1. Bevezetés

A számítógépes hálózatokon keresztül történő kommunikáció térhódítása nyomán előtérbe került az ún. *nyilvános jelkulcsú* titkosítási eljárások iránti igény. A nyilvánosság ebben az esetben azt jelenti, hogy a titkosítás módja (az üzenetek kódolásának és dekódolásának elve) minden, a kommunikációban résztvevő szereplő számára ismert, így a rendszerhez bárki csatlakozhat, ha készít magának egy csakis általa ismert titkos „kulcsot" (bizonyos, a rendszer által előírt szabványok szerint) és nyilvánosságra hoz (mintegy a saját „telefonszámaként") egy másik kulcsot; az előbbi és a címzett nyilvános kulcsa segítségével titkosítja az általa elküldött üzenetet, amelyet a címzett a saját titkos és a feladó nyilvános kulcsa segítségével tud megfejteni. E „kétkulcsos" rendszernek a részletes leírása helyett itt csupán arra a tényre utalunk, hogy az egyik ilyen, széles körben elterjedt rendszer (az RSA-séma) esetében a kulcsok előállításához két nagy (több száz jegyből álló) prímszámra van szükség, és a rendszer eleget tesz annak a kívánalomnak, hogy az A által B-nek írt üzenetet csak B képes megfejteni, viszont bárki képes meggyőződni arról, hogy az üzenet csakis A-tól származhatott, tehát hamisíthatatlan. Ezek az egymásnak ellentmondani látszó követelmények egy roppant „negatív" ténynek köszönhetően elégíthetők ki: jelenleg nem ismert olyan algoritmus, amellyel egy sokszáz jegyű számot prímszámok szorzatára lehetne bontani — természetesen számítógéppel — kevesebb, mint néhány milliárd év leforgása alatt!

Hogyan készíthet viszont magának egy résztvevő ilyen nagy prímszámot? Tegyük fel, hogy találomra választ sok nagy számot, és megnézi, van-e közöttük prím. Megmutatható, hogy ha „elég sokat" választ, akkor a számok között nagy valószínűséggel talál prímet. A kérdés azonban az, hogyan döntse el egy kiválasztott n számról, hogy az prímszám-e. A szám prímtényezőkre bontása, mint arra már utaltunk, reménytelennek látszó próbálkozás.

Fermat tétele szerint $a^{p-1} \equiv 1 \pmod{p}$, ha $(a,\ p) = 1$ és p prím. Ennek nyomán kézenfekvőnek tűnik a következő: választ egy, az n-hez relatív prím a egészet (ez valóban megtehető) majd kiszámítja a^{n-1}-nek az n-nel való osztási maradékát (géppel ez könnyűszerrel elvégezhető). Ha a kapott maradék nem az 1, akkor n bizonyosan nem prím. A másik esetben, ha a maradék 1, nagyon egyszerű lenne feltételezni, hogy n prím; csakhogy néhány összetett n szám is rendelkezik a következő tulajdonsággal:

$$a^{n-1} \equiv 1 \pmod{n} \qquad \text{minden } a\text{-ra, amelyre } (a,\ n) = 1. \tag{1}$$

Ezeket a számokat *Carmichael-számoknak* nevezzük. Ha (1) teljesül n-re, akkor csak abban lehetünk biztosak, hogy a kérdéses szám prím vagy Carmichael-szám.

Azt hogy Carmichael-szám létezik, 1910 óta tudjuk, amikor is R. D. Carmichael megadott néhány ilyen tulajdonságú számot. Bár az első példák 1910-ből valók, az ún. *Korselt-kritérium* 1899-re datálódik:

Egy összetett n szám pontosan akkor Carmichael-szám, ha n négyzetmentes, és minden p prímre $p \mid n$-ből $(p-1) \mid (n-1)$ következik.

Az alábbiakban ezt be is fogjuk bizonyítani. A legkisebb Carmichael-szám $3{\cdot}11{\cdot}17 = 561$, továbbiak: $5{\cdot}13{\cdot}17 = 1105$, $7 \cdot 31 \cdot 73 = 15\,841$.

Ezt követően 1939-ben Chernick [6] talált egy univerzális formulát, amelynek segítségével Carmichael-számokat kaphatunk:

$$U_k(m) = (6m+1)(12m+1)\prod_{i=1}^{k-2}(9 \cdot 2^i m + 1),$$

ha az összes tényező prím.

Mások sok prímtényezős Carmichael-számokat állítottak elő: 1978-ban Yorinaga [7] legfeljebb 15 tényezősöket, Zhang [8] 1305 tényezős, Guillame és Morain [9] 5104 tényezős számokat konstruáltak. Szisztematikus kereséssel Pinch [2] megtalálta az összes Carmichael-számot 10^{16}-ig. Manapság az egyik legnagyobb ismert Carmichael-számnak 1 101 518 tényezője van, Günter Löh és Wolfgang Niebuhr [1] találta 1996-ban.

Persze a legfontosabb kérdés az, hogy van-e végtelen sok Carmichael-szám. A válasz: igen. Ezt W. R. Alford, A. Granville és C. Pomerance [3] bizonyította be 1994-ben, nem elemi úton. A bizonyítás alapjául szolgáló heurisztikus algoritmus Erdős Páltól származik, erre később még vissza fogunk térni.

Az alábbiakban megemlítünk néhány, Carmichael-számot konstruáló algoritmust:

1. Definiáljuk először a λ függvényt: ez n-hez azt a legkisebb $\lambda(n)$ pozitív egészet rendeli, amelyre $a^{\lambda(n)} \equiv 1 \pmod{n}$ minden, az n-hez relatív prím a egészre teljesül. A λ függvénynek fontos tulajdonsága, hogy $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ esetén

$$\lambda(n) = \left[\lambda(p_1^{\alpha_1}),\ \ldots,\ \lambda(p_k^{\alpha_k})\right],$$

és az is belátható, hogy

$$\lambda(p_i^{\alpha_i}) = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1),\ \text{ha } p_i > 2 \text{ vagy } \alpha_i \le 22^{\alpha_i - 2},\ \text{ha } p_i = 2 \text{ és } \alpha_i > 2$$

(φ az Euler-függvényt és $[\ldots]$ a legkisebb közös többszöröst jelöli). Löh és Niebhur algoritmusának alapja R. D. Carmichael tétele, mely szerint *egy összetett N szám pontosan akkor Carmichael-szám, ha* $N \equiv 1 \pmod{\lambda(N)}$.

Legyen N a keresett Carmichael-szám. Az algoritmus egy adott L számmal indul, amelyre $L = \lambda(N)$ teljesül majd. Ezután meghatározzuk N összes lehetséges prímosztóját, tekintetbe véve a Carmichael-féle λ függvény tulajdonságait és a Korselt-kritérium alábbi következményét:

Legyen S az N prímosztóinak a halmaza, az S-beli prímek szorzatának a maradéka L-lel osztva legyen k.

Ha $k = 1$, akkor S elemeinek szorzata Carmichael-szám.

Ha $k > 1$, akkor megkeressük az S-nek egy olyan valódi T részhalmazát, amelyben az elemek szorzata szintén k maradékot ad L-lel osztva. Az S-nek a T-be nem tartozó elemeit összeszorozva kapunk Carmichael-számot.

2. A következő eljárás segítségével határozta meg R. G. E. Pinch [2] a Carmichael-számokat 10^{15}-ig. Két eredményt használt: az egyik N. G. W. H. Beeger [11]-től származik 1950-ből: *ha $r > q > p$ prímek és pqr Carmichael-szám, akkor $2p^2 > q$ és $p^3 > r$.* Ezt később Duparc [12] általánosította: *ha q, r prímek és mqr Carmichael-szám, akkor $2m^2 > q$ és $m^3 > r$.* Ezeket speciális esetekre egyébként R. G. E. Pinch is belátja az említett cikkben, az általános eset szép és rövid bizonyítása például [10]-ben található meg. Az eljárás tulajdonképpen megkeresi minden rögzített d-re a d prímtényezős Carmichael-számokat 10^{15}-ig úgy, hogy rögzít $d-2$ darab prímet a Korselt-kritérium már említett következményét figyelembe véve, és ezekhez keres a fenti tulajdonságok és még néhány egyéb tulajdonság segítségével két új prímtényezőt.

3. H. Dubner [4] is foglalkozott Carmichael-szám konstrukciós algoritmusokkal, cikkében egyiptomi törtek segítségével állít elő Carmichael-számokat. Konstrukciójának az a lényege, hogy minden p_i prímtényezőt $a_iSM + 1$ alakban ír fel. Ekkor a Korselt-kritériumból kapjuk, hogy minden prímtényezőre $\dfrac{SG}{a_i}$ egész, ahol S az a_i-k összege, G pedig egy igen bonyolult kifejezés. Ekkor, mivel G tulajdonságai nehezen meghatározhatóak, S-re teszünk feltételt. Ha S-nek osztója minden a_i, akkor a kritérium teljesül, és a prímek szorzata Carmichael-szám lesz. Ez a feltétel elvezet a tökéletes és a majdnem tökéletes számok elméletéhez, ami kapcsolódik az egyiptomi törtek kérdésköréhez.

4. A legfontosabb algoritmus Erdős Pál nevéhez fűződik. Mint már említettük, végül ennek alapján sikerült bizonyítani azt, hogy végtelen sok Carmichael-szám létezik. A heurisztikus eljárásban olyan L-et keresünk, amelyhez sok olyan p prímszám van, amelyre $p-1$ osztója L-nek. Ha ezek közül néhánynak a szorzata L-lel osztva 1 maradékot ad, akkor ez a szorzat Carmichael-szám. Valóban, a $p-1$ számok osztják L-et, amire nézve a szorzat 1-gyel kongruens, így a Korselt-kritérium alapján a szorzat Carmichael-szám.

A Carmichael-számok elméletében nagyon fontos a Korselt-kritérium. Ennek nem elemi bizonyítása ismert, ld. [10] (a kritériumot csoportelméleti eszközökkel bizonyítja a szerző). Ebben a cikkben olyan bizonyítást mutatunk be a kritériumra, amely nem használja a csoport fogalmát, és rámutatunk néhány fontosabb következményre, mint például arra, hogy miért nincs páros Carmichael-szám. A cikk második részében egy olyan algoritmust írunk le, amely viszonylag gyorsan tud már ismert Carmichael-számokból továbbiakat előállítani . A legnagyobb így konstruált Carmichael-szám a

$$7 \cdot 37 \cdot 541 \cdot 12739 \cdot 10317781 \cdot 22554667081 \cdot 447063138358143121 \cdot$$
$$\cdot 309508589089767668781759436022139311882371 21 =$$
$$= 57477340032203190007788994991884733995704235434402463914610420136262833719214383930262 41.$$

2. A Korselt-kritérium elemi bizonyítása

Az alábbiakban bebizonyítjuk a Korselt-kritériumot. Ehhez két segédtételen keresztül jutunk el. Közülük igazán csak az elsőre lesz szükségünk, a másodikat csupán arra fogjuk használni, hogy az egyik tételre kétféle bizonyítást is adhassunk.

1. Lemma. *Legyenek a, n, x, y pozitív egészek, $(a,\ n) = 1$, $x > y$ és*

$$a^x \equiv 1 \pmod{n}, (1) a^y \equiv 1 \pmod{n}. (2)$$

Ekkor $a^{(x,\ y)} \equiv 1 \pmod{n}$.

Bizonyítás. Felhasználjuk, hogy ha $z = (x,\ y)$, akkor léteznek olyan c, d egészek, amelyekre $z = cx + dy$. Ha (1)-et és (2)-t ezekre a hatványokra emeljük, akkor azt kapjuk, hogy $a^{|c|x} \equiv 1 \pmod{n}$ és $a^{|d|y} \equiv 1 \pmod{n}$. Legyen $r = |c|x$ és $s = |d|y$, ekkor az előzőek $a^r \equiv 1 \pmod{n}$ és $a^s \equiv 1 \pmod{n}$ alakba írhatóak; tegyük fel, hogy például $r > s$, akkor $r - s = cx + dy = z$. Kivonva az utolsó kongruenciát az előzőből: $a^r - a^s = a^s(a^{r-s} - 1) \equiv 0 \pmod{n}$, és így $a^s(a^{r-s} - 1) = kn$ egy alkalmas egész k-ra. De $(a,\ n) = 1$, így $n \mid a^{r-s} - 1$, vagyis $a^z = a^{r-s} \equiv 1 \pmod{n}$.

2. Lemma. *Legyenek $p_1, \ldots, p_k$ páronként különböző prímek, és legyen $n = p_1 \cdot \ldots \cdot p_k$. Ekkor*

$$\sum_{i=1}^{k} \left(\frac{n}{p_i}\right)^{p_i - 1} \equiv 1 \pmod{n}.$$

Bizonyítás. Mivel $\left(\frac{n}{p_i},\ p_i\right) = 1$, felírhatjuk minden i-re a kis Fermat tételt:

azaz

$$\left(\frac{n}{p_i}\right)^{p_i-1} \equiv 1 \pmod{p_i},$$
$$\left(\frac{n}{p_i}\right)^{p_i-1} - 1 = c_i \cdot p_i,$$

alkalmas c_i pozitív egészekkel. Szorozzuk össze ezeket az egyenlőségeket:

$$\prod_{i=1}^{k}\left(\left(\frac{n}{p_i}\right)^{p_i-1} - 1\right) = n \cdot \prod_{i=1}^{k} c_i.$$

A bal oldalon a szorzások elvégzése után egy szorzatokból álló összeget kapunk; ezt az összeget három részre oszthatjuk: az első részben szerepeljenek azok a tagok, amelyek két vagy több $\left(\frac{n}{p_i}\right)^{p_i-1}$ alakú tényezőt tartalmaznak. Ezek a tagok oszthatóak n-nel, így átvihetjük őket a jobb oldalra, ami így osztható marad n-nel. A második rész a

$$(-1)^{k-1} \cdot \sum_{i=1}^{k}\left(\frac{n}{p_i}\right)^{p_i-1}$$

tag, a harmadik pedig $(-1)^k$. Ezek után az egyenletet így írhatjuk:

$$(-1)^{k-1} \cdot \sum_{i=1}^{k}\left(\frac{n}{p_i}\right)^{p_i-1} + (-1)^k = A \cdot n,$$

vagyis

$$\sum_{i=1}^{k}\left(\frac{n}{p_i}\right)^{p_i-1} - 1 \equiv 0 \pmod{n}.$$

Most pedig következik a Korselt-kritérium bizonyítása. Ezt három lépésben tesszük meg.

1. Tétel. *Ha n Carmichael-szám, akkor négyzetmentes.*

Bizonyítás. Tegyük fel, hogy $n = p^2 m$, ahol p prím, és m egész. Írjuk fel n prímtényezős felbontását:

$$n = p^\alpha \cdot \prod_{i=1}^{k} p_i^{\alpha_i},$$

ahol $\alpha \geq 2$. Az n Carmichael-szám, így ha $(a,\ n) = 1$, akkor $a^{n-1} \equiv 1 \pmod{n}$. Az $(a,\ n) = 1$ miatt $(a,\ p) = 1$, és az előző kongruenciából $a^{n-1} \equiv 1 \pmod{p}$. Felírhatjuk az Euler–Fermat tételt a-ra és p^α -ra, mivel $(a,\ p^\alpha) = 1$:

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

Felhasználva az első lemmát: ha $z = (n-1,\ p^{\alpha-1}(p-1))$, akkor $a^z \equiv 1 \pmod{p^\alpha}$. Vizsgáljuk meg z-t! Látható, hogy $z = (n-1,\ p^{\alpha-1}(p-1)) = (n-1,\ p-1)$, mivel ha $p^{\alpha-1} \mid n$, akkor p nem oszthatja $(n-1)$-et. Mivel $\alpha \geq 2$, azért $a^z \equiv 1 \pmod{p^2}$. Viszont $z = (n-1,\ p-1)$, így létezik olyan $t \in \mathbf{Z}^+$, hogy $p-1 = zt$. Így ha az utolsó kongruenciát a t-edik hatványra emeljük, akkor azt kapjuk, hogy $a^{p-1} \equiv 1 \pmod{p^2}$. Legyen $c = p - p^{\varphi(m)+1}$, ekkor az Euler–Fermat tétel szerint $c \equiv p - p = 0 \pmod{m}$, és nyilván $c \equiv p \pmod{p^2}$; speciálisan $(c+1,\ n) = 1$. Legyen $a = c+1$; a binomiális tétel szerint (alkalmas b pozitív egésszel)

$$a^{p-1} = (c+1)^{p-1} = bc^2 + (p-1)c + 1 \equiv (p-1)p + 1 = p^2 - p + 1 \equiv 1 - p \not\equiv 1 \pmod{p^2}.$$

Ellentmondásra jutottunk, tehát nincs olyan p prím, amelyre $p^2 \mid n$.

2. Tétel. *Ha n Carmichael-szám, és p az n prímosztója, akkor $(p-1) \mid (n-1)$.*

Bizonyítás. Mivel n Carmichael-szám, n négyzetmentes, és $a^{n-1} \equiv 1 \pmod{n}$ minden a-ra, ha $(a,\ n) = 1$. Felhasználva a Carmichael-féle λ függvényt és tulajdonságait, azt kapjuk, hogy $a^{\lambda(n)} \equiv 1 \pmod{n}$. Mivel $n = p_1 \cdot \ldots \cdot p_k$, azért $\lambda(n) = [p_1 - 1,\ \ldots,\ p_k - 1]$, és az 1. lemma miatt $\lambda(n) \mid (n-1)$. Így ha $p \mid n$ és n Carmichael-szám, akkor $(p-1) \mid (n-1)$.

3. Tétel. *Ha $n = p_1 \cdot \ldots \cdot p_k$, ahol $p_1,\ \ldots,\ p_k$ páronként különböző prímek, továbbá $(p_i - 1) \mid (n-1)$ $(i = 1,\ \ldots,\ k)$, akkor n Carmichael-szám.*

Bizonyítás. Legyen $(a,\ n) = 1$, és írjuk fel a kis Fermat tételt minden p_i-re ($(a,\ p_i) = 1,\ i = 1, \ldots, k$):

$$1 \equiv a^{p_1-1} \pmod{p_1}, \vdots 1 \equiv a^{p_k-1} \pmod{p_k}.$$

Emeljük az i-edik kongruenciát a $c_i = \dfrac{(n-1)}{(p_i-1)}$-edik hatványra:

$$a^{n-1} \equiv 1 \pmod{p_1}, \vdots a^{n-1} \equiv 1 \pmod{p_k}.$$

Ezen a ponton két lehetőség közül választhatunk: Először nézzük meg az egyszerűbbet. A fenti kongruenciákból következik, hogy $a^{n-1} - 1$ osztható $p_1, \ldots, p_k$-val, tehát $a^{n-1} \equiv 1 \pmod{n}$. A másik lehetőség kissé hosszabb. Tekintsük a kongruenciákat úgy, mint egy szimultán kongruenciarendszert az a^{n-1}-re mint ismeretlenre nézve. Ezek után, felhasználva a kínai maradéktételt és a 2. lemmát, kapjuk, hogy $a^{n-1} \equiv 1 \pmod{n}$.

A Korselt-kritérium bizonyítása után lássuk annak néhány következményét:

1.p_j nem oszthatja $(p_i - 1)$-et $(1 \le j < i \le k)$, mert ez ellentmondana annak, hogy $(p_i - 1) \mid (n - 1)$ és $p_j \mid n$ egyszerre teljesül. Ezért nincs páros Carmichael-szám.

2.Ha n Carmichael-szám és van $4k + 1$ alakú prímosztója, akkor a $4k - 1$ alakú prímosztóinak száma páros. Hasonló igaz 4 helyett 6-ra is. Beláa hosszadalmas.

3.Minden Carmichael-számnak legalább három különböző prímosztója van. Ha ugyanis csak két prímosztója lenne, azaz $n = pq$, ahol p, q prímek, akkor:

$$\frac{pq-1}{q-1} = \frac{pq-p+p-1}{q-1} = p + \frac{p-1}{q-1} \text{ egész,}$$

így $\dfrac{p-1}{q-1}$ egész, és ugyanígy $\dfrac{q-1}{p-1}$ is egész; tehát $\dfrac{p-1}{q-1} = 1$, amiből $p = q$ következik, de ez ellentmond a négyzetmentes tulajdonságnak.

3. Carmichael-számok konstruálása Carmichael-számokból

Az alábbiakban azt vizsgáljuk meg, miként lehet és érdemes Carmichael-számokat konstruálni már ismertekből. Elsőként a számtani sorozat lehetőségét vizsgáljuk. Megmutatjuk, hogy ilyen módon csak nagyon korlátozott mértékben juthatunk Carmichael-számokhoz, sőt az azoknál lényegesen gyakoribb négyzetmentes számokhoz.

4. Tétel. *A négyzetmentes számok halmazában nincs végtelen számtani sorozat.*

Bizonyítás. Tegyük fel, hogy létezik egy kívánt sorozat. Legyen $p_1p_2 \ldots p_n$ az első elem és d a differencia. Ekkor a sorozat minden eleme $p_1p_2 \ldots p_n + kd$ alakba írható, és ezek a számok négyzetmentesek. Tehát p_i^2 nem lehet osztója $p_1 \ldots p_n + kd$-nek semmilyen i-re és k-ra. Minden i-re két lehetőség van: $(d,\ p_i) = 1$ vagy $(d,\ p_i) = p_i$. Ha $(d,\ p_i) = 1$, akkor létezik olyan x, amelyre

$$xd \equiv -p_1 \ldots p_{i-1}p_{i+1} \ldots p_n \pmod{p_i},$$

így p_i-vel beszorozva:

$$p_1 \ldots p_n + p_i xd \equiv 0 \pmod{p_i^2};$$

tehát ekkor $k = p_i x$ választással egy olyan tagját találtuk meg a sorozatnak, amelynek van négyzetszám osztója. Ezért minden i-re $(d,\ p_i) = p_i$, tehát $d = p_1 \ldots p_n d_1$.

A sorozat k-adik eleme:

$$p_1 \ldots p_n + kd = p_1 \ldots p_n + kp_1 \ldots p_n d_1 = p_1 \ldots p_n(1 + kd_1).$$

A fenti okoskodást folytathatjuk d_1-re: ha $(d_1, p_i) = 1$, akkor p_i-hez létezik olyan x_i, amelyre

$$x_i d_1 \equiv -1 \pmod{p_i},$$

és akkor $p_i \mid x_i d_1 + 1$, tehát $p_i^2 \mid p_1 \ldots p_n(x_i d_1 + 1)$, ellentmondás.

Tehát azt kaptuk, hogy $p_i^2 \mid d$ minden $i = 1, \ldots, n$-re. Legyen $a = p_1 \ldots p_n$; ezzel a jelöléssel minden elem $a + ka^2 d_2$ alakba írható. De $a + ka^2 d_2 = a(1 + kad_2)$-ben $k = ad_2 + 2$-t helyettesítve:

$$a(1 + kad_2) = a(1 + (ad_2 + 2)ad_2) = a(1 + 2ad_2 + (ad_2)^2) = a(1 + ad_2)^2.$$

Így ellentmondásra jutottunk, megmutattuk hogy minden végtelen számtani sorozatban van olyan elem, amelynek osztója egy négyzetszám.

Megjegyzés. Ugyanennek a tételnek egy elegánsabb és jól általánosítható bizonyítását adta Wladyslaw Narkiewicz egy levelében, a tétel bizonyítását egy két tagból álló szimultán kongruenciarendszer megoldására vezetve vissza.

A következőkben megvizsgáljuk, mikor lehet két Carmichael-szám szorzata is Carmichael-szám. Ezzel azonban a négyzetmentes tulajdonság miatt Carmichael-számok véges halmazából csak véges halmazt tudunk előállítani. A $\lambda(N)$ függvény segítségével egyszerű választ adhatunk a fenti kérdésre. A kapott feltétel a Korselt-kritérium következménye.

5. Tétel. *Legyenek N és Q Carmichael-számok. Az NQ szám pontosan akkor Carmichael-szám, ha $(N,\ Q) = 1$, valamint $N \equiv 1 \pmod{\lambda(Q)}$ és $Q \equiv 1 \pmod{\lambda(N)}$.*

Bizonyítás. $(N,\ Q) = 1$ szükséges a szorzat négyzetmentességéhez. A Korselt-kritériumot fogjuk használni: NQ Carmichael-szám, ha $p \mid NQ$-ból $p - 1 \mid NQ - 1$ következik. Legyen $N = p_1 \ldots p_k$, $Q = q_1 \ldots q_s$. Ezzel a jelöléssel a feltétel az, hogy az $\dfrac{NQ-1}{p_i-1}$ és az $\dfrac{NQ-1}{q_j-1}$ hányadosok értéke egész legyen.

Alakítsuk át ezeket a kifejezéseket:

$$\frac{NQ-1}{p_i-1} = \frac{NQ-Q+Q-1}{p_i-1} = \frac{Q(N-1)}{p_i-1} + \frac{Q-1}{p_i-1}.$$

Mivel N Carmichael-szám, azért $\dfrac{N-1}{p_i-1}$ egész, így $\dfrac{Q-1}{p_i-1}$-nek kell egésznek lennie, ha $i = 1, \ldots, k$; ez viszont akkor és csak akkor teljesül, ha $Q \equiv 1 \pmod{[p_1 - 1, \ldots, p_k - 1]}$. A Carmichael-függvényt használva ez éppen azt jelenti, hogy $Q \equiv 1 \pmod{\lambda(N)}$. A másik kongruencia ugyanígy látható be.

A következőkben azt az esetet vizsgáljuk meg, amikor nem egy Q Carmichael számot, hanem csupán egy négyzetmentes R számot választunk az N-hez szorzónak. Ekkor, ha $N = p_1 \ldots p_k$, $R = q_1 \ldots q_s$, annyit mondhatunk, hogy

$$\frac{NR-R+R-1}{p_i-1} = \frac{R(N-1)}{p_i-1} + \frac{R-1}{p_i-1}$$

szerint $R \equiv 1 \pmod{\lambda(N)}$ szükséges, de a másik esetben ez nem működik, mivel nem tudjuk, van-e egyáltalán olyan j, amelyre $\dfrac{R-1}{q_j-1}$ egész. Az előző bizonyítás gondolatmenetét használva mindössze annyit állíthatunk, hogy $\dfrac{\frac{NR}{q_j}-1}{q_j-1}$ egész kell legyen minden $j = 1, \ldots, s$-re. Ezek alapján konstruálhatunk egy algoritmust ilyen R-ek keresésére, de az bonyolult és lassú lenne a négyzetmentesség vizsgálata miatt. Ezért N-et csak egyetlen prímmel szorozzuk; legyen ez a prím q. Ekkor a Korselt-kritérium alapján

$$\frac{Nq-1}{q-1} = \frac{Nq-N+N-1}{q-1} = N + \frac{N-1}{q-1} \text{ egész,}$$

így $\dfrac{N-1}{q-1}$ egész, és ha $N = p_1 \ldots p_k$ és $i = 1, \ldots, k$, akkor

$$\frac{Nq-1}{p_i-1} = \frac{Nq-q+q-1}{p_i-1} = \frac{q(N-1)}{p_i-1} + \frac{q-1}{p_i-1} \text{ egész.}$$

Mivel N Carmichael-szám, azért $\dfrac{q-1}{p_i-1}$ egész kell legyen minden $i = 1, \ldots, k$-ra. Ez azt jelenti, hogy $[p_1 - 1, \ldots, p_k - 1] \mid q - 1$, vagyis $\lambda(N) \mid (q-1)$.

Ezek és az előző megállapítások alapján, ha létezik olyan k, amelyre $q = k\lambda(N) + 1$ prím, és $\dfrac{N-1}{k\lambda(N)}$ egész, akkor Nq Carmichael-szám. *Dirichlet* tétele szerint az $n\lambda(N) + 1$ ($n \in \mathbf{Z}^+$) számtani sorozatban végtelen sok prímszám található, így van rá esélyünk, hogy kívánt alakú prímet találjunk. Vajon találhatunk-e egy újabb p prímet Nq-hoz? Talán igen. Az előzőek alapján p-t így kereshetjük: kiszámítjuk $\lambda(Nq)$-t és $\dfrac{Nq-1}{\lambda(Nq)}$-t, meghatározzuk $\dfrac{Nq-1}{\lambda(Nq)}$ összes osztóját, ezeket megszorozzuk $\lambda(Nq)$-val, és hozzáadunk 1-et, végül megnézzük, hogy ezek közül melyik prím. Ebben az algoritmusban $\lambda(Nq)$ nagyon fontos, és úgy tűnik, nehéz kiszámítani. Szerencsére ez nincs így. Ha ismerjük $\lambda(N)$-et az előző ciklusból, akkor könnyen kiszámítható $\lambda(Nq)$:

$$\lambda(N) = [p_1 - 1, \ldots, p_k - 1], \lambda(Nq) = [p_1 - 1, \ldots, p_k - 1, q - 1], \qquad \text{de } q = k_1\lambda(N) + 1, \text{ így} \lambda(Nq) = \big[p_1 - 1, \ldots, p_k - 1, k_1[p_1 - 1, .$$

Ezek alapján a következő algoritmust alkothatjuk meg:

1.[inicializálás] $m_0 := \lambda(N)$, $i := 1$, $k_0 := 1$;

2.[a Carmichael függvény értéke] $m_i := k_{i-1}^{(j)} m_{i-1}$;

3.$r_i := \dfrac{N_{i-1}^{(j)} - 1}{m_i}$;

4.meghatározzuk az összes olyan j-t, amelyre $k_i^{(j)} \mid r_i$; legyen a megfelelő j indexek halmaza J;

5.[prímtesztek] a $k_i^{(j)} m_i + 1$ számok prímségi tesztelése; legyen A azon j indexek halmaza, amelyekre $k_i^{(j)} m_i + 1$ prím; ha A üres, akkor a ciklus véget ér;

6.[az újabb Carmichael-szám] $N_i^{(j)} := N_{i-1}^{(l)}(k_i^{(j)} m_i + 1)$;

7.[ciklusléptetés] vissza a 2. lépésre: $i := i + 1$;

Az első lépés előtt $m_0 = \lambda(N)$-et és $k_0 = 1$-et kell megadni az induláshoz, ahol N a kiindulásul vett Carmichael-szám. Mivel egy ciklusban több $k_i^{(j)} m_i + 1$ alakú prímet is találhatunk, azért ezt az algoritmust kombinálni kell egy *backtrack* (visszaléptető) algoritmussal, hogy megtaláljuk az összes lehetséges Carmichael-számot. Ez az algoritmus egyszerűnek tűnik, azonban tartalmaz néhány bonyolult számítást, amelyek hosszú időt vehetnek igénybe.

A kritikus lépések a következők:

1.$\dfrac{N_{i-1}^{(l)} - 1}{m_i}$ kiszámítása;

2.$k_i^{(j)}$-k keresése;

3.a $k_i^{(j)} m_i + 1$ számok prímségi tesztelése.

Az utolsó problémára nagyon jó és gyors tesztek vannak. Véleményem szerint, ha a három esetet párhuzamosan kezeljük, akkor ezzel eléggé meggyorsíthatjuk az algoritmust. Az összekötő kapocs a számok ábrázolása. Ha a számokat prímhatványok szorzataként ábrázolnánk, akkor nagyon gyorsan lehetne osztani, osztókat meghatározni és $n-1$ prímfelbontása ismeretében viszonylag gyorsan meg lehet határozni n prím voltát. Tehát ha találnánk egy viszonylag gyors algoritmust n prímfelbontására $n-1$ prímfelbontásának ismeretében, akkor az egész algoritmus sokat gyorsulna. A prímtesztben a $k_i^{(j)} m_i + 1$ kifejezésben $k_i^{(j)}$ is nagyon fontos. Szerencsére r_i nagyságát jól tudjuk becsülni N_{i-2} nagyságával:

$$r_i = \frac{N_{i-1} - 1}{m_i} = \frac{N_{i-2}(k_{i-1}^{(j)} m_{i-1} + 1) - 1}{k_{i-1}^{(j)} m_{i-1}} = N_{i-2} + \frac{N_{i-2} - 1}{m_{i-1}} \frac{1}{k_{i-1}^{(j)}} = N_{i-2} + \frac{r_{i-1}}{k_{i-1}^{(j)}},$$

ezért $r_i \geq N_{i-2}$ minden lehetséges i-re, N_{i-2} értéke pedig minden ciklusban egy prímszorzóval növekszik, r_i is legalább így növekszik, és minden reményünk megvan arra, hogy egy nagy számnak sok $k_i^{(j)}$ osztója legyen.

Irodalomjegyzék

[1]*G. Löh* és *W. Niebuhr:* A new algorithm for constructing large Carmichael numbers, Math. of Comput. 65 (1996) 823–836.

[2]*R. G. E. Pinch:* The Carmichael numbers up to 10^{15}, Math. of Comput. **61** (1993), 381–391.

[3]*W. R. Alford, A. Granville* és *C. Pomerance:* There are infinitely many Carmichael numbers, Annals of Math., **140** (1994), 703–722.

[4]*H. Dubner:* Carmichael numbers and egyptian fractions, Math. Japonica **43** (1996), 411–419.

[5]*D. E. Knuth:* The art of computer programming, Vol 2., 2. edition, section 4.5.4.

[6]*J. Chernick:* On Fermat's simple theorem, Bull. Amer. Math. Soc. **45** (1939), 269–274.

[7]*M. Yorinaga:* Numerical computations of Carmichael numbers, Math. J. Okayama Univ. **20** (1978), 151–163.

[8]*M. Zhang:* Searching for large Carmichael numbers, Sichuan Daxue Xuebao **29,** 472–474 (1992).

[9]*D. Guillame* és *F. Morain:* Building Carmichael numbers with a large number of prime factors and generalization to other numbers, preprint, June (1992).

[10]*C. Pomerance:* Carmichael numbers, 28th Nederlands Matematisch Congres, Delft, April 22, 1992.

[11]*N. G. W. H. Beeger:* On composite numbers n for which $an - 1 \equiv 1 \pmod{n}$ for every a prime to n, Scripta Math. **16,** (1950) 133–135.

[12]*H. J. A. Duparc:* On Carmichael numbers, Simon Stevin **29,** (1952) 21–24.

Járási István
matematikus egyetemi hallgató,
Debreceni Egyetem