ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР
LXVI 1978 4

УДК 5198

МАТЕМАТИКА

Член-корреспондент АН Армянской ССР Р. Р. Варшамов, А. М. Антонян

Об одном методе синтеза неприводимых полиномов над конечными полями

(Представлено 22/XII 1977)

Одной из наиболее важных и актуальных проблем теории приводимости полиномов над конечными полями является проблема построения неприводимых полиномов высоких степеней в явном виде и определения порядков их корней.

В заметке приводится некоторое решение этой задачи. Рассмотрим вначале случай поля порядка $\theta=2$.

Пусть $p>2$ — простое, ν — показатель, которому 2 принадлежит по модулю p, $f(x)=\sum_{u=0}^{m} a_u x^u$ — неприводимый в поле $GF(2)$ полином степени m, $2+m$, $(m, \nu)=1$, $r=\nu^{-1}(p-1)$, $r=1$, 2 или 4,

$\pi(f(x))=a_{m-1}$, $\rho(x)=f(x+a_{m-1}+1)$, $\psi(x)(\deg\psi(x)=m)$

$\psi(x^p)\equiv 0(\mathrm{mod}\ \rho(x))$, $\Lambda(x)=\rho(x)^{-1}\psi(x^p)$ решение системы

$$\Omega(x)\equiv 1+\sum_{u=0}^{m-1} x2^u \ (\mathrm{mod}\ \Lambda(x)) \tag{1}$$

и

$$\omega(x)=(\Omega(x),\ \Lambda(x)).$$

Имеет место следующая

Теорема 1. *Полином степени $n=m\nu$*

$$F(x)=\begin{cases}\omega(x) & \text{если } \deg\omega(x)=n\\ \omega(x)^{-1}\Lambda(x) & \text{если } \deg\omega(x)>n,\end{cases}$$

неприводим в поле $GF(2)$ и $\mathrm{per}\,F(x)=p\,\mathrm{per}\,\rho(x)$.

Приведем схему доказательства.

Согласно ([1]), полином $\Lambda(x)$ разлагается на r различных неприводимых в поле $GF(2)$ полиномов $\Lambda_u(x)$ степени n. Но $\pi(\rho(x))=1$, поэтому $\pi(\Lambda(x))=1$. А это значит, что $\sum_{u=1}^{r}\pi(\Lambda_u(x))=1$, и стало быть, $\omega(x)=\prod_{u=1}^{\sigma}\Lambda_u(x)$, где $\sigma=1$ или 3.

Этим фактически и завершается доказательство теоремы.

Замечание 1. Теорема 1 имеет место также и в случае, когда $2/m$. Однако для этого необходимо, чтобы $\pi(f(x))=1$ и $(\nu, m)r = 1, 2$ или 4.

Аналогичным способом строятся неприводимые над полем $GF(\theta)$ (где $\theta=q^h$, q — простое, $h\geqslant 1$) полиномы степени $n=\prod_{u=1}^{\tau} d_u^{-1} p_u^{*u-1}\nu_u$, периоды которых равны $(\prod_{u=1}^{\tau} p_u^{*u})\operatorname{per} f(x)$, где $p_u\neq q$ $(u=\overline{1,\tau})$, простые, $\varkappa_u$ — натуральные числа, ν_u — показатель, которому θ принадлежит по модулю p_u, $d_u=(\nu_u, m\prod_{i=1}^{u-1} d_i^{-1}\nu_i)$ и $\nu^{-1}(p_u-1)d_u\leqslant 4$. Кроме того, доказывается также и следующий факт:

Пусть

$$d(x)=\left(1+\sum_{u=0}^{\nu-1} x2^u,\quad \sum_{u=0}^{p-1} x^u\right),\qquad \nu^{-1}(p-1)\leqslant 4$$

$$\lambda(x)=\begin{cases} d(x) & \text{если } \deg d(x)=\nu \\ d(x)^{-1}\sum_{u=0}^{p-1} x^u & \text{если } \deg d(x)>\nu \end{cases}$$

$\lambda(x^p)=\Lambda(x)$, $\sigma(x)$ $(\deg\sigma(x)<p\nu)$ — любое нетривиальное решение системы $\sigma(x^{2p})-x\sigma(x)\equiv 0(\bmod \Lambda(x))$, удовлетворяющее условию $x^T\neq\sigma(x)(\bmod\Lambda(x))$, где $T=(2^p-1)^{-1}(p^2z+1)$, z — решение сравнения $p^2z\equiv -1(\bmod 2^p-1)$ и $H(x)(\deg H(x)=p\nu)$ — решение системы

$$H(\sigma(x))\equiv 0(\bmod H(x)). \tag{2}$$

Тогда справедлива следующая

Теорема 2. *Полином $F(x)$ степени p, удовлетворяющий соотношению*

$$F(x^{p^2})\equiv 0(\bmod H(x)),$$

неприводим над полем $GF(2)$.

Аналогичный результат можно получить также и в произвольном поле $GF(\theta)$. Для этого в качестве $\lambda(x)$ нужно взять неприводимый в поле $GF(\theta)$ полином степени ν, а $\sigma(x)$ — любое нетривиальное решение системы $\sigma(x^{\theta p})-x\sigma(x)\equiv 0(\bmod\Lambda(x))$ удовлетворяющее условию $x^T\neq\sigma(x)$ $(\bmod\Lambda(x))$, где $T=(\theta^p-1)^{-1}(p^2z+1)$ и z — решение сравнения $p^2z\equiv -1(\bmod\theta^p-1)$.

Замечание 2. Системы сравнений, подобные (2), можно решать следующим образом ([1]).

Вначале определить $r_u(x)=\sum_{v=0}^{m} a_{u,v}x^v$ $(m=p\nu,\quad u=\overline{0,\ m})$ вычеты выражений $\sigma(x)^u$ по модулю $\Lambda(x)$. Затем построить квадратную матрицу $M=|A_{u,v}|$, где $A_{u,v}=a_{u,v}$ $(u=\overline{0,\ m},\quad v=\overline{0,\ m-1})$ и $A_{v,m}=x^v$. И, наконец, элементарными операциями добиться того, чтобы в новой

матрице $M' = |A'_{u,v}|$ на первых m местах ее последней строки стояли нули. В таком случае выражение, стоящее в крайнем нижнем углу матрицы M', будет решением (2) т. е. $A'_{m,m} = F(x)$.

Аналогично по сложности решается (²), также и сравнение вида (1), т. е. решается задача определения вычетов функции сколь угодно высоких степеней по заданному полиному. В обоих случаях оценка сложности не превосходит $O(n^3)$ единичных операций, где $n = \deg A(x)$.

Вычислительный центр Академии наук Армянской ССР
и Ереванского государственного университета

Հայկական ՍՍՀ ԳԱ բդբակից-անդամ Ռ. Ռ. ՎԱՐՇԱՄՈՎ, Ա. Մ. ԱՆՏՈՆՅԱՆ

Վերջավոր դաշտերի վրա չհանգնցվող բազմանդամների կառուցման մի մեթոդի մասին

Վերջավոր դաշտերի վրա բազմանդամների հանգնցման տեսության կարևորագույն խնդիրներից մեկը հանդիսանում է բարձր աստիճանների չհանգնցվող բազմանդամների կառուցման և նրանց կարգերի որոշման պրոբլեմը։ Աշխատանքում բերվում է այդ խնդրի որոշակի լուծումը։

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *Р. Р. Варшамов*, Некоторые вопросы конструктивной теории приводимости полиномов над конечными полями, Проблемы кибернетики, вып. 27, Изд. «Наука», 127—134, 1973. [2] *Р. Р. Варшамов и др.*, «Известия АН ГССР», т. 5, № 26 (1965).