

A KÍNAI MARADÉKTÉTEL ALKALMAZÁSAI

Waldhauser Tamás

SZTE Bolyai Intézet

2023. március 21.

Kínai maradéktétel

Tétel

Tekintsük az alábbi kongruenciarendszert.

$$\left. \begin{array}{l} x \equiv c_1 \pmod{m_1} \\ \vdots \\ x \equiv c_k \pmod{m_k} \end{array} \right\}$$

- Ha a modulusok páronként relatív prímek, akkor a c_1, \dots, c_k számoktól függetlenül mindig van megoldás.
- Modulo $m_1 \cdot \dots \cdot m_k$ egyetlen megoldás van.
- A megoldás leírható egy egyszerű képlettel a c_1, \dots, c_k paraméterek függvényében.

Kínai maradéktétel

Oldjuk meg az alábbi két kongruenciarendszert.

$$\left. \begin{aligned} x &\equiv 1 \pmod{4} \\ x &\equiv 0 \pmod{5} \end{aligned} \right\}$$

megoldás: $x \equiv 5 \pmod{20}$

$$\left. \begin{aligned} x &\equiv 0 \pmod{4} \\ x &\equiv 1 \pmod{5} \end{aligned} \right\}$$

megoldás: $x \equiv 16 \pmod{20}$

Állítás

Ekkor az

$$\left. \begin{aligned} x &\equiv c_1 \pmod{4} \\ x &\equiv c_2 \pmod{5} \end{aligned} \right\}$$

paraméteres kongruenciarendszer megoldása:

$$x \equiv 5c_1 + 16c_2 \pmod{20}.$$

Ellenőrzés

$$5c_1 + 16c_2 \equiv 1 \cdot c_1 + 0 \cdot c_2 \equiv c_1 \pmod{4} \checkmark$$

$$5c_1 + 16c_2 \equiv 0 \cdot c_1 + 1 \cdot c_2 \equiv c_2 \pmod{5} \checkmark$$

„Kínai számrendszer”

Tetszőleges $c_1 \in \{0, 1, 2, 3\}$ és $c_2 \in \{0, 1, 2, 3, 4\}$ esetén van megoldása az alábbi kongruenciarendszernek, és a megoldás modulo 20 egyértelműen meghatározott:

$$\left. \begin{array}{l} x \equiv c_1 \pmod{4} \\ x \equiv c_2 \pmod{5} \end{array} \right\}.$$

Tehát egyetlen 0 és 19 közé eső megoldás van; jelölje ezt $f(c_1, c_2)$.

(c_1, c_2)						$f(c_1, c_2)$				
0,0	0,1	0,2	0,3	0,4		0	16	12	8	4
1,0	1,1	1,2	1,3	1,4	→	5	1	17	13	9
2,0	2,1	2,2	2,3	2,4		10	6	2	18	14
3,0	3,1	3,2	3,3	3,4		15	11	7	3	19

„Kínai számrendszer”

Az f függvény és inverze formálisan így festenek:

$$f: \{0, 1, 2, 3\} \times \{0, 1, 2, 3, 4\} \rightarrow \{0, 1, 2, \dots, 19\}$$

$$(c_1, c_2) \mapsto 5c_1 + 16c_2 \bmod 20$$

$$\{0, 1, 2, 3\} \times \{0, 1, 2, 3, 4\} \leftarrow \{0, 1, 2, \dots, 19\} : f^{-1}$$

$$(x \bmod 4, x \bmod 5) \leftarrow x \bmod 20$$

(c_1, c_2)

$f(c_1, c_2)$

0,0	0,1	0,2	0,3	0,4
1,0	1,1	1,2	1,3	1,4
2,0	2,1	2,2	2,3	2,4
3,0	3,1	3,2	3,3	3,4



0	16	12	8	4
5	1	17	13	9
10	6	2	18	14
15	11	7	3	19

Számolás „kínai számrendszerben”

Tegyük fel, hogy sok számolást kell végeznünk 0 és 2047 közötti számokkal.

Válasszunk néhány kicsi, páronként relatív prím modulust, amelyeknek szorzata nagyobb, mint 2047:

$$m_1 = 5, \quad m_2 = 7, \quad m_3 = 8, \quad m_4 = 9, \quad m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 2520.$$

Oldjuk meg az alábbi négy kongruenciarendszert:

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 0 \pmod{7} \\ x &\equiv 0 \pmod{8} \\ x &\equiv 0 \pmod{9} \end{aligned}$$

$$\begin{aligned} x &\equiv 0 \pmod{5} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 0 \pmod{8} \\ x &\equiv 0 \pmod{9} \end{aligned}$$

$$\begin{aligned} x &\equiv 0 \pmod{5} \\ x &\equiv 0 \pmod{7} \\ x &\equiv 1 \pmod{8} \\ x &\equiv 0 \pmod{9} \end{aligned}$$

$$\begin{aligned} x &\equiv 0 \pmod{5} \\ x &\equiv 0 \pmod{7} \\ x &\equiv 0 \pmod{8} \\ x &\equiv 1 \pmod{9} \end{aligned}$$

megoldás:

$$\begin{aligned} x &\equiv 2016 \\ &\pmod{2520} \end{aligned}$$

megoldás:

$$\begin{aligned} x &\equiv 1800 \\ &\pmod{2520} \end{aligned}$$

megoldás:

$$\begin{aligned} x &\equiv 945 \\ &\pmod{2520} \end{aligned}$$

megoldás:

$$\begin{aligned} x &\equiv 280 \\ &\pmod{2520} \end{aligned}$$

Számolás „kínai számrendszerben”

Ennek alapján az

$$\left. \begin{aligned} x &\equiv c_1 \pmod{5} \\ x &\equiv c_2 \pmod{7} \\ x &\equiv c_3 \pmod{8} \\ x &\equiv c_4 \pmod{9} \end{aligned} \right\}$$

paraméteres kongruenciarendszer megoldása:

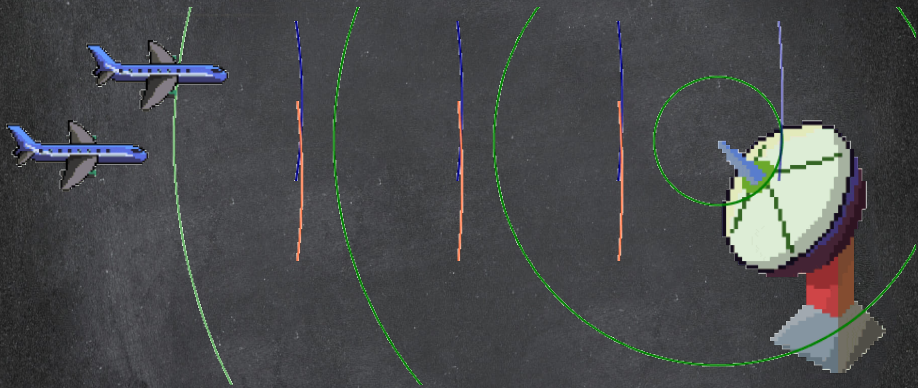
$$x \equiv 2016 \cdot c_1 + 1800 \cdot c_2 + 945 \cdot c_3 + 280 \cdot c_4 \pmod{2520}.$$

Ezzel a képlettel könnyen tudunk oda-vissza váltani „kínai számrendszerre”.

Tfh. ezt kell kiszámolnunk: $22 \cdot 47 + 83 = ?$

		mod 5	mod 7	mod 8	mod 9
22	→	2	1	6	4
47	→	2	5	7	2
83	→	3	6	3	2
162371117	←	72	114	455	101

Távolságmérés radarral



A kép forrása:

<https://prove-me-wrong.com/2019/08/13/radars-and-the-chinese-remainder-theorem/>.

Távolságmérés radarral

Ha a radar 30 kHz-es frekvencián működik, akkor másodpercenként 30 000 impulzust bocsát ki. Tehát két impulzus között $\frac{1}{30\,000}$ másodperc telik el; ezalatt a rádióhullám által megtett út

$$\frac{1}{30\,000} \text{ s} \cdot 300\,000 \frac{\text{km}}{\text{s}} = 10 \text{ km.}$$

Ha két tárgy (pl. repülőgép) távolsága 5 km, akkor egyszerre érkeznek vissza a róluk visszavert hullámok, ezért nem tudunk különbséget tenni közöttük. Ezért egy 30 kHz-es radarral „modulo 5 km” tudunk csak távolságot mérni. Ha 5, 7, 8, 9 km-es távolságnak megfelelő frekvenciákon is elvégezzük a mérést, akkor $5 \cdot 7 \cdot 8 \cdot 9 = 2520$ km-en belül nem lesz két repülő, amit összetévesztünk.



Titokmegosztás kongruenciákkal (emlék 2021-ből)



Waldhauser Tamás (CD6GZI) 02/24/2021 11:44 AM

Az ellenség egy vírust telepített a Discordra, ami hétfőn törölni fogja a Dimat 2 szervert. A vírust egy 4 számjegyből álló titkos kóddal lehet leállítani. A kód annyira titkos, hogy senki nem tudja a világon. Az ellenségnek van három ügynöke: a 49-es, a 64-es és a 81-es ügynök. Mindhárom ügynök tudja a titkos kód maradékát modulo a saját sorszáma. WT riadóztatta a legjobb embereit, a gyakorlatvezetőket, akik rögtön munkához láttak: átkutatták az *U* univerzum minden részhalmozát, és sikerült is elfogniuk mindhárom ügynököt. Az ügynököket válogatott diszkrét kínzásoknak vetették alá, így sikerült vallomásra bírni őket.

49-es ügynök: *„Jaj, ne! Még egy diofantoszi egyenletet nem bírok ki!
Inkább elárulom, amit tudok: 34.”*

64-es ügynök: *„Csak kongruenciákkal ne kínozzatok, inkább vallok:
14.”*

81-es ügynök: *„Kiskorom óta rettegek az ismétléses kombinációtól!
38 a titkos számom, de úgysem mentek velem semmire.”*

Majd meglátjuk! – dörzsölte a kezét WT. – A gyakorlatvezetők már kimerültek az ügynök vadászatban és a kínvallatásban, úgyhogy most a második legjobb embereimet, a hallgatókat állítom rá az ügyre. Három xp-t kap, aki elsőként megfejt a vírust hatástalanító kódot!

Titokmegosztás kongruenciákkal (emlék 2021-ből)



Waldhauser Tamás (CD6GZI) 02/25/2021 8:14 AM

WT kábán ébredt. Az álom foszlányai még ott kavarogtak a fejében, de nem tudta összerakni őket. Valami furcsa volt a szobában. Tikk-takk-tikk-takk... A falióra ketyegése, ami máskor oly megnyugtató háttérzajt adott az előadás-videókhöz, most fenyegetően hangzott. Egy időzített bomba ketyegésére emlékeztette. És ekkor beugrott: sajnos csak álom volt, hogy sikerült az ügynököket elfogni és @NO U megfejtette a kódot! A veszély még nem múlt el. A rádió bementa a pontos időt és a dátumot. Csütörtököt mondott. Nagyon kevés már az idő, az U halmaz pedig óriási, és csak 8 gyakvezér van. Képtelenség hétfőig levadászni mindhárom ügynököt. Talán kettőt sikerülhet elkapni, ha csak arra a kettőre koncentrálnak.

Melyik kettőt lenne jó elkapni? Tudni kell, hogy a vírus egy hibázást megenged, de másodszorra muszáj a jó kódot megadni, különben mindennek vége... 3 xp-t adok annak, aki megmondja **és megindokolja**, hogy melyik két ügynököt kellene elkapni.

Titokmegosztás kongruenciákkal (emlék 2021-ből)



Waldhauser Tamás (CD6GZI) 02/27/2021 1:50 PM

A történet harmadik része:

A gyakorlatvezetők kitartóan átvizsgálták az U halmaz minden zegét-zugát, és végül transzfinít indukcióval sikerült elkapniuk a 64-es és a 81-es ügynököt. Még javában folyt a vattatásuk, amikor váratlanul beállított a 49-es azzal, hogy átáll a mi oldalunkra, és önként elárulja, amit tud. Majd bolondok leszünk hinni neki! Szépen kivallatjuk a másik kettőt, és legfeljebb második próbálkozásra megvan a kód. És ha a vírus mégsem enged két próbálkozást, és törli a Discord-szerverünket, akkor sincs tragédia: szépen átköltözünk a CooSpace-re. Persze nem lesz olyan jó, mint a Discord, de majd kibírjuk valahogy. Ez az ostoba 49-es viszont az életével játszik: ha olyan számot mond, ami a másik két ügynök vallomásának ellentmond, akkor a Maróti-féle nagyfeszültségű elektronikus tesztnek vetjük alá. Azt még senki sem élte túl... Vajon mekkora kockázatot vállal a 49-es ügynök, ha hazudik?

Titokmegosztás kongruenciákkal (emlék 2021-ből)



Waldhauser Tamás (CD6GZI) 02/27/2021 10:53 PM

Íme a befejező rész és az utolsó feladat (ettől még a fenti feladat is él, azt az alábbiaktól függetlenül kell megoldani):

Sikerült vallomásra bírni a 64-es és a 81-es ügynököt: a 64-es titkos száma 19, a 81-esé 43. Ennek alapján két lehetőség van a vírust hatástalanító kódra (a 49-es ügynököt ugye nem vesszük komolyan). A happy endhez már csak ezt a két számot kellene megtalálni...

(edited)

Három xp üti a markát annak, aki először írja meg azt a két 0000 és 9999 közötti számot, ami a két szavahihető ügynök vallomása alapján lehetséges. (Aki szemfüles, az a fentiek alapján ezt már nagyon kevés számolással kihozhatja!)

Lásd még:

https://en.wikipedia.org/wiki/Secret_sharing_using_the_Chinese_remainder_theorem