ДЕРЕВЬЯ ХУА ЛО-КЕНА В ТЕОРИИ СРАВНЕНИЙ ПО МОДУЛЮ, РАВНОМУ СТЕПЕНИ ПРОСТОГО ЧИСЛА

В. Н. Чубариков (Москва)

Первые утверждения о разрешимости полиномиальных уравнений в целых p-адических числах сводились к нахождению условий, при которых решение соответствующего решения сравнения по некоторому модулю, равному степени простого числа p, возможно было бы «поднять» до решения соответствующего уравнения в целых p-адических числах. Как правило, таким способом удавалось получать обобщения утверждений для однократных корней сравнений и уравнений.

В основу схемы Хуа Ло-кена положено утверждение о взаимосвязи кратностей корней соответствующих p-адических сравнений по простому модулю (теорема Д). В частности, в случае многочленов от одной переменной он показал, что все решения сравнения можно интерпретировать как некоторое дерево.

Критерий, теорема Гензеля и ее следствия для разрешимости уравнения в целых p-адических числах. Взаимосвязь теории сравнений по модулям, равным степеням фиксированного простого числа с теорией p-адических чисел содержится в следующем простом критерии.

Теорема А. *Для многочлена $F(x_1,\ldots,x_r)$, $r\geq 1$ с целыми рациональными коэффициентами разрешимость уравнения*

$$F(x_1,\ldots,x_r)=0$$

в целых p-адических числах эквивалентна разрешимости при любом натуральном числе k сравнения

$$F(x_1,\ldots,x_r)\equiv 0 \pmod{p^k}.$$

Первый результат о «подъеме» решения сравнения до решения соответствующего уравнения в p-адических чисел известен как лемма Гензеля.

Теорема Б. *Пусть $f(x)$ многочлен с целыми коэффициентами и*

$$f(x)\equiv g_0(x)h_0(x) \pmod{p},$$

где $g_0(x)$ и $h_0(x)$ взаимно простые многочлены, тогда существуют два многочлена $g(x)$, $h(x)$ с целыми p-адическими коэффициентами, такие, что

$$f(x)=g(x)h(x).$$

Весьма простое достаточное условие для p-адической разрешимости полиномиального уравнения в случае однократного корня с использованием всего лишь конечного числа сравнений дает следующее утверждение, основанное по существу на методе касательных Ньютона для приближенного решения уравнения в действительных числах.

Теорема В. *Пусть $F(x_1, \ldots, x_r)$ — многочлен с целыми p-адическими коэффициентами, δ — неотрицательное целое рациональное число и пусть существует набор целых p-адических чисел $(\gamma_1, \ldots, \gamma_r)$ таких, что при некотором s, $1 \le s \le r$, справедливы соотношения*

$$F(\gamma_1, \ldots, \gamma_r) \equiv 0 \pmod{p^{2\delta+1}},$$

$$\frac{\partial F(\gamma_1, \ldots, \gamma_r)}{\partial x_s} \equiv 0 \pmod{p^{\delta}},$$

$$\frac{\partial F(\gamma_1, \ldots, \gamma_r)}{\partial x_s} \not\equiv 0 \pmod{p^{\delta+1}},$$

Тогда существует набор целых p-адических чисел $(\theta_1, \ldots, \theta_r)$ такой, что

$$F(\theta_1, \ldots, \theta_r) = 0$$

$$\theta_1 \equiv \gamma_1 \pmod{p^{\delta_1}}, \ldots, \theta_r \equiv \gamma_r \pmod{p^{\delta_r}}.$$

Следующий критерий p-адической разрешимости диофантовых уравнений нашли Б.Д. Бёрч и К. Мак Кэнн. Они определили эффективно вычислимое число $D_n(F)$, названное ими «дискриминантом» многочлена $F = F(x_1, \ldots, x_r)$ с целыми рациональными коэффициентами. Это число $D_n(F)$ находится из самого многочлена F и всех его формальных частных производных. Далее, определим наивысшую степень R числа p, входящую в $D_n(F)$.

Теорема Г. *Пусть $F(x_1, \ldots, x_r)$ — многочлен с целыми рациональными коэффициентами, R — неотрицательное целое рациональное число, определенное выше, и пусть существует набор целых рациональных чисел $(\gamma_1, \ldots, \gamma_r)$ таких, что справедливо сравнение*

$$F(\gamma_1, \ldots, \gamma_r) \equiv 0 \pmod{p^{R}}.$$

Тогда существует набор целых p-адических чисел $(\theta_1, \ldots, \theta_r)$ такой, что

$$F(\theta_1, \ldots, \theta_r) = 0$$

$$\theta_1 \equiv \gamma_1 \pmod{p^R}, \dots, \theta_r \equiv \gamma_r \pmod{p^R}.$$

Последняя теорема является многомерным обобщением леммы Гензеля – Рычлика.

Деревья Хуа Ло-кена для полиномиальных сравнений от одной переменной по модулю, равному степени простого числа. Необходимость разработки другого подхода к понятию разрешимости полиномиальных сравнений возникла в связи нахождением оценок полных рациональных тригонометрических сумм Хуа Л.-к. при нахождении точного значения показателя сходимости особого ряда в проблеме Терри.

Пусть p — фиксированное простое число и $l \geq 1$ — фиксированное натуральное число. Пусть $f_1(x) = f(x)$ — многочлен степени n с коэффициентами из кольца вычетов по модулю p^l. Пусть $\tau_0 \geq 0$ — наибольшее целое число такое, что p^{τ_0} делит все коэффициенты многочлена $f_1(x)$. Пусть x_1 — решение сравнения

$$p^{-\tau_0} f_1(x) \equiv 0 \pmod{p}, \quad 0 \leq x_1 < p.$$

Положим

$$f_2(x) = p^{\tau_0} f_1(px + x_1).$$

Рассмотрим $f_2(x)$ вместо $f_1(x)$ и модуль $p^{l-\tau_0}$ вместо модуля p^l. Тогда определим наивысшую степень τ_1 числа p такую, что p^{τ_1} делит все коэффициенты многочлена $f_2(x)$. Имеем $\tau_1 \geq 1$. Пусть, теперь, x_2 — решение сравнения

$$p^{-\tau_1} f_2(x) \equiv 0 \pmod{p}, \quad 0 \leq x_2 < p.$$

Аналогично строится многочлен $f_3(x)$ и модуль $p^{l-\tau_0-\tau_1}$ и т.д.

После s шагов получим $\tau_0 + \cdots + \tau_{s-1} \geq l$, но $\tau_0 + \cdots + \tau_{s-2} < l$, и все коэффициенты $g_l(x)$ делятся на $p^{l-(\tau_0+\cdots+\tau_{s-2})}$.

Символически рассмотренное решение сравнения $f(x) \equiv 0 \pmod{p^l}$ обозначим через

$$x_1 + px_2 + \cdots + p^{s-1}x_s. \tag{1}$$

Пусть, теперь, k, $1 \leq k \leq s$ и $g(x) = f_k(x)$. Тогда справедливо следующее утверждение.

Теорема Д. *Пусть $g(x)$ — многочлен с целыми рациональными коэффициентами и a — корень кратности m сравнения*

$$g(x) \equiv 0 \pmod{p}.$$

Пусть, далее, u — наивысшая степень числа p, делящая все коэффициенты многочлена $h(x) = g(px + a)$. Тогда число корней с учетом их кратности сравнения

$$p^{-u}h(x) \equiv 0 \pmod p,$$

не превосходит m.

Заметим, что величина показателя степени u не превосходит m.

Множество решений (1) сравнения $f(x) \equiv 0 \pmod{p^l}$ по теореме Д будет представлять совокупность деревьев в количестве, не превосходящем степени n многочлена $f(x) = f_1(x)$. Пусть количество деревьев равно $n_1 \leq n$. Их вершины $a_{1,u},\ 1 \leq u \leq n_1$, отвечают решениям $x_1 = x_{1,u}$ кратности m_u сравнения $f_1(x) \equiv 0 \pmod p$. Для того, чтобы рассматривать одно дерево введем вершину a_0. Проведем из нее n_1 ребер к вершинам $a_{1,u},\ 1 \leq u \leq n_1$. Далее из каждой вершины $a_{1,u},\ 1 \leq u \leq n_1$, проведем не более m_u, которые отвечают решениям $x_1 + px_2 = x_{1,u} + px_{2,u,v},\ 1 \leq u \leq n_1,\ 1 \leq v \leq m_u$, кратности $m_{u,v} \leq m_u$.

Таким образом для каждого корня (1) сравнения $f(x) \equiv 0 \pmod{p^l}$ однозначно определяется ветвь построенного дерева некоторой длины s. Количество корней (1) не превосходит n.

DOI: 10.20948/dms-2022-2