Сравнения от първа степен с едно неизвестно. Системи сравнения. Китайска теорема за остатъците.

проф. Стефка Буюклиева

1 Сравнения от първа степен с едно неизвестно.

Сравненията с едно неизвестно са еквивалент на алгебричните уравнения и имат вида

$$f(x) \equiv 0 \pmod{n}, \tag{1}$$

където $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ е полином с цели коефициенти, а n е фиксирано естествено число. Търсим всички цели числа, които удовлетворяват това сравнение. Ако $x_0 \in \mathbb{Z}$ е решение и $x_1 \equiv x_0 \pmod{n}$, то $f(x_1) \equiv f(x_0) \equiv 0 \pmod{n}$. Това доказва, че ако едно цяло число x_0 е решение на сравнението (1), то всички числа от класа остатъци с представител x_0 са решения на това сравнение. Затова търсим решенията като класове остатъци по модул n, или

$$\text{търсим } x \equiv ? \pmod{n}.$$

Две сравнения от типа (1) са еквивалентни (или още равносилни), ако имат едни и същи решения. Ясно е, че ако заменим коефициентите на $f(x)$ с техните остатъци по модул n, ще получим сравнение, еквивалентно на (1).

Ще разгледаме по-подробно сравненията от първа степен:

$$ax \equiv b \pmod{n},\ a, b \in \mathbb{Z}. \tag{2}$$

Лема 1. *Ако числата a и n са взаимно прости, то сравнението $ax \equiv b \pmod{n}$ има точно едно решение по модул n.*

Доказателство: Ще докажем, че числата $0, a, 2a, \ldots, (n-1)a$ образуват пълна система остатъци по модул n. За целта трябва да докажем, че $ka \not\equiv la \pmod{n}$ за $0 \leq l < k \leq n-1$. Да допуснем противното, т.е. че $ka \equiv la \pmod{n}$. Тъй като a и n са взаимно прости, можем да съкратим на a. Получаваме, че $k \equiv l \pmod{n}$, и тъй като $k, l \in \{0, 1, \ldots, n-1\}$, то $k = l$ - противоречие.

След като $0, a, 2a, \ldots, (n-1)a$ образуват пълна система остатъци, то за точно едното от тези числа, да кажем ka, е в сила $b \equiv ka \pmod{n}$. Следователно решение на даденото сравнение е класа остатъци с представител k. $\square$

Теорема 2. *Сравнението* $ax \equiv b \pmod{n}$ *има решение тогава и само тогава, когато* $\gcd(a, n) \mid b$.

Доказателство: Нека $d = \gcd(a, n)$, $a = da_1$, $n = dn_1$, $\gcd(a_1, n_1) = 1$. Да допуснем, че x_0 е решение на даденото сравнение. Тогава

$$ax_0 \equiv b \pmod{n} \Rightarrow n \mid ax_0 - b \Rightarrow dn_1 \mid da_1x_0 - b \Rightarrow d \mid da_1x_0 - b \Rightarrow d \mid b.$$

Обратно, нека $d \mid b$ и $b = db_1$. Тогава

$$ax \equiv b \pmod{n} \Leftrightarrow da_1x \equiv db_1 \pmod{dn_1} \Leftrightarrow a_1x \equiv b_1 \pmod{n_1}.$$

Тъй като a_1 и n_1 са взаимно прости, от Лема 1 следва, че сравнението има решение. $\square$

Следствие 3. *Ако* $\gcd(a, n) \mid b$, *точно* $\gcd(a, n)$ *класа остатъци по модул* n *са решения на сравнението (сравнението има* $\gcd(a, n)$ *решения).*

Доказателство: Ще използваме означенията от доказателството на Теорема 2. Понеже a_1 и n_1 са взаимно прости, сравнението $a_1x \equiv b_1 \pmod{n_1}$ има единствено решение по модул n_1. Нека това е класът остатъци с представител r, $0 \leq r \leq n_1 - 1$, т.е. множеството цели числа от вида $n_1q + r$, където q обхожда всички цели числа. Но това множество е обединение на класовете $nq + r, nq + n_1 + r, nq + 2n_1 + r, \ldots, nq + (d-1)n_1 + r$, които са точно d на брой.$\square$

Казваме, че цялото число a е *обратимо по модул* n, когато сравнението $ax \equiv 1 \pmod{n}$ има решение. Решението на това сравнение (когато такова съществува) се бележи с $a^{-1} \pmod{n}$ и се нарича *мултипликативен обратен елемент на* a *по модул* n. Теорема 2 дава критерий за обратимост, формулиран в следващото следствие.

Следствие 4. *Цялото число* a *е обратимо по модул* n *тогава и само тогава, когато* $\gcd(a, n) = 1$.

За пресмятането на мултипликативен обратен се използва разширения алгоритъм на Евклид. Наистина, понеже $\gcd(a, n) = 1$, то съществуват числа x и y, такива че $ax + ny = 1$. Следователно

$$ax + ny \equiv 1 \pmod{n} \Rightarrow ax \equiv 1 \pmod{n}.$$

2 Системи сравнения от първа степен с едно неизвестно. Китайска теорема за остатъците.

Да разгледаме системата сравнения

$$\left|\begin{array}{l} f_1(x) \equiv 0 \pmod{n_1} \\ f_2(x) \equiv 0 \pmod{n_2} \\ \qquad \cdots \\ f_k(x) \equiv 0 \pmod{n_k} \end{array}\right. \tag{3}$$

където $f_i(x)$ са полиноми с цели коефициенти и $n_i \in \mathbb{N}$, $i = 1, 2, \ldots, k$, $k \in \mathbb{N}$.

Ако числото a е решение на системата и $b \equiv a \pmod{\text{НОК}(n_1, n_2, \ldots, n_k)}$, то b също е решение. Наистина от $\text{НОК}(n_1, n_2, \ldots, n_k) \mid (b-a)$ следва, че $n_i \mid (b-a)$ и оттук $b \equiv a \pmod{n_1}$, $i = 1, 2, \ldots, k$. Това показва, че $f_i(b) \equiv f_i(a) \equiv 0 \pmod{n_i}$ за $i = 1, 2, \ldots, k$, т.е. b също е решение. Така че ако числото a е решение на системата (3), всички числа от класа остатъци по модул $\text{НОК}(n_1, n_2, \ldots, n_k)$ с представител a са решения на тази система. Ще смятаме целия клас остатъци за едно решение и ще записваме

$$x \equiv a \pmod{\text{НОК}(n_1, n_2, \ldots, n_k)}.$$

Ако $x \equiv c_i \pmod{n_i}$ е решение на i-тото сравнение, то всяко решение на системата

$$\left|\begin{array}{l} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \qquad \cdots \\ x \equiv c_k \pmod{n_k} \end{array}\right. \tag{4}$$

е решение и на системата (3).

Следващата теорема е популярна под името Китайска теорема за остатъците. Формулирана е в книга на китайския математик Сун Дзъ (около 250 г.), но вероятно е била известна на китайските математици още преди новата ера.

Теорема 5. (Китайска теорема за остатъците) *Ако числата $n_1, n_2, \ldots, n_k$, $k \geq 2$, са две по две взаимно прости, то системата* (4) *има решение.*

Доказателство: Ще докажем теоремата с индукция по броя на сравненията k. При $k = 2$ от теоремата на Безу следва, че съществуват цели числа u и v такива, че $n_1u + n_2v = \gcd(n_1, n_2) = 1$. Да разгледаме числото $c = c_2n_1u + c_1n_2v$. Като заместим в двете сравнения, получаваме

$$c = c_2n_1u + c_1n_2v \equiv c_1n_2v = c_1(1 - n_1u) \equiv c_1 \pmod{n_1},$$

$$c = c_2n_1u + c_1n_2v \equiv c_2n_1u = c_2(1 - n_2v) \equiv c_2 \pmod{n_2}.$$

Следователно c е решение на системата

$$\left|\begin{array}{ll} x \equiv c_1 & (\mathrm{mod}\ n_1) \\ x \equiv c_2 & (\mathrm{mod}\ n_2) \end{array}\right.$$

Да допуснем сега, че твърдението е вярно за система от $k-1$ сравнения и $x \equiv d \pmod{\gcd(n_1, n_2, \ldots, n_{k-1})}$ е решение на тази система. Като използваме, че $\gcd(n_1, n_2, \ldots, n_{k-1}) = n_1 n_2 \cdots n_{k-1}$, понеже числата $n_1, n_2, \ldots, n_{k-1}$ са две по две взаимно прости, свеждаме задачата до система с две сравнения, а именно

$$\left|\begin{array}{ll} x \equiv d & (\mathrm{mod}\ n_1 n_2 \cdots n_{k-1}) \\ x \equiv c_k & (\mathrm{mod}\ n_k) \end{array}\right.$$

Тъй като числата $n_1 n_2 \cdots n_{k-1}$ и n_k също са взаимно прости, то последната система има едно решение по модул $n_1 n_2 \cdots n_{k-1} n_k$, което е решение и на системата (4). □

Да дадем като пример и една задача.

Пример 1. Да се реши системата сравнения

$$\left|\begin{array}{ll} x \equiv 1 & (\mathrm{mod}\ 2) \\ x \equiv 2 & (\mathrm{mod}\ 3) \\ x \equiv 3 & (\mathrm{mod}\ 5) \end{array}\right.$$

Решение: Тъй като 2, 3 и 5 са две по две взаимно прости числа, системата има решение. Решенията на първото сравнение са всички цели числа от вида $x = 2y + 1$. С тях заместваме във второто сравнение и получаваме

$$2y + 1 \equiv 2 \pmod{3} \Rightarrow 2y \equiv 1 \pmod{3}.$$

Това сравнение има решение $y \equiv 2 \pmod{3}$, а това са всички цели числа от вида $y = 3z + 2$. Оттук следва, че числата $x = 2(3z+2) + 1 = 6z + 5$ са решения едновременно на първите две сравнения. Остава да отделим тези от тях, които удовлетворяват и третото сравнение. Като заместим, получаваме

$$6z + 5 \equiv 3 \pmod{5} \Rightarrow z \equiv 3 \pmod{5} \Rightarrow z = 5t + 3,$$

понеже $6 \equiv 1 \pmod{5}$ и $5 \equiv 0 \pmod{5}$. Следователно числата от вида $x = 6(5t+3) + 5 = 30t + 23$ са решения на дадената система, или решението е $x \equiv 23 \pmod{30}$. □

Ще използваме като пример и още една система, вече от четири сравнения.

Пример 2. Да се реши системата сравнения

$$\left|\begin{array}{ll} x \equiv 5 & (\mathrm{mod}\ 13) \\ x \equiv 2 & (\mathrm{mod}\ 17) \\ x \equiv 6 & (\mathrm{mod}\ 9) \\ x \equiv 4 & (\mathrm{mod}\ 7) \end{array}\right.$$

Да представим още едно доказателство на Китайската теорема за остатъците, което ни дава и друг метод за решаване на системи сравнения от вида (4). Нека $M = n_1 n_2 \cdots n_k$, а $M_i = M/n_i$, $i = 1, 2, \ldots, k$. Тъй като $\gcd(n_1, n_2, \ldots, n_k) = 1$, то и $\gcd(M_1, M_2, \ldots, M_k) = 1$. Следователно съществуват цели числа $u_1, u_2, \ldots, u_k$, такива че $u_1 M_1 + u_2 M_2 + \cdots + u_k M_k = 1$. Понеже $n_i \mid M_j$ за $j \neq i$, то $u_i M_i \equiv 1 \pmod{n_i}$, $i = 1, 2, \ldots, k$. Следователно $x = c_1 u_1 M_1 + c_2 u_2 M_2 + \cdots + c_k u_k M_k$ е решение на системата (4), или по-точно

$$x \equiv c_1 u_1 M_1 + c_2 u_2 M_2 + \cdots + c_k u_k M_k \pmod{M}.$$

Можем да намираме числата $u_1, u_2, \ldots, u_k$ и независимо едно от друго, като решения съответно на сравненията $M_i x \equiv 1 \pmod{n_i}$, $i = 1, 2, \ldots, k$.

Да се върнем към Пример 1. В случая $M = 30$, $M_1 = 15$, $M_2 = 10$, $M_3 = 6$. Търсим числа u_1, u_2, u_3, такива че $15u_1 + 10u_2 + 6u_3 = 1$. Тъй като $-45 + 40 + 6 = 1$, можем да вземем $u_1 = -3, u_2 = 4, u_3 = 1$. Тогава решението на системата е

$$x \equiv -45 + 80 + 18 = 53 \equiv 23 \pmod{30}.$$

За Пример 2 $M = 13923$, $M_1 = 1071$, $M_2 = 819$, $M_3 = 1547$, $M_4 = 1989$. Как да решим уравнението $1071u_1 + 819u_2 + 1547u_3 + 1989u_4 = 1$? Можем да използваме метода, представен в Част **??** на Глава 3. Но в случая по ефективно е да подходим по друг начин, като използваме съображенията от второто доказателство на китайската теорема. Ще намерим числа u_1, u_2, u_3, u_4 като решения съответно на сравненията $1071x \equiv 1 \pmod{13}$, $819x \equiv 1 \pmod{17}$, $1547x \equiv 1 \pmod{9}$, $1989x \equiv 1 \pmod{7}$. Да решим поотделно тези сравнения.

$$\begin{array}{rlrlrl} 1071x \equiv 1 & (\mathrm{mod}\ 13) & \Rightarrow 5x \equiv 1 & (\mathrm{mod}\ 13) & \Rightarrow x \equiv 8 & (\mathrm{mod}\ 13), \\ 819x \equiv 1 & (\mathrm{mod}\ 17) & \Rightarrow 3x \equiv 1 & (\mathrm{mod}\ 17) & \Rightarrow x \equiv 6 & (\mathrm{mod}\ 17), \\ 1547x \equiv 1 & (\mathrm{mod}\ 9) & \Rightarrow 8x \equiv 1 & (\mathrm{mod}\ 9) & \Rightarrow x \equiv 8 & (\mathrm{mod}\ 9), \\ 1989x \equiv 1 & (\mathrm{mod}\ 7) & \Rightarrow x \equiv 1 & (\mathrm{mod}\ 7). & & \end{array}$$

Можем да вземем $u_1 = 8$, $u_2 = 6$, $u_3 = 8$, $u_4 = 1$. Следователно

$$x \equiv 5 \cdot 8 \cdot 1071 + 2 \cdot 6 \cdot 819 + 6 \cdot 8 \cdot 1547 + 4 \cdot 1 \cdot 1989 = 134880 \equiv 9573 \pmod{13923}$$

е решение на системата от Пример 2.

3 Приложение на китайската теорема за остатъците в криптографията

Ще представим и едно от приложенията на китайската теорема за остатъците. Нека K е някаква тайна (или криптографски ключ), представена във вид на естествено число, която трябва да се съхранява в група от k човека. При това се изисква всеки от тях да има някаква информация за ключа, така че всеки s човека ($s \leq k$), събрани заедно, да могат да използват своята информация и да възстановят ключа, но никоя група от по-малко от s човека не може да направи това. Такива конфигурации се наричат *схеми за разпределение на тайната* (SSS – Secret Sharing Schemes). Ето как се осъществява тази схема.

Да изберем множество от естествени числа $\{p, d_1, d_2, \ldots, d_k\}$, такова че:

1. $p > K$,
2. $d_1 < d_2 < \cdots < d_k$,
3. $\gcd(p, d_i) = 1$, $i = 1, 2, \ldots, k$,
4. $\gcd(d_i, d_j) = 1$ за $i \neq j$,
5. $d_1 d_2 \cdots d_s > p \cdot d_{k-s+2} \cdot d_{k-s+3} \cdots d_k$.

Последното изискване означава, че произведението на кои да е s от числата е по-голямо от p пъти произведението на най-големите $s-1$ числа. Нека $D = d_1 d_2 \cdots d_s$. Тогава числото D/p е по-голямо от произведението на които и да е $s-1$ от числата d_i.

Да изберем сега случайно естествено число r в интервала $[0, \lfloor D/p \rfloor - 1]$ и да пресметнем $K' = K + rp$. За полученото число K' са в сила неравенствата $0 < K' < D$. Между участниците в схемата се разпределят остатъците K_i при делението на K' на d_i, $i = 1, 2, \ldots, k$, т.е. $K_i \equiv K' \pmod{d_i}$.

Пример 3. Нека $K = 5$, $k = 3$, $s = 2$. Това означава, че схемата е между трима човека, като всеки двама от тях трябва да могат да определят ключа, но никой от тези трима не може да 'отключи' тайната сам. Избираме $p = 7$, $d_1 = 11$, $d_2 = 13$, $d_3 = 17$. След проверка се уверяваме, че тези числа удовлетворяват исканите свойства. В случая $D = 11 \cdot 13 = 143$. Да изберем случайно цяло число в интервала $[0, \lfloor 143/7 \rfloor - 1] = [0, 19]$, например 2. Тогава

$$K' = 5 + 2 \cdot 7 = 19, \;\; K_1 = 19 \mod 11 = 8, \;\; K_2 = 19 \mod 13 = 6, \;\; K_3 = 19 \mod 17 = 2.$$

Всеки две от тези числа могат да възстановят ключа. Например за K_1 и K_3 имаме

$$K' \equiv 8 \pmod{11}, \quad K' \equiv 2 \pmod{17}.$$

Като приложим китайската теорема за остатъците намираме решение на тази система сравнения, а именно $K' = 19$, и оттук $K = K' - r \cdot p = 5$.

Задачи

Задача 1. Да се решат системите сравнения:

$$a) \left| \begin{array}{lll} x \equiv 1 & (\mathrm{mod}\ 4) \\ x \equiv 2 & (\mathrm{mod}\ 7) \\ x \equiv 5 & (\mathrm{mod}\ 9) \end{array} \right. \qquad b) \left| \begin{array}{lll} x \equiv 2 & (\mathrm{mod}\ 11) \\ x \equiv 3 & (\mathrm{mod}\ 15) \\ x \equiv 5 & (\mathrm{mod}\ 9) \\ x \equiv 4 & (\mathrm{mod}\ 7) \end{array} \right. \qquad c) \left| \begin{array}{lll} x \equiv 24 & (\mathrm{mod}\ 13) \\ x \equiv 52 & (\mathrm{mod}\ 15) \\ x \equiv -1 & (\mathrm{mod}\ 20) \end{array} \right.$$