Математичка гимназија у Београду
Додатна настава за трећи разред
21.02.2006.

Експоненцијалне конгруенције

Миливоје Лукић

1. Кармајклова функција

Дефиниција 1: Кармајклова функција $\lambda : \mathbb{N} \to \mathbb{N}$ дефинише се на следећи начин:

1. $\lambda(1) = 1,\ \lambda(2) = 1,\ \lambda(4) = 2,\ \lambda(2^\alpha) = 2^{\alpha-2},$ за $\alpha > 2$
2. $\lambda(p^\alpha) = p^{\alpha-1}(p-1)$, за непаран прост број p и природан број α
3. $\lambda\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) = [\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})]$

Теорема 1: Нека је n природан број. За сваки цео број a узајамно прост са n важи

$$a^{\lambda(n)} \equiv 1 \pmod{n}. \tag{1}$$

Теорема 2: За све $n \in \mathbb{N}$ важи $\lambda(n)|\varphi(n)$, при чему је $\lambda(n) = \varphi(n)$ ако и само ако је $n = 1$, 2, 4, p^α или $2p^\alpha$ где је p непаран прост број, и α природан број.

2. Поредак броја по модулу и примитиван корен

Дефиниција 2: За природан број $m > 1$, и цео број a узајамно прост са m, **поредак броја** a **по модулу** m је најмањи природан број δ за који важи $a^\delta \equiv 1 \pmod{m}$; односно,

$$\delta_m(a) = \min\{k \in \mathbb{N} | a^k \equiv 1 \pmod{p}\}. \tag{2}$$

Теорема 3:

$$m|a^x - 1 \ \Leftrightarrow\ \delta_m(a)|x. \tag{3}$$

Доказ: Нека је $a^x \equiv 1 \pmod{m}$. Означимо $x = r\delta_m(a) + s$, где је $r, s \in \mathbb{N}_0$ и $0 \le s < \delta_m(a)$. Тада је

$$a^s \equiv 1^r a^s \equiv (a^{\delta_m(a)})^r a^s \equiv a^x \equiv 1 \pmod{m}.$$

Како је $s < \delta_m(a)$, а према дефиницији $\delta_m(a)$ не може постојати мањи природан степен a који даје остатак 1, следи да s није природан број, односно $s = 0$. Супротан смер се доказује непосредно. □

Последица: $\delta_m(a)|\lambda(m)$

Дефиниција 3: Број a је **примитиван корен** по модулу m ако и само ако је

$$\delta_m(a) = \varphi(m). \tag{4}$$

Примитивни корени постоје по модулима 1, 2, 4, p^α, $2p^\alpha$.

Теорема 4: Нека је p прост број и $\delta \in \mathbb{N}$ делилац броја $p-1$. Тада тачно $\varphi(\delta)$ бројева из скупа $\{1, 2, \ldots, p-1\}$ имају поредак δ по модулу p.

Последица: Сваки прост број p има бар један примитиван корен; тачније, има их $\varphi(p-1)$.

Теорема 5: Природан број $m > 1$ има примитивне корене ако и само ако је облика 2, 4, p^α, $2p^\alpha$, где је p непаран прост број и α природан број. Број примитивних корена оваквог броја m је $\varphi(\varphi(m))$.

3. Експоненцијалне конгруенције

Теорема 6: Нека је p непаран прост број, $a \in \mathbb{Z}$, и $p|a \pm 1$. Тада

$$p^s || a \pm 1 \Rightarrow p^{s+1} || a^p \pm 1$$

Последица: Означимо $\delta_p(a) = \delta$, и $p^\alpha || a^\delta - 1$. Тада

$$p^{\alpha+r} | a^s - 1 \Leftrightarrow \delta p^r | s$$

Теорема 7: Нека је $a \in \mathbb{Z}$, $4 | a \pm 1$. Тада

$$2^s || a \pm 1 \Rightarrow 2^{s+1} || a^2 - 1$$

Последица: Означимо $\delta_4(a) = \delta$, и $2^\alpha || a^\delta - 1$. Тада

$$2^{\alpha+r} | a^s - 1 \Leftrightarrow \delta 2^r | s$$

4. Задаци

1. У зависности од природног броја k, одредити остатак по модулу p суме

$$S_k = \sum_{i=1}^{p-1} i^k.$$

2. За дат непаран прост број p, одредити све функције $f : \mathbb{Z} \to \mathbb{Z}$ које задовољавају следеће услове:

   (1) $f(m) = f(n)$ за све $m, n \in \mathbb{Z}$ за које $m \equiv n \pmod{p}$

   (2) $f(mn) = f(m)f(n)$ за све $m, n \in \mathbb{Z}$

3. Да ли је могуће распоредити бројеве 1, 2,. . . , 1996 у темена правилног 1996-угла тако да за свака три суседна броја a, b, c таква да је b између a и c важи $1997 | b^2 - ac$?

4. Доказати да је за сваки прост број $p \geq 5$ бројилац m разломка

$$\frac{m}{n} = \frac{1}{1} + \frac{1}{2} + \ldots \frac{1}{p-1}$$

   дељив са p^2.

5. (БМО1999.2) Нека је $p > 3$ прост број облика $3m + 2$. Означимо са S скуп свих бројева облика $x^2 - y^3 - 1$ за $0 \leq x, y \leq p - 1$. Доказати да је највише $p - 1$ елемент скупа S дељив са p.

6. Доказати да ако је k непаран природан број, и n природан број, онда $2^{n+2} | k^{2^n} - 1$.

7. Доказати да за свако природно $m > 1$ постоји природан број n такав да $2^m | 19^n - 97$.

8. Доказати да ако је број $1 + 2^n + 4^n$ прост за неко $n \in \mathbb{N}$, онда је $n = 3^k$, за неко $k \in \mathbb{N} \cup \{0\}$.

9. Наћи све просте бројеве p за које $p | 2^p + 1$.

10. Наћи све природне бројеве n такве да $n^2 | 2^n + 1$.

11. Наћи све природне бројеве n такве да $n | 2^n - 1$.

12. Наћи све непарне бројеве n такве да $n | 3^n + 1$.

13. Доказати да постоји бесконачно много природних бројева n таквих да $n | 2^n + 1$.

14. Доказати да постоји бесконачно много природних бројева n таквих да $n | 3^n + 1$.

15. Доказати да за свако природно $a > 1$ постоји бесконачно много природних бројева n, таквих да $n | a^n + 1$.

16. Наћи највећи степен k броја 1991 за који 1991^k дели број

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

17. Одредити све парове простих бројева p и q за које је за свако природно a испуњено

$$a^{3pq} \equiv a \pmod{3pq}.$$

18. Нека је $p > 2$ прост број. Доказати да је сваки делилац броја $2^p - 1$ облика $2kp + 1$ за неки природан број k.

19. Нека је p прост број већи од 3. Доказати да је сваки делилац броја $(2^p + 1)/3$ облика $2kp + 1$, где је k цео број.

20. (ИМО1997.предлог) Нека су b, m, n природни бројеви такви да је $b > 1$ и $m \neq n$. Доказати: ако $b^m - 1$ и $b^n - 1$ имају исте просте делиоце онда је $b + 1$ степен броја 2.

21. (ИМО2000.5) Одредити да ли постоји природан број n који има тачно 2000 различитих делилаца, такав да $n|2^n + 1$.

22. (ИМО1999.4) Одредити све парове (n, p) позитивних целих бројева за које важи: p је прост број; $n \leq 2p$; број $(p-1)^n + 1$ је дељив са n^{p-1}.

23. (ИМО2000.предлог) Одредити све природне бројеве a, m и n за које

$$a^m + 1 | (a+1)^n.$$

5. Решења

1. Познато нам је да постоји примитиван корен по модулу p. Означимо један такав примитиван корен са g. Тада постоји пермутација π скупа $N = \{1, 2, \ldots, p-1\}$ таква да је за свако $i \in N$ испуњено $\pi(i) \equiv g^i \pmod{p}$. Тада је

$$S \equiv \sum_{i=1}^{p-1} i^k \equiv \sum_{i=1}^{p-1} \pi(i)^k \equiv \sum_{i=1}^{p-1} (g^i)^k \equiv \sum_{i=1}^{p-1} (g^k)^i \pmod{p}.$$

Означимо последњу суму са S'. Ако је $g^k \equiv 1 \pmod{p}$ (што важи ако и само ако $p-1|k$, јер је g примитиван корен!) онда је $S' \equiv \sum_{i=1}^{p-1} 1^i \equiv p - 1 \equiv -1 \pmod{p}$. У супротном, пошто је $S' = (g^{kp} - g^k)/(g^k - 1)$, и $p|g^{kp} - g^k$, $p \not| g^k - 1$, важи $p|S'$. Дакле,

$$S \equiv \begin{cases} -1 & \text{за} \quad p-1|k \\ 0 & \text{за} \quad p-1 \not| k \end{cases} \pmod{p}. \quad \square$$

2. Означимо са g примитиван корен по модулу p. Из (2), за $m = n = 0$, добијамо $f(0) = f(0)^2$, а за $m = n = 1$ добијамо $f(1) = f(1)^2$. Дакле, $f(0), f(1) \in \{0, 1\}$. Раздвојимо случајеве:

   (а) $f(1) = 0$: У овом случају је $f(m) = f(m \cdot 1) = f(m)f(1) = 0$, па је решење $f_1 \equiv 0$.

   (б) $f(1) = 1$: Како је $g^{p-1} \equiv 1 \pmod{p}$, то је $f(g)^{p-1} = f(1) = 1$, одакле је $f(g) \in \{-1, 1\}$. Раздвојимо поново случајеве:

      и. $f(g) = 1$: Овим је одређена функција за све вредности аргумента које нису дељиве са p. Имајући у обзир да $f(0) \in \{0, 1\}$, добијамо два решења: $f_2 \equiv 1$ и

$$f_3(n) = \begin{cases} 1 & \text{за} \quad p \not| n \\ 0 & \text{за} \quad p|n \end{cases} \pmod{p}.$$

Непосредно се проверава да ове функције заиста задовољавају тражене услове.

ии. $f(g) = -1$: У овом случају $f(0) = f(0 \cdot g) = f(0)f(g) = -f(0)$, па је $f(0) = 0$. Такође је $f(g^k) = (-1)^k$. У овој функцији препознајемо управо Лежандров симбол, па је последње решење

$$f_4(x) = \left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}. \quad \square$$

3. Да. Приметимо да је 1997 прост број. Нека је g примитиван корен по модулу 1997. Ставимо остатак при дељењу g^i са 1997 у i-то теме 1996-угла. Тада ће за узастопна темена бити $b^2 - ac \equiv (g^i)^2 - (g^{i-1} \cdot g^{i+1}) \equiv g^{2i} - g^{2i} \equiv 0 \pmod{1997}$. $\square$

18. Пошто је производ два броја облика $2kp+1$ и сам број овог облика, и пошто је сваки делилац броја $2^p - 1$ производ неких његових простих делилаца, довољно је тврђење доказати за све просте делиоце броја $2^p - 1$. Нека је q прост број такав да $q|2^p - 1$. Нека је δ поредак броја 2 по модулу q. Тада $\delta|p$, па пошто је p прост, $\delta \in \{1, p\}$. Ако би било $\delta = 1$, било би $p|2^1 - 1 = 1$, чиме долазимо до контрадикције. Дакле, $p = \delta$. Према малој Фермаовој теореми, $q|2^{q-1} - 1$, па и $\delta|q - 1$, односно $p|q - 1$. Другим речима, $q = lp + 1$, за неко $l \in \mathbb{Z}$. Лако се проверава да l мора бити паран број, па је $q = 2kp + 1$. $\square$

19. Слично решењу претходног задатка.