Конгруенције вишег степена

трећа-1 верзија: 20.12.2012.

Душан Ђукић

1° Фермаова теорема и уопштења

Овде ћемо се бавити углавном понашањем степена фиксног целог броја по датом модулу. На пример, шта запажамо ако посматрамо остатке бројева $1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, \ldots$ при дељењу са 7? Остаци су редом $1, 2, 4, 1, 2, 4, 1, 2, 4, \ldots$ - примећујемо да се низ $1, 2, 4$ периодично понавља, са периодом 3, и да се не појављују остаци $0, 3, 5, 6$. Међутим, ако уместо степена двојке посматрамо степене тројке, при дељењу са 7 добијамо остатке $3, 2, 6, 4, 5, 1$ који се понављају са периодом 6 - овог пута, сви остаци по модулу 7 осим нуле су ту.

Вероватно најпознатије тврђење је Фермаова теорема, понекад звана "мала" како би се нагласила разлика од тзв. Велике Фермаове теореме.

T.1 (*Фермаова теорема*). За сваки прост број p и цео број a важи $a^p \equiv a \pmod{p}$.

Доказ. Оба скупа $\{1, 2, \ldots, p-1\}$ и $\{a, 2a, \ldots, (p-1)a\}$ чине потпуне системе остатака по модулу p, па су им производи елемената конгруентни по модулу p, тј. $(p-1)! \equiv a^{p-1}(p-1)!$. Скраћивањем $(p-1)!$ добијамо тражено тврђење. □

Поменимо и *Ојлеров критеријум*, којег се сећамо из теорије квадратних остатака:

- Ако је p прост и a цео прој, онда је $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

У Фермаовој теореми је кључан услов да је p прост број. За сложене бројеве, исто тврђење у општем случају не важи - нпр. $a^4 - a$ није обавезно дељиво са 4 за $a \in \mathbb{Z}$. Ипак, оно се може без тешкоћа допунити тако да важи и за сложене бројеве. За то нам је потребна позната Ојлерова функција φ.

Дефиниција. За произвољан природан број $n > 1$, *Ојлерова функција* $\varphi(n)$ означава број свих природних бројева мањих од n који су узајамно прости са n.

Ојлерова функција је мултипликативна у аритметичком смислу, тј. ако је $(m, n) = 1$, онда је $\varphi(mn) = \varphi(m)\varphi(n)$. Може се лако показати да је, ако се n раставља на просте чиниоце као $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$,

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right).$$

T.2 *(Ојлерова теорема).* Ако је n природан и a цео број такав да је $(a, n) = 1$, важи $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Доказ је аналоган доказу Фермаове теореме. Ако је $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ сведен систем остатака по модулу n, онда је то и $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$. Према томе, производи елемената у ова два скупа су једнаки по модулу n: $r_1 r_2 \cdots r_{\varphi(n)} \equiv a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}$. Остаје да се скрати $r_1 r_2 \cdots r_{\varphi(n)}$. □

Задатак 1. Испитујући случај $n = 561$, доказати да *није тачно* следеће: ако за свако $a \in \mathbb{Z}$ узајамно просто са n важи $a^{n-1} \equiv 1 \pmod{n}$, онда је n прост број.

Решење. Имамо $n = 561 = 3 \cdot 11 \cdot 17$. За свако a које није дељиво са $3, 11$ или 17 важи $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$ и $a^{16} \equiv 1 \pmod{17}$. Степеновањем ове три конгруенције са експонентима $280, 56, 35$ редом добијамо $a^{560} \equiv 1$ по модулима 3, 11 и 17, дакле $a^{560} \equiv 1 \pmod{561}$. △

Напомена. Бројеви n са овим својством се зову *Кармајклови бројеви.* Једини Кармајклов број мањи од 1000 је $n = 561$.

Приметимо да из решења претходног задатка следи да је $a^{80} \equiv 1 \pmod{561}$, што је јаче од тврђења Ојлерове теореме по коме је $a^{320} \equiv 1 \pmod{561}$ (јер је $\varphi(561) = 2\dot{1}0 \cdot 16 = 320$). Ово нам сугерише да експонент $\varphi(n)$ у Ојлеровој теореми може у општем случају да се побољша.

Дефиниција. Кармајклова функција $\lambda(n)$ се дефинише за $n > 1$ формулама $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^k) = 2^{k-2}$ за $k \geq 3$, $\lambda(p^k) = p^{k-1}(p-1)$ за непаран прост број p и $k \geq 1$, и

$$\lambda(n) = [\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})] \quad \text{за} \quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Очигледно, $\lambda(n)$ дели $\varphi(n)$. На пример, $\lambda(56) = [\lambda(7), \lambda(8)] = [6, 2] = 6$ дели $\varphi(56) = 24$.

Т.3 *(Кармајклова теорема).* Ако је n природан и a цео број такав да је $(a, n) = 1$, важи $a^{\lambda(n)} \equiv 1 \pmod{n}$.

Доказ. Довољно је доказати да важи $a^{\lambda(p^k)} \equiv 1 \pmod{p^k}$ за сваки прост број p и $k \geq 0$. Пошто $\lambda(p^k) \mid \lambda(n)$ кад год $p^k \mid n$, степеновањем са $\lambda(n)/\varphi(p^k)$ ће следити да $p^k \mid a^{\lambda(n)} - 1$, и одатле $n \mid a^{\lambda(n)} - 1$.

Ако је p непарно, $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$ важи по Ојлеровој теореми. У случају $p = 2$ и $k \geq 3$ је $a^{\lambda(2^k)} - 1 = a^{2^{k-2}} - 1 = (a^2 - 1) \prod_{i=1}^{k-3} (a^{2^i} + 1)$, при чему $2^3 \mid a^2 - 1$ и сви остали чиниоци су парни, одакле следи тврђење. □

Ако је n прост број, Кармајклова теорема не даје побољшање Фермаове јер је тада $\lambda(n) = n - 1$. Међутим, у општем случају побољшање је често значајно. Касније ћемо показати да је Т.3 оптимална, у смислу да се експонент $\lambda(n)$ не може побољшати.

Пример. По Кармајкловој теореми је $a^{60} \equiv 1 \pmod{N}$ за $(a, N) = 1$, где је $N = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$, јер је $\lambda(N) = 60$. Поређења ради, $\varphi(N) = 2^{13} \cdot 3^5 \cdot 5^4 = 1.244.160.000$.

2° Поредак по модулу

Три теореме у претходној глави важе за све a. У циљу испитивања понашања степена датог броја a по датом модулу n, уводимо појам поретка по модулу.

Дефиниција. Поредак броја a по модулу n ($a \in \mathbb{Z}$, $n \in \mathbb{N}$) је најмањи природан број $\delta = \delta(a, n)$ такав да је $a^\delta \equiv 1 \pmod{n}$.

На пример, $\delta(3, 11) = 5$ јер је $3^5 \equiv 1$ и $3^i \not\equiv 1 \pmod{11}$ за $1 \leq i \leq 4$.

Низ $1, a, a^2, \ldots$ је периодичан по модулу n са периодом $\delta = \delta(a, n)$ - заиста, $a^{k+\delta} = a^k a^\delta \equiv a^k \cdot 1 = a^k \pmod{n}$. Осим тога, $1, a, a^2, \ldots, a^{\delta-1}$ су међусобно различити по модулу n. То значи да, ако је $a^m \equiv 1 \pmod{n}$, онда $\delta \mid m$; другим речима:

Т.4. Поредак $\delta(a, n)$ броја a по модулу n дели број $\varphi(n)$. Низ $1, a, a^2, \ldots$ је периодичан по модулу n са минималним периодом $\delta(a, n)$. □

Задатак 2. Ако је $p > 2$ прост број и $a \in \mathbb{Z}$, доказати да сваки прост делилац q броја $\frac{a^p - 1}{a - 1} = a^{p-1} + a^{p-2} + \cdots + 1$ задовољава $p \mid q - 1$ или $p = q$.

Решење. Ако $q \mid a - 1$, онда $q \mid a^{p-1} + a^{p-2} + \cdots + 1 \equiv 1 + 1 + \cdots + 1 = p \pmod{q}$, дакле $q = p$. С друге стране, ако $q \nmid a - 1$, поредак броја a по модулу q дели p, дакле једнак је p. Како тај поредак дели $q - 1$, следи $p \mid q - 1$. △

Следеће једноставно помоћно тврђење је веома важно.

Т.5. За произвољне бројеве $a \in \mathbb{Z}$, $m, n \in \mathbb{N}$, важи $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Доказ. Означимо $d = (a^m - 1, a^n - 1)$. Како $a^{(m,n)} - 1$ дели бројеве $a^m - 1$ и $a^n - 1$ (нпр. ако је $m = k(m,n)$, онда је $a^m - 1 = (a^{(m,n)} - 1)(a^{(k-1)(m,n)} + \cdots + a^{(m,n)} + 1)$), број d је дељив са $a^{(m,n)} - 1$. С друге стране, познато је да постоје природни бројеви x, y такви да је $(m,n) = mx - ny$, одакле следи $1 \equiv a^{mx} \equiv a^{ny} \cdot a^{(m,n)} \equiv a^{(m,n)} \pmod{d}$, дакле d дели $a^{(m,n)} - 1$, што повлачи $d = a^{(m,n)} - 1$. □

Последица. За $a, b \in \mathbb{Z}$, $(a,b) = 1$, и $m, n \in \mathbb{N}$ важи $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$.

Доказ. Означимо $d = (a^m - b^m, a^n - b^n)$. Очигледно $a^{(m,n)} - b^{(m,n)} \mid d$. С друге стране, ако је $c \in \mathbb{Z}$ такво да је $bc \equiv 1 \pmod{d}$, онда d дели $(ac)^m - 1$ и $(ac)^n - 1$, дакле $d \mid (ac)^{(m,n)} - 1$, што множењем са $b^{(m,n)}$ даје $d \mid a^{(m,n)} - b^{(m,n)}$. □

На почетку смо видели да је $2^n - 1$ дељиво са 7 за $3 \mid n$, тј. $\delta(2,7) = 3$. Може нас занимати и за које n је $2^n - 1$ дељиво неким већим степеном седмице.

Задатак 3. Наћи све $n \in \mathbb{N}$ за које је $2^n - 1$ дељиво са 49.

Решење. Јасно је да је такво n дељиво са 3. Напишимо $n = 3m$. Тада је $2^n = 8^m = (1+7)^m$, што се по биномној формули развија као $1 + \binom{m}{1}7 + \binom{m}{2}7^2 + \binom{m}{3}7^3 + \cdots + \binom{m}{m}7^m$. Сви сабирци осим прва два су дељиви са 7^2. Према томе, $2^n \equiv 1 + 7m \pmod{7^2}$. Закључујемо да је $2^n \equiv 1 \pmod{7^2}$ ако и само ако је m дељиво са 7, тј. ако и само ако $21 \mid n$.

Другим речима, $\delta(2,49) = 21$. △

Аналоган начин размишљања може да се примени у општем случају, што нам омогућава да држимо под контролом степен простог броја p у канонском развоју $a^n - 1$.

Следећу ознаку ћемо редовно користити. За прост број p, $k \in \mathbb{N}$ и $m \in \mathbb{Z}$, пишемо $p^k \parallel m$ и говорићемо "p^k тачно дели m" ако је p^k највећи степен p који дели m, тј. $p^k \mid m$ и $p^{k+1} \nmid m$.

Т.6. Нека је $p > 2$ прост број, $a \neq 1$ цео и $n \in \mathbb{N}$. Ако $p^k \parallel a - 1$ и $p^l \parallel n$, онда $p^{k+l} \parallel a^n - 1$.

Доказ. Имамо $a = p^k B + 1$ за неко цело B које није дељиво са p. Тада је по биномној формули

$$a^n - 1 = (1 + p^k B)^n - 1 = np^k B + \binom{n}{2} p^{2k} B^2 + \cdots + p^{nk} B^n. \qquad (*)$$

Тврђење показујемо индукцијом по l. За $l = 0$ и $l = 1$, очигледно су сви сабирци на десној страни $(*)$ осим првог дељиви са p^{k+l+1}, док је први тачно дељив са p^{k+l}, одакле следи $p^{k+l} \parallel a^n - 1$.

Нека је $l = t > 1$. На основу случаја $l = 1$ важи $p^{k+1} \parallel a^p - 1$. Пошто $p^{t-1} \parallel N = n/p$, по индуктивној претпоставци за $l = t - 1$ примењеној на $A = a^p$ и N имамо $p^{(k+1)+(t-1)} \parallel A^N - 1$, тј. $p^t \delta \mid n$. □

Последица 1. Ако је $\delta = \delta(p,a)$ и $p^k \parallel a^\delta - 1$, онда је $\delta(p^{k+l}, a) = p^l \delta$.

Доказ. Следи из теореме 6 примењене на a^δ. □

Задатак 4. Доказати да је, за свако $n \in \mathbb{N}$, број $2^{3^n} + 1$ дељив са 3^{n+1}, а није са 3^{n+2}.

Решење. Како $3^1 \parallel (-2) - 1$ и $3^n \parallel 3^n$, теорема 6 даје $3^{n+1} \parallel (-2)^{3^n} - 1 = -(2^{3^n} + 1)$. △

За сваки цео број b, $p \nmid b$, постоји цео број c такав да је $bc \equiv 1 \pmod{p^{k+l}}$. Заменимо у теореми 6 број a са ac. Услови $p^k \parallel ac - 1$ и $p^{k+l} \parallel (ac)^n - 1$ су еквивалентни са $p^k \parallel a - b$ и $p^{k+l} \parallel a^n - b^n$ (множењем са b, односно b^n). Тако добијамо:

Последица 2. Ако $p^k \parallel a - b$ и $p^l \parallel n$ за непарно просто p, онда $p^{k+l} \parallel a^n - b^n$. □

За $p = 2$ теорема 6 није тачна: на пример, $2 \parallel 3 - 1$, али $2^3 \mid 3^2 - 1$. Наиме, у овом случају немамо безусловну гаранцију да p^{k+l+1} дели други сабирак у $(*)$ - ако је $k = 1$, онда $p^{l-1} \parallel \binom{m}{2}$ и одатле $p^{k+l} \parallel \binom{m}{2} p^{2k} B^2$. Зато Т.6 за $p = 2$ важи у мало измењеном облику, уз практично исти доказ.

Т.7. Нека је a ($|a| > 1$) непаран број и нека $2^k \parallel a^2 - 1$. Тада за свако цело $l \geq 0$, $2^{k+l} \mid a^n - 1$ ако и само ако $2^{l+1} \mid n$. □

3° Примитивни корени

Знамо да поредак $\delta(a, n)$ дели $\varphi(n)$. Може ли се за дато n одабрати a тако да је $\delta(a, n)$ тачно једнако $\varphi(n)$?

Дефиниција. Цео број a је *примитивни корен* по модулу природног броја n са $(a, n) = 1$ ако је $\delta(a, n) = \varphi(n)$.

Значај примитивног корена a по модулу n се, између осталог, огледа у томе што се у низу $1, a, a^2, \ldots, a^{\varphi(n)-1}$ појављују *сви* могући остаци по модулу n који су узајамно прости са n - тј. овај низ је сведени систем остатака $\pmod n$.

Видели смо на почетку да је $a = 3$ примитиван корен за $n = 7$. Провером налазимо да се такво a може наћи за $n = 2, 3, 5, 7, 11, 13, 17, \ldots$ - на пример, $a = 1, 2, 2, 3, 2, 2, 3, \ldots$ редом. Испоставља се да примитиван корен постоји по сваком простом модулу. Да бисмо ово показали, подсетићемо се једног основног тврђења о полиномима:

- Полином степена d са коефицијентима у пољу $\mathbb{F}$ има највише d нула у $\mathbb{F}$.

На пример, $\mathbb{F}$ може да буде поље реалних или комплексних бројева. Међутим, нас овде занима $\mathbb{Z}_p$ - поље остатака по модулу простог броја p. У том пољу, тврђење ($\bullet$) нам заправо каже ово:

- Нека је $P(x)$ полином степена d са целим коефицијентима. Тада једначина $P(x) \equiv 0 \pmod p$ има највише d решења по модулу p.

Доказ не наводимо, јер је исти као и доказ којег се сећамо - да реалан или комплексан полином степена d има највише d нула. Читаоцу саветујемо да испише детаље.

Лема.1. Ако $d \mid p - 1$, број решења конгруенције $x^d \equiv 1 \pmod p$ је једнак d.

Доказ. Полином $x^d - 1$ има највише d нула по модулу p. С друге стране, полином $\frac{x^{p-1}-1}{x^d-1}$ је степена $p - 1 - d$, па има највише $n - d$ нула по модулу p. Како полином $x^{p-1} - 1$ има тачно $p - 1$ нула $\pmod p$, следи тврђење. □

Лема.2. За свако $n \in \mathbb{N}$ важи $\sum_{d|n} \varphi(d) = n$.

Доказ. Тврдимо да је, за свако d ($d \mid n$), број елемената $x \in \{1, 2, \ldots, n\}$ за које је $(x, n) = \frac{n}{d}$ једнак $\varphi(d)$. Заиста, $(x, n) = \frac{n}{d}$ је еквивалентно са $x = \frac{n}{d} \cdot k$, где је k ($1 \leq k \leq d$) цео и $(k, d) = 1$, а оваквих бројева k има тачно $\varphi(d)$.

Следи да је сума $\varphi(d)$ по свим $d \mid n$ једнака броју свих елеманата $x \in \{1, 2, \ldots, n\}$, а то је n. □

Т.8. За сваки прост број p постоји примитиван корен по модулу p.

Доказ. Показујемо индукцијом по делиоцима d броја $p - 1$ да постоји тачно $\varphi(d)$ елемената $\mathbb{Z}_p$ поретка d. Ово је тривијално за $d = 1$. Претпоставимо да је тачно за све делиоце броја $p - 1$ мање од d. На основу леме 1 постоји тачно d елеманата $\mathbb{Z}_p$ чији поредак дели d. По индукцијској претпоставци, међу тих d елемената, тачно $\varphi(e)$ има поредак e, где је e ма који делилац d мањи од d. Преосталих $d - \sum_{d>e|d} \varphi(e)$ елемената имају поредак d, а по леми 2 је $d - \sum_{d>e|d} \varphi(e) = \varphi(d)$, што завршава индукцију.

Специјално, има тачно $\varphi(p - 1)$ елемената поретка $p - 1$, тј. примитивних корена. □

Последица. Ако је $a^n - 1$ дељиво простим бројем p за свако a, $(a, p) = 1$, онда је n дељиво са $p - 1$.

Доказ. Довољно је убацити $a = g$, где је g примитивни корен по модулу p. □

Задатак 5. Доказати да се бројеви $1, 2, \ldots, 100$ могу распоредити у поља таблице 10×10 тако да су у сваком квадрату 2×2 производи по два броја по дијагонали једнаки по модулу 101.

Решење. Нека је g примитивни корен по модулу 101. Упишимо у поље i-те врсте и j-те колоне ($i, j \in \{0, 1, \ldots, 9\}$) остатак g^{10i+j} при дељењу са 101. У сваком квадрату одређеном врстама $i, i+1$ и колонама $j, j+1$, производ бројева по свакој дијагонали је $g^{10(2i+1)+(2j+1)} \pmod{101}$. △

Постојање примитивног корена g по простом модулу p значи да је мултипликативна група $\mathbb{Z}_p^*$ циклична, генерисана елементом g. То је и разлог што примитивни корен често означавамо словом g.

Примећујемо да, осим по простим модулима, примитивни корен постоји и за модуле $n = 4, 6, 9, 10$ који нису прости - нпр. $g = 3, 5, 2, 3$ редом.

Т.9. Ако је p непаран прост број и $n \in \mathbb{N}$, постоји примитиван корен по модулима p^n и $2p^n$.

Доказ. Нека је g примитивни корен по модулу p. Покажимо прво да постоји примитивни корен по модулу p^2.

Тврдимо да је бар један од бројева g, $g + p$ примитивни корен по модулу p^2 - тј. да има поредак $\varphi(p^2) = p(p-1)$ по модулу p^2. Поретци ових бројева по модулу p су једнаки $p - 1$, па су њихови поретци по модулу p^2 дељиви са $p - 1$ - дакле, једнаки су $p - 1$ или $p(p-1)$. Ако ни g ни $g + p$ нису примитивни корени по модулу p^2, имамо $g^{p-1} \equiv (g+p)^{p-1} \equiv 1 \pmod{p^2}$. Међутим, биномни развој нам даје $(g+p)^{p-1} - g^{p-1} \equiv (p-1)pg^{p-2} \not\equiv 0 \pmod{p^2}$, контрадикција.

Нека је сада g примитивни корен по модулу p^2. Покажимо да је он такође примитивни корен по модулу p^n. Како p тачно дели $g^{p-1} - 1$, по теореми 6 имамо да је $g^m - 1$ дељиво са p^n ако и само ако је m дељиво са $p^{n-1}(p-1)$, тј. поредак g по модулу p^n је једнак $\varphi(p^n)$, што смо и тврдили.

Најзад, како је $\varphi(2p^n) = \varphi(p^n)$, сваки непаран примитиван корен по модулу p^n је уједно и примитиван корен по модулу $2p^n$. Дакле, g или $g + p^n$ задовољава услове. □

С друге стране, за неке модуле попут $n = 8, 12, 15$ не постоји примитивни корен, јер по Кармајкловој теореми ниједан број нема ред већи од $2, 2, 4$ редом по датим модулима.

Ако постоји број a чији је поредак по модулу n једнак $\varphi(n)$, из Кармајклове теореме следи да мора бити $\lambda(n) = \varphi(n)$. То одмах искључује степене двојке веће од 2^2. Шта више, искључује и све бројеве n који су једнаки производу два узајамно проста броја n_1, n_2 већа од 2, јер су $\lambda(n_1)$ и $\lambda(n_2)$ парни по дефиницији, па је $\lambda(n) = [\lambda(n_1), \lambda(n_2)] \leq \frac{1}{2}\lambda(n_1)\lambda(n_2) \leq \frac{1}{2}\varphi(n_1)\varphi(n_2) = \frac{1}{2}\varphi(n) < \varphi(n)$. Тако добијамо:

Т.10. Примитиван корен по модулу n ($n \in \mathbb{N}$) постоји ако и само ако је $n = p^n$ или $2p^n$ за неки непаран прост број p, или $n \in \{2, 4\}$.

Доказ. Свако $n \in \mathbb{N}$ које није у неком од наведених облика је или степен двојке већи од 4, или производ два узајамно проста броја већа од 2, па тврђење следи из претходног разматрања. □

Сада можемо да покажемо и аналогон последице теореме 9 за сложене модуле, који смо најавили после Кармајклове теореме.

Т.11. Ако је $a^m - 1$ дељиво природним бројем n за сваки цео број a, $(a, n) = 1$, онда је експонент m дељив са $\lambda(n)$ (где је λ Кармајклова функција).

Доказ. Нека је $n = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, где су p_i различити непарни прости бројеви и $\alpha_i > 0$. По теореми 10, за свако i постоји g_i чији је поредак по модулу $p_i^{\alpha_i}$ једнак $\varphi(p_i^{\alpha_i})$.

Примитивни корен по модулу 2^α не постоји за $\alpha > 3$; уместо тога, важи да је поредак нпр. броја 5 по модулу 2^α једнак $2^{\alpha-2}$ - ово следи директно из Т.7.

По Кинеској теореми о остацима постоји a такво да је $a \equiv 5 \pmod{2^\alpha}$ и, за све i, $a \equiv g_i \pmod{p_i^{\alpha_i}}$. Тада је $a^m - 1$ дељиво са n ако и само ако је дељиво са 2^α и са $p_i^{\alpha_i}$ за све i, а то важи ако и само ако је m дељиво са $\lambda(2^\alpha)$ и $\lambda(p_i^{\alpha_i})$, што је еквивалентно са $\lambda(n) \mid m$. □

4° Задаци

1. Решити једначину $3^x - 2^y = 1$ у скупу природних бројева.

   Решење. За $y = 1$ једино решење је $(x, y) = (1, 1)$. Нека је $y > 1$. Тада $4 \mid 2^y = 3^x - 1$, одакле следи $2 \mid x$. Сада је $2^y = (3^{x/2} - 1)(3^{x/2} + 1)$, па су и $3^{x/2} - 1$ и $3^{x/2} + 1$ степени двојке. Једини степени двојке чија је разлика 2 су 2 и 4, па је $3^{x/2} = 3$ и најзад $(x, y) = (2, 3)$.

2. Постоји ли n за које $247 \mid 2^n + 1$?

   Решење. Број 247 се растављa на просте чиниоце као $13 \cdot 19$. Ако $13 \mid 2^n + 1$, онда је $n \equiv 6 \pmod{12}$, дакле n мора да буде паран. С друге стране, ако $19 \mid 2^n + 1$, онда је $n \equiv 9 \pmod{19}$, дакле n је непаран, контрадикција.

3. Нека су x и y цели бројеви. Ако $9 \mid x^2 + xy + y^2$, доказати да $3 \mid x, y$.

   Решење. По услову, $3 \mid (x-y)(x^2+xy+y^2) = x^3-y^3$. Како је $x^3-y^3 \equiv x-y \pmod 3$, следи да је $x - y = 3z$ за неки цео број z. Али тада је $x^2+xy+y^2 = \frac{x^3-y^3}{x-y} = (y+3z)^3 - y^3 3z = 3(y^2 + 3yz + 3z^2)$. Ако је то дељиво са 9, онда $3 \mid y$.

4. Нека су x, y цели и $p > 2$ прост број. Ако $p^2 \mid \frac{x^p-y^p}{x-y}$, доказати да $p \mid x, y$.

   Решење. Како $p \mid x^p-y^p \equiv x-y \pmod p$, можемо да пишемо $x-y = pz$ за неки цео број z. Биномна формула даје $\frac{x^p-y^p}{x-y} = \frac{(y+pz)^p-y^p}{pz} = py^{p-1}+p\binom{p}{2}y^{p-2}z+p^2\binom{p}{3}y^{p-3}z^2+\cdots+p^{p-1}z^p$. У овом изразу сви сабирци почев од другог су дељиви са p^2, па и први мора да буде дељив са p^2, одакле $p \mid y$.

5. Наћи све природне бројеве x, y, n и прост број p ($p \nmid xy$) такве да је $x^p + y^p = p^n$.

   Решење. За $p = 2$ једначина постаје $x^2 + y^2 = 2^n$. Пошто $4 \nmid x^2 + y^2$, могуће је једино $x = y = n = 1$.

   Нека је $p > 2$. Имамо $x^{p-1} - x^{p-2}y + \cdots + y^{p-1} = \frac{x^p+y^p}{x+y} = p^s$ за неко s. Из претходног задатка за x и $-y$ следи $s \leq 1$, тј. $A = x^{p-1} - x^{p-2}y + \cdots + y^{p-1} \leq p$. Међутим, ако је $x \geq y$, онда је $A \geq y^{p-1}$, па је $y^{p-1} \leq p$. Како је $2^{p-1} \geq p$, мора бити $y = 1$. Такође, због $x \geq 2$ је $A = x^{p-1} - x^{p-2} + \cdots + 1 > (x-1)x^{p-2}$, па је $x^{p-2} \leq p$, што је могуће једино за $x = 2$ и $p = 3$. Овако добијамо решење $(x, y, p, n) = (2, 1, 3, 2)$.

6. Доказати да полином $x^{p-1} - 1 - (x-1)(x-2)\cdots(x-p+1)$ има све коефицијенте дељиве са p.

   Решење. У пољу $\mathbb{Z}_p$, нуле полинома $x^{p-1} - 1$ су $1, 2, \ldots, p-1$, па је тај полином једнак $(x-1)(x-2)\cdots(x-p+1)$ по модулу p.

   Напомена. Упоређивање слободних чланова на левој и десној страни нам даје алтернативни доказ Вилсонове теореме: $(p-1)! \equiv -1 \pmod p$.

7. Наћи све парове (p, q) простих бројева таквих да је за свако a које задовољава $(a, 3pq) = 1$ број $a^{3pq} - a$ дељив са $3pq$.

   Решење. Бројеви p и q су очигледно непарни; приметимо да су већи и од 3, јер би у супротном важило $9 \mid 2^{3pq-1} - 1$, одакле $6 \mid 3pq - 1$ што је немогуће. По последици Т.9, из услова задатка следи да је $3pq - 1$ дељиво са $p - 1$ и $q - 1$, што даје $p - 1 \mid 3pq - 1 - 3q(p-1) = 3q - 1$ и аналогно $q - 1 \mid 3p - 1$. Нека је, без смањења општости,

$p \geq q$. Тада је $3q-1 < 4(p-1)$ и $3 \nmid 3q-1$, одакле је $3q-1 = p-1$ или $3q-1 = 2(p-1)$. Први случај је немогућ јер $p \neq 3q$. Остаје други случај, тј. $2p = 3q+1$. Како $q-1 \mid 2(3p-1) = 6p-2 = 9q+1$, имамо $q-1 \mid 9q+1-9(q-1) = 10$. Једина могућност је $q = 11$ и одатле $p = 17$.

8. Наћи све парове простих бројева p, q за које $pq \mid (5^p - 2^p)(5^q - 2^q)$.

   Решење. Јасно је да су p и q непарни. Приметимо да ако $p \mid 5^p - 2^p \equiv 3 \pmod{p}$, онда је $p = 3$. Претпоставимо да је $p = 3$ (аналогно за $q = 3$). Тада $3q \mid (5^3 - 2^3)(5^q - 2^q) = 3^2 \cdot 13(5^q - 2^q)$, одакле је $q = 3$ или $q = 13$.

   Претпоставимо сада да је $p > q > 3$. Тада $p \mid 5^q - 2^q$ и $q \mid 5^p - 2^p$. Како $q \mid 5^{q-1} - 2^{q-1}$, важи $5^n \equiv 2^n \pmod{q}$ за све n дељиве са $q-1$ или са p. При том су $q-1$ и p узајамно прости, па постоје $x, y \in \mathbb{N}$ за које је $px = (q-1)y + 1$. Тада је $5 \cdot 2^{(q-1)y} \equiv 5 \cdot 5^{(q-1)y} = 5^{px} \equiv 2^{px} = 2 \cdot 2^{(q-1)y} \pmod{q}$, одакле $q \mid 3 \cdot 2^{(q-1)y}$, што је контрадикција.

9. Ако су m, n природни бројеви и $2^m - 1$ је дељиво са $(2^n - 1)^2$, доказати да је m дељиво са $n(2^n - 1)$.

   Решење. Из $2^n - 1 \mid 2^m - 1$ следи $n \mid m$. Нека је $m = kn$. Тада је $\frac{2^m-1}{2^n-1} = 2^{(k-1)n} + 2^{(k-2)n} + \cdots + 2^n + 1 \equiv 1 + 1 + \cdots + 1 = k \pmod{2^n - 1}$, а то је дељиво са $2^n - 1$ ако и само ако $2^n - 1 \mid k$, одакле следи тврђење.

10. Доказати да за свако природно $m > 1$ постоји природан број n такав да је $n^2 + 7$ дељиво са 2^m.

    Решење. Користимо индукцију по m. За $m \leq 3$ довољно је узети $n = 1$. Претпоставимо да тврђење важи за $m-1$ ($m \geq 4$), тј. да $2^{m-1} \mid n^2 + 7$ за неко n. Ако је $n^2 + 7$ дељив и са 2^m, индукцијски корак је готов. У супротном је $n^2 + 7 \equiv 2^{m-1} \pmod{2^m}$, а тада је $(n + 2^{m-2})^2 + 7 = n^2 + 7 + 2^{m-1}n + 2^{2m-4} \equiv 2^{m-1} + 2^{m-1} \equiv 0 \pmod{2^m}$, па је и у овом случају индукцијски корак завршен.

11. Доказати да за свако $m \in \mathbb{N}$, $m > 1$ постоји $n \in \mathbb{N}$ такав да је $2^n + 2003$ дељиво са 3^m.

    Решење. Означимо тражено n са n_m. За $m \leq 2$ довољно је узети $n_m = 2$. Претпоставимо да за неко $m \geq 3$ постоји $n = n_{m-1}$ такво да је $2^n \equiv -2003 \pmod{3^{m-1}}$. Показаћемо да се тада може узети n_m из скупа $\{n + 2j \cdot 3^{m-2} \mid j = 0, 1, 2\}$ тако да је $2^{n_m} \equiv -2003 \pmod{3^m}$.

    Приметимо да је, по Т.6, $2^{2j \cdot 3^{m-2}} - 1$ ($j \in \{1, 2\}$) дељиво са 3^{m-1}, а није са 3^m. Следи да су бројеви 2^n, $2^{n+2 \cdot 3^{m-2}}$ и $2^{n+4 \cdot 3^{m-2}}$ конгруентни са -2003 по модулу 3^{m-1}, али никоја два нису конгруентна по модулу 3^m. То значи да је један од њих је конгруентан са $-2003 \pmod{3^m}$, што смо и желели.

12. Ако је a цео број и $p \neq 3$ прост делилац $a^2 + 3a + 3$, доказати да је $p \equiv 1 \pmod{6}$.

    Решење. Како је $a^2 + 3a + 3 = \frac{(a+1)^3 - 1}{(a+1) - 1}$, број p дели $(a+1)^3 - 1$, тј. поредак $a+1$ по модулу p дели 3. Тај поредак није 1 јер $p \nmid (a+1) - 1 = a$, па следи $\delta(a+1, p) = 3$. Пошто поредак по модулу p дели $\varphi(p) = p - 1$, следи $3 \mid p - 1$ и, самим тим, $6 \mid p - 1$.

    Напомена. Други доказ произилази из основних тврђења о квадратним остацима. Наиме, ако $p \mid a^2 + 3a + 3$, онда је $(2a+3)^2 \equiv 3 \pmod{p}$, дакле -3 је квадратни остатак по модулу p. По Гаусовом закону реципроцитета је $1 = \left(\frac{-3}{p}\right) = \left(\frac{p}{-3}\right) = \left(\frac{p}{3}\right)$, одакле је $p \equiv 1 \pmod{3}$.

13. Нека је n природан број и $F = 2^{2^n} + 1$. Доказати да је број F прост ако и само ако је $3^{\frac{F-1}{2}} \equiv -1 \pmod{F}$.

    Решење. Претпоставимо да је $3^{\frac{F-1}{2}} \equiv -1 \pmod{F}$. Нека је p неки прост делилац F. Како $p \mid 3^{F-1} - 1$, поредак броја 3 по модулу p дели $F - 1 = 2^{2^n}$, дакле $\delta(3, p) = 2^k$ за неко k. Ако је $k < 2^n$, онда $2^k \mid 2^{2^n - 1} = \frac{F-1}{2}$ и према томе $3^{\frac{F-1}{2}} \equiv 1 \pmod{p}$ што није

тачно. Следи да је $k = 2^n$, тј. $\delta(3,p) = 2^{2^n}$, одакле $2^{2^n} \mid p-1$. То је могуће једино ако је $p = F$, тј. F је прост.

Претпоставимо сада да је F прост. По Ојлеровом критеријуму је $3^{\frac{F-1}{2}} \equiv \left(\frac{3}{F}\right) \pmod F$. По Гаусовом закону реципроцитета је $\left(\frac{3}{F}\right) = \left(\frac{F}{3}\right) = \left(\frac{2}{3}\right) = -1$ јер је $F \equiv 2 \pmod 3$, па тврђење следи.

14. (а) Доказати да је сваки непаран делилац p броја a^2+1 (где $a \in \mathbb{Z}$) облика $p = 4k+1$.

    (б) Слично, за $t \in \mathbb{N}$ доказати да је сваки непаран делилац p броја $a^{2^t}+1$ облика $p = 2^{t+1}k+1$.

    Решење. Нека $p \mid a^{2^t}+1$. Тада p дели $a^{2^{t+1}}-1$ и a^{p-1}, па по Т.3 имамо $p \mid a^{(p-1,2^{t+1})}-1 = a^{2^s}-1$, где је $2^s = (p-1, 2^{t+1})$. Ако је $s \le t$, из $a^{2^s} \equiv 1 \pmod p$ следи $a^{2^t} \equiv 1 \pmod p$, контрадикција. Према томе, $s = t+1$, тј. $2^{t+1} \mid p-1$.

15. Нека $\Phi_n(x)$ означава n-ти циклотомични полином[1]. Доказати да ако прост број p дели $\Phi_n(a)$ за неко $a \in \mathbb{Z}$, онда $p \mid n$ или $p \equiv 1 \pmod n$.

    Решење. Важи $\prod_{d\mid n} \Phi_d(x) = x^n - 1$. Показаћемо да је поредак a по модулу p једнак n, одакле ће следити $n \mid p-1$.

    Претпоставимо да је поредак a по модулу p једнак d, где је $d < n$ и $d \mid n$. Тада је a нула полинома $x^d - 1$ и $\Phi_n(x)$ над $\mathbb{Z}_p$, и при том $\Phi_n(x) \mid \frac{x^n-1}{x^d-1}$, па је a двострука нула полинома $x^n - 1$ над $\mathbb{Z}_p$. Одавде следи да је a такође нула полинома $(x^n-1)' = nx^{n-1}$ по модулу p, што је једино могуће ако је $n \equiv 0 \pmod p$, тј. $p \mid n$.

16. (Специјалан случај *Дирихлеове теореме.*) За дати природан број n, доказати да постоји бесконачно много простих бројева q облика $q = nx+1$.

    Решење. Претпоставимо да су $p_1, p_2, \ldots, p_k$ сви такви прости бројеви и посматрајмо број $N = \Phi_n(np_1p_2\cdots p_k)$. По претходном задатку, сви прости делиоци броја N су конгруентни са 1 по модулу n или деле n. Међутим, N је узајамно просто са n и није дељиво ниједним од бројева p_i, па је то немогуће.

17. Ако је a остатак n-тог степена по сваком модулу, доказати да је a n-ти степен.

    Решење. По услову, a је остатак n-тог степена по модулу a^2. Ако је p ма који прост делилац a и $p^k \parallel a$, из $x^n \equiv a \pmod{a^2}$ следи $p^k \parallel x^n$, дакле $n \mid k$. То важи за свако p, па је a n-ти степен.

18. Решити у скупу природних бројева једначину $7^a = 3 \cdot 2^b + 1$.

    Решење. За $b \le 4$ налазимо решења $(a,b) \in \{(1,1),(2,4)\}$. Нека је $b > 4$. Из једначине следи $2^b \mid 7^a - 1$. Како $2^4 \parallel 7^2 - 1$, Т.7 нам даје $2^{b-3} \mid a$, значи $a \ge 2^{b-3}$. Међутим, лако се види да је $7^a - 1 \ge 7^{2^{b-3}} - 1 > 3 \cdot 2^b$ за $b > 4$, па у овом случају нема решења.

19. Решити у скупу природних бројева једначину $2^m - 5^n = 7$.

    Решење. За $m \le 5$ једино решење је $(m,n) = (5,2)$.

    Претпоставимо да је $m \ge 6$. Тада $2^6 \mid 5^n + 7$, а праволинијска провера показује да то важи само за $n \equiv 10 \pmod{16}$. Како је $5^n + 7 \equiv 5^{10} + 7 \equiv -1 \pmod{17}$, следи да је $2^m \equiv -1 \pmod{17}$, а то је могуће само када $4 \mid m$. Међутим, тада је $5^n + 7 = 2^m \equiv 1 \pmod 5$, што је контрадикција.

20. Одредити све природне бројеве x за које је $1 + 2^x + 2^{2x+1}$ потпун квадрат.

    Решење. Нека је $1 + 2^x + 2^{2x+1} = y^2$. Из $2^x \mid y^2 - 1$ следи да 2^{x-1} дели $y-1$ или $y+1$, тј. $y = 2^{x-1}z \pm 1$. С друге стране, очигледно је $2^x + 1 < y < 2^{x+1} - 1$ за $x \ge 2$, па је $z = 3$. Сада лако налазимо да је $x = 4$ једино решење: $1 + 2^4 + 2^9 = 23^2$.

[1] n-ти циклотомични полином је полином чије су нуле n-ти примитивни корени јединице, тј. $\Phi_n(x) = \prod(x - \epsilon^k)$, где је $\epsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, а производ је по природним бројевима k ($k \le n$) узајамно простим са n.

21. Наћи највећи степен броја 1001 који дели $Z = 1000^{1001^{1002}} + 1002^{1001^{1000}}$.

Решење. Приметимо да је $1001 = 7 \cdot 11 \cdot 13$. Одредићемо највећи степен броја 7 који дели Z. Како $7 \parallel 1002-1$ и $7^{1000} \parallel 1001^{1000}$, теорема 6 нам даје $7^{1001} \parallel X = 1002^{1001^{1000}} - 1$. Такође, $7 \parallel (-1000) - 1$ и $7^{1002} \parallel 1001^{1002}$, па по Т.6 имамо $7^{1003} \parallel Y = (-1000)^{1001^{1002}} - 1$. Следи да $7^{1001} \parallel X - Y = Z$. Аналогно, $11^{1001}, 13^{1001} \parallel Z$, па закључујемо да је Z дељиво са 1001^{1001}, а није са 1001^{1002}.

22. Ако је $n \in \mathbb{N}$ непарно, доказати да је $n(n-1)^{(n-1)^n+1} + n$ дељиво са $((n-1)^n + 1)^2$.

Решење. Означимо $(n-1)^n + 1 = nA$, где је $A \in \mathbb{Z}$. Имамо $n(n-1)^{(n-1)^n+1} + n = n((nA-1)^A + 1) = n \cdot nA\left((nA-1)^{A-1} - (nA-1)^{A-2} + \cdots - (nA-1) + 1\right) = n^2 A \cdot B$. При том је $B \equiv (-1)^{A-1} - (-1)^{A-2} + \cdots + 1 = A \pmod{A}$, тј. $A \mid B$, одакле следи тврђење.

23. Дефинишимо $T_1 = 2$ и $T_k = 2^{T_{k-1}}$. Дат је природан број n. Доказати да је низ $T_1, T_2, \ldots$ константан по модулу n почев од неке тачке.

Решење. Тврђење показујемо индукцијом по n. За $n = 1$ је тривијално. Претпоставимо да је низ (T_i) константан по свим модулима $1, 2, \ldots, n-1$ почев од неке тачке. Између осталог, то важи и за модул $\varphi(n)$. Како из $T_i \equiv T_{i+1} \pmod{\varphi(n)}$ следи $T_{i+1} = 2^{T_i} \equiv 2^{T_{i+1}} = T_{i+2} \pmod{n}$ за довољно велико i, следи да је (T_i) такође константно по модулу n почев од неке тачке.

24. Доказати да за сваки природан број n и цео број c постоји природан број x такав да је $2^x - x \equiv c \pmod{n}$.

Решење. Посматрајмо низ A_i дат са $A_0 = 1$ и $A_{k+1} = 2^{A_k} - c$ за $k \geq 0$. На исти начин као у претходном задатку показује се да је низ (A_k) константан по модулу n почев од неке тачке - дакле, $2^{A_k} - c = A_{k+1} \equiv A_k \pmod{n}$ за неко k. Узмимо $x = A_k$.

25. Наћи сва решења једначине $a^m + b^m = (a+b)^n$ у природним бројевима (a, b, m, n).

Решење. Јасно је да је $m > n$. За $a = b$ добијамо да су једина решења $a = b = 2^k$ и $n - 1 = k(m-n)$. Надаље подразумевамо да је $a \neq b$. Нека је $d = (a, b)$, $a = da_1$, $b = db_1$. Једначина постаје $d^{m-n}(a_1^m + b_1^m) = (a_1 + b_1)^n$.

Ако је m парно, онда $a_1 + b_1 \mid a_1^2 - b_1^2 \mid a_1^m - b_1^m$, па је $(a_1^m + b_1^m, a_1 + b_1) = (2a_1^m, a_1 + b_1) \mid 2$ јер је $(a_1, b_1) = 1$. Како $4 \nmid a_1^m + b_1^m \mid (a_1 + b_1)^m$, следи $a_1^m + b_1^m = 2$ што је немогуће.

Претпоставимо сада да је m непарно и посматрајмо неки његов прост делилац q. Број $A = \frac{a_1^q + b_1^q}{a_1 + b_1}$ дели $(a_1 + b_1)^n$. Нека је p прост делилац броја A. Тада $p \mid a_1 + b_1$, тј. $b_1 \equiv -a_1 \pmod{p}$, па имамо $p \mid A = a_1^{q-1} - a_1^{q-2}b_1 + \cdots + b_1^{q-1} \equiv qa_1^{q-1} \pmod{p}$. Следи да $p \mid qa_1^{q-1}$, дакле $p = q$. Према томе, $A = q^r$ за неко $r \in \mathbb{N}$. Међутим, ако $q^t \parallel a_1 + b_1$, онда Т.6 (последица 3 за a_1 и $-b_1$) даје $q^{t+1} \parallel a_1^q + b_1^q$, што значи $q \parallel A$. Следи да је $A = q$. Ако су a_1, b_1 већи од 1, ово је немогуће јер је $a_1^q > qa_1$ и $b_1^q > qb_1$. Зато мора бити $a_1 = 1$ или $b_1 = 1$. Нека је $b_1 = 1$. Тада имамо $a_1^q + 1 = q(a_1 + 1)$. Лако се показује да је лева страна већа од десне за $a_1 > 2$, као и за $a_1 = 2$ и $q > 3$, тако да је једина могућност $a_1 = 2$ и $q = 3$. Следи да је m степен тројке и $d^{m-n}(2^m + 1) = 3^n$, дакле $2^m + 1$ је степен тројке. Међутим, за $9 \mid m$ број $2^m + 1$ је дељив са $2^9 + 1 = 513$, па не може да буде степен тројке. Према томе, мора бити $m = 3$, одакле лако добијамо $d = 1$, па је $(m, n) = (3, 2)$ и $(a, b) = (2, 1)$ или $(1, 2)$.

26. Одредити све бројеве $n \in \mathbb{N}$ за које $n \mid 2^n - 1$.

Решење. Претпоставимо да је $n > 1$ и нека је p његов најмањи прост делилац. Тада из $p \mid 2^{p-1} - 1$ и $p \mid 2^n - 1$ следи $p \mid 2^{(p-1,n)} - 1 = 1$, јер је $(p-1, n) = 1$, што је немогуће. Закључујемо да је $n = 1$ једино решење.

27. Доказати да постоји бесконачно много бројева n за које $n \mid 2^n + 1$.

Решење. Један пример је $n = 3$.

Ако $n \mid m = 2^n + 1$, онда $m = 2^n + 1 \mid 2^m + 1$, дакле и m $(m > n)$ задовољава услов. Овако добијамо бесконачно много примера.

Напомена. У ствари, тврђење задатка следи из задатка 4 у тексту.

28. Доказати да постоји природан број n који има тачно 2000 простих делилаца и за који важи $n \mid 2^n + 1$.

Решење. Доказаћемо индукцијом по k да за свако $k \in \mathbb{N}$ постоји $n_k \in \mathbb{N}$ које има тачно k различитих простих делилаца такав да $n_k \mid 2^{n_k} + 1$ и $3 \mid n_k$.

За $k = 1$, $n_1 = 3$ задовољава услов. Претпоставимо да је $k \geq 1$ и $n_k = 3^\alpha m$, где $3 \nmid m$, па m има $k-1$ простих делилаца. Тада број $3n_k = 3^{\alpha+1}m$ има тачно k простих делилаца и $2^{3n_k} + 1 = (2^{n_k} + 1)(2^{2n_k} - 2^{n_k} + 1)$ је дељиво са $3n_k$, јер $3 \mid 2^{2n_k} - 2^{n_k} + 1$. Одабраћемо прост број p који не дели n_k тако да буде $n_{k+1} = 3pn_k$. Довољно је узети p тако да $p \mid 2^{3n_k} + 1$ и $p \nmid 2^{n_k} + 1$.

Важи и јаче тврђење, да за сваки цео број $a > 2$ постоји прост број p који дели $a^3+1 = (a+1)(a^2-a+1)$, а не дели $a+1$. Заиста, важи нзд$(a^2-a+1, a+1)$ =нзд$(3, a+1)$, па ако $3 \nmid a+1$, довољно је узети $p = 3$; у супротном, ако је $a = 3b-1$, онда $a^2-a+1 = 9b^2-9b+3$ није дељиво са 3^2, па за p можемо узети било који прост делилац броја $\frac{a^2-a+1}{3}$.

29. Одредити све $n \in \mathbb{N}$ такве да $n^2 \mid 2^n + 1$.

Решење. Број n је очигледно непаран. Претпоставимо да је $n > 1$ и да је p његов најмањи прост делилац. Тада $p \mid 2^n + 1 \mid 2^{2n} - 1$ и $p \mid 2^{p-1} - 1$, па из Т.5 и чињенице да је $(2n, p-1) = 1$ следи $p \mid 2^{(2n,p-1)} - 1 = 2^2 - 1 = 3$, дакле $p = 3$.

Нека $3^k \parallel n$. По теореми 6, из $3 \parallel 2^2 - 1$ следи $3^{k+1} \parallel 2^{2n} - 1$, и одатле $3^{k+1} \parallel 2^n + 1$. Како $3^{2k} \parallel n^2 \mid 2^n + 1$, добијамо да је $k = 1$. Према томе, број $N = \frac{2^n+1}{3}$ није дељив са 3. Претпоставимо да је $N > 1$ и нека је $q > 3$ његов најмањи прост делилац. Тада $q \mid 2^{q-1} - 1, 2^{2n} - 1$, па опет по Т.6 имамо $q \mid 2^{(2n,q-1)} - 1$. Овде је $(2n, q-1) \mid 6$ јер $2n$ нема других простих делилаца мањих од q осим тројке. То значи да $q \mid 2^6 - 1 = 63 = 3^2 \cdot 7$, дакле $q = 7$. Међутим, $7 \nmid 2^n + 1$ ни за једно n, па нас је претпоставка $N > 1$ одвела у контрадикцију. Зато мора бити $N = 1$ и одатле $n = 3$.

30. Наћи све парове (n, p) такве да је p прост, $n \in \mathbb{N}$, $n \leq 2p$ и $n^{p-1} \mid (p-1)^n + 1$.

Решење. Једина решења за $n < 3$ или $p < 3$ су $(2, 2)$ и $(1, p)$ за произвољан прост број p. Надаље сматрамо да је p, а самим тим и n, непарно.

Посматрајмо најмањи прост делилац q броја n. Како тада $q \mid (p-1)^n + 1 \mid (p-1)^{2n} - 1$ и $q \mid (p-1)^{q-1} - 1$, следи $q \mid (p-1)^{(2n,q-1)} - 1 = (p-1)^2 - 1 = p(p-2)$. При том није могуће да $q \mid p-2$, јер тада $q \nmid (p-1)^n + 1 \equiv 2 \pmod{q}$. Следи да је $q = p$. Како је $n < 2p$, мора бити $n = p$. Услов задатка постаје $p^{p-1} \mid (p-1)^p + 1$, тј. $p^{p-1} \mid (1-p)^p - 1$. Међутим, по теореми 6 из $p \parallel (1-p) - 1$ следи $p^2 \parallel (1-p)^p - 1$, па закључујемо да је $p = 3$. Заиста, $(n, p) = (3, 3)$ задовољава услове.

31. Наћи све природне бројеве n за које постоји тачно једно $a \in \mathbb{N}$, $a < n!$, такво да $n! \mid a^n + 1$.

Решење. Ако је n парно и $n > 2$, $a^n + 1$ никад није дељиво са $n!$ јер $4 \mid n!$. Ако је n непарно и сложено, и d његов прост делилац или $d = 1$, онда $n! \mid a^n + 1$ за $a = \frac{n!}{d} - 1$, па имамо бар два избора за a. Дакле, n мора да буде просто.

За просто n, n не дели $\varphi(n!)$, па постоји непарно m такво да је $mn \equiv 1 \pmod{\varphi(n!)}$. Тада је $a \equiv a^{mn} = (-1)^m = -1 \pmod{n!}$ јединствено по модулу $n!$.

32. Доказати да за сваки прост број p постоји просто q такво да q није делилац $x^p - p$ ни за једно $x \in \mathbb{Z}$.

Решење. Претпоставимо да за сваки прост број q постоји n за које је $n^p \equiv p \pmod{q}$. Знамо да за $q \not\equiv 1 \pmod{p}$ степени n^p дају све могуће остатке по модулу q. Зато, нека је $q = kp + 1$ $(k \in \mathbb{N})$. Како је $p^k \equiv n^{kp} = n^{q-1} \equiv 1 \pmod{q}$, имамо $q \mid p^k - 1$ за свако такво q.

Узмимо за q било који прост делилац броја $\frac{p^p-1}{p-1}$. Како $q \nmid p-1$ јер је $\frac{p^p-1}{p-1} \equiv 1 \pmod{p-1}$, поредак p по модулу q је p, одакле је заиста $q = pk + 1$ за неко k. Сада из $q \mid p^k - 1, p^p - 1$ следи $q \mid p^{(p,k)} - 1$, што повлачи $(p, k) > 1$. То значи да $p \mid k$, тј. $q \equiv 1$

$(\mathrm{mod}\ p^2)$. Међутим, $\frac{p^p-1}{p-1} = p^{p-1}+\cdots+p+1 \not\equiv 1\ (\mathrm{mod}\ p^2)$ има бар један прост делилац који није конгруентан 1 по модулу p^2, што је контрадикција.

33. Нека су a и b различити природни бројеви већи од 1. Доказати да постоји n за које $(a^n-1)(b^n-1)$ није потпун квадрат.