A kis Fermat-tétel ma matematikai közhely. Azt mondja ki, hogy egy p prímszámra és egy a egész számra $a^p \equiv a \pmod{p}$, vagy – ezzel egyenértékűen – hogy ha a p prímszámra $(a,\, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$. Fermat éppen 400 éve, 1601-ben született, a tételt 1640 körül találta. Soha nem közölt bizonyítást, és mivel a kongruencia jelölést több, mint 150 évvel később Gauss vezette be, erős anakronizmus volna, ha a mai alakot, illetve a kérdés ilyen fölvetését Fermat-nak tulajdonítanánk. Milyen formában bukkanhatott a tételre ?

Fermat idején nem voltak hivatásos matematikusok, Toulouse városának ügyészeként ő maga is amatőr volt, kiváló klasszikus műveltséggel és széles nyelvtudással, latinul, görögül, olaszul és spanyolul egyaránt folyékonyan írt. Mai értelemben véve matematikai közleményt Fermat lényegében nem publikált, eredményei elsősorban kiterjedt levelezése nyomán maradtak fenn.

A kor tudományos közéletének fő formája a levelezés volt. Fermat legfontosabb partnerei, ezekben az években Mersenne, Frenicle és Descartes (később Huygens és Pascal) voltak. Az optika, a geometria, a görbék tulajdonságainak vizsgálata mellett az egész számok világa volt Fermat fő érdeklődési területe. Egy több mint 2000 éves kérdés, a *tökéletes számok*[1]Egy pozitív egészt tökéletes számnak nevezünk, ha egyenlő a nála kisebb pozitív osztói összegével. vizsgálata vezethette őt a számelmélet egyik legtöbbet idézett eredményére.

Már Euklidesz is tudta és az Elemek IX. könyvében lényegében bebizonyította, hogy ha $2^n - 1$ prímszám, akkor $2^{n-1}\left(2^n - 1\right)$ tökéletes szám. A jól ismert tökéletes számokra $6 = 1 + 2 + 3 = 2^1\left(2^2 - 1\right)$, $28 = 1 + 2 + 4 + 7 + 14 = 2^2\left(2^3 - 1\right)$. Azt, hogy a páros tökéletes számok valamennyien ilyen alakúak, Euler igazolta 150 évvel később. Azt pedig mind a mai napig nem tudjuk, hogy van-e egyáltalán páratlan tökéletes szám.

Egy másik népszerű görög örökség a *barátságos*[2]Két pozitív egészt barátságos számoknak nevezünk, ha bármelyikük egyenlő a másiknak a nála kisebb pozitív osztói összegével. számok fogalma volt. Mersenne 1638-ban tudatta Descartes-tal, hogy

$$2^{n+1} \cdot \left(18 \cdot 2^{2n} - 1\right) \qquad \text{és} \qquad 2^{n+1} \cdot \left(3 \cdot 2^{2n} - 1\right) \cdot \left(6 \cdot 2^{2n} - 1\right)$$

biztosan barátságosak, ha előbbi második, utóbbi második és harmadik tényezője prímszám. Ha $n = 1$, akkor a $4 \cdot 71 = 284$, $4 \cdot 5 \cdot 11 = 220$ számokat kapjuk; ez a legkisebb barátságos számpár.

Fermat és kortársai között egyfajta vetélkedés folyt az ilyesfajta számok felkutatásáért, egymással általában az eredményeket közölték, ritkábban a módszert, bizonyítást pedig szinte soha. A lehetséges megoldásban alapvető szerepet játszott annak eldöntése, hogy nagy, rendszerint $2^n - 1$ vagy $3 \cdot 2^n - 1$ alakú számok prímek-e vagy sem; ha pedig összetettek, akkor milyen prímosztóik vannak. Mersenne például 1640-ben azzal a kérdéssel fordult Fermat-hoz, hogy ismer-e tökéletes számot 10^{20} és 10^{22} között. Az euklideszi feltétel:

$$10^{20} < 2^{n-1}\left(2^n - 1\right) < 10^{22}$$

azt jelenti, hogy $34 \leq n \leq 37$. Mivel pedig $2^n - 1$ nem lehet prím, ha n összetett, Mersenne kérdése lényegében arra vonatkozott, prím-e a $2^{37} - 1$. Ez a 12 jegyű szám, 137 438 953 471 semmilyen gondot nem okoz a mai matematikai szoftvereknek, egy átlagos kalkulátor lehetőségeit azonban meghaladja, a XVII. században pedig alaposan próbára tehette a számolók türelmét. Fermat még abban az évben rátalált a $2^{37} - 1$ törzstényezős felbontására. 1640 őszén írt levelében az alábbi eredményről számol be:

Ha n prím és p a $2^n - 1$ egy prímosztója, akkor $p - 1$ az n-nek többszöröse.

Nem sokkal később ő maga így kommentálta a fenti állítást:

„Tetszőleges p prímszámra és 1, a, a^2, ... mértani sorozatra p-nek osztania kell az $a^n - 1$ különbséget a $p - 1$ valamilyen n osztójára; ha pedig N tetszőleges többszöröse a legkisebb ilyen n-nek, akkor a p osztója $(a^N - 1)$-nek is."

Így talán jobban ráismerünk a tétel mai alakjára: N értéke ott $p - 1$, a legkisebb olyan szám, amelyik már minden esetben biztosítja az oszthatóságot.

Fermat tehát eredetileg a $2^{37} - 1$ prímosztóit kereste. Megközelítésének lényege jól mutatja gondolkodásának mélységét: megváltoztatva a kérdés tárgyát, az adott szám, $2^{37} - 1$ helyett a p prímszámot rögzítve kérdezte, hogy milyen kitevőkre lesznek a p-nek $2^n - 1$ alakú többszörösei. Az ilyen típusú átfogalmazás gyakran döntő egy probléma megoldása során.

Általában vizsgálta tehát a 2 hatványainak a maradékát tetszőleges páratlan p prímszámmal osztva. Azt könnyű látni, hogy létezik olyan kitevő, amelyre ez a maradék éppen 1. A 2 hatványai ugyanis véges sok – legfeljebb $(p - 1)$ – maradékot adhatnak a p-vel osztva, így lesznek közöttük azonosak. Mai jelöléssel $2^k \equiv 2^m \pmod{p}$, és innen következik, hogy $2^{|k-m|} \equiv 1 \pmod{p}$.

A továbbiakban hívjuk az ilyen kitevőket *jó kitevőknek*. Az általa olyan sikeresen alkalmazott *descent* módszere szerint Fermat természetes módon fordulhatott ezután a pozitív jó kitevők legkisebbikéhez, amit egyébként ma a p prímszám *rendjének* nevezünk moduló 2. (Az általános tétel a 2 helyett tetszőleges $a > 1$ egészre vonatkozik, ahol $(a,\, p) = 1$.) Ha ez k_0, akkor nyomban látszik, hogy értéke legfeljebb $(p - 1)$, és a Fermat kommentárjában említett tulajdonság egy változata is többé kevésbé nyilvánvaló: az N pontosan akkor jó kitevő, azaz $2^N - 1$ pontosan akkor osztható a p-vel, ha N osztható k_0-lal.

Ehhez osszuk el az N-et maradékosan k_0-lal. Ha $N = k_0 \cdot q + r$, akkor

$$2^N = \left(2^{k_0}\right)^q \cdot 2^r \equiv 1^q \cdot 2^r \pmod{p},$$

az N-nel együtt tehát r is jó kitevő. Mivel pedig $0 \leq r < k_0$, csak $r = 0$ lehetséges.

Látható, hogy Fermat tételének mai alakja ebből a sokszálú összefüggésrendszerből emel ki egy lényeges elemet: azt állítja, hogy $(p-1)$ mindenképpen jó kitevő[3]A kis Fermat-tétel ‚hivatalos' bizonyítása lényegében valamennyi bevezető jellegű számelmélet tankönyvben megtalálható, így azt most nem közöljük.. A fentiekből pedig kiderül, hogy ha nem a legkisebb, akkor annak többszöröse. Nem tudjuk, hogyan okoskodhatott Fermat, amikor világossá váltak számára ezek a kapcsolatok, de bizonyosra vehető, hogy teljes mélységében átlátta ezt a kérdéskört.

A $2^{37} - 1$ lehetséges prímosztóit keresve ezután világos, hogy az ilyen prímekre a 37 szükségképpen a *legkisebb* jó kitevő, hiszen a 37 maga prímszám. Mivel pedig Fermat tudta, hogy $(p-1)$ biztosan jó kitevő, a fentiek szerint többszöröse kell legyen a 37-nek: $p-1 = 37m$. Az m értéke nyilván páros – ez már csak ráadás – így a $2^{37}-1$ prímosztói $74k+1$ alakúak. A k legkisebb szóbajövő értéke 3, amire $3 \cdot 74 + 1 = 223$, és valóban,

$$\frac{2^{37}-1}{223} = 616\,318\,177.$$

A jó matematikusnak még szerencséje is van, a 223 váratlanul kis prímtényezőnek bizonyult. A másik tényező, $616\,318\,177 = 74 \cdot 8\,328\,624 + 1$, ez pedig valószínűsíti, hogy az is prím – ami egyébként igaz is.

Felhasznált irodalom:

Robert M. Young: Excursions in Calculus, The Dolciani Mathematical Expositions, 13

Pataki János