

Подготовка за МОМ2019

Сравнения по прост модул с едно неизвестно

Да разгледаме сравнения от вида $f(x) \equiv 0 \pmod{p}$, където p е просто число, а $f(x) = c_0x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n$ е полином с цели коефициенти, като $(c_0, p) = 1$.

Лема 1. Сравнението $c_0x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n \equiv 0 \pmod{m}$ е еквивалентно на сравнение от вида

$$x^n + b_1x^{n-1} + \dots + b_{n-1}x + b_n \equiv 0 \pmod{m}.$$

Доказателство: Достатъчно да умножим двете страни на даденото сравнение с число от класа, който е решение на сравнението $c_0y \equiv 1 \pmod{p}$. Тъй като $(c_0, p) = 1$, такова решение има.

Лема 2. Ако $f(x)$ и $g(x)$ са полиноми с цели коефициенти, то

$$f(x) \equiv 0 \pmod{p} \iff f(x) - (x^p - x)g(x) \equiv 0 \pmod{p}.$$

Доказателство: Достатъчно да отбележим, че $x^p - x \equiv 0 \pmod{p}$ за всяко цяло x съгласно теоремата на Ферма.

Лема 3. Ако степента на $f(x)$ е по-голяма или равна на p и

$$f(x) = (x^p - x)g(x) + r(x),$$

където степента на $r(x)$ е по-малка от p , то

$$f(x) \equiv 0 \pmod{p} \iff r(x) \equiv 0 \pmod{p}.$$

Доказателство: Следва от Лема 2.

Лема 4. Ако полиномите с цели коефициенти $f(x)$, $g(x)$, $h(x)$ и $r(x)$ са такива, че $f(x) = g(x)h(x) + r(x)$ и всички коефициенти на $r(x)$ се делят на p , то всяко число, което удовлетворява сравнението $f(x) \equiv 0 \pmod{p}$, удовлетворява и поне едно от сравненията $g(x) \equiv 0 \pmod{p}$ и $h(x) \equiv 0 \pmod{p}$.

Доказателство: Ясно е, че $r(x) \equiv 0 \pmod{p}$ за всяко x . Тогава от $f(x_0) \equiv 0 \pmod{p}$ следва, че $g(x_0)h(x_0) \equiv 0 \pmod{p}$, т.е. p дели произведението $g(x_0)h(x_0)$, т.е. p дели поне едно от числата $g(x_0)$ и $h(x_0)$. Обратно, ако x_0 е решение на някое от сравненията $g(x) \equiv 0 \pmod{p}$ и $h(x) \equiv 0 \pmod{p}$, то p дели $g(x_0)h(x_0)$, т.е.

$$f(x_0) = g(x_0)h(x_0) + r(x_0) \equiv 0 \pmod{p}.$$

Теорема 1. Сравнението

$$f(x) = c_0x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n \equiv 0 \pmod{p},$$

където $(c_0, p) = 1$, има не повече от n решения.

Доказателство: Ще проведем индукция по степента на сравнението n . При $n = 1$ твърдението е вярно. Нека $n \geq 2$ и твърдението е вярно за сравнения от степен $n - 1$.

Ако $f(x) \equiv 0 \pmod{p}$ няма решение, твърдението е вярно. Нека x_0 е цяло число, за което $f(x_0) \equiv 0 \pmod{p}$ и да представим $f(x)$ във вида

$$f(x) = (x - x_0)g(x) + f(x_0)$$

(това представяне също се нарича Теорема на Безу). Полиномът $g(x) = b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-2}x + b_{n-1}$ е от степен $n-1$ и очевидно $c_0 = b_0$, т.е. $(b_0, p) = 1$.

Съгласно Лема 4 всяко решение на $f(x) \equiv 0 \pmod{p}$ е решение на $g(x) \equiv 0 \pmod{p}$ или на $x - x_0 \equiv 0 \pmod{p}$. От индукционното предположение следва, че $g(x) \equiv 0 \pmod{p}$ има най-много $n-1$ решения, а линейното сравнение $x - x_0 \equiv 0 \pmod{p}$ има единствено решение $x \equiv x_0 \pmod{p}$. Следователно сравнението $f(x) \equiv 0 \pmod{p}$ има не повече от $(n-1) + 1 = n$ решения.

Да отбележим, че твърдението на Теорема 1 не е вярно за съставен модул. Например сравнението $x^2 - 3x + 2 \equiv 0 \pmod{6}$ е то втора степен и има четири решения $\bar{1}, \bar{2}, \bar{4}, \bar{5}$.

Следствие 1. Ако сравнението

$$f(x) = c_0x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n \equiv 0 \pmod{p}$$

има повече от n решения, то всички коефициенти се делят на p .

Доказателство: От Теорема 1 следва, че p дели c_0 . Тогава сравнението е еквивалентно на

$$c_1x^{n-1} + \dots + c_{n-1}x + c_n \equiv 0 \pmod{p},$$

за което можем отново да приложим Теорема 1 и т.н.

Теорема 2. (Теорема на Лагранж) Нека $f(x) = x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n$ е полином с цели коефициенти, $(c_n, p) = 1$ и $p-1 \geq n$. Сравнението $f(x) \equiv 0 \pmod{p}$ има точно n решения тогава и само тогава, когато всички коефициенти на остатъка при делението на $x^{p-1} - 1$ на $f(x)$ се делят на p .

Доказателство: Нека $x^{p-1} - 1 = f(x)g(x) + r(x)$, където степента на r е по-малка от n .

(Достатъчност) Нека всички коефициенти на $r(x)$ се делят на p и сравненията $f(x) \equiv 0 \pmod{p}$ и $g(x) \equiv 0 \pmod{p}$ имат съответно по s и t решения.

Сравнението $x^{p-1} - 1 \equiv 0 \pmod{p}$ има $p-1$ решения съгласно Теоремата на Ферма. Съгласно Лема 4, всяко от тези решения е решение на поне едно от сравненията $f(x) \equiv 0 \pmod{p}$ и $g(x) \equiv 0 \pmod{p}$. Следователно $s + t \geq p-1$. От друга страна, сравнението $g(x) \equiv 0 \pmod{p}$ е от степен $p-1-n$ и коефициентът пред най-високата степен е 1. Тогава от Теорема 1 следва, че $g(x) \equiv 0 \pmod{p}$ има най-много $p-1-n$ решения, т.е. $t \leq p-1-n$. Следователно

$$s \geq p-1-t \geq p-1-(p-1-n) = n.$$

Но $s \leq n$ според Теорема 1 и окончателно получаваме $s = n$.

(Необходимост) Нека $f(x) \equiv 0 \pmod{p}$ има точно n решения. Ако x_0 е едно от тях, то от $f(x_0) \equiv 0 \pmod{p}$ и $(c_n, p) = 1$ следва, че $(x_0, p) = 1$. Тогава по Теоремата на Ферма имаме $x_0^{p-1} \equiv 1 \pmod{p}$ и оттук

$$r(x_0) \equiv x_0^{p-1} - 1 + f(x_0)g(x_0) \equiv 0 \pmod{p}.$$

Следователно сравнението $r(x) \equiv 0 \pmod{p}$ има поне n решения (решенията на $f(x) \equiv 0 \pmod{p}$), което съгласно Следствие 1 означава, че всички коефициенти на $r(x)$ се делят на p .

Задача 1. Нека $p > 3$ е просто число и $1 + \frac{1}{2} + \dots + \frac{1}{p} = \frac{r}{ps}$, където $r, s \in \mathbb{N}$ и $(r, s) = 1$. Да се докаже, че $p^3 | r - s$.

Решение. Да разгледаме полинома $f(x) = (x-1)(x-2)\dots(x-(p-1)) - (x^{p-1} - 1)$. Тъй като $f(x) \equiv 0 \pmod{p}$ за всяко x , а $\deg(f) = p-2$, всички коефициенти на $f(x)$ се делят на p , т.е. $a_{p-2} \equiv a_{p-3} \equiv \dots \equiv a_1 \equiv a_0 \equiv 0 \pmod{p}$, където $f(x) = a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \dots + a_1x + a_0$.

Да отбележим, че $a_0 = f(0) = (p-1)! + 1$. Тогава при $x = p$ получаваме равенството $a_{p-2}p^{p-2} + a_{p-3}p^{p-3} + \dots + a_1p + a_0 = (p-1)! + 1 + p^{p-1} = a_0 + p^{p-1}$, откъдето $a_{p-2}p^{p-2} + a_{p-3}p^{p-3} + \dots + a_1p \equiv 0 \pmod{p^3}$. Следователно $a_1p \equiv 0 \pmod{p^3}$, откъдето

$$p^2|a_1 = -(p-1)! \sum_{i=1}^{p-1} \frac{1}{i} = -(p-1)! \left(\frac{r}{ps} - \frac{1}{p} \right).$$

От последното лесно следва, че $p^3|r - s$.

Задача 2. Нека $m, n \in \mathbb{N}$, $m, n \geq 2$. Да се докаже, че ако $a^n \equiv 1 \pmod{m}$ за всяко $a = 1, 2, \dots, n$, то $(m, n) = (p, p-1)$ за някое просто число p .

Решение. Нека p е прост делител на m . Тогава $p > n$, защото в противен случай условието не е изпълнено за $a = p$. Да разгледаме полинома $f(x) = (x-1)(x-2)\dots(x-n) - (x^n - 1)$. Имаме $f(a) = a^n - 1 \equiv 0 \pmod{p}$ за всяко $a = 1, 2, \dots, n$. Следователно сравнението $f(x) \equiv 0 \pmod{p}$ от степен $n-1$ има поне n решения, което означава, че всички коефициенти на $f(x)$ се делят на p .

В частност, p дели старшия коефициент на $f(x)$, т.е. $p|1 + 2 + \dots + n = \frac{n(n+1)}{2}$. Оттук и от $p > n$ следва, че $p = n + 1$. Нещо повече, от последното равенство следва, че m няма други прости делители, т.е. $m = p^a$, където a е естествено число. Ще докажем, че $a = 1$.

Да допуснем, че $a > 1$ и да разгледаме сравнението $n^n \equiv 1 \pmod{m} \iff (p-1)^{p-1} - 1 \equiv 0 \pmod{p^a}$. Тогава $0 \equiv (p-1)^{p-1} - 1 \equiv -(p-1)p \equiv p \pmod{p^2}$, което е невъзможно.

Задача 3. Да се докаже, че не съществува неконстантен полином $f(x)$, който да приема само прости стойности за всички достатъчно големи цели стойности на x .

Решение. Да допуснем противното и нека $f(x)$ е неконстантен полином, който приема само прости стойности за всички достатъчно големи цели стойности на x . Нека $f(y) = p$ за някое $y \in \mathbb{N}$ и някое просто p . Да разгледаме полинома $g(t) = f(y + tp)$. Ясно е, че $\deg(g) = \deg(f)$, в частност g също е неконстантен. Освен това имаме $g(t) \equiv f(y) \equiv 0 \pmod{p}$, което означава, че за всички достатъчно големи t ще имаме $g(t) = p$. Оттук обаче следва, че $g(t)$ е константата p , което е противоречие.

Задача 4. Нека p е просто число, а k е естествен делител на $p-1$. Да се докаже, че x^k приема точно $\frac{p-1}{k} + 1$ различни стойности по модул p , когато x се мени от 0 до $p-1$.

Решение. Нека различните остатъци, които приема x^k по модул p са $0, y_1, y_2, \dots, y_s$. Да забележим, че $s \leq \frac{p-1}{k}$, тъй като y_1, y_2, \dots, y_s са различни решения на $x^{\frac{p-1}{k}} - 1 \equiv 0 \pmod{p}$. Нека сега $A_i, 1 \leq i \leq s$, е множеството от остатъци, за които $x^k \equiv y_i \pmod{p}$. Тогава $|A_i| \leq k$ за всяко i . Тъй като $|A_1| + |A_2| + \dots + |A_s| = p-1$, заключаваме, че $s = \frac{p-1}{k}$ и $|A_i| = k$ за всяко k .

Задача 5. (RMM 2016) Полином от вида $f(n) = n^3 + bn^2 + cn + d$, където b, c и d са цели, а n се мени в множеството от целите числа, се нарича кубичен.

а) Да се докаже, че съществува кубичен полином, за който само числата $f(2015)$ и $f(2016)$ са точни квадрати.

б) За всеки полином от а) да се определят всички възможни стойности на произведението $f(2015)f(2016)$.

Решение. Тъй като трансляция на променливата n не променя интересувашите ни свойства, можем да работим с $f(0)$ и $f(1)$ вместо с $f(2015)$ и $f(2016)$.

а) Полиномът $f(n) = n^3 - n^2 + n$ има исканото свойство.

б) Отговор: Единствената възможност е $f(0)f(1) = 0$.

Нека $f(n)$ има исканите свойства и $f(0) = p^2$, $f(1) = q^2$ са точни квадрати. Да разгледаме правата $y = (q-p)x+p$, която минава през точките $(0, p)$ и $(1, q)$ (т.е. тази права пресича графиката на функцията $y^2 = x^3 + bx^2 + cx + d$ в тези точки). Тъй като уравнението

$$[(q-p)x+p]^2 = x^3 + bx^2 + cx + d$$

има и трети корен x_0 (освен 0 и 1), да разгледаме този корен. От формулите на Виет следва, че $x_0 = (q-p)^2 - b - 1$ е цяло число, а тогава и числото $y_0 = (q-p)x_0 + p$ е цяло (всъщност точката (x_0, y_0) е трета пресечна точка на нашата права и графиката на $y^2 = x^3 + bx^2 + cx + d$). Следователно $x_0 = 0$ или 1, защото в противен случай имаме трети точен квадрат, който е стойност на нашия полином. Получаваме $(q-p)^2 = b+1$ или $(q-p)^2 = b+2$.

Същото разсъждение, но за правата през точките $(0, -p)$ и $(1, q)$, дава $(q+p)^2 = b+1$ или $(q+p)^2 = b+2$. Тъй като $(q-p)^2$ и $(q+p)^2$ имат еднаква четност, те трябва да са равни, откъдето веднага получаваме $pq = 0$.