PHAM VAN CHUNG

EGY KLASSZIKUS PROBLÉMA ÁLTALÁNOSÍTÁSA II.

Abstract: (A generalization of a classical problem II.). In the present paper we solve a generation of a classical problem. The problem was dawn first up in the "Annales de Math." ([8], p. 220.). Since that time this problem, i.e. the solution of the congruence $x^2 \equiv x \pmod{m^k}$, was investigated by several authors, the first solution of it was given by M. Tédenant [8] in 1814. Our purpose is to generalize this problem by solving the congruence $x^n \equiv ax^s \pmod{m^k}$, where n,a,s,m and k are given natural numbers. We give the number and the explicite form of the solutions; and show some properties of them in some special cases. For example, in the case $(n-1, \varphi(m)) = 1$ we solve the congruence $x^n \equiv x \pmod{m^k}$ and give some properties of this.

1814-ben az „Annales de Math." c. folyóirat azt a problémát vetette fel, hogy „Melyek azok a természetes számok, amelyeknek négyzete ugyanarra a k-jegyű számra végződik, mint

az eredeti szám?". Ezt M. Tédenant [8] oldotta meg és igazolta, hogy két nem triviális megoldásának összege $10^k + 1$. Azóta többen foglalkoztak ilyen, illetve hasonló problémával (lásd L. E. Dickson [4]). Ez a probléma az

$$x^2 \equiv x \pmod{m^k}$$

kongruencia pozitív megoldásának keresését jelenti. [10]-ben foglalkoztunk egy általánosabb problémával, nevezetesen megoldottuk az $x^2 \equiv ax \pmod{m^k}$ kongruenciát; megadtuk a megoldások számát és a megoldások explicit alakját, valamint egy eljárást a kongruencia numerikus megoldására.

A probléma még a következőképpen általánosítható: „Melyek azok a természetes számok az m-alapú számrendszerben, amelyeknek az n-edik hatványa ugyanarra a k-jegyű számra végződik, mint az eredeti szám s-edik hatványának a-szorosa?", azaz keressük az

$$x^n \equiv ax^s \pmod{10^k}$$

kongruencia pozitív egész megoldásait.

A kongruencia speciális eseteivel sokan foglalkoztak, különösen az $m = 10$ esettel. Egy általános eredményt C. P. Popovici [7] adott meg, mégpedig az $x^n \equiv x \pmod{m^k}$ kongruencia megoldásainak explicit alakjával. Általános m esetén az $x^n \equiv x \pmod{m^k}$ kongruenciával P. Kiss [5] foglalkozott. Megadta a kongruencia megoldásainak számát és a megoldások explicit alakját.

Többen foglalkoztak a kongruenciánk $x^n \equiv x \pmod{n}$ speciális esetével a pszeudoprimszámokkal kapcsolatban. (Például R. D. Carmichael [2], A. Korselt [6], M. R. Chapson [3] és P. Bachmann [1].)

Ebben a II. cikkben explicit alakban megadjuk a

$$x^n \equiv ax^s \pmod{m^k}$$

kongruencia nem túl nagy abszolút értékű megoldásait, valamint a megoldások számát. Megmutatjuk, hogy az $s = 1$ esetben elegendő az $n \leq \varphi(m^k)$ esetet, továbbá az $a = 1$ és $(n-1, \varphi(m)) = 1$ együttes fennállása esetén az $n = 2$ esetet megoldani. Ezután vizsgáljuk a megoldásokat általában.

Mielőtt rátérünk az

(1) $$x^n \equiv ax^s \pmod{m}$$

kongruencia megoldására, néhány speciális esettel foglalkozunk.

1. Tétel: Ha $(a,m) = 1$ és $n = k\varphi(m) + r$ (φ az Euler-függvény) és $0 < r \leq \varphi(m)$, akkor a következő két kongruencia ekvivalens

(2) $$x^n \equiv ax \pmod{m}$$

(3) $$x^r \equiv ax \pmod{m}.$$

Bizonyítás: Megmutatjuk, hogy az első kongruencia megoldásai kielégítik a másodikat és viszont.

Legyen x_0 egy megoldása a (2) kongruenciának, továbbá $(x_0, m) = d$. Ezek alapján léteznek x_1 és m_1 egészek, melyekre $x_0 = dx_1$, $m = dm_1$ és $(x_1, m_1) = 1$. Ezeket (2)-be helyettesítve és d-vel osztva

$$x_1^n d^{n-1} \equiv ax_1 \pmod{m_1}.$$

De $(x_1, m_1) = 1$ miatt mindkét oldalát x_1-gyel osztva kapjuk, hogy

$$(x_1 d)^{n-1} \equiv a \pmod{m_1}.$$

Ez csak úgy állhat fenn, ha $(x_1 d, m_1) = 1$, mivel $(a,m) = 1$.

Mivel $(d,m_1)=1$ folytán $\varphi(m)=\varphi(d)\cdot\varphi(m_1)$, így a bal oldal tovább alakítható, felhasználva az Euler-Fermat tételt:

$$(x_1d)^{n-1}=(x_1d)^{k\varphi(d)\cdot\varphi(m_1)}(x_1d)^{r-1}\equiv(x_1d)^{r-1}(\text{mod } m_1).$$

Tehát a fenti kongruencia a következőre redukálódik:

$$(x_1d)^{r-1}\equiv a \pmod{m_1}.$$

Itt d-vel szorozva mindkét oldalt és a modulust is, majd x_1-gyel szorozva a két oldalt és , ill. m_1d helyébe visszaírva x_0-t, ill. m-et, az

$$x_0^r\equiv ax_0 \pmod{m}$$

kongruenciát kapjuk, mivel igazoltuk a tételt az egyik irányban.

Ha x_0 megoldása a (3) kongruenciának, akkor az előzőekhez hasonlóan látható be, hogy megoldása a (2)-nek is.

Ezután bebizonyítjuk a következő tételt, amely bizonyos esetekben egyszerűsítheti a számításokat.

2. Tétel: Ha $(n-1,\varphi(m))=1$, akkor az

(4) $$x^n\equiv x \pmod{m}$$

és az

(5) $$x^2\equiv x \pmod{m}$$

kongruencia ekvivalens.

Bizonyítás: Tegyük fel, hogy x_0 megoldása a (4) kongruenciának. Mivel $(n-1,\varphi(m))=1$, léteznek olyan v és u természetes számok, amelyekre

(6) $$v\cdot(n-1)=u\cdot\varphi(m)+1.$$

Mint az előző tétel bizonyításában, ha $(x_0,m)=d$ és a felhasznált jelöléseket tartva (4) átalakítható

(7) $$(x_1d)^{n-1}\equiv 1 \pmod{m_1}$$

alakra, ahol $(x_1 d)^{v(n-1)} \equiv 1 \pmod{m_1}$

(6)-ot a (7)-be helyettesítve

$$1 \equiv (x_1 d)^{v(n-1)} \equiv (x_1 d)^{u\cdot\varphi(m)+1} \equiv \left[(x_1 d)^{\varphi(m)}\right]^u \cdot x_1 d \equiv x_1 d \pmod{m},$$

mert $(x_1 d, m_1) = 1$ miatt $\varphi(m) = \varphi(m_1 d) = \varphi(d)\cdot\varphi(m_1)$, amiből $(x_1 d)^{\varphi(m)} \equiv 1 \pmod{m_1}$. Tehát $x_1 d \equiv 1 \pmod{m_1}$. Ezt d-vel végigszorozva, azután mind a két oldalt x_1-gyel szorozva és $x_1 d$ helyére x_0-t visszaírva $x_0^2 \equiv x_0 \pmod{m}$ adódik, amivel a tétel első részét bebizonyítottuk.

Viszont, ha x_0 megoldása az (5)-nek, akkor ez kielégíti a (4)-et is. Ugyanis $x_0^2 \equiv x_0 \pmod{m}$ miatt $n \geq 2$ esetén

$$x_0^n \equiv x_0^{n-2} \cdot x_0^2 \equiv x_0^{n-2} x_0 = x_0^{n-1} \equiv \cdots \equiv x_0 \pmod{m}.$$

Megjegyzés:

1. Tetszőleges a-ra az $(n-1, \varphi(m)) = 1$ feltétel teljesülése esetén nem mindig ekvivalensek az $x^n \equiv ax \pmod{m}$ és $x^2 \equiv ax \pmod{m}$ kongruenciák. Például $a = 3$, $n = 4$ és $m = 10$ esetén $x^4 \equiv 3x \pmod{10}$ és $x^2 \equiv 3x \pmod{10}$ nem ekvivalensek. Hiszen $x \equiv 8 \pmod{10}$ megoldása a második kongruenciának, de nem elégíti ki az $x^4 \equiv 3x \pmod{10}$ kongruenciát.

2. Ebből a tételből következik, hogy az $(n-1, \varphi(m)) = 1$ esetén minden $x^2 \equiv x \pmod{m}$ kongruenciára vonatkozó tétel érvényesül az $x^n \equiv x \pmod{m}$ kongruenciára is. Ezért igaz például a következő:

3. Tétel: Ha $(n-1, \varphi(m)) = 1$ és $m = P_1^{k_1} \cdots P_s^{k_s}$, akkor az

$$x^n \equiv x \pmod{m}$$

kongruenciának

(i) összes megoldása $u^{\varphi(v)} \pmod{m}$ alakú, ahol $uv = m$ és $(u,v) = 1$;

(ii) 2^s inkongruens megoldása van;

(iii) az inkongruens megoldások összege 2^{s-1}-gyel kongruens mod m.

Bizonyítás: A 2. Tétel miatt elegendő csak az $x^2 \equiv x \pmod{m}$ kongruenciát megoldani. A továbbiakban u és v mindig olyan számokat jelentsen, amelyekre $u \cdot v = m$ és $(u,v) = 1$.

(i) Könnyű belátni, hogy $x \equiv u^{\varphi(v)} \pmod{uv}$ megoldása az $x^2 \equiv x \pmod{m}$ kongruenciának. Még azt kell igazolni, hogy minden megoldás $u^{\varphi(v)}$ alakban írható (mod m). Valóban ha x_0 kielégíti az $x^2 \equiv x \pmod{m}$ kongruenciát, akkor $u = (x_0, m)$ jelöléssel vannak y_0 és v egészek, amelyekre

$$x = uy_0 \quad \text{és} \quad m = u \cdot v, \quad \text{ahol } (y_0, v) = 1.$$

Ezeket az $x^2 \equiv x \pmod{m}$ kongruenciába behelyettesítve az

$$(uy_0)^2 \equiv uy_0 \pmod{u \cdot v}$$

kongruenciához jutunk, amiből $(y_0, v) = 1$ miatt

$$uy_0 \equiv 1 \pmod{v}.$$

Innen $(u,v) = 1$, továbbá $y_0 \equiv u^{\varphi(v)-1} \pmod{v}$. Tehát

$$x_0 \equiv u^{\varphi(v)} \pmod{uv}$$

alakú, amit kívántunk.

(ii) A bizonyítás a [10]-ben lévő 4. Tételhez hasonló,

(iii) A tétel (i) állítása alapján $m = uv$, $(u,v) = 1$ felírással, ha $x_1 \equiv u^{\varphi(v)} \pmod{m}$ egy megoldás, akkor $x_2 \equiv v^{\varphi(u)} \pmod{m}$ egy másik megoldás. Mivel $(u,v) = 1$, így

$$u^{\varphi(v)} + v^{\varphi(u)} \equiv 1 \pmod{u \cdot v}.$$

(ii) miatt 2^{s-1} ilyen megoldáspár van, ezért a megoldásokra

$$\sum x_1 \equiv \sum_{1}^{2^{s-1}} 1 = 2^{s-1} \pmod{m}.$$

Most rátérünk az általános esetre.

Oldjuk meg a

(8) $$x^n \equiv a \cdot x^s \pmod{m};\ (a,m) = 1$$

kongruenciát. Megmutatjuk, hogy elég csak az $n > s$ esetre szorítkozni. Ha ugyanis $(a,m) = 1$, akkor (8) mindkét oldalát $a^{\varphi(m)-1}$-gyel beszorozva

$$a^{\varphi(m)-1} \cdot x^n \equiv a^{\varphi(m)} \cdot x^s \pmod{m}$$

Innen $(a,m) = 1$ miatt $a^{\varphi(m)} \equiv 1 \pmod{m}$. Ezért (8) alakja

$$x^s \equiv a' \cdot x^n \pmod{m}, \text{ ahol } a' = a^{\varphi(m)-1}$$

lesz, amelyet kívántunk. A megmaradt $n = s$ esetén a megoldás triviális.

Tehát a továbbiakban legyen $n > s$ és $m = P_0^{k_0} \cdot P_1^{k_1} \cdots P_r^{k_r}$ $(P_0 = 2)$. A (8) kongruencia ekvivalens a

$$x^n \equiv ax^s \pmod{2^{k_0}}$$

$$x^n \equiv ax^s \pmod{P_i^{k_i}} \qquad i = 1,2,\ldots,r$$

kongruencia-rendszerrel.

Az

(9) $$x^n \equiv ax^s \pmod{P_i^{k_i}} \qquad i = 1,2,\ldots,r$$

kongruenciából

(10) $$x^s(x^{n-s} - a) \equiv 0 \pmod{P_i^{k_i}}.$$

De $(x^s, x^{n-s} - a) = (x^s, a)$ és $(m,a) = 1$ miatt x^s és $x^{n-s} - a$ közül pontosan csak az egyik osztható P_i-vel. Ezek alapján (10)-ből

(11) $$x^s \equiv 0 \pmod{P_i^{k_i}}$$

vagy

(12) $$x^{n-s} \equiv a \pmod{P_i^{k_i}}.$$

a) Tekintsük a (11) kongruenciát! Nyilván, hogy ennek megoldása

$$x \equiv P_i^{k_i} \cdot t \pmod{P_i^{k_i}}, \text{ ahol } v_i = \left[\frac{k_i + s - 1}{s}\right]$$

és $t = 1, 2, \ldots p^{k_i - v_i}$, $i = 0, 1, \cdots, r$.

b) Ezuán (12) következőképpen oldható meg. Ha $k_0 \leq 2$, ill. $P_i > 2$, akkor az $x^{n-s} \equiv a \pmod{p_k^{k_i}}$ kongruencia primitív gyökök segítségével visszavezethetők $(n-s)y_i \equiv b_i \pmod{\varphi(P_i^{k_i})}$ alakú kongruenciára, ahol y_i és b_i sorrendben indexei az x-nek és a-nak. Ezek alapján a megoldások száma

$$D_1 = \begin{cases} d = \left((n-s), \varphi(P_i^{k_i})\right), & \text{ha } d | b_i, \\ 0, & \text{különben.} \end{cases}$$

$k_0 \geq 3$ esetén legyen $c = 2$ és $c_0 = 2^{k_0 - 2}$. Ekkor az $x^{n-s} \equiv a \pmod{2^{k_0}}$ kongruenciához létezik b és b_0, hogy $a \equiv (-1)^b \cdot 5^{b_0} \pmod{2^{k_0}}$, továbbá létezik y és y_0, hogy

$$\begin{cases} (n-s)y \equiv b \pmod{c} \\ (n-s)y_0 \equiv b_0 \pmod{c_0} \end{cases}$$

$x \equiv (-1)^y \cdot 5^{y_0} \pmod{2^{k_0}}$ (lásd [9]). Ebben az esetben a megoldások száma

$$D_0 = \begin{cases} d \cdot d_0, & \text{ha } d = (n-s, c) | b \quad \text{és } d_0 = (n-s, c_0) | b_0, \\ 0, & \text{egyébként.} \end{cases}$$

ha $d = (n-s, c) | b$ egyébként.

és $d_0 = (n-s, c_0) | b_0$,

Az előző jelöléseket használva kapjuk a következő tételt:

4. Tétel: Az

$$x^n \equiv a \cdot x^s \pmod{2^{k_0} \cdot P_1^{k_1} \cdot \ldots \cdot P_r^{k_r}}, \quad (a,m) = 1$$

kongruencia inkongruens megoldásainak száma

$$M = \left(D_0 + P_0^{k_0 - \nu}\right)\left(D_1 + P_1^{k_1 - \nu_1}\right) \ldots \left(D_r + P_r^{k_r - \nu_r}\right).$$

Nézzük meg ezután a (8) kongruencia általános megoldását!

Először bizonyítás nélkül közlünk két segédtételt, amelyek Kiss Pétertől [5] származnak.

1. Segédtétel. Tetszőleges $m > 1$ és k természetes számok esetén

$$\varphi(m^k) \geq k.$$

2. Segédtétel. Legyen $M = q_0 \cdot q_1 \cdots q_r$, ahol $q_i > 1$ és $q_0, q_1, \cdots q_r$ páronként relatív prímek, továbbá $Q_i = \frac{M}{q_i}$. Ekkor

$$\sum_{j=1}^{r} Q_j^{\varphi(q_j^k)} \equiv 1 \pmod{M^k}.$$

Ezután az $x^n \equiv ax^s \pmod{m^k}$, $(a,m) = 1$ kongruencia így oldható meg: Legyen G_1 megoldása az $x^n \equiv ax^s \pmod{P_i^{k_1}}$ kongruenciának $(i = 0,1,\ldots,r)$, ahol $m^k = P_0^{t_0} \cdot P_1^{t_1} \cdots P_r^{t_r}$. A $h = (t_0, t_1, \ldots, t_r)$ (azaz $t_0, t_1, \ldots, t_r$ legnagyobb közös osztója) jelöléssel $t_i = h \cdot t_i'$, továbbá $M = 2^{t_0'} \cdot P_1^{t_1'} \cdots P_r^{t_r'}$, így $M^h = m^k$. Vezessük be a $T_j = \frac{M}{P_j^{t_j'}}$, $j = 0,1,\ldots,r$ jelölést. A fentiek alapján

$$T_i^{\varphi\left(P_i^{t_i}\right)} \cdot x \equiv G_i \cdot T_i^{\varphi\left(P_i^{t_i}\right)} \left(\bmod P_i^{t_i} \cdot T_i^{\varphi\left(P_i^{t_i}\right)}\right).$$

De az 1. Segédtétel miatt

$$\varphi\left(P_i^{t_i}\right) = \varphi\left[\left(P_i^{t_i}\right)^h\right] \geq h, \text{ amiből } T_i^h \mid T_i^{\varphi\left(P_i^{t_i}\right)}.$$

Így $M^h \mid P_i^{t_i} \cdot T_i^{\varphi\left(P_i^{t_i}\right)}$. Tehát

$$T_i^{\varphi\left(P_i^{t_i}\right)} \cdot x \equiv G_i \cdot T_i^{\varphi\left(P_i^{t_i}\right)} \pmod{M^h}.$$

Ezeket 0-tól r-ig összegezve kapjuk

$$\left(\sum_{i=1}^{r} T_i^{\varphi\left(P_i^{t_i}\right)}\right) \cdot x \equiv \sum_{i=0}^{r} G_i \cdot T_i^{\varphi\left(P_i^{t_i}\right)} \pmod{M^h}.$$

De a 2. segédtétel miatt x együtthatója 1-gyel kongruens $(\mathrm{mod}\ M^h)$. Ezzel bizonyítottuk a következő tételt:

5. Tétel. Az

$$x^n \equiv a \cdot x^s \pmod{m^k}$$

kongruenciának összes megoldása

$$x \equiv \sum_{i=0}^{r} G_i \cdot Q_i^{\varphi\left(P_i^{t_i}\right)} \pmod{m^k},$$

ahol $m^k = P_0^{t_0} \cdot P_1^{t_1} \cdots P_r^{t_r}$, G_i megoldása az $x^n \equiv a \cdot x^s \pmod{P_i^{t_i}}$, $i = 0,1,\ldots,r$ kongruenciának és $Q_i = \dfrac{M}{P_i^{t_i}}$, $M = \prod_{i=0}^{r} P_i^{t_i}$ a $t_i' = t_i / (t_0, t_1, \ldots, t_r)$ jelölés mellett.

IRODALOM

[1] P. Bachmann: Über Fermat „kleinen" Satz. Archiv. Math. und physik, 21 (1913) 185–187.

[2] R. D. Carmichael: Note on a new number theory function; Bull. of Amer. Math. Soc., 16 (1910) 232–238.

[3] M. R. Chapron: Sur one proposition erronée Korselt relative aux nombres composes m qui divisent a^n-a, Bull. Sci. Mat., 80 (1956) 81–83.

[4] L. E. Dickson: History of the theory of thenumbers I., Chelsea Publ. Co., New York, (1971) 453–456.

[5] P. Kiss. Egy binom kongruenciáról, Acta Acad. Paed. Agr.-Nova Eger, XIV (1978) 453–464.

[6] A. Korselt: Le probéme chinois ..., Interm. des Math., VI (1899) 143.

[7] C. P. Popovici: Sur une équation arith. de D. Pompeiu; Bull. Math. de La Soc. Sci. Math. R.S.R., 9 (1967) 92–97.

[8] M. Tédenant: Probléme d'arith., Anales de Math., 5 (1814) 809–821.

[9] I. M. Vinogrodov: A számelmélet alapjai. Tankönyvkiadó, Budapest (1968)

[10] P. V. Chung: Egy klasszikus probléma általánosítása. Acta Acad. Pead. Agr.-Nova, Eger, XX (1991) 3–13.