MLADI NADARENI MATEMATIČARI
Marin Getaldić

Mali Fermatov i Eulerov teorem

7.2.2016.

Uvod/teorijske osnove

U ovom ćemo predavanju podrazumijevati da ste se upoznali s osnovnim pojmovima i rezultatima iz djeljivosti i kongruencija. Jedan od osnovnih rezultata u teoriji brojeva jest sljedeći

Teorem 1 (Mali Fermatov teorem)**.** *Neka je p prost broj i $a \in \mathbb{N}$ takav da $p \nmid a$. Tada*

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

Ukoliko $p \nmid a$, onda su brojevi p i a relativno prosti, tj. $(p, a) = 1$ (zašto?). Prisjetimo se, na predavanju o kongruencijama smo pokazali da tada vrijedi

$$a^{p-1} \equiv 1 \pmod{p} \Leftrightarrow a^p \equiv a \pmod{p}.$$

Također, ukoliko $p|a$, onda imamo $a^p \equiv a \equiv 0 \pmod{p}$. Zato tvrdnju malog Fermatovog teorema možemo i ovako izreći:

Za svaki prost broj p i svaki prirodan broj a vrijedi

$$a^p \equiv a \pmod{p}.$$

Zadatak 1.
Ovu ekvivalentnu tvrdnju malog Fermatovog teorema možemo dokazati matematičkom indukcijom po $a \in \mathbb{N}$. Provedite taj dokaz.
Uputa: iskoristite činjenicu da ukoliko je p prost broj, vrijedi kongruencija

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

za sve $a, b \in \mathbb{Z}$.

Mali Fermatov teorem se pokazuje kao izuzetno korisno sredstvo kod računanja kongruencija, što možemo vidjeti na sljedećem primjeru.

Primjer 1. *Odredimo ostatak pri dijeljenju broja 5^{5000} brojem 7. Prema malom Fermatovom teoremu vrijedi*

$$5^6 \equiv 1 \pmod{7},$$

a kako je $5000 = 833 \cdot 6 + 2$, imamo

$$5^{5000} = (5^6)^{833} \cdot 5^2 \equiv 1 \cdot 5^2 \equiv 25 \equiv 4 \pmod{7}.$$

Uz mali Fermatov teorem često se navodi i Eulerov teorem čija je jednostavna posljedica mali Fermatov teorem. Uskoro ćemo taj teorem iskazati, no nećemo ga dokazati ali savjetujemo svima da pokušaju sami dokazati ili potražiti dokaz. Prije iskaza trebamo definirati Eulerovi funkciju φ. To je funkcija koja prirodnom broju n pridružuje broj relativno prostih brojeva s n manjih od n. Na primjer, 15 je relativno prost s 1, 2, 4, 7, 8, 11, 13 i 14, dakle $\varphi(15) = 8$. Sad smo u stanju izreći Eulerov teorem.

Teorem 2 (Eulerov teorem)**.** *Neka su a, $n \in \mathbb{N}$ međusobno relativno prosti. Tada*

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

Iako zvuči jednostavno, dokaz teorema nije jednostavan. Napomenimo još samo kako je mali Fermatov teorem lagana posljedica Eulerovog teorema jer birajući $n = p$, gdje je p prost, jasno je da je $\varphi(p) = p - 1$ (provjerite!).

Primjer 2. *Odredimo zadnju znamenku broja* 43^{44}.

Određivanje zadnje znamenke je zapravo traženje čemu je kongruentan zadani broj modulo 10. *Budući da je* $43 \equiv 3 \pmod{10}$, *vrijedi* $43^{44} \equiv 3^{44} \pmod{10}$. *Ispisivanjem prvih nekoliko potencija broja* 3 *modulo* 10 *uočavamo,* $3^1 \equiv 3 \pmod{10}$, $3^2 \equiv 9 \pmod{1}0$, $3^3 \equiv 7 \pmod{1}0$, $3^4 \equiv 1 \pmod{10}$. *Iz zadnje kongruencije zaključujemo* $3^{44} \equiv (3^4)^{11} \equiv 1^{11} \equiv 1 \pmod{10}$, *pa time i* $43^{44} \equiv 3^{44} \equiv 1 \pmod{10}$, *odnosno zadnja znamenka traženog broja je* 1.

Sad ćemo ilustrirati kako se korištenjem Eulerovog teorema može doći do elegantnijeg rješenja. Budući da je od brojeva manjih od njega, 10 *relativno prost s brojevima* 1, 3, 7 *i* 9, *zato je* $\varphi(10) = 4$. *Kako je* 43 *relativno prost s* 10, *vrijedi* $43^{44} \equiv (43^{11})^4 \equiv 1 \pmod{10}$, *prema Eulerovom teoremu.*

Zadatci i rješenja

Zadatak 2.
Odredite posljednje dvije znamenke broja 3^{400}.

Rješenje.
Za Eulerovu funkciju vrijedi multiplikativnost, odnosno $\varphi(mn) = \varphi(m)\varphi(n)$, za sve prirodne brojeve m i n. To se jednostavno provjeri iz sljedeće formule za Eulerovu funkciju koja se može provjeriti da vrijedi:

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ prost}}} \left(1 - \frac{1}{p}\right),$$

gdje je $\prod$ simbol koji označava produkt. Stoga vrijedi:

$$\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 1 \cdot 5 \cdot 4 = 40,$$

pa je $3^{40} \equiv 1 \pmod{100}$. Zato je

$$3^{400} \equiv (3^{40})^{100} \equiv 1 \pmod{100}.$$

Dakle, posljednje dvije znamenke u zapisu broja 3^{400} su 01.

Zadatak 3.
Neka su $a_1, \ldots, a_{2015}$ takvi da $10 | a_1 + \ldots + a_{2015}$. Dokažite da

$$10 | a_1^5 + \ldots + a_{2015}^5.$$

Rješenje.
Uočimo da je

$$\sum_{i=1}^{2015} a_i^5 - \sum_{i=1}^{2015} a_i = \sum_{i=1}^{2015} a_i(a_i^4 - 1),$$

gdje smo simbolom $\sum$ označili zbroj. Za svaki $i = 1, \ldots, 2015$, točno je jedan od brojeva $a_i, a_i^4 - 1$ paran. Također, prema malom Fermatovom teoremu imamo $5 | a_i^5 - a_i$, $i = 1, \ldots, 2015$. Zato vrijedi

$$10 | \sum_{i=1}^{2015} a_i(a_i^4 - 1),$$

a odavde slijedi tvrdnja zadatka.

Zadatak 4.
Ako su p i q različiti prosti brojevi, dokažite da je broj $p^{q-1} + q^{p-1} - 1$ djeljiv sa pq.

Rješenje.
Po malom Fermatovom teoremu imamo $p | q^{p-1} - 1$, $q | p^{q-1} - 1$, a odavde slijedi $p | q^{p-1} + p^{q-1} - 1$, $q | p^{q-1} + q^{p-1} - 1$. Budući da su p i q relativno prosti, slijedi tvrdnja zadatka.

Zadatak 5.
Nađite sve proste brojeve p takve da p dijeli $4^p + 5^p$

Rješenje.
Po malom Fermatovom teoremu imamo $4^p \equiv 4 \pmod{p}$ i $5^p \equiv 5 \pmod{p}$, pa slijedi $4^p + 5^p \equiv 9 \pmod{p}$. No, kako je prema uvjetu zadatka $4^p + 5^p \equiv 0 \pmod{p}$, imamo $p|9$, pa je jedini traženi broj $p = 3$ (i provjerom vidimo da zaista i zadovoljava uvjeta zadatka).

Zadatak 6.
Nađite sve proste brojeve p takve da p^2 dijeli $5^{p^2} + 1$

Rješenje.
Iz $p^2|5^{p^2} + 1$ slijedi $p|5^{p^2} + 1$. S druge strane, prema malom Fermatovom teoremu imamo

$$5^{p^2} + 1 \equiv (5^p)^p + 1 \equiv 5^p + 1 \equiv 5 + 1 \equiv 6 \pmod{p},$$

što s uvjetom zadatka povlači $p|6$. Dakle, imamo dvije mogućnosti, $p = 2$ ili $p = 3$, a provjerom dobivamo da je $p = 3$ jedino rješenje.

Zadatak 7.
Ako prost broj p dijeli $a^p - 1$ za neki $a \in \mathbb{N}$, tada p^2 također dijeli $a^p - 1$. Dokažite.

Rješenje.
Prema malom Fermatovom teoremu imamo $a^p \equiv a \pmod{p}$, a prema uvjetu zadatka $a^p \equiv 1 \pmod{p}$. Dakle, $a \equiv 1 \pmod{p}$, tj. $p|a - 1$. Nadalje,

$$a^{p-1} + a^{p-2} + \ldots + a + 1 \equiv 1 + 1 + \ldots + 1 + 1 \equiv p \equiv 0 \pmod{p},$$

pa vidimo da vrijedi i $p|a^{p-1} + a^{p-2} + \ldots + a + 1$. Zato

$$p^2|(a - 1)(a^{p-1} + a^{p-2} + \ldots + a + 1) = a^p - 1.$$

Zadatak 8.
Dokažite da za svaki prost broj p postoji beskonačno mnogo brojeva oblika $2^n - n$, $n \in \mathbb{N}$, koji su djeljivi sa p.

Rješenje.
Ukoliko je $p = 2$, tvrdnja zadatka vrijedi jer $p|2^n - n$ za svaki paran n. Pretpostavimo sada $p > 2$. Prema malom Fermatovom teoremu imamo

$$2^{p-1} \equiv 1 \pmod{p} \Rightarrow 2^{(p-1)^k} \equiv 1 \pmod{p}$$

za svaki $k \in \mathbb{N}$. Nadalje, $(p - 1)^k \equiv (\pm 1)^k \pmod{p}$ za svaki $k \in \mathbb{N}$, pa posebno imamo $(p - 1)^{2k} \equiv 1 \pmod{p}$ za svaki $k \in \mathbb{N}$. Dakle,

$$2^{(p-1)^{2k}} - (p - 1)^{2k} \equiv 0 \pmod{p}$$

za svaki $k \in \mathbb{N}$, pa vrijedi tvrdnja zadatka.

Slijedi nekoliko težih zadataka čija rješenja navodimo u idućem odjeljku ali savjetujemo da prvo dobro razmislite o njima i pokušate ih samostalno riješiti. Ipak, imajte na umu da su nešto teži od predhodnih.

Zadatak 9.
Dokažite da iz bilo kojeg aritmetičkog niza čiji su članovi prirodni brojevi može biti izabran beskonačan geometrijski niz.
Napomena. Za niz prirodnih brojeva $(a_n)_{n\in\mathbb{N}}$ kažemo da je **aritmetički niz** ako je razlika svaka dva uzastopna člana tog niza stalna i jednaka nekom (cijelom) broju d, tj.

$$a_{n+1} - a_n = d \quad \forall n \in \mathbb{N}.$$

Slično, za niz prirodnih brojeva $(a_n)_{n\in\mathbb{N}}$ kažemo da je **geometrijski niz** ako je kvocijent svaka dva uzastopna člana tog niza stalan i jednak nekom (racionalnom) broju q, tj.

$$\frac{a_{n+1}}{a_n} = q \quad \forall n \in \mathbb{N}.$$

Inače, potpuno se isto definiraju i aritmetički i geometrijski niz realnih brojeva, s time da promatramo geometrijske nizove pozitivnih realnih brojeva.

Zadatak 10.
Dokažite da postoji beskonačan niz brojeva oblika $2^n - 3$, $n \in \mathbb{N}$, za koji vrijedi da su svaka dva među njima relativno prosta.

Zadatak 11.
Dokažite da ne postoji prirodan broj $n > 1$ takav da $n|2^n - 1$.

Rješenje.
Uputa: pretpostavite suprotno i razlikujte slučajeve kada je n prost i kada je složen. U drugom slučaju stavite da je p najmanji prost djelitelj od n. Također, označite sa d najmanji prirodan broj takav da $2^d \equiv 1 \pmod{p}$. Uočite da je $1 < d \leqslant p - 1$ te pokušajte dokazati da je n djeljiv sa d.

Zadatak 12.
Dokažite da ne postoje prirodni brojevi $n_1, n_2 > 1$ takvi da $n_1|2^{n_2} - 1$ i $n_2|2^{n_1} - 1$.

Rješenja ostalih zadataka

Rješenje zadatka 9. Označimo sa a i d prvi član i razliku aritmetičkog niza, tim redom. Uvjet naprosto govori $a, d \in \mathbb{N}$. Nadalje, za bilo koji prirodan b vrijedi da je b član niza ako i samo ako vrijedi $b \geqslant a$ i $b \equiv a \pmod{d}$.

Neka je h bilo koji prirodan broj koji je relativno prost sa d (npr., možemo uzeti $h = d + 1, 2d + 1, 3d + 1, \ldots$). Prema Eulerovom teoremu

$$h^{\varphi(d)} \equiv 1 \pmod{d} \Rightarrow ah^{\varphi(d)} \equiv a \pmod{d},$$

pa vidimo da se broj $ah^{\varphi(d)}$ nalazi u polaznom aritmetičkom nizu. Općenito, za proizvoljan $n \in \mathbb{N}_0$ imamo

$$h^{n\varphi(d)} \equiv 1 \pmod{d} \Rightarrow ah^{n\varphi(d)} \equiv a \pmod{d},$$

pa vidimo da se svi članovi geometrijskog niza s prvim članom a i kvocijentom $h^{\varphi(d)}$ nalaze u polaznom aritmetičkom nizu.

Rješenje zadatka 10. Neka su $p_1, p_2, \ldots, p_k$ različiti neparni prosti brojevi. Tada postoji $n \in \mathbb{N}$, $n > \max\{p_1, \ldots, p_k\}$, takav da $2^n - 3$ nije djeljiv nijednim od brojeva $p_1, \ldots, p_k$. Naime, prema malom Fermatovom teoremu za svaki $i \in \{1, \ldots, k\}$ imamo

$$2^{(p_1-1)(p_2-1)\cdots(p_k-1)} \equiv 1 \pmod{p}_i$$
$$\Rightarrow 2^{(p_1-1)(p_2-1)\cdots(p_k-1)} - 3 \equiv -2 \pmod{p}_i,$$

i također, $-2 \not\equiv 0 \pmod{p}_i$, $(p_1 - 1)(p_2 - 1)\cdots(p_k - 1) > \max\{p_1, \ldots, p_k\}$.

Sada ćemo rekurzivno konstruirati traženi niz. Za prvi član niza uzmimo npr. $2^3 - 3 = 5$. Pretpostavimo da smo definirali prvih n članova niza, $a_1, \ldots, a_n$. Neka su $p_1, \ldots, p_k$ svi (međusobno različiti) prosti djelitelji brojeva $a_1, \ldots, a_n$ (uočimo da su svi $p_1, \ldots, p_k$ neparni). Tada stavimo

$$a_{n+1} = 2^{(p_1-1)(p_2-1)\cdots(p_k-1)} - 3$$

i prema prethodnoj diskusiji znamo da nijedan od brojeva $p_1, \ldots, p_k$ ne dijeli a_{n+1}.

Uočimo sada da su u ovako konstruiranom nizu $(a_n)_{n\in\mathbb{N}}$ svaka dva člana međusobno relativno prosta jer, prema konstrukciji, nemaju nijedan zajednički prosti djelitelj.

Rješenje zadatka 11. Pretpostavimo da postoji takav n. Razlikujemo slučajeve:

1° n je prost. Tada imamo $2^n \equiv 1 \pmod{n}$, što je u kontradikciji s malim Fermatovim teoremom ($2^n \equiv 2 \pmod{n}$).

2° n je složen. Neka je p najmanji prost djelitelj od n. Budući da n dijeli $2^n - 1$, što je neparan broj, i n mora biti neparan. Zato i p mora biti neparan, tj. $p > 2$. Uz $n = kp$, $k > 1$, imamo

$$p|2^n - 1 \Rightarrow (2^k)^p \equiv 1 \pmod{p}.$$

No, prema malom Fermatovom teoremu vrijedi

$$(2^k)^p \equiv 2^k \pmod{p},$$

pa slijedi

$$2^k \equiv 1 \pmod{p}.$$

Neka je d najmanji prirodan broj takav da $2^d \equiv 1 \pmod{p}$; zbog malog Fermatovog teorema znamo da takav d sigurno postoji i da vrijedi $d \leqslant p-1$. Tada je također $d \leqslant k$. Zato k možemo podijeliti s ostatkom sa d, tj. postoje brojevi $q \in \mathbb{N}$, $r \in \mathbb{N}_0$, $r < d$, takvi da $k = qd + r$. Sada iz kongruencije $2^k \equiv 1 \pmod{p}$ slijedi

$$2^{qd+r} \equiv (2^d)^q \cdot 2^r \equiv 1^q \cdot 2^r \equiv 2^r \equiv 1 \pmod{p}.$$

No, prema pretpostavci je d najmanji prirodan broj takav da $2^d \equiv 1 \pmod{p}$, pa mora biti $r = 0$. Dakle, $k = qd$, pa je k djeljiv sa d. No, kako je $d \leqslant p-1$ i očito $d > 1$, slijedi da d ima prost djelitelj strogo manji od p pa zato i k ima prost djelitelj strogo manji p. Dakle, n ima prost djelitelj strogo manji od p, što je kontradikcija s pretpostavkom da je p najmanji prost djelitelj od n.

Rješenje zadatka 12. Pretpostavimo da postoje takvi n_1, n_2. Neka je $k = [m, n]$ njihov najmanji zajednički višekratnik. No tada

$$2^{n_1} - 1|2^k - 1 \Rightarrow n_2|2^k - 1,$$
$$2^{n_2} - 1|2^k - 1 \Rightarrow n_1|2^k - 1,$$

a odavde, po definiciji najmanjeg zajedničkog višekratnika, slijedi

$$k|2^k - 1.$$

No to je nemoguće prema prethodnom zadatku.