О группах точек на абелевых многообразиях над конечными полями

Юля Котельникова

НИУ ВШЭ, ИППИ РАН

24 августа 2018 г.

Постановка задачи

$\mathbb{F}_q$ – поле из $q = p^r$ элементов
$X/\mathbb{F}_q$ – абелево многообразие размерности g
$=$ проективное многообразие $+$ абелева группа
Конечная абелева группа $X(\mathbb{F}_q)$ – ?

XX век

- Эллиптические кривые: Цфасман 85, Rück 87, Schoof 87, Voloch 88
- Простая суперсингулярная поверхность: Xing 96

Пример: эллиптические кривые

Теорема

(Цфасман 1985) Группа G порядка $N = 1 + q - m$ тогда и только тогда является группой точек некоторой эллиптической кривой, когда выполнено одно из следующих условий:

1. $(q, m) = 1$, $|m| < 2\sqrt{q}$, *и* $G \cong \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$, *где* $n_2 | n_1$ *и* $n_2 | m - 2$;
2. $q = \square$, $|m| = 2\sqrt{q}$ *и* $G \cong (\mathbb{Z}/n_1)^2$, *где* $n_1 = \sqrt{q} \mp 1$;
3. $q = \square$, $p \not\equiv 1 \bmod 3$, $|m| = \sqrt{q}$ *и* G *циклическая;*
4. $q \neq \square$, $p = 2$ *или* 3, $|m| = \sqrt{pq}$ *и* G *циклическая;*

5a. $q = \square$, $p \not\equiv 1 \bmod 4$ *или* $q \neq \square$, $p \not\equiv 3 \bmod 4$, $m = 0$ *и* G *циклическая;*

5b. $q \neq \square$, $p \equiv 3 \bmod 4$, $m = 0$ *и* G *циклическая или* $G = \mathbb{Z}/n_1 \oplus \mathbb{Z}/2$ *и* $n_1 = \frac{q+1}{2}$.

Фробениус и модуль Тейта

Морфизм Фробениуса

$$X \xrightarrow{\mathrm{Fr}_{X,q}} X$$

действует тривиально на $|X|$ и $a \mapsto a^q$ для $a \in \mathcal{O}_X$.

Степень изогении $\cdot n : X \to X$ равна $2g$, где $g = \dim X$. Поэтому, если $(n, p) = 1$, то $\#\ker(\cdot n)(\overline{\mathbb{F}}_q) \cong (\mathbb{Z}/n)^{2g}$
Пусть $l \neq p$ простое. Модуль Тейта — это

$$\mathrm{T}_l(X) := \varprojlim \ker\left(X \xrightarrow{\cdot l} X\right)(\overline{\mathbb{F}}_q) \cong \mathbb{Z}_l^{2g}$$

$$X(\mathbb{F}_q)_l = \mathrm{coker}\left(1 - \mathrm{Fr}_{X,q}\,|_{\mathrm{T_l(X)}}\right)$$

Полиномы Вейля

Полином Вейля — это унитарный многочлен с целыми коэффициентами, все комплексные корни которого по абсолютной величине равны $\sqrt{q}$, причем те из ни, которые вещественны, имеют четные кратности.

Fr_X действует на $\mathrm{T}_l(X)$ полупросто.
Харакеристический многочлен f_X Фробениуса — это полином Вейля.

(Honda 1967, Tate 1968)

$$\{\text{Классы изогении простых абелевых многообразий}\}$$

$$\updownarrow$$

$$\{\text{Неприводимые полиномы Вейля}\}$$

Группы точек очень широкого класса многообразий

Теорема 1 (Рыбаков 2010)

Многоугольник Ньютона характеристического многочлена $f_X(1-t)$ оператора $1-\mathrm{Fr}_{X,q}$ на $T_l(X)$ лежит не ниже многоугольника Ходжа группы $X(\mathbb{F}_q)_l$.

Теорема (Рыбаков 2010)

Пусть $f(t)$ — многочлен Вейля. Если многоугольник Ньютона многочлена $f(1-t)$ лежит не ниже многоугольника Ходжа группы G и при этом $f(1-t)$ неприводим, то найдется абелево многообразие X для которого $f(t)$ и G будут, соответственно, характеристическим многочленом Фробениуса и группой точек.

И одного неширокого класса поверхностей

Теорема (Рыбаков 2012)

Пусть $f(t) = P^2(t)$, где $P(t)$ — сепарабельный многочлен Вейля степени 2. Группа G тогда и только тогда является группой точек какого-то многообразия в классе изогении многочлена $f(t)$ когда $G = G_1 \oplus G_2$ и многоугольник Ньютона $P(t)$ лежит не ниже многоугольников Ходжа групп G_1 и G_2.

Вообще ясно, что в классе изогении многочлена $P_1(t) \cdot P_2(t)$ лежат группы типа $G = G_1 \oplus G_2$, для которых пары (g_1, P_1) и (g_2, P_2) удовлетворяют Теореме 1.

Пусть имеется последовательность абелевых многообразий

$$0 \longrightarrow Y \longrightarrow X \longrightarrow Z \longrightarrow 0,$$

и пусть характеристические многочлены Фробениусов f_Y и f_z взаимно просты.
Тогда имеются точная последовательность $\mathbb{Z}_l[Fr]$–модулей

$$0 \longrightarrow \mathrm{T}_l(Y) \longrightarrow \mathrm{T}_l(X) \longrightarrow \mathrm{T}_l(Z) \longrightarrow 0$$

и точная последовательность коядер

$$0 \longrightarrow \mathrm{coker}(Fr_Y) \longrightarrow \mathrm{coker}(Fr_X) \longrightarrow \mathrm{coker}(Fr_Z) \longrightarrow 0.$$

Экспоненты этих групп называются инвариантами Смита оператора Fr действующего на соответствующем модуле.

Пусть вообще имеется последовательность $\mathbb{Z}_l(S)$-модулей

$$0 \longrightarrow A \longrightarrow C \longrightarrow B \longrightarrow 0.$$

Что можно сказать об инвариантах Смита модуля C, зная таковые для модулей B и A?

Теорема (Green? Klein? Thompson? Santana-Queró-Marques de Sá?)

Тройка $((a_1, \ldots, a_m), (b_1, \ldots, b_m), (c_1, \ldots, c_m))$ *тогда и только тогда является тройкой инвариантов Смита* $\mathbb{Z}_l(S)$*-модулей* A, B *и* C, *таких что*

$$0 \longrightarrow A \longrightarrow C \longrightarrow B \longrightarrow 0,$$

когда это тройка Литтлвуда-Ричардсона.

Тройки Литтлвуда-Ричардсона

На наборы $((a_1,\ldots,a_m),(b_1,\ldots,b_m),(c_1,\ldots,c_m))$ ищем условия типа

$(*_{IJK})$. $$\sum_{i\in I} a_i + \sum_{j\in J} b_j \geq \sum_{k\in K} c_k$$

$M_n = \{1,2,\ldots,n\}$;
$\Lambda_p^{\leq n} = \{\,(i_1 < i_2 < \ldots < i_p) \in (\mathbb{Z}_{\geq 0})^p \quad | \quad 1 \leq i_1; \quad i_p \leq n\,\}$;
$U_p^n = \left\{ (I,J,K) \in \left(\Lambda_p^{\leq n}\right)^3 \quad | \quad \sum_{i\in I} i + \sum_{j\in J} j = \sum_{k\in K} k + \frac{p(p+1)}{2} \right\}$.

Положим $T_1^n = U_1^n$. Множества T_p^n определяются рекурсивно

$$T_p^n = \left\{ (I,J,K) \in U_p^n \;\middle|\; \forall\, 1 \leq r < p \quad \forall\, (F,G,H) \in T_r^p \right.$$
$$\left. \sum_{f\in F} i_f + \sum_{g\in G} j_g \geq \sum_{h\in H} k_h + \frac{r(r+1)}{2} \right\}.$$

Теорема (Green? Klein? Thompson? Santana-Queró-Marques de Sá?)

Тройка $((a_1, \ldots, a_m), (b_1, \ldots, b_m), (c_1, \ldots, c_m))$ *тогда и только тогда является тройкой инвариантов Смита* $\mathbb{Z}_l(S)$*-модулей* A, B *и* C, *таких что*

$$0 \longrightarrow A \longrightarrow C \longrightarrow B \longrightarrow 0,$$

когда для $((a_1, \ldots, a_m), (b_1, \ldots, b_m), (c_1, \ldots, c_m))$ *выполнены неравенства* $(*_{IJK})$ *для всех* $(I, J, K) \in T_p^n$ *при всех* $p \in \{1, \ldots, n\}$.

Если $\dim X = 3$, то в тройке

$$0 \longrightarrow Y \longrightarrow X \longrightarrow Z \longrightarrow 0,$$

$\dim Y, \dim Z \leq 2$. Для таких многообразий имеется классификация групп точек.

Лемма

Пусть $T \subset T_l(X)$, *такой что* $\mathrm{Fr}_X T \subset T$ *и* $T \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = T_l(X) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, *то найдется многообразие* $\tilde{X}$ *и* l*-изогения* $\varphi\tilde{X} \to X$, *такая что* $\varphi : \mathrm{T}_l(X) \to T$ *— это изоморфизм*

Теорема

Группа

$$\tilde{X}(\mathbb{F}_q)_l = \mathbb{Z}/l^{c_1}\mathbb{Z}/l^{c_2}\ldots\mathbb{Z}/l^{c_6}$$

тогда и только тогда является группой точек многообрзия $\tilde{X}$ *в классе изогении с характеристическим многочленом Фробениуса* $f_X(t) = P^2(t)Q(t)$, $\deg P = \deg Q = 2$, PQ *сепарабельный, где* $(m_1 \geq m_2)$ *и* $(n_1 \geq n_2)$ *суть абсолютные значения в* $\mathbb{Z}_l$ *нулей* $P(1-t)$ *и* $Q(1-t)$ *соответственно, когда существуют наборы неотрицательных чисел* $\mathfrak{a} = (a_1, a_2, a_3, a_4)$, $\mathfrak{b} = (b_1, b_2)$ *такие что*

1. $c_1 + \ldots + c_6 = 2m_1 + 2m_2 + n_1 + n_2$
2. $a_2 \leq a_1 \leq m_1$
   $a_1 + a_4 = a_2 + a_3 = m_1 + m_2$
   $n_2 \leq b_2 \leq b_1 \leq n_1$
   $b_1 + b_2 = n_1 + n_2$

и выполнены следующие неравенства

$$
\begin{array}{lrcll}
[1] & & b_1 & \geq & c_5 \\
[2] & & b_2 & \geq & c_6 \\
[3] & & a_i & \geq & c_{i+2}, & 1 \leq i \leq 4 \\
[4] & & b_1 & \leq & c_1 \\
[5] & & b_2 & \leq & c_2 \\
[6] & & a_i & \leq & c_i, & 1 \leq i \leq 4 \\
[7] & \sum_{i \in I} a_i + b_2 & \geq & \sum_{i \in I} c_{i+1} + c_6 & & I \subset M_4 \\
[8] & a_i + b_1 & \geq & c_i + c_6, & & 1 \leq i \leq 4 \\
[9] & a_i + b_1 & \geq & c_{i+1} + c_5, & & 1 \leq i \leq 3 \\
[10] & a_i + b_2 & \leq & c_1 + c_{i+2}, & & 1 \leq i \leq 4 \\
[11] & a_i + b_2 & \leq & c_2 + c_{i+1}, & & 1 \leq i \leq 3
\end{array}
$$

$$
\begin{array}{lrcl}
[12] & a_1 + a_2 + b_1 & \geq & c_1 + c_3 + c_6 \\
[13] & a_1 + a_2 + b_1 & \geq & c_2 + c_3 + c_5 \\
[14] & a_1 + a_3 + b_1 & \geq & c_2 + c_3 + c_6 \\
[15] & a_1 + a_3 + b_1 & \geq & c_2 + c_4 + c_5 \\
[16] & a_1 + a_4 + b_1 & \geq & c_1 + c_5 + c_6 \\
[17] & a_1 + a_4 + b_1 & \geq & c_2 + c_4 + c_6 \\
[18] & a_2 + a_3 + b_1 & \geq & c_2 + c_4 + c_6 \\
[19] & a_2 + a_3 + b_1 & \geq & c_3 + c_4 + c_5 \\
[20] & a_2 + a_4 + b_1 & \geq & c_2 + c_5 + c_6 \\
[21] & a_2 + a_4 + b_1 & \geq & c_3 + c_4 + c_5 \\
[22] & a_3 + a_4 + b_1 & \geq & c_3 + c_5 + c_6
\end{array}
$$

Theorem

Для многочлена $f_X(t) = P(t)(t \pm \sqrt{q})^2$, $P(t) \cdot (t \pm \sqrt{q})$ *сепарабельный,* $(m_1 \geq m_2 \geq m_3 \geq m_4)$ *абсолютные значения нулей* $P(1-t)$ *и* $v_l(1 \pm \sqrt{q}) = b$ *подходит группа*

$$\tilde{X}(\mathbb{F}_q)_l = \mathbb{Z}/l^{c_1}\mathbb{Z}/l^{c_2} \ldots \mathbb{Z}/l^{c_6}$$

если и только если существует набор $\mathfrak{a} = (a_1, a_2, a_3, a_4)$, *такой что*

1. $c_1 + \ldots + c_6 = m_1 + \ldots + m_4 + 2b$
2. $a_1 \leq m_1$
   $a_1 + a_2 \leq m_1 + m_2$
   $a_1 + a_2 + a_3 \leq m_1 + m_2 + m_3$
   $a_1 + a_2 + a_3 + a_4 = m_1 + m_2 + m_3 + m_4$
3. *выполнены следующие неравенства*

$$\begin{array}{llll} [1] & b & \geq & c_5 \\ [2] & a_i & \geq & c_{i+2}, \qquad 1 \leq i \leq 4 \\ [3] & b & \leq & c_2 \\ [4] & a_i & \leq & c_i \qquad 1 \leq i \leq 4 \end{array}$$

$$
\begin{array}{lrcll}
[5] & a_i + b & \geq & c_i + c_6, & 1 \leq i \leq 4 \\
[6] & a_i + b & \geq & c_{i+1} + c_5, & 1 \leq i \leq 3 \\
[7] & a_i + b & \leq & c_1 + c_{i+2}, & 1 \leq i \leq 4 \\
[8] & a_i + b & \leq & c_2 + c_{i+1}, & 1 \leq i \leq 3 \\
[9] & a_1 + a_2 + b & \geq & c_1 + c_3 + c_6 & \\
[10] & a_1 + a_2 + b & \geq & c_2 + c_3 + c_5 & \\
[11] & a_1 + a_3 + b & \geq & c_1 + c_4 + c_6 & \\
[12] & a_1 + a_3 + b & \geq & c_2 + c_3 + c_6 & \\
[13] & a_1 + a_3 + b & \geq & c_2 + c_4 + c_5 & \\
[14] & a_1 + a_4 + b & \geq & c_1 + c_5 + c_6 & \\
[15] & a_1 + a_4 + b & \geq & c_2 + c_4 + c_6 & \\
[16] & a_2 + a_3 + b & \geq & c_2 + c_4 + c_6 & \\
[17] & a_2 + a_3 + b & \geq & c_3 + c_4 + c_5 & \\
[18] & a_2 + a_4 + b & \geq & c_2 + c_5 + c_6 & \\
[19] & a_2 + a_4 + b & \geq & c_3 + c_4 + c_5 & \\
[20] & a_3 + a_4 + b & \geq & c_3 + c_5 + c_6 &
\end{array}
$$

Theorem

Для многочлена $f_X(t) = P^2(t)(t \pm \sqrt{q})^2$, $P(t) \cdot (t \pm \sqrt{q})$ *сепарабельный,* $(m_1 \geq m_2)$ *абсолютные значения нулей* $P(1-t)$ *и* $v_l(1 \pm \sqrt{q}) = b$. *подходит группа*

$$\tilde{X}(\mathbb{F}_q)_l = \mathbb{Z}/l^{c_1}\mathbb{Z}/l^{c_2} \ldots \mathbb{Z}/l^{c_6}$$

если и только если существует набор $\mathfrak{a} = (a_1, a_2, a_3, a_4)$, *такой что*

1. $c_1 + \ldots + c_6 = 2m_1 + 2m_2 + 2b$
2. $a_2 \leq a_1 \leq m_1$
   $a_1 + a_4 = a_2 + a_3 = m_1 + m_2$
3. *выполнены следующие неравенства*

$$\begin{array}{llll} [1] & b & \geq & c_5 \\ [2] & a_i & \geq & c_{i+2}, \qquad 1 \leq i \leq 4 \\ [3] & b & \leq & c_2 \\ [4] & a_i & \leq & c_i, \qquad 1 \leq i \leq 4 \end{array}$$

$$
\begin{array}{lrcll}
[5] & a_i + b & \geq & c_i + c_6, & 1 \leq i \leq 4 \\
[6] & a_i + b & \geq & c_{i+1} + c_5, & 1 \leq i \leq 3 \\
[7] & a_i + b & \leq & c_1 + c_{i+2}, & 1 \leq i \leq 4 \\
[8] & a_i + b & \leq & c_2 + c_{i+1}, & 1 \leq i \leq 3 \\
[9] & a_1 + a_2 + b & \geq & c_1 + c_3 + c_6 & \\
[10] & a_1 + a_2 + b & \geq & c_2 + c_3 + c_5 & \\
[11] & a_1 + a_3 + b & \geq & c_2 + c_3 + c_6 & \\
[12] & a_1 + a_3 + b & \geq & c_2 + c_4 + c_5 & \\
[13] & a_1 + a_4 + b & \geq & c_1 + c_5 + c_6 & \\
[14] & a_1 + a_4 + b & \geq & c_2 + c_4 + c_6 & \\
[15] & a_2 + a_3 + b & \geq & c_2 + c_4 + c_6 & \\
[16] & a_2 + a_3 + b & \geq & c_3 + c_4 + c_5 & \\
[17] & a_2 + a_4 + b & \geq & c_2 + c_5 + c_6 & \\
[18] & a_2 + a_4 + b & \geq & c_3 + c_4 + c_5 & \\
[19] & a_3 + a_4 + b & \geq & c_3 + c_5 + c_6 &
\end{array}
$$

Спасибо!