Václav Šimerka

Zbytky z arithmetické posloupnosti

Časopis pro pěstování mathematiky a fysiky, Vol. 14 (1885), No. 5, 221--225

Persistent URL: http://dml.cz/dmlcz/122245

Zbytky z arithmetické posloupnosti.

Napsal

Václav Šimerka,

farář v Jenšovicích u Vysokého Mýta.

1. Dosadíme-li do shody

$$u_r \equiv a + br \pmod{p},$$

kdež u_r nejmenší kladný zbytek z $r$tého členu arithm. posloupnosti $a+b$, $a+2b$, $a+3b$, ... jest, $p\varphi + r$ místo r, obdržíme $u\,(p\varphi + r) \equiv a + b\,(p\varphi + r) \equiv a + bp\varphi + br \equiv a + br \equiv u_r$ t. j. $u(p\varphi + r) = u_r$, tedy $u_r = u_{(p+r)} = u_{(2p+r)}$ . . .

Zbytky z arithm. posloupnosti činí při mod. p periodu o p členech, což ostatně se stává, jak netěžko nahlédnouti, u každé shody tvaru

$$u_r \equiv a + br + cr^2 + \ldots + gr^n \pmod{p}.$$

2. Z $u_r \equiv a + br \pmod{p}$

jde též $u_{(p-r)} \equiv a + b(p-r) = a + bp - br \equiv a - br$; z té příčiny obdržíme

$$u_r + u_{(p-r)} \equiv 2a \pmod{p}.$$

Tak při $u_r \equiv 3 + 4r \pmod{11}$ nalezneme

$$u_0 = 3;\ 7,\ 0,\ 4,\ 8,\ 1,\ 5,\ 9,\ 2,\ 6,\ 10,\ 3;$$

$$3 + 3 \equiv 7 + 10 \equiv 0 + 6 \equiv 4 + 2 \equiv \ldots \equiv 6.$$

Jiná vlastnost této periody jest, že se členy od 0 stejně vzdálené do modulu doplňují.

Z $u_r \equiv a + br \pmod{p}$ jde totiž

$$u_{r-v} \equiv a + br - bv,\quad u_{r+v} \equiv a + br + bv,$$

pročež i $u_{r-v} + u_{r+v} \equiv 2(a + br)$.

Je-li tedy $a + br \equiv 0 \equiv p$, bude i $u_{r-v} + u_{r+v} = p$.

Při $8 + 3r \pmod{13}$ jest na př. 11, 1, 4, 7, 10, 0, 3, 6, 9, 12, 2, 5, 8; a $10 + 3 = 7 + 6 = 4 + 9 = \ldots = 13$.

3. Jsou-li b, p čísla nesoudělná, vyskytuji se v periodě z $a + br \pmod{p}$ povstalé jakožto zbytky všechna čísla od 0 až do $p - 1$. Kdyby totiž výrazy $a + br$, $a + b\varrho$ stejné zbytky dávaly, obdržíme ze shody

$$a + br \equiv a + b\varrho \pmod{p},$$

$$br \equiv b\varrho,\quad \text{tedy i}\quad r \equiv \varrho\quad \text{čili}\quad r = \varrho,$$

poněvadž jak r tak $\varrho < p$ jest. Tak dává na př.
$2 + 3r \pmod 8$ periodu 5, 0, 3, 6, 1, 4, 7, 2; 5, 0 atd.

4. Z předešlého odstavce snadno poznati, že, je-li $a = 0$, řada b, $2b$, $3b$, . . ., $(p-1)b$ při mod p za zbytky čísla 1, 2, 3, . . ., $(p-1)$ v jiném seřadění dává. Při $7r \pmod{10}$ jest na př. 7, 4, 1, 8, 5, 2, 9, 6, 3.

5. Kolikátým členem jest dané číslo c v periodě, již

$$a + br \pmod p$$

dává, nalezneme řešením shody

$$a + bx \equiv c \pmod p.$$

Na př. jest při $7 + 45x \equiv 1 \pmod{103}$, $x \equiv -7 \equiv 96$.

6. *Perioda, vzniknuvší z* $a + bqr \pmod{pq}$, *kdež* b, p *čísla nesoudělná jsou, má pouze* p *členů.* Netřeba, tuším, dokládati, že se délka periody nemění, přičteme-li ke všem členům totéž číslo, neb odejmeme-li je od nich. Z té příčiny má hořejší výraz totéž množství periodických členů jako $bqr \pmod{pq}$. Je-li pak při $bqr : pq$ podíl x, bude zbytek číslem q čili cq dělitelný, pročež obdržíme $bqr = pqx + cq$, což zkráceno byvši, dává $br = px + c$, tak že tím ku shodě $br \equiv c \pmod p$ přicházíme, která pouze pčlennou periodu má. Ve $4 + 6r \pmod{15}$ jest na př. následkem $p = 5$, $q = 3$ perioda 5tičlenná, totiž 10, 1, 7, 13, 4; 10 atd.

V tomto případě rozpadá se, hledíc k odstavci prvnímu, perioda pqčlenná v q period o p členech.

7. *Při nesoudělných* p, q *jest v mezích* 0, $pq - 1$ *vždy jedno číslo* k *(a ne více), jež potažně zbytky* a, b *dává;* čili jinými slovy: rovnice

$$k = px + a = qy + b$$

jest vždy při $k < pq$ řešitelna. Z výrazu $a + px$ obdržíme totiž při $x = 0, 1, 2, \ldots, q-1$ posloupnost:

$$a,\ a + p,\ \ldots,\ a + (q-1)\,p,$$

ta pak dává při mod q dle odstavce 3. za zbytky všechna celá čísla od 0 až do $q-1$, mezi nimiž tedy bude i zbytek b, a člen, u něhož b se skytá, bude $= k$. Poněvadž poslední největší člen $a + pq - p$ za příčinou $p > a$ jest $< pq$, budou takovými i ostatní členy, tedy i k. Tak dává

$$k = 5x + 2 = 7y + 3 \text{ při (mod 5)},$$
$$2 \equiv 2y + 3, \quad 2y \equiv -1 \equiv 4, \quad y = 2, \quad k = 17.$$

V rovnici

$$k = nx + a = py + b = qz + c,$$

kdež n, p, q jsou čísla nesoudělná, určí se nejprve

$$k' = n\varphi + a = p\psi + b,$$

kdež tedy k' při mod n, p za zbytky a, b má, načež pak nalezneme

$$k = npt + k' = qz + c,$$

při čemž z podobné příčiny $k < npq$ býti musí.

Při $k = 3x + 1 = 5y + 2 = 8z + 3$ nalezneme na př. $k' = 7$, tedy $k = 15t + 7 = 8z + 3 = 67$.

Týmž způsobem třeba i u
$k = mx + a = ny + b = pz + c = q\omega + d$ atd. pokračovati.

8. Aby rovnice

$$k = \alpha\beta px + a = \beta qy + b,$$

kdež αp, q nesoudělna jsou, řešitelna byla, musí býti

$$a \equiv b \pmod{\beta}.$$

Je-li tomu tak, položme $\beta y = z$, a jest

$k = \alpha\beta px + a = qz + b$, při čemž se objeví $k < \alpha\beta pq$.

Z $k = 24x + 5 = 20y + 9$ jde dle toho

$$k = 24x + 5 = 5z + 9,$$

a při (mod 5), $-x \equiv -1, x = 1$, tedy $k = 29 < 120$.

Tím způsobem třeba i v jiných podobných případech počítati.

9. Dle odstavce 4. dává řada b, $2b$, $3b$, . . ., $(p-1)b$ při modulu p, jenž s b nesoudělný jest, zbytky 1, 2, 3, . . ., $(p-1)$, pročež nalezneme

$$b \,.\, 2b \,.\, 3b \,\ldots\, (p-1)b \equiv 1 \,.\, 2 \,.\, 3 \,\ldots\, (p-1)$$

čili

$$b^{p-1}(p-1)! \equiv (p-1)!.$$

Kdykoli tedy p jest kmenné číslo, jež proto s $(p-1)!$ společného dělitele nemá, bude

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

Udává-li pro lepší přehled b_n nejmenší zbytek z b^n, bude na př. při $p = 61$, $b = 2$, $2_6 = 3$, $2_{12} = (2_6)^2 = 9$,
$2_{15} \equiv 2_{12} \,.\, 2_3 = 9 \,.\, 8 \equiv 11, 2_{30} \equiv (2_{15})^2 = 121 \equiv -1, 2_{60} = +1.$

Podobně nalezneme při $p = 193$, $b = 3$, $3_4 = 81$, $3_8 = -1$, $3_{16} = +1$, $(3_{16})^{12} = 3_{192} = +1$.

Poučka tato dle vynálezce řečená Fermatovou jest jednou z nejdůležitějších v neurčité analytice; neudává však charakteristickou známku kmenných čísel, (jíž by se tato ode všech ostatních lišila), ježto podobně i při některých dělitelných číslech bývá. Tak na př. při $561 = 3 \cdot 11 \cdot 17$, $b = 2$ nalezneme

$$2_{10} = -98,\ 2_{20} = 67,\ 2_{40} = 1,\ (2_{40})^{14} = 2_{560} = 1.$$

Tolikéž u čísel

$1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$,
$2821 = 7 \cdot 13 \cdot 31$, $6601 = 7 \cdot 23 \cdot 41$, $8911 = 7 \cdot 19 \cdot 67$ a j. v.,
kdykoli b s modulem nesoudělné jest.

10. K úvahám těmto můžeme též připojiti poučku *Wilsonovu* zahrnutou ve výraze

$$(p-1)! + 1 \equiv 0 \pmod{p},$$

jež jest charakteristickou známkou každého kmenného čísla p.

Shodu

$$az \equiv 1 \pmod{p},$$

kdež a jedno z čísel 2, 3, 4, ..., $p-2$ jest, lze vždy jednou podobnou hodnotou z řešiti, ježto a, p nesoudělna jsou. Dvou hodnot z nemá; neboť by z $az \equiv 1$, $az' \equiv 1$ šlo $az \equiv az'$ čili $z = z'$. Následkem toho rozpadají se uvedená čísla v $\frac{p-3}{2}$ párů, z nichž součin každého 1 za zbytek dává. Je-li $p = 11$, jsou na př. takové páry $2 \cdot 6$, $3 \cdot 4$, $5 \cdot 9$, $7 \cdot 8$. Z té příčiny jest i $2 \cdot 3 \cdot 4 \ldots (p-2) \equiv 1$. K tomu dává případ $a = z$ čili shoda $z^2 \equiv 1$, ještě pár $1, -1$ čili $1 \cdot (p-1)$, tak že obdržíme $1 \cdot 2 \cdot 3 \ldots (p-2)(p-1) \equiv p - 1 \equiv -1$,
což ku hořejšímu výrazu vede.

U $p = 5$ jest na př. $4! + 1 = 25 \equiv 0 \pmod{5}$; $p = 7$ má $6! + 1 = 721 = 7 \cdot 103$.

U $p = mn$ jest i m i $n < p - 1$, pročež $(p-1)!$ součinem $mn = p$ dělitelno. Totéž stává se u $p = m^2$, kde m za příčinou

$$(p-1)! = 1 \cdot 2 \ldots m\,(m+1) \ldots (2m) \ldots (p-1)$$

po druhé ve $2m$ pochází.

Krampovo číslo $(p-1)!$ můžeme si zde mysliti rozvrženo ve dva součiny po $\frac{p-1}{2}$ činitelích, a sice

$$1.2.3\ldots\frac{p-1}{2}=\frac{p-1}{2}!\text{ a }\frac{p+1}{2}.\frac{p+3}{2}\ldots(p-2)(p-1);$$

odejmeme-li od každého činitele posledního výrazu modul p, t. j. počítáme-li se zbytky na prosto nejmenšími, bude

$$-\frac{p-1}{2}.-\frac{p-3}{2}\ldots.-2.-1=1.2.3\ldots$$

$$.\frac{p-1}{2}.\left(-1\right)^{\frac{p-1}{2}}=\frac{p-1}{2}!\left(-1\right)^{\frac{p-1}{2}}.$$

Pak výraz

$$(p-1)!+1\equiv 0 \text{ čili } (p-1)!\equiv -1 \pmod p$$

obdrží podobu

$$\left(\frac{p-1}{2}!\right)\left(-1\right)^{\frac{p-1}{2}}\equiv -1$$

t. j.
$$\left(\frac{p-1}{2}!\right)^2\equiv\left(-1\right)^{\frac{p+1}{2}}\pmod p.$$

Protož nalezneme při mod $(p=4\varphi\mp 1)$,

$$\left(\frac{p-1}{2}!\right)^2\equiv\pm 1.$$

U $p=11$ jest $(5!)^2=120^2\equiv(-1)^2=+1$,
kdežto $p=13$, dává $(6!)^2=720^2\equiv 5^2\equiv 25\equiv -1$.

11. Poněvadž dle předcházejícího odstavce u modulu $p=4\varphi-1$ jest $\left(\frac{p-1}{2}!\right)^2\equiv+1$, bude u každého takového kmenného čísla zbytek z $\frac{p-1}{2}!$ buď $+1$ neb -1. Prvější stává se u $p=3, 23, 59, 71$ a j. v.,
druhé pak u $p=7, 11, 19, 31, 43, 47, 67, 79$ atd.

S touto vlastností kmenných čísel z podoby $p=4\varphi-1$ zdá se, že u $p=4\varphi+1$ souhlasí okolnost ta, že v $x^2\equiv -1$, béřeme-li $x<\frac{p}{2}$, má x buď sudou neb lichou hodnotu.

Tak pro $p=5, 17, 29, 37, 41, 53, 61, 73, 89$ atd.
nalezneme $x=2, 4, 12, 6, 9, 23, 11, 27, 34$ atd.