

### Teorija brojeva, M smer, februar 2012

1. Rešite sistem kongruencija:

$$x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{11}, \quad 4x \equiv 5 \pmod{17}.$$

2. Dokažite da za svako  $n \in \mathbb{N}$  važi:

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu(d)^2}{\varphi(d)}.$$

3. Odredite prsten celih u kvadratnom raširenju  $\mathbb{Q}(\sqrt{14})$  (sa dokazom). Odredite bar jednu njegovu integralnu bazu.

4. Ako je  $\omega = \frac{-1+\sqrt{-3}}{2}$ ,  $\mathbb{Z}[\omega]$  prsten celih u  $\mathbb{Q}(\sqrt{-3})$  i  $\pi$  proizvoljan prost element u  $\mathbb{Z}[\omega]$ , dokažite da je količički prsten  $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$  konačno polje sa  $N(\omega)$  elemenata.

5. Neka je  $n$  neparan prirodan broj i  $(a, n) = 1$ . Simbol Zolotareva  $\left(\frac{a}{n}\right)_Z$  definišemo kao znak permutacije  $x \mapsto ax$  kompletnog sistema ostataka  $\{0, 1, 2, \dots, n-1\}$  modulo  $n$ .

(a) Izračunajte simbol Zolotareva  $\left(\frac{8}{15}\right)_Z$ .

(b) Za pozitivno neparno  $n$  dokažite:  $\left(\frac{-1}{n}\right)_Z = (-1)^{(n-1)/2}$ .

(c) Neka je  $p$  prost broj. Neka je  $h$  red elementa  $a$  u multiplikativnoj grupi  $(\mathbb{Z}/p\mathbb{Z})^\times$ . Dokažite da se onda permutacija  $x \mapsto ax$  raspada na jedan 1-cikl i  $\frac{p-1}{h}$   $h$ -ciklova.

(d) Dokažite da se za  $p$  prost i  $(a, p) = 1$ , simboli Zolotareva i Legendre-a poklapaju, tj. da važi:

$$\left(\frac{a}{p}\right)_Z = \left(\frac{a}{p}\right)_L.$$

### Teorija brojeva, L smer, februar 2012

1. Rešite sistem kongruencija:

$$x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{11}, \quad 4x \equiv 5 \pmod{17}.$$

2. Odredite vrednosti Legendre-ovih simbola  $\left(\frac{-30}{61}\right)$ ,  $\left(\frac{442}{139}\right)$ .

3. Dokažite da za svako  $n \in \mathbb{N}$  važi:

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu(d)^2}{\varphi(d)}.$$

4. Odredite prsten celih u kvadratnom raširenju  $\mathbb{Q}(\sqrt{14})$  (sa dokazom). Odredite bar jednu njegovu integralnu bazu.

5. Dokažite da za prost broj  $p$  važi:  $(p-1)! \equiv -1 \pmod{p}$ .