УДК 519.48+519.92

Г. А. Гараков

Об одном свойстве первообразных элементов поля Z_p^*

(Представлено чл.-корр. АН Армянской ССР Р. А. Александряном 1/III 1968)

В настоящей заметке приводится результат, который позволяет, в некоторых случаях, сравнительно просто определять показатели** неприводимых в поле Z_p полиномов по их свободному члену.

В дальнейшем всюду: p — простое число; $g_1, g_2, \dots, g_n$ *** — первообразные элементы поля Z_p , мультипликативную группу которого обозначим через Z_p^* и $r_1, r_2, \dots, r_s$ — всевозможные различные делители $p - 1$.

Лемма. Пусть

$$\lambda_u = \{g_\sigma^{r_u}\}_{(\sigma=\overline{1, n})}, \quad (u = \overline{1, s}),$$

тогда

$$\lambda_i \cap \lambda_j = \emptyset \quad (i \neq j) \quad \text{и} \quad \bigcup_{u=1}^s \lambda_u = Z_p^*.$$

Доказательство. Допустим противное, а именно, что два различных множества λ_i и λ_j ($i \neq j$) пересекаются, т. е. что найдутся по крайней мере два элемента g_σ и g_{σ_1} , удовлетворяющие условию:

$$g_\sigma^{r_i} = g_{\sigma_1}^{r_j}.$$

Пусть $r_i < r_j$, тогда, возведя обе части этого равенства в $r_j^{-1}(p - 1)$ степень, получим

$$g_\sigma^{r_i r_j^{-1} (p-1)} = 1,$$

что невозможно, так как порядок примитивного элемента g_σ не может быть меньше $p - 1$.

Кроме того, как легко понять, множество λ_u содержит те и только те элементы группы Z_p^* , порядок которых равен $r_u^{-1}(p - 1)$.

* Z_p — поле классов вычетов по модулю p (1).

** Показателем неприводимого в поле Z_p полинома $f(x)$ называется наименьшее натуральное число l такое, что $f(x) | X^l - 1$.

*** $n = \varphi(p - 1)$, где $\varphi(\cdot)$ — мультипликативная функция Эйлера.

Поэтому $|\lambda_u|$ — число различных элементов λ_u равно $\varphi(r_u^{-1}(p-1))$, а следовательно (2)

$$|\bigcup_{u=1}^s \lambda_u| = \sum_{u=1}^s \varphi(r_u^{-1}(p-1)) = \sum_{d|p-1} \varphi(d) = p-1$$

и

$$\bigcup_{u=1}^s \lambda_u = Z_p^*$$

Лемма доказана.

Пусть далее целое $m > 2$, $L = p^m - 1$ и $l_p(m) = \{l_1, l_2, \dots, l_k\}$ — совокупность всевозможных делителей L , удовлетворяющих условию $p^\gamma \not\equiv 1 \pmod{l}$ ($\gamma < m$). Имеет место следующая

Теорема. Пусть

$$\Lambda_u = \{g_{\sigma}^{Ll_u^{-1}}\}_{(\sigma=\overline{1, n})}, (u = \overline{1, k}),$$

тогда для выполнения условия

$$\Lambda_i \cap \Lambda_j = \emptyset \quad (i \neq j)$$

необходимо и достаточно, чтобы число $N = (p^m - 1)(p - 1)^{-1}$ было простым.

Доказательство. Достаточность. В случае простого N выражение L , очевидно, будет иметь $2s$ различных делителей вида $r_u N^\delta$, где $\delta = 0, 1$. Между тем, как легко понять, ни одно из этих чисел, у которого $\delta = 0$, не может принадлежать множеству $l_p(m)$. В то время как числа с $\delta = 1$ являются элементами $l_p(m)$. Действительно, для любого натурального $\gamma \leq m$ произведение

$$(p-1)(p^{\gamma-1} + p^{\gamma-2} + \dots + 1) = p^\gamma - 1$$

будучи кратным $r_u N$, должно делиться на простое число $N = p^{m-1} + p^{m-2} + \dots + 1$. Но это, очевидно, возможно только лишь в случае $\gamma = m$. Следовательно, $l_p(m) = \{r_1 N, r_2 N, \dots, r_s N\}$ и $\Lambda_v = \lambda_u$ (где v и u связаны соотношением $r_v \cdot r_u = p - 1$). Поэтому из доказанной леммы следует, что для любой различной пары i и j действительно $\Lambda_i \cap \Lambda_j = \emptyset$.

Необходимость. Допустим обратное, т. е. что число N составное. Тогда можно показать, что по модулю, по крайней мере, одного из его делителей, число p принадлежит показателю m . В самом деле, возможны два случая:

1. m — простое,
2. m — составное.

В случае простого m ясно, что показателем числа p по модулю любого делителя N могут быть лишь числа 1 или m . Однако сравнения $p \equiv 1 \pmod{N_1}$ и $p \equiv 1 \pmod{N_2}$, где $N = N_1 \cdot N_2$, одновременно не могут выполняться, ибо тогда

$$N_1 \cdot N_2 \leq (p-1)^2 < p^2,$$

откуда $p^{m-1} < p^2$ и $m \leq 2$, что противоречит условию $m > 2$.

В случае составного m , полагая $m = a \cdot b$ ($a, b > 1$ — целые) и $N_2 = p^{a(b-1)} + p^{a(b-2)} + \dots + 1$ можно показать, что по $\text{mod } N_2$ число p принадлежит показателю m .

В самом деле, показатель ω , которому принадлежит p по модулю N_2 , очевидно, должен удовлетворять соотношению $\omega > a(b-1)$. И если предположить, что $\omega < m$, то тогда

$$1 < \frac{m}{\omega} < 1 + \frac{a}{\omega} < 2,$$

что противоречиво, так как $\frac{m}{\omega}$ — целое число.

Таким образом, мы показали, что в случае составного N по модулю, по крайней мере одного из его собственного делителя, скажем N_2 , число p , действительно принадлежит показателю m . А это значит, что $l_p(m)$ будет содержать числа $l_i = N_2$ и $l_j = N$, а следовательно, $\Lambda_i = \Lambda_j = \{l\}$ и

$$\Lambda_i \cap \Lambda_j \neq \emptyset,$$

где $i \neq j$, так как $N_2 \neq N$.

Этим завершается доказательство теоремы.

Теперь о приложении результата.

Показатель l неприводимого в поле Z_p полинома степени m и его свободный член a связаны соотношением

$$\{(-1)^m a = g^{Ll^{-1}},$$

где g — некоторый первообразный элемент поля Z_p , справедливость которого легко устанавливается на основании теоремы Вьета и свойства корней неприводимых полиномов. Следовательно, число a является элементом множества Λ_u или $-\Lambda_u$, в зависимости от четности m . Однако, согласно приведенной теореме, множества Λ не пересекаются, когда число N простое, поэтому в этом случае имеется возможность определять показатели полиномов по их свободному члену.

Пример: $L = 7^5 - 1 = 6 \times 2801$; здесь $p = 7$; $m = 5$; $N = 2801$ — простое; $g_1 = 3$ и $g_2 = 5$ первообразные элементы Z_7 .

Из сказанного следует, что неприводимые в поле Z_7 полиномы 5-ой степени принадлежат показателям: $l_1 = 2801$, $l_2 = 2 \times 2801$, $l_3 = 3 \times 2801$ и $l_4 = 6 \times 2801$, в зависимости от того, какому из множеств $\{6, 6\}$, $\{1, 1\}$, $\{5, 3\}$ и $\{4, 2\}$ соответственно принадлежит их свободный член.

В заключение отметим, что рассмотренная задача, естественно приводит к проблеме о простоте чисел вида $N = (p^m - 1)(p - 1)^{-1}$; бесконечно ли множество таких простых чисел или оно обрывается.

Ереванский политехнический институт
им. К. Маркса

Z_p դաշտի նախնական էլեմենտների մի հասկույթյան մասին*

Հոդվածում բերված է թեորեմ, որը հնարավորություն է տալիս որոշ դեպքում, համեմատաբար հեշտ եղանակով որոշել Z_p դաշտում չվերածվող բազմանդամների ցուցանիշները ըստ նրանց ազատ անդամների:

Ընդունված են նշանակումներ՝ p -ն պարզ թիվ է, $g_1, g_2, \dots, g_n$ ($n = \varphi(p-1)$) դաշտի նախնական էլեմենտներ են, m -ը ամբողջ թիվ է > 2 , $L = p^m - 1$, իսկ $l_1, l_2, \dots, l_k$ թվերը L -ի այն բաժանարարներն են, որոնք բաժարարում են առնչությունը՝

$p\gamma \equiv 1 \pmod{l}$ ($\gamma < m$); $r_1, r_2, \dots, r_s$ թվերը $(p-1)$ -ի բոլոր հնարավոր տարբեր բաժանարարներն են:

Թեորեմ: Ընդունենք

$$\Lambda_u = \left\{ g_{\sigma}^{L^i u} \right\}_{(\sigma=1, \bar{n})} \quad (u = \bar{1}, \bar{k})$$

որպեսզի

$$\Lambda_i \cap \Lambda_j = \emptyset \quad (i \neq j)$$

անհրաժեշտ և բավարար է $N = (p^m - 1)(p - 1)^{-1}$ բધի պարզ լինելու պայմանը:

Հոդվածում քննակված խնդիրը բերում է $N = (p^m - 1)(p - 1)^{-1}$ տեսքի թվերի պարզության պրոբլեմին:

* Z_p — ըստ p մոդուլի մնացքների դաշտ է:

Л И Т Е Р А Т У Р А — Գ Ր Ա Կ Ա Ն Ո Ւ Թ Յ Ո Ւ Ն

¹ В. Л. Ван-дер-Варден, Современная алгебра, ч. 1, 1947. ² И. М. Виноградов, Основы теории чисел, М., 1965.