Конгруенције вишег степена по модулу p^k

У преосталом делу ове главе наводимо неке особине конгруенција чији су докази нешто сложенији, те предлажемо читаоцима да их приликом првог упознавања са овим предметом прескоче и врате се на њих касније. У овом одељку навешћемо нека тврђења о конгруенцијама по модулу p^k, где је p прост број, а у наредном доказ егзистенције примитивног корена по простом модулу који смо најавили раније.

Нека је $m > 1$ природан и a цео број, при чему је $(a, m) = 1$. Нека је n поредак броја a по модулу m, тј. најмањи природан број за који $m \mid a^n - 1$. Подсетимо се да, на основу теореме 10, за свако $s \in \mathbf{N}$, $m \mid a^s - 1$ ако и само ако $n \mid s$.

Ако је a произвољан цео број и p прост број, $p \nmid a$, тада постоји $n \in \mathbf{N}$ такво да $p^k \mid a^n - 1$. Штавише, како $p^k \mid a^{\varphi(p^k)} - 1 = a^{p^{k-1}(p-1)} - 1$, најмање такво n (тј. поредак броја a по модулу p^k) је делилац броја $p^{k-1}(p-1)$.

Теорема 14. *Нека је $a \neq 1$ цео број, n природан број и p непаран прост делилац броја $a - 1$. Ако $p^\alpha \mid a - 1$ и $p^{\alpha+1} \nmid a - 1$, тада $p^{\alpha+\beta} \mid a^n - 1$ ако и само ако $p^\beta \mid n$ (где $\alpha \in \mathbf{N}$ и $\beta \in \mathbf{N}_0$).*

Доказ. Нека је $a = 1 + p^\alpha a_1$, где $p \nmid a_1$, и нека је p^β највећи степен броја p који дели n. Тада је

$$a^n - 1 = (1 + p^\alpha a_1)^n - 1 = np^\alpha a_1 + \frac{n(n-1)}{2} p^{2\alpha} a_1^2 + \cdots + p^{n\alpha} a_1^n.$$

Како су сви сабирци у овој суми осим првог дељиви са $p^{\alpha+\beta+1}$, док је први дељив са $p^{\alpha+\beta}$ и није са $p^{\alpha+\beta+1}$, тврђење следи. ■

Следеће тврђење је директна последица претходног.

Теорема 15. *Нека је δ поредак целог броја a по модулу непарног простог броја p (при чему је $(a, p) = 1$), и нека је p^α највећи степен броја p који дели $a^\delta - 1$. Тада је поредак броја a по модулу $p^{\alpha+\beta}$ једнак $p^\beta \delta$ за свако $\beta \in \mathbf{N}_0$.* ■

Аналогно тврђење за степене двојке је мало другачије.

Теорема 16. *Нека је $a \neq 1$ непаран и n природан број. Ако $2^\alpha \mid a^2 - 1$ и $2^{\alpha+1} \nmid a^2 - 1$, тада $2^{\alpha+\beta} \mid a^n - 1$ ако и само ако $2^{\beta+1} \mid n$ (где $\alpha \in \mathbf{N}$ и $\beta \in \mathbf{N}_0$).*

Доказ. Лако се види да мора бити $\alpha \geqslant 3$. Нека је $n = 2^{\beta+1} n_1$, где је n_1 непаран број. Означимо $b = a^{2^{\beta+1}}$. Важи једнакост

$$a^n - 1 = b^{n_1} - 1 = (b-1)(b^{n_1-1} + \cdots + b + 1).$$

Приметимо да је $b^{n_1-1} + \cdots + b + 1$ непаран број за свако b. С друге стране, важи $b - 1 = (a^2-1)(a^2+1)(a^4+1)\cdots(a^{2^\beta}+1)$, при чему су a^2+1, $a^4+1, \ldots,$ $a^{2^\beta}+1$ сви дељиви са 2, а нису са 4. Према томе, $a^n - 1$ је дељиво са $2^{\alpha+\beta}$, а није са $2^{\alpha+\beta+1}$. ■

Задатак 10. Доказати да је $2^{3^n}+1$ дељиво са 3^{n+1}, а није са 3^{n+2}.

Решење. Како је $2^{3^n} \equiv 2 \pmod 3$, највећи степен тројке који дели $2^{3^n}+1$ једнак је највећем степену тројке који дели $2^{2\cdot 3^n}-1=(2^{3^n}+1)(2^{3^n}-1)$. С обзиром да $3 \mid 2^2-1$ и $3^2 \nmid 2^2-1$, на основу теореме 14, највећи степен тројке који дели $2^{2\cdot 3^n}-1$ је једнак 3^{n+1}. △

Задатак 11. Наћи све природне бројеве n такве да $n^2 \mid 2^n+1$.

Решење. Тривијално решење је $n=1$. Претпоставимо да неко $n>1$ задовољава $n^2 \mid 2^n+1$. Јасно је да је n непарно. Нека је $p>2$ најмањи прост делилац броја n. Тада $p \mid 2^n+1$ повлачи $p \mid 2^{2n}-1$, а по малој Фермаовој теореми $p \mid 2^{p-1}-1$. Према томе, $p \mid (2^{2n}-1, 2^{p-1}-1) = 2^d-1$, где је $d=(2n,p-1)=2$ јер n нема простих делилаца мањих од p. Дакле, $p \mid 2^2-1=3$ па је $p=3$.

Напишимо n у облику $n=3^k n_1$, где је $k \geqslant 1$ и n_1 природан број који није дељив са 3. На основу теореме 14, највећи степен тројке који дели $2^{2n}-1$ је 3^{k+1}. Међутим, из $n^2 \mid 2^{2n}-1$ следи $3^{2k} \mid 2^{2n}-1$. Закључујемо да је $k=1$.

Претпоставимо да је $n_1>1$, и нека је q најмањи прост делилац броја n_1. Како $q \mid 2^{2n}-1=2^{6n_1}-1$ и $q \mid 2^{q-1}-1$, следи да $q \mid 2^d-1$, где је $d=(6n_1,p-1)$. Како су n_1 и $p-1$ узајамно прости на основу избора броја p, важи $d \mid 6$. Сада $q \mid 2^6-1=63=3^2\cdot 7$, па мора бити $q=7$. Међутим $7 \mid 2^n-1$ не важи ни за један природан број n, што је контрадикција. Дакле, једино решење n веће од 1 је $n=3$. △

Доказ егзистенције примитивног корена по простом модулу

Лема 2. *Ако је $r_m(x)=ab$, онда је $r_m(x^a)=b$.*

Доказ. Означимо $r_m(x^a)=\gamma$. Тада је $(x^a)^\gamma \equiv 1 \pmod m$, тј. $x^{a\gamma} \equiv 1 \pmod m$, па $r_m(x)=ab \mid a\gamma$, одакле следи $b \mid \gamma$.

Обратно, из $x^{ab} \equiv 1 \pmod m$ следи $(x^a)^b \equiv 1 \pmod m$, одакле $r_m(x^a)=\gamma \mid b$. Значи, $\gamma=b$. ■

Лема 3. *Ако је $r_m(x)=a$, $r_m(y)=b$ и $(a,b)=1$, онда је $r_m(xy)=ab$.*

Доказ. Означимо $r_m(xy)=\gamma$. Тада је $(xy)^\gamma \equiv 1 \pmod m$, па и $x^{b\gamma}y^{b\gamma} \equiv 1 \pmod m$. Због $r_m(y)=b$ (дакле, $y^b \equiv 1 \pmod m$) одавде следи да је $x^{b\gamma} \equiv 1 \pmod m$, а како је $r_m(x)=a$, и $a \mid b\gamma$. Из $(a,b)=1$ одавде следи и да $a \mid \gamma$. Слично се доказује и да $b \mid \gamma$, дакле $ab \mid \gamma$.

С друге стране, из $x^a \equiv 1 \pmod m$ и $y^b \equiv 1 \pmod m$ следи $(xy)^{ab} \equiv 1 \pmod m$, па $\gamma = r_m(xy) \mid ab$. Значи, $\gamma=ab$. ■

Лема 4. *Нека је p прост број, $n \in \mathbf{N}$ и*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

полином с целобројним коефицијентима. Ако конгруенција

$$f(x) \equiv 0 \pmod p \tag{1}$$

има више од n решења (различитих по модулу p), онда $p \mid a_k$ за свако $k = 0, 1, \ldots, n$.

Доказ. Нека су x_1, x_2, ..., x_{n+1} остаци по модулу p различитих решења конгруенције (1). Полином $f(x)$ се може представити у облику

$$\begin{aligned} f(x) = {} & b_n(x-x_1)(x-x_2)\cdots(x-x_{n-1})(x-x_n) \\ & + b_{n-1}(x-x_1)(x-x_2)\cdots(x-x_{n-1}) \\ & + \cdots \\ & + b_1(x-x_1) \\ & + b_0. \end{aligned} \tag{2}$$

Заиста, изаберимо најпре $b_n = a_n$. Затим бирамо коефицијент b_{n-1} тако да збир коефицијената уз x_{n-1} полинома на десној страни (уствари, полинома који се добија када се измноже заграде у прва два његова сабирка) буде једнак a_{n-1}. Настављајући овај поступак одређују се остали коефицијенти b_{n-2}, ..., b_1, b_0.

Замењујући у релацији (2), редом, $x = x_1$, $x = x_2$, ..., $x = x_{n+1}$, закључујемо да $p \mid b_0$, $p \mid b_1$, ..., $p \mid b_n$, одакле непосредно следи да су и сви коефицијенти a_n, a_{n-1}, ..., a_0 полазног полинома дељиви са p, као суме бројева дељивих са p. ■

Теорема 17. *За сваки прост број p постоји примитивни корен по модулу p.*

Доказ. За $p = 2$ тврђење је тривијално. Претпоставимо да је p непаран.

Нека је

$$\{r_p(1), r_p(2), \ldots, r_p(p-1)\} = \{\gamma_1, \gamma_2, \ldots, \gamma_r\},$$

тј. нека су γ_1, γ_2, ..., γ_r сви могући различити поретци бројева 1, 2, ..., $p-1$ по модулу p. Означимо са $S = [\gamma_1, \gamma_2, \ldots, \gamma_r]$ најмањи заједнички садржалац тих бројева и нека је $S = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ његова канонска факторизација. Сваки фактор $q_i^{\alpha_i}$ тог разлагања је делилац бар једног од бројева γ_j, тј. важи $\gamma_j = \beta q_i^{\alpha_i}$. Нека је сада c_j било који од бројева 1, 2, ..., $p-1$ за који је $r_p(c_j) = \gamma_j$. На основу леме 2, за $d_j = c_j^{\beta}$ је $r_p(d_j) = q_i^{\alpha_i}$, па из леме 3 следи да за број $g = d_1 d_2 \cdots d_k$ важи $r_p(g) = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k} = S$. Но, то значи да $S \mid p-1 = \varphi(p)$.

Сада, међутим, имамо да сви бројеви γ_1, γ_2, ..., γ_r деле S, што значи да је за свако $x \in \{1, 2, \ldots, p-1\}$ задовољена конгруенција $x^S \equiv 1 \pmod p$. Но, према леми 4, онда мора бити $p - 1 \leqslant S$, па из доказаног $S \mid p-1$ следи да је $S = p-1$ и g је примитивни корен по модулу p. ■

Искористимо још лему 4 за нови доказ теореме 12.

Други доказ Вилсонове теореме. За $p=2$ тврђење је очигледно. Нека је $p>2$ и посматрајмо конгруенцију

$$(x-1)(x-2)\cdots(x-(p-1))-(x^{p-1}-1)\equiv 0 \pmod p.$$

Она је степена не већег од $p-2$, а има $p-1$ различито решење (бројеве 1, 2, ... , $p-1$, на основу мале Фермаове теореме). Из леме 4 следи да су сви коефицијенти полинома на левој страни дељиви са p, специјално са p је дељив његов слободни члан $(p-1)!+1$, што је и требало доказати. ∎