Časopis pro pěstování mathematiky a fysiky

Ludvík Kraus

Důkaz věty, že existuje nekonečně mnoho kmenných čísel $(kp + 1)$, je-li p kmenné

Časopis pro pěstování mathematiky a fysiky, Vol. 15 (1886), No. 2, 61--62

Persistent URL: http://dml.cz/dmlcz/122229

$$\varphi = \frac{A_1 A_9 A_3}{A_0}.$$

Řadami snadno se lze přesvědčiti, *že pro ony soustavy hodnot, pro něž vymizí právě napsaná funkce* φ, *nemůže vymizeti žádná celistvá funkce stupně druhého,* takže tato funkce φ nutně musí býti jednou z oněch 5 hledaných. Cyklickou záměnou výrazu

$$\frac{A_1 A_9 A_3}{A_0}$$

obdržíme všechny hledané funkce φ a sice:

$$\frac{A_1 A_9 A_3}{A_0}, \quad \frac{A_4 A_3 A_1}{A_0}, \quad \frac{A_5 A_1 A_4}{A_0}, \quad \frac{A_9 A_4 A_5}{A_0}, \quad \frac{A_3 A_5 A_9}{A_0},$$

čímž úloha naše úplně řešena jest.

Upotřebíme-li pak ještě transformace uvedené na počátku této stati, jest nám možno i pro křivku $\mathfrak{C}$ udati příslušné funkce φ.

Applikací Abelova theoremu dojdeme konečně té zajímavé věty, *že jest hodnota našeho integralu, vzata podél křivky* C *ve dvou mezích, jež k našim 5 dříve uvedeným soustavám hodnot přísluší,* $\frac{1}{5}\frac{1}{5}$ *jedné periody tohoto integralu.*

Důkaz věty, že existuje nekonečně mnoho kmenných čísel $kp+1$, je-li p kmenné.

Napsal

dr. **Ludvík Kraus.**

Je-li

$$M = a^p - 1,$$

platí

$$\varphi(M) \equiv 0 \pmod{p},$$

značí-li $\varphi(M)$ jako obyčejně počet čísel nesoudělných s M a nepřevyšujících M.*)

*) Je-li $M = a^\nu - 1$, kdež a, ν značí *libovolná* čísla, platí též

$$\varphi(M) \equiv 0 \pmod{\nu},$$

jak ukázáno v pojednání „O jisté větě číselné“ od Ed. Weyra, tento Časopis sv. XI., čl. 7. *Pozn. redakce.*

Neboť nazvu-li b libovolné číslo s M nesoudělné, bude i $a^\lambda b$ takové číslo. Pak je teprve při $q = p$

$$b \equiv a^q b \pmod{M}$$

a ne při $q < p$. Tím obdržím p čísel b, ab, a^2b, ..., $a^{p-1}b$ nesoudělných s M a různých dle mod M. Je-li c další číslo nesoudělné s M a různé od oněch dle mod M, jsou c, ac, a^2c, ..., $a^{p-1}c$ opět nesoudělná s M a dle mod M různá mezi sebou i od předcházejících čísel. Neboť kdyby na př.

$$a^h c \equiv a^g b \pmod{M},$$

tu by

$$a^{h+p-h} c \equiv a^{g+p-h} b \pmod{M},$$

t. j.

$$c \equiv a^{g+p-h} b \pmod{M}$$

t. j. c by bylo shodné s některým z čísel b, ab, a^2b, ..., $a^{p-1}b$, proti supposici. Pokračujíce touto cestou vidíme, že všecka čísla nesoudělná s M a nepřevyšující M lze vyčerpati skupinami po p, pročež jest $\varphi(M)$ dělitelno p.

Obsahuje-li M kmenné faktory r, s, t, ..., bude

$$\varphi(M) = M\left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{s}\right)\ldots$$

Neobsahuje-li M číslo p jakožto faktor, musí tedy na př. $r - 1$ býti dělitelno p a tedy kmenné číslo r tvaru $kp + 1$. Číslo M nebude obsahovati p, je-li p obsaženo v a jakožto faktor. Mohu tím nalézti kmenných čísel tvaru $kp + 1$ kolik chci; neboť nalezl-li jsem jich n na př. p_1, p_2, ..., p_n, naleznu taky $n+1^{ní}$ p_{n+1} od nich různé, kladu-li

$$M = (p p_1 p_2 \ldots p_n)^p - 1.$$