TL;DR: мы пытаемся понять, является ли алгоритмически неразрешимой задача о существовании хотя бы одного решения системы диофантовых уравнений в $F(t)$ (рациональные функции над F) или $F[[t]]$ (формальные степенные ряды над F), где F — конечное поле.

Пусть нам дано простое число p, а F — конечное поле характеристики p (можно считать, что $F = \mathbb{F}_p$, то есть просто остатки по модулю p; для простоты я рассказывал только этот случай).

Напомню, что как $F[t]$ обозначается кольцо многочленов с коэффициентами из F, $F[[t]]$ — кольцо формальных степенных рядов с коэффициентами из F, $F(t)$ — поле рациональных функций над F (поле частных $F[t]$, иными словами, отношения многочленов с естественно определёнными равенствами и операциями (знаменатель не должен быть нулевым многочленом)), $F((t))$ — поле рядов Лорана над F (поле частных $F[[t]]$, можно понять, что это ряды, которым разрешено уходить в отрицательные степени, но только на конечную длину).

В идеале мы хотели бы решить такую задачу: пусть у нас есть n неизвестных $f_1, f_2, \ldots, f_n$ из $F[[t]]$ или $F(t)$ и есть некая система полиномиальных уравнений от f_i с коэффициентами из $F[t]$ (тогда такие системы являются конечными объектами, которые можно перечислить в каком-нибудь естественном порядке) Например,

$$(1 + t + 4t^2)f_1 f_2 + f_1^2 + 11 = 0$$

$$(1 + t + 4t^2)f_1^2 + (t^3 + 1)f_2^2 + t^2 f_1 f_2 = 0$$

Главный вопрос: существует ли алгоритм, который говорит, разрешима ли эта система в $F[[t]]$ или $F(t)$ соответственно (разрешима = существует хотя бы один набор f_i, что все равенства выполняются)? Знающие люди могут заметить, что эта задача очень похожа на 10-ую задачу Гильберта, только в ней вместо целых чисел рассматриваются формальные степенные ряды или рациональные функции.

Мы сможем однозначно ответить “Нет.” для рациональных функций и получить ответ “Нет, если добавить к системе уравнений несколько дополнительных условий особого вида” для формальных степенных рядов. Это не очень удивительно, так как для целых чисел ответ тоже был "Нет.". Нашим основным методом доказательства будет сведение следующей неразрешимой (я этого не доказывал, так как это муторно и выходило за рамки доклада) задачи к нашим (то есть задачи, которые мы решаем сложнее неразрешимой, поэтому тоже неразрешимы):

Теорема 1 (Об эталонной задаче.)**.** *Пусть фиксировано простое число p. Пусть у нас есть формула вида $\exists x_1 \exists x_2 \ldots \exists x_n : \varphi(x_1, x_2, \ldots, x_n)$ в логике первого порядка $(\mathbb{N}, +, 0, 1, |_p)$ ($|_p$ — предикат от двух переменных, $|_p(x, y)$ истинно тогда и только тогда, когда существует целое неотрицательное s, что $x = p^s y$), где φ имеет вид “конъюнкция условий вида «терм = терм» или «выполняется $|_p(x_i, x_j)$»” (если*

вас пугает страшное слово «терм», то в данном случае это просто какая-то сумма переменных и единичек). Вопрос об истинности этой формулы алгоритмически неразрешим.

Теорема 2. *Первый результат касается нашей задачи для $F[[t]]$. А именно, если разрешить к системе уравнений добавить требования вида "существует неотрицательное целое k, что $f_i = t^k$" (назовём это условием P) для некоторых (не обязательно всех) переменных f_i, то задача неразрешима.*

План доказательства. Пытаемся закодировать эталонную задачу. Натуральное число x_k будем просто кодировать как $f_k = t^{x_k}$ (потребуем от f_k условия P). Тогда равенство $k + l = m$ кодируется как $f_k f_l = f_m$. Осталось научиться кодировать $|_p(x_k, x_m)$. Это тоже можно сделать (не думаю, что Гиршу будут нужны такие подробности). □

Теорема 3. *Для $F(t)$ всё радужней: можно доказать неразрешимость без дополнительных условий (я это делал только для $p = 3$, для $p = 2$ нужно немного поменять методы).*

Def. Пусть $q \in F(t)$, то есть рациональная функция. Определим $\deg(q)$ как минимальное такое $k \in \mathbb{Z}$, что коэффициент при t^k в представлении q рядом Лорана ненулевой (иными словами, посмотрим на предствавление $q = t^k \frac{a}{b}$, где a, b — многочлены с ненулевым свободным членом и скажем, что $\deg(q) = k$). $\deg(0)$ положим равным $+\infty$.

Кодируем условие на несколько переменных = выражаем это условие через систему диофантовых уравнений, возможно добавив несколько новых переменных.

.
- Научиться для переменной f кодировать условие, что существует такое целое число s, что $f = t^{p^s}$.
- Научиться для переменных x, y кодировать условие, что существует такое целое число s, что $x = y^{p^s}$.
- Научиться кодировать условие, что $\deg(x) \geqslant 0$.
- Заметим, что условие $f \neq 0$ кодируется просто как $\exists g : fg = 1$.
- Будем кодировать число n как любую $f \in F(t)$, для которой $deg(f) = n$ (уже умеем требовать неотрицательность $\deg(f)$ и не равность бесконечности, поэтому это можно сделать).
- f и g кодируют равные числа, проверяем как $\deg(fg^{-1}) \geqslant 0$ и $\deg(f^{-1}g) \geqslant 0$.
- Если f и g кодируют n и m, то fg кодирует $n + m$.
- Пусть f и g кодируют n и m. Предикат $|_p(n, m)$ выполняется тогда и только тогда, когда существует такое s, что f и g^{p^s} кодируют одинаковые числа.
- Всё выразили, молодцы.
- Интересные пункты я как раз пропустил, так как Гирш ими точно интересоваться не будет. Если интересно, то основным методом доказательств выступало

изучение полюсом и нулей функций (полюса — корни знаменателя над алгебраическим замыканием, нули — корни числителя)

□