

УДК 512.62

МАТЕМАТИКА

М. К. Кюрегян

Об одном приложении теоремы Варшамова

(Представлено чл-корр. АН Армянской ССР Р. Р. Варшамовым 22/V 1987)

Одной из наиболее важных и актуальных проблем современной алгебры является проблема построения неприводимых полиномов высоких степеней в явном виде.

В настоящей работе разработан новый метод построения неприводимых полиномов высоких степеней в явном виде над полями Галуа с помощью результатов Р. Р. Варшамова ^(1,2)

Пусть $GF(q)$ — поле Галуа порядка $q = p^s$, p — простое число, s — натуральное число.

Будем говорить, что степень элемента α над полем $GF(q)$ равна k или же α является собственным элементом поля $GF(q^k)$, если $\alpha \in GF(q^k)$ и $\alpha \notin GF(q^d)$, где d — любой собственный делитель k . В этом случае пишется $\deg_q(\alpha) = k$.

Введем в рассмотрение оператор Варшамова ⁽¹⁾

$$L^{\theta} f(x) = \frac{1}{\theta(x)} \sum_{u=0}^n \sum_{v=0}^m a_u \theta_v x^{vq^u},$$

$$\text{где } f(x) = \sum_{u=0}^n a_u x^u \text{ и } \theta(x) = \sum_{v=0}^m \theta_v x^v (\theta \neq 0), a_u, \theta_v \in GF(q).$$

Пусть $\Sigma_{\sigma} = \{f_1(x), f_2(x), \dots, f_{\sigma}(x)\}$ множество из σ примитивных над полем $GF(2)$ полиномов с попарно взаимно простыми степенями $n_1, n_2, \dots, n_{\sigma}$, ($n_i > 1$) соответственно, $T = \prod_{i=1}^{\sigma} (2^{n_i} - 1)$, $\varphi(x)$ — неприводимый в

поле $GF(2)$ полином степени n , $(n, T) = 1$, G_{σ} — совокупность всевозможных последовательностей $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\sigma})$ длины σ , где $\varepsilon_i = 0$ или 1. Пусть, далее, для любой последовательности $\varepsilon \in G_{\sigma}$, $f(x, \varepsilon, \Sigma_{\sigma}) = L^x \prod_{i=1}^{\sigma} f_i(x)^{\varepsilon_i}$, $xf(x, \varepsilon, \Sigma_{\sigma}) \equiv R^{(\varepsilon)}(x) \pmod{\varphi(x)}$ и $\psi^{(\varepsilon)}(x) = \sum_{u=0}^n \psi_u^{(\varepsilon)} x^u$, где $\psi_u^{(\varepsilon)}$ — нетривиальное решение сравнения

$$\sum_{u=0}^n \psi_u^{(\varepsilon)} R^{(\varepsilon)}(x)^u \equiv 0 \pmod{\varphi(x)}^*.$$

Тогда

Теорема 1. Полиномы

* В данных условиях это сравнение всегда имеет решение.

$$F(x) = (\varphi(x))^{(-1)^T} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2+\sigma-|\varepsilon|}} \psi^{(\varepsilon)}(xf(x, \varepsilon, \Sigma_\sigma)) \right)^{-1} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2|\sigma-|\varepsilon|}} \psi^{(\varepsilon)}(xf(x, \varepsilon, \Sigma_\sigma)) \right) \quad (1)$$

и $\psi^{(v)}(x)$ степени nT и n соответственно, где $|\varepsilon| = \sum_{i=1}^{\sigma} \varepsilon_i$ и $v \in G_\sigma$ неприводимы над полем $GF(2)$.

Доказательство. При $n=1$ справедливость теоремы непосредственно вытекает из (1). Поэтому докажем ее для $n>1$. Согласно (1) полином степени T .

$$H(x) = \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2+\sigma-|\varepsilon|}} f(x, \varepsilon, \Sigma_\sigma) \right)^{-1} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2|\sigma-|\varepsilon|}} f(x, \varepsilon, \Sigma_\sigma) \right)$$

неприводим над полем $GF(2)$. Но $(n, T)=1$, а поэтому $H(x)$ неприводим также и над полем $GF(2^n)$. Нетрудно видеть, что

$$H(x) = x^{(-1)^T} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2+\sigma-|\varepsilon|}} xf(x, \varepsilon, \Sigma_\sigma) \right)^{-1} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2|\sigma-|\varepsilon|}} xf(x, \varepsilon, \Sigma_\sigma) \right).$$

Поэтому, если α — корень уравнения $\varphi(\alpha)=0$, то среди коэффициентов полинома $H(x-\alpha)=h(x)=\sum_{u=0}^T h_u x^u$ согласно (3) найдется хотя бы один коэффициент h_u такой, что $\deg_2(h_u)=n$. Стало быть, $h(x)$ неприводим над полем $GF(2^n)$. Далее, поскольку $h^{(v)}(x)=H(x-\alpha^{2^v})=\sum_{u=0}^T h_u^{2^v} x^u$, то

согласно (4) полином $H_1(x)=\prod_{v=0}^{n-1} h^{(v)}(x)$ — неприводим над полем $GF(2)$. Стало быть,

$$H_1(x) = \prod_{v=0}^{n-1} (x-\alpha^{2^v})^{(-1)^T} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2+\sigma-|\varepsilon|}} (xf(x, \varepsilon, \Sigma_\sigma) - \beta_\varepsilon^{2^v}) \right)^{-1} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2|\sigma-|\varepsilon|}} (xf(x, \varepsilon, \Sigma_\sigma) - \beta_\varepsilon^{2^v}) \right),$$

$$\text{где } f(x, \varepsilon, \Sigma_\sigma) = \sum_{v=0}^{r_\varepsilon} b^{(\varepsilon)} x^{2^v}, \quad \beta_\varepsilon = \sum_{v=0}^{r_\varepsilon} b^{(\varepsilon)} \alpha^{2^v} \text{ и } r_\varepsilon = \sum_{i=1}^{\sigma} \varepsilon_i n_i$$

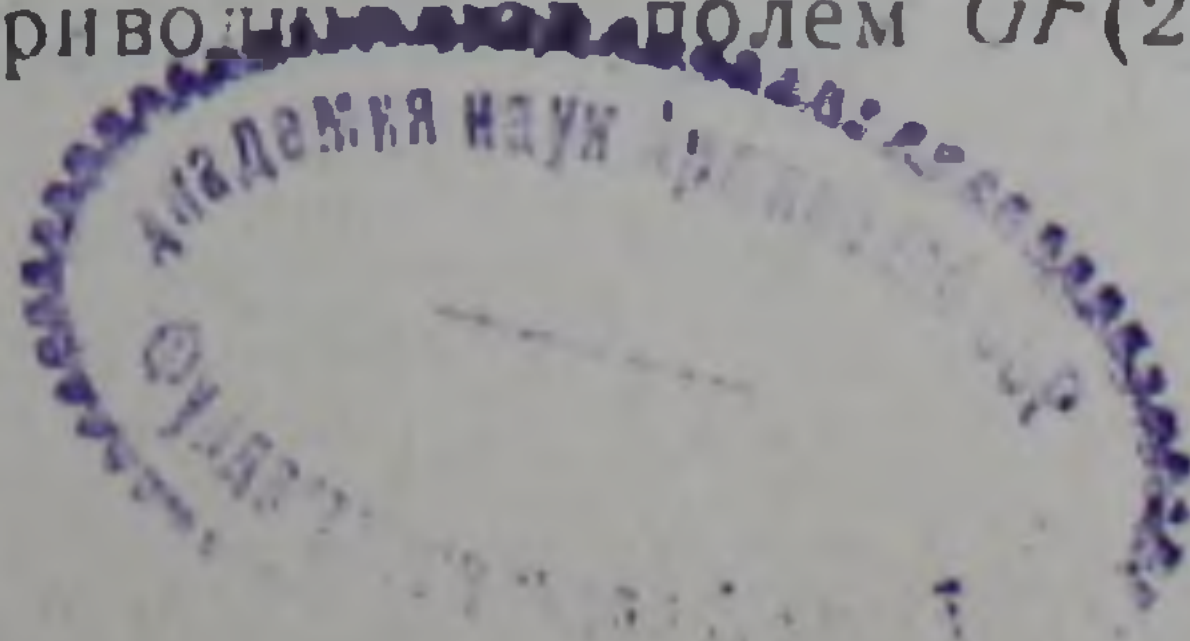
или

$$H_1(x) = \varphi(x)^{(-1)^T} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2+\sigma-|\varepsilon|}} \prod_{v=0}^{n-1} (xf(x, \varepsilon, \Sigma_\sigma) - \beta_\varepsilon^{2^v}) \right)^{-1} \left(\prod_{\substack{\varepsilon \in G_\sigma \\ 2|\sigma-|\varepsilon|}} \prod_{v=0}^{n-1} (xf(x, \varepsilon, \Sigma_\sigma) - \beta_\varepsilon^{2^v}) \right). \quad (2)$$

Покажем теперь, что для любого $\varepsilon \in \beta_\varepsilon$ является собственным элементом поля $GF(2^n)$. Допустим противное, а именно, предположим, что степень элемента β_ε над полем $GF(2)$ равна d , т. е. $\deg_2(\beta_\varepsilon)=d$, где d — собственный делитель n . Пусть $\Sigma_k = \{f_{i_1}(x), f_{i_2}(x), \dots, f_{i_k}(x)\}$ — любое подмножество Σ_σ , состоящее из k элементов $f_{i_1}(x), f_{i_2}(x), \dots, f_{i_k}(x)$, тогда согласно (1) полином

$$\lambda(x, \Sigma_k) = \left(\prod_{\substack{\varepsilon \in G_k \\ 2+k-|\varepsilon|}} f(x, \varepsilon, \Sigma_k) \right)^{-1} \left(\prod_{\substack{\varepsilon \in G_k \\ 2|k-|\varepsilon|}} f(x, \varepsilon, \Sigma_k) \right)$$

степени $T_k = \prod_{u=0}^k (2^{n_i u} - 1)$ неприводим над полем $GF(2)$. Учитывая, что



$(L^x g_1(x), L^x g_2(x)) = L^x(g_1(x), g_2(x))$, а также сепарабельность выражения $f(x, \varepsilon, \Sigma_k)$ ⁽²⁾, находим $(\lambda(x, \Sigma_k), f(x, \varepsilon, \Sigma_\sigma)) = 1$, если $|\varepsilon| < k$, и $(\lambda(x, \Sigma_k), f(x, \varepsilon, \Sigma_\sigma)) = \lambda(x, \Sigma_k)$, если $\Sigma_k \subseteq \Sigma_{|\varepsilon|=t} = \{f_{j_1}(x), f_{j_2}(x), \dots, f_{j_t}(x)\}$. Существует в точности $C_{\sigma-k}^{t-k}$ подмножеств $\Sigma_{|\varepsilon|=t}$, включающих Σ_k .

Значит, $\lambda(x, \Sigma_k)$ является делителем полинома $\prod_{|\varepsilon|=t} f(x, \varepsilon, \Sigma_\sigma)$ кратности $C_{\sigma-k}^{t-k}$. Стало быть, если обозначить $\varphi = \sum_{2|u} C_{\sigma-k}^u$ и $\varphi_1 = \sum_{2 \nmid u} C_{\sigma-k}^u$, то

$\lambda(x, \Sigma_k)$ является делителем полинома $\prod_{\substack{\varepsilon \in G_\sigma \\ 2 + \sigma - |\varepsilon|}} f(x, \varepsilon, \Sigma_\sigma)$ и $\prod_{\substack{\varepsilon \in G_\sigma \\ 2|\sigma - |\varepsilon|}} f(x, \varepsilon, \Sigma_\sigma)$

кратности φ и φ_1 , если σ нечетно и φ_1 и φ соответственно, если σ

четно. Из разложения $(x-1)^{\sigma-k} = \sum_{u=0}^{\sigma-k} C_{\sigma-k}^u x^u$ видно, что φ есть сумма

коэффициентов при четных, а φ_1 — при нечетных степенях x . Поэтому

$\varphi - \varphi_1 = (1-1)^{\sigma-k} = 0$. Значит $\lambda(x, \Sigma_k)$ входит в $\prod_{\substack{\varepsilon \in G_\sigma \\ 2 + \sigma - |\varepsilon|}} f(x, \varepsilon, \Sigma_\sigma)$ и

$\prod_{\substack{\varepsilon \in G_\sigma \\ 2|\sigma - |\varepsilon|}} f(x, \varepsilon, \Sigma_\sigma)$ с одинаковой кратностью, а поэтому с нулевой крат-

ностью в их частное.

Теперь, применяя процедуру, описанную выше, для любого ε , например, $|\varepsilon| = t$ и $\varepsilon_{i_1} = 1, \varepsilon_{i_2} = 1, \dots, \varepsilon_{i_t} = 1$, получим

$$\lambda(x, \Sigma_{|\varepsilon|=t}) = \frac{L^x \prod_{u=1}^t f_{i_u}(x)}{\prod_{k=1}^{t-1} \prod_{\Sigma_k \subset \Sigma_t} \lambda(x, \Sigma_k)},$$

где полиномы $\lambda(x, \Sigma_{|\varepsilon|})$ и $\lambda(x, \Sigma_k)$ степени $T_t = \prod_{u=1}^t (2^{n_{i_u}} - 1)$ и $T_k =$

$= \prod_{u=1}^k (2^{n_{i_u}} - 1)$ соответственно неприводимы над полем $GF(2)$. Так

как $(n, T_t) = 1$ и $(n, T_k) = 1$, то полиномы $\lambda(x, \Sigma_t)$ и $\lambda(x, \Sigma_k)$ неприводимы также и над полем $GF(2^n)$. Тогда среди коэффициентов полиномов

$$\lambda(x - \alpha, \Sigma_t) = \prod_{u=0}^{T_t} \lambda_u x^u$$

и

$$\lambda(x - \alpha, \Sigma_k) = \prod_{v=0}^{T_k} \lambda'_v x^v$$

(3)

в силу ⁽³⁾ и поскольку $n > 1$ найдутся коэффициенты λ_u и λ'_v такие, что $\deg_2(\lambda_u) = n$, $\deg_2(\lambda'_v) = n$ и полиномы (3) неприводимы над полем $GF(2^n)$. Если учесть также следующую легко доказываемую формулу:

$$\lambda(x - \alpha^{2^v}, \Sigma_t) = \sum_{u=0}^{T_t} \lambda_u^{2^v} x^u$$

и

$$\lambda(x - \alpha^{2^v}, \Sigma_k) = \sum_{r=0}^{T_k} \lambda'_r^{2^v} x^r,$$

то согласно (4) полиномы $F_1(x, \Sigma_t) = \prod_{u=0}^{n-1} \lambda(x - \alpha^{2^u}, \Sigma_t)$ и $F_1(x, \Sigma_k) = \prod_{v=0}^{n-1} \lambda(x - \alpha^{2^v}, \Sigma_k)$ будут неприводимы над полем $GF(2)$. Следовательно, будем иметь

$$F_1(x, \Sigma_t) = \frac{\prod_{v=0}^{n-1} \left(x L^x \prod_{j=1}^t f_{i_j}(x) - \left(\sum_{u=0}^N V_u \alpha^{2^u} \right)^{2^v} \right)}{\varphi(x) \prod_{k=1}^{t-1} \prod_{\Sigma_k \subset \Sigma_t} F_1(x, \Sigma_k)}, \quad (4)$$

где $x L^x \prod_{j=1}^t f_{i_j}(x) = \sum_{u=0}^N V_u x^{2^u}$ и $N = \sum_{u=1}^t n_{i_u}$. Заметим, что, так как полином $x L^x \prod_{v=0}^t f_{i_v}(x) - \sum_{u=0}^N V_u x^{2^u}$ сепарабелен, то полиномы $\lambda(x - \alpha, \Sigma_t)$ и $\lambda(x - \alpha, \Sigma_k)$ ($k < t$) — различные, а это значит, что при попарно взаимно простых $n_1, n_2, \dots, n_s$ ($n_i > 1$) полиномы $F_1(x, \Sigma_t)$ и $F_1(x, \Sigma_k)$ ($k < t$) тоже различны. Тогда, если $\deg_2 \left(\sum_{u=0}^N V_u \alpha^{2^u} \right) = d$, то $\prod_{v=0}^{n-1} \left(x - \left(\sum_{u=0}^N V_u \alpha^{2^u} \right)^{2^v} \right) = (\psi(x, \Sigma_t))^M$, где $n = dM$ и $M > 1$. Следовательно, согласно (4) будем иметь

$$F_1(x, \Sigma_t) = \frac{\psi \left(x L^x \prod_{u=1}^t f_{i_u}(x), \Sigma_t \right)^M}{\varphi(x) \prod_{k=1}^{t-1} \prod_{\Sigma_k \subset \Sigma_t} F(x, \Sigma_k)}.$$

Но поскольку полиномы $\varphi(x)$ и $F_1(x, \Sigma_k)$ ($\Sigma_k \subset \Sigma_t$) различны и неприводимы над полем $GF(2)$, то имеем $F_1(x, \Sigma_t) = \psi \left(x L^x \prod_{u=1}^t f_{i_u}(x), \Sigma_t \right)^M G(x)$, что невозможно, так как $F_1(x, \Sigma_t)$ неприводим над полем $GF(2)$. Значит $M=1$ и для любого $\varepsilon \in \beta_\varepsilon$ является собственным элементом поля $GF(2^n)$, что в свою очередь для любого ε устанавливает неприводимость полиномов $\psi^{(\varepsilon)}(x) = \prod_{u=0}^{n-1} (x - \beta_\varepsilon^{2^u})$ над полем $GF(2)$. Таким образом, в силу (2) полином (1) неприводим над полем $GF(2)$. Теперь нетрудно убедиться в том, что $\psi^{(\varepsilon)}(R^{(\varepsilon)}(x)) \equiv 0 \pmod{\varphi(x)}$ или $\sum_{u=0}^n \psi_u^{(\varepsilon)}(R^{(\varepsilon)}(x))^u \equiv 0 \pmod{\varphi(x)}$. Итак, теорема доказана полностью.

Опираясь на работы (1-4), можно доказать аналогично теореме 1 следующий факт.

Теорема 2 Пусть $\theta \in \{0; 1; 2; \}$, $(n, 2^{\theta} \prod_{i=1}^s (2^{n_i} - 1)) = 1$, $f(\theta, \varepsilon, \Sigma_s) = \theta(x) L^{\theta} \prod_{i=1}^s f_i(x)^{\varepsilon_i}$, $\theta(x) = x L^x (x + 1)^{\theta} + 1$, $(\theta(x) + 1) L^{\theta+1} \prod_{i=1}^s f_i(x)^{\varepsilon_i} \equiv R^{(\theta)}(x) \pmod{\varphi(x)}$, $\theta(x) + 1 \equiv W(x) \pmod{\varphi(x)}$, $\psi^{(\theta)}(x) = \sum_{u=0}^n \psi_u^{(\theta)} x^u$ и $\omega(x) =$

$= \sum_{u=0}^n \omega_u x^u$, где $\psi_u^{(s)}$ и ω_u нетривиальные решения сравнений

$\sum_{u=0}^n \psi_u^{(s)} (R^{(s)}(x))^u \equiv 0 \pmod{\varphi(x)}$ и $\sum_{u=0}^n \omega_u (W(x))^u \equiv 0 \pmod{\varphi(x)}$ соответственно. Тогда полиномы $\psi^{(v)}(x)$, $\omega(x)$ степени n и полином

$$F(x) = (\omega(\theta(x))^{(-1)^{\sigma}} \left(\prod_{\substack{\varepsilon \in G_{\sigma} \\ 2 + \sigma - |\varepsilon|}} \psi^{(\varepsilon)}(f(\theta, \varepsilon, \Sigma_{\sigma})) \right)^{-1} \left(\prod_{\substack{\varepsilon \in G_{\sigma} \\ 2|\sigma - |\varepsilon|}} \psi^{(\varepsilon)}(f(\theta, \varepsilon, \Sigma_{\sigma})) \right)$$

степени $2^n n T$ неприводимы над полем $GF(2)$.

Автор считает своим приятным долгом выразить благодарность чл.-корр. АН Армянской ССР Р. Р. Варшамову за полезные советы в процессе работы над статьей.

Вычислительный центр Академии наук Армянской ССР
и Ереванского государственного университета

Մ. Կ. ԿՅՈՒՐԵՂՅԱՆ

Վարչամովի մի բեռեմի կիրառության մասին

Վերջավոր դաշտերի վրա չվերածվող բազմանդամների տեսության կարևորագույն խնդիրներից մեկը հանդիսանում է բացահայտ տեսքով բարձր աստիճանների ալգաիսի բազմանդամների կառուցման պրոբլեմը:

Աշխատանքում դիտարկվում է Վարչամովի L^0 գծային օպերատորը, որի որոշման տիրույթը՝ Գալուայի $GF(q)$ դաշտից վերցված գործակիցներով բազմանդամներն են: L^0 օպերատորի օգնությամբ ապացուցվում են մի շարք թեորեմներ, որոնք թույլ են տալիս բացահայտ տեսքով բարձր աստիճանների չվերածվող բազմանդամներ կառուցել Գալուայի $GF(2)$ դաշտի վրա:

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

- ¹ Р. Р. Варшамов ДАН СССР, т. 156, № 6 (1964). ² Р. Р. Варшамов, ДАН АрмССР, т. 79, № 1 (1984). ³ М. К. Кюрегян, ДАН АрмССР, т. 83, № 2 (1986). ⁴ М. К. Кюрегян, ДАН АрмССР, т. 81, № 2 (1985).