Miroslav Kureš

Najdete třetí Wieferichovo prvočíslo?

Jedním ze základních a matematikům dobře známých výsledků matematické teorie čísel je tzv. **malá Fermatova věta**. Podle ní pro libovolné prvočíslo p a libovolné číslo x, které není násobkem p, platí

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

Vysvětleme nyní tento zápis. Nejprve připomeňme, že prvočíslo je takové přirozené číslo větší než 1, které nemá vlastní dělitele, tzn. je dělitelné kromě 1 jen sebou samým: seznam prvočísel začíná čísly 2, 3, 5, 7, 11, 13, atd. a není těžké ukázat, že prvočísel je nekonečně mnoho. Zápis $x^{p-1} \equiv 1 \pmod{p}$ vyjadřuje, že po umocnění libovolného čísla na $p-1$ a následném vydělení číslem p dostaneme jako zbytek po dělení 1. Jako příklad vezměme dejme tomu p=5 a x=3. Spočteme-li $3^{5-1}=3^4=81$, máme po dělení 81:5 skutečně zbytek 1.

Nyní zvolme x=2. Pak malá Fermatova věta platí pro každé liché prvočíslo, tedy rovnici

$$2^{p-1} \equiv 1 \pmod{p}$$

splňuje nekonečně mnoho prvočísel p, vlastně všechna prvočísla počínaje 3. Položme si nyní otázku: splňují některá prvočísla také rovnici

$$2^{p-1} \equiv 1 \pmod{p^2}?$$

Ještě jednou: po umocnění dvojky na $p-1$ a následném vydělení druhou mocninou čísla p máme obdržet jako zbytek po dělení 1. Pokud ano, nazveme takové prvočíslo **Wieferichovo prvočíslo**.

Arthur Josef Alwin Wieferich se narodil 27. dubna 1884 v německém Münsteru. Publikoval pět původních článků, z toho čtyři, které napsal v letech 1908 a 1909, se ukázaly jako důležité pro další rozvoj teorie čísel. V jednom z nich nazvaném *Zum letzten Fernat'schen Theorem* ukazuje souvislost mezi popsanými speciálními prvočísly a nejslavnějším matematickým problémem (zodpovězeným až 23. června 1993 A. Wilesem), **velkou Fermatovou větou**. (Podle velké Fermatovy věty neexistují pro $n>2$ taková nenulová celá čísla a, b, c, aby platilo $a^n+b^n+c^n=0$.) Arthur Wieferich se po absolvování univerzity v Münsteru stal středoškolským profesorem a dále ve výzkumu nepokračoval, zemřel 15. září 1954 v Meppenu. Jeho publikované výsledky jsou hluboké a dodnes ceněné. Připomeňme alespoň hlavní větu dokázanou ve zmíněném článku.

Věta (Wieferich 1909). Je-li p liché prvočíslo, a, b, c nenulová celá čísla taková, že $a^p+b^p+c^p=0$ a p není dělitelem součinu abc, pak p splňuje $2^{p-1} \equiv 1 \pmod{p^2}$.

Je dokázána řada vlastností Wieferichových prvočísel, například Wieferichovo prvočíslo nemůže být současně Mersennovým prvočíslem (prvočíslo ve tvaru 2^n-1). Přitom známa jsou dosud pouhá dvě Wieferichova prvočísla: **1093** (objevil W. Meissner v roce 1913) a **3511** (N. G. W. H. Beeger v roce 1922). Bude-li chtít čtenář zkontrolovat, že skutečně platí rovnosti

$$2^{1092} \equiv 1 \pmod{1194649} \quad \text{a} \quad 2^{3510} \equiv 1 \pmod{12327121},$$

upozorňujeme, že existují algoritmy na umocňování podstatně zjednodušující výpočet poněkud odstrašujících „velkých" mocnin.

Není ani známo, zda Wieferichových čísel je nutně konečně mnoho. Dostupná časopisecká literatura uvádí, že zhruba do řádu 10^{15} neexistuje další Wieferichovo prvočíslo kromě zmíněných dvou; horní hranice se pochopitelně s nasazením výpočetní techniky bude dále posouvat.