НЯКОИ СВОЙСТВА НА ХОМОГЕННИТЕ УРАВНЕНИЯ В КРАЙНИ ПОЛЕТА

Кирил Дочев и Димитър Димитров

Съгласно една известна теорема на Шевалие всяко хомогенно сравнение при прост модул p има нетривиално решение винаги щом броят на неизвестните е по-голям от степента на сравнението. Аналогичен резултат е в сила и за хомогенните уравнения в произволно крайно поле. В частност при $m>(n,\ p-1)$ и $a_i \not\equiv 0 \pmod p$, $i=1, 2, \ldots, m$, сравнението

$$a_1x_1^n + a_2x_2^n + \ldots + a_mx_m^n \equiv 0 \pmod p \tag{1}$$

ще има нетривиално решение.

В настоящата работа са посочени достатъчни условия, при които сравнението (1) има абсолютно ненулеви решения, т. е. такива решения $(x_1, x_2, \ldots, x_m)$, за които

$$x_1 x_2 \ldots, x_m \not\equiv 0 \pmod p. \tag{2}$$

Подобна постановка на проблема, а именно да се изследва сравнение от вида (1) по отношение на съществуването на абсолютно ненулево решение, се съдържа в [1]. В посочената работа на Хурвиц е показано, че сравнението от вида (1) при $m=3$ има абсолютно ненулево решение за достатъчно големи стойности на простия модул p и при произволно фиксирано n. В редица работи на други автори са направени аналогични и по-общи изследвания за съществуване на абсолютно ненулеви решения на хомогенни уравнения в крайни полета при едни или други предположения за броя на неизвестните, степента n и характеристика p. Както в работата [1], така и в цитираните работи [2]—[7] резултатите се отнасят до хомогенни сравнения (или хомогенни уравнения в крайни полета) с фиксирана степен и с фиксиран брой на неизвестните при достатъчно големи стойности на простото число p. Общото в методите на доказателство при тези работи се състои в това, че с помощта на явни, точни или асимптотични формули се оценява броят на решенията на разглежданите сравнения (или уравнения), и при условие, че този брой се окаже достатъчно голям, се прави заключението за съществуване и на абсолютно ненулево решение. В статията [7] се съдържа подробен обзор на резултатите в това направление до 1965 г.

Като използваме метод, основаващ се на друга идея, ще докажем следната теорема

Теорема 1. Нека $p>2$ е просто число и m е делител на $p-1$. Да предположим, че целите числа $a_1, a_2, \ldots, a_m$ не се делят на p, т. е.

$$a_1 a_2 \ldots a_m \not\equiv 0 (\mathrm{mod}\, p).$$

Тогава сравнението

$$a_1 x_1^n + a_2 x_2^n + \ldots + a_m x_m^n \equiv 0 \,(\mathrm{mod}\, p)$$

при $m>(n, p-1)$ има поне едно абсолютно ненулево решение $(x_1, x_2, \ldots, x_m)$ т. е. такова решение, за което

$$x_1 \not\equiv 0, \quad x_2 \not\equiv 0, \ldots, \; x_m \not\equiv 0 \,(\mathrm{mod}\, p).$$

Доказателство. Да отбележим най-напред, че без ограничение на общността можем да разглеждаме само случая, когато $n/p-1$. Наистина, ако положим $(n, p-1)=d$ и използваме равенството $d=an+b(p-1)$, където a и b са цели числа, ще имаме

$$x^d = x^{an} \cdot x^{b(p-1)} \equiv (x^a)^n \,(\mathrm{mod}\, p)$$

за всяко $x \not\equiv 0 \,(\mathrm{mod}\, p)$. Ясно е тогава, че сравнението (1) при условие (2) ще може да се сведе до сравнение от вида

$$a_1 y_1^d + a_2 y_2^d + \ldots + a_m y_m^d \equiv 0 \,(\mathrm{mod}\, p)$$

$$(y_i \not\equiv 0 \,(\mathrm{mod}\, p), \quad i=1, 2, \ldots, m).$$

За да илюстрираме по-добре използвания метод на доказателство ще разгледаме най-напред случая $n=\frac{p-1}{2}$. При $x \not\equiv 0 \;(\mathrm{mod}\, p)$ ще имаме

$$x^n = x^{\frac{p-1}{2}} \equiv \pm 1 \,(\mathrm{mod}\, p).$$

Като положим

$$x^{\frac{p-1}{2}} \equiv \varepsilon_i \,(\mathrm{mod}\, p), \quad \varepsilon_i = \pm 1, \quad i=1, 2, \ldots, m,$$

сравнението (1) ще добие вида

$$a_1 \varepsilon_1 + a_2 \varepsilon_2 + \ldots + a_m \varepsilon_m \equiv 0 \,(\mathrm{mod}\, p).$$

Тук предполагаме, както и преди, че

$$a_1 \not\equiv 0, \quad a_2 \not\equiv 0, \ldots, \; a_m \not\equiv 0 \,(\mathrm{mod}\, p).$$

По условие имаме $m \nmid p-1$ и

$$(n, p-1)-\left(\frac{p-1}{2}, p-1\right)-\frac{p-1}{2}<m,$$

откъдето следва, че $m=p-1$. И така ще докажем, че каквито и да са целите числа $a_1, a_2, \ldots, a_m$, неделящи се на простото число $p>2$, при подходящ избор на знаците $\varepsilon_i=\pm 1$, $i=1, 2, \ldots, m$, е в сила сравнението

$$\varepsilon_1 a_1+\varepsilon_2 a_2+\ldots+\varepsilon_m a_m \equiv 0 \pmod p. \tag{3}$$

За целта да разгледаме сумата

$$S=\sum_{(\varepsilon)} \varepsilon_1 \varepsilon_2 \ldots \varepsilon_m (\varepsilon_1 a_1+\varepsilon_2 a_2+\ldots+\varepsilon_m a_m)^m, \tag{4}$$

където $m=p-1$ и сумирането е разпространяно върху всевъзможните комбинации на знаците $\varepsilon_i=\pm 1$ $(i=1, 2, \ldots, m)$. При развитието на $(\varepsilon_1 a_1+\varepsilon_2 a_2+\ldots+\varepsilon_m a_m)^m$ ще получим общ член от вида

$$\frac{m!}{k_1! k_2! \ldots k^m!}(\varepsilon_1 a_1)^{k_1}(\varepsilon_2 a_2)^{k_2} \ldots (\varepsilon_m a_m)^{k_m},$$

където $k_i \geqq 0$ и $k_1+k_2+\ldots+k_m=m$. Изразът S от (4) ще приеме вида

$$S=\sum_{(\varepsilon)} \sum_{k_1+\ldots+k_m=m} \frac{m!}{k_1! k_2! \ldots k_m!} \varepsilon_1^{k_1+1} \varepsilon_2^{k_2+1} \ldots \varepsilon_m^{k_m+1} a_1^{k_1} a_2^{k_2} \ldots a_m^{k_m}.$$

При сумирането по променливите $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_m$ събираемите, в които поне един от показателите $k_1+1, k_2+1, \ldots, k_m+1$ е нечетно число, ще дадат сбор, равен на нула. Следователно можем да считаме, че показателите $k_1, k_2, \ldots, k_m$ са нечетни числа, и понеже техният сбор е равен на m, ще имаме

$$k_1=k_2=\ldots=k_m=1.$$

По такъв начин се убеждаваме, че е в сила тъждеството

$$S=m!\, 2^m a_1 a_2 \ldots a_m. \tag{5}$$

Ако допуснем, че при произволен избор на $\varepsilon_i=\pm 1$, $i=1, 2, \ldots, m$, е в сила $\varepsilon_1 a_1+\varepsilon_2 a_2+\ldots+\varepsilon_m a_m \not\equiv 0 \pmod p$, съгласно теоремата на Ферма ще имаме

$$(\varepsilon_1 a_1+\varepsilon_2 a_2+\ldots+\varepsilon_m a_m)^m \equiv 1 \pmod p.$$

Тогава от (4) ще следва

$$S \equiv \sum_{(\varepsilon)} \varepsilon_1 \varepsilon_2 \ldots \varepsilon_m \equiv 0 \pmod p.$$

Последното противоречи на (5), понеже

$$m!\,2^m a_1 a_2 \ldots a_m \not\equiv 0 \pmod p.$$

Изложеното доказателство за частния случай $n=\frac{p-1}{2}$ притежава необходимата степен на общност, за да може съдържащата се в него идея да бъде използвана с известни модификации от технически характер и за общия случай. Тъждеството (5), на което се основаваше приведеното доказателство, е известно на авторите от една задача на Д. Скордев от неотдавна проведен конкурс между студенти на Математическия факултет

Нека сега $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ да означават различни решения на биномното сравнение

$$x^s \equiv 1 \pmod p, \tag{6}$$

където $s=\frac{p-1}{n}$. Вместо израза S от (4) да разгледаме сумата

$$T=\sum_{(\eta)} \eta_1^l \eta_2^l \ldots \eta_m^l (\eta_1 a_1+\eta_2 a_2+\ldots+\eta_m a_m)^{p-1}, \tag{7}$$

където $m>n$, $m \nmid (p-1)$ и $l=s\frac{p-1}{m}$.

Тук сумирането се отнася до всевъзможните комбинации от решения η_i на сравнението (6). Имаме

$$l=s\frac{p-1}{m}=(p-1)\left(\frac{1}{n}-\frac{1}{m}\right)>0,$$

т. е. l е естествено число. Ще преобразуваме израза T от (7) по подобен начин, както S. Тук обаче ще използваме известните сравнения

$$\sum_{i=1}^{s} \varepsilon_i^k \equiv \begin{cases} 0, & \text{при } k \not\equiv 0 \pmod s, \\ s, & \text{при } k \equiv 0 \pmod s. \end{cases} \tag{8}$$

Развивайки $(\eta_1 a_1+\eta_2 a_2+\ldots+\eta_m a_m)$ по степените на $a_1, a_2, \ldots a_m$, ще имаме

$$T=\sum_{(\eta)} \sum_{k_1+\ldots+k_m=p-1} \frac{(p-1)!}{k_1!\,k_2!\ldots k_m!}\, \eta_1^{k_1-l} \eta_2^{k_2+l} \ldots \eta_m^{k_m+l} a_1^{k_1} a_2^{k_2} \ldots a_m^{k_m}.$$

При сумирането по целите неотрицателни показатели k_i, $i=1, 2, \ldots, m$, $\sum_{i=1}^{m} k_i=p-1$ ще се получи съгласно (8) сбор, който се дели на p ви-

наги когато поне за едно k_i+l имаме $k_i+l \not\equiv 0 \pmod s$. Поради това можем да считаме, че всичките показатели k_i в T удовлетворяват условието

$$k_i+l \equiv 0 \pmod s, \quad i=1, 2, \ldots, m.$$

Да положим $k_i+l=K_i s$, $i=1, 2, \ldots, m$. От равенството $\sum_{i=1}^{m} k_i=p-1$ следва, че

$$\sum_{i=1}^{m} K_i s=p-1+ml=sm,$$

т. е.

$$\sum_{i=1}^{m} K_i=m. \tag{9}$$

Понеже K_i са естествени числа, от (9) ще получим

$$K_1=K_2= \ldots =K_m=1.$$

Така се убеждаваме, че е в сила сравнението

$$T \equiv \frac{s^m (p-1)!}{[(s-l)!]^m} (a_1 a_2 \ldots a_m)^{s-l} \pmod p. \tag{10}$$

Ако допуснем, че при всеки избор на η_i, където $\eta_i^s \equiv 0 \pmod p$, имаме

$$\eta_1 a_1+\eta_2 a_2+ \ldots +\eta_m a_m \not\equiv 0 \pmod p, \tag{11}$$

съгласно теоремата на Ферма бихме получили

$$(\eta_1 a_1+\eta_2 a_2 + \ldots +\eta_m a_m)^{p-1} \equiv 1 \pmod p.$$

Тогава за израза T от формула (7) ще имаме

$$T \equiv \sum_{(\eta)} \eta_1^l \eta_2^l \ldots \eta_m^l \pmod p.$$

Тъй като $0<l<s$ и следователно $l \not\equiv 0 \pmod p$, от (8) ще следва, че $\sum_{i=1}^{s} \eta_i^l \equiv 0 \pmod p$, където η_i пробягват всичките решения на биномното сравнение (6), разглеждани по модул p. И така от направеното предположение, че е в сила (11) при произволен избор на s-тите корени от единицата по модул p, следва сравнението

$$T \equiv 0 \pmod p.$$

От друга страна обаче, съгласно (10) и условието

$$a_i \not\equiv 0 \pmod p, \quad i=1, 2, \ldots, m,$$

трябва да имаме

$$T \not\equiv 0 \pmod p.$$

По такъв начин доказахме, че съществуват числа $\eta_1, \eta_2, \ldots, \eta_m$, които са решения на (6) и за които е в сила сравнението

$$\eta_1 a_1 + \eta_2 a_2 + \ldots + \eta_m a_m \equiv 0 \pmod p. \tag{12}$$

Остава да отбележим, че, както е известно от елементарната теория на числата, от $\eta^s \equiv 1 \pmod p$, където $s = \frac{p-1}{n}$, следва съществуването на число ξ, за което $\eta \equiv \xi^n \pmod p$. По такъв начин се убеждаваме, че сравнението (12) може да се запише във вида

$$a_1 \xi_1^n + a_2 \xi_2^n + \ldots + a_m \xi_m^n \equiv 0 \pmod p, \tag{13}$$

където $\xi_1 \not\equiv 0 \pmod p$, $\xi_2 \not\equiv 0 \pmod p, \ldots, \xi_m \not\equiv 0 \pmod p$. С това теоремата е доказана.

От доказателството се вижда, че резултатът от теорема 1 може да се формулира по-общо, като вместо сравнения от вида (1) се разглежда съответно хомогенно уравнение в произволно крайно поле $GF(p^\lambda)$ с характеристика $p>2$ и p^λ на брой елементи. В приведеното доказателство използвахме теоремата на Ферма и по същество (макар и в неявна форма) — цикличността на мултипликативната група на простото поле $Z_p = GF(p)$. Тези факти, както е добре известно, се пренасят и за произволно поле на Галуа $GF(p^\lambda)$. Очевидно е, че останалите разсъждения и пресмятания ще функционират без изменение и в случая на произволно крайно поле с характеристика $p>2$. И така в сила е следната

Теорема 2. Ако $a_1, a_2, \ldots, a_m$ са различни от нула елементи на крайното поле $GF(p^\lambda)$ с характеристика $p>2$ и n е естествено число, за което $(n, p^\lambda - 1) < m$, уравнението

$$a_1 x_1^n + a_2 x_2^n + \ldots + a_m x_m^n = 0$$

при $m / p^\lambda - 1$ ще има поне едно абсолютно ненулево решение в $GF(p^\lambda)$ (т. е. такова решение $(x_1, x_2, \ldots, x_m)$, за което $x_i \in GF(p^\lambda)$, $x_i \neq 0$ за всяко $i=1, 2, \ldots, m$).

Ще покажем, че условието $m / p-1$ от теорема 1 (а с това и условието $m / p^\lambda - 1$ от теорема 2) е съществено. За целта ще разгледаме няколко примера.

Пример 1. От $x_1 x_2 x_3 \not\equiv 0 \pmod 5$ следва

$$x_1^2 + x_2^2 + x_3^2 \not\equiv 0 \pmod 5.$$

С други думи, сравнението (1) при $m=3$, $n=2$, $p=5$ и $a_1 = a_2 = a_3 = 1$ няма абсолютно ненулево решение.

Пример 2. От $x_1 x_2 x_3 x_4 \not\equiv 0 \pmod 7$ следва

$$2x_1^3 + x_2^3 + x_3^3 + x_4^3 \not\equiv 0 \pmod 7.$$

С други думи, сравнението (1) при $m=4$, $n=3$, $p=7$ и $a_1=2$, $a_2=a_3=a_4=1$ няма абсолютно ненулево решение.

Пример 3. От $x_1 x_2 x_3 x_4 x_5 \not\equiv 0 \pmod{13}$ следва

$$x_1^4 + x_2^4 + x_3^4 - x_4^4 + x_5^2 \not\equiv 0 \pmod{13}.$$

С други думи, сравнението (1) при $m=5$, $n=4$, $p=13$ и $a_1=a_2=a_3=1$, $a_4=a_5=-1$ няма абсолютно ненулево решение.

Във верността на твърденията от горните три примера се убеждаваме чрез непосредствена проверка.

Пример 4. При $n=\frac{p-1}{2}$ и $\frac{p-1}{2}<m<p-1$, където m е нечетно число, сравнението (1) за $a_1=a_2=\ldots=a_m=1$ няма абсолютно ненулево решение.

Наистина, ако $x_i \not\equiv 0 \pmod p$, $i=1, 2, \ldots, m$, и

$$x_1^n + x_2^n + \ldots + x_m^n \equiv 0 \pmod p,$$

където $n=\frac{p-1}{2}$, то $x_i^n \equiv \varepsilon_i = \pm 1 \pmod p$ и следователно бихме имали

$$\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_m \equiv 0 \pmod p.$$

Но тъй като

$$|\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_m| \leqq m < p,$$

би трябвало да е в сила равенството

$$\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_m = 0 \quad (\varepsilon_i = \pm 1,\ i=1, 2, \ldots, m),$$

което при нечетно m очевидно е невъзможно.

Да отбележим накрая две елементарни следствия от теорема 1.

Следствие 1. Ако p е просто число от вида $p=6k+1$ и A, a, b са цели числа, които не се делят на p, ще съществуват два квадратични остатъка x и y по модул p, така че $A \equiv ax + by \pmod p$.

Следствие 2. Ако p е просто число от вида $p=12k+1$ и A, a, b, c са цели числа, неделящи се на p, ще съществуват три кубични остатъка по модул p: x, y, z, така че да е в сила сравнението $A \equiv ax + by + cz \pmod p$.

Първото следствие се получава от теорема 1 при $n=2$ и $m=3$, а второто — при $n=3$ и $m=4$. За достатъчно големи стойности на простия модул p първото от тези следствия може да се получи и от

цитирания резултат на Хурвиц. В цялата си общност обаче теорема 1 (и съответно теорема 2) не може да се докаже с методите, приложени в цитираните статии [1]—[7], както личи от приведения по-горе пример 4.

ЛИТЕРАТУРА

1. Hurwitz, A: Über die Kongruenz $ax^l+by^l+cz^l\equiv 0 \pmod p$. Journ. für die reine und angew. Math. **136** (1909), 272—292.
2. Hua, L., Vandiver, H.: On the existence of solutions of certain equations in a finite field. Proc. of Nat. Acad. of Sc., **34** (1948).
3. Diskson, L. E.: Linear groups with an exposition of the Galois field theory. Dover, 1958.
4. Chowla, S.: On the congruence $\sum_{i=1}^{s} a_i x_i^k \equiv 0 \pmod p$. J. Ind. Math. Soc., **25** (1961), 47—48.
5. Segre, B.: Arithmetische Eigenschaften von Galois-Räumen. I. Math. Ann., **154** (1964), 195—256.
6. Stevens, H.: Linear homogeneous equations over finite rings. Canad J. Math., **16** (1964), 532—538.
7. Tietäväinen, A.: On the non-trivial solvability of some equations and systems of equations in finite fields. Ann. Acad. Sc. Fennicae (1965).

Постъпила на 24. XI. 1970 г.

QUELQUES PROPRIÉTÉS DES ÉQUATIONS HOMOGÈNES EN CORPS FINIS

K. Dočev et D. Dimitrov

(RÉSUMÉ)

Soit $GF(p^\lambda)$ un corps fini à caractéristique $p>2$. Ou démontre que l'équation

$$a_1 x_1^n + a_2 x_2^n + \ldots + a_m x_m^n = 0,$$

où $a_i \in GF(p^\lambda)$ et $a_i \neq 0$ pour $i=1, 2, \ldots, m$, $(n, p^\lambda-1)<m$ et $m \mid p^\lambda-1$ admet une solution $(x_1, \ldots, x_m)$, telle que $x_i \in GF(p^\lambda)$ et $x_i \neq 0$, $i=1, \ldots, m$.

La condition $m \mid p^\lambda-1$ est essentielle pour tout nombre premier $p>2$.