Diskretne strukture UNI, 28.12.2021 (12:15 - 14:00, P19)

1. Reši linearne diofantske enačbe

(a) $21x + 15y - 6z = 9$, (b) $10x + 13y + 17z = 50$, (c) $28x + 30y + 31z = 365$.

Opiši še tiste rešitve teh enačb, za katere velja $x \geq 0$, $y \geq 0$ in $z \geq 0$.

(b) $10x + 13y + 17z = 50$

Pri reševanju (z Eulerjevo metodo) izpostavimo neznanko, ki ima po abs. vrednosti najmanjši koeficient:

$$x = \frac{50}{10} - \frac{13}{10}y - \frac{17}{10}z \underset{\uparrow}{=} 5 - y - \frac{3}{10}y - z - \frac{7}{10}z =$$

ločimo celi del in "ulomek" < 1

$$= 5 - y - z - \underbrace{\left(\frac{3}{10}y + \frac{7}{10}z\right)}_{u}$$

"Ne-celi" del vzamemo za novo neznanko:

$$u = \frac{3}{10}y + \frac{7}{10}z \xrightarrow[\cdot 10]{\text{oziroma}} 10u = 3y + 7z$$

$3y + 7z - 10u = 0$ (to je spet LDE)

Izpostavimo y (saj ima po abs. vrednosti najm. koef.):

$$y = \frac{10}{3}u - \frac{7}{3}z = 3u + \frac{1}{3}u - 2z - \frac{1}{3}z = 3u - 2z + \underbrace{\left(\frac{1}{3}u - \frac{1}{3}z\right)}_{v}$$

Sedaj imamo $v = \frac{1}{3}u - \frac{1}{3}z \;/\cdot 3 \;\ldots\; 3v = u - z$

oziroma $z = u - 3v$

zato $y = 3u - 2(u - 3v) + v = u + 7v$

in $x = 5 - y - z - u = 5 - u - 7v - u + 3v - u =$

$= 5 - 3u - 4v$

Splošna rešitev je $(x, y, z) = (5 - 3u - 4v,\ u + 7v,\ u - 3v)$, $u, v \in \mathbb{Z}$.

(c) $28x + 30y + 31z = 365$

$$x = \frac{365}{28} - \frac{30}{28}y - \frac{31}{28}z = 13 + \frac{1}{28} - y - \frac{2}{28}y - z - \frac{3}{28}z =$$

$$= 13 - y - z + \underbrace{\frac{1}{28}(1 - 2y - 3z)}_{u}$$

$28u = 1 - 2y - 3z$ ... $28u + 2y + 3z = 1$

$$y = \frac{1}{2} - \frac{3}{2}z - 14u = -z - 14u + \underbrace{\left(-\frac{1}{2}z + \frac{1}{2}\right)}_{v}$$

$2v = -z + 1$ ... $z = -2v + 1$

$$y = -(-2v+1) - 14u + v = 3v - 14u - 1$$

$$x = 13 - (3v - 14u - 1) - (-2v + 1) + u =$$

$$= 15u - v + 13$$

Kdaj je $x \geq 0$, $y \geq 0$ in $z \geq 0$?

$z \geq 0$ ... $-2v + 1 \geq 0$ ... $1 \geq 2v \;/:2$ ... $v \leq \frac{1}{2}$ .... $v \leq 0$ ($v \in \mathbb{Z}$)

$x \geq 0$ ... $15u \underbrace{- v}_{\geq 0} + 13 \geq 0$ .... $15u \geq v - 13$ ... $u \geq \frac{v}{15} - \frac{13}{15}$

$y \geq 0$ ... $3v - 14u - 1 \geq 0$ ... $-14u \geq 1 - 3v$ ... $u \leq \frac{3}{14}v - \frac{1}{14}$

Preverimo za nekaj vrednosti v:

v	0	-1	-2	.... SAMOSTOJNO!
$u \geq$	$-13/15$	$-14/15$	-1	
$u \leq$	$-\frac{1}{14}$	$-\frac{4}{14}$	$-\frac{7}{14}$	

$u = -1$

$x = 0,\ y = 7,\ z = 5$

3. (a) Izračunaj $\varphi(1215)$ in $\varphi(1216)$.
   (b) Določi $1024^{3241} \pmod{1215}$.

(a) $\varphi(n)$ je število celih števil med 1 in n, ki so tuja n.

$\varphi(p) = p-1$, p praštevilo

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

$\vdots$

$$\varphi(n) = \varphi(\underbrace{p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}}_{\text{prafaktorji } n}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdot \ldots \cdot (p_m^{k_m} - p_m^{k_m-1})$$

$1215 = 3^5 \cdot 5 \ldots \varphi(1215) = \underbrace{(3^5 - 3^4)}_{162} \cdot \underbrace{(5^1 - 5^0)}_{4} = 648$,

$1216 = 2^6 \cdot 19 \ldots \varphi(1216) = \underbrace{(2^6 - 2^5)}_{32} \cdot \underbrace{(19-1)}_{18} = 576$.

(b) $1024^{3241} \pmod{1215}$

$$\boxed{\text{Eulerjev izrek } a^{\varphi(n)} \equiv 1 \pmod{n}, \text{ če } \gcd(a,n) = 1.}$$

V našem primeru $a = 1024 = 2^{10}$
$n = 1215 = 3^5 \cdot 5$,
torej $\gcd(a,n) = 1$.

Dobimo torej: $1024^{\overset{\varphi(1215)}{\overset{\shortparallel}{648}}} \equiv 1 \pmod{1215}$

$3241 : 648 = 5$ (ost. 1), tj. $3241 = 648 \cdot 5 + 1$

Zato $1024^{3241} = 1024^{648 \cdot 5 + 1} = (1024^{648})^5 \cdot 1024 \equiv$

$\equiv 1^5 \cdot 1024 \pmod{1215} \equiv 1024 \pmod{1215}$.

5. (a) Koliko je ostanek števila $((5^9)^{13})^{17}$ pri deljenju z 11?

(b) Koliko je ostanek števila $5^{9^{13^{17}}}$ pri deljenju z 11?

(a) $((5^9)^{13})^{17} = 5^{9\cdot 13\cdot 17} = 5^{1989}$

Poiščimo ostanke zaporednih potenc št. 5 pri deljenju z 11:

$5^0 = 1 \equiv 1 \pmod{11}$
$5^1 = 5 \equiv 5 \pmod{11}$
$5^2 = 25 \equiv 3 \pmod{11}$
$5^3 \equiv 15 \equiv 4 \pmod{11}$
$5^4 \equiv 9 \pmod{11}$
$5^5 \equiv 3\cdot 4 \equiv 1 \pmod{11}$
$5^6 = 5\cdot 5^5 \equiv 5\cdot 1 \equiv 5 \pmod{11}$
$\vdots$

Torej $5^{1989} = 5^{5k+4} = 5^{5k}\cdot 5^4 \equiv 1^k \cdot 9 \pmod{11} = 9 \pmod{11}$.

$1989 : 5 = k$ (ost. 4) .... $1989 = 5k+4$

Direktno, z uporabo Eulerjevega izreka: $5^{\varphi(11)} \equiv 1 \pmod{11}$, (saj $\gcd(5,11)=1$)

torej $5^{10} \equiv 1 \pmod{11}$.

Zato uporabimo $1989 = 198\cdot 10 + 9$ in dobimo

$5^{1989} = 5^{10\cdot 198}\cdot 5^9 \equiv 1^{198}\cdot 5^9 \pmod{11} \equiv 9 \pmod{11}$.

(b) $5^{9^{13^{17}}} \pmod{11} \equiv ?$

Vemo (iz (a)), da je $5^5 \equiv 1 \pmod{11}$.

Kako lahko izrazimo ostanek $9^{13^{17}}$ pri deljenju s 5?

Kar z Eulerjevim izrekom: $9^{\varphi(5)} \equiv 1 \pmod 5$ oz. $9^4 \equiv 1 \pmod 5$

Kako lahko izrazimo ostanek 13^{17} pri deljenju s 4?

$13^{\varphi(4)} \equiv 1 \pmod 4$ ... $13^2 \equiv 1 \pmod 4$

Zato: $\quad 13^{17} = 13^{2\cdot 8+1} = (13^2)^8 \cdot 13 \equiv 1^8 \cdot 13 \pmod 4 \equiv 1 \pmod 4$.

in: $\quad 9^{13^{17}} = 9^{4k+1} = (9^4)^k \cdot 9 \equiv 1^k \cdot 9 \pmod 5 \equiv 4 \pmod 5$

končno: $\quad 5^{9^{13^{17}}} \equiv 5^{5\ell+4} \equiv (5^5)^\ell \cdot 5^4 \equiv 1^\ell\, 5^4 \pmod{11} \equiv 9 \pmod{11}$.