Kongruencije

Azra Tafro

Uvod

Primjer 1. Odredi sve peteroznamenkaste brojeve $\overline{47a9b}$ koji su djeljivi s brojem 18.
Rješenje. Ako je broj djeljiv s 18 tada je djeljiv s 2 i s 9. Iz djeljivosti s 2 slijedi da je znamenka b jednaka 0,2,4,6 ili 8. Ako je $b = 0$, tada zbog djeljivosti s 9 i zbroj $4 + 7 + a + 9 + 0$ mora biti djeljiv s 9, tj. $a = 7$. Ako je $b = 2$, tada je $a = 5$. Ako je $b = 4$, tada je $a = 3$. Ako je $b = 6$, tada je $a = 1$. Ako je $b = 8$, tada je $a = 8$. Dakle, traženi brojevi su 47790, 47592, 47394, 47196, 47898. ■

Ovaj zadatak zadan je na općinskom natjecanju 2000. godine učenicima petih razreda. Uočavamo da čak i u ovako jednostavnom zadataku iz područja teorije brojeva koristimo neke 'općepoznate' tvrdnje, recimo onu da je broj djeljiv s 9 ako i samo ako mu je i zbroj znamenki djeljiv s 9. Ipak, da pitamo nekog osnovnoškolca zašto je to tako, on vjerojatno ne bi znao odgovor. Odgovor na takva pitanja daje **teorija kongruencija**, specifična algebra unutar teorije brojeva, koja je razvila poseban jezik za rješavanje problema o djeljivosti brojeva. Osim definicije i osnovnih svojstava kongruencija, u ovom članku navedeni su i neki blisko povezani teoremi i funkcije, kao što su Eulerova funkcija te Eulerov i (mali) Fermatov teorem. Uz pomoć njih postiže se krajnji cilj, a to je rješavanje kongruencija, linearnih kongruencija i sustava kongruencija. Dokazani su i neki drugi teoremi vezani uz djeljivost brojeva. Gotovo svaka tvrdnja popraćena je riješenim primjerima i zadacima. Mnogo je matematičara dalo značajan doprinos ovom području matematike , ali nijednog ne bismo mogli posebno istaknuti, pripisati mu zasnivanje ili otkrivanje ove zanimljive teorije. Ipak, valja napomenuti da je kongruencije kao pojam prvi uveo veliki njemački matematičar *Gauss*[1] u svom čuvenom djelu "*Disquisitiones Arithmeticae*" 1801. godine.

Pojam kongruencije

Definicija 1. Ako za cijele brojeve a, b te prirodan broj m vrijedi da m dijeli razliku $a - b$ onda to možemo zapisati u slijedećem obliku: $a \equiv b \pmod{m}$.

Ovaj zapis zovemo kongruencijom, broj m njezinim modulom, a zapis čitamo a je kongruentno s b modulo m. Naravno, zapis je ekvivalentan ovima: $m|(a - b)$ ili $a - b = mk$, gdje je k cijeli broj.

Primjer 2. Navedimo nekoliko primjera kongruencija:

$$38 \equiv 14 \pmod{6}, \text{ jer je } 38 - 14 = 24 = 6 \cdot 4,$$

$$75 \equiv 0 \pmod{25}, \text{ jer je } 75 - 0 = 25 \cdot 3,$$

$$-25 \equiv -1 \pmod{4} \text{ jer je } -25 - (-1) = -24 = 4 \cdot (-6),$$

$$7 \equiv -1 \pmod{4} \text{ jer je } 7 - (-1) = 8 = 2 \cdot 4,$$

$$-5 \equiv -2 \pmod{3} \text{ jer je } -5 - (-2) = 3,$$

$$17 \equiv 0 \pmod{17} \text{ jer je } 17 - 0 = 17 \cdot 1.$$

[1] **Karl Friedrich Gauss** (1777. - 1855.)

Zbog činjenice da za svaka dva cijela broja a i b vrijedi $a \equiv b \pmod 1$, u našim razmatranjima ćemo uzeti da je $m \geq 2$.
PRIMJEDBA 1. Primijetimo da $a \equiv 0 \pmod m$ znači da je a djeljivo sa m. Kongruencije se najčešće koriste da se dokaže da nešto jest ili nije djeljivo.

Svojstva kongruencija

Način na koji zapisujemo kongruencije uvelike podsjeća na jednakosti, a pokazat ćemo da jednakosti i kongruencije imaju mnoga zajednička svojstva.

Teorem 1. Za cijele brojeve[2] a, b i c i prirodan broj m uvijek vrijedi:

1. $a \equiv a \pmod m$ (refleksivnost);
2. $a \equiv b \pmod m \Leftrightarrow b \equiv a \pmod m$ (simetričnost);
3. $a \equiv b \pmod m$ i $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ (tranzitivnost).

Dokaz. 1. $a - a = 0 = 0 \cdot m$; 2. $a - b = m \cdot k \Leftrightarrow b - a = m \cdot (-k)$; 3. $a - b = m \cdot k_1$ i $b - c = m \cdot k_2 \Rightarrow a - c = m \cdot (k_1 + k_2)$. ■

Teorem 2. $a \equiv b \pmod m$ i $c \equiv d \pmod m \Rightarrow$

1. $a + c \equiv b + d \pmod m$;
2. $a - c \equiv b - d \pmod m$;
3. $ac \equiv bd \pmod m$;
4. $ka \equiv kb \pmod m$.

Dokaz. 1. i 2. $a - b = m \cdot k_1$ i $c - d = m \cdot k_2 \Rightarrow (a \pm c) - (b \pm d) = m \cdot (k_1 \pm k_2)$; 3. $m^2 \cdot (k_1 k_2) = (a-b)(c-d) = ac - bc - ad + bd = ac - bd - bc + bd - ad + bd = ac - bd - b(c-d) - d(a-b) = ac - bd - m \cdot (dk_1) - m \cdot (bk_2) \Rightarrow ac - bd = m \cdot (m(k_1 k_2) + dk_1 + bk_2)$; Uzmimo $b = c = k$ tada iz 3. izravno slijedi 4. ■

PRIMJEDBA 2. Primijetimo da vrijedi

$$a \equiv a + mk \pmod m$$

gdje je $k \in \mathbb{Z}$.

Primjer 3. Pogledajmo sljedeće kongruencije:

$$7 \equiv 7 - 2 \equiv 7 - 2 \cdot 2 \equiv 7 - 3 \cdot 2 \equiv 1 \pmod 2,$$

$$19 \equiv 10 \equiv 1 \pmod 9.$$

Za kongruencije dakle vrijede svojstva asocijativnosti, komutativnosti i distributivnosti te ih možemo zbrajati, oduzimati i množiti, ali samo one s istim modulom, pri čemu modul ostaje nepromijenjen. Važno je napomenuti da se kongruencije ne mogu proizvoljno kratiti, odnosno dijeliti. Uzmimo kao primjer kongruenciju $20 \equiv 30 \pmod 5$, iz koje bismo kraćenjem s 10 dobili $2 \equiv 3 \pmod 5$, što očito nije točno jer 5 ne dijeli $2 - 3 = -1$. Stoga pri kraćenju vrijedi sljedeći teorem.

[2]Svi brojevi koji će se pojavljivati u ovom članku biti će cijeli (a, b, c, d, k), te to više nećemo napominjati.

Teorem 3. $k \cdot a \equiv k \cdot b \pmod{m}$ i $\mathrm{nzd}(k,m) = d \Rightarrow a \equiv b \pmod{\frac{m}{d}}$. *Dokaz.* Ako je $\mathrm{nzd}(k,m) = d$, onda $ml = k(a-b) \Leftrightarrow \frac{m}{d}l = \frac{k}{d}(a-b)$. Kako je $\mathrm{nzd}\left(\frac{m}{d}, \frac{k}{d}\right) = 1 \Rightarrow \frac{m}{d}l_1 = (a-b)$. ■

Primjer 4. Uzmimo kongruenciju $120 \equiv 45 \pmod{15}$. Sada računamo $\mathrm{nzd}(120, 45) = 15$, a $\mathrm{nzd}(15, 15) = 1$, pa cijelu kongruenciju možemo skratiti i dobiti slijedeći izraz: $8 \equiv 3 \pmod{1}$, što je točno.

Teorem 4. Brojevi a i b imaju isti ostatak pri dijeljenju s brojem m ako i samo ako je $a \equiv b \pmod{m}$. *Dokaz.* Neka je $a = mq_1 + r_1, (0 \leq r_1 \leq m-1)$ i $b = mq_2 + r_2, (0 \leq r_2 \leq m-1)$. Ako je $r_1 = r_2$ onda je $a - b = m(q_1 - q_2)$. Ako je $a \equiv b \pmod{m}$ onda vrijedi $mk = a - b = m(q_1 - q_2) + (r_1 - r_2) \Rightarrow -(m-1) \leq r_1 - r_2 = m(k - q_1 + q_2) \leq m - 1 \Rightarrow r_1 = r_2$ jer je 0 jedini cijeli broj djeljiv s m na intervalu $[-(m-1), m-1]$. ■

Teorem 5. Ako je $a \equiv b \pmod{m}$ i n prirodan broj onda vrijedi $a^n \equiv b^n \pmod{m}$.
Dokaz. Neka je $a - b = m \cdot k$. Znamo da je

$$a^n - b^n = (a-b)\underbrace{(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1})}_{A} = mkA$$

$\Rightarrow a^n \equiv b^n \pmod{m}$. ■

Zadatak 1. Ako je f polinom s cjelobrojnim koeficijentima i $a \equiv b \pmod{m}$, tada je $f(a) \equiv f(b) \pmod{m}$.
Rješenje. Neka je $f(x) = c_n x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0$, gdje su $cn, \ldots, c0$ cijeli brojevi , polinom n-tog stupnja. Dobivamo

$$a \equiv b \pmod{m} \Rightarrow a^j \equiv b^j \pmod{m} \Rightarrow c_j a^j \equiv c_j b^j \pmod{m}.$$

Ako zbrojimo ove kongruencije (za $j = 1, \ldots, n$), dobit ćemo:

$$f(a) \equiv f(b) \pmod{m}.$$

■

Zadatak 2. Dokažite da je broj djeljiv s 9 ako je zbroj njegovih znamenki djeljiv s 9.
Rješenje. Uzmimo neki m, i neka on ima decimalni prikaz

$$m = c_n 10^n + c_{n-1}10^{n-1} + \cdots + c_0.$$

Promotrimo polinom

$$f(x) = c_n x^n + \cdots + c_0.$$

Tada je $f(10) = m$. No zbroj znamenki od m je $f(1)$. Kako je $10 \equiv 1 \pmod{9}$, tada slijedi (vidi prethodni zadatak) $f(10) \equiv f(1) \pmod{9}$. Odavde slijedi da su oba broja $f(10)$ i $f(1)$ istodobno ili djeljiva ili nisu djeljiva s 9, i tvrdnja je dokazana. ■

Zadatak 3. Nađite kriterij djeljivosti s 11.
Rješenje. Uzmimo m kao u prethodnom zadatku. $10 \equiv -1 \pmod{11} \Rightarrow f(10) \equiv f(-1) \pmod{11}$. No, $f(-1)$ je alternirana suma znamenaka pa imamo ovaj kriterij: broj je djeljiv s 11 ako i samo ako je njegova alternirana suma znamenaka djeljiva s 11, odnosno ako i samo ako je razlika zbroja

znamenaka na parnim mjestima i zbroja znamenaka na neparnim mjestima djeljiva s 11. Npr. 121 je djeljiv s 11 jer je $1-2+1=0=0\cdot 11$. ■

Napomena: U mnogim računalnim programima postoji naredba mod koja ima slično značenje kao i ovdje. Ona izbacuje ostatak pri dijeljenju broja a s brojem b, tj. a mod b daje c.

Eulerova funkcija

Broj članova niza $1, 2, 3, \ldots, m$ koji su relativno prosti s brojem m označavamo s $\varphi(m)$. Na taj smo način dobili (*brojevnu* ili *aritmetičku*) funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ koja je definirana s $m \to \varphi(m)$. Tu funkciju zovemo Eulerovom[3] funkcijom i ona igra važnu ulogu u teoriji brojeva.
Primjerice, $\varphi(10) = 4$, jer su u nizu

$$\mathbf{1}, 2, \mathbf{3}, 4, 5, 6, \mathbf{7}, 8, \mathbf{9}, 10,$$

deblje otisnuti (**bold**) brojevi relativno prosti s 10. Iz same definicije funkcije slijedi da za svaki prosti broj p vrijedi $\varphi(p) = p - 1$, jer su u nizu

$$1, 2, \ldots, p-1, p$$

svi brojevi osim p relativno prosti s p, a njih ima točno $p-1$. Navedimo prvih nekoliko vrijednosti funkcije $\varphi(n)$.

n	1	2	3	4	5	6	7	8
$\varphi(n)$	1	1	2	2	4	2	6	4

Da bismo pak odredili vrijednost funkcije za složene brojeve, koristimo *multiplikativno* svojstvo funkcije φ koje je dano ovim teoremom:

Teorem 6. $m, n \in \mathbb{N}$ $\mathrm{nzd}(m,n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.
Dokaz. Da odredimo $\varphi(mn)$, korisno je brojeve od 1 do $m \cdot n$ razvrstati u sljedeću tablicu:

$$\begin{array}{ccccccc}
1 & 2 & \ldots & k & \ldots & m \\
m+1 & m+2 & \ldots & m+k & \ldots & 2m \\
2m+1 & 2m+2 & \ldots & 2m+k & \ldots & 3m \\
\vdots & \vdots & & \vdots & & \vdots \\
(n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+k & \ldots & nm
\end{array}$$

Da bi neki broj bio relativno prost s umnoškom mn, on mora biti relativno prost i s m i s n (jer su m i n relativno prosti po pretpostavci teorema). Prema tome, iz tablice možemo odrediti brojeve relativno proste s m i relativno proste s n. Vidimo da u istom stupcu imamo brojeve koji pri dijeljenju s m daju isti ostatak. Dakle, brojevi u istom stupcu ili svi jesu relativno prosti s m ili nijedan nije relativno prost s m. Prema tome, stupaca u kojima su brojevi relativno prosti s m ima $\varphi(m)$.

Uzmimo sada jedan od tih $\varphi(m)$ stupaca, recimo da je to k-ti. On je sastavljen od brojeva:

$$k, m+k, 2m+k, ..., (n-1)m+k.$$

Pokažimo da svaki od tih brojeva daje različit ostatak pri dijeljenju s n. Naime, kada bi dva broja $mx_1+k, mx_2+k,\ x_1, x_2 \in \{0, 1, ..., n-1\}$, $(x_1 \neq x_2)$ davala isti ostatak pri dijeljenju s n, imali bismo

[3] **Leonhard Euler** (1707.-1783.)– vidi prošli broj.

da je $mx_1 + k \equiv mx_2 + k \pmod{n}$, odnosno da je $mx_1 \equiv mx_2 \pmod{n}$. Kako je $\mathrm{nzd}(m, n) = 1$, to bi prema teoremu 3 odavde slijedilo:

$$x_1 \equiv x_2 \pmod{n},$$

što je nemoguće jer razlika dvaju različitih brojeva iz skupa $\{0, 1, \ldots, n-1\}$ nije nikad djeljiva s n.

Sada možemo uočiti i opće pravilo: Ako je $a = nq+r$, $(0 \leq r \leq n-1)$ tada je $\mathrm{nzd}(a, n) = \mathrm{nzd}(r, n)$. Ova činjenica se vrlo lako dokazuje. Broj relativno prostih brojeva s n u k-tom stupcu je $\varphi(n)$ zato što u tom stupcu brojevi imaju ostatke od 0 do $n-1$ pri dijeljenju s n. A broj ostataka relativno prostih s n jednak je $\varphi(n)$. Znači, ukupni broj brojeva relativno prostih s mn je $\varphi(m) \cdot \varphi(n)$. Tj. $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. ■

Primjer 5. Provjerimo $\varphi(10) = 4$. Koristeći multiplikativno svojstvo funkcije φ dobivamo

$$\varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4.$$

Teorem 7. Za prosti broj p vrijedi da je $\varphi(p^a) = p^{a-1}(p-1)$.
Dokaz. Složimo brojeve na sljedeći način u sljedeću tablicu:

$$\begin{array}{cccc} 1 & 2 & \ldots & p \\ p+1 & p+2 & \ldots & 2p \\ \vdots & \vdots & & \vdots \\ kp+1 & kp+2 & & (k+1)p \\ \vdots & \vdots & & \vdots \\ (p^a-1)p+1 & (p^a-1)p+2 & & p^{a-1} \cdot p \end{array}$$

U svakom redu ima $p-1$ broj relativno prost s p (svi osim zadnjeg). A redova ima p^{a-1} što znači da je ukupan broj brojeva u tablici relativno prostih s p jednak $p^{a-1}(p-1)$. Tj.

$$\varphi(p^a) = p^{a-1}(p-1).$$

■

Teorem 8. Ako je $m = p_1^{a_1} p_1^{a_2} \ldots p_i^{a_i}$ (*kanonski*) rastav prirodnog broja m na proste faktore, onda vrijedi

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_i}\right).$$

Dokaz. Iz teorema 6. slijedi:

$$\varphi(m) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \ldots \varphi(p_i^{a_i}).$$

Iz toga koristeći teorem 7., dobivamo

$$\varphi(m) = p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right) \ldots p_i^{a_i}\left(1 - \frac{1}{p_i}\right) =$$

$$= m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_i}\right).$$

■

Zadatak 4. Odredimo $\varphi(120)$.
Rješenje. Najprije rastavimo 120 na proste faktore: $120 = 2^3 \cdot 3 \cdot 5$. Sada je $\varphi(120) = 120(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 32$. ■

Zadatak 5. Izračunaj $\varphi(10!)$.
Rješenje. Ako 10! rastavimo na proste faktore, dobit ćemo $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.
Sada vrijedi:

$$j(10!) = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 829440.$$

■

Eulerov i Fermatov teorem

Teorem 9. Ako je $\mathrm{nzd}(a, m) = 1$, vrijedi $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Dokaz. Neka je m prirodan broj i neka x poprima vrijednosti iz skupa

$$S = \{r_1, r_2, \ldots, r_s\},\ s = \varphi(m),$$

gdje je S skup brojeva relativno prostih s m i manjih od m. Tada je

$$ar_i \equiv r_i' \pmod{m},\ 0 \leq r_i' \leq m - 1$$

slijedi da je $r_i' \in S$. Kad bi bilo suprotno, to bi značilo da je $\mathrm{nzd}(r_i', m) = d > 1$, odnosno da je $ar_i - r_i' = mk$, iz čega slijedi da je ar_i djeljivo s d, što je nemoguće jer je $\mathrm{nzd}(ar_i, m) = 1$. Za svaki $i \neq j$ vrijedi da je $r_i' \neq r_j'$. Pretpostavimo suprotno, tj. da postoje i, j takvi da je $r_i' = r_j'$. Tad iz

$$ar_i \equiv r_i' \pmod{m},$$

$$ar_j \equiv r_j' \pmod{m},$$

po svojstvu tranzitivnosti slijedi

$$ar_i \equiv ar_j \pmod{m},$$

što iz definicije povlači $a(r_i - r_j) = mk$. Budući da je a relativno prost s m, slijedi da je $-m < r_i - r_j < m$ djeljiv s m, što povlači $r_i = r_j$. Kontradikcija! Tada brojevi ax čine isti takav skup, samo u drugom redoslijedu $r_1', r_2', ..., r_s'$. Odavde slijedi

$$ar_1 \equiv r_1' \pmod{m},$$

$$ar_2 \equiv r_2' \pmod{m},$$

$$\vdots$$

$$ar_s = r_s' \pmod{m}.$$

Pomnožimo li ove jednakosti, dobivamo

$$a^s r_1 r_2 \ldots r_s \equiv r_1' r_2' \ldots r_s' \pmod{m},$$

odnosno

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

■

Iz Eulerovog teorema izravno slijedi tzv. mali Fermatov teorem.

Teorem 10. Ako je p prost broj i ako su a i p relativno prosti, onda vrijedi $a^{p-1} \equiv 1 \pmod{p}$.
Dokaz. Tvrdnja odmah slijedi iz činjenice da za svaki prosti broj p vrijedi $\varphi(p) = p - 1$. ■
PRIMJEDBA 3. Primijetimo da obrat Fermatovog teorema ne vrijedi, odnosno iz $\mathrm{nzd}(a, m)$ i $a^{n-1} \equiv 1 \pmod{m}$ ne slijedi da je m prost. Primjerice, $2^{340} \equiv 1 \pmod{341}$, $\mathrm{nzd}(2, 341) = 1$, ali $341 = 31 \cdot 11$.

Primjer 6. Nađite ostatak pri dijeljenju 2^{30} s 7.
Rješenje. Po malom Fermatovom teoremu vrijedi $2^6 \equiv 1 \pmod{7}$, iz čega slijedi $2^{30} = (2^6)^5 \equiv 1^5 \equiv 1 \pmod{7}$. Znači, ostatak pri dijeljenju je 1. ■

Zadatak 6. Dokaži da postoji beskonačno mnogo potencija broja 7893 koje završavaju na $\underbrace{0\ldots0}_{8}1$.

Dokaz. Zapišimo našu tvrdnju u obliku kongruencija. Tvrdimo da postoji beskonačno brojeva x takvih da je $7893^x \equiv 1 \pmod{10^9}$. Po Eulerovom teoremu znamo da je $x = \varphi(10^9)$ jedan takav broj. Po svojstvu kongrencija također vrijedi da je $x = k\varphi(10^9)$, $k \in \mathbb{Z}$ također takav broj. ■

Zadatak 7. Za svaki neparan broj n vrijedi da je $2^{n!} - 1$ djeljivo s n. ($n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$)
Rješenje. Broj $\varphi(n) \leq n - 1$, što znači da je $n!$ djeljivo s $\varphi(n)$. Iz toga slijedi $2^{n!} = \left(2^{\varphi(n)}\right)^{\frac{n!}{\varphi(n)}} \equiv 1^{\frac{n!}{\varphi(n)}} = 1 \pmod{n}$. ■

Zadaci za vježbu

1. Dokažite da je za svaki prosti broj p broj $(a+b)^p - a^p - b^p$ djeljiv s p.
2. Neka je a_i ostatak pri dijeljenju broja i^p ($i \in \mathbb{N}$) s p. Dokaži da je
$$a_1 + a_2 + a_3 + \cdots + a_{p-1} = \frac{p(p-1)}{2}.$$
3. Dokažite: ako je $10 | a_1 + a_2 + \cdots + a_{2003}$ onda je $10 | a_1^5 + \cdots + a_{2003}^5$.
4. Dokaži: ako prost broj p dijeli dijeli $a^p - 1$ za neki $a \in \mathbb{N}$, tada p^2 također dijeli $a^p - 1$.
5. Neka su a, b, c cijeli brojevi i m prirodan broj veći od 1. Ako je
$$a^n + bn + c \equiv 0 \pmod{m}$$
za svaki prirodan broj n, dokaži da je $b^2 \equiv 0 \pmod{m}$.

UPUTE I RJEŠENJA NA STRANICI 45.

ZAPAMTITE!

- *Kongruencije* su vrlo važne i korisne ne samo u matematici nego i u šifriranju, informatici,... O tome ćete čitati u sljedećim brojevima (a nešto i u ovom). Dobro je zapamtiti i njihova svojstva.
- *Mali Fermatov teorem* jedan je od važnijih teorema u teoriji brojeva, iako je samo specijalni slučaj Eulerovog teorema.
- *Eulerov teorem* je također važan, uz njega valja zapamtiti i *Eulerovu* funkciju!