A 31, 331, 3331, 33331, 333331, 3333331, 33333331 számok mind prímek. Ezt úgy is kifejezhetjük, hogy a $(10^n-7)/3$ képlet prímszámot szolgáltat az $n = 2, 3, \ldots, 8$ értékek mindegyikére. A $333333331 = (10^9 - 7)/3$ szám azonban már összetett, mert osztható 17-tel. Ezt az osztás elvégzése nélkül is beláthatjuk a kongruencia jelölésének felhasználásával. Azt mondjuk, hogy a kongruens b-vel modulo m (képletben $a \equiv b \pmod m$), ha a és b azonos maradékot adnak m-mel osztva; azaz, ha $a - b$ osztható m-mel. Könnyű ellenőrizni, hogy azonos modulushoz tartozó kongruenciákat szabad összeadni és szorozni. Azaz, ha $a \equiv b \pmod m$ és $c \equiv d \pmod m$, akkor $a+c \equiv b+d \pmod m$ és $a \cdot c \equiv b \cdot d \pmod m$.

Mivel $102 = 17 \cdot 6$, így $10^9 = 100^4 \cdot 10 \equiv (-2)^4 \cdot 10 \equiv -10 \equiv 7 \pmod{17}$, tehát $10^9 - 7$ osztható 17-tel. Meg lehet mutatni egyébként, hogy $33\ldots331$ sohasem osztható a 2, 3, 5, 7, 11, 13, 37 prímek egyikével sem. Nem ismeretes, hogy van-e végtelen sok $33\ldots331 = (10^n - 7)/3$ alakú prímszám. Ez a kérdés minden bizonnyal éppolyan nehéz, mint hogy van-e végtelen sok $2^n - 1$ alakú, ún. Mersenne-prím. Az utóbbi probléma pedig több száz éve megoldatlan.

Az alábbi táblázatban a bekeretezett (nem áthúzott) számok sokáig prímeknek bizonyultak:

19 21 **23** 25 27 **29** 31 33 35 **37** 39 41 43 45 **47** 49 51 53 55 57 **59** 61 63 65 67 69 71 **73** 75 77 79 81 83 85 87 **89** 91 93 95 97 99 101 103 105 **107** 109 111 113 ....

De mégsem lesz mindegyikük prím. A k-adik bekeretezett szám ugyanis $17 + (1 + 2 + \cdots + k) \cdot 2 = k^2 + k + 17$, és ez biztosan összetett $k = 16$-ra, hiszen ekkor $k^2 + k + 17 = k(k + 1) + 17 = 17^2$. Meglepő módon a $k^2 + k + 17$ képlet a $k = 0, 1, \ldots, 15$ helyettesítési értékek mindegyikére prímet ad.

Ha meg akarjuk keresni azokat a p pozitív egészeket, amelyekre $k^2 + k + p$ prímszám a $k = 0, 1, \ldots, p - 2$ értékek mindegyikére, akkor a következőképpen okoskodhatunk. Először is ($k = 0$-t véve) p prímszám kell, hogy legyen. Ha $p > 3$, akkor az $1^2 + 1 + p$ és $2^2 + 2 + p$ számok nem lehetnek sem 3-mal, sem 5-tel oszthatók, így p 3-mal osztva 2-t, 5-tel osztva pedig 1-et vagy 2-t ad maradékul. Mivel p páratlan is, ezért a 30-cal való osztási maradéka csak 11 vagy 17 lehet. Egy további feltétel, hogy $4p-1$-nek is prímnek kell lennie. Tegyük fel ugyanis, hogy $d \mid 4p-1$ és $1 < d < 4p-1$. Ekkor $d \le (4p - 1)/3$ és $d = 2x + 1$, ahol tehát

$$x < \frac{d}{2} \le \frac{4p-1}{6} \le p - 2,$$

ha $p > 5$. Így x^2+x+p-nek prímnek kell lennie. Azonban d osztója $4(x^2+x+p) = (2x+1)^2+4p-1 = d^2+(4p-1)$-nek, tehát x^2+x+p-nek is, hiszen páratlan. Ez csak úgy lehetséges, ha $d = 2x+1 = x^2+x+p > x^2+x+2$, $x^2-x+1 < 0$, ami lehetetlen.

Azt kaptuk tehát, hogy vagy $p = 2, 3, 5$, vagy pedig p olyan $30k + 11$ vagy $30k + 17$ alakú prímszám, amelyre $4p - 1$ is prím. A 100-nál kisebb számok közül ezeket a feltételeket csak a 2, 3, 5, 11, 17, 41, valamint a 71 elégítik ki. Ezek közül a $p = 2, 3, 5, 11, 17, 41$ számokra valóban teljesül, hogy $k^2 + k + p$ prímszám a $k = 0, 1, \ldots, p - 2$ értékek mindegyikére. A 71-re ez már nem igaz, mert $2^2 + 2 + 71 = 77$ összetett. Sokáig megoldatlan volt, hogy a 41 után van-e még ilyen tulajdonságú szám. Csak az 1960-as években sikerült bebizonyítani, hogy ilyen szám nem létezik.

$\star$

A fentiek alapján természetesen vetődik fel az a kérdés, hogy van-e olyan képlet, amelynek a pozitív egészekben felvett értékei mind prímek. Először megmutatjuk, hogy egy egész együtthatós polinom – hacsak nem konstans – nem szolgáltathat ilyen képletet. Ennek bizonyításához két segédtételre lesz szükségünk. Először is belátjuk, hogy ha $p(x) = c_k x^k + c_{k-1}x^{k-1} + \ldots + c_0$ egész együtthatós polinom, akkor $a \equiv b \pmod m$ esetén $p(a) \equiv p(b) \pmod m$. Valóban,

$$p(b) - p(a) = c_k(b^k - a^k) + c_{k-1}(b^{k-1} - a^{k-1}) + \ldots + c_1(b - a). \tag{1}$$

Itt $b^i - a^i$-ből $(b - a)$ kiemelhető: $b^i - a^i = (b - a)(b^{i-1} + b^{i-2}a + \ldots + ba^{i-2} + a^{i-1})$. Ha (1) jobb oldalának minden tagjából kiemeljük $b - a$-t, akkor azt kapjuk, hogy $p(b) - p(a) = (b - a) \cdot A$, ahol A egész szám, hiszen a, b, c_0, ..., c_k mindannyian egészek. Így $p(b) - p(a)$ osztható $b - a$-val. Ha $a \equiv b \pmod m$, akkor m osztója $b - a$-nak, tehát $p(b) - p(a)$-nak is, azaz $p(a) \equiv p(b) \pmod m$.

A másik állítás, amelyre szükségünk van, azt állítja, hogy ha a

$$p(x) = c_k x^k + c_{k-1}x^{k-1} + \ldots + c_0$$

polinom nem konstans és a főegyütthatója pozitív, akkor $p(x)$ minden előre megadott számnál nagyobb lesz, ha x elég nagy. Ezt így láthatjuk be: Jelöljük a $|c_{k-1}| + \ldots + |c_1| + |c_0|$ számot c-vel. Ha $x > 1$, akkor $1 < x < x^2 < \ldots < x^{k-1}$, tehát

$$\begin{gathered} p(x) \ge c_k x^k - |c_{k-1}|x^{k-1} - \ldots - |c_1|x - |c_0| \ge \\ \ge c_k x^k - |c_{k-1}|x^{k-1} - \ldots - |c_1|x^{k-1} - |c_0|x^{k-1} = \\ = c_k x^k - cx^{k-1} = x^{k-1}(c_k x - c). \end{gathered}$$

Ha $x > c/c_k$, akkor $c_k x - c > 0$, tehát $x > 1$ alapján $p(x) > c_k x - c$. Ha tehát azt akarjuk, hogy $p(x)$ nagyobb legyen egy előre megadott $K > 0$ számnál, akkor x-et elég úgy választani, hogy nagyobb legyen 1 és $(c+K)/c_k$ mindegyikénél. Ekkor ugyanis a fentiek szerint $p(x) > c_k x - c > K$ teljesülni fog.

Világos, hogy ha p nem konstans, és a főegyütthatója negatív, akkor $p(x)$ minden előre magadott számnál kisebb lesz, ha x elég nagy.

Most már könnyen beláthatjuk, hogy ha az egész együtthatós $p(x)$ polinom nem konstans, akkor a $p(n)$ értékek nem lehetnek mind prímek. Válasszunk ugyanis egy olyan n_0 pozitív egészet, amelyre $|p(n_0)| = m > 1$. Ha $n = n_0 + i \cdot m$ ($i = 1, 2, \dots$), akkor $n \equiv n_0 \pmod{m}$, tehát $p(n) \equiv p(n_0) = \pm m \equiv 0 \pmod{m}$, azaz $p(n)$ osztható m-mel. De tudjuk, hogy $|p(x)| > m$, ha x elég nagy; mondjuk, ha $x > x_0$. Ekkor minden elég nagy i-re $n = n_0 + i \cdot m > x_0$, így $|p(n)| > m$ és $p(n)$ osztható m-mel, tehát $p(n)$ összetett.

A polinomoknál jóval komplikáltabb képletekről is beláthatjuk, hogy nem szolgáltathatnak csupa prímszámot. Ennek tárgyalásához szükségünk lesz az ún. „kis Fermat-tételre", ami azt állítja, hogy ha p prím és n nem osztható p-vel, akkor $n^{p-1} \equiv 1 \pmod{p}$. Ezt így láthatjuk be:

Az n, $2n$, $\dots$, $(p-1)n$ számok csupa különböző maradékot adnak p-vel osztva. Valóban, ha $in \equiv jn \pmod{p}$, akkor $p \mid in - jn = (i-j)n$. Mivel p prím és n nem osztható p-vel, ebből következik, hogy $p \mid i - j$. Ha tehát $1 \le i, j \le p-1$, akkor szükségképpen $i = j$.

Mivel az $n, 2n, \dots, (p-1)n$ számok egyike sem osztható p-vel, ebből következik, hogy a p-vel vett osztási maradékaik az $1, 2, \dots, p-1$ számok (esetleg más sorrendben). Így $n \cdot 2n \cdots (p-1)n \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$, azaz $n^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Ezért $p \mid \left(n^{p-1} - 1\right)(p-1)!$, tehát $p \mid \left(n^{p-1} - 1\right)$, hiszen p nem osztója $(p-1)!$-nak.

Ennek felhasználásával lássuk be például, hogy az $f(n) = 22^n + 18^n + 1$ képlet nem szolgáltathat csupa prímet. Az $f(1) = 41$ érték mindenesetre prím, ezért $22^{40} \equiv 1 \pmod{41}$ és $18^{40} \equiv 1 \pmod{41}$. Ebből következik, hogy $22^{40k} \equiv 1 \pmod{41}$ és $18^{40k} \equiv 1 \pmod{41}$ minden k pozitív egészre. Ha tehát $n = 40k + 1$, akkor

$$22^n + 18^n + 1 = 22^{40k+1} + 18^{40k+1} + 1 =$$
$$= 22 \cdot 22^{40k} + 18 \cdot 18^{40k} + 1 \equiv 22 + 18 + 1 = 41 \equiv 0 \pmod{41},$$

és így $f(40k+1)$ nem lehet prím, ha $k > 0$.

Most bizonyítsuk be, hogy az

$$f(n) = 100(n^2 + n)^{n^3+n^2+2n} + 1$$

képlet sem szolgáltathat csupa prímet! (Ez kicsit nehezebb lesz.) Először is válasszunk egy olyan n_0 pozitív egészet, amelyre $p = f(n_0) > n_0^2 + n_0$. Ilyen például $n_0 = 1$, amikor is $p = 1601 > 2$. Ha p összetett szám, akkor máris beláttuk, hogy f értékei a pozitív egészekben nem mind prímek. Ha p prím (mint az adott esetben is), akkor tekintsük az $n = n_0 + ip(p-1)$ alakú számokat, ahol $i = 1, 2, \dots$. Belátjuk, hogy ezekre az n-ekre $f(n)$ mindig osztható p-vel. Valóban, rögzítsünk egy ilyen n-et, és tekintsük a $q(x) = 100x^{n^3+n^2+2n}+1$ polinomot. Tudjuk, hogy ha $a \equiv b \pmod{m}$, akkor $q(a) \equiv q(b) \pmod{m}$. Mivel $n \equiv n_0 \pmod{p}$, ezért $q(n) \equiv q(n_0) \pmod{p}$, azaz

$$f(n) = 100(n^2 + n)^{n^3+n^2+2n} + 1 \equiv 100(n_0^2 + n_0)^{n^3+n^2+2n} + 1 \pmod{p}. \tag{2}$$

Ugyanígy, felhasználva, hogy $n \equiv n_0 \pmod{p-1}$, azt kapjuk, hogy $n^3 + n^2 + 2n \equiv n_0^3 + n_0^2 + 2n_0 \pmod{p-1}$, tehát $n^3 + n^2 + 2n = n_0^3 + n_0^2 + 2n_0 + c(p-1)$, ahol c pozitív egész. Ezt (2)-be helyettesítve azt kapjuk, hogy

$$f(n) \equiv 100(n_0^2 + n_0)^{n_0^3+n_0^2+2n_0+c(p-1)} + 1 \equiv\equiv 100(n_0^2 + n_0)^{n_0^3+n_0^2+2n_0} \cdot (n_0^2 + n_0)^{c(p-1)} + 1 \pmod{p}. \tag{3}$$

Mivel $1 \le n_0^2 + n_0 < p$, ezért a kis Fermat-tétel szerint $(n_0^2 + n_0)^{(p-1)} \equiv 1 \pmod{p}$, és így, tekintve, hogy c pozitív egész, azt kapjuk, hogy $(n_0^2 + n_0)^{c(p-1)} \equiv 1 \pmod{p}$. Ezt (3)-ba helyettesítve:

$$f(n) \equiv 100(n_0^2 + n_0)^{n_0^3+n_0^2+2n_0} + 1 = p \equiv 0 \pmod{p},$$

tehát $f(n)$ valóban osztható p-vel. Mivel f szigorúan monoton növő, ezért $i > 0$-ra $n = n_0 + ip(p-1) > n_0$-ból $f(n) > f(n_0)$ következik, ezért $f(n)$ összetett szám lesz. Így például f értéke az $1 + 1601 \cdot 1600 = 2561601$ helyen osztható 1601-gyel, és ezért összetett.

A következő általános tétel hasonló módszerrel bizonyítható. *Legyen $f(n)$ olyan képlet, amely $p(n)^{q(n)}$ alakú kifejezések szorzatainak összege, ahol $p(n)$ és $q(n)$ egész együtthatós polinomok, melyek közül a $q(n)$-ek főegyütthatói pozitívak. Ha az $f(n)$ ($n = 1, 2, \dots$) értékek között van végtelen sok különböző, akkor ezen értékek között van végtelen sok összetett szám.*

Itt a végtelen sok különböző értékre vonatkozó feltétel lényeges, mert pl. az $f(n) = 18 + (-1)^n$ képlet a fenti alakú és f minden értéke prím.

$\star$

A fenti tétel azt állítja, hogy ha $f(n)$ csupa prímszámot ad minden n pozitív egészre, akkor az f-et definiáló képlet a fent leírtaknál bonyolultabb kell, hogy legyen. Ha például olyan prímképletet keresünk, amelyben csak az összeadás, kivonás, szorzás és hatványozás műveleteit használhatjuk, akkor szerepelnie kell benne olyan „emeletes hatványnak" (azaz kitevőben szereplő hatványnak), amelynek a kitevője tartalmazza az n változót. A legegyszerűbb ilyen képlet: 2^{2^n}. Ez persze $n > 0$-ra nem ad prímeket, mert mindig páros. De mi a helyzet a $2^{2^n} + 1$ képlettel? Az $n = 0, 1, 2, 3, 4$

számokat behelyettesítve a 3, 5, 17, 257, 65537 értékeket kapjuk; mindnyájan prímek. Ennek alapján Pierre de Fermat azt sejtette (1640 körül), hogy $F_n = 2^{2^n} + 1$ minden n-re prímszám. Ez a sejtés csaknem 100 éven át megoldatlan maradt, mert a következő szám:

$$F_5 = 2^{2^5} + 1 = 4294967297$$

már olyan nagy, hogy annak eldöntése, hogy prím-e vagy sem, reménytelennek látszott. Valóban, gondoljunk csak bele: ha sem kalkulátor, sem számítógép nem állna rendelkezésünkre, el tudnánk-e dönteni, hogy F_5 prím-e? Volna-e jobb ötletünk, mint elosztani F_5-öt minden nála kisebb számmal? Persze elég volna csupán a $\sqrt{F_5}$-nél nem nagyobb számokkal osztani, hiszen ha egy n szám összetett, akkor van olyan d osztója, amelyre $1 < d \le \sqrt{n}$. Az adott esetben tehát csak a 65536-nál nem nagyobb számokkal kellene osztani; sőt, ezek közül elég lenne a prímeket venni, melyek száma kb. 6500. Ha minden osztás két percet vesz igénybe, még ez is 200 óra munka volna; nem csoda, ha olyan sokáig senki nem vállalkozott rá.

Végül is Leonhard Euler volt az, aki 1732-ben a kérdést eldöntötte. Euler felismerte, hogy F_n prímosztói csak speciális alakúak lehetnek, nevezetesen F_n minden prímosztója $k \cdot 2^{n+1}+1$ alakú, ahol k pozitív egész. Ezt a következőképpen láthatjuk be. Legyen p egy prímosztója F_n-nek. Mivel p páratlan, ezért a kis Fermat-tétel szerint $2^{p-1} \equiv 1 \pmod p$. Legyen d a legkisebb pozitív egész, amelyre $2^d \equiv 1 \pmod p$. Ekkor a 2-hatványok p-vel való osztási maradékai d szerint periodikus sorozatot alkotnak. Valóban, $2^d \equiv 1 = 2^0$ alapján $2^{d+1} \equiv 2 = 2^1$, $2^{d+2} \equiv 2 \cdot 2^1 = 2^2$, $2^{d+3} \equiv 2 \cdot 2^2 = 2^3$, és hasonlóan, $2^{d+i} \equiv 2^i$ minden i-re (a kongruenciákat (mod p) értve). Ebből következik, hogy $2^{s \cdot d} \equiv 1$ minden $s = 1, 2, \ldots$-re. Másrészt d választása folytán $2^i \not\equiv 1$ ha $0 < i < d$, ezért a periodicitásból következik, hogy 2^m akkor és csak akkor ad 1 maradékot p-vel osztva, ha m osztható d-vel.

Mármost $2^{2^{n+1}} \equiv 1 \pmod p$, ugyanis $2^{2^{n+1}} - 1 = \left(2^{2^n} + 1\right) \cdot \left(2^{2^n} - 1\right)$, tehát $2^{2^{n+1}} - 1$ osztható F_n-nel, tehát p-vel is. A fentiek szerint ebből következik, hogy $d \mid 2^{n+1}$. Megmutatjuk, hogy szükségképpen $d = 2^{n+1}$. Valóban, $d < 2^{n+1}$ esetén d osztója lenne 2^n-nek is. Ebből viszont $2^{2^n} \equiv 1$ következne, holott $2^{2^n} = F_n - 1 \equiv -1 \pmod p$, hiszen $p \mid F_n$. Ezzel beláttuk, hogy $d = 2^{n+1}$. Mivel pedig $2^{p-1} \equiv 1 \pmod p$, ezért $2^{n+1} = d \mid p - 1$, tehát $p - 1 = k \cdot 2^{n+1}$, azaz $p = k \cdot 2^{n+1} + 1$, ahol k pozitív egész.

Valójában Euler azt is belátta, hogy ha $n \ge 2$ és a p prím osztója F_n-nek, akkor $p = k \cdot 2^{n+2} + 1$, ahol k pozitív egész. Meg lehet mutatni ugyanis, hogy ha a p prím $8k + 1$ alakú, akkor $2^{(p-1)/2} \equiv 1 \pmod p$. A fenti okoskodásban ezért $2^{n+1} = d \mid (p-1)/2$, tehát $(p-1)/2 = k \cdot 2^{n+1}$, azaz $p = k \cdot 2^{n+2} + 1$, ahol k pozitív egész.

Ezt $n = 5$-re alkalmazva azt kapjuk, hogy F_5 minden prímosztója $2^7 \cdot k + 1 = 128k + 1$ alakú. Ez jelentősen leszűkíti a lehetőségeket. A 2-nél nagyobb prímek ugyanis 128-cal osztva 64-féle maradékot adhatnak (nevezetesen az 1, 3, …, 127 számokat), és azt várhatjuk, hogy a 65536-nál kisebb prímeknek durván 1/64-ed része lesz $128k + 1$ alakú. Ez kb. $6500/64 < 102$ prímet jelent. Ezért annak eldöntéséhez, hogy F_5 prímszám-e, a 6500 osztás helyett várhatóan a legrosszabb esetben is elég száz-egynéhány osztást elvégezni. Euler elszánta magát ennek az elvégzésére. Óriási szerencséje volt; az első $128k + 1$ alakú prím, 257, ugyan nem osztója F_5-nek, de a második, 641, már igen: $F_5 = 4294967297 = 641 \cdot 6700417$. Ezzel Fermat sejtése megdőlt: az $F_n = 2^{2^n} + 1$ képlet nem állít elő minden n-re prímszámot.

Egyébként a következő Fermat-szám, F_6 prímtényezőkre bontását csak 1880-ban sikerült megtalálni: $F_6 = 274177 \cdot 67280421310721$. Az ezt követő Fermat-szám, F_7 faktorizációját 1970-ben találták meg; eszerint F_7 egy 17-jegyű és egy 22-jegyű prím szorzata. Azóta kiderült, hogy F_n összetett szám minden $5 \le n \le 21$-re (bár nem mindegyiküknek sikerült meghatározni a prímtényezős alakját). Sok nagyobb indexű Fermat-számot is megvizsgáltak, de még egy prímet sem találtak közöttük.

A fentiekből az a tanulság, hogy hacsak egy képletről nem tudjuk eleve, hogy valamilyen oknál fogva minden értéke prímszám lesz, akkor nem várhatjuk el, hogy ezt „szívességből” megtegye, még akkor sem, ha az első néhány értéke prím (mint pl. az $n^2 + n + 17$, $n^2 + n + 41$ vagy a $2^{2^n} + 1$ képletek esetében).

Eddig senki nem talált olyan képletet, amely egész számokból és az n változóból az összeadás, kivonás, szorzás és hatványozás műveleteinek segítségével épül fel, és amely minden pozitív egész n-re prímszámot szolgáltat (azt is feltéve persze, hogy a képlet végtelen sok különböző értéket ad). A következőkben megmutatjuk, hogy a feltételek enyhítésével már találhatunk ilyen képleteket.

⋆

Először olyan képleteket tekintünk, amelyekben nemcsak egészek, hanem tetszőleges valós konstansok is szerepelhetnek. Ekkor persze az x szám egészrészét megadó $[x]$ függvény használatát is meg kell engednünk, mert különben nem tudjuk biztosítani, hogy a képlet egész számokat szolgáltasson. (E függvény definíciója a következő: $[x]$ az az egyértelműen meghatározott egész szám, amelyre $[x] \le x < [x] + 1$. Így pl. $[3/2] = 1$, $[\pi] = 3$, $[7] = 7$, $[-4] = -4$, $[-3/2] = -2$, $[-\pi] = -4$.) Ezek felhasználásával már viszonylag egyszerű képletet adhatunk az n-edik prímszámra, amelyet a következőkben p_n-nel fogunk jelölni. Megmutatjuk, hogy van olyan α valós szám, amelyre

$$p_n = \left[10^{n^2}\alpha\right] - 10^{2n-1}\left[10^{(n-1)^2}\alpha\right] \qquad (n = 1, 2, \ldots). \tag{4}$$

Képezzünk ugyanis a prímszámok p_n sorozatából egy végtelen tizedestörtet a következőképpen. A tizedestört egészrésze 0 lesz. A tizedesvessző után írjuk le egymás után a prímszámokat, megfelelő számú 0-val elválasztva őket. Az elválasztó

0-k számát úgy választjuk meg, hogy p_n utolsó számjegye éppen a tizedesvessző utáni n^2-edik helyre kerüljön. Tehát az 1., 4., 9., 16. jegy a 2-es, 3-as, 5-ös, 7-es lesz, a 24. és a 25. 1-es, a 35. ismét 1-es, a 36. 3-as, stb. Legyen az így definiált végtelen tizedestört α, tehát legyen

$$\alpha = 0,20030000500000070\ldots0110\ldots0130\ldots.$$

Ekkor $A_n = \left[10^{n^2}\alpha\right]$ az az egész szám, amelynek a jegyeit az α-nak a tizedesvessző utáni első n^2 jegye adja. A konstrukcióból adódik, hogy A_n egy olyan n^2-jegyű szám, amely éppen p_n jegyeivel végződik. Nyilvánvaló, hogy az A_n első $(n-1)^2$ jegyéből képzett szám $A_{n-1} = \left[10^{(n-1)^2}\alpha\right]$ lesz. Ha tehát A_{n-1}-et kiegészítjük $n^2-(n-1)^2 = 2n-1$ darab 0-val, azaz megszorozzuk 10^{2n-1}-gyel, és az így kapott számot kivonjuk A_n-ből, akkor éppen p_n-et kapjuk. Ezzel (4)-et beláttuk.

A fenti konstrukcióban hallgatólagosan felhasználtuk, hogy p_n jegyeinek száma legfeljebb $n^2-(n-1)^2 = 2n-1$, mert különben p_n „nem férne el". Megmutatjuk, hogy p_n jegyeinek száma legfeljebb n.

Nevezzünk egy m számot négyzetmentesnek, ha nem osztható 1-nél nagyobb négyzetszámmal. Ez azzal ekvivalens, hogy az m prímtényezős felbontásában minden prím első hatványon szerepel; azaz, hogy m különböző prímek szorzata. Bármely k egész szám előáll mint egy négyzetszám és egy négyzetmentes szám szorzata. Ha ugyanis k-t elosztjuk azzal a legnagyobb osztójával, amely négyzetszám, akkor a hányados nyilván négyzetmentes lesz. (Ha k négyzetmentes, akkor 1-gyel osztunk.)

Írjuk fel a p_n-nél nem nagyobb számokat b^2c alakban, ahol c négyzetmentes. Itt $b^2 \le p_n$, tehát $b \le \sqrt{p_n}$. A c szám különböző prímek szorzata, melyek mindegyike legfeljebb p_n, hiszen $c \le p_n$. Így c-t úgy kapjuk, hogy a p_1, p_2, …, p_n prímek közül néhányat összeszorzunk. Ezt 2^n-féleképpen tehetjük meg (annyiféleképpen, ahány részhalmaza van a $\{p_1,\ p_2,\ \ldots,\ p_n\}$ halmaznak). A b számot tehát legfeljebb $\sqrt{p_n}$-féleképpen, a c számot pedig legfeljebb 2^n-féleképpen választhatjuk meg. Mivel b^2c alakban minden p_n-nél nem nagyobb szám előáll, ebből következik, hogy $p_n \le \sqrt{p_n}\cdot 2^n$, $\sqrt{p_n} \le 2^n$, és így $p_n \le 4^n$. Mivel $4^n < 10^n$, ezért p_n legfeljebb n-jegyű. Ez a becslés lényegesen javítható: valójában p_n jegyeinek száma alig nagyobb n jegyeinek számánál. Így pl. $p_{100} = 541$, $p_{1000} = 7919$, $p_{10000} = 104729$, $p_{10^{10}}$ 11-jegyű, $p_{10^{100}}$ pedig 102-jegyű. Az utóbbi két állítás abból következik, hogy

$$n(\log n + \log\log n - 1{,}5) < p_n < n(\log n + \log\log n + 8), \qquad \text{valamint} \quad n\log n < p_n$$

minden $n \ge 2$-re. E képletekben $\log n$ az ún. természetes, vagy e alapú logaritmus, amelynek alapja $e = \lim\limits_{n\to\infty}\left(1+\dfrac{1}{n}\right)^n = 2,71828\ldots$.

A (4) képletre visszatérve megállapíthatjuk, hogy a puszta érdekességén kívül más haszna nemigen van; például nem használhatjuk fel prímszámok gyártására. Ahhoz ugyanis, hogy a képlet segítségével p_n értékét meghatározhassuk, tudnunk kellene α értékét. Ehhez viszont már ismernünk kellene az összes prímszámot. Egyébként vannak még egyszerűbb prímképletek is: létezik például egy $c > 1$ valós szám úgy, hogy $\left[c^{3^n}\right]$ prímszám lesz n minden pozitív egész értékére. Ennek a képletnek ugyanaz a baja, mint (4)-nek: c meghatározásához végtelen sok prímszámot kell felhasználni.

⋆

Most rátérünk azokra a prímképletekre, amelyekben a konstansok csak egész számok lehetnek, de a felhasználható műveleteket nem korlátozzuk. Megmutatjuk, hogy ha az alapműveleteken kívül felhasználhatjuk az $[x]$ (egészrész), $\{x\} = x - [x]$ (törtrész) függvényeket, valamint a

$$\sum_{i=k}^{n} a_i = a_k + a_{k+1} + \ldots + a_n \quad \text{és} \quad \prod_{i=k}^{n} a_i = a_k \cdot a_{k+1} \cdot \ldots \cdot a_n$$

jelöléseket, akkor szintén kaphatunk képleteket p_n-re. Jelöljük $\pi(x)$-szel az x számnál nem nagyobb prímek számát. Először $\pi(x)$-re adunk képletet.

Ha az $n > 2$ szám prím, akkor az $\dfrac{n}{2}, \dfrac{n}{3}, \ldots, \dfrac{n}{n-1}$ számok egyike sem egész, tehát az $\left\{\dfrac{n}{2}\right\}, \left\{\dfrac{n}{3}\right\}, \ldots, \left\{\dfrac{n}{n-1}\right\}$ törtrészek egyike sem 0. Ekkor tehát a $\prod\limits_{i=2}^{n-1}\left[-\left\{\dfrac{n}{i}\right\}\right]$ szorzat minden tényezője -1 (mert egy -1 és 0 közé eső szám egészrésze). A szorzat értéke tehát -1, hiszen a tényezők száma $n-2$, ami páratlan. Ha viszont n összetett, akkor n/i egész szám lesz legalább egy $2 \le i \le n-1$-re, és ekkor $\left[-\left\{\dfrac{n}{i}\right\}\right] = [-0] = 0$ alapján a fenti szorzat értéke 0. Így $x \ge 3$ esetén a

$$-\sum_{n=3}^{x}\prod_{i=2}^{n-1}\left[-\left\{\frac{n}{i}\right\}\right]$$

képlet értéke $\pi(x)-1$, hiszen a szumma n-edik tagja -1 ha n prím, és 0 ha n összetett. ($\pi(x)$-ből azért kell 1-et levonni, mert a 2-t kizártuk a szummából.) Azt kaptuk tehát, hogy

$$\pi(x) = 1 - \sum_{n=3}^{x} \prod_{i=2}^{n-1} \left[- \left\{ \frac{n}{i} \right\} \right] \quad (x = 3,\ 4,\ \ldots). \tag{5}$$

Valamivel egyszerűbb képletet is kaphatunk $\pi(x)$-re az ún. Wilson-tétel felhasználásával. Ez azt állítja, hogy ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Ezt így láthatjuk be: Az állítás $p = 2$, 3-ra nyilvánvaló, tehát feltehetjük, hogy $p \geq 5$. A kis Fermat tétel bizonyításakor megmutattuk, kogy ha n nem osztható p-vel, akkor az n, $2n$, …, $(p-1)n$ számok p-vel vett osztási maradékai az 1, 2, …, $p-1$ számok (esetleg más sorrendben). Ebből következik, hogy az 1, 2, …, $p-1$ számok között pontosan egy olyan i szám van, amelyre $n \cdot i \equiv 1 \pmod{p}$. Nevezzük ezt a számot n *reciprokának* (mod p). Ha $n \not\equiv m \pmod{p}$, akkor n és m reciprokai különbözők. Valóban, $n \cdot i \equiv m \cdot i \equiv 1$-ből következik, hogy $p \mid ni - mi = (n-m)i$, tehát $p \mid n-m$, hiszen $1 \leq i \leq p-1$. Ha egy $1 \leq n \leq p-1$ szám reciproka önmaga, akkor $n^2 \equiv 1$, $p \mid n^2 - 1 = (n-1)(n+1)$, tehát $n = 1$ vagy $n = p-1$.

A fentiekből következik, hogy a 2, 3, …, $p-2$ számok mindegyikét a reciprokával párosítva diszjunkt párokat kapunk. Mivel az egy párhoz tartozó számok szorzata p-vel osztva 1-et ad maradékul, ezért $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$, tehát $(p-1)! \equiv -1 \pmod{p}$. A Wilson-tétel megfordítható: ha $n > 1$ osztója $(n-1)!+1$-nek, akkor n prím. Valóban, ha $1 < d < n$, akkor $d \mid (n-1)!$. Ha d osztója volna n-nek, akkor $n \mid (n-1)!+1$ alapján d is osztója volna $(n-1)!+1$-nek, ami lehetetlen. Így n nem osztható a 2, …, $n-1$ számok egyikével sem, tehát prím. Összefoglalva: az $((n-1)!+1)/n$ tört akkor és csak akkor egész, ha $n = 1$ vagy n prím. Ebből következik, hogy

$$\sum_{n=1}^{x} \left[- \left\{ \frac{(n-1)!+1}{n} \right\} \right] = -\left(x - \pi(x) - 1\right),$$

hiszen összetett n-re a szumma n-edik tagja -1, míg prím n-re és $n = 1$-re 0. Ebből azt kapjuk, hogy

$$\pi(x) = x - 1 + \sum_{n=1}^{x} \left[- \left\{ \frac{(n-1)!+1}{n} \right\} \right] \quad (x = 1,\ 2,\ \ldots). \tag{6}$$

Az (5) és (6) képletek mindegyikét felhasználhatjuk p_n kifejezésére. Jelöljük ϕ-vel azt a függvényt, amelyre

$$\phi(x) = 1, ha$$

x=0, 1, 2, …, 0, *ha*x=-1,-2, ….(*A*ϕ függvényt csak az egész számokban értelmezzük.) A ϕ függvényre könnyen adhatunk képletet, pl. $\phi(x) = 1 + \left[\dfrac{1}{3x+2} \right]$ minden x egész számra. Mármost $k \leq p_n$ esetén $\pi(k) \leq n$, tehát $\phi(n - \pi(k)) = 1$, míg $k > p_n$ esetén $\pi(k) > n$, tehát $\phi(n - \pi(k)) = 0$. Ebből következik, hogy

$$p_n = \sum_{k=1}^{4^n} \phi(n - \pi(k)).$$

Valóban, a szumma tagjainak értéke $k = 1, \ldots, p_n$ esetén 1, egyébként pedig 0. Mivel $p_n \leq 4^n$, ezért a szumma értéke p_n. Ha ebben a formulában $\phi(x)$ helyébe $1 + [1/(3x+2)]$-t írunk, $\pi(x)$-et pedig (6)-tal helyettesítjük, akkor a következő képletet kapjuk p_n-re:

$$p_n = 4^n + \sum_{k=1}^{4^n} \left[\frac{1}{3n - 3k + 5 - 3 \sum\limits_{i=1}^{k} \left[- \left\{ \frac{(i-1)!+1}{i} \right\} \right]} \right] \quad (n = 1,\ 2,\ \ldots).$$

(Itt (6) helyett (5)-öt is alkalmazhatjuk, de ekkor apró módosítás szükséges, tekintve, hogy (5) csak $x \geq 3$-ra érvényes.)

Természetesen jó volna olyan prímképletet találni, amelyben a felhasznált műveletek száma minimális. Már említettük, hogy nem ismeretes olyan prímképlet, amelyben csak összeadás, szorzás és hatványozás szerepel. A következőkben a célunk annak bizonyítása, hogy *van olyan prímképlet, amelyben csak összeadás, kivonás, szorzás,* $[x]$, $\sqrt{x}$ *és maximum szerepel.* Ennek az ismertetését messziről kell kezdenünk.

$\star$

Diophantosz görög matematikus volt, aki a harmadik században élt Alexandriában. „Aritmetika” című művében egész együtthatós egyenletek egész, illetve racionális megoldásait vizsgálta, és az ilyen egyenleteket azóta diofantoszi vagy diofantikus egyenleteknek nevezik. Ilyenek például

$$x^2 - 2y^2 = 1, \quad x^2 - 60y^2 = 1, \quad x^2 - 61y^2 = 1, \tag{7}$$

vagy

$$x^3+y^3=u^3+v^3,\quad x^4+y^4=u^4+v^4,\quad x^5+y^5=u^5+v^5. \tag{8}$$

A (7) alatt felsorolt három egyenlet mindegyikének megoldása $x=1,\ y=0$; ezeket triviális megoldásnak hívjuk. Nem triviális megoldások is léteznek: az első egyenlet legkisebb pozitív egész megoldása $x=3,\ y=2$, a másodiké pedig $x=31,\ y=4$. A harmadiké viszont $x=1766319049,\ y=226153980$.

A (8) alatt felsorolt egyenletek triviális megoldásai azok, amelyekre $x=u,\ y=v$ vagy $x=v,\ y=u$. Az első két egyenletnek vannak nem-triviális megoldásai is, pl. $9^3+10^3=1^3+12^3$, illetve $133^4+134^4=59^4+158^4$. A harmadiknak viszont nem ismerjük egyetlen nem-triviális megoldását sem, de az sincs bizonyítva, hogy ilyen megoldás nem létezik.

Ezek a jelenségek tipikusak: előfordul, hogy egész egyszerűnek látszó diofantikus egyenletek megoldása a legnagyobb nehézségbe ütközik, sőt, gyakori eset, hogy azt sem tudjuk eldönteni, hogy a kérdéses egyenletnek van-e egyáltalán megoldása. Ezek a tapasztalatok vezették David Hilbertet 1900-ban az alábbi kérdéshez: van-e olyan algoritmus (valamely mechanikus, automatikus eljárás), amely bármely megadott diofantikus egyenletről el tudja dönteni, hogy van-e megoldása? Ha Hilbert korában már léteztek volna számítógépek, nyilván úgy tette volna a kérdést, hogy van-e ilyen számítógépes program. A probléma megoldására 70 évig kellett várni. Ahhoz, hogy a megoldást megérthessük, be kell vezetnünk három fogalmat.

Azt mondjuk, hogy természetes számoknak egy végtelen sorozata *rekurzív,* ha van olyan algoritmus (azaz számítógépes program), amely bármely számról el tudja dönteni, hogy tagja-e a sorozatnak vagy sem. Például a 2-hatványok sorozata rekurzív, mert bármely n pozitív egészről el tudjuk dönteni, hogy 2-hatvány-e vagy sem: addig osztjuk 2-vel, amíg páratlan számot kapunk. Ha ez a szám 1, akkor n 2-hatvány; egyébként pedig nem. A prímszámok sorozata is rekurzív, hiszen bármely számról el tudjuk dönteni, hogy prím-e: csak azt kell megvizsgálni, hogy osztható-e valamely nála kisebb, de 1-nél nagyobb számmal. (Azzal most nem foglalkozunk, hogy ennek eldöntése mennyi ideig tart; a lényeg az, hogy az algoritmus véges sok lépésben elvégezhető legyen.)

Egy sorozat akkor és csak akkor rekurzív, ha van olyan számítógépes program, amely a sorozat tagjait növekvő sorrendben kinyomtatja. Ha ugyanis a sorozat rekurzív, akkor írhatunk egy olyan programot, amely egymás után megvizsgálja a természetes számokat és eldönti, hogy tagjai-e a sorozatnak, és ha egy n számról úgy találja, hogy igen, akkor n-et kinyomtatja. Megfordítva, ha van egy nyomtatóprogram, amely a sorozat tagjait növekvő sorrendben kinyomtatja, akkor a következő algoritmust készíthetjük annak eldöntésére, hogy egy n szám tagja-e a sorozatnak. Indítsuk el a nyomtatóprogramot, és várjunk addig, amíg egy n-nél nagyobb szám megjelenik. Ha az eddig kinyomtatott számok között n szerepel, akkor tagja a sorozatnak, egyébként pedig nem (hiszen később már nem kerülhet sorra).

Más a helyzet, ha van ugyan olyan program, amely a sorozat elemeit kinyomtatja, de nem feltétlenül növekvő sorrendben. (Az ilyen sorozatokat *rekurzíve felsorolható* sorozatoknak nevezzük.) Egy ilyen sorozat esetében, ha egy n szám megjelenik a kinyomtatott számok között, akkor tagja a sorozatnak. Ha viszont n nem tagja a sorozatnak, akkor ezt esetleg soha nem tudjuk meg, hiszen soha nem lehetünk biztosak abban, hogy n nem lesz-e később kinyomtatva. Tehát egy rekurzíve felsorolható sorozat nem feltétlenül rekurzív. A matematikai logika egyik nevezetes felfedezése, hogy rekurzíve felsorolható, de nem rekurzív sorozatok valóban léteznek, sőt, konkrétan meg is adhatók. (Ezt úgy kell érteni, hogy konkrétan megadható olyan program, amely kinyomtatja a sorozat elemeit. A sorozatot magát nem tudjuk megadni abban az értelemben, hogy a tagjait felsoroljuk növekvő sorrendben, hiszen akkor a sorozat rekurzív volna.)

A harmadik fogalom, amelyre szükségünk lesz, a diofantikus sorozat fogalma. Egy diofantikus egyenlet általános alakja (az egyenlet jobb oldalának bal oldalra vitele után) $P(x_1,\ x_2,\ \ldots,\ x_k)=0$, ahol $P(x_1,\ x_2,\ \ldots,\ x_k)$ egész együtthatós polinom; azaz olyan kifejezés, amely az $x_1,\ \ldots,\ x_k$ változókból és egész számokból képződik az összeadás, kivonás és szorzás műveleteinek felhasználásával. Egy sorozatot akkor nevezünk *diofantikusnak,* ha létezik egy egész együtthatós $P(x_1,\ \ldots,\ x_k,\ x_{k+1})$ polinom a következő tulajdonsággal: egy y természetes szám akkor és csak akkor tagja a sorozatnak, ha a $P(x_1,\ \ldots,\ x_k,\ y)=0$ diofantikus egyenletnek van megoldása a természetes számok körében, azaz ha vannak $x_1,\ \ldots,\ x_k$ természetes számok úgy, hogy $P(x_1,\ \ldots,\ x_k,\ y)=0$. Ekkor azt mondjuk, hogy a sorozatot a $P(x_1,\ \ldots,\ x_k,\ x_{k+1})$ polinom generálja. A négyzetszámok sorozata például diofantikus, mert egy y szám akkor és csak akkor négyzetszám, ha az $x^2-y=0$ (egyváltozós) egyenlet megoldható a természetes számok körében. Tehát a négyzetszámok sorozatát az $x_1^2-x_2$ polinom generálja.

Nem nehéz belátni, hogy minden diofantikus sorozat rekurzíve felsorolható. Tegyük fel ugyanis, hogy a sorozatot a $P(x_1,\ \ldots,\ x_k,\ x_{k+1})$ polinom generálja. A rövidség kedvéért nevezzük *vektornak* a természetes számokból álló $k+1$-hosszúságú számsorozatokat. Ekkor az összes vektort felsorolhatjuk egyetlen végtelen sorozatban. Ezt úgy tehetjük meg, hogy elsőként felírjuk az $(0,\ \ldots,\ 0)$ vektort, majd azokat, amelyekben $x_1+\ldots+x_{k+1}=1$ (ezekből $k+1$ van), majd azok jönnek, amelyekben $x_1+\ldots+x_{k+1}=2$, és így tovább. Minden egyes $(x_1,\ \ldots,\ x_{k+1})$ vektorra számítsuk ki a $P(x_1,\ \ldots,\ x_k,\ x_{k+1})$ értéket. Ha ez nulla, akkor nyomtassuk ki x_{k+1}-et. Ha nem nulla, akkor ugorjunk át a következő vektorra. Nyilvánvaló, hogy ilyen módon éppen azokat az y számokat nyomtattuk ki, amelyekre a $P(x_1,\ \ldots,\ x_k,\ y)=0$ diofantikus egyenlet megoldható, és ezzel megmutattuk, hogy a kérdéses sorozat rekurzíve felsorolható.

Mármost Hilbert problémájának megoldásában a kulcslépés annak bizonyítása volt, hogy minden rekurzíve felsorolható sorozat szükségképpen diofantikus. A három fogalom logikai kapcsolata tehát a következő:

$$\text{rekurzív} \Longrightarrow \text{rekurzíve felsorolható} \Longleftrightarrow \text{diofantikus}.$$

Ebből pedig már következik, hogy *nincs olyan algoritmus, amely bármely megadott diofantikus egyenletről el tudná dönteni, hogy van-e megoldása.* Vegyünk ugyanis egy olyan sorozatot, amely rekurzíve felsorolható, de nem rekurzív. Mivel ez a sorozat szükségképpen diofantikus, létezik egy $P(x_1,\ \ldots,\ x_k,\ x_{k+1})$ polinom, amely generálja. Ha létezne olyan algoritmus, amely bármely diofantikus egyenletről el tudja dönteni, hogy van-e megoldása, akkor minden y-ról eldönthetnénk, hogy tagja-e a sorozatnak vagy sem, hiszen a $P(x_1,\ \ldots,\ x_k,\ y) = 0$ diofantikus egyenletet az állítólagos algoritmussal megvizsgálva megállapíthatnánk, hogy megoldható-e vagy sem. Ez azonban lehetetlen, mert akkor a sorozatunk rekurzív lenne, holott olyan sorozatból indultunk ki, ami nem az.

A Hilbert-problémának ez a negatív megoldása nem jelenti azt, mintha találtunk volna egy olyan diofantikus egyenletet, amelyről sohasem dönthetjük el, hogy van-e gyöke vagy sem. Elvileg elképzelhető, hogy előbb-utóbb mindegyik diofantikus egyenletről kideríthetjük, hogy megoldható-e. Ebben az esetben azonban a módszernek egyenletről egyenletre változnia kell; általános, minden egyenletre egyaránt alkalmazható algoritmus nincs.

$\star$

Most térjünk vissza a prímszámokhoz. Mivel a prímszámok sorozata rekurzív, ezért rekurzíve felsorolható, tehát diofantikus. Így létezik egy $P(x_1,\ \ldots,\ x_k,\ x_{k+1})$ polinom, amely a prímszámok sorozatát generálja. Képezzük a

$$Q(x_1,\ \ldots,\ x_k,\ x_{k+1}) = x_{k+1}\left(1 - 2P^2(x_1,\ \ldots,\ x_k,\ x_{k+1})\right)$$

polinomot. Ha Q-ban az $x_1, \ldots, x_k, x_{k+1}$ változók helyére természetes számokat helyettesítünk, akkor két eset lehetséges.

(i) $P(x_1,\ \ldots,\ x_k,\ x_{k+1}) = 0$. Ekkor x_{k+1} prím (mert P a prímeket generálja), és $Q(x_1,\ \ldots,\ x_k,\ x_{k+1}) = x_{k+1}$.

(ii) $P(x_1,\ \ldots,\ x_k,\ x_{k+1}) \neq 0$. Ekkor $1 - 2P^2(x_1,\ \ldots,\ x_k,\ x_{k+1}) \leq 1 - 2 < 0$ és így

$$Q(x_1,\ \ldots,\ x_k,\ x_{k+1}) \leq 0.$$

Azt kaptuk tehát, hogy Q-ba természetes számokat helyettesítve vagy prímet vagy nem-pozitív számot kapunk. Másrészt így minden prímet megkapunk, mert ha p prím, akkor $P(x_1,\ \ldots,\ x_k,\ p) = 0$ alkalmas $x_1, \ldots, x_k$-ra, tehát $Q(x_1,\ \ldots,\ x_k,\ p) = p$. A fentieket összefoglalva megállapíthatjuk, hogy a

$$\max(Q(x_1,\ \ldots,\ x_k,\ x_{k+1}),\ 2) \tag{9}$$

kifejezés a változók nemnegatív egész értékeire mindig prímet ad, és minden prímet megad. Ilyen tulajdonságú Q polinomok explicite is megadhatók; sajnos mindegyikük komplikált. Van közöttük 10-változós, ennek a foka azonban nagyobb 10^{45}-nél. Van 5-ödfokú ilyen polinom is; ez azonban 42 változót tartalmaz. A jelenleg ismert legegyszerűbb egy 26-változós, 25-ödfokú polinom, amely kinyomtatva 9 sort foglal el a [3] könyv 115-116. oldalán.

A bonyolultságtól eltekintve (9) majdnem ideális prímképletnek tekinthető; csak a többváltozós jellege zavaró egy kicsit. Felmerül a kérdés, nem lehetne-e hasonló, de egyváltozós képletet nyerni. Esetleg lemondhatnánk arról, hogy a képlet *minden* prímet előállítson, megelégednénk végtelen sok prím előállításával is. Egy egyszerű ötlettel (9) azonnal egyváltozóssá tehető: írjunk az x_i változók helyébe egy-egy $f_i(n)$ függvényt. Az így kapott

$$\max(Q(f_1(n),\ \ldots,\ f_{k+1}(n)),\ 2) \tag{10}$$

képlet egyváltozós, és ha az $f_i(n)$ érték nemnegatív egész minden $i = 1, \ldots, k+1$-re és $n = 0, 1, 2, \ldots$-re, akkor (10) minden n-re prímet fog előállítani.

Látszólag készen vagyunk. Azonban a dolog mégsem ilyen egyszerű: ha pl. $f_1, \ldots, f_{k+1}$ gyanánt egész együtthatós polinomokat választunk, akkor a (10) képlet csak véges sok különböző értéket fog előállítani. Ugyanis ebben az esetben $Q(f_1(n),\ \ldots,\ f_{k+1}(n)) = q(n)$ is egész együtthatós polinom lesz. Ha q konstans, akkor $\max(q(n), 2)$ is konstans. Ha q nem konstans és a főgyütthatója negatív, akkor minden elég nagy n-re $q(n) < 0$, tehát $\max(q(n), 2) = 2$. Ha viszont q nem konstans és a főgyütthatója pozitív, akkor minden elég nagy n-re $q(n) > 2$, tehát $\max(q(n), 2) = q(n)$. Ez azt jelentené, hogy $q(n)$ minden elég nagy n-re prímszám, amiről már beláttuk, hogy lehetetlen (egy nem konstans egész együtthatós polinom az n végtelen sok értékére összetett számot ad). Ez az eset tehát nem fordulhat elő!

Ez a jelenség első pillantásra hihetetlennek tűnik: a $Q(x_1,\ \ldots,\ x_k,\ x_{k+1})$ polinomnak végtelen sok pozitív értéke van (hiszen minden prímet felvesz), de akárhogy helyettesítünk egész együtthatós polinomokat a változók helyébe, a kapott $Q(f_1(n),\ \ldots,\ f_{k+1}(n)) = q(n)$ polinom vagy konstans, vagy pedig negatív minden elég nagy n-re. Ez a különös jelenség azonban már egész egyszerű polinomok körében is fellép. Meg lehet mutatni, hogy a $Q(x,\ y) = (x^2+1)(1 - 2(x^2 - 2y^2 - 1)^2)$ polinom is rendelkezik ezzel a tulajdonsággal.

Ha el akarjuk érni, hogy a (10) képlet végtelen sok prímet szolgáltasson, a legegyszerűbb az $f_1,\ \ldots,\ f_{k+1}$ függvényeket úgy megválasztani, hogy minden $(a_1,\ \ldots,\ a_{k+1})$ vektor előálljon $(f_1(n),\ \ldots,\ f_{k+1}(n))$ alakban. Ekkor (10) minden prímet elő fog állítani. Ha egy $(a_1,\ \ldots,\ a_{k+1})$ vektorhoz létezik egy n természetes szám, melyre $f_1(n) = a_1,\ \ldots,\ f_{k+1}(n) = a_{k+1}$, akkor azt fogjuk mondani, hogy az $f_1,\ \ldots,\ f_{k+1}$ függvények *kódolják* az $(a_1,\ \ldots,\ a_{k+1})$ vektort. Olyan függvényeket keresünk tehát, amelyek minden, nemnegatív egészekből álló vektort kódolnak. Mint láttuk, ezt polinomokkal nem érhetjük el, ezért fel kell használnunk más függvényeket is. Ekkor azonban egy újabb technikai nehézség lép fel. Ha szeretnénk minél egyszerűbb képleteket használni, akkor az f_i függvények

nemcsak a pozitív egészekből, hanem a tetszőleges egészekből álló vektorokat is kódolni fogják. A Q polinom a negatív egészekben felvehet pozitív összetett számot is, és akkor (10) értéke nem lesz minden n-re prím. Ezen a következő módszerrel segíthetünk. Legyen $m = 4(k+1)$, és tekintsük a

$$Q_1(y_1,\ \ldots,\ y_m) = Q(y_1^2+y_2^2+y_3^2+y_4^2,\ y_5^2+y_6^2+y_7^2+y_8^2.\ \ldots,\ y_{m-3}^2+y_{m-2}^2+y_{m-1}^2+y_m^2)$$

polinomot. Ezt tehát úgy kapjuk Q-ból, hogy mindegyik x_i változó helyére négy új változó négyzetösszegét írjuk. Most felhasználjuk azt a nevezetes tételt, amely szerint minden természetes szám előáll négy négyzetszám összegeként (lásd [1], 237. oldal). Nyilvánvaló, hogy Q_1-ben a változók helyére tetszőleges egészeket helyettesítve ugyanazokat az értékeket kapjuk, mint amikor Q-ban a változók helyére tetszőleges természetes számokat helyettesítünk. Így a $\max(Q_1(y_1,\ \ldots,\ y_m), 2)$ képlet prímszámot szolgáltat valahányszor $y_1,\ \ldots,\ y_m$ egészek, továbbá minden prímszámot megkapunk már akkor is, ha az y_i-k helyére természetes számokat helyettesítünk.

Olyan függvényeket fogunk gyártani, amelyek minden m-hosszúságú, természetes számokból álló vektort kódolnak. Ezeket az y_i változók helyére írva egyváltozós prímképletet kapunk. A konstrukciót csak $m = 2$-re és $m = 3$-ra adjuk meg, de világos lesz, hogy minden m-re elvégezhető.

Lássuk be először, hogy az $(\left[\sqrt{n}\right],\ n - \left[\sqrt{n}\right]^2)$ függvénypár minden olyan $(b_1,\ b_2)$ számpárt kódol, amelyre $b_1 \geq b_2 \geq 0$. Legyen ugyanis $n = b_1^2 + b_2$. Ekkor

$$b_1^2 \leq n < b_1^2 + 2b_1 + 1$$

(hiszen $b_2 \leq b_1$), tehát $b_1 \leq \sqrt{n} < b_1 + 1$. Így $[\sqrt{n}] = b_1$ és

$$n - \left[\sqrt{n}\right]^2 = (b_1^2 + b_2) - b_1^2 = b_2.$$

Ha most a_1, a_2 tetszőleges természetes számok, akkor $a_1 + a_2 \geq a_2$, tehát van olyan n amelyre $[\sqrt{n}] = a_1 + a_2$ és $n - \left[\sqrt{n}\right]^2 = a_2$. Ekkor $[\sqrt{n}] - \left(n - \left[\sqrt{n}\right]^2\right) = a_1$ és $n - \left[\sqrt{n}\right]^2 = a_2$, tehát az $([\sqrt{n}] - n + \left[\sqrt{n}\right]^2,\ n - \left[\sqrt{n}\right]^2)$ függvénypár minden természetes számokból álló számpárt kódol.

Most tekintsük az $m = 3$ esetet. Belátjuk először, hogy a

$$g_1(n) = \left[\sqrt[4]{n}\right], \quad g_2(n) = \left[\sqrt{n}\right] - g_1(n)^2, \quad g_3(n) = n - \left(g_1(n)^2 + g_2(n)\right)^2$$

függvények minden olyan $(b_1,\ b_2,\ b_3)$ vektort kódolnak, melyekre $b_1 \geq b_2 \geq b_3 \geq 0$. Valóban, legyen $n = (b_1^2+b_2)^2+b_3$. Ekkor $(b_1^2+b_2)^2 \leq n < (b_1^2+b_2)^2+2(b_1^2+b_2)+1$ (hiszen $b_3 \leq b_2$), tehát $b_1^2+b_2 \leq \sqrt{n} < b_1^2+b_2+1$ és $b_1^2 \leq \sqrt{n} < b_1^2+2b_1+1$ (hiszen $b_2 \leq b_1$). Így $\left[\sqrt{n}\right] = b_1^2 + b_2$, $\left[\sqrt[4]{n}\right] = b_1$, amiből $g_1(n) = b_1$, $g_2(n) = b_2$, és $g_3(n) = b_3$.

Ha most a_1, a_2, a_3 tetszőleges természetes számok, akkor $a_1 + a_2 + a_3 \geq a_2 + a_3 \geq a_3$, tehát van olyan n, amelyre $g_1(n) = a_1 + a_2 + a_3$, $g_2(n) = a_2 + a_3$ és $g_3(n) = a_3$. Ebből következik, hogy a $g_1 - g_2$, $g_2 - g_3$ és g_3 függvények minden természetes számokból álló számhármast kódolnak.

Ezt a konstrukciót minden m-re elvégezhetjük. Ha az így kapott függvényeket Q_1-be helyettesítjük, akkor végül is a következő tételt kapjuk.

Létezik olyan $f(n)$ kifejezés, amely az n, $\left[\sqrt{n}\right]$, $\left[\sqrt[4]{n}\right]$, $\ldots$, $\left[\sqrt[2^r]{n}\right]$ függvények egész együtthatós polinomja (azaz a fenti függvényekből és egész számokból kapható az összeadás, kivonás és szorzás műveleteinek segítségével), és amelyre a $\max(f(n),\ 2)$ ($n = 0,\ 1,\ \ldots$) számok halmaza pontosan a prímszámok halmazával egyenlő.

Ilyen alakban nem csak a prímszámok állíthatók elő. Ha ismét áttekintjük a tételhez vezető gondolatmenetet, láthatjuk, hogy bármely rekurzíve felsorolható sorozatnak van ilyen előállítása. Mindazonáltal a prímszámok előállításával kapcsolatban felmerül néhány érdekes kérdés.

1. A prímszámokat előállító képletekben mennyi az r minimális értéke? (A fenti gondolatmenet $r = 39$-et ad, hiszen k-ra az ismert legkisebb érték 9, és $r = m - 1 = 4(k+1) - 1$.) Lehet-e pl. olyan prímképletet megadni, amely csak az n és $\left[\sqrt{n}\right]$ függvényeket használja?

2. Megadható-e olyan, fenti alakú f függvény, amelyre $f(n) = p_n$ minden n-re?

Irodalom

[1] Erdős Pál és Surányi János: *Válogatott fejezetek a számelméletből.* Polygon, Szeged, 1996.

[2] G. H. Hardy and E. M. Wright: *An Introduction to the Theory of Numbers.* Oxford University Press, Oxford, 1975.

[3] P. Ribenboim: *The Little Book of Big Primes.* Springer, 1991.

[4] D. Shanks: *Solved and Unsolved Problems in Number Theory.* Chelsea, New York, 1985.

Laczkovich Miklós