлена f равна 3 (т. е. X – эллиптическая кривая), то существует ровно три нетривиальных неэквивалентных примера таких f , что $\sqrt{f}$ раскладывается в периодическую непрерывную дробь в поле $\mathbb{Q}((h))$.

В. П. Платоновым была обнаружена глубокая связь между ганкелевыми матрицами и полями рациональных функций на эллиптических кривых. С использованием этой связи удалось с помощью эффективного рекуррентного алгоритма конструктивно получить удивительный результат: существует бесконечномерная ганкелева матрица с целыми коэффициентами или коэффициентами вида $m/2^l$, где m и l – целые числа, такая, что все ее главные подматрицы H_r размера $r \times r$, где $r = 1, 2, 3, \dots$, невырождены, а множество простых делителей числителей определителей этих подматриц H_r совпадает с множеством всех нечетных простых чисел. Это исследование открывает новый перспективный подход к изучению указанного класса матриц.

Мы желаем Владимиру Петровичу здоровья и новых творческих успехов.

*С. И. Адян, В. М. Бухштабер, Е. И. Зельманов, С. В. Кисляков,
В. В. Козлов, Ю. В. Матиясевич, С. П. Новиков,
Д. О. Орлов, А. Н. Паршин, В. Л. Попов, Д. В. Трещев*

Список литературы

- [1] В. П. Платонов, М. М. Петрунин, “Фундаментальные S -единицы в гиперэллиптических полях и проблема кручения в якобианах гиперэллиптических кривых”, *Докл. РАН*, **465**:1 (2015), 23–25; англ. пер.: V. P. Platonov, M. M. Petrunin, “Fundamental S -units in hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves”, *Dokl. Math.*, **92**:3 (2015), 667–669.
- [2] В. П. Платонов, Г. В. Федоров, “ S -единицы и периодичность непрерывных дробей в гиперэллиптических полях”, *Докл. РАН*, **465**:5 (2015), 537–541; англ. пер.: V. P. Platonov, G. V. Fedorov, “ S -units and periodicity of continued fractions in hyperelliptic fields”, *Dokl. Math.*, **92**:3 (2015), 752–756.
- [3] В. П. Платонов, М. М. Петрунин, “Новые кривые рода 2 над полем рациональных чисел, якобианы которых содержат точки кручения больших порядков”, *Докл. РАН*, **461**:6 (2015), 638–639; англ. пер.: V. P. Platonov, M. M. Petrunin, “New curves of genus 2 over the field of rational numbers whose Jacobians contain torsion points of high order”, *Dokl. Math.*, **91**:2 (2015), 220–221.
- [4] В. П. Платонов, М. М. Петрунин, “ S -единицы в гиперэллиптических полях и периодичность непрерывных дробей”, *Докл. РАН*, **470**:3 (2016), 260–265; англ. пер.: V. P. Platonov, M. M. Petrunin, “ S -units in hyperelliptic fields and periodicity of continued fractions”, *Dokl. Math.*, **94**:2 (2016), 532–537.
- [5] В. П. Платонов, В. С. Жгун, Г. В. Федоров, “Непрерывные дроби в гиперэллиптических полях и представление Мамфорда”, *Докл. РАН*, **471**:6 (2016), 640–644; англ. пер.: V. P. Platonov, V. S. Zhgoon, G. V. Fedorov, “Continued rational fractions in hyperelliptic fields and the Mumford representation”, *Dokl. Math.*, **94**:3 (2016), 692–696.
- [6] В. П. Платонов, М. М. Петрунин, “ S -единицы и периодичность в квадратичных функциональных полях”, *УМН*, **71**:5(431) (2016), 181–182; англ. пер.: V. P. Platonov, M. M. Petrunin, “ S -units and periodicity in quadratic function fields”, *Russian Math. Surveys*, **71**:5 (2016), 973–975.
- [7] В. П. Платонов, “О новых свойствах ганкелевых матриц над полем рациональных чисел”, *УМН*, **72**:5(437) (2017), 187–188; англ. пер.: V. P. Platonov, “On new properties of Hankel matrices over the field of rational numbers”, *Russian Math. Surveys*, **72**:5 (2017), 963–964.
- [8] В. П. Платонов, Г. В. Федоров, “О периодичности непрерывных дробей в эллиптических полях”, *Докл. РАН*, **475**:2 (2017), 133–136; англ. пер.: V. P. Platonov, G. V. Fedorov, “On the periodicity of continued fractions in elliptic fields”, *Dokl. Math.*, **96**:1 (2017), 332–335.
- [9] В. П. Платонов, Г. В. Фёдоров, “О периодичности непрерывных дробей в гиперэллиптических полях”, *Докл. РАН*, **474**:5 (2017), 540–544; англ. пер.: V. P. Platonov, G. V. Fedorov, “On the periodicity of continued fractions in hyperelliptic fields”, *Dokl. Math.*, **95**:3 (2017), 254–258.
- [10] В. П. Платонов, М. М. Петрунин, В. С. Жгун, Ю. Н. Штейников, “О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ ”, *Докл. РАН*, **483**:6 (2018), 609–613; англ. пер.: V. P. Platonov, V. S. Zhgoon, M. M. Petrunin, Yu. N. Shteinikov, “On the finiteness of hyperelliptic fields with special properties and periodic expansion of $\sqrt{f}$ ”, *Dokl. Math.*, **98**:3 (2018), 641–645.
- [11] В. П. Платонов, Г. В. Федоров, “Бесконечное семейство кривых рода 2 над полем рациональных чисел, якобианы многообразия которых содержат рациональные точки порядка 28”, *Докл. РАН*, **482**:4 (2018), 385–388; англ. пер.: V. P. Platonov, G. V. Fedorov, “An infinite family of curves of genus 2 over the field of rational numbers whose Jacobian varieties contain rational points of order 28”, *Dokl. Math.*, **98**:2 (2018), 468–471.

- [12] В. П. Платонов, М. М. Петрунин, “О новых арифметических свойствах определителей ганкелевых матриц”, *Докл. РАН*, **481**:5 (2018), 484–485; англ. пер.: V. P. Platonov, M. M. Petrunin, “On new arithmetic properties of determinants of Hankel matrices”, *Dokl. Math.*, **98**:1 (2018), 370–372.
- [13] В. П. Платонов, В. С. Жгун, Г. В. Федоров, “О периодичности непрерывных дробей в гиперэллиптических полях над квадратичным полем констант”, *Докл. РАН*, **482**:2 (2018), 137–141; англ. пер.: V. P. Platonov, V. S. Zhgoon, G. V. Fedorov, “On the periodicity of continued fractions in hyperelliptic fields over quadratic constant field”, *Dokl. Math.*, **98**:2 (2018), 430–434.
- [14] В. П. Платонов, М. М. Петрунин, “Группы S -единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях”, *Топология и физика, Сборник статей. К 80-летию со дня рождения академика Сергея Петровича Новикова*, Тр. МИАН, **302**, МАИК “Наука/Интерпериодика”, М., 2018, 354–376; англ. пер.: V. P. Platonov, M. M. Petrunin, “Groups of S -units and the problem of periodicity of continued fractions in hyperelliptic fields”, *Proc. Steklov Inst. Math.*, **302** (2018), 336–357.
- [15] В. П. Платонов, Г. В. Федоров, “О проблеме периодичности непрерывных дробей в гиперэллиптических полях”, *Матем. сб.*, **209**:4 (2018), 54–94; англ. пер.: V. P. Platonov, G. V. Fedorov, “On the problem of periodicity of continued fractions in hyperelliptic fields”, *Sb. Math.*, **209**:4 (2018), 519–559.
- [16] В. П. Платонов, М. М. Петрунин, Ю. Н. Штейников, “О конечности числа эллиптических полей с заданными степенями S -единиц и периодическим разложением $\sqrt{f}$ ”, *Докл. РАН*, **488**:3 (2019), 237–242; англ. пер.: V. P. Platonov, M. M. Petrunin, Yu. N. Shteinikov, “On the finiteness of the number of elliptic fields with given degrees of S -units and periodic expansion of $\sqrt{f}$ ”, *Dokl. Math.*, **100**:2 (2019), 440–444.
- [17] В. П. Платонов, Г. В. Федоров, “ S -единицы для линейных нормирований и периодичность непрерывных дробей обобщённого типа в гиперэллиптических полях”, *Докл. РАН*, **486**:3 (2019), 280–286; англ. пер.: V. P. Platonov, G. V. Fedorov, “On S -units for linear valuations and the periodicity of continued fractions of generalized type in hyperelliptic fields”, *Dokl. Math.*, **99**:3 (2019), 277–281.
- [18] В. П. Платонов, М. М. Петрунин, “О бесконечномерных целочисленных ганкелевых матрицах”, *Докл. РАН*, **485**:6 (2019), 667–669; англ. пер.: V. P. Platonov, M. M. Petrunin, “On infinite-dimensional integer Hankel matrices”, *Dokl. Math.*, **99**:2 (2019), 218–220.