Мала Фермаова теорема

Јован Гарић

30. новембар 2025.

Садржај

1 Увод **3**

2 Мала Фермаова теорема **4**
2.1 Конгруенције 4
2.2 Прости бројеви 4
2.3 Теорема 4

3 Примене **5**

4 Закључак **6**

1 Увод

Мала Фермаова теорема је део математичке области теорије бројева. У наставку рада говорићемо више о њој и њеном значају, као и математичару који ју је открио и по коме носи име.

2 Мала Фермаова теорема

Малу Фермаову теорему формулисао је француски математичар **Пјер де Ферма** у 17. веку, у оквиру својих истраживања о својствима простих бројева. Иако је теорему изнео без доказа, она је касније потврђена од стране више математичара и представља темељ многих савремених алгоритама.

Слика 1: Пјер де Ферма

Први математичар који ју је доказао био је **Готфрид Лајбниц** и његов доказ је пронађен у рукопису без датума.

Пре него што прикажемо теорему, прво ћемо дефинисати појмове конгруенције и простих бројева, на којима се ова теорема заснива.

2.1 Конгруенције

Дефиниција 1. *Нека су* $a, b, m \in \mathbb{Z}$, $m > 0$. *Кажемо да су* a *и* b ***конгруентни по модулу*** m *ако важи*

$$a \equiv b \pmod{m}.$$

Ово значи да бројеви a *и* b *дају исти остатак при дељењу бројем* m.

a	m	$a \bmod m$
10	3	1
25	7	4
47	5	2

Табела 1: Примери остатака при дељењу.

2.2 Прости бројеви

Природан број $p > 1$ је **прост** ако је дељив само *самим собом* и *бројем* 1. Број 1 **није** ни прост, ни сложен.

Теорема 1 (Еуклид)**.** *Постоји бесконачно много простих бројева.*

Лема 1. *Ако прост број* p *дели производ* ab*, онда важи да* p *дели* a *или* p *дели* b.

2.3 Теорема

Ако је p *прост број* и **не дели** број a, онда је:

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

Ова теорема има кључну примену у **криптографији**.

3 Примене

Неке од примена ове теореме су:

- **Криптографија(RSA и други алгоритми)**
- **Убрзање модуларног степеновања**
- **Фермаов тест простости**

4 Закључак

У овом раду приказане су конгруенције и прости бројеви, мала Фермаова теорема, као и неке од примена у математичким и рачунарским областима.