4.1 Сравнения от произволна степен с едно неизвестно. Теорема на Лагранж. Теорема на Уилсън

Нека $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ е полином с цели коефициенти и $m > 1$ е цяло число.

Определение 4.1.1. Ако c е цяло число, за което $f(c) \equiv 0 \pmod{m}$, то ще казваме, че c е *удовлетворява* сравнението

$$f(x) \equiv 0 \pmod{m}. \tag{4.1}$$

Ясно е, че ако числото c удовлетворява (4.1), то всяко число x_0, което е сравнимо с c по модул m също го удовлетворява. Това следва от основните свойства на сравненията. Следователно, сравнението (4.1) се удовлетворява от всяко x, за което $x \equiv c \pmod{m}$. В този случай решение на (4.1) ще наричаме класът с представител c, което ще записваме

$$x \equiv c \pmod{m}.$$

Различните решения на (4.1) са различните класове по модул m, елементите на които удовлетворяват (4.1).

Ако $a_0 \not\equiv 0 \pmod{m}$, то сравнението (4.1) има степен n.

Определение 4.1.2. Ако $h(x)$ и $q(x)$ са два полинома от една и съща степен, то сравнението $h(x) \equiv q(x) \pmod{m}$ означава, че коефициентите пред равните степени на x в полиномите $h(x)$ и $q(x)$ са сравними по модул m. Тогава за всяко цяло число a е изпълнено $h(a) \equiv q(a) \pmod{m}$.

Лема 4.1.1. *Ако числото c удовлетворява сравнението от n-та степен*

$$f(x) \equiv 0 \pmod{m},$$

то съществува такъв полином $g(x)$ от $(n-1)$-ва степен, че

$$f(x) \equiv (x - c)g(x) \pmod{m}.$$

Доказателство. Разделяме полинома $f(x)$ на $x - c$ и получаваме

$$f(x) = (x - c)g(x) + r,$$

където $r = f(c)$.

Ясно е, че $g(x)$ е полином от $(n-1)$-ва степен. Тъй като c е решение на сравнението (4.1), то $f(c) \equiv 0 \pmod{m}$, т.е. $r \equiv 0 \pmod{m}$.

Тогава

$$f(x) \equiv (x-c)g(x) \pmod{m}.$$

□

Теорема 4.1.2 (Лагранж). *Нека p е просто число и*

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

е полином с цели коефициенти, където $p \nmid a_0$. Тогава сравнението

$$f(x) \equiv 0 \pmod{p} \tag{4.2}$$

има най-много n различни решения.

Доказателство. Допускаме противното, т.е. (4.2) има повече от n различни решения и нека $c_1, c_2, \ldots, c_n, c_{n+1}$ са такива решения, т.е. $c_i \not\equiv c_j \pmod{p}$ при $i \neq j$. Съгласно Лема 4.1.1 е изпълнено сравнението

$$f(x) \equiv (x-c_1)f_1(x) \pmod{p}, \tag{4.3}$$

където $f_1(x)$ е полином от $n-1$-ва степен. Тогава

$$f(c_2) \equiv (c_2-c_1)f_1(c_2) \pmod{p}.$$

Но $f(c_2) \equiv 0 \pmod{p}$, защото c_2 е решение на (4.2). Следователно

$$(c_2-c_1)f_1(c_2) \equiv 0 \pmod{p}.$$

Тъй като $p \nmid c_2 - c_1$ (имаме $c_i \not\equiv c_j \pmod{p}$), то $p \mid f_1(c_2)$, т.е.

$$f_1(c_2) \equiv 0 \pmod{p}.$$

Следователно c_2 е решение на сравнението

$$f_1(x) \equiv 0 \pmod{p}.$$

Прилагайки отново лемата получаваме

$$f_1(x) \equiv (x-c_2)f_2(x) \pmod{p}. \tag{4.4}$$

Заместваме $f_1(x)$ в (4.3) с полинома получен в (4.4) и получаваме

$$f(x) \equiv (x-c_1)(x-c_2)f_2(x) \pmod{p},$$

където $f_2(x)$ е полином от $(n-2)$-ра степен.

По този начин след n-тата стъпка ще получим

$$f(x) \equiv a_0(x-c_1)(x-c_2)\dots(x-c_n) \pmod{p}. \tag{4.5}$$

Числото c_{n+1} е решение на (4.2), т.е. $f(c_{n+1}) \equiv 0 \pmod{p}$. Заместваме c_{n+1} в (4.5) и получаваме

$$f(c_{n+1}) \equiv a_0(c_{n+1}-c_1)(c_{n+1}-c_2)\dots(c_{n+1}-c_n) \pmod{p}$$

или

$$a_0(c_{n+1}-c_1)(c_{n+1}-c_2)\dots(c_{n+1}-c_n) \equiv 0 \pmod{p}.$$

Тъй като p е просто число, то съгласно Следствие 1.4.6, числото p ще дели поне едно от числата a_0, $c_{n+1}-c_1$, $c_{n+1}-c_2$, $\dots$, $c_{n+1}-c_n$. Така достигаме до противоречие с направеното допускане. □

Забележка: Условието модулът в сравнението (4.2) да е просто число е съществено. Например сравнението

$$x^2 - 1 \equiv 0 \pmod{12}$$

има четири различни решения

$$x \equiv \pm 1 \pmod{12}, \quad x \equiv \pm 5 \pmod{12}.$$

Въпросът за броя на решенията на сравнения при съставен модул е доста по-сложен и няма да се спираме на него.

Ще приложим Теорема 4.1.2, за да докажем известната теорема на Уилсън.

Теорема 4.1.3 (Уилсън). *Естественото число $p > 1$ е просто тогава и само тогава, когато е в сила сравнението*

$$(p-1)! + 1 \equiv 0 \pmod{p}. \tag{4.6}$$

Доказателство. Първо ще докажем достатъчността на условието на теоремата. Нека е изпълнено сравнението (4.6) и $d < p$ е произволен положителен делител на числото p. Тогава d участва като множител и в числото

$$(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-2) \cdot (p-1),$$

т.е. $d \mid (p-1)!$. Тъй като $d \mid p$, то $d \mid ((p-1)!+1)$ и следователно $d \mid 1$. Тогава $d = 1$, т.е. p е просто число.

Сега ще докажем необходимостта. Нека p е просто число. Ако $p = 2$, то е изпълнено сравнението $(2-1)! + 1 = 2 \equiv 0 \pmod 2$.

Нека $p > 2$, т.е. p е нечетно просто число. Да разгледаме сравнението $x^{p-1} \equiv 1 \pmod p$ или

$$x^{p-1} - 1 \equiv 0 \pmod p.$$

Съгласно теоремата на Ферма-Ойлер, числата $1, 2, \ldots, p-1$ са $p-1$ на брой различни решения на сравнението (4.1). От Теоремата на Лагранж следва още, че това са всички решения на сравнението. Тогава от Лема 4.1.1 имаме че:

$$x^{p-1} - 1 \equiv (x-1) \cdot (x-2) \cdots [x-(p-1)] \pmod p.$$

В това сравнение полагаме $x = 0$ и получаваме:

$$\begin{aligned} -1 &\equiv (-1) \cdot (-2) \cdots [-(p-1)] \pmod p, \quad \text{т.е.} \\ -1 &\equiv (-1)^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod p. \end{aligned}$$

Тъй като $p-1$ е четно число, то $(-1)^{p-1} = 1$ и получаваме

$$-1 \equiv 1 \cdot 2 \cdots (p-1) \pmod p, \text{ т.е. } (p-1)! + 1 \equiv 0 \pmod p.$$

□

Задачи

4.1.1. Намерете

а) остатъкът от делението на $15!$ с 17;

б) остатъкът от делението на $2 \cdot 26!$ с 29.

4.1.2. Докажете, че ако $p \geq 5$ е нечетно просто число, то е изпълнено сравнението $6(p-4)! \equiv 1 \pmod p$.

4.1.3. Докажете твърденията:

а) цялото число $n > 1$ е просто, тогава и само тогава, когато $(n-2)! \equiv 1 \pmod n$;

б) ако $n > 4$ е съставно, то докажете, че $(n-1)! \equiv 0 \pmod n$.

4.1.4. Докажете, че $18! \equiv -1 \pmod{437}$.

4.1.5. Използвайки теоремата на Уилсън докажете, че за всяко нечетно просто число p е изпълнено сравнението

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$