Dodatna nastava iz matematike u MG-u

EKSPONENCIJALNE KONGRUENCIJE

Predavač: Peki

Uvodne napomene

1. **Kineska teorema o ostacima (KTO)**: Neka su $m_1, m_2, ..., m_k$ po parovima uzajamno prosti prirodni brojevi i $a_1, ..., a_k$ bilo koji celi brojevi. Tada postoji jedinstven po modulu $m_1...m_k$ broj x takav da je $x \equiv a_i \pmod{m_i}$ za $1 \leq i \leq k$.

2. **Ojlerova teorema**: Neka su a i n uzajamno prosti prirodni brojevi. Tada je $a^{\varphi(n)} \equiv 1 \pmod{n}$, gde je $\varphi(n) = p_1^{\alpha_1 - 1}...p_k^{\alpha_k - 1}(p_1 - 1)...(p_k - 1)$ (ako je $p_1^{\alpha_1}...p_k^{\alpha_k}$ kanonska faktorizacija broja n) broj prirodnih brojeva manjih od n i uzajamno prostih sa n. $\varphi(n)$ se zove **Ojlerova funkcija.** Jasno je da $\delta(a, m)$ (poredak broja a po modulu m) deli $\varphi(n)$. Ako je poredak baš jednak $\varphi(n)$, kaže se da je a **primitivni koren** po modulu n. Moduli po kojima postoje primitivni koreni su $2, 4, p^k, 2p^k$, gde je p prost broj.

3. **Lema**: Ako su m i n prirodni, a a ceo broj, onda je $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

4. **Lema**: Neka su a, k, t prirodni brojevi i p prost broj. Tada važi:

   (a) $2^k \| a^{2t} - 1 \Rightarrow 2^{k+1} \| a^{4t} - 1$;

   (b) $p^k \| a^t - 1 \Rightarrow p^{k+1} \| a^{pt} - 1$;

   (c) $p^k \| a^t - 1 \bigwedge p^{k+1} | a^{\alpha t} - 1 \Rightarrow p | \alpha$;
   b i c VAŽI I ZA PLUS!

   Posledica: Ako je g primitivni koren po modulu p, gde je p prost broj i p^2 ne deli $g^{p-1} - 1$, onda je g primitivni koren po modulu p^k za svako prirodno k.

Zadaci

1. Odrediti sve parove (a, b) prirodnih brojeva takvih da je $7^a - 3 \cdot 2^b = 1$.

2. Postoji li prirodan broj n tako da je $2^n + 1$ deljivo sa 247?

3. Naći sve proste brojeve p i q takve da je $a^{3pq} - a$ deljivo sa $3pq$ za svako prirodno a.

4. Naći sve parove prostih brojeva p i q takvih da je $(5^p - 2^p)(5^q - 2^q)$ deljivo sa pq.

5. Dokazati da za svaki prirodan broj m postoji prirodan broj broj n takav da je $n^2 + 7$ deljivo sa 2^m.

6. Dokazati da za svaki prirodan broj m postoji prirodan broj broj n takav da je $2^n + 2005$ deljivo sa 3^m.

7. Odrediti sve prirodne brojeve n za koje $n | 2^n - 1$.

8. Neka je $t \in N$ i p prost faktor broja $2^{2^t} + 1$. Dokazati da je $p \equiv 1 \pmod{2^{t+1}}$.

9. Odrediti sve prirodne brojeve n za koje n^2 deli $2^n + 1$.

10. Dokazati da za svaki neparan prirodan broj n važi da $((n-1)^n + 1)^2$ deli $n[(n-1)^{(n-1)^n + 1} + 1]$.

11. Dokazati da je svaki prost delilac broja $\frac{p^p - 1}{p - 1}$ oblika $kp + 1$, $k \in N$.

12. Neka je $p > 2$ prost i $a > 2$ prirodan broj. Ako p deli $a+1$, dokazati da postoji prost broj $q > p$, takav da q deli $a^p + 1$.

13. Neka je p prost broj. Dokazati da postoji prost broj q takav da kongruencija $x^p - p \equiv 0 \pmod{q}$ nema rešenja.

14. Odrediti sve prirodne brojeve a, m, n, za koje $a^m + 1 | (a+1)^n$.

15. Odrediti sve prirodne brojeve b, m, n takve da je $b > 1, m > n$ i brojevi $b^m - 1$ i $b^n - 1$ imaju iste proste faktore.

16. Odrediti sve parove (n, p) prirodnih brojeva, takve da važi:

    (a) p je prost broj;

    (b) $n \leq 2p$;

    (c) $n^{p-1} | (p-1)^n + 1$;

17. Da li postoji prirodan broj n takav da važi

    (a) broj n je deljiv sa tačno 2000 različitih prostih faktora;

    (b) broj $2^n + 1$ je deljiv sa n?

Rešenja i uputstva za rešavanje nekih zadataka

2. Prvo dokazati sledeću lemu: Neka je a prirodan i p neparan prost broj. Kongruencija $a^c \equiv -1 \pmod{p}$ ima rešenja (po c) akko je poredak broja a po modulu p paran broj. Za dokaz leme koristiti:

    (a) Ako je t poredak broja a po modulu p, tada ako posmatramo ostatke koje daju eksponenti broja a $(a^1, a^2, ...)$ po modulu p, prvih t će biti različiti, a nadalje će se periodično ponavljati.

    (b) Ako je $a^c \equiv -1 \pmod{p}$, i $c < t$, onda je $a^{2c} \equiv 1 \pmod{p}$. Ako je $a^t \equiv 1 \pmod{p}$, gde je t poredak broja a po modulu p i t je parno, koliko je $a^{\frac{t}{2}}$ po modulu p?

3. Prvo zameniti $a = 2$, a zatim odabrati a tako da po modulu p daje ostatak g_p, a po modulu q daje ostatak g_q, gde su g_p i g_q primitivni koreni po modulima p i q redom (takvo a postoji po KTO).

6. Na osnovu 4.Leme i Posledice(vidi teorijski uvod), 2 je primitivni koren po modulu 3^m za svako $m \in N$. Dalje koristiti činjenicu da ako je a primitivni koren po modulu n, tada brojevi $a, a^2, ..., a^{\varphi(n)}$ daju po modulu n različite ostatke uzajamno proste sa n-svaki tačno po jednom.

7. Neka je p najmanji prost faktor od n. Primeniti 3.*Lemu*.

8. Očito važi da p ne deli $2^{2^t} - 1$ i p deli $2^{2^{t+1}} - 1$. Iskoristiti svojstva poretka i MFT.

10. Pretpostavimo da $p^k \| (n-1)^n + 1 = n^n - \binom{n}{1} n^{n-1} + ... - \binom{n}{n-2} n^2 + \binom{n}{n-1} n = An^3 + n^2, A \in N$. Ovo poslednje je zato što je $\binom{n}{n-2} = n\frac{n-1}{2}$, što je deljivo sa n. Neka je p proizvoljan prost faktor broja $(n-1)^n + 1$ i neka $p^k \| (n-1)^n + 1$. Razlikujemo dva slučaja:

    (a) $p | n$. Neka $p^t \| n$. Tada je $k = 2t$. Kako $p^t \| (n-1) + 1 = n$ i $p^{2t} \| (n-1)^n + 1$, to na osnovu 4. Leme $p^{3t} \| (n-1)^{(n-1)^n+1} + 1$, odnosno $p^{4t} \| n((n-1)^{(n-1)^n+1} + 1)$. Kako $p^{4t} \| ((n-1)^n + 1)^2$, u ovom slučaju je tvrdjenje jasno.

    (b) $(n, p) = 1$. Tada $p^k \| \frac{(n-1)^n+1}{n}$, pa na osnovu 4. leme $p^{2k} \| ((n-1)^n)^{\frac{(n-1)^n+1}{n}} + 1 = (n-1)^{(n-1)^n+1}$.

11. Dokažimo prvo da je dati broj uzajamno prost sa $p-1$. Kako je svaki prost faktor broja $p-1$ različit od p, na osnocu 4. leme sledi da je njegova potencija koja deli p^p-1 ista kao i kod $p-1$. Dalje se na osnovu 3. Leme i MFT lako izvodi da p deli $q-1$.

12. Prvo dokazujemo da postoji prost broj q takav da q deli a^p+1, a ne deli $a+1$. Pretpostavimo suprotno, tj. da brojevi $a+1$ i a^p+1 imaju sve iste proste faktore. Analizirajmo proizvoljan prost faktor koji ih deli oba. Kako je broj $a^{p-1}-a^{p-2}+...-a+1$ neparan, potencije dvojke koje ih dele su iste. Ako je taj prost faktor neparan i nije jednak p, njegove potencije koje dele a^p+1 i $a+1$ su na osnovu 4.Leme jednake. Ako p ne deli $a+1$, (na osnovu MFT $p|a+1 \Leftrightarrow p|a^p+1$,) onda pošto a^p+1 nije deljiv nijednim prostim faktorom kojim nije deljiv $a+1$, količnik $\frac{a^p+1}{a+1}$ mora biti 1. Ako za neko $t>0$ $p^t \| a+1$, onda $p^{t+1} \| a^p+1$. Tada je $\frac{a^p+1}{a+1}=p$, odnosno $a^{p-1}-a^{p-2}+...-a+1=p$. Označimo levu sa X. Važi $X>a^{p-1}-a^{p-2}=a^{p-2}(a-1)\geq 2^{p-2}>p$ za $p\geq 5$. Dakle, $p=3$, što povlači $a=2$. Kontradikcija.
Dokažimo sada da je $q>p$. Pretpostavimo suprotno. Iz prethodnog sledi da ne može biti jednak p, pa je $q<p$. Iz $q|a^{q-1}-1$ i $q|a^{2p}-1$, na osnovu 3.Leme sledi da q deli $a^{(2p,q-1)}-1=a^2-1$ ($(2p,q-1)=2$ zbog $q<p$.) Kako q ne deli $a+1$, q mora deliti $a-1$, što povlači da q deli a^p-1. Sada iz $q|a^p+1$ sledi $q=2$. Kontradikcija! Kraj dokaza.

14. Jasno je da je ako je $a=1$ ili $m=1$, uslov ispunjen. Neka je $a>1$. Dokažimo prvo da je m parno. Ako a^m+1 ima neparan prost delilac $p \Rightarrow p|a+1 \Rightarrow a\equiv -1 \pmod p \Rightarrow a^m \equiv (-1)^m \pmod p \Rightarrow$ m je neparno. Ako je $a^m+1=2^s$, m je neparno jer broj oblika b^2+1 nije deljiv sa 4.
Neka je sada p neparan prost faktor broja m. Iz uslova zadatka sledi da brojevi $a+1$ i a^p+1 imaju iste proste faktore, što je na osnovu 12. zadatka moguće jedino za $a=2$ i $p=3 \Rightarrow m=3^k \Rightarrow 2^{3^k}+1|3^n$, ako $k\geq 2$ to iz $3^3\cdot 19=2^{3^2}+1|2^{3^k}+1|3^n$, što je nemoguće. Dakle, drugo rešenje je $a=2, m=3, n\geq 2$.

15. Jasno je da $(b^m-1, b^n-1)=b^{(m,n)}-1$ ima iste te proste faktore. Stavimo $k=\frac{m}{(m,n)}$ Pretpostavimo da k ima neparan prost faktor p. Tada brojevi $a-1$ i a^p-1 imaju iste proste faktore. Sličnim razmatranjem kao u 12. zadatku dobijamo $a^{p-1}+...+a+1=p$ što povlači $a=1$. Dakle $k=2^v$. Ako je $v\geq 2$, iz $a^2+1|a^{2^v}-1 \Rightarrow$ svaki prost faktor q od a^2+1 deli $a-1 \Rightarrow q=2$. Medjutim $2^u|a^2+1$ je nemoguće. Dakle $u=1$, tj $k=2$ i a^2-1 i $a-1$ imaju iste proste faktore. Sledi da je $a+1$ stepen dvojke, tj. $a=2^s-1$, $s\geq 2$. Stavimo $d=(m,n)$. Iz $4|b^d+1$ sledi da je d neparno. Ako pretpostavimo da je $d>1$, iz $b^d+1=(b+1)(b^{d-1}-b^{d-2}+...-b+1)$ dobijamo kontradikciju jer je sa desne strane poslednje jednakosti drugi faktor neparan broj veći od 1. Dakle $m=2$. Analogno sledi $n|2$, te je $n=1$. Dakle $b=2^s-1, s\geq 2, m=2, n=1$.

DOMAĆI ZADATAK

1. Neka je $a>0$ i $0<b<1$. Dokazati nejednakost
$$\sqrt{1+a^2}+\sqrt{1-b^2}\leq \frac{a}{b}+\frac{b}{a}.$$

2. Dat je niz $a_1=3$ i $a_{n+1}=\frac{3a_n^2+1}{2}-a_n$. Ako je n stepen trojke, dokazati da n deli a_n.

3. Naći sve $f: R\to R$ takve da je
$$f(f(x)+y)=f(x^2-y)+4f(x)y.$$