## UVOD U TEORIJU BROJEVA

Treće predavanje - 17.10.2011.

### Kongruencije

Teoriju kongruencija (i oznaku za kongruenciju) uveo je **Carl Friedrich Gauss** (1777-1855) - jedan od najvećih matematičara svih vremena.

**Definicija 2.1.** Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, kažemo da je $a$ **kongruentan** $b$ **modulo** $m$ i pišemo $a \equiv b \pmod{m}$. U protivnom, kažemo da $a$ nije kongruentan $b$ modulo $m$ i pišemo $a \not\equiv b \pmod{m}$.

Primijetimo da je $a - b$ djeljivo s $m$ ako i samo ako je djeljivo s $-m$ pa, bez smanjenja općenitosti, možemo uzeti da je modul $m$ prirodan broj.

Kongruencije imaju mnoga svojstva zajednička s jednakostima. Neka svojstva kongruencija dana su u narednim propozicijama.

**Propozicija 2.1.** Relacija "biti kongruentan modulo $m$" je relacija ekvivalencije na skupu $\mathbb{Z}$.

*Dokaz:* Na vježbama.

**Propozicija 2.2.** Neka su $a, b, c, d$ cijeli brojevi.
*(1)* Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, tada je $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
*(2)* Ako je $a \equiv b \pmod{m}$ i $d|m$, tada je $a \equiv b \pmod{d}$.
*(3)* Ako je $a \equiv b \pmod{m}$, tada je $ac \equiv bc \pmod{mc}$ za svaki $c \neq 0$.

*Dokaz:*
*(1)* Vrijedi $a-b = mk$ i $c-d = ml$, gdje su $k, l \in \mathbb{Z}$. Sada je $(a+c)-(b+d) = m(k + l)$ i $(a - c) - (b - d) = m(k - l)$. Dakle, vrijedi $a + c \equiv b + d \pmod{m}$ i $a - c \equiv b - d \pmod{m}$. Jednostavnom transformacijom dobivamo $ac - bd = a(c - d) + d(a - b) = m(al + dk)$ pa slijedi da je $ac \equiv bd \pmod{m}$.
*(2)* Kako $d|m$, slijedi da postoji cijeli broj $e$ takav da je $m = de$. Sada, iz $a - b = mk$, dobivamo $a - b = d \cdot (ek)$ pa zaključujemo da vrijedi $a \equiv b \pmod{d}$.
*(3)* Iz $a - b = mk$, množenjem s proizvoljnim nenul cijelim brojem $c$ dobi-

vamo $ac - bc = (mc) \cdot k$. Dakle, vrijedi $ac \equiv bc \pmod{mc}$. ■

**Propozicija 2.3.** Neka je $f$ polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{m}$, tada je $f(a) \equiv f(b) \pmod{m}$.

*Dokaz:* Na vježbama.

Slijedi nekoliko važnijih teorema o kongruencijama.

**Teorem 2.4.** Vrijedi $ax \equiv ay \pmod{m}$ ako i samo ako $x \equiv y \pmod{\frac{m}{(a,m)}}$. Posebno, ako je $ax \equiv ay \pmod{m}$ i $(a, m) = 1$, tada je $x \equiv y \pmod{m}$.

*Dokaz:*
Ako je $ax \equiv ay \pmod{m}$, tada postoji $z \in \mathbb{Z}$ takav da je $ax - ay = mz$. Podijelimo li tu jednakost s $(a, m)$, dobivamo $\frac{a}{(a,m)}(x - y) = \frac{m}{(a,m)}z$. Dakle, $\frac{m}{(a,m)}$ dijeli $\frac{a}{(a,m)}(x - y)$. Primijetimo da $\frac{a}{(a,m)}$ i $\frac{m}{(a,m)}$ nemaju zajedničkih djelitelja, odnosno da su relativno prosti. Dakle, $\frac{m}{(a,m)}$ dijeli $x - y$. Drugim riječima, $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Obratno, neka je $x \equiv y \pmod{\frac{m}{(a,m)}}$. Po Propoziciji 2.2. (3), vrijedi $ax \equiv ay \pmod{\frac{am}{(a,m)}}$. Jasno je da $(a, m) \mid a$. Uzmimo da je $a = (a, m)d$, gdje je $d \in \mathbb{Z}\backslash\{0\}$. Sada imamo $ax \equiv ay \pmod{md}$ pa je, po Propoziciji 2.2. (2), $ax \equiv ay \pmod{m}$. ■

**Definicija 2.2.** Skup $\{x_1, ..., x_m\}$ nazivamo **potpuni sustav ostataka modulo** $m$ ako za svaki $y \in \mathbb{Z}$ postoji točno jedan $x_j$, $j \in \{1, ..., m\}$, takav da je $y \equiv x_j \pmod{m}$. Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo $m$ uzmemo po jedan član. (Klasu ekvivalencije modulo $m$ čine svi cijeli brojevi koji su kongruentni modulo $m$ istom cijelom broju.)

Postoji beskonačno mnogo potpunih sustava ostataka modulo $m$. Jedan od njih je tzv. **sustav najmanjih nenegativnih ostataka**

$$\{0, 1, ..., m - 1\}.$$

Koji god $y \in \mathbb{Z}$ uzmemo, broj $y - x$ je djeljiv s $m$ za točno jedan $x \in \{0, 1, ..., m - 1\}$.

**Teorem 2.5.** Neka je $\{x_1, ..., x_m\}$ potpuni sustav ostataka modulo $m$ i neka je $(a, m) = 1$. Tada je i $\{ax_1, ..., ax_m\}$ potpuni sustav ostataka modulo $m$.

*Dokaz:*
Kako je $\{x_1, ..., x_m\}$ potpuni sustav ostataka modulo $m$, slijedi da je svaki $x_i$, $i = 1, ..., m$, predstavnik po jedne klase ekvivalencije modulo $m$. Nikoja dva od njih nisu iz iste klase ekvivalencije modulo $m$. Moramo pokazati da isto vrijedi i za skup $\{ax_1, ..., ax_m\}$, gdje je $(a, m) = 1$.

Ako bi neki $ax_k$ i $ax_l$, gdje je $k \neq l$ i $k, l \in \{1, ..., m\}$, bili iz iste klase ekvivalencije modulo $m$, vrijedilo bi $ax_k \equiv ax_l \pmod{m}$. Kako je $(a, m) = 1$, Teorem 2.4. povlači da je $x_k \equiv x_l \pmod{m}$, odnosno $k = l$, što je kontradikcija. ■

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Rješenje kongruencije $f(x) \equiv 0 \pmod{m}$ je svaki cijeli broj $x$ za koji ta kongruencija vrijedi.

Uzmimo da je $x_1$ rješenje ove kongruencije te neka je $x_2 \equiv x_1 \pmod{m}$. Propozicija 2.3. povlači da je i $f(x_2) \equiv f(x_1) \pmod{m}$ pa zaključujemo da je i $x_2$ rješenje polazne kongruencije.

Dva **rješenja** $x$ i $x'$ smatramo **ekvivalentnim** ako je $x \equiv x' \pmod{m}$. **Broj rješenja kongruencije** je broj neekvivalentnih rješenja.

**Teorem 2.6.** Neka su $a$ i $m$ prirodni, a $b$ cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $(a, m)|b$. Ako ovaj uvijet vrijedi, onda gornja kongruencija ima točno $(a, m)$ rješenja modulo $m$.

*Dokaz:*
Ako kongruencija $ax \equiv b \pmod{m}$ ima rješenja, tada postoji $y \in \mathbb{Z}$ takav da je $ax - b = my$. Neka je $d = (a, m)$. Iz jednakosti $ax - b = my$ slijedi da $d|b$ (jer $d|a$ i $d|m$).

Krenimo sada od toga da $d|b$. Uzmimo da je $a = da'$, $b = db'$ i $m = dm'$. Riješimo najprije kongruenciju $a'x \equiv b' \pmod{m'}$. Ta kongruencija ima točno jedno rješenje modulo $m'$. Obrazložimo. Kako je $(a', m') = 1$, slijedi da postoje cijeli brojevi $u$ i $v$ takvi da je $a'u + m'v = 1$. Pomnožimo li tu jednakost s $b'$, dobivamo $a'ub' + m'vb' = b'$. Dakle,

$$a'(ub') - b' = -m'(vb'),$$

iz čega vidimo da je $a'(ub') \equiv b' \pmod{m'}$. Prema tome, jedno rješenje kongruencije $a'x \equiv b' \pmod{m'}$ je $x = ub'$. Neka su $x_1$ i $x_2$ bilo koja dva rješenja te kongruencije. Iz $a'x_1 \equiv b' \pmod{m'}$, $a'x_2 \equiv b' \pmod{m'}$ i Propozicije 2.2. (1) slijedi da je $a'x_1 \equiv a'x_2 \pmod{m'}$. Kako je $(a', m') = 1$, iz Teorema 2.4. slijedi da je $x_1 \equiv x_2 \pmod{m'}$. Dakle, sva ostala rješenja su ekvivalentna prvom rješenju.

Ako je $x^{'}$ rješenje jednadžbe $ax \equiv b \pmod{m}$, tada vrijedi $ax^{'} - b = lm$, za neki cijeli broj $l$. Podijelimo li tu jednakost s $d$ dobivamo $a^{'}x^{'} - b^{'} = lm^{'}$. Dakle, $x^{'}$ je ujedno i rješenje jednadžbe $a^{'}x \equiv b^{'} \pmod{m^{'}}$ (množenjem s $d$ analogno se dokaže i obrat pa tako zaključujemo da polazna kongruencija ima rješenja), a sva rješenja te jednadžbe u cijelim brojevima dana su s $x = x^{'} + nm^{'}$, gdje je $n$ cijeli broj. (Odnosno, sva rješenja su međusobno kongruentna modulo $m^{'}$.) Sva međusobno neekvivalentna rješenja polazne jednadžbe (ona koja nisu međusobno kongruentna modulo $m$) dobivamo za $n = 0, 1, ..., d-1$. Dakle, ako $d|b$, onda kongruencija $ax \equiv b \pmod{m}$ ima točno $d$ rješenja modulo $m$. ■

Iz Teorema 2.6. slijedi da ako je $p$ prost broj i $a$ nije djeljiv s $p$, tada kongruencija $ax \equiv b \pmod{p}$ uvijek ima rješenje i to rješenje je jedinstveno. Iz toga slijedi da skup ostataka $\{0, 1, ..., p-1\}$ pri dijeljenju s $p$, uz zbrajanje i množenje modulo $p$, čini polje. Ono se obično označava sa $\mathbb{Z}_p$ ili sa $\mathbb{F}_p$.

Jedno zanimljivo pitanje je kako riješiti kongruenciju $a^{'}x \equiv b^{'} \pmod{m^{'}}$, gdje je $(a^{'}, m^{'}) = 1$. Kako je $(a^{'}, m^{'}) = 1$, to postoje cijeli brojevi $u$ i $v$ takvi da je $a^{'}u + m^{'}v = 1$, koji se mogu odrediti pomoću Euklidovog algoritma. U dokazu Teorema 2.6. pokazali smo da je jedno rješenje kongruencije $a^{'}x \equiv b^{'} \pmod{m^{'}}$ dano s $x = ub^{'}$, a sva ostala rješenja su ekvivalentna $x$.

**Primjer:** Riješite kongruenciju $555x \equiv 15 \pmod{5005}$.

*Rješenje:*
Primijetimo da je $(555, 5005) = 5$ i da $5|15$. Dakle, zadana će kongruencija imati 5 rješenja modulo 5005. Nakon dijeljenja s 5, dobivamo kongruenciju

$$111x \equiv 3 \pmod{1001},$$

koju ćemo najprije riješiti. Njezino jedno rješenje je $x = 3u$, gdje je $111u + 1001v = 1$. Da bi odredili $u$, koristimo Euklidov algoritam:

$$\begin{aligned} 1001 &= 111 \cdot 9 + 2 \\ 111 &= 2 \cdot 55 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

Vrijedi $r_2 = 1 = (1001, 111)$ pa moramo odrediti $y_2$ po rekurzivnoj formuli opisanoj u prethodnim predavanjima. Imamo $q_1 = 9$, $q_2 = 55$. Zatim $y_{-1} =$

0, $y_0 = 1$, $y_1 = -9$, $y_2 = 496$. Dakle, $u = 496$ pa je $x = 1488$. Vrijedi $1488 \equiv 487 \pmod{1001}$ pa možemo reći da su rješenja kongruencije $111x \equiv 3 \pmod{1001}$ dana s $x \equiv 487 \pmod{1001}$. Kako je $d = 5$, rješenja polazne kongruencije dana su s

$$x \equiv 487, 1488, 2489, 3490, 4491 \pmod{5005}$$

jer je $487 = 487 + 0 \cdot 1001$, $1488 = 487 + 1 \cdot 1001$, $2489 = 487 + 2 \cdot 1001$, $3490 = 487 + 3 \cdot 1001$, $4491 = 487 + 4 \cdot 1001$ (vidjeti dokaz Teorema 2.6.).

**Teorem 2.7. (Kineski teorem o ostacima)** Neka su $m_1, m_2, ..., m_r$ u parovima relativno prosti prirodni brojevi te neka su $a_1, a_2, ..., a_r$ cijeli brojevi. Tada sustav kongruencija

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, ..., \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

ima rješenja. Ako je $x_0$ jedno rješenje, onda su sva rješenja tog sustava dana s $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

*Dokaz:*
Neka je $m = m_1 m_2 \cdots m_r$ te neka je $n_j = \frac{m}{m_j}$ za $j = 1, ..., r$. Tada je $(m_j, n_j) = 1$ pa postoji cijeli broj $x_j$ takav da je $n_j x_j \equiv a_j \pmod{m_j}$. (Naime, postoje cijeli brojevi $u$ i $v$, takvi da je $m_j u + n_j v = 1$. Pomožimo li ovu jednakost s $a_j$, slijedi navedeni zaključak.) Promotrimo broj

$$x_0 = n_1 x_1 + ... + n_r x_r.$$

Svi pribrojnici ovoga zbroja djeljivi su s $m_j$ osim možda $n_j x_j$ pa je $x_0 \equiv n_j x_j \pmod{m_j}$. Dakle, $x_0 \equiv a_j \pmod{m_j}$ pa je $x_0$ rješenje zadanog sustava kongruencija.

Ako su $x$ i $y$ dva rješenja zadanog sustava kongruencija, koristeći Propoziciju 2.2. (1), dobivamo $x \equiv y \pmod{m_j}$ za $j = 1, ..., r$. Dakle, vrijedi $x - y = k_j m_j$, gdje su $k_j$ cijeli brojevi, za $j = 1, ..., m$. Korištenjem činjenice da su $m_1, ..., m_r$ u parovima relativno prosti, dobivamo da je $x \equiv y \pmod{m}$. ■

**Primjer:** Riješite sustav kongruencija $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$, $x \equiv 4 \pmod{11}$.

*Rješenje:*

Koristimo oznake iz Teorema 2.7. Imamo $m = 5 \cdot 7 \cdot 11 = 385$. Zatim $n_1 = \frac{385}{5} = 77$, $n_2 = \frac{385}{7} = 55$, $n_3 = \frac{385}{11} = 35$ te $x_0 = 77x_1 + 55x_2 + 35x_3$, gdje je $77x_1 \equiv 2 \pmod 5$, $55x_2 \equiv 3 \pmod 7$ i $35x_3 \equiv 4 \pmod{11}$.

Prethodne tri kongruencije se mogu malo "pojednostnvniti" pa imamo $2x_1 \equiv 2 \pmod 5$, $6x_2 \equiv 3 \pmod 7$ i $2x_3 \equiv 4 \pmod{11}$. Sada je lako vidljivo da možemo uzeti $x_1 = 1$, $x_2 = 4$ i $x_3 = 2$ pa je $x_0 = 367$. Konačno, sva rješenja zadanog sustava dana su sa $x \equiv 367 \pmod{385}$.