1. Z Evklidovim algoritmom poiščite $gcd(1771, 1485)$. V spodnjo tabelo vpišite vrednosti vhodnih parametrov procedure EUCLID ob vsakem rekurzivnem klicu.

Rešitev:

$iter$	a	b
0	1771	1485
1	1485	286
2	286	55
3	55	11
4	11	0

$$gcd(1771, 1485) = \underline{11}$$

2. Z iterativnim razširjenim Evklidovim algoritmom poiščite $d = gcd(133, 99)$ in ga zapišite v obliki $d = ax + by$. Izpolnite spodnjo tabelo z ustreznimi vrednostmi, ki jih izračunate med postopkom reševanja. Na dodatno črto zapišite iskano enačbo.

Rešitev:

korak	kvocient	ostanek	substitucija	kombiniran izraz
1		133		$133 = 133 \cdot 1 + 99 \cdot 0$
2		99		$99 = 133 \cdot 0 + 99 \cdot 1$
3	$\underline{1}$	$\underline{34}$=$\underline{133}$-$\underline{99}$·$\underline{1}$	$\underline{34} = (133 \cdot \underline{1} + 99 \cdot \underline{0}) - (133 \cdot \underline{0} + 99 \cdot \underline{1}) \cdot \underline{1}$	$\underline{34}$=133·$\underline{1}$+99·$\underline{-1}$
4	$\underline{2}$	$\underline{31}$=$\underline{99}$-$\underline{34}$·$\underline{2}$	$\underline{31} = (133 \cdot \underline{0} + 99 \cdot \underline{1}) - (133 \cdot \underline{1} + 99 \cdot \underline{-1}) \cdot \underline{2}$	$\underline{31}$=133·$\underline{-2}$+99·$\underline{3}$
5	$\underline{1}$	$\underline{3}$=$\underline{34}$-$\underline{31}$·$\underline{1}$	$\underline{3} = (133 \cdot \underline{1} + 99 \cdot \underline{-1}) - (133 \cdot \underline{-2} + 99 \cdot \underline{3}) \cdot \underline{1}$	$\underline{3}$=133·$\underline{3}$+99·$\underline{-4}$
6	$\underline{10}$	$\underline{1}$=$\underline{31}$-$\underline{3}$·$\underline{10}$	$\underline{1} = (133 \cdot \underline{-2} + 99 \cdot \underline{3}) - (133 \cdot \underline{3} + 99 \cdot \underline{-4}) \cdot \underline{10}$	$\underline{1}$=133·$\underline{-32}$+99·$\underline{43}$
7	$\underline{3}$	$\underline{0}$	konec algoritma	

$\underline{1}$= 133·$\underline{-32}$+99·$\underline{43}$

3. Rešite enačbo $70x \equiv 2 \pmod{58}$. Z iterativnim razširjenim Evklidovim algoritmom najprej poiščite $d = gcd(70, 58)$, tako da izpolnite spodnjo tabelo z ustreznimi vrednostmi, ki jih izračunate med postopkom reševanja. Nato na črto pod tabelo zapišite vse rešitve podane modulske enačbe, če je ta rešljiva. V nasprotnem primeru na črto zapišite razlog, zakaj enačba ni rešljiva.

Rešitev:

korak	kvocient	ostanek	substitucija	kombiniran izraz
1		70		$70 = 70 \cdot 1 + 58 \cdot 0$
2		58		$58 = 70 \cdot 0 + 58 \cdot 1$
3	$\underline{1}$	$\underline{12}$=$\underline{70}$-$\underline{58}$·$\underline{1}$	$\underline{12} = (70 \cdot \underline{1} + 58 \cdot \underline{0})$ $-(70 \cdot \underline{0} + 58 \cdot \underline{1}) \cdot \underline{1}$	$\underline{12}$=70·$\underline{1}$+58·$\underline{-1}$
4	$\underline{4}$	$\underline{10}$=$\underline{58}$-$\underline{12}$·$\underline{4}$	$\underline{10} = (70 \cdot \underline{0} + 58 \cdot \underline{1})$ $-(70 \cdot \underline{1} + 58 \cdot \underline{-1}) \cdot \underline{4}$	$\underline{10}$=70·$\underline{-4}$+58·$\underline{5}$
5	$\underline{1}$	$\underline{2}$=$\underline{12}$-$\underline{10}$·$\underline{1}$	$\underline{2} = (70 \cdot \underline{1} + 58 \cdot \underline{-1})$ $-(70 \cdot \underline{-4} + 58 \cdot \underline{5}) \cdot \underline{1}$	$\underline{2}$=70·$\underline{5}$+58·$\underline{-6}$
6	$\underline{5}$	$\underline{0}$	konec algoritma	

Rešitve enačbe: 5, 34,

4. Rešite enačbo $58x \equiv 7 \pmod{88}$. Z iterativnim razširjenim Evklidovim algoritmom najprej poiščite $d = gcd(58, 88)$, tako da izpolnite spodnjo tabelo z ustreznimi vrednostmi, ki jih izračunate med postopkom reševanja. Nato na črto pod tabelo zapišite vse rešitve podane modulske enačbe, če je ta rešljiva. V nasprotnem primeru na črto zapišite razlog, zakaj enačba ni rešljiva.

Rešitev:

korak	kvocient	ostanek	substitucija	kombiniran izraz
1		58		$58 = 58 \cdot 1 + 88 \cdot 0$
2		88		$88 = 58 \cdot 0 + 88 \cdot 1$
3	$\underline{0}$	$\underline{58}=\underline{58}-\underline{88}\cdot\underline{0}$	$\underline{58} = (58 \cdot \underline{1} + 88 \cdot \underline{0})$ $-(58 \cdot \underline{0} + 88 \cdot \underline{1}) \cdot \underline{0}$	$\underline{58}=58\cdot\underline{1}+88\cdot\underline{0}$
4	$\underline{1}$	$\underline{30}=\underline{88}-\underline{58}\cdot\underline{1}$	$\underline{30} = (58 \cdot \underline{0} + 88 \cdot \underline{1})$ $-(58 \cdot \underline{1} + 88 \cdot \underline{0}) \cdot \underline{1}$	$\underline{30}=58\cdot\underline{-1}+88\cdot\underline{1}$
5	$\underline{1}$	$\underline{28}=\underline{58}-\underline{30}\cdot\underline{1}$	$\underline{28} = (58 \cdot \underline{1} + 88 \cdot \underline{0})$ $-(58 \cdot \underline{-1} + 88 \cdot \underline{1}) \cdot \underline{1}$	$\underline{28}=58\cdot\underline{2}+88\cdot\underline{-1}$
6	$\underline{1}$	$\underline{2}=\underline{30}-\underline{28}\cdot\underline{1}$	$\underline{2} = (58 \cdot \underline{-1} + 88 \cdot \underline{1})$ $-(58 \cdot \underline{2} + 88 \cdot \underline{-1}) \cdot \underline{1}$	$\underline{2}=58\cdot\underline{-3}+88\cdot\underline{2}$
7	$\underline{14}$	$\underline{0}$	konec algoritma	

Rešitve enačbe: $\underline{\text{enačba ni rešljiva, ker } 2 \nmid 7}$

5. Poiščite multiplikativni inverz x od 48, modulo 25, uporabite razširjeni Evklidov algoritem. Izpolnite spodnjo tabelo z ustreznimi vrednostmi, ki jih izračunate med postopkom reševanja. Če multiplikativni inverz obstaja, na dodatno črto zapišite njegovo vrednost, sicer nanjo zapišite razlog, zakaj ne obstaja.

Rešitev:

korak	kvocient	ostanek	substitucija	kombiniran izraz
1		48		$48 = 48 \cdot 1 + 25 \cdot 0$
2		25		$25 = 48 \cdot 0 + 25 \cdot 1$
3	$\underline{1}$	$\underline{23}$=$\underline{48}$-$\underline{25}$·$\underline{1}$	$\underline{23} = (48 \cdot \underline{1} + 25 \cdot \underline{0})$ $-(48 \cdot \underline{0} + 25 \cdot \underline{1}) \cdot \underline{1}$	$\underline{23}$=48·$\underline{1}$+25·$\underline{-1}$
4	$\underline{1}$	$\underline{2}$=$\underline{25}$-$\underline{23}$·$\underline{1}$	$\underline{2} = (48 \cdot \underline{0} + 25 \cdot \underline{1})$ $-(48 \cdot \underline{1} + 25 \cdot \underline{-1}) \cdot \underline{1}$	$\underline{2}$=48·$\underline{-1}$+25·$\underline{2}$
5	$\underline{11}$	$\underline{1}$=$\underline{23}$-$\underline{2}$·$\underline{11}$	$\underline{1} = (48 \cdot \underline{1} + 25 \cdot \underline{-1})$ $-(48 \cdot \underline{-1} + 25 \cdot \underline{2}) \cdot \underline{11}$	$\underline{1}$=48·$\underline{12}$+25·$\underline{-23}$
6	$\underline{2}$	$\underline{0}$	konec algoritma	

Rešitev: x=12

6. Poiščite multiplikativni inverz x od 26, modulo 86, uporabite razširjeni Evklidov algoritem. Izpolnite spodnjo tabelo z ustreznimi vrednostmi, ki jih izračunate med postopkom reševanja. Če multiplikativni inverz obstaja, na dodatno črto zapišite njegovo vrednost, sicer nanjo zapišite razlog, zakaj ne obstaja.

Rešitev:

korak	kvocient	ostanek	substitucija	kombiniran izraz
1		26		$26 = 26 \cdot 1 + 86 \cdot 0$
2		86		$86 = 26 \cdot 0 + 86 \cdot 1$
3	$\underline{0}$	$\underline{26}=\underline{26}$-$\underline{86}\cdot\underline{0}$	$\underline{26} = (26 \cdot \underline{1} + 86 \cdot \underline{0}) - (26 \cdot \underline{0} + 86 \cdot \underline{1}) \cdot \underline{0}$	$\underline{26}=26\cdot\underline{1}+86\cdot\underline{0}$
4	$\underline{3}$	$\underline{8}=\underline{86}$-$\underline{26}\cdot\underline{3}$	$\underline{8} = (26 \cdot \underline{0} + 86 \cdot \underline{1}) - (26 \cdot \underline{1} + 86 \cdot \underline{0}) \cdot \underline{3}$	$\underline{8}=26\cdot\underline{-3}+86\cdot\underline{1}$
5	$\underline{3}$	$\underline{2}=\underline{26}$-$\underline{8}\cdot\underline{3}$	$\underline{2} = (26 \cdot \underline{1} + 86 \cdot \underline{0}) - (26 \cdot \underline{-3} + 86 \cdot \underline{1}) \cdot \underline{3}$	$\underline{2}=26\cdot\underline{10}+86\cdot\underline{-3}$
6	$\underline{4}$	$\underline{0}$	konec algoritma	

Rešitev: multiplikativni inverz od 26, modulo 86, ne obstaja, ker $gcd(26, 86) \neq 1$

7. Izračunajte vrednost Eulerjeve funkcije za število 46305. Postopek izračuna zapišite na spodnjo črto.

Rešitev:

$\varphi(46305) = \underline{\varphi(3^3 \cdot 7^3 \cdot 5^1) = 46305 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{5}\right) = 21168}$

8. S pomočjo Eulerjevega izreka izračunajte 8^{684} mod 11. Na zgornjo črto zapišite postopek izračuna $\varphi(n)$. Na srednjo črto zapišite kongruenco, ki jo dobite po Eulerjevem izreku. Postopek zniževanja potence in končni rezultat zapišite na spodnjo črto.

Rešitev:

$\varphi(11) = \underline{\varphi(11) = 11\left(1 - \frac{1}{11}\right) = 10}$

$\underline{8^{10} \equiv 1 \pmod{11}}$

$8^{684} \equiv \underline{8^{10\cdot 68+4} \equiv (8^{10})^{68} \cdot 8^4 \equiv 1^{68} \cdot 8^4 \equiv 4096 \pmod{11} = 4}$

9. Z binarno metodo modulskega potenciranja rešite enačbo 18^{744} mod 620. Na prvo spodnjo črto zapišite binarni zapis eksponenta, tabelo pod njo zapolnite z vrednostmi, ki jih dobite med postopkom izračuna. Končno rešitev zapišite na zadnjo črto.

Rešitev:

$744_{[10]} = \underline{1011101000_{[2]}}$

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	1	1	1	0	1	0	0	0
d	18	324	428	152	472	204	128	264	256	436

$18^{744} \bmod 620 = \underline{436}$

10. Dani sta praštevili $p = 113$ in $q = 139$. Z njuno pomočjo izračunajte javni in tajni ključ RSA. Za e izberite prvo primerno vrednost, ki je večja od 30, izračun s pa izvedite s pomočjo spodnje tabele. Na najnižji črti zapišite javni in tajni ključ.

Rešitev:

$n = \underline{15707}$

$\varphi(n) = \underline{15456}$

$e = \underline{31}$

korak	kvocient	ostanek	substitucija	kombiniran izraz
1		31		$31 = 31 \cdot 1 + 15456 \cdot 0$
2		15456		$15456 = 31 \cdot 0 + 15456 \cdot 1$
3	$\underline{0}$	$\underline{31}$=$\underline{31}$-$\underline{15456}$·$\underline{0}$	$\underline{31} = (31 \cdot \underline{1} + 15456 \cdot \underline{0})$ $-(31 \cdot \underline{0} + 15456 \cdot \underline{1}) \cdot \underline{0}$	$\underline{31}$=31·$\underline{1}$+15456·$\underline{0}$
4	$\underline{498}$	$\underline{18}$=$\underline{15456}$-$\underline{31}$·$\underline{498}$	$\underline{18} = (31 \cdot \underline{0} + 15456 \cdot \underline{1})$ $-(31 \cdot \underline{1} + 15456 \cdot \underline{0}) \cdot \underline{498}$	$\underline{18}$=31·$\underline{-498}$+15456·$\underline{1}$
5	$\underline{1}$	$\underline{13}$=$\underline{31}$-$\underline{18}$·$\underline{1}$	$\underline{13} = (31 \cdot \underline{1} + 15456 \cdot \underline{0})$ $-(31 \cdot \underline{-498} + 15456 \cdot \underline{1}) \cdot \underline{1}$	$\underline{13}$=31·$\underline{499}$+15456·$\underline{-1}$
6	$\underline{1}$	$\underline{5}$=$\underline{18}$-$\underline{13}$·$\underline{1}$	$\underline{5} = (31 \cdot \underline{-498} + 15456 \cdot \underline{1})$ $-(31 \cdot \underline{499} + 15456 \cdot \underline{-1}) \cdot \underline{1}$	$\underline{5}$=31·$\underline{-997}$+15456·$\underline{2}$
7	$\underline{2}$	$\underline{3}$=$\underline{13}$-$\underline{5}$·$\underline{2}$	$\underline{3} = (31 \cdot \underline{499} + 15456 \cdot \underline{-1})$ $-(31 \cdot \underline{-997} + 15456 \cdot \underline{2}) \cdot \underline{2}$	$\underline{3}$=31·$\underline{2493}$+15456·$\underline{-5}$
8	$\underline{1}$	$\underline{2}$=$\underline{5}$-$\underline{3}$·$\underline{1}$	$\underline{2} = (31 \cdot \underline{-997} + 15456 \cdot \underline{2})$ $-(31 \cdot \underline{2493} + 15456 \cdot \underline{-5}) \cdot \underline{1}$	$\underline{2}$=31·$\underline{-3490}$+15456·$\underline{7}$
9	$\underline{1}$	$\underline{1}$=$\underline{3}$-$\underline{2}$·$\underline{1}$	$\underline{1} = (31 \cdot \underline{2493} + 15456 \cdot \underline{-5})$ $-(31 \cdot \underline{-3490} + 15456 \cdot \underline{7}) \cdot \underline{1}$	$\underline{1}$=31·$\underline{5983}$+15456·$\underline{-12}$
10	$\underline{2}$	$\underline{0}$	konec algoritma	

$s = \underline{5983}$

P=$\underline{(31,15707)}$

S=$\underline{(5983,15707)}$

11. Dani sta praštevili $p = 137$ in $q = 139$. Z njuno pomočjo izračunajte javni in tajni ključ RSA. Za e izberite prvo primerno vrednost, ki je večja od 30, izračun s pa izvedite s pomočjo spodnje tabele. Na najnižji črti zapišite javni in tajni ključ.

Rešitev:

$n = \underline{19043}$

$\varphi(n) = \underline{18768}$

$e = \underline{31}$

korak	kvocient	ostanek	substitucija	kombiniran izraz
1		31		$31 = 31 \cdot 1 + 18768 \cdot 0$
2		18768		$18768 = 31 \cdot 0 + 18768 \cdot 1$
3	$\underline{0}$	$\underline{31}$=$\underline{31}$-$\underline{18768}$·$\underline{0}$	$\underline{31} = (31 \cdot \underline{1} + 18768 \cdot \underline{0})$ $-(31 \cdot \underline{0} + 18768 \cdot \underline{1}) \cdot \underline{0}$	$\underline{31}$=31·$\underline{1}$+18768·$\underline{0}$
4	$\underline{605}$	$\underline{13}$=$\underline{18768}$-$\underline{31}$·$\underline{605}$	$\underline{13} = (31 \cdot \underline{0} + 18768 \cdot \underline{1})$ $-(31 \cdot \underline{1} + 18768 \cdot \underline{0}) \cdot \underline{605}$	$\underline{13}$=31·$\underline{-605}$+18768·$\underline{1}$
5	$\underline{2}$	$\underline{5}$=$\underline{31}$-$\underline{13}$·$\underline{2}$	$\underline{5} = (31 \cdot \underline{1} + 18768 \cdot \underline{0})$ $-(31 \cdot \underline{-605} + 18768 \cdot \underline{1}) \cdot \underline{2}$	$\underline{5}$=31·$\underline{1211}$+18768·$\underline{-2}$
6	$\underline{2}$	$\underline{3}$=$\underline{13}$-$\underline{5}$·$\underline{2}$	$\underline{3} = (31 \cdot \underline{-605} + 18768 \cdot \underline{1})$ $-(31 \cdot \underline{1211} + 18768 \cdot \underline{-2}) \cdot \underline{2}$	$\underline{3}$=31·$\underline{-3027}$+18768·$\underline{5}$
7	$\underline{1}$	$\underline{2}$=$\underline{5}$-$\underline{3}$·$\underline{1}$	$\underline{2} = (31 \cdot \underline{1211} + 18768 \cdot \underline{-2})$ $-(31 \cdot \underline{-3027} + 18768 \cdot \underline{5}) \cdot \underline{1}$	$\underline{2}$=31·$\underline{4238}$+18768·$\underline{-7}$
8	$\underline{1}$	$\underline{1}$=$\underline{3}$-$\underline{2}$·$\underline{1}$	$\underline{1} = (31 \cdot \underline{-3027} + 18768 \cdot \underline{5})$ $-(31 \cdot \underline{4238} + 18768 \cdot \underline{-7}) \cdot \underline{1}$	$\underline{1}$=31·$\underline{-7265}$+18768·$\underline{12}$
9	$\underline{2}$	$\underline{0}$	konec algoritma	

$s = \underline{11503 \text{ (prva pozitivna vrednost oblike } -7265 + k \cdot 18768)}$

P=$\underline{(31{,}19043)}$

S=$\underline{(11503{,}19043)}$

12. Dana sta javni ključ RSA $P = (31, 18209)$ in tajni ključ RSA $S = (4049, 18209)$. Z javnim ključem najprej zašifrirajte sporočilo $M = 2310$, tako da izpolnite prvo spodnjo tabelo. Enačbo in rezultat zapišite na prvo črto. Nato izvedite dešifriranje s tajnim ključem, postopek pa zapišite v drugo tabelo. Enačbo z rezultatom zapišite na drugo črto. Na zadnjo črto zapišite še utemeljen odgovor na vprašanje, ali (sodeč po danem primeru) podana ključa tvorita par ključev RSA?

Rešitev:

i	4	3	2	1	0
b_i	1	1	1	1	1
d	2310	8749	2585	6569	4287

$C = P(M) = \underline{2310^{31} \bmod 18209 = 4287}$

i	11	10	9	8	7	6	5	4	3	2	1	0
b_i	1	1	1	1	1	1	0	1	0	0	0	1
d	4287	1028	15599	5963	692	7308	18076	10467	12745	10745	9965	883

$M = S(C) = \underline{4287^{4049} \bmod 18209 = 883}$

Odgovor: Ključa ne tvorita para ključev RSA, ker ne velja $M = S(P(M))$!

13. Dana sta javni ključ RSA $P = (31, 15707)$ in tajni ključ RSA $S = (5983, 15707)$. Z javnim ključem najprej zašifrirajte sporočilo $M = 3744$, tako da izpolnite prvo spodnjo tabelo. Enačbo in rezultat zapišite na prvo črto. Nato izvedite dešifriranje s tajnim ključem, postopek pa zapišite v drugo tabelo. Enačbo z rezultatom zapišite na drugo črto. Na zadnjo črto zapišite še utemeljen odgovor na vprašanje, ali (sodeč po danem primeru) podana ključa tvorita par ključev RSA?

Rešitev:

i	4	3	2	1	0
b_i	1	1	1	1	1
d	3744	12754	2245	13545	7104

$C = P(M) = \underline{3744^{31} \bmod 15707 = 7104}$

i	12	11	10	9	8	7	6	5	4	3	2	1	0
b_i	1	0	1	1	1	0	1	0	1	1	1	1	1
d	7104	225	12528	10976	6908	2598	3827	7005	11737	354	3518	12445	3744

$M = S(C) = \underline{7104^{5983} \bmod 15707 = 3744}$

Odgovor: Ključa tvorita par ključev RSA, ker velja $M = S(P(M))$!

14. Z uporabo psevdo testa preverite, ali je 3469 praštevilo. Na prve tri črte zapišite vrednosti, ki nastopajo v enačbi testa. Postopek vnesite v tabelo, utemeljen odgovor pa zapišite na črto pod njo!

Rešitev:

$a = \underline{2}$

$n = \underline{3469}$

$b = \underline{3468}_{[10]} = \underline{110110001100}_{[2]}$

i	11	10	9	8	7	6	5	4	3	2	1	0
b_i	1	1	0	1	1	0	0	0	1	1	0	0
d	2	8	64	1254	2118	507	343	3172	2968	2466	3468	1

Odgovor: 3469 je praštevilo ali psevdo praštevilo z bazo 2, ker $2^{3468} \equiv 1 \pmod{3469}$

15. Z uporabo psevdo testa preverite, ali je 3893 praštevilo. Na prve tri črte zapišite vrednosti, ki nastopajo v enačbi testa. Postopek vnesite v tabelo, utemeljen odgovor pa zapišite na črto pod njo!

Rešitev:

$a = \underline{2}$

$n = \underline{3893}$

$b = \underline{3892}_{[10]} = \underline{111100110100}_{[2]}$

i	11	10	9	8	7	6	5	4	3	2	1	0
b_i	1	1	1	1	0	0	1	1	0	1	0	0
d	2	8	128	1624	1815	747	2620	2082	1815	1494	1347	271

Odgovor: 3893 ni praštevilo, ker $2^{3892} \not\equiv 1 \pmod{3893}$

16. Z uporabo Miller-Rabinovega testa preverite, ali je 3907 praštevilo, pri čemer uporabite bazo $a = 717$. Na prve tri črte zapišite vrednosti, ki nastopajo v inicializaciji testa. V prvo tabelo zapišite potek modulskega potenciranja $a^u \bmod n$, na črto pod njo pa rezultat postopka. V drugo tabelo zapišite potek metode `WITNESS`. Rezultat testa zapišite na zadnjo črto!

Rešitev:

$n = \underline{3907}$

$n - 1 = \underline{3906}_{[10]} = \underline{111101000010}_{[2]}$

$u = \underline{11110100001}_{[2]} = \underline{1953}_{[10]}$

$t = \underline{1}$

i	10	9	8	7	6	5	4	3	2	1	0
b_i	1	1	1	1	0	1	0	0	0	0	1
d	717	3712	879	2253	816	2887	1138	1827	1351	632	1

$x_0 = a^u \bmod n = \underline{717^{1953} \bmod 3907 = 1}$

i	0	1
x_i	1	1

Odgovor: <u>3907 je praštevilo</u>

17. Z uporabo Miller-Rabinovega testa preverite, ali je 4235 praštevilo, pri čemer uporabite bazo $a = 427$. Na prve tri črte zapišite vrednosti, ki nastopajo v inicializaciji testa. V prvo tabelo zapišite potek modulskega potenciranja $a^u \bmod n$, na črto pod njo pa rezultat postopka. V drugo tabelo zapišite potek metode `WITNESS`. Rezultat testa zapišite na zadnjo črto!

Rešitev:

$n = \underline{4235}$

$n - 1 = \underline{4234}_{[10]} = \underline{1000010001010}_{[2]}$

$u = \underline{100001000101}_{[2]} = \underline{2117}_{[10]}$

$t = \underline{1}$

i	11	10	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	0	1	0	0	0	1	0	1
d	427	224	3591	3941	1736	1092	2429	686	511	3822	1169	2072

$x_0 = a^u \bmod n = \underline{427^{2117} \bmod 4235 = 2072}$

i	0	1
x_i	2072	3129

Odgovor: <u>4235 ni praštevilo</u>

18. Z izboljšano Shamirjevo metodo želimo implementirati (3,4)-pragovno shemo za deljenje skrivnosti $S = 79$. Izbrali smo že praštevilo $P = 89$, za koeficienta a_1 in a_2 pa izberite prvi dve praštevili med 20 in 30 (v tem vrstnem redu). V spodnjo predlogo najprej zapišite vse vrednosti koeficientov, nato pa še vse tri izračunane deleže skrivnosti!

Rešitev:

$a_0 = \underline{79}$

$a_1 = \underline{23}$

$a_2 = \underline{29}$

$\langle 1; f(1) \mod P\rangle = \underline{\langle 1; 42\rangle}$

$\langle 2; f(2) \mod P\rangle = \underline{\langle 2; 63\rangle}$

$\langle 3; f(3) \mod P\rangle = \underline{\langle 3; 53\rangle}$

$\langle 4; f(4) \mod P\rangle = \underline{\langle 4; 12\rangle}$

19. Z izboljšano Shamirjevo metodo smo implementirali (2,3)-pragovno shemo za deljenje skrivnosti pri $P = 73$. Izračunajte skrivnost S iz deležev $\langle 1; 13 \rangle$ in $\langle 2; 44 \rangle$!

Rešitev:

$S = \left(f(1) \cdot \frac{2}{2-1} + f(2) \cdot \frac{1}{1-2} \right) \bmod 73 = (26 - 44) \bmod 73 = -18 \bmod 73 = 55$

20. Ali je zaporedje $[3, 11, 37, 83, 139]$ Mignottejevo zaporedje za (4,5)-pragovno shemo deljenja skrivnosti? Če da, s katerega intervala je lahko vrednost skrivnosti S?

Rešitev:

Zaporedje $[11, 17, 37, 83, 139]$ je Mignottejevo zaporedje za (4,5)-pragovno shemo, ker $37 \cdot 83 \cdot 139 = 426869 < 574277 = 11 \cdot 17 \cdot 37 \cdot 83$. Skrivnost S je vrednost z intervala $[426869, 574277]$

21. Ali je zaporedje $[11, 17, 37, 83, 139]$ Mignottejevo zaporedje za (4,5)-pragovno shemo deljenja skrivnosti? Če da, s katerega intervala je lahko vrednost skrivnosti S?ž

Zaporedje $[11, 17, 37, 83, 139]$ je Mignottejevo zaporedje za (4,5)-pragovno shemo, ker $37 \cdot 83 \cdot 139 = 426869 < 574277 = 11 \cdot 17 \cdot 37 \cdot 83$. Skrivnost S je vrednost z intervala $[426869, 574277]$

22. Določite najmanjšo primerno vrednost X, tako da bo zaporedje $[7, 13, X, 23, 73]$ Mignottejevo zaporedje za (3,5)-pragovno shemo deljenja skrivnosti!

Rešitev:

Iščemo $13 < X < 23$, za katerega velja $7 \cdot 13 \cdot X > 23 \cdot 73$ oz. $91X > 1679$. Najmanjše celo število, ki ustreza tem pogojem in je tuje ostalim številom v zaporedju, je 19.

$X = \underline{19}$

23. Po zaključku prve zanke **for** v proceduri `GAUSS_ELIMINATION` smo dobili matriko:

$$\tilde{\mathbf{A}} = [\mathbf{A} \;\; \mathbf{b}] = \begin{bmatrix} \underline{-1} & \underline{1} & \underline{3} & \underline{31} \\ \underline{0} & \underline{-5} & \underline{3} & \underline{1} \\ \underline{0} & \underline{0} & \underline{8} & \underline{56} \end{bmatrix}$$

Določite vektor $\mathbf{x}$! Na spodnje črte za vsako spremenljivko x_i zapišite enačbo, ki jo dobite s substitucijo nazaj, in izračunano vrednost.

Rešitev:

$x_3 = \underline{\frac{56}{8}} = \underline{7}$

$x_2 = \underline{\frac{1-3x_3}{-5}} = \underline{4}$

$x_1 = \underline{\frac{31-x_2-3x_3}{-1}} = \underline{-6}$

24. Dan je naslednji sistem linearnih enačb:

$$
\begin{aligned}
3x_1 + 3x_2 + 4x_3 &= 42 \\
6x_1 + x_2 - 2x_3 &= 19 \\
-x_1 + 9x_2 - 3x_3 &= 51
\end{aligned}
$$

Izvedite prvo zanko **for** v proceduri `GAUSS_ELIMINATION`! V spodnjo predlogo zapišite začetno matriko $\tilde{\mathbf{A}}$, zatem pa njeno vsebino ob zaključku vsake iteracije prve zanke **for** metode `GAUSS_ELIMINATION`. Vse vrednosti pri zapisu zaokrožite na tri decimalke (računajte pa s polno natančnostjo)!

Rešitev:

$$
\tilde{\mathbf{A}} = \begin{bmatrix} 3 & 3 & 4 & 42 \\ 6 & 1 & -2 & 19 \\ -1 & 9 & -3 & 51 \end{bmatrix} \sim \begin{bmatrix} 3 & 3 & 4 & 42 \\ 0 & -5 & -10 & -65 \\ 0 & 10 & -1.667 & 65 \end{bmatrix} \sim \begin{bmatrix} 3 & 3 & 4 & 42 \\ 0 & -5 & -10 & -65 \\ 0 & 0 & -21.667 & -65 \end{bmatrix}
$$

25. Z Gaussovo eliminacijo rešite naslednji sistem linearnih enačb:

$$\begin{aligned} -8x_1 - 5x_3 &= -60 \\ -5x_2 - 3x_3 &= -42 \\ -x_1 - 9x_2 - 7x_3 &= -87 \end{aligned}$$

V spodnjo predlogo najprej zapišite začetno matriko $\tilde{\mathbf{A}}$, zatem pa njeno vsebino ob zaključku vsake iteracije prve zanke **for** metode `GAUSS_ELIMINATION`. Na preostale črte za vsako spremenljivko x_i zapišite enačbo, ki jo dobite s substitucijo nazaj, in izračunano vrednost. Vse vrednosti pri zapisu zaokrožite na tri decimalke (računajte pa s polno natančnostjo)!

Rešitev:

$$\tilde{\mathbf{A}} = \begin{bmatrix} \underline{-8} & \underline{0} & \underline{-5} & \underline{-60} \\ \underline{0} & \underline{-5} & \underline{-3} & \underline{-42} \\ \underline{-1} & \underline{-9} & \underline{-7} & \underline{-87} \end{bmatrix} \sim \begin{bmatrix} \underline{-8} & \underline{0} & \underline{-5} & \underline{-60} \\ \underline{0} & \underline{-5} & \underline{-3} & \underline{-42} \\ \underline{0} & \underline{-9} & \underline{-6.375} & \underline{-79.5} \end{bmatrix} \sim \begin{bmatrix} \underline{-8} & \underline{0} & \underline{-5} & \underline{-60} \\ \underline{0} & \underline{-5} & \underline{-3} & \underline{-42} \\ \underline{0} & \underline{0} & \underline{-0.975} & \underline{-3.9} \end{bmatrix}$$

$x_3 = \underline{\frac{-3.9}{-0.975}} = \underline{4}$

$x_2 = \underline{\frac{-42+3x_3}{-5}} = \underline{6}$

$x_1 = \underline{\frac{-60+0x_2+5x_3}{-8}} = \underline{5}$

26. Dan je vektor $\mathbf{b} = [27 \quad -17 \quad 223]^T$ in naslednji LU razcep matrike $\mathbf{A}$:

$$\mathbf{L} = \begin{bmatrix} \underline{1} & \underline{0} & \underline{0} \\ \underline{-1} & \underline{1} & \underline{0} \\ \underline{4} & \underline{9} & \underline{1} \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} \underline{6} & \underline{3} & \underline{-9} \\ \underline{0} & \underline{5} & \underline{2} \\ \underline{0} & \underline{0} & \underline{-5} \end{bmatrix}$$

Poiščite rešitev sistema $\mathbf{Ax} = \mathbf{b}$ s proceduro `LU_SOLVE`! Na spodnje črte najprej za vsako spremenljivko y_i zapišite enačbo, ki jo dobite s substitucijo naprej, in izračunano vrednost. Na nižje črte zatem za vsako spremenljivko x_i zapišite enačbo, ki jo dobite s substitucijo nazaj, in izračunano vrednost.

Rešitev:

$y_1 = \underline{27.0}$

$y_2 = \underline{-17.0 + 1.0y_1} = \underline{10}$

$y_3 = \underline{223.0 - 4.0y_1 - 9.0y_2} = \underline{25}$

$x_3 = \underline{\frac{y_3}{-5}} = \underline{-5}$

$x_2 = \underline{\frac{y_2 - 2.0x_3}{5}} = \underline{4}$

$x_1 = \underline{\frac{y_1 - 3.0x_2 + 9.0x_3}{6}} = \underline{-5}$

27. Dan je naslednji sistem linearnih enačb:

$$\begin{aligned} x_1 + x_2 + 4x_3 &= -24 \\ -4x_1 - 9x_2 - 7x_3 &= 75 \\ -6x_1 - 16x_2 - 8x_3 &= 110 \end{aligned}$$

Izvedite LU razcep matrike **A** po proceduri `LU_DECOMPOSITION`! V spodnjo predlogo na vrhu zapišite matriko **A** in vektor **b**, pod njo pa v posamezni vrsti vsebine matrik **L**, **U** in **A** po vsaki iteraciji zanke **for** procedure `LU_DECOMPOSITION`. Vse vrednosti pri zapisu zaokrožite na dve decimalki (računajte pa s polno natančnostjo)!

Rešitev:

$$\mathbf{A} = \begin{bmatrix} \underline{1} & \underline{1} & \underline{4} \\ \underline{-4} & \underline{-9} & \underline{-7} \\ \underline{-6} & \underline{-16} & \underline{-8} \end{bmatrix} \qquad \mathbf{b} = \begin{bmatrix} \underline{-24} \\ \underline{75} \\ \underline{110} \end{bmatrix}$$

$$\mathbf{L} = \begin{bmatrix} 1 & 0 & 0 \\ \underline{-4} & 1 & 0 \\ \underline{-6} & ? & 1 \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} \underline{1} & \underline{1} & \underline{4} \\ 0 & ? & ? \\ 0 & 0 & ? \end{bmatrix} \qquad \mathbf{A} = \begin{bmatrix} \underline{1} & \underline{1} & \underline{4} \\ \underline{-4} & \underline{-5} & \underline{9} \\ \underline{-6} & \underline{-10} & \underline{16} \end{bmatrix}$$

$$\mathbf{L} = \begin{bmatrix} 1 & 0 & 0 \\ \underline{-4} & 1 & 0 \\ \underline{-6} & \underline{2} & 1 \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} \underline{1} & \underline{1} & \underline{4} \\ 0 & \underline{-5} & \underline{9} \\ 0 & 0 & ? \end{bmatrix} \qquad \mathbf{A} = \begin{bmatrix} \underline{1} & \underline{1} & \underline{4} \\ \underline{-4} & \underline{-5} & \underline{9} \\ \underline{-6} & \underline{-10} & \underline{-2} \end{bmatrix}$$

$$\mathbf{L} = \begin{bmatrix} 1 & 0 & 0 \\ \underline{-4} & 1 & 0 \\ \underline{-6} & \underline{2} & 1 \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} \underline{1} & \underline{1} & \underline{4} \\ 0 & \underline{-5} & \underline{9} \\ 0 & 0 & \underline{-2} \end{bmatrix}$$

28. Dan je naslednji sistem linearnih enačb:

$$\begin{aligned} -5x_1 + 8x_2 + 7x_3 &= 117 \\ 25x_1 - 34x_2 - 36x_3 &= -556 \\ 35x_1 - 20x_2 - 48x_3 &= -596 \end{aligned}$$

Izvedite LU razcep matrike **A** po proceduri `LU_DECOMPOSITION`, nato pa poiščite rešitev sistema po proceduri `LU_SOLVE`! V spodnjo predlogo na vrhu zapišite matriko **A** in vektor **b**, pod njo pa v posamezni vrsti vsebine matrik **L**, **U** in **A** po vsaki iteraciji zanke **for** procedure `LU_DECOMPOSITION`. Zatem na zgornje črte za vsako spremenljivko y_i zapišite enačbo, ki jo dobite s substitucijo naprej, in izračunano vrednost. Na koncu na nižje črte za vsako spremenljivko x_i zapišite enačbo, ki jo dobite s substitucijo nazaj, in izračunano vrednost. Vse vrednosti pri zapisu zaokrožite na dve decimalki (računajte pa s polno natančnostjo)!

Rešitev:

$$\mathbf{A} = \begin{bmatrix} \underline{-5} & \underline{8} & \underline{7} \\ \underline{25} & \underline{-34} & \underline{-36} \\ \underline{35} & \underline{-20} & \underline{-48} \end{bmatrix} \qquad \mathbf{b} = \begin{bmatrix} \underline{117} \\ \underline{-556} \\ \underline{-596} \end{bmatrix}$$

$$\mathbf{L} = \begin{bmatrix} 1 & 0 & 0 \\ \underline{-5} & 1 & 0 \\ \underline{-7} & ? & 1 \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} \underline{-5} & \underline{8} & \underline{7} \\ 0 & ? & ? \\ 0 & 0 & ? \end{bmatrix} \qquad \mathbf{A} = \begin{bmatrix} \underline{-5} & \underline{8} & \underline{7} \\ \underline{25} & \underline{6} & \underline{-1} \\ \underline{35} & \underline{36} & \underline{1} \end{bmatrix}$$

$$\mathbf{L} = \begin{bmatrix} 1 & 0 & 0 \\ \underline{-5} & 1 & 0 \\ \underline{-7} & \underline{6} & 1 \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} \underline{-5} & \underline{8} & \underline{7} \\ 0 & \underline{6} & \underline{-1} \\ 0 & 0 & ? \end{bmatrix} \qquad \mathbf{A} = \begin{bmatrix} \underline{-5} & \underline{8} & \underline{7} \\ \underline{25} & \underline{6} & \underline{-1} \\ \underline{35} & \underline{36} & \underline{7} \end{bmatrix}$$

$$\mathbf{L} = \begin{bmatrix} 1 & 0 & 0 \\ \underline{-5} & 1 & 0 \\ \underline{-7} & \underline{6} & 1 \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} \underline{-5} & \underline{8} & \underline{7} \\ 0 & \underline{6} & \underline{-1} \\ 0 & 0 & \underline{7} \end{bmatrix}$$

$y_1 = \underline{117.0}$

$y_2 = \underline{-556.0 + 5.0y_1} = \underline{29}$

$y_3 = \underline{-596.0 + 7.0y_1 - 6.0y_2} = \underline{49}$

$x_3 = \underline{\frac{y_3}{7}} = \underline{7}$

$x_2 = \underline{\frac{y_2+1.0x_3}{6}} = \underline{6}$

$x_1 = \underline{\frac{y_1-8.0x_2-7.0x_3}{-5}} = \underline{-4}$

29. Dan je začetni pogoj $\mathbf{x}^{(0)} = [-5 \;\; 2 \;\; 6 \;\; -3 \;\; 1]^T$. Izvedite prvo iteracijo Gauss-Seidelove metode po proceduri `GAUSS_SEIDEL` za naslednji sistem linearnih enačb:

$$\begin{aligned}
19x_1 - 7x_2 - 4x_3 - 5x_4 + x_5 &= -119 \\
3x_1 - 21x_2 + 9x_3 + 6x_4 - 2x_5 &= -22 \\
-4x_2 + 16x_3 + 4x_4 + 5x_5 &= 70 \\
9x_1 + 9x_2 + 4x_3 - 32x_4 + 7x_5 &= 117 \\
2x_1 + x_2 + 6x_3 - 8x_4 - 18x_5 &= 15
\end{aligned}$$

V spodnjo predlogo najprej zapišite vsebino matrike $\mathbf{A}$ in vektorja $\mathbf{b}$. Na črte zatem zapišite enačbe in izračunane vrednosti za posamezne komponente vektorja $\mathbf{x}^{(1)}$. Vrednosti zaokrožujte na dve decimalki.

Rešitev:

$$\mathbf{A} = \begin{bmatrix} \underline{19} & \underline{-7} & \underline{-4} & \underline{-5} & \underline{1} \\ \underline{3} & \underline{-21} & \underline{9} & \underline{6} & \underline{-2} \\ \underline{0} & \underline{-4} & \underline{16} & \underline{4} & \underline{5} \\ \underline{9} & \underline{9} & \underline{4} & \underline{-32} & \underline{7} \\ \underline{2} & \underline{1} & \underline{6} & \underline{-8} & \underline{-18} \end{bmatrix} \qquad \mathbf{b} = \begin{bmatrix} \underline{-119} \\ \underline{-22} \\ \underline{70} \\ \underline{117} \\ \underline{15} \end{bmatrix}$$

$$x_1^{(1)} = \underline{-\tfrac{1}{19}\left(+(-7)\cdot x_2^{(0)} + (-4)\cdot x_3^{(0)} + (-5)\cdot x_4^{(0)} + 1\cdot x_5^{(0)} - (-119)\right)} = \underline{-5.11}$$

$$x_2^{(1)} = \underline{-\tfrac{1}{-21}\left(3\cdot x_1^{(1)} + 9\cdot x_3^{(0)} + 6\cdot x_4^{(0)} + (-2)\cdot x_5^{(0)} - (-22)\right)} = \underline{1.94}$$

$$x_3^{(1)} = \underline{-\tfrac{1}{16}\left(0\cdot x_1^{(1)} + (-4)\cdot x_2^{(1)} + 4\cdot x_4^{(0)} + 5\cdot x_5^{(0)} - 70\right)} = \underline{5.3}$$

$$x_4^{(1)} = \underline{-\tfrac{1}{-32}\left(9\cdot x_1^{(1)} + 9\cdot x_2^{(1)} + 4\cdot x_3^{(1)} + 7\cdot x_5^{(0)} - 117\right)} = \underline{-3.67}$$

$$x_5^{(1)} = \underline{-\tfrac{1}{-18}\left(2\cdot x_1^{(1)} + 1\cdot x_2^{(1)} + 6\cdot x_3^{(1)} + (-8)\cdot x_4^{(1)} - 15\right)} = \underline{2.1}$$

30. Pretvorite naslednji linearni program v standardno obliko in rešitev zapišite na spodnje črte:

Minimiziraj

$$-3x_1 + 8x_2 - 3x_3$$

glede na

$$\begin{aligned}
-5x_1 + 5x_2 + 5x_3 &\leq 85 \\
-7x_1 - 8x_2 + 8x_3 &= 58 \\
-8x_1 - 5x_2 - 8x_3 &\geq 36 \\
x_1, x_3 &\geq 0
\end{aligned}$$

Rešitev:

Maksimiziraj

$$3x_1 - 8x_2' + 8x_2'' + 3x_3$$

glede na

$$\begin{aligned}
-5x_1 + 5x_2' - 5x_2'' + 5x_3 &\leq 85 \\
-7x_1 - 8x_2' + 8x_2'' + 8x_3 &\leq 58 \\
7x_1 + 8x_2' - 8x_2'' - 8x_3 &\leq -58 \\
8x_1 + 5x_2' - 5x_2'' + 8x_3 &\leq -36 \\
x_1, x_2', x_2'', x_3 &\geq 0
\end{aligned}$$

31. Pretvorite spodnji linearni program iz standardne oblike v ohlapno obliko in rešitev zapišite na črte. Za osnovne spremenljivke po vrsti uporabite najmanjše manjkajoče indekse. V predlogo na dnu zapišite rešitev še v obliki $(N, B, \mathbf{A}, \mathbf{b}, \mathbf{c}, v)$!

Maksimiziraj

$$-16 - x_2 + 2x_4 - 3x_5 - 3x_7$$

glede na

$$\begin{aligned} -3x_2 + x_4 + 4x_5 - 3x_7 &\leq 12 \\ -2x_2 + 4x_4 - 2x_5 + 3x_7 &\leq 4 \\ 5x_2 + 5x_4 - 4x_5 - 3x_7 &\leq 3 \\ 2x_2 + 3x_4 - 2x_5 + 3x_7 &\leq 20 \\ x_2, x_4, x_5, x_7 &\geq 0 \end{aligned}$$

Rešitev:

$$\begin{aligned} z &= -16 - x_2 + 2x_4 - 3x_5 - 3x_7 \\ x_1 &= 12 + 3x_2 - x_4 - 4x_5 + 3x_7 \\ x_3 &= 4 + 2x_2 - 4x_4 + 2x_5 - 3x_7 \\ x_6 &= 3 - 5x_2 - 5x_4 + 4x_5 + 3x_7 \\ x_8 &= 20 - 2x_2 - 3x_4 + 2x_5 - 3x_7 \end{aligned}$$

$$\mathbf{A} = \begin{bmatrix} \underline{-3} & \underline{1} & \underline{4} & \underline{-3} \\ \underline{-2} & \underline{4} & \underline{-2} & \underline{3} \\ \underline{5} & \underline{5} & \underline{-4} & \underline{-3} \\ \underline{2} & \underline{3} & \underline{-2} & \underline{3} \end{bmatrix} \qquad \mathbf{b} = \begin{bmatrix} \underline{12} \\ \underline{4} \\ \underline{3} \\ \underline{20} \end{bmatrix} \qquad \mathbf{c} = \begin{bmatrix} \underline{-1} \\ \underline{2} \\ \underline{-3} \\ \underline{-3} \end{bmatrix}$$

$$N = \underline{\{2, 4, 5, 7\}} \qquad B = \underline{\{1, 3, 6, 8\}} \qquad v = \underline{-16}$$

32. Rešite naslednji linearni program z metodo simpleks. V vsaki iteraciji izberite primerno vstopno spremenljivke z najmanjšim indeksom. Postopek reševanja dokumentirajte tako, da v spodnjo predlogo za vsako iteracijo zapišete:

- izbrano vstopno spremenljivko,
- vrednosti Δ_i,
- izbrano izhodno spremenljivko (v primeru enakovrednih možnosti izberite spet tisto z nižjim indeksom),
- novo obliko linearnega programa

Na črti na dnu zapišite še optimalno rešitev $\mathbf{x}$ in njeno vrednost z. Računajte s polno natančnostjo, zapisujte pa na tri decimalke natančno!

$$\begin{aligned} z &= 15x_1 + 16x_2 + 11x_5 \\ x_3 &= 43 + x_1 + x_2 - x_5 \\ x_4 &= 26 - 5x_1 - 2x_2 + x_5 \\ x_6 &= 47 + 2x_1 - 4x_5 \end{aligned}$$

Rešitev:

1. iteracija:

vstopna spremenljivka: x_1 izstopna spremenljivka: x_4

$\Delta_3 = \infty$

$\Delta_4 = 5.2$

$\Delta_6 = \infty$

$$\begin{aligned} z &= 78 + 10x_2 - 3x_4 + 14x_5 \\ x_1 &= 5.2 - 0.4x_2 - 0.2x_4 + 0.2x_5 \\ x_3 &= 48.2 + 0.6x_2 - 0.2x_4 - 0.8x_5 \\ x_6 &= 57.4 - 0.8x_2 - 0.4x_4 - 3.6x_5 \end{aligned}$$

2. iteracija:

vstopna spremenljivka: x_2 izstopna spremenljivka: x_1

$\Delta_1 = 13$

$\Delta_3 = \infty$

$\Delta_6 = 71.75$

$$\begin{aligned} z &= 208 - 25x_1 - 8x_4 + 19x_5 \\ x_2 &= 13 - 2.5x_1 - 0.5x_4 + 0.5x_5 \\ x_3 &= 56 - 1.5x_1 - 0.5x_4 - 0.5x_5 \\ x_6 &= 47 + 2x_1 - 4x_5 \end{aligned}$$

3. iteracija:

vstopna spremenljivka: x_5 izstopna spremenljivka: x_6

$\Delta_2 = \infty$

$\Delta_3 = 112$

$\Delta_6 = 11.75$

$$\begin{aligned} z &= 431.25 - 15.5x_1 - 8x_4 - 4.75x_6 \\ x_2 &= 18.875 - 2.25x_1 - 0.5x_4 - 0.125x_6 \\ x_3 &= 50.125 - 1.75x_1 - 0.5x_4 + 0.125x_6 \\ x_5 &= 11.75 + 0.5x_1 - 0.25x_6 \end{aligned}$$

Rešitev:

$\mathbf{x} = (x_1, x_2, x_5) = (0, 18.875, 11.75)$ $z = 431.25$