Časopis pro pěstování mathematiky a fysiky

Václav Šimerka

Über die Auflösung der Congruenz $C^2 \equiv C, (\text{mod.} M)$

Časopis pro pěstování mathematiky a fysiky, Vol. 13 (1884), No. 4, 236--238

Persistent URL: http://dml.cz/dmlcz/121109

Jednočlenná perioda zbytků z mocnin bez předchozích členů t. j. řešení shody $C^2 \equiv C$, (mod. M).

Napsal

Václav Šimerka,
farář v Jenšovicích u Vysokého Mýta.

1. V nadepsané shodě jest C nejmenší kladný zbytek při mod. M, tak že tu platí výraz $0 \leqq C < M$.

Objevilo-li by se kdesi $C > M$, třeba je o M neb násobné z něho zmenšiti. Je-li na opak C záporné, uvede se přičtením modulu na kladné.

2. U každého M jest, jakž patrno, jednou $C = 0$, a po druhé $C = 1$. Na tyto dvě hodnoty, co všem případům společné, nemusíme tedy bráti ohled.

3. Násobíme-li nadepsaný výraz číslem C, bude u téhož modulu $C^3 \equiv C^2 \equiv C$ t. j. $C^3 \equiv C$, z toho jde podobně $C^4 \equiv C^2 \equiv C$, tak že při každém celém kladném n, obdržíme $C^n \equiv C$, (mod. M).

U $M = 12$ jest na př. $4^2 \equiv 4$, $4^3 = 64 \equiv 4$, $4^4 = 256 \equiv 4$ a t. d. Periody takové mají tedy pouze jeden člen, před nímž žádné jiné číslo nepřichází, jakož se to na př. děje u $M = 12$, $C_1 = 10$, $C_2 = C^2_1 = 100 \equiv 4$, $C_3 \equiv C^3_1 \equiv C^2_1 . C_1 \equiv 4 . 10 \equiv 4$, a t. d.

4. Z $C^2 \equiv C_1$ (mod. M) jde $C^2 - C = C(C-1) \equiv 0$; je-li tedy $M = pq$, bude $C(C-1)$ součinem pq dělitelno, tak že $C(C-1) = pqxy$ obdržíme. Rovnici této učiníme zadost při $C = px$, $C - 1 = qy$, z čehož pak jde

$$C = px = qy + 1.$$

Z toho viděti, že p, q musí býti čísla nesoudělná, a že má C pouze hodnoty 0, 1, je-li M číslo kmenné neb mocnina z čísla takového. Co do řešení této rovnice, bere se u $px = qy + 1$ buď p neb q za modul, tím určí se nejmenší kladná hodnota pro y neb x, jež svrchu dosazena dává C.

U $M = 35$ jest na př. $C = 5x = 7y + 1$; z toho jde při (mod. 5), $5x \equiv 0$, $7y \equiv 2y$, tedy $0 \equiv 2y + 1$, a $y = 2$ t. j. $C = 15$, tak že obdržíme $C^2 = 225 \equiv 15$, (mod. 35).

Podobně má $M = 119$, $C = 7x = 17y + 1$, což při (mod. 7) $3y + 1 \equiv 0$, $3y \equiv -1$, $3y \equiv 6$, a poněvadž 3 se 7 nesoudělna jsou, bude $y = 2$, tedy $C = 35$.

5. Každé rozvedeni modulu M v činitele $p \,.\, q$ dává dva členy, totiž $C_1 = px = qy + 1$, $C_2 = qx' = py' + 1$, jichž součet $C_1 + C_2 = M + 1$, a které proto doplňky jmenovati můžeme. Uvedené rovnice dávají totiž

$$C_1 + C_2 = px + py' + 1 = qx' + qy + 1 = p(x + y') + 1 = \\ = q(x' + y) + 1,$$

tak že $C_1 + C_2 - 1$ jak činitelem p tak i činitelem q děleno pochází, z čehož při $C_1 < pq$, $C_2 < pq$ jde $C_1 + C_2 - 1 = pq = M$. U $M = 21$ jest na př.

$$C_1 = 3x = 7y + 1 = 15, \quad C_2 = 7x' = 3y' + 1 = 7.$$

Poněvadž $C_1 = px$, $C_2 = qx'$, jest $C_1 C_2 = pqxx'$ modulem M dělitelno. U $M = 21$ nalezneme $15 \,.\, 7 = 105 = 5 \,.\, 21$.

Dále sluší připomenouti, že čtverec rozdílu u doplňků dává zbytek $= 1$, což plyne ze shod

$$(C_1 - C_2)^2 = C_1^2 - 2C_1C_2 + C_2^2 \equiv C_1^2 + C_2^2 \equiv C_1 + C_2 \\ = M + 1 \equiv 1, \text{ (mod. } M).$$

6. Kolik jednočlenných period má modul sestávající z n nesoudělných činitelů?

Máme-li zde $M = a_1 a_2 a_3 \ldots a_n$, dává rozvrh

$$p = 1, \quad q = a_1 a_2 \ldots a_n$$

jednu hodnotu C čili $\binom{n}{0}$.

Vezmeme-li po sobě $p = a_1, a_2, a_3, \ldots, a_n$, za q pak ostatní činitele, obdržíme n hodnot C t. j. $\binom{n}{1}$.

Při $p = a_1 a_2, a_1 a_3, \ldots, a_1 a_n, a_2 a_3, \ldots$ nalezneme tolik hodnot C, kolik *amb* n prvků dává, totiž $\binom{n}{2}$; podobně bude u teren $\binom{n}{3}$ a t. d., tak že hledané množství jest

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n;$$

nehledíme-li pak při tom na 0, 1, bude jich $2^n - 2$.

U $M = 30 = 2 \,.\, 3 \,.\, 5$, kdež tedy $n = 3$, jsou to 6, 10, 15, 16, 21, 25, doplňky jsou pak stejně od předu i zadu vzdáleny totiž $6 + 25 = 10 + 21 = 15 + 16 = 31$.

7. U některých modulů lze již z pouhé jejich podoby jeden pár periodických členů nalézti. U $M = 4\varphi + 2$ jde na př.

z $C_1 = 2x = (2\varphi + 1)y + 1$, při $y = 1$, $C_1 = 2\varphi + 2$, $C_2 = 2\varphi + 1$.
$M = 6$ má dle toho $C = 3, 4$, $M = 10$, $C = 5, 6$.
Podobným způsobem obdržíme u
$M = 16\varphi + 4$, $C = 4\varphi + 1, 12\varphi + 4$.
$M = 16\varphi + 12$, $C = 4\varphi + 4, 12\varphi + 9$.

Poznámka k úrokování složitému.

Napsal
Prof. Dr. **F. J. Studnička.**

Tak zvané úrokování složité, zakládající se v kapitalisování úroků, představuje nám souvislost *pěti* veličin proměnných a sice pod úrok složeného kapitálu K, k němuž se v n ročních lhůtách přirážejí úroky po r let, takže za tuto dobu vyroste k hodnotě K_{nr}, bylo-li vymíněno ročně platiti p ze sta. Souvislost tuto vyjadřuje pak vzorec

$$K_{nr} = K\left(1 + \frac{p}{100n}\right)^{nr}.$$

Jak se tu z daných čtyř veličin vypočítá pátá, neposkytuje žádných obtíží, vyjmouc případ ten, kde hledá se veličina n, jelikož v tomto vzorci obsažena jest co dělitel a co mocnitel. Plyneť zde, logarithmujeme-li, napřed

$$lg\, K_{nr} = lg\, K + nr\, lg\left(1 + \frac{p}{100n}\right),$$

takže jest, položíme-li

$$\frac{1}{r}(lg\, K_{nr} - lg\, K) = b, \qquad (1)$$

nutno řešiti transcendentní rovnici

$$nlg\left(1 + \frac{p}{100n}\right) = b, \qquad (2)$$

aby se ustanovila hodnota veličiny n.

V případech praktických možná však obejíti delší tuto cestu přibližného řešení. Násobíme-li totiž na obou stranách vzorce (2) modulem $m = 2{\cdot}302585$, obdržíme na levé straně logarithmus přirozený a položíme-li na místo něho pouze první dva členy příslušné řady, povstane napřed