Válasz Gyarmati Katalin bírálatára

Köszönöm Gyarmati Katalinnak a doktori mű elolvasására fordított időt és fáradságot, valamint a vitára bocsátás támogatását. A bíráló két kérdést tett fel a bírálatában, az alábbiakban ezekre reagálok.

> Itt mindjárt lenne is kérdésem a jelölthöz: algebrai görbék egész pontjaihoz ($\mathbb{Q}$ felett) hogyan kapcsolódnak a lehetséges kriptográfiai alkalmazások?

Válasz: A számelmélet és a kriptográfia nagyon sok szálon kapcsolódik egymáshoz, például az egyik legismertebb titkosítási eljárás az RSA esetében az húzódik meg a háttérben, hogy az egész számok faktorizációja nehéz probléma. Számelméleti eszközök a kriptográfiai rendszerek támadásánál is fontos szerepet töltenek be, a fent említett RSA algoritmus esetében a faktorizáció irányából közelítve az elliptikus görbéken alapuló faktorizáció pontosan a kérdésben megfogalmazott algebrai görbékhez kapcsolódik, érdemes megemlíteni a lánctörteken alapuló faktorizációs eljárást. Az RSA vizsgálatában a lánctörtek az úgynevezett Wiener-támadásban is fontos szerepet játszanak, bizonyos feltételek mellett hatékony törési eljárást ad.
Az elliptikus görbék különböző modelljei esetében (Edwards modell, Hessian modell, Huff modell, Jacobi modell, Montgomery modell, Weierstrass modell) a görbék pontjain összeadást lehet definiálni, így véges csoportokhoz jutunk (véges testek felett tekintve a görbéket), természetesen adódik a diszkrét logaritmus probléma vizsgálata, azaz adott P, Q pontok esetén meghatározni olyan n értéket, amire $Q = nP$ (ha létezik ilyen). Néhány kapcsolódó kriptográfiai eljárást említenék meg: Diffie-Hellman kulcscsere, ElGamal rendszer, Massey-Omura titkosítás.
Végezetül szeretném még megemlíteni a titkosítási eljárások támadásaiban sokszor hatékonyan bevethető Arjen Lenstra, Hendrik Lenstra és Lovász László nevéhez fűződő LLL-algoritmust. A Merkle-Hellman hátizsák problémán alapuló titkosítási eljárás esetében és az NTRU titkosítás (bizonyos paraméterek mellett) esetében is hatékony eszköznek bizonyult.

> Itt szeretném megkérdezni a jelöltet, hogy mi tudható egy hasonló alakú egyenletről, nevezetesen:
>
> $$x^3 + y^3 + z^3 = 3xyz\text{-ről?}$$
>
> Ez utóbbi egyenlet átrendezve az szorzattá bomlik:
>
> $$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 + y^2 + z^2 - xy - xz - yz),$$
>
> így talán a megoldások keresése egyszerűbb pl. a Gauss egészek körében. Esetleg tud erről a jelölt valamit mondani?

Válasz: A kérdésben található felírás módosított formája az alábbi:

$$2(x^3 + y^3 + z^3 - 3xyz) = (x + y + z)((x - y)^2 + (y - z)^2 + (z - x)^2),$$

ami az egészek felett leegyszerűsíti a kérdést, mivel vagy $x + y + z = 0$ vagy $x = y = z$ adódik. A polinommal kapcsolatban MacHale [5] cikkében találhatunk több szép összefüggést. Mindkét esetben azonosságot kapunk. A Gauss egészek körében az $x + y + z = 0$ szintén azonossághoz vezet. A másik faktor itt érdekesebb, mert

$$(x - y)^2 + (y - z)^2 = -(z - x)^2 = i^2(z - x)^2 = (iz - ix)^2$$

adódik, azaz pitagoraszi számhármasokat kell meghatározni a Gauss egészek körében. Ilyen irányban történtek kutatások, Cross [2] nyert szép eredményt, továbbá Zanardo és Zannier [7] eredményeit említeném meg, akik más számtestek esetében is sikeresen vizsgálták a problémát. Itt még szeretném megemlíteni, hogy az egészek felett ismertek eredmények a még általánosabb

$$ax^3 + by^3 + cz^3 = dxyz$$

egyenlettel kapcsolatban is [1, 3, 4, 6]. Ismertek családok, amelyekre csak triviális megoldás létezik, a helyzet számtestek felett természetesen változhat. Az $a = b = c = d = 1$ esetben az egészek felett csak triviális megoldások léteznek, a Gauss egészek felett végtelen sok megoldás létezik, például

$$\begin{aligned} x = i, \quad y = -i, \quad z = 1, \\ x = 1 + i, \quad y = 1 - i, \quad z = 2, \\ x = 136 + 273i, \quad y = -231 - 143i, \quad z = 305. \end{aligned}$$

Ilyen esetekben a háttérben lévő elliptikus görbe rangja $\mathbb{Q}$ felett 0, míg az adott számtest felett már pozitív.

Debrecen, 2022. szeptember 22.

Tengely Szabolcs (Debreceni Egyetem)

Hivatkozások

[1] A. Bremner and R. K. Guy. Two more representation problems. *Proc. Edinburgh Math. Soc. (2)*, 40(1):1–17, 1997.

[2] J. T. Cross. Primitive Pythagorean triples of Gaussian integers. *Math. Mag.*, 59(2):106–110, 1986.

[3] E. Dofs. Solutions of $x^3 + y^3 + z^3 = nxyz$. *Acta Arith.*, 73(3):201–213, 1995.

[4] E. Dofs. Unsolvable cases of $P^3+Q^3+cR^3 = dPQR$. *Rocky Mountain J. Math.*, 28(3):927–938, 1998.

[5] D. MacHale. My favourite polynomial. *The Mathematical Gazette*, 75(472):157–165, 1991.

[6] J.J. Sylvester. Xlvii. on the equation in numbers ax 3 +by 3+cz 3=dxyz, and its associate system of equations. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 31(208):293–296, 1847.

[7] P. Zanardo and U. Zannier. The group of Pythagorean triples in number fields. *Ann. Mat. Pura Appl. (4)*, 159:81–88, 1991.