Magasabbfokú kongruenciák megoldása

Szalkai István
Pannon Egyetem, Veszprém,
szalkai@almos.uni-pannon.hu

2017.12.29.

www: Haladvány Kiadvány, 2017.12.29.

Bevezetés

Az

$$x^h \equiv a \pmod{m} \tag{1}$$

alakú (úgynevezett "**binom**") kongruenciák megoldásaival fogunk foglalkozni. Általános megoldási módszer nincs, kivéve az "utolsó szalmaszál" módszert, ami pedig nagy m modulus esetén sok számolást igényel, nagyon lassú. Tehát csak néhány ötletet próbálhatunk ki, amelyek csak bizonyos esetekben működnek.

Amennyiben rendelkezünk primitív *gyök-* és *index-* táblázattal (mod m) ([2],[3]), akkor a fenti (1) egyenlet a táblázat segítségével könnyen és gyorsan megoldható (hasonlóan a valós számok logaritmusához).

Alapok

1. Definíció. *Tetszőleges* $m \in \mathbb{Z} \setminus \{0, -1, +1\}$ *, egész szám esetén* $\varphi(m)$ *jelöli az* ***Euler-féle*** φ ***függvényt****, vagyis az* m *-nél kisebb,* m *-hez relatív prím poztitív számok számát, azaz*

$$\varphi(m) := |\{x : 1 \leq x < m \text{ és } lnko(m, x) = 1\}| \ . \quad \square \tag{2}$$

2. Tétel. *(L.Euler) Ha*

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t} \quad (0 < \alpha_i) \tag{3}$$

az m szám prímtényezős felbontása, akkor

$$\varphi(m) = m \cdot \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) = m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_t}\right) \ . \quad \square \tag{4}$$

3. Megjegyzés. *Vegyük észre, hogy a p_i prímszámok kitevői nem érdekesek (4) -ben, csak az, hogy m mely p_i prímszámokkal osztható: $p_i \mid m$.*

4. Állítás. *Euler tételének speciális esetei:*
i) ha $m = p$ prímszám, akkor

$$\varphi(p) = p - 1 \ , \tag{5}$$

ii) ha $m = p^\ell$ egy prímszám hatványa, akkor

$$\varphi\left(p^\ell\right) = p^\ell - p^{\ell-1} \ , \tag{6}$$

iii) ha $m = pq...r$ több <u>különböző</u> prímszám szorzata, akkor

$$\varphi(pq...r) = (p-1)(q-1)...(r-1) \ . \quad \square \tag{7}$$

5. Tétel. *(L.Euler): Ha $lnko(a,m) = 1$ akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.* $\square$

6. Következmény. *(P.Fermat): Ha $m = p \in \mathbb{P}$ prímszám és $p \nmid a$ akkor*

$$a^{p-1} \equiv 1 \pmod{p} \ . \quad \square \tag{8}$$

Érdemes még tudni a következőt is:

7. Tétel. *Ha u és m relatív prímek (azaz $lnko(u,m) = 1$), akkor* van u *-nak* ((mod m) *egyetlen)* ***multiplikatív inverze****, vagyis olyan u^{-1} szám, amelyre*

$$u \cdot u^{-1} \equiv 1 \pmod{m} \ . \quad \square \tag{9}$$

A $z \equiv u^{-1}$ számot az $u \cdot z - m \cdot v = 1$ Diophantikus egyenlet megoldásával nyerjük, és nyilván u^{-1} inverze u .

Nagyon fontos még a következő eredmény:

8. Tétel. ***Fokszámtétel*** *[1]:* *Ha $m \in \mathbb{P}$ prímszám, akkor* (mod m)
i) bármely h *-adfokú kongruenciának* legfeljebb h *db gyöke van,*
ii) az (1) alakú binom kongruenciának pontosan *lnko(h,p-1) db gyöke van.* $\square$

A fenti Tételt például akkor alkalmazhatjuk, amikor már (valahogyan megtaláltuk) a kongruenciának h db gyökét, mert nem kell keresgélnünk további gyököket.

Az alábbiakban a következő jelöléseket fogjuk használni:

9. Jelölés. $x^h \equiv a \pmod{m}$, $s = \varphi(m)$,

$\mathbb{Z}_m := \{0, 1, ..., m-1\}$ *a lehetséges maradékok halmaza (m -el való osztás után).*

Ötletek

Az **első ötlet**et az RSA algoritmusban is használjuk. A következőt kell észrevennünk (átgondolnunk):

10. Segédállítás. *i) Ha $x^h \equiv a \pmod{m}$, akkor minden $x, h, y, a, m \in \mathbb{Z}$ számok esetén* $\left(x^h\right)^y \equiv a^y \pmod{m}$.

ii) Ha $h \cdot y \equiv 1 \pmod{s}$ *azaz*

$$h \cdot y = t \cdot s + 1 \quad \textit{vagyis} \quad h \cdot y - t \cdot s = 1, \tag{10}$$

akkor

$$\left(x^h\right)^y \equiv x^{ts+1} \equiv \left(x^s\right)^t \cdot x \equiv x \pmod{m} \tag{11}$$

az Euler-Fermat tétel szerint, vagyis az (1) kongruencia-egyenlet megoldása:

$$x \equiv a^y \pmod{m} \ . \tag{12}$$

Tudjuk, hogy a (10) lineáris Diophantikus egyenletnek pontosan akkor van megoldása, ha

$$lnko\,(h,s) = 1 \ . \tag{13}$$

□

Figyelem: A fenti ötlet csak akkor működik, ha a (13) feltétel teljesül! A (13) feltételben szereplő *lnko(h,s)* -t és a (10) lineáris Diophantikus egyenletet a (kiterjesztett) Euklideszi algoritmussal tudjuk kiszámolni, a (12) -beli hatványt pedig a "gyorsított hatványozás" algoritmussal.

Második ötlet: Ha a (13) feltétel nem teljesül és m különböző prímekből összetett szám, vagyis (3) -ban t legalább 2 , akkor használhatjuk a következő egyszerűsítési módszert:

11. Tétel. *Ha* $m = m_1 \cdot ... \cdot m_t$ *és* $m_1, ..., m_t$ páronként *relatív prímek (azaz* $lnko(m_i, m_j) = 1$ *ha* $i \neq j$*), akkor tetszőleges* $v, w \in \mathbb{Z}$ *számokra*

$$v \equiv w \pmod{m} \tag{14}$$

ekvivalens a következő ("szimultán") kongruencia rendszerrel:

$$\begin{cases} v \equiv w \pmod{m_1} \\ \quad \cdot \ \cdot \ \cdot \\ v \equiv w \pmod{m_t} \end{cases} \tag{15}$$

□

12. Következmény. *(3) esetén (1) ekvivalens a következő kongruencia rendszerrel:*

$$\begin{cases} x^h \equiv a \pmod{p_1^{\alpha_1}} \\ \quad \cdot \ \cdot \ \cdot \\ x^h \equiv a \pmod{p_t^{\alpha_t}} \end{cases} \tag{16}$$

□

Tehát ez esetben a következőképpen oldhatjuk meg (1) -et:

13. Algoritmus. *Az* $x^h \equiv a \pmod{m}$ *kongruencia megoldása:*
ha $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot ... \cdot p_t^{\alpha_t} \quad (0 < \alpha_i)$, *akkor:*

o) jelöljük $p_i^{\alpha_i}$ *-t* m_i *-vel, azaz legyen* $m_i := p_i^{\alpha_i}$ $(1 \leq i \leq t)$,
i) külön-külön megoldjuk az $x^h \equiv a \pmod{m_i}$ *kongruenciákat, melyek megoldásai legyenek* $x_i \pmod{m_i}$,
ii) oldjuk meg az

$$\begin{cases} x \equiv x_1 \pmod{m_1} \\ \quad \cdot \ \cdot \ \cdot \\ x \equiv x_t \pmod{m_t} \end{cases} \tag{17}$$

(szimultán) kongruencia rendszert.
A (17) kongruencia rendszert a Kínai Maradéktétel algoritmussal tudjuk megoldani (ld.[1],[3]). □

14. Algoritmus. *A* ***Kínai Maradéktétel*** *(CRT): a (17) kongruencia rendszer megoldására, ahol* $m_1, ..., m_t$ páronként *relatív prímek (azaz* $lnko(m_i, m_j) = 1$ *ha* $i \neq j$*), és* $m = m_1 \cdot ... \cdot m_t$ *:*
i) először oldjuk meg (külön-külön) az

$$y_i \cdot \frac{m}{m_i} \equiv 1 \pmod{m_i} \ , \quad i = 1, 2, ..., t$$

kongruenciákat (van megoldásuk, mert $\frac{m}{m_i}$ *és* m_i *relatív prímek mindegyik* i *-re),*
ii) ekkor (17) megoldása:

$$x := \sum_{i=1}^{r} x_i \cdot y_i \cdot \frac{m}{m_i} \pmod{m} \ . \tag{18}$$

iii) Könnyen belátható ([2]), hogy (17) megoldása egyértelmű $\pmod{m}$*, vagyis a (18) megoldást* $\pmod{m}$ *kell tekinteni.*

Harmadik ötlet: Az "utolsó szalmaszál" módszer (lásd alább) *előtt* még megpróbálkozhatunk a következő ötlettel: (1) ekvivalens az $x^h = \ell m + a$ egyenlőséggel, vagyis az

$$m \mid x^h - a \tag{19}$$

oszthatósággal. Ha az $x^h - a$ kifejezést szorzattá tudjuk bontani, akkor a fenti (19) oszthatóságról (kicsit) több információnk lesz.

Ha a (13) feltétel nem teljesül és semmi más nem jut eszünkbe, akkor végig kell próbálni $\mathbb{Z}_m$ összes elemét (**"utolsó szalmaszál módszer"**).

Annyit segíthetünk magunkon, hogy $\frac{m}{2} < x$ esetén ha már az $x' := m - x < \frac{m}{2}$ számot kipróbáltuk (vagyis kiszámítottuk $(x')^h$ értékét (mod m)), és $x \equiv -x'$ (mod m) miatt, h párosságától függően vagy $x^h \equiv (x')^h$ vagy $x^h \equiv -(x')^h$ (mod m).

Prímek 1-100 -ig

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Segédprogramok

A feladatok megoldásához ajánljuk a [4] alatti HATVMODDD.EXE, EUKLDIOP.EXE és KINAI3D.EXE programokat. A programok a következő jelöléseket használják:

15. Jelölés. *i)* <n> *a keletkezett maradék (más jelölése:* $\underline{n}$ *),*
ii) a programok csak = jeleket írnak $\equiv$ *helyett, de a (mod m) megjegyzést kiírják,*
iii) ^ *a hatványozás jele.*

Feladatok

wo) $x^3 \equiv 1 \pmod{13}$,

wu) $x^{11} \equiv 4 \pmod{91}$,

wa) $x^{11} \equiv 12 \pmod{221}$,

wb) $x^{15} \equiv 4 \pmod{391}$,

wv) $x^{17} \equiv 3 \pmod{143}$,

wc) $x^{30} \equiv 2 \pmod{1024}$,

wd) $x^{31} \equiv 6 \pmod{187}$.

Megoldások

wo) $x^3 \equiv 1 \pmod{13}$

$m = 13$, így $s = \varphi(m) = 12$, de mivel $lnko(h, s) = lnko(3, 12) \neq 1$, ráadásul $m = 13$ prímszám, ezért az első kettő "Ötlet" módszer *nem* működik.

A Fokszámtétel alapján az egyenletnek $lnko(3, 13-1) = 3$ db gyöke van!

A harmadik módszerrel csökkenthetjük a kongruenci fokszámát 3 -ról 2 -re a (19) átalakítás felhasználásával, azonban hiába következik az

$$13 \mid x^3 - 1 = (x-1)\left(x^2 + x + 1\right) \tag{20}$$

átalakításból vagy $x \equiv 1 \pmod{13}$ vagy $13 \mid x^2+x+1$, az így kapott $x^2+x+1 \equiv 0$ vagy $x(x+1) \equiv -1 \pmod{13}$ kongruenciák egyike sem egyszerűóbb az eredeti $x^3 \equiv 1 \pmod{13}$ egyenletnél.

Mivel $m = 13$ és $h = 3$ nem annyira nagy számok, marad az "utolsó szalmaszál" módszer: végigpróbáljuk $\mathbb{Z}_{13}$ összes elemét(mod 13):

$1^3 \equiv 1$ tehát $\underline{x_1 \equiv 1}$, $2^3 \equiv 8$, $3^3 = 27 \equiv 1$ tehát $\underline{x_2 \equiv 3}$, $4^3 = 64 \equiv -1 \equiv 12$, $5^3 = 125 \equiv -5 \equiv 8$, $6^3 = 216 \equiv -5 \equiv 8$, $7^3 \equiv (-6)^3 \equiv +5$, $8^3 \equiv (-5)^3 \equiv +5$, $9^3 = (-4)^3 \equiv +1$ tehát $\underline{x_3 \equiv 9}$, $10^3 \equiv (-3)^3 \equiv -1$, $11^3 \equiv (-2)^3 \equiv -8 \equiv 5$, $12^3 \equiv (-1)^3 \equiv -1$.

wu) $x^{11} \equiv 4 \pmod{91}$

$m = 91 = 7 \cdot 13$, így $s = \varphi(m) = 6 \cdot 12 = 72$, tehát először olyan y -t keresünk, amelyre $11y \equiv 1 \pmod{72}$ vagyis $11y - 72z = 1$:

< 72> = < 11> * 6 + < 6>
< 11> = < 6> * 1 + < 5>
< 6> = < 5> * 1 + < 1>
< 5> = < 1> * 5 + < 0>

d = lnko(72,11) = 1 = 1 * < 6> + (-1) * < 5> = 1 * < 6> + (-1) * (< 11> - 1 * < 6>) = -1 * < 11> + 2 * < 6> = -1 * < 11> + 2 * (< 72> - 6 * < 11>) = 2 * < 72> + (-13) * < 11>

y_0 = -13*C/d = -13 , z_0 = -2*C/d = -2 ,

az általános megoldás:
y = x_0+k*B/d = -13 +k*72 (k egész)
z = y_0+k*A/d = -2 +k*11 (k egész)

k=1 => **y** = $-13 + 72 =$ **59** , z=-2+11=9 , (ELL: $11 * 59 - 72 * 9 = 1$)

Tehát $(x^{11})^{59} \equiv x^{79 \cdot 9 + 1} \equiv x \equiv 4^{59} \pmod{91}$ és így $4^{59} \equiv ? \pmod{91}$, u=4
u[0] = u^(2^0) = 4 (mod 91)
u[1] = u^(2^1) = 16 (mod 91)
u[2] = u^(2^2) = 74 (mod 91)
u[3] = u^(2^3) = 16 (mod 91)
u[4] = u^(2^4) = 74 (mod 91)
u[5] = u^(2^5) = 16 (mod 91) , k = 111011 (bin)
u^k = 4*16*16*74*16 = 64*16*74*16 = 23*74*16 = 64*16 = **23** Tehát: $4^{59} \equiv 23 \pmod{91}$,

vagyis $\underline{x \equiv 23 \pmod{91}}$.

Ellenőrzés: $23^{11} \equiv ? \pmod{91}$:
u[0] = u^(2^0) = 23 (mod 91)
u[1] = u^(2^1) = 74 (mod 91)
u[2] = u^(2^2) = 16 (mod 91)
u[3] = u^(2^3) = 74 (mod 91) , k = 1011 (bin)
u^k = 23*74*74 = 64*74 = 4

Tehát: $23^{11} = 4 \pmod{91}$ **OK.**

wa) $x^{11} \equiv 12 \pmod{221}$

$m = 221 = 13 \cdot 17$, így $s = \varphi(m) = 12 \cdot 16 = 192$, tehát először olyan y -t keresünk, amelyre $11y \equiv 1 \pmod{192}$ vagyis $11y - 192z = 1$:

< 192> = < 11> * 17 + < 5>
< 11> = < 5> * 2 + < 1>
< 5> = < 1> * 5 + < 0>

d = lnko(192,11) = 1 = 1 *< 11> + (-2) *< 5> = 1 *< 11> + (-2) *(< 192> - 17 *< 11>) = (-2) * < 192> + 35 * < 11>

y_0 = 35*C/d = 35 , z_0 = 2*C/d = 2 .

Az általános megoldás:

y = y_0+k*B/d = 35 +k*192 (k egész)
z = z_0+k*A/d = 2 +k*11 (k egész)
k=0 => **y = 35** , z=2 (ELL: $11 * 35 - 192 * 2 = 1$)

Tehát $(x^{11})^{35} \equiv x \equiv 12^{35} \pmod{221}$ és így $12^{35} \equiv ? \pmod{221}$, u=12

u[0] = u^(2^0) = 12 (mod 221)
u[1] = u^(2^1) = 144 (mod 221)
u[2] = u^(2^2) = 183 (mod 221)
u[3] = u^(2^3) = 118 (mod 221)
u[4] = u^(2^4) = 1 (mod 221)
u[5] = u^(2^5) = 1 (mod 221) , k = 100011 (bin)
u^k = 12*144*1 = 181*1 = 181 Tehát: $12^{35} = 181 \pmod{221}$

vagyis $\underline{x \equiv 181 \pmod{221}}$.

Ellenőrzés: $181^{11} \equiv ? \pmod{221}$ kiszámítása:
u[0] = u^(2^0) = 181 (mod 221)
u[1] = u^(2^1) = 53 (mod 221)
u[2] = u^(2^2) = 157 (mod 221)
u[3] = u^(2^3) = 118 (mod 221) , k = 1011 (bin)
u^k = 181*53*118 = 90*118 = 12

Tehát: $181^{11} = 12 \pmod{221}$ **OK**

wb) $x^{15} \equiv 4 \pmod{391}$

$m = 391 = 17 \cdot 23$, így $s = \varphi(m) = 16 \cdot 22 = 352$, tehát először olyan y -t keresünk, amelyre $15y \equiv 1 \pmod{352}$ vagyis $15y - 352z = 1$:

< 352> = < 15> * 23 + < 7>
< 15> = < 7> * 2 + < 1>
< 7> = < 1> * 7 + < 0>

d = lnko(352,15) = 1 = 1 *< 15> + (-2) *< 7> = 1 *< 15> + (-2) *(< 352> - 23 * < 15>) = (-2) * < 352> + 47 * < 15>

y_0 = 47*C/d = 47 , z_0 = 2*C/d = 2 .

Az általános megoldás:

y = y_0+k*B/d = 47 +k*352 (k egész)
z = z_0+k*A/d = 2 +k*15 (k egész)
k=0 => **y** = 47 , z=2 (ELL: $15 * 47 - 352 * 2 = 1$)

Tehát $(x^{15})^{47} \equiv x \equiv 4^{47} \pmod{391}$ és így $4^{47} \equiv ? \pmod{391}$, u=4

u[0] = u^(2^0) = 4 (mod 391)
u[1] = u^(2^1) = 16 (mod 391)
u[2] = u^(2^2) = 256 (mod 391)
u[3] = u^(2^3) = 239 (mod 391)
u[4] = u^(2^4) = 35 (mod 391)
u[5] = u^(2^5) = 52 (mod 391) , k = 101111 (bin)
u^k = 4*16*256*239*52 = 64*256*239*52 = 353*239*52 = 302*52 = 64
Tehát: $4^{47} = 64 \pmod{391}$

vagyis $\underline{x \equiv 64 \pmod{391}}$.

Ellenőrzés: $64^{15} \equiv ? \pmod{391}$ kiszámítása:
u[0] = u^(2^0) = 64 (mod 391)
u[1] = u^(2^1) = 186 (mod 391)
u[2] = u^(2^2) = 188 (mod 391)
u[3] = u^(2^3) = 154 (mod 391) , k = 1111 (bin)
u^k = 64*186*188*154 = 174*188*154 = 259*154 = 4

Tehát: $64^{15} = 4 \pmod{391}$ **OK**

wv) $x^{17} \equiv 3 \pmod{143}$

$m = 143 = 11 \cdot 13$, így $s = \varphi(m) = 10 \cdot 12 = 120$, tehát először olyan y -t keresünk, amelyre $17y \equiv 1 \pmod{120}$ vagyis $17y - 120z = 1$:

< 120> = < 17> * 7 + < 1>
< 17> = < 1> * 17 + < 0>
d = lnko(120,17) = 1 = 1 * < 120> + (-7) * < 17>
y_0 = -7*C/d = 7 , z_0 = -1*C/d = -1 .

Az általános megoldás:
y = y_0+k*B/d = -7 +k*120 (k egész)
z = z_0+k*A/d = -1 +k*17 (k egész)
k=1 => **y** = $-7 + 120 = 113$, z=-1+17=16 , (ELL: $17 * 113 - 120 * 16 = 1$)

Tehát $(x^{17})^{113} \equiv x \equiv 3^{113} \pmod{143}$ és így $3^{113} \equiv ? \pmod{143}$, u=3

3^{113} (mod 143) kiszámítása:
u[0] = u^(2^0) = 3 (mod 143)
u[1] = u^(2^1) = 9 (mod 143)
u[2] = u^(2^2) = 81 (mod 143)
u[3] = u^(2^3) = 126 (mod 143)
u[4] = u^(2^4) = 3 (mod 143)
u[5] = u^(2^5) = 9 (mod 143)
u[6] = u^(2^6) = 81 (mod 143) , k = 1110001 (bin)
u^k = 3*3*9*81 = 9*9*81 = 81*81 = 126
Tehát: $3^{113} = 126 \pmod{143}$

vagyis $\underline{x \equiv 126 \pmod{143}}$.

Ellenőrzés:
126^{17} (mod 143) kiszámítása:
u[0] = u^(2^0) = 126 (mod 143)
u[1] = u^(2^1) = 3 (mod 143)
u[2] = u^(2^2) = 9 (mod 143)
u[3] = u^(2^3) = 81 (mod 143)
u[4] = u^(2^4) = 126 (mod 143) , k = 10001 (bin)
u^k = 126*126 = 3

Tehát: $126^{17} = 3 \pmod{143}$ **OK**

wc) $x^{30} \equiv 2 \pmod{1024}$

$m = 1024 = 2^{10}$, így $s = \varphi(m) = m \cdot \left(1 - \frac{1}{2}\right) = 512$, de mivel $lnko(h, s) = lnko(30, 512) \neq 1$, , ráadásul $m = 1024$ prímhatvány (egyetlen prímszám hatványa), ezért egyik "Ötlet" módszer **nem** működik.

Póbálkozások: ha x páratalan, akkor x^{30} is páratlan, tehát ekkor $x^{30} \neq 1024\ell + 2$. Ha pedig x páros, vagyis $2 \mid x$, akkor $2^{30} \mid x^{30}$, vagyis ekkor szintén $x^{30} \neq 1024\ell + 2$.

Tehát az $x^{30} \equiv 2 \pmod{1024}$ kongruenciának **nincs megoldása.**

wd) $x^{31} \equiv 6 \pmod{187}$

$m = 187 = 11 \cdot 17$, így $s = \varphi(m) = 10 \cdot 16 = 160$, tehát először olyan y -t keresünk, amelyre $31y \equiv 1 \pmod{160}$ vagyis $31y - 160z = 1$:

< 160> = < 31> * 5 + < 5>
< 31> = < 5> * 6 + < 1>
< 5> = < 1> * 5 + < 0>
d = lnko(160,31) = 1 = 1 * < 31> + (-6) * < 5> = 1 * < 31> + (-6) * (< 160> - 5 * < 31>) = (-6) * < 160> + 31 * < 31>
y_0 = 31*C/d = 31 , z_0 = 6*C/d = 6 .

Az általános megoldás:
y = y_0+k*B/d = 31 +k*160 (k egész)
z = z_0 +k*A/d =6 +k*31 (k egész)
k=0 => **y = 31** , z=6 (ELL: $31 * 31 - 160 * 6 = 1$)

Tehát $(x^{31})^{31} \equiv x \equiv 6^{31} \pmod{187}$ és így $6^{31} \equiv ? \pmod{187}$, u=6

6^{31} (mod 187) kiszámítása:
u[0] = u^(2^0) = 6 (mod 187)
u[1] = u^(2^1) = 36 (mod 187)
u[2] = u^(2^2) = 174 (mod 187)
u[3] = u^(2^3) = 169 (mod 187)
u[4] = u^(2^4) = 137 (mod 187) , k = 11111 (bin)
u^k = 6*36*174*169*137 = 29*174*169*137 = 184*169*137 = 54*137 = 105
Tehát: $6^{31} = 105 \pmod{187}$

vagyis $\underline{x \equiv 105 \pmod{187}}$.

Ellenőrzés:

$105^{31} \pmod{187}$ kiszámítása:
u[0] = u^(2^0) = 105 (mod 187)
u[1] = u^(2^1) = 179 (mod 187)
u[2] = u^(2^2) = 64 (mod 187)
u[3] = u^(2^3) = 169 (mod 187)
u[4] = u^(2^4) = 137 (mod 187) , k = 11111 (bin)
u^k = 105*179*64*169*137 = 95*64*169*137 = 96*169*137 = 142*137 = 6

Tehát: $105^{31} = 6 \pmod{187}$ **OK**

Másik megoldás, a **második ötlet** alapján: $187 = 11 \cdot 17$ miatt $x^{31} \equiv 6 \pmod{187}$ ekvivalens a következő kongruenciarendszererel: $x^{31} \equiv 6 \pmod{11}$ ÉS $x^{31} \equiv 6 \pmod{17}$.

i) $x^{31} \equiv 6 \pmod{11}$ megoldása: $\varphi(11) = 10$ és a Fermat-tétel miatt *minden* x -re $(11 \nmid x)$ $x^{10} \equiv 1$ tehát $x^{31} \equiv (x^{10}) \cdot x \equiv x$, tehát $x \equiv 6 \pmod{11}$, vagyis $\underline{x = 11\ell + 6}$.

ii) $x^{31} \equiv 6 \pmod{17}$ megoldása: $\varphi(11) = 16$ és a Fermat-tétel miatt *minden* x -re $(11 \nmid x)$ $x^{16} \equiv 1$ tehát $(x^{16})^2 \equiv x^{32} \equiv 1^2 \equiv 1$, amit tehát x multiplikatív inverzével megszorozva kapjuk: $x^{31} \equiv 1 \cdot x^{-1} \equiv x^{-1} \equiv 6$ vagyis $x \equiv 6^{-1} \pmod{17}$. Próbálgatással (mod 17) is megkaphatjuk x értékét: $6 \cdot 3 = 18 \equiv 1 \pmod{17}$, tehát $x \equiv 3 \pmod{17}$, vagyis $\underline{x = 17k + 3}$.

iii) A fenti eredmények szerint $x = 11\ell + 6 = 17k + 3$, tehát ilyen ℓ és k számokat kell keresnünk ($0 \le \ell \le 16$ és $0 \le k \le 10$), vagy egyszerűbben:

$$11\ell + 3 = 17k \ . \tag{21}$$

Kis próbálgatás után (vagy az Euklideszi algoritmussal) megtaláljuk az $\ell = 9$ és $k = 6$ számokat, és így az $\underline{x \equiv 105 \pmod{187}}$ megoldást.

Javasolt irodalom

[1] **Sárközy András:** *Számelmélet*, példatár, "Bolyai könyvek" sorozat, Műszaki Kiadó 1976

[2] **Szalkai István:** *Algebra Feladatgyűjtemény*, Veszprémi Egyetemi Kiadó, 2005.

[3] **Szalkai István, Dósa György:** *Algoritmikus Számelmélet*, Typotex Kiadó, ISBN 978-963-279-523-2,

http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_szalkai_dosa_szamelmelet/adatok.html,
http://oszkdk.oszk.hu/DRJ/5848,
http://tananyagfejlesztes.mik.uni-pannon.hu/images/stories/vegleges_tananyagok/
Digitalismellekletek/szalkai_dosa_algoritmikus_szamelm.zip,

[4] **Szalkai István:** *Számelméleti programok* ([3] mellékletei): HATVMODDD.EXE,
EUKLDIOP.EXE, KINAI3D.EXE,
http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_szalkai_dosa_szamelmelet/programok.zip