Wilsonov teorem

Ilija Ilišević*

Sažetak. *U radu je iskazan i dokazan Wilsonov teorem, koji je jedan od vrlo važnih teorema teorije brojeva. Kroz mnoštvo primjera i zadataka koji su prilagođeni učenicima srednjih škola ilustrirane su različite primjene tog teorema.*

Ključne riječi: *teorija brojeva, kongruencije*

Wilsons theorem

Abstract. *In this paper the Wilson's theorem has been explained and proved, which is one of the important theorems in the number theory. By using many examples and exercises adapted to high-school students we illustrate different applications of that theorem.*

Key words: *number theory, congruence*

Wilsonov teorem je jedan od poznatih teorema iz teorije brojeva. Iskazao ga je John Wilson, student engleskog matematičara Edwarda Waringa. Potonji ga je objavio 1770. godine, ali ga niti jedan niti drugi nisu dokazali. Slavni francuski matematičar Lagrange je 1771. godine prvi dokazao ovaj teorem.

Za razliku od poznatijeg malog Fermatovog teorema, Wilsonov teorem daje i nužan i dovoljan uvjet da bi broj bio prost.

Iskazat ćemo Wilsonov teorem, dati dva dokaza i riješiti nekoliko zadataka u kojima se teorem primjenjuje.

Teorem 1 [Wilsonov teorem]. *Prirodan broj $p \geq 2$ je prost ako i samo ako je*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Dokaz 1. Za $p = 2$ tvrdnja očigledno vrijedi. Ako je p prost broj veći od 2, tada je p neparan, pa se u produktu $1 \cdot 2 \cdot 3 \ldots (p-1)$ pojavljuje paran broj faktora. Neka je $k \in \{2, 3, \ldots, p-2\}$. Brojevi $k, 2k, 3k, \ldots, (p-1)k, pk$ tvore potpuni sustav ostataka po modulu p, pa u nekom redoslijedu daju ostatke $0, 1, 2, \ldots p-1$ po modulu p. Obzirom da vrijedi $k \not\equiv 1 \pmod{p}$, $(p-1)k \not\equiv 1 \pmod{p}$ i $pk \not\equiv 1 \pmod{p}$, to je $kl \equiv 1 \pmod{p}$ za jedan (i samo jedan) $l \in \{2, 3, \ldots, p-2\}$. Pretpostavimo li da je $l = k$, tada imamo $k^2 \equiv 1 \pmod{p}$ odnosno $(k-1)(k+1) \equiv 0 \pmod{p}$ što povlači $k \equiv 1 \pmod{p}$ ili $k \equiv -1 \pmod{p}$, suprotno tome da je $k \in \{2, 3, \ldots, p-2\}$. Prema

*III. gimnazija, Kamila Firingera 14, HR-31 000 Osijek

tome, skup $\{2, 3, \ldots, p-2\}$ možemo podijeliti na dva jednaka dijela tako da za svaki k iz jednog dijela postoji jedinstven l iz drugog dijela sa svojstvom $kl \equiv 1 \pmod{p}$. Slijedi

$$2 \cdot 3 \ldots (p-2) \equiv \underbrace{1 \cdot 1 \ldots 1}_{\frac{p-3}{2}} \pmod{p},$$

odnosno

$$(p-2)! \equiv 1 \pmod{p}.$$

Za $k = p-1$ je $k \equiv -1 \pmod{p}$, pa je konačno

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

Dokažimo sada da iz $p \mid (p-1)! + 1$ slijedi da je p prost broj. Pretpostavimo da p nije prost broj i da ima djelitelj d, $d < p$. Tada $d \mid (p-1)!$ odakle slijedi $d \nmid (p-1)! + 1$ i stoga $p \nmid (p-1)! + 1$. Ovim smo došli u kontradikciju, pa p mora biti prost broj. □

Dokaz 2. Rabit ćemo Vandermondeovu determinantu. Ako su $x_1, x_2, \ldots, x_{p-1}$ različiti kompleksni brojevi, tada je

$$\begin{aligned} & V(x_1, x_2, \ldots, x_{p-1}) = \\ = \quad & \det \begin{pmatrix} 1 & x_1 & {x_1}^2 & \ldots & {x_1}^{p-2} \\ 1 & x_2 & {x_2}^2 & \ldots & {x_2}^{p-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_{p-1} & {x_{p-1}}^2 & \ldots & {x_{p-1}}^{p-2} \end{pmatrix} = \Pi_{i<j}(x_j - x_i). \end{aligned}$$

Neka je p neparan prost broj. Tada je $\det V = V(1, 2, \ldots, p-1)$ produkt brojeva manjih od p, pa $p \nmid \det V$. Pomnožimo i-ti redak determinante $\det V$ brojem i $(i = 1, 2, \ldots, p-1)$. Prema malom Fermatovom teoremu je

$$\begin{aligned} & (p-1)! \cdot \det V = \det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 2 & 4 & \ldots & 2^{p-1} \\ \ldots & \ldots & \ldots & \ldots \\ p-1 & (p-1)^2 & \ldots & (p-1)^{p-1} \end{pmatrix} \equiv \\ & \equiv \det \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 2 & 4 & \ldots & 2^{p-2} & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ p-1 & (p-1)^2 & \ldots & (p-1)^{p-2} & 1 \end{pmatrix} = \\ & = (-1)^{p-2} \det V = -\det V \pmod{p}. \end{aligned}$$

Obzirom da $p \nmid \det V$, slijedi

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

tj. slijedi Wilsonov teorem za neparne proste brojeve. Slučaj $p = 2$ se jednostavno provjeri. □

Zadatak 1. *Dokažite da za svaki prost broj p vrijedi*

$$(p-2)! \equiv 1 \pmod{p}.$$

Rješenje. Prema Wilsonovom teoremu je

$$(p-1)!+1 \equiv 0 \pmod{p}.$$

Dalje imamo redom,

$$(p-2)!\cdot(p-1)+1 \equiv 0 \pmod{p},$$

$$(p-2)!\cdot p-(p-2)!+1 \equiv 0 \pmod{p},$$

$$p\cdot(p-2)!-\big((p-2)!-1\big) \equiv 0 \pmod{p},$$

$$(p-2)!-1 \equiv 0 \pmod{p},$$

$$(p-2)! \equiv 1 \pmod{p}.$$

Zadatak 2. *Dokažite da za svaki prost broj p vrijedi*

$$(p!)^2-p^2 \equiv 0 \pmod{p^3}.$$

Rješenje. Kako je

$$\begin{aligned} & (p!)^2-p^2=(p!+p)(p!-p)= \\ = \;& \big(p(p-1)!+p\big)\big(p(p-1)!-p\big)= \\ = \;& p^2\big((p-1)!+1\big)\big((p-1)!-1\big), \end{aligned}$$

a prema Wilsonovom teoremu je $(p-1)!+1 \equiv 0 \pmod{p}$, to je

$$(p!)^2-p^2 \equiv 0 \pmod{p^3}.$$

Zadatak 3. *Dokažite da za svaki prost broj p i svaki cijeli broj a vrijedi*

$$a^p+(p-1)!\cdot a \equiv 0 \pmod{p}.$$

Rješenje. Ako je cijeli broj a djeljiv prostim brojem p, tvrdnja je očigledna. Neka cijeli broj a nije djeljiv prostim brojem p. Tada je prema malom Fermatovom teoremu

$$a^p-a \equiv 0 \pmod{p},$$

a kako je prema Wilsonovom teoremu

$$(p-1)!+1 \equiv 0 \pmod{p},$$

to je

$$a^p-a+a\big((p-1)!+1\big) \equiv 0 \pmod{p},$$

tj.

$$a^p+(p-1)!\cdot a \equiv 0 \pmod{p}.$$

Zadatak 4. *Neka su p i q različiti prosti brojevi. Dokažite da je*

$$q \cdot 2q \dots (p-1)q \equiv -1 \pmod{p}.$$

Rješenje. Prema malom Fermatovom teoremu je

$$q^{p-1} \equiv 1 \pmod{p},$$

a prema Wilsonovom teoremu

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

Množenjem ovih kongruencija dobivamo

$$q^{p-1} \cdot (p-1)! \equiv -1 \pmod{p},$$

tj.

$$q \cdot 2q \cdot \dots \cdot (p-1)q \equiv -1 \pmod{p}.$$

Zadatak 5. *Neka je p prost broj veći od 2. Dokažite da je*

$$2 \cdot 4 \cdot 6 \dots (2p-2) \equiv -1 \pmod{p}.$$

Rješenje. Kako je

$$\begin{aligned} & 2 \cdot 4 \cdot 6 \dots (2p-2) = (2 \cdot 1)(2 \cdot 2)(2 \cdot 3) \dots \big(2 \cdot (p-1)\big) = \\ = \quad & 2^{p-1} \cdot \big(1 \cdot 2 \cdot 3 \dots (p-1)\big) = 2^{p-1} \cdot (p-1)!, \end{aligned}$$

a 2 i p su različiti prosti brojevi, to je prema zadatku 4

$$2 \cdot 4 \cdot 6 \dots (2p-2) \equiv -1 \pmod{p}.$$

Zadatak 6. *Odredite sve neparne prirodne brojeve n sa svojstvom*

$$n^2 \nmid (n-1)!.$$

Rješenje. Ako n možemo zapisati u obliku $n = ab$, gdje je $a \geq 3$, $b \geq 3$, $a \neq b$, onda se u produktu $1 \cdot 2 \dots (n-1)$ nalaze faktori $a, 2a$ i $b, 2b$, pa je stoga $(n-1)!$ djeljiv sa $a^2b^2 = n^2$.

Neka je sada $n = p^2$, gdje je p prost broj. Kako za sve proste brojeve p, $p \geq 5$ vrijedi nejednakost $p^2 - 1 > 4p$, to se u produktu $1 \cdot 2 \cdot 3 \dots (p^2-1)$ nalaze faktori $p, 2p, 3p$ i $4p$ pa je $(p^2-1)!$ djeljiv sa $p^4 = n^2$. Za $p = 3$ je $n = 9$, a broj $(9-1)! = 8!$ je djeljiv sa 9, ali nije sa 81.

Konačno, neka je n prost broj. Tada je prema Wilsonovom teoremu $(n-1)! + 1$ djeljivo sa n pa $(n-1)!$ nije djeljivo sa n, a onda ni sa n^2. Dakle, samo za proste brojeve n i za $n = 9$ broj $(n-1)!$ nije djeljiv sa n^2.

Zadatak 7. *Dokažite da za svaki prost broj $p = 4k + 1$, $k \in \mathbb{N}$, vrijedi*

$$\big((2k)!\big)^2 + 1 \equiv 0 \pmod{p}.$$

Rješenje. Izmnoživši očigledne kongruencije

$$\begin{aligned} 1 &\equiv 1 \pmod{p} \\ 2 &\equiv 2 \pmod{p} \\ &\dots \\ 2k &\equiv 2k \pmod{p} \\ 2k+1 &\equiv -2k \pmod{p} \\ 2k+2 &\equiv -(2k-1) \pmod{p} \\ &\dots \\ 4k &\equiv -1 \pmod{p} \end{aligned}$$

dobivamo redom

$$\begin{aligned} (4k)! &\equiv (-1)^{2k}\big((2k)!\big)^2 \pmod{p}, \\ (4k)! &\equiv \big((2k)!\big)^2 \pmod{p}, \\ (4k)!+1 &\equiv \big((2k)!\big)^2 + 1 \pmod{p}. \end{aligned}$$

Kako je $p = 4k + 1$ prost broj, to je prema Wilsonovom teoremu

$$(4k)! + 1 \equiv 0 \pmod{p},$$

pa je

$$\big((2k)!\big)^2 + 1 \equiv 0 \pmod{p}.$$

Zadatak 8. *Dokažite da su brojevi p i $p + 2$ susjedni prosti brojevi ako i samo ako je*

$$4\big((p-1)! + 1\big) + p \equiv 0 \pmod{p(p+2)}.$$

Dokažite.

Rješenje. Ako pomnožimo obje strane kongruencije $p \equiv -2 \pmod{p+2}$ sa $p + 1$, imamo redom

$$\begin{aligned} p(p+1) &\equiv -2(p+1) \pmod{p+2}, \\ p(p+1) &\equiv -2(p+2)+2 \pmod{p+2}, \\ p(p+1) &\equiv 2 \pmod{p+2}. \end{aligned}$$

Ako pomnožimo obje strane posljednje kongruencije sa $(p-1)! \cdot 2$, dobivamo

$$(p-1)! \cdot p \cdot (p+1) \cdot 2 \equiv (p-1)! \cdot 4 \pmod{p+2},$$

tj.

$$(p+1)! \cdot 2 \equiv (p-1)! \cdot 4 \pmod{p+2}.$$

Dodamo objema stranama $4+p$:

$$(p+1)!\cdot 2+2+(p+2)\equiv (p-1)!\cdot 4+4+p \pmod{p+2},$$

$$2\big((p+1)!+1\big)+(p+2)\equiv 4\big((p-1)!+1\big)+p \pmod{p+2}. \tag{1}$$

Pretpostavimo da su p i $p+2$ prosti brojevi. Prema Wilsonovom teoremu je

$$(p+1)!+1\equiv 0 \pmod{p+2},$$

pa je

$$2\big((p+1)!+1\big)+(p+2)\equiv 0 \pmod{p+2}.$$

Stoga je, zbog (1),

$$4\big((p-1)!+1\big)+p\equiv 0 \pmod{p+2}. \tag{2}$$

Prema Wilsonovom teoremu je i

$$(p-1)!+1\equiv 0 \pmod{p}.$$

Pomnožimo li članove te kongruencije sa 4 i pribrojimo očiglednoj kongruenciji $p\equiv 0 \pmod{p}$, dobivamo

$$4\big((p-1)!+1\big)+p\equiv 0 \pmod{p}. \tag{3}$$

Sada iz (2) i (3) prema svojstvu kongruencije imamo

$$4\big((p-1)!+1\big)+p\equiv 0 \pmod{p(p+2)}. \tag{4}$$

Obratno, ako vrijedi (4), tada vrijedi i (2) odakle zbog (1) dobivamo

$$2\big((p+1)!+1\big)\equiv 0 \pmod{p+2},$$

odnosno

$$(p+1)!+1\equiv 0 \pmod{p+2},$$

a to prema Wilsonovom teoremu znači da je $p+2$ prost broj. Ako je $p<5$, tada je jedina mogućnost $p=3$, a to je prost broj. Zato bez smanjenja općenitosti pretpostavljamo da je $p\geq 5$. Iz (4) slijedi (3), pa je

$$4\big((p-1)!+1\big)\equiv 0 \pmod{p},$$

odakle je

$$(p-1)!+1\equiv 0 \pmod{p},$$

pa je p prost prema Wilsonovom teoremu.

Zadatak 9. *Dokažite da za sve prirodne brojeve n i sve proste brojeve p za koje je $n!\equiv(-1)^n \pmod{p}$ vrijedi*

$$(p-n-1)!+1\equiv 0 \pmod{p}.$$

Rješenje. Množenjem kongruencija

$$\begin{aligned} p-1 &\equiv -1 \pmod p,\\ p-2 &\equiv -2 \pmod p,\\ &\dots\\ p-n &\equiv -n \pmod p \end{aligned}$$

dobivamo

$$(p-1)(p-2)\dots(p-n) \equiv (-1)^n \cdot n! \pmod p. \tag{5}$$

Prema Wilsonovom teoremu je

$$(p-1)! + 1 \equiv 0 \pmod p,$$

tj.

$$(p-1)(p-2)\dots(p-n)(p-n-1)! + 1 \equiv 0 \pmod p$$

što zbog (5) postaje

$$(-1)^n \cdot n! \cdot (p-n-1)! + 1 \equiv 0 \pmod p.$$

Zbog uvjeta zadatka konačno dobivamo

$$(p-n-1)! + 1 \equiv 0 \pmod p.$$

Zadatak 10. *Neka je p neparan prost broj. Dokažite da je*

(a) $1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$,

(b) $2^2 \cdot 4^2 \cdot 6^2 \dots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$.

Rješenje. Neka je p neparan prost broj. Prema Wilsonovom teoremu vrijedi

$$1 \cdot 2 \cdot 3 \dots (p-1) \equiv -1 \pmod p. \tag{6}$$

Za svaki cijeli broj k vrijedi kongruencija

$$k \equiv -(p-k) \pmod p. \tag{7}$$

(a) Zamijenimo $\frac{p-1}{2}$ parnih brojeva na lijevoj strani kongruencije (6) brojevima koji su njima kongruentni po modulu p, a dobijemo ih iz (7) za $k = 2, 4, 6, \dots, p-1$. Grupiranjem jednakih faktora dobivamo

$$1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \cdot (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

tj.

$$1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p,$$

što je i trebalo dokazati.

(b) Analogno na lijevoj strani kongruencije (6) zamijenimo $\frac{p-1}{2}$ neparnih brojeva brojevima kongruentnim njima po modulu p, koje dobijemo iz (7) za $k = 1, 3, 5, \ldots p-2$. Grupiranjem jednakih faktora dobivamo

$$2^2 \cdot 4^2 \cdot 6^2 \ldots (p-1)^2 \cdot (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

tj.

$$2^2 \cdot 4^2 \cdot 6^2 \ldots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Zadatak 11. *Ako je $a+b+1$ prost broj, onda je bar jedan od brojeva $a! \cdot b! + 1$, $a! \cdot b! - 1$ djeljiv sa $a+b+1$.*

Rješenje. Neka je $a+b+1 = p$ prost broj. Tada je prema Wilsonovom teoremu $(a+b)! + 1$ djeljiv sa $a+b+1$. Kako je $(a+b)! = a! \cdot b! \cdot \binom{a+b}{a}$, to je $a! \cdot b! \cdot \binom{a+b}{a} + 1$ djeljiv sa $a+b+1$. Dalje je

$$\binom{a+b}{a} = \binom{p-1}{a} = \frac{(p-1)(p-2)\ldots(p-a)}{a!}.$$

Obzirom da je (vidjeti (5) iz rješenja zadatka 9)

$$(p-1)(p-2)\ldots(p-a) \equiv (-1)^a \cdot a! \pmod{p},$$

imamo

$$\binom{p-1}{a} \equiv (-1)^a \pmod{p}$$

odnosno

$$\binom{a+b}{a} \equiv (-1)^a \pmod{a+b+1}.$$

Slijedi

$$\binom{a+b}{a}^2 \equiv 1 \pmod{a+b+1}.$$

Kako je

$$(a+b)! \equiv -1 \pmod{a+b+1},$$

to je

$$\big((a+b)!\big)^2 \equiv \binom{a+b}{a}^2 \pmod{a+b+1}.$$

Odatle dijeljenjem sa $\binom{a+b}{a}^2$ dobijemo

$$(a! \cdot b!)^2 \equiv 1 \pmod{a+b+1},$$

pa je $(a! \cdot b! + 1)(a! \cdot b! - 1) = (a! \cdot b!)^2 - 1$ djeljivo prostim brojem p. Stoga je bar jedan od faktora djeljiv s p.

Literatura

[1] A. A. BUHŠTAB, *Teorija čisel*, Prosveščenie, Moskva, 1966.

[2] U. S. DAVIDOV, Š. ZNAM, *Teoria čisel*, SPN, Bratislava, 1972.

[3] V. U. GRIBANOV, P. I. TITOV, *Sbornik upražnenii po teorii čisel*, Prosveščenie, Moskva, 1964.

[4] D. O. SHKLYARSKY, N. N. CHENTSOV, I. M. YAGLOM, *Selected Problems and Theorems in Elementary Mathematics, Arithmetic and Algebra*, Mir Publishers, Moscow, 1979.

[5] Š. ZNAM, *Teoria čisel*, Alfa, Bratislava, 1986.