Конгруенције

Лука Мијатовић

15. februar 2026.

Sadržaj

1 Увод у конгруенције **2**

2 Вилсонова теорема **2**

2.1 Примена и примери 2

3 Табеларни приказ остатака **2**

4 Закључак **3**

1 Увод у конгруенције

Теорија конгруенција представља један од темеља модерне теорије бројева. Увео ју је Карл Фридрих Гаус у свом делу *Disquisitiones Arithmeticae*.

Дефиниција 1.1. *Нека је $n \in \mathbb{N}$. Кажемо да су цели бројеви a и b* ***конгруентни по модулу*** *n ако n дели њихову разлику $a-b$. То записујемо као:*

$$a \equiv b \pmod{n}$$

2 Вилсонова теорема

Џон Вилсон (1741–1793)

Вилсонова теорема даје неопходан и довољан услов да број буде прост.

Лема 2.1. *Ако је p прост број, тада је једини елемент $a \in \{1, 2, \dots, p-1\}$ који је сам себи инверзан по модулу p (тј. $a^2 \equiv 1 \pmod{p}$) заправо 1 или $p-1$.*

Теорема 2.1 (Вилсонова теорема)**.** *Природан број $p > 1$ је прост ако и само ако важи:*

$$(p-1)! \equiv -1 \pmod{p} \tag{1}$$

2.1 Примена и примери

Примена ове теорије је огромна, посебно у **криптографији** и рачунарству.

- Провера простости бројева.
- Генерисање *RSA* кључева.
- Теорија група.

3 Табеларни приказ остатака

У следећој табели приказани су остаци при дељењу са малим простим бројевима за вредност $(p-1)!$.

Број p	**Формула** $(p-1)!$	**Остатак по модулу** p
2	$1! = 1$	$1 \equiv -1 \pmod{2}$
3	$2! = 2$	$2 \equiv -1 \pmod{3}$
5	$4! = 24$	$24 \equiv -1 \pmod{5}$

Провера Вилсонове теореме за мале бројеве

4 Закључак

Конгруенције нам омогућавају да на елегантан начин решавамо сложене проблеме дељивости. Иако је Вилсонова теорема од великог теоријског значаја, у пракси се за велике бројеве чешће користе други алгоритми због факторијела који брзо расте.

1. Први корак: Разумевање дељивости.

2. Други корак: Примена на просте бројеве.