23.04.2009
М.А. Всемирнов

$(2,3,7;n)$

В общем случае $(k,l,m;n) = \langle x,y \mid x^k = y^l = (xy)^m = [x,y]^n = 1 \rangle$

__Вопрос__: когда такие группы конечны, когда бесконечны?

$(2,3,7;n)$ бесконечна $\Leftrightarrow n \geq 9$.

Лич, Симс — $n=9$
Holt, Plesken $n \geq 11$ (1992)
Howie
Holt, Plesken, Souvignier $n=11$
интересное д-во: семимерное представление и образ — группа типа G_2.
$PSL(2,43) \hookrightarrow GL(7,11)$

и это почти все, где можно дать точный ответ

$(2,3,k;n)$ — уже неизвестно, но почти известно
один открытый случай:

$(2,3,13;4) = ?$

У нее известно 3 конечных фактора:

$PSL(3;3) = \langle x,y \mid x^2 = y^3 = (xy)^{13} = [x,y]^4 = e,\ (xyxyxy^2)^8 = 1 \rangle$

$2^{12} . PSL(3,3) = \langle \quad (\ldots)^{16} = 1 \rangle$

$PSL(2,25) = \langle \quad (\ldots)^{13} = 1 \rangle$

$n = 1, 2, 3, 5$ [redacted] $\to$ группа тривиальна
$n=4 \rightsquigarrow PSL(2,7) \cong (2,3,7;4)$
$n=6 \rightsquigarrow (2,3,7;6) \cong PSL_2(13)$
$n=8 \rightsquigarrow (2,3,7;8) \cong 2^6 \cdot PSL_2(7)$

При каких n у $(2,3,7;n)$ есть ^кон.^ фактор, у которого не происходит коллапса в соотношениях?

Задача Для каких n существует конечная $(2,3,7)$-группа такая, что порядок коммутатора __в точности__ n?

Гипотеза Для достаточно больших n $\exists q$: ~~PSL~~ $PSL_2(q)$ — гурвицева и порядок коммутатора гурвицевых образующих в точности равен n.

Ответ Для $n > 30$ и оценка точная.

$\{u_n\}_{n \geq 0}$ — числовая последовательность
p — __примитивный делитель__ u_n, если $p \mid u_n$, $p \nmid u_k$, $0 < k < n$.

Примеры $a \in \mathbb{N}$, $a > 1$

$u_n = a^n - 1$. Когда $\exists$ примитивный делитель?

① $a = 2^k - 1$, $u_1 = 2(2^{k-1} - 1)$ $\quad u_2 = 2^{2k} - 2^{2k+1} = 2^{2k}(2^{k-1} - 1)$

② $2^6 - 1$ нет примитивного делителя

т. Жарманди (1892)

Теорема Жигмонды – Бирихофа – Вандиверра (приятное д-во Артина)

u_n имеет примитивный делитель, кроме случаев

$n = 2$, $a = 2^k - 1$

$n = 6$, $a = 2$

Кармайкл – для чисел Фибоначчи

F_n: $F_{12} = 144$, для всех $n > 12$ F_n имеет примитивный делитель (Carmichael)

более общо: $u_{n+1} = au_n - bu_{n-1}$, если характеристический имеет 2 вещ. корня.

Последовательности Люка (Lucas – не Лукас!)

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

Последовательность Лемера (Lehmer)

$$\begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta}, & n \text{ – нечетно} \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & n \text{ – четно} \end{cases}$$

α/β – не корень из 1.

$$\rightsquigarrow \alpha^n\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right)$$

↖ может быть $\left|\frac{\beta}{\alpha}\right| \approx 1$, увы.

но не слишком близко, т.е. можно отделить от 1 функцией, которая убывает не сильнее $(\ )^n$.

Шинзель: α, β – алг. числа, (α/β) – не корень из 1

$\rightsquigarrow \forall n > n_0(\alpha, \beta)$ u_n имеет примитивный делитель (в смысле идеалов)

Оценки у кого были типа $2^{100} \cdot e^{470}$ уже для двузначных лок-сет Люка

Voutier (сер. 90-х): $n > 30030$

$= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

Для двучленных лок-сет Люка прим. делитель существует при $n > 30$, и эта оценка точная (Bilu – Hanrot – Voutier – Mignotte)

// но это 30 и то 30 – просто совпадение! ∠ ≈ 1 год профессорского времени он. 1998.

Возьмем $\varepsilon = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$, $\Theta = \varepsilon + \varepsilon^{-1}$

$u_{n+1} = (\Theta^2 - 1)u_n - u_{n-1}$, $u_0 = 0, u_1 = 1$. $\Rightarrow u_n \in \mathbb{Z}[\Theta]$

нельзя дискриминанта 49 ~ оно одноклассное.

Теорема 2 В гипотезе Holt-Pleskena ответ положительный $\Leftrightarrow$ u_n имеет примитивный делитель.

Теорема 3 При $n > 30$ у u_n есть примитивный делитель.

$T(2,3,7)$

$$x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad xy = \begin{pmatrix} \varepsilon & 1 \\ 0 & \varepsilon^{-1} \end{pmatrix} \Rightarrow \langle x, y \rangle / \{\pm 1\} \cong T(2,3,7)$$

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \mathbb{i} = x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\mathbb{j} = \begin{pmatrix} \varepsilon - \varepsilon^{-1} & 1 \\ 1 & -(\varepsilon - \varepsilon^{-1}) \end{pmatrix} \quad \mathbb{k} = \begin{pmatrix} -1 & \varepsilon - \varepsilon^{-1} \\ \varepsilon - \varepsilon^{-1} & 1 \end{pmatrix}$$

$\mathbb{i}^2 = -\mathbb{1}$, $\mathbb{j}^2 = (\Theta^2 - 3)\mathbb{1}$, ...

$\rightsquigarrow$ кватернионная алгебра типа $\left(\frac{-1, \Theta^2 - 3}{\mathbb{Q}(\Theta)}\right) = \mathcal{H}$.

$$y = -\frac{(\mathbb{1} + \Theta\mathbb{i} + \mathbb{k})}{2}$$

$\langle x, y \rangle \leqslant \mathcal{H}_1^*$ ← обратимые кватернионы нормы 1

$$\widetilde{\mathcal{H}} := \left\{ x_0\mathbb{1} + x_1\mathbb{i} + x_2\mathbb{j} + x_3\mathbb{k} \;\middle|\; \begin{array}{l} 2x_i \in \mathbb{Z}[\Theta] \\ x_0 - x_3 - x_2\Theta \in \mathbb{Z}[\Theta] \\ x_1 + x_2 - x_3\Theta \in \mathbb{Z}[\Theta] \end{array} \right\}$$

$\langle x, y \rangle \leqslant \widetilde{\mathcal{H}}_1^*$, и на самом деле имеет место равенство (и для $k = 9, 11, 15$ конечный тоже)

$T(2,3,7) \cong \widetilde{\mathcal{H}}_1^* / \{\pm 1\}$

$\mathbb{Z}[\theta]$ — кольцо с однозначным разложением на множители

$p \equiv \pm 1 \ (7) \Rightarrow p = \pi_1 \pi_2 \pi_3$

$p \equiv \pm 2, \pm 3 \ (7) \Rightarrow p$ остается простым

$p = 7 \Rightarrow p \sim \pi^3$

Далее рассматриваем „нечетные" простые, т.е. лежащие над нечетными p

$\mathcal{H} \longrightarrow \mathcal{H}/_{\mathrm{mod}\,\pi}$

$\| \mathbb{R}$ — потому что кват. алгебра над кон. полем

$M_2(p^k)$, $k = 1$ или 3

С другой стороны,

$\langle x, y \rangle \subseteq \mathcal{H} \longrightarrow$ подгруппа $SL_2(p^k)$

— и это на самом деле сюръекция

(см. вторую часть т. Майбета)

Куда переходит коммутатор?

$$[x, y] \longmapsto \tau = \frac{\left((\theta^2 - 1)\mathbb{1} + \theta\mathbb{j} - \mathbb{k}\right)}{2}$$

Эл-ты кватернионной алгебры квадратичны

$$\Rightarrow \tau^n = \left(w_n \mathbb{1} + u_n(\theta\mathbb{j} - \mathbb{k})\right)/2,$$

где u_n удовлетворяет тому самому рекуррентному соотношению:

$$u_{n+1} = (\theta^2 - 1)u_n - u_{n-1}$$

Если $\tau^n \xrightarrow[\mathrm{mod}\,\pi]{} 1 \Rightarrow \pi \mid u_n$

Обратно, если $\pi \mid u_n$, то (поскольку кватернионная норма $= \det$), $\tau^n \xrightarrow[\mathrm{mod}\,\pi]{} \pm 1$, а это то, что нужно (у нас проективный образ).

В $PSL_2(13)$ порядки коммутаторов гурвицевых образующих может быть $6, 7, 13$ — ибо для $n = 13$ есть 3 простых идеала

Θ – фикс.

α — такое, что $\alpha^2 - (\Theta^2 - 1)\alpha + 1 = 0$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$, среди сопр. с α два вещественных и 2 компл. сопр. пары.

$\rightsquigarrow u_n = \dfrac{\alpha^n - \alpha^{-n}}{\alpha - \alpha^{-1}}$

$\Phi_n(A,B)$ ← многочлен деления круга от двух переменных.

$\prod\limits_{d|n} \Phi_d(A,B) = A^n - B^n$, ну или $\Phi_n(A,B) = \prod\limits_{d|n} \left(A^{n/d} - B^{n/d}\right)^{\mu(d)}$,

тогда

$u_n = \prod\limits_{\substack{d|n \\ d>1}} \Phi_n(\alpha, \alpha^{-1})$

$\rightsquigarrow$ при $n>1$ $\quad \Phi_n(\alpha,\alpha^{-1}) = \prod \left(u_{n/d}\right)^{\mu(d)}$

Значит $\Phi_n(\alpha,\alpha^{-1})$ ~~вещ.~~ целое алг. число, лежащее в $\mathbb{Z}[\Theta]$

// при $n=1$ $\alpha - \alpha^{-1}$ – не вещественное

Кроме того, если π – прим. делитель u_n, то π делит $\Phi_n(\alpha,\alpha^{-1})$

Обратное, вообще говоря, неверно, но есть ослабленный аналог:

Если $\pi \mid \Phi_n(\alpha,\alpha^{-1})$ и π – не примитивный делитель, то

① π входит в разложение $\Phi_n(\alpha,\alpha^{-1})$ в первой степени

② $\pi \mid n$

Посмотрим, на какие множители раскладывается и

Из ①: $N(\pi) \mid N(\Phi_n(\alpha,\alpha^{-1}))$

$N(\pi) = \begin{cases} p \\ p^3 \end{cases}$

Считаем произведение норм всех плохих простых

$\rightsquigarrow$ Если $N(\Phi_n(\alpha,\alpha^{-1})) > n^3$, то прим. делитель существует.

$n > 1{,}8 \cdot 10^{11}$, то прим. делитель $\exists$ — первый шаг

(лин. форма от лог.)

$30 < n < 1{,}8 \cdot 10^{11}$

Далее $5200 < n < 1{,}8 \cdot 10^{n}$ – после трюка с цепной дробью.

$(2,3,7;n)$ – это было

Давайте посмотрим на $(2,3,k;n)$

$T(2,3,k)$ вкладывается в некоторую кватернионную алгебру

$\widetilde{H_1}\left(\overline{\mathbb{Q}(\varepsilon+\varepsilon^{-1})}\right)$ и снова SAF по т. Мандбета

И опять ответ – в виде вопроса о $\exists$ прим. делителей.

Но среди $\alpha^2-((\varepsilon+\varepsilon^{-1})^2-1)\alpha+1=0$

у которых много комплексных пар

Вопрос можно ли получить оценку, равномерную по k?

А давайте вместо соотн. на коммутатор рассмотрим другие:

$\langle x,y \mid x^2=y^3=(xy)^7=(R(x,y))^n=1\rangle$

Если фиксировано слово R, верно ли, что

$\forall\ \exists n$: его образом невырожд. явл-я PSL?

Пусть $R(x,y) \longmapsto \tau \notin \{1,x,y,xy$ и их степени$\}$

Вопрос Верно ли, что и здесь ответ положительный?

Вместо $u_{n+1}=(\Theta^2-1)u_n-u_{n-1}$ – на что-то заменить Θ^2-1

$u_{n+1}=Au_n-u_{n-1}$, $A\in\mathbb{Z}[\Theta]$

и нужно обобщить численные результаты на кубич. кольцо $\mathbb{Z}[\Theta]$,

но здесь можно ожидать ответ, равномерный по R