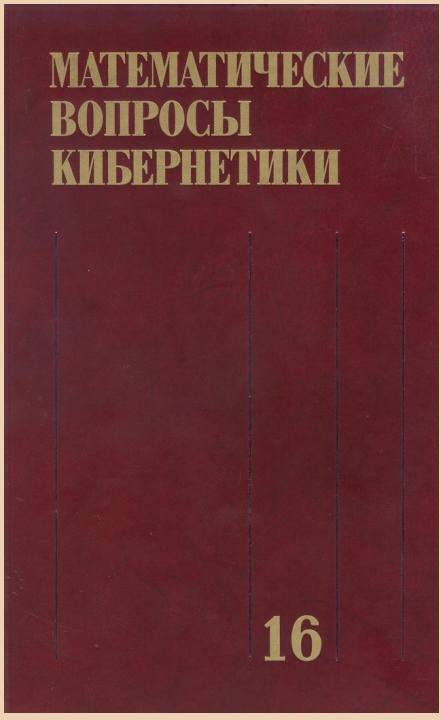
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 16



В. Н. Чубариков

Деревья Хуа Ло-кена в теории сравнений

Рекомендуемая форма библиографической ссылки: Чубариков В. Н. Деревья Хуа Ло-кена в теории сравнений // Математические вопросы кибернетики. Вып. 16. — М.: ФИЗМАТЛИТ, 2007. — С. 73–78. URL: http://library.keldysh.ru/mvk.asp?id=2007-73

ДЕРЕВЬЯ ХУА ЛО-КЕНА В ТЕОРИИ СРАВНЕНИЙ

В. Н. ЧУБАРИКОВ

(МОСКВА)

Введение

Настоящая работа посвящена памяти Олега Борисовича Лупанова. На одном из заседаний семинара по дискретной математике и математической кибернетике он обратил внимание на перспективность рассмотрения взаимосвязи между разрешимостью сравнений по модулю, равному степени простого числа, и теорией графов. На этом заседании обсуждалась теорема Хуа Ло-кена о построении p-адического решения уравнения $f(x) = 0$ для произвольного многочлена с целыми рациональными коэффициентами, лежащая в основе вывода оценки полной рациональной тригонометрической суммы [5, с. 17—18].

Заметим, что 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 своей схемы Хуа Ло-кен положил 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.

§ 1. 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 [2].

Т е о р е м а А. *Для многочлена $F(x_1, \ldots, x_r)$, $r \geqslant 1$, 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 числах известен как лемма Гензеля [6].

Т е о р е м а 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 [2].

Т е о р е м а 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, $1 \leqslant s \leqslant r$, 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 [4]. 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 $D_n(F)$.

Т е о р е м а 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

$$F(\theta_1, \ldots, \theta_r) = 0$$
$$\theta_1 \equiv \gamma_1 \pmod{p^R}, \ldots, \theta_r \equiv \gamma_r \pmod{p^R}.$$

Последняя теорема является многомерным обобщением леммы Гензеля — Рычлика, описанном в [3].

§ 2. 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. [5] при нахождении точного значения показателя сходимости особого ряда в проблеме Терри.

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

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

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 $\tau_1 \geqslant 1$. Пусть, теперь, x_2 — решение сравнения

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

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

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

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

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

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

Т е о р е м а 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 $n_1 \leqslant n$. Их вершины $a_{1,u}$, $1 \leqslant u \leqslant n_1$, 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 $a_{1,u}$, $1 \leqslant u \leqslant n_1$. Далее из каждой вершины $a_{1,u}$, $1 \leqslant u \leqslant n_1$, проведем не более m_u, которые отвечают решениям $x_1 + px_2 = x_{1,u} + px_{2,u,v}$, $1 \leqslant u \leqslant n_1$, $1 \leqslant v \leqslant m_u$, кратности $m_{u,v} \leqslant m_u$.

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.

Свяжем описанную схему построения решения сравнения по модулю, равному степени простого числа, с оценкой модуля тригонометрической суммы.

Пусть $(a_n, \ldots, a_1, p) = 1$ и $g(x) = a_n x^n + \ldots + a_1 x + a_0$ — многочлен с целыми рациональными коэффициентами.

Рассмотрим, следуя Хуа Л.-к., решение $x_0 + px + \ldots + p^r x_r$ сравнения $g'(x) \equiv 0 \pmod{p^l}$. Определим последовательность многочленов $g_1(x), \ldots, g_r(x)$ и набор показателей $u_1, \ldots, u_r$ из следующих соотношений

$$p^{u_1} g_1(x) = g(x_0 + px) - g(x_0),$$

где коэффициенты многочлена $g_1(x)$ в совокупности взаимно просты с p.

Аналогично определяются многочлены $g_s(x)$, $s = 2, \ldots, r$,

$$\begin{aligned} p^{u_s} g_s(x) &= g_{s-1}(x_{s-1} + px) - g_{s-1}(x_{s-1}) = \\ &= p^{-u_1 - \ldots - u_{s-1}} \left(g(x_0 + px_1 + \ldots + p^{s-1} x_{s-1} + p^s x^s) - \right. \\ &\qquad \left. - g(x_0 + px_1 + \ldots + p^{s-1} x_{s-1}) \right). \end{aligned}$$

Заметим, что показатели u_s, $s = 1, \ldots, r$, удовлетворяют условиям

$$n \geqslant u_1 \geqslant u_2 \geqslant \ldots \geqslant u_r \geqslant 2,$$

и количество многочленов с данным набором показателей не превосходит

$$p^\alpha, \ \alpha = r + nl - 0.5u_1(u_1 - 1) - \ldots - 0.5u_r(u_r - 1).$$

Полной рациональной тригонометрической суммой по модулю q называют сумму вида

$$S = S(q; f(x)) = \sum_{x=1}^{q} e^{2\pi i \frac{f(x)}{q}},$$

где $q > 1$ — натуральное число и $f(x) = a_n x^n + \ldots + a_1 x$ — многочлен с целыми рациональными коэффициентами.

Положим $w = \left[\dfrac{\ln n}{\ln p} \right]$.

Т е о р е м а Е. *Пусть $g(x)$ — многочлен с целыми рациональными коэффициентами, которые в совокупности взаимно просты с p, и ξ не является корнем сравнения*

$$p^{-\tau} g'(x) \equiv 0 \pmod{p}.$$

где τ — наивысшая степень числа p, делящая все коэффициенты многочлена $g'(x)$. Тогда при $l > 2w + 1$ имеем

$$\sum_{x=1}^{p^{l-1}} e^{\frac{2\pi i g(\xi + px)}{p^l}} = 0.$$

Отсюда следует равенство

$$S(p^l; f(x)) = \sum_{\xi} p^{u_1 - 1} e^{\frac{f(\xi)}{p^l}} \sum_{x=1}^{p^{l-u_1}} e^{\frac{2\pi i f_1(x)}{p^{l-u_1}}},$$

где ξ пробегает по всем корням сравнения

$$p^{-\tau} f'(x) \equiv 0 \pmod{p}.$$

§ 3. Полиномиальные сравнения от нескольких переменных по модулю, равному степени простого числа

Здесь мы построим решение сравнения

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

где $F(x_1,\ldots,x_r)$ — многочлен с целыми рациональными коэффициентами, которые в совокупности взаимно просты с p, $r>1$, $a(0,\ldots 0)=0$ и

$$F(x_1,\ldots,x_r)=\sum_{t_1=0}^{n_1}\ldots\sum_{t_r=0}^{n_r}a(t_1,\ldots,t_r)x_1^{t_1}\ldots x_r^{t_r}.$$

Рассмотрим решение $x_{s,0}+px_{s,1}+\ldots+p^tx_{s,t}$, $s=1,\ldots,r$, системы сравнений

$$\begin{cases} F'_{x_1}(x_1,\ldots,x_r)\equiv 0 \pmod{p^l},\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ F'_{x_r}(x_1,\ldots,x_r)\equiv 0 \pmod{p^l}. \end{cases}$$

Определим последовательность многочленов $F_1(x_1,\ldots,x_r),\ldots,F_t(x_1,\ldots,x_r)$ и набор показателей $u_1,\ldots,u_t$ из следующих соотношений

$$p^{u_1}F_1(x_1,\ldots,x_r)=F(x_{1,0}+px_1,\ldots,x_{r,0}+px_r)-F(x_{1,0},\ldots,x_{r,0}),$$

где коэффициенты многочлена $F_1(x_1,\ldots,x_r)$ в совокупности взаимно просты с p.

Аналогично определяются многочлены $F_s(x_1,\ldots,x_r)$, $s=2,\ldots,t$,

$$p^{u_s}F_s(x_1,\ldots,x_r)=F_{s-1}(x_{1,0}+px_1,\ldots,x_{r,0}+px_r)-F_{s-1}(x_{1,0},\ldots,x_{r,0}).$$

Отсюда имеем

$$\begin{aligned} &p^{-u_1-\ldots-u_s}F_s(x_1,\ldots,x_r)=\\ &=F(x_{1,0}+px_{1,1}+\ldots+p^{s-1}x_{1,s-1}+p^sx_1,\ldots,x_{r,0}+px_{r,1}+\ldots+p^{s-1}x_{r,s-1}+p^sx_r)-\\ &\quad-F(x_{1,0}+px_{1,1}+\ldots+p^{s-1}x_{1,s-1},\ldots,x_{r,0}+px_{r,1}+\ldots+p^{s-1}x_{r,s-1}). \end{aligned}$$

Заметим, что показатели u_s, $s=1,\ldots,t$, удовлетворяют условиям

$$n\geqslant u_1\geqslant u_2\geqslant\ldots\geqslant u_r\geqslant 2,$$

и количество многочленов с данным набором показателей не превосходит

$$p^\alpha,\ \alpha=t+nl-0.5ru_1(u_1-1)^r-\ldots-0.5ru_t(u_t-1)^r.$$

В качестве приложения построенного множества решений дадим оценку тригонометрической суммы (см., например, [1, с. 77]).

Полной кратной рациональной тригонометрической суммой по модулю q называют сумму вида

$$S=S(q;F(x_1,\ldots,x_r))=\sum_{x_1=1}^{q}\ldots\sum_{x_r=1}^{q}e^{2\pi i\frac{F(x_1,\ldots,x_r)}{q}},$$

где $q>1$ — натуральное число и

$$F(x_1,\ldots,x_r)=\sum_{t_1=0}^{n_1}\ldots\sum_{t_r=0}^{n_r}a(t_1,\ldots,t_r)x_1^{t_1}\ldots x_r^{t_r}$$

многочлен с целыми рациональными коэффициентами.

В основе оценки лежит следующая теорема.

Положим $n=\max(n_1,\ldots,n_r)$, $w=\left[\dfrac{\ln n}{\ln p}\right]$.

Т е о р е м а. *Пусть $F(x_1,\ldots,x_r)$ — многочлен с целыми рациональными коэффициентами, которые в совокупности взаимно просты с p, и $(\xi_1,\ldots,\xi_r)$ не является корнем системы сравнений*

$$\begin{cases} p^{-\tau_1}F'_{x_1}(x_1,\ldots,x_r)\equiv 0 \pmod p, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p^{-\tau_r}F'_{x_r}(x_1,\ldots,x_r)\equiv 0 \pmod p. \end{cases}$$

где τ_s, $s=1,\ldots,r$, — наивысшая степень числа p, делящая все коэффициенты многочлена $F'_{x_s}(x_1,\ldots,x_r)$. Тогда при $l>2w+1$ имеем

$$\sum_{x_1=1}^{p^{l-1}}\ldots\sum_{x_r=1}^{p^{l-1}} e^{\frac{2\pi i F(\xi_1+px_1,\ldots,\xi_r+px_r)}{p^l}}=0.$$

Отсюда следует равенство

$$S(p^l;F(x_1,\ldots,x_r))=\sum_{(\xi_1,\ldots,\xi_r}p^{r(u_1-1)}e^{\frac{F(\xi_1,\ldots,\xi_r)}{p^l}}\sum_{x_1=1}^{p^{l-u_1}}\ldots\sum_{x_1=1}^{p^{l-u_1}}e^{\frac{2\pi i F_1(x_1,\ldots,x_r)}{p^{l-u_1}}},$$

где наборы $(\xi_1,\ldots,\xi_r)$ пробегают по всем корням системы сравнений

$$\begin{cases} p^{-\tau_1}F'_{x_1}(x_1,\ldots,x_r)\equiv 0 \pmod p, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p^{-\tau_r}F'_{x_r}(x_1,\ldots,x_r)\equiv 0 \pmod p. \end{cases}$$

Таким образом получена рекуррентная формула для полной кратной рациональной тригонометрической суммы по модулю, равному степени простого числа p. Она позволяет получить оценку этой суммы. К сожалению, найти аналог теоремы Д пока не удалось.

СПИСОК ЛИТЕРАТУРЫ

1. А р х и п о в Г. И., К а р а ц у б а А. А., Ч у б а р и к о в В. Н. Теория кратных тригонометрических сумм. — М.: Наука. Физматлит. 1987.
2. Б о р е в и ч З. И., Ш а ф а р е в и ч И. Р. Теория чисел. — М.: Наука. Физматлит. 1972.
3. A x J., K o c h e n S. Diophantine problems over local fields // I. American J. Math. — 1965. — V. 87. — P. 605–630.
4. B i r c h B. J., M c C a n n K. A criterion for the p-adic solubility of diophantine equations // Quart. J. Math. — 1967. — V. 18, № 69. — P. 59–63.
5. H u a L.-k. On the number of solutions of Tarry's problem // Acta Sci. Sinica. — 1952. — V. 1. — P. 1–76.
6. H u a L.-k. Introduction to Number Theory. — Springer-Verlag. 1982.

Поступило в редакцию 15 VIII 2006