Odjel za matematiku
Sveučilište u Osijeku

Prvi kolokvij iz Uvoda u teoriju brojeva

14. svibnja 2012.

1. (a) Ako je r ostatak pri dijeljenju broja a brojem $b \neq 0$ dokažite da je $(a, b) = (b, r)$.
   (b) Neka je $n \in \mathbb{N}$, $n \geq 3$, i $p, q \in \mathbb{N}$ prosti brojevi sa svojstvom da $p | n!$ i $q | (n! - 1)$. Dokažite da je $p < q$.

2. Neka je $n \in \mathbb{N}$ i $a \neq 1$ sa svojstvom $(a, n) = 1$. Označimo sa d najmanji $x \in \mathbb{N}$ za koji vrijedi
$$a^x \equiv 1 \pmod{n}. \tag{1}$$
   (a) Ako za $x = m$, $m \in \mathbb{N}$, također vrijedi relacija (1) dokažite da tada $d | m$.
   (b) Ako je p neparan prost broj i $n = 5^p + 1$ za $a = 5$ odredite pripadni d.

3. Ako se za učenike neke škole koja ima više od 100 učenika želi organizirati autobusni prijevoz, onda pri raspoređivanju u autobuse s 15 mjesta nakon popunjavanja svih autobusa u posljednjem autobusu ostane 6 učenika. Analogno, ako se popunjavaju autobusi sa 40, odnosno 50 mjesta, onda u posljednjem autobusu ostane 1, odnosno 31 učenik. Može li škola imati paran broj učenika? Koliko škola ima učenika ako je poznato da ih je manje od 1000?

4. Provjerite da li postoje prirodni brojevi n i m takvi da vrijedi $\varphi(n) = 2 \cdot 7^m$.

5. U RSA kriptosustavu s javnim ključem (1241,709) dešifrirajte brojeve 1197,1239. Ako je neki od tako dobivenih brojeva prost, dokažite to, a zatim odredite ostatak pri dijeljenju broja 777^{2018} tim prostim brojem.

Napomena. Sve svoje tvrdnje obrazložite.