Számelmélet

(2017. február 8.)

Bogya Norbert, Kátai-Urbán Kamilla

1. Oszthatóság

1. Definíció. Legyen $a, b \in \mathbb{Z}$. Az a osztója b-nek, ha létezik olyan $c \in \mathbb{Z}$ egész szám, melyre $ac = b$. Jelölése: $a \mid b$.

2. Példa. $3 \mid 12$, $\quad -2 \mid 6$, $\quad 1 \mid -132$, $\quad 7 \mid 0$, $\quad 0 \mid 0$.

3. Megjegyzés. Az oszthatóság nem egyezik meg az osztás fogalmával, mint látható a 0 osztható 0-val, de ettől még a nullával való osztás értelmetlen marad.

4. Tétel (Az oszthatóság tulajdonságai). Tetszőleges a, b, c, d egész számokra érvényesek az alábbiak:

(1) $a \mid a$;
(2) ha $a \mid b$ és $b \mid a$, akkor $a = \pm b$;
(3) ha $a \mid b$ és $b \mid c$, akkor $a \mid c$;
(4) $1 \mid a$;
(5) $a \mid 0$;
(6) $a \mid b$ akkor és csak akkor, ha $|a| \mid |b|$;
(7) ha $a \mid b$ és $a \mid c$, akkor $a \mid b \pm c$;
(8) ha $a \mid b$, akkor $a \mid bc$;
(9) ha $a \mid b$ és $c \mid d$, akkor $ac \mid bd$;
(10) ha $ac \mid bc$ és $c \neq 0$, akkor $a \mid b$.

5. Definíció. A c egész számot az a és b egész számok közös osztójának nevezzük, ha $c \mid a$ és $c \mid b$. A c egész szám az a és b legnagyobb közös osztója, ha közös osztója, és a és b minden d közös osztójára $d \mid c$. Hasonlóan definiáljuk a közös többszöröst és a legkisebb közös többszöröst.

6. Lemma. Tetszőleges a, b, c egész számokra érvényesek az alábbiak:

(1) ha c legnagyobb közös osztója a és b-nek, akkor $-c$ is az és rajtuk kívűl nincsen másik;
(2) 0 és a legnagyobb közös osztója a és $-a$;
(3) a és b közös osztói ugyan azok mint $a + bc$ és b közös osztói.

7. Megjegyzés. Az előbbi lemma (1) pontja alapján a legnagyobb közös osztó nem egyértelmű az egész számok körében. Ha $a, b \in \mathbb{N}$, akkor a legnagyobb közös osztót is az $\mathbb{N}$ halmazból választjuk, így egyértelműen meghatározott.

8. Jelölés. Az a és b legnagyobb közös osztóját $\operatorname{lnko}(a, b)$-vel, míg a legkisebb közös többszörösét $\operatorname{lkkt}(a, b)$-vel jelöljük.

9. Tétel. Legyen $a, b \in \mathbb{N}$, ekkor $ab = \operatorname{lnko}(a, b) \operatorname{lkkt}(a, b)$.

10. Definíció. Az a és b természetes számok relatív prímek, ha $\operatorname{lnko}(a, b) = 1$.

1.1. Prímszámok

11. Megjegyzés. A prímszámok definíciója különbözni fog attól, amit középiskolában tanítanak. Felsőbb matematikában be kell vezetni az irreducibilis elemek fogalmát, mely különbözhet a prím elemek fogalmától.

12. Definíció. A $p \in \mathbb{N}$, $p > 1$ számot irreducibilisnek (felbonthatatlannak) nevezzük, ha $p = ab$ estén $a = 1$ vagy $b = 1$ teljesül.

13. Definíció. A $p \in \mathbb{N}$, $p > 1$ számot prímszámnak nevezzük, ha $p \mid ab$ esetén $p \mid a$ vagy $p \mid b$.

14. Megjegyzés. A nemnegatív egész számok halmazában az irreducibilis számok ugyanazok, mint a prímszámok, ezért fordulhat elő, hogy a prímszámokat szokták definiálni a felbonthatatlansággal. Azonban a két fogalom nem fog mindig egybeesni, ezért szükség van a definíciók elkülönítésére. Például a páros számok körében a 6 irreducibilis, mert nem tudjuk előállítani két páros szám szorzataként, viszont nem prím, mert $6 \mid 18 \cdot 30$, hiszen $540 = 6 \cdot 90$, de $6 \nmid 18$ és $6 \nmid 30$ a páros számok körében.

Sok prímszámmal kapcsolatos kérdést sikerült már megválaszolni, azonban sok még csak sejtésként van jelen a matematikában. Ha valaki először találkozik prímszámokkal, akkor felmerülhet az a kérdése is, hogy egyáltalán hány darab prímszám van? A választ már Euler is tudta a kérdésre.

15. Tétel (Euler tétele). Végtelen sok prímszám van.

Bizonyítás. Tegyük fel, hogy véges sok prímszám van, ezek $p_1, p_2, \ldots, p_k$. Az $n = p_1 p_2 \ldots p_k + 1$ szám p_i-kkel vett osztási maradéka mindig 1, így n nem osztható egyik p_i-vel sem. Tehát n prím, vagy létezik egy p_i-től különböző prímosztója. Mindkét esetben ellentmondásra jutottunk, ugyanis találtunk egy p_i-től különböző prímet, viszont az elején feltettük, hogy $p_1, p_2, \ldots, p_k$ az összes prímszám. □

16. Tétel (Számelmélet alaptétele). Bármely természetes szám felbontható prímszámok szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

1.2. Maradékos osztás

17. Tétel. Az egész számok körében mindig elvégezhető a maradékos osztás. Azaz bármely $a \in \mathbb{Z}$ és $b \in \mathbb{Z} \setminus \{0\}$ esetén létezik olyan egyértelműen meghatározott $q, r \in \mathbb{Z}$, hogy $a = b \cdot q + r$, ahol $0 \leq r < |b|$. (A q-t nevezzük hányadosnak, míg az r-et maradéknak.)

A következő tétel egy olyan algoritmust ad, mellyel gyorsan és könnyen kiszámítható két szám legnagyobb közös osztója.

18. Tétel (Euklideszi algoritmus). Legyen $a, b \in \mathbb{N}$, és tekintsük az alábbi maradékos osztásokat (mindig q_i jelenti a hányadost, r_i pedig a maradékot):

$$\begin{aligned}
a &= bq_1 + r_2 && (0 < r_2 < b),\\
b &= r_2 q_2 + r_3 && (0 < r_3 < r_2),\\
r_2 &= r_3 q_3 + r_4 && (0 < r_4 < r_3),\\
&\vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && (0 < r_n < r_{n-1}),\\
r_{n-1} &= r_n q_n + r_{n+1} && (r_{n+1} = 0).
\end{aligned}$$

Ekkor r_n, azaz az utolsó nemnulla maradék lesz az a és b számok legnagyobb közös osztója.

19. Megjegyzés. Az euklideszi algoritmus során mindig az előző osztóból lesz az osztandó, illetve az előző maradék lesz az osztó. Mivel $b > r_2 > r_3 > \ldots$ véges lépésben véget ér (a maradék nemnegativitása miatt), eljutunk addig, míg az utolsó maradék 0 lesz, ekkor állunk meg.

20. Megjegyzés. Az euklideszi algoritmus hatékony kiszámítási módját adja két szám legnagyobb közös osztójának meghatározásához, mely könnyen programozható.

21. Példa. Határozzuk meg 246 és a 132 legnagyobb közös osztóját.

$$\begin{aligned}
246 &= 132 \cdot 1 + 114\\
132 &= 114 \cdot 1 + 18\\
114 &= 18 \cdot 6 + 6\\
18 &= 6 \cdot 3 + 0
\end{aligned}$$

Mivel az utolsó nemnulla maradék 6, így $\text{lnko}(246, 132) = 6$.

Az euklideszi algoritmus segítségével bizonyíthatóak a legnagyobb közös osztó alábbi tulajdonságai.

22. Tétel (A legnagyobb közös osztó tulajdonságai).

(1) Bármely két egész számnak van legnagyobb közös osztója.
(2) Ha $a, b \in \mathbb{Z}$, akkor van olyan $u, v \in \mathbb{Z}$, hogy $\text{lnko}(a, b) = ua + vb$.

(3) Ha $a, b, c \in \mathbb{Z}$, akkor $\text{lnko}(ca, cb) = |c| \,\text{lnko}(a, b)$, azaz a legnagyobb közös osztó képzésekor a közös tényező kiemelhető.
(4) Ha $a, b \in \mathbb{Z}$ és legalább az egyik nem nulla, akkor

$$\text{lnko}\left(\frac{a}{\text{lnko}(a,b)}, \frac{b}{\text{lnko}(a,b)}\right) = 1.$$

Két szám legkisebb közös többszörösét is hatékonyan tudjuk számolni.

23. Példa. Határozzuk meg 246 és a 132 legkisebb közös többszörösét. Az 21. Példa alapján tudjuk, hogy $\text{lnko}(246, 132) = 6$. Így a 9. Tétel felhasználásval $\text{lkkt}(246, 132) = \frac{246 \cdot 132}{6} = 5412$.

Felmerülhet a kérdés, hogy miért nem a középiskolában tanult módszerrel határozzuk meg a legnagyobb közös osztót, mely szerint a számok prímtényezős felbontását használjuk. Azonban a problémát az jelenti, hogy hogyan határozzuk meg a számok prímtényezős felbontását. A jelenleg ismert algoritmusok erre a célra teljesen használhatatlanok egy több száz számjegyű szám esetén, és ezen múlik az adataink online biztonsága. Ezzel szemben az euklideszi algoritmus két több száz számjegyű számra is rendkívül gyorsan lefut.

2. Lineáris diofantoszi egyenletek

Gyakran előfordul, hogy egy egyenletnek csak az egész értékű megoldásai érdekelnek minket, főleg, ha az egyenlet valamilyen gyakorlati probléma modellezéséből keletkezett. Az ilyen egyenletek egyik legegyszerűbb formájával ismerkedünk meg ebben a fejezetben.

24. Definíció. Lineáris diofantoszi egyenleten egy

$$ax + by = c$$

egyenletet értünk, ahol $a, b, c \in \mathbb{Z}$, és az x, y ismeretleneket is az egész számok körében keressük.

25. Tétel. A fenti diofantoszi egyenlet pontosan akkor oldható meg, ha $\text{lnko}(a, b) \mid c$. Ha az egyenlet megoldható és (x_0, y_0) egy ismert megoldása, akkor az egyenlet általános megoldása

$$x = x_0 + \frac{b}{\text{lnko}(a,b)} \cdot t, \qquad y = y_0 - \frac{a}{\text{lnko}(a,b)} \cdot t \qquad (t \in \mathbb{Z}).$$

26. Példa. Adjuk meg a $12x + 18y = 186$ diofantoszi egyenlet általános megoldását.

I. Ellenőrizzük, hogy létezik-e megoldása, azaz ki kell számítani a 12 és 18 legnagyobb közös osztóját. Ezt az euklideszi algoritmussal célszerű megtenni, mert később az egész algoritmus számításait fel fogjuk használni. (Természetesen látszik, hogy $\text{lnko}(12, 18) = 6$, de tegyük fel, hogy ezt nem tudjuk ránézésre meghatározni.) Tehát az euklideszi algoritmust végrehajtva:

$$\begin{aligned} 18 &= 12 \cdot 1 + 6, \\ 12 &= 6 \cdot 2 + 0. \end{aligned}$$

Mivel az utolsó nem nulla maradék 6, így $\text{lnko}(12, 18) = 6$, és ezt osztja a 186-ot, tehát van megoldás.

II. Megkeressük az egyenlet egy partikuláris megoldását, azaz a tételben szereplő (x_0, y_0) számpárt. Erre használjuk az euklideszi algoritmus menetét $6 = 18 \cdot 1 - 12 \cdot 1$. Mivel a 6 osztja a 186-ot, így megszorozzuk az egyenlet mindkét oldalát azzal a számmal, hogy bal oldalon 186-ot kapjunk:

$$\begin{aligned} 6 &= 18 \cdot 1 - 12 \cdot 1, \\ (186 =) 6 \cdot 31 &= 18 \cdot 31 - 12 \cdot 31. \\ 186 &= 12 \cdot (-31) + 18 \cdot 31 \end{aligned}$$

Megkaptuk az egyenlet egy partikuláris megoldását: $(x_0, y_0) = (-31, 31)$.

III. A tételbeli képlet segítségével megkapjuk az általános megoldást:

$$x = -31 + 3t \quad \text{és} \quad y = 31 - 2t,$$

ahol $t \in \mathbb{Z}$ tetszőleges egész szám.

27. Példa. Adjuk meg a $97x + 35y = 13$ diofantoszi egyenlet általános megoldását.

I. Meghatározzuk a 97 és 35 legnagyobb közös osztóját.

$$\begin{aligned} 97 &= 35 \cdot 2 + 27, \\ 35 &= 27 \cdot 1 + 8, \\ 27 &= 8 \cdot 3 + 3, \\ 8 &= 3 \cdot 2 + 2, \\ 3 &= 2 \cdot 1 + 1, \\ 2 &= 1 \cdot 2 + 0, \end{aligned}$$

Mivel az utolsó nem nulla maradék 1, így $\text{lnko}(97, 35) = 1$, és ezt osztja a 13-at, tehát van megoldás.

II. Megkeressük az egyenlet egy partikuláris megoldását, azaz a tételben szereplő egy (x_0, y_0) számpárt. Erre használjuk az euklideszi algoritmus végrehajtása során kapott adatokat. Kifejezzük a maradékokat, és egyesével visszahelyettesítjük azokat, a legnagyobb közös osztót kiadó egyenletbe.

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - (8 - 3 \cdot 2) \cdot 1 = 8 \cdot (-1) + 3 \cdot 3 \\ &= 8 \cdot (-1) + 3 \cdot 3 = 8 \cdot (-1) + (27 - 8 \cdot 3) \cdot 3 = 8 \cdot (-10) + 27 \cdot 3 \\ &= 8 \cdot (-10) + 27 \cdot 3 = (35 - 27) \cdot (-10) + 27 \cdot 3 = 35 \cdot (-10) + 27 \cdot 13 \\ &= 35 \cdot (-10) + 27 \cdot 13 = 35 \cdot (-10) + (97 - 35 \cdot 2) \cdot 13 = 35 \cdot (-36) + 97 \cdot 13 \end{aligned}$$

Tehát azt kaptuk, hogy $35 \cdot (-36) + 97 \cdot 13 = 1$. Nekünk az egyenlet jobb oldalán 13-nak kellene lennie, így mindkét oldalt megszorozzuk 13-mal, így azt kapjuk, hogy $35 \cdot (-36) \cdot 13 + 97 \cdot 13 \cdot 13 = 13$, azaz $35 \cdot (-468) + 97 \cdot 169 = 13$. Megkaptuk az egyenlet egy partikuláris megoldását: $(x_0, y_0) = (169, -468)$.

III. A tételbeli képlet segítségével megkapjuk az általános megoldást:

$$x = 169 + 35t \quad \text{és} \quad y = -468 - 97t,$$

ahol $t \in \mathbb{Z}$ tetszőleges egész szám.

3. Kongruencia

28. Definíció. Legyen $a, b, m \in \mathbb{Z}$. Azt mondjuk, hogy a kongruens b-vel modulo m, ha $m \mid a - b$. Jelölésben: $a \equiv b \pmod{m}$.

29. Megjegyzés. Az $a \equiv b \pmod{m}$ kifejezés azt jelenti, hogy a és b ugyanazt a maradékot adják m-mel osztva.

30. Példa. $6 \equiv 4 \pmod{2}$, $22 \equiv -2 \pmod{8}$, $23 \equiv 8 \pmod{5}$.

31. Tétel. Rögzített $m \in \mathbb{N}$, $m \geq 2$ modulus és tetszőleges a_1, b_1, a_2, b_2 egész számok esetén ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \quad \text{és} \quad a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

32. Tétel. Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{\frac{m}{\text{lnko}(m,c)}}$.

3.1. Lineáris kongruencia

33. Definíció. Egy $ax \equiv b \pmod{m}$ alakú kongruenciát lineáris kongruenciának nevezünk, ha $a, b \in \mathbb{Z}$ és $m \in \mathbb{N}$ adott, és $x \in \mathbb{Z}$ ismeretlen.

Egy $ax \equiv b \pmod{m}$ alakú lineáris kongruencia megoldásának kérdése tulajdonképpen ekvivalens az $ax - my = b$ diofantoszi egyenlet megoldásainak kérdésével, természetesen az x-re vonatkozóan. Így a diofantoszi egyenletre vonatkozó tételek átfogalmazhatók lineáris kongruenciákra.

34. Tétel. Az $ax \equiv b \pmod{m}$ kongruencia pontosan akkor oldható meg, ha $\text{lnko}(a, m)$ osztója b-nek. Ha van megoldása, akkor egy x_0 partikuláris megoldás ismeretében az általános megoldás $x \equiv x_0 \pmod{\frac{m}{\text{lnko}(a,m)}}$.

35. Példa. Oldjuk meg a $21x \equiv 14 \pmod{35}$ lineáris kongruenciát.

Első megoldás. Ha a lineáris kongruencia megoldható, akkor a kongruencia jobb oldalát addig növeljük (vagy csökkentjük) a modulus értékével, amíg osztható nem lesz az x együtthatójával: $21x \equiv 14 \equiv 14 + 2 \cdot 35 \pmod{35}$, azaz $21x \equiv 84 \pmod{35}$. A 32. Tétel alapján, ha 21-gyel osztunk, a következőt kapjuk: $x \equiv 4 \pmod{\frac{35}{\text{lnko}(35,21)}}$, tehát a lineáris kongruencia megoldása $x \equiv 4 \pmod{5}$.

Második megoldás. A kongruenciát átírjuk diofantoszi egyenletté. Általában a diofantoszi egyenletre való átírás lényegesen meghosszabbítja a megoldás menetét, az előnye viszont, hogy algoritmikusan végrehajtható. A feladat ekvivalens azzal, hogy oldjuk meg a $21x - 35y = 14$ diofantoszi egyenletet. Mivel $\text{lnko}(21, 35) = 7 \mid 14$, így az egyenlet megoldható. Az egyenlet általános megoldása (ami megkapható a 26. és 27. Példákban látott módon) $x = 4 + 5t$, $y = 2 + 3t$, ahol $t \in \mathbb{Z}$ tetszőleges egész szám. Nekünk csak az x ismeretlen értékére van szükségünk, így a kongruencia általános megoldása $x \equiv 4 \pmod{5}$.

36. Definíció. Lineáris kongruenciarendszernek nevezzük a

$$\begin{aligned} c_1 x &\equiv d_1 \pmod{n_1} \\ &\vdots \\ c_k x &\equiv d_k \pmod{n_k} \end{aligned} \tag{1}$$

alakú kongruenciarendszert, ha $2 \leq k \in \mathbb{N}$, $n_1, \ldots, n_k \in \mathbb{N}$, $c_1, \ldots, c_k, d_1, \ldots, d_k \in \mathbb{Z}$ adott számok, és az $x \in \mathbb{Z}$ ismeretlen.

37. Megjegyzés. A fenti (1) kongruenciarendszer megoldhatóságának szükséges feltétele, hogy a kongruenciák külön-külön megoldhatóak legyenek. Ha megoldhatóak, akkor a kongruenciarendszer

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{2}$$

alakúra hozható.

A kongruenciarendszerek megoldásának menete, hogy felírjuk a kongruenciarendszer (2) alakját, majd kettesével oldjuk meg a kongruenciákat, ahogy azt a következő tétel mutatja.

38. Tétel. Az

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

kongruenciarendszer pontosan akkor oldható meg, ha $\text{lnko}(m_1, m_2) \mid a_1 - a_2$. Amennyiben megoldható és x_0 egy rögzített megoldása, akkor a fenti kongruenciarendszer ekvivalens az alábbi kongruenciával:

$$x \equiv x_0 \pmod{\text{lkkt}(m_1, m_2)}.$$

39. Példa. Oldjuk meg a következő kongruenciarendszert:

$$\begin{aligned} 5x &\equiv 3 \pmod{6} \\ 4x &\equiv 6 \pmod{18}. \end{aligned}$$

Először külön-külön megoldjuk a lineáris kongruenciákat a 35. Példában látott módon, így kapjuk az

$$\begin{aligned} x &\equiv 3 \pmod{6} \\ x &\equiv 6 \pmod{9} \end{aligned}$$

kongruenciarendszert.

Első megoldás. Ha mindkét kongruencia jobb oldalából kivonjuk a megfelelő modulus értékét, mindkét esetben -3-at kapunk, így megkaptuk a kongruenciarendszer egy megoldását ($x_0 = -3$). A 38. Tétel alapján az általános megoldás: $x \equiv -3 \pmod{\text{lkkt}(6, 9)}$, azaz $x \equiv 15 \pmod{18}$.

Másik megoldás. Az első kongruenciából kifejezve az x-et kapjuk, hogy $x = 6k + 3$, ahol $k \in \mathbb{Z}$. Ezt behelyettesítjük a második kongruenciába: $6k + 3 \equiv 6 \pmod{9}$, majd megoldjuk a lineáris

kongruenciát k-ra a 35. Példában látott módon. Így kapjuk, hogy $k \equiv 2 \pmod 3$, ami azt jelenti, hogy $k = 3l + 2$, ahol $l \in \mathbb{Z}$, ezt visszahelyettesítve: $x = 6k + 3 = 6(3l + 2) + 3 = 18l + 15$. Tehát a kongruenciarendszer megoldása: $x \equiv 15 \pmod{18}$.

A következő tétel összefoglalja, hogy mikor oldható meg egy lineáris kongruenciarendszer.

40. Tétel. A (2) kongruenciarendszer pontosan akkor oldható meg, ha bármely kételemű részrendszere megoldható, azaz bármely $1 \leq i < j \leq k$ esetén $\text{lnko}(m_i, m_j) \mid a_i - a_j$. Tehát páronként relatív prím modulusok esetén mindig van megoldás.

41. Tétel (Kínai maradéktétel). Legyenek $m_1, \ldots, m_k$ modulusok páronként relatív prímek, jelölje $M = m_1 m_2 \ldots m_k$ szorzatot, és legyen $M_i = \frac{M}{m_i}$. Továbbá jelölje y_i az $M_i y \equiv 1 \pmod{m_i}$ segédkongruencia egy megoldását. Ekkor a (2) kongruenciarendszer megoldása:

$$x \equiv \sum_{i=1}^{k} a_i M_i y_i \pmod M.$$

3.2. Maradékosztályok

42. Tétel. Legyen $n \in \mathbb{N}$ egy rögzített modulus. Ekkor a

$$\varrho = \{(a, b) \in \mathbb{Z}^2 : a \equiv b \pmod n\} \subseteq \mathbb{Z}^2$$

modulo n kongruencia ekvivalenciareláció a $\mathbb{Z}$ halmazon. (Tehát reflexív, szimmetrikus és tranzitív.)

43. Definíció. A modulo n kongruenciához tartozó osztályozás osztályait modulo n maradékosztályoknak hívjuk, tehát az $a \in \mathbb{Z}$ elemet tartalmazó osztályon az $\overline{a} = \{\, b \in \mathbb{Z} \mid b \equiv a \pmod n \,\}$ halmazt értjük. A modulo n maradékosztályok halmazát $\mathbb{Z}_n$ jelöli, azaz $\mathbb{Z}_n = \{\, \overline{0}, \overline{1}, \ldots, \overline{n-1} \}$.

44. Definíció. Az $\overline{a}$ modulo n maradékosztály redukált maradékosztály, ha $\text{lnko}(a, n) = 1$.

45. Definíció. Az Euler-féle φ-függvénynek nevezzük azt a $\varphi(n)$ függvényt, amely megadja a modulo n redukált maradékosztályok számát, tehát az n-hez relatív prímek számát 0 és $n - 1$ között.

46. Példa. Például $\varphi(1) = 1$, $\varphi(6) = 2$ és ha p prím, akkor $\varphi(p) = p - 1$.

47. Definíció. Az egész számok egy részhalmazát modulo n teljes maradékrendszernek nevezzük, ha minden modulo n maradékosztályból pontosan egy elemet tartalmaz. Az egész számok egy részhalmazát modulo n redukált maradékrendszernek nevezzük, ha minden modulo n redukált maradékosztályból pontosan egy elemet tartalmaz.

48. Példa. Modulo 9 egy teljes maradékrendszer: 1, 4, 7, 8, 12, 18, 33, 38, 41. Modulo 9 egy redukált maradékrendszer: 4, 7, 10, 20, 26, 41, amelynek elemszáma $\varphi(9) = 6$.

A φ függvény értékének meghatározását segítik a következő tételek.

49. Tétel. Ha $m, n \in \mathbb{N}$ relatív prímek, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

50. Tétel. Ha az $n \in \mathbb{N}$ szám prímtényezős alakja $n = \prod_{i=1}^{t} p_i^{k_i}$, akkor

$$\varphi(n) = \prod_{i=1}^{t} \left(p_i^{k_i} - p_i^{k_i - 1} \right) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i} \right).$$

51. Példa. $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\varphi(5^2) = (2^2 - 2^1)(5^2 - 5^1) = 2 \cdot 20 = 40$.

3.3. Hatványozás modulo n

52. Tétel (Euler-Fermat tétel). Ha $n \in \mathbb{N}$ és $a \in \mathbb{Z}$ relatív prímek, akkor

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

53. Példa. Mi az utolsó két számjegye (a tízes számrendszerben) a

$$7^{160002}$$

számnak? Az igazi kérdés itt az, hogy mivel kongruens a 7^{160002} szám modulo 100? Tudjuk, hogy $\varphi(100) = 40$ (lásd az 51. Példa), illetve Euler tétele szerint $7^{40} \equiv 1 \pmod{100}$. Ebből következik, hogy

$$7^{160002} = 7^{4000 \cdot 40 + 2} = \left(7^{40}\right)^{4000} \cdot 7^2 \equiv 1^{4000} \cdot 49 \equiv 49 \pmod{100}.$$

(A kongruenciák végig modulo 100 értendők.)

Mivel tetszőleges p prímre $\varphi(p) = p - 1$ a következőt kapjuk.

54. Tétel (Kis Fermat-tétel). Ha p prímszám és $a \in \mathbb{Z}$, amelyre $p \nmid a$, akkor

$$a^{p-1} \equiv 1 \pmod{p}.$$