Скрипта решених задатака из криптографије

Сана СтојановићЂурђевић

15 июня 2015 г.

Содержание

1 Решени задаци

Задатак 1 *Доказати да* $6|m(m^2+5)$ *важи за произвољан природни број* m.

Решење: Задатак решити коришћењем математичке индукције.

1° За $m=1$ израз $m(m^2+5)$ је једнак 6 па је овај случај тривијалан (база индукције).

2° Претпоставимо да је $m \geq 1$ и да важи $6|m(m^2+5)$ (индукцијска претпоставка). Доказујемо да важи $6|(m+1)((m+1)^2+5)$. Важи следећа једнакост:
$(m+1)((m+1)^2+5) = m(m^2+5) + 3(m(m+1)+2)$.
На основу индукцијске претпоставке први члан овог збира је дељив са 6. Други члан збира је очигледно дељив са 6 (дељив је са 3 и израз $m(m+1)$ је увек паран). Тиме је доказана индукцијска хипотеза.

Решење (други начин): Израз $m(m^2+5)$ се може трансформисати на следећи начин:

$$m(m^2+5) = m^3+5m = m^3-m+6m = m(m^2-1)+6m = (m-1)m(m+1)+6m$$

Како је производ три суседна броја увек дељив са 6 (макар један од тих бројева биће паран број и барем један од тих бројева ће бити дељив са 3) први члан збира је дељив са 6. Други члан збира је очигледно дељив са 6 па је и цео збир дељив са 6.

Задатак 2 *Доказати да* $30|m^5-m$ *важи за произвољан природни број* m.

Решење: Израз m^5-m се може трансформисати на следећи начин:

$$m^5-m = m(m^4-1) = m(m^2-1)(m^2+1) = m(m-1)(m+1)(m^2+1)$$

Овај израз је увек дељив са 6 (производ три узастопна броја је увек дељив са 6). Да бисмо доказали да је овај израз дељив са 30 довољо је доказати да је дељив са 5.
Број m се може записати као $m = 5k+r$, при чему је $r = 0, \pm 1, \pm 2$.

Ако је $r=0$ онда је број m дељив са 5 па је и цео израз дељив са 5.

Ако је $r=\pm 1$ онда је један од бројева $r-1$, $r+1$ дељив са 5 па је и цео израз дељив са 5.

Ако је $r=\pm 2$ онда важи $m^2+1 = (5k\pm 2)^2+1 = 25k^2 \pm 20k + 5$ што је дељиво са 5 па је и цео израз дељив са 5.

Задатак 3 *Доказати да* $30|mn(m^4-n^4)$ *важи за произвољне природне бројеве* m *и* n.

Решење: Како важи да је $mn(m^4 - n^4) = (m^5 - m)n + m(n - n^5)$, и како су појединачни сабирци дељиви са 30 (на основу претходног задатка) онда следи и да је цео израз дељив са 30.

Задатак 4 *Доказати да* $42|m^7 - m$ *важи за произвољан природан број* m.

Решење: Показује се да важи
$m^7 - m = m(m-1)(m+1)(m^2+m+1)(m^2-m+1)$.
Производ прва три члана је увек дељив са 6 па је довољно доказати да је цео производ дељив са 7.
Број m се може записати као $m = 7k + r$, при чему је $r = 0, \pm 1, \pm 2, \pm 3$.

Ако је $r = 0$ онда је m дељиво са 7 па је и цео израз дељив са 7.

Ако је $r = \pm 1$ онда је $m^2 - 1$ дељиво са 7.

Ако је $r = \pm 2$ онда се могу уочити последња два члана производа $(m^2+m+1)(m^2-m+1) = m^4 + m^2 + 1$. Остатак при дељењу m^2 са 7 је једнак 4, остатак при дељењу m^4 са 7 је једнак 2, па је остатак при дељењу са 7 овог израза једнак 0.

Ако је $r = \pm 3$ уочимо израз $m^4 + m^2 + 1$. Остатак при дељењу m^2 са 7 је једнак 2, остатак при дељењу m^4 са 7 је једнак 4, па је остатак при дељењу са 7 овог израза једнак 0.

Решење (други начин): Задатак се може решити коришћењем математичке индукције.

1° За $m = 1$ израз је једнак 0 па је овај случај тривијалан.

2° Претпоставка је да је $m > 1$ и да израз важи за m. Посматрајмо разлику
$[(m+1)^7 - (m+1)] - [m^7 - m] = 7m^6 + 21m^5 + 35m^4 + 35m^3 + 21m^2 + 7m$.
Она је очигледно дељива са 7 чиме је доказа индуктивна хипотеза.

Задатак 5 *Доказати да је за* $m \in N$ *производ* $(m+1)(m+2)\ldots(m+m)$ *дељив са* 2^m.

Решење: Дати израз се може записати као $\frac{(2m)!}{m!}$. Задатак се решава коришћењем математичке индукције.

1° За $m = 1$ израз је једнак 2 па је овај случај тривијалан.

2° Претпоставка је да је $m > 1$ и да израз важи за m. Треба доказати да дати израз важи и за $m + 1$.
Дати израз се може тривијално трансформисати
$\frac{(2(m+1))!}{(m+1)!} = 2(2m+1)\frac{(2m)!}{m!}$ одакле видимо да је индуктивна хипотеза такође доказана.

Задатак 6 *Доказати да је број дељив са* 3 *ако му је збир цифара дељив са* 3.

Решење: Ако број запишемо преко његових цифара: $a_n a_{n-1} \dots a_0$, вредност тог броја је $\sum_{k=0}^{n} 10^k * a_k$. Сума цифара тог броја је онда $\sum_{k=0}^{n} a_k$. Да бисмо доказали тврђење довољно је да покажемо да је разлика вредности броја и суме његових цифара дељива са 3, што се тривијално показује:
c$\sum 10^k * a_k - \sum a_k = \sum (10^k - 1) * a_k = \sum 9 * (10^{k-1} + \dots + 1)$.

Задатак 7 *Нека је* $\text{nzd}(a, b) = 1$. *Доказати да је* $\text{nzd}(a + b, a - b) \leq 2$.

Решење: Нека је $k = nzd(a + b, a - b)$. Ако k дели $a + b$ и $a - b$ онда k дели и збир и разлику та два броја: $k|(a + b) + (a - b)$, тј. $k|2a$, и $k|(a + b) - (a - b)$, тј. $k|2b$.
Како су a и b узајамно прости, на основу Еуклидовог алгоритма постоје бројеви m и n тако да важи $1 = a * m + b * n$. На основу претходног пасуса важи и да $k|2a * m$ и $k|2b * n$ па онда k дели и њихов збир, тј. $k|2a * m + 2b * n = 2 * (am + bn) = 2$ чиме је доказано тврђење.

Задатак 8 *Израчунати* $\text{nzd}(549, 387)$, $\text{nzd}(589, 343)$, $\text{nzd}(12606, 6494)$, $\text{nzd}(6188, 4709)$, *а затим изразити НЗД као линеарну комбинацију тих бројева.*

Решење:

- Одредимо $\text{nzd}(549, 387)$. Када применимо Еуклидов алгоритам добијамо:

$$\begin{aligned} 549 &= 387 * 1 + 162 \\ 387 &= 162 * 2 + 63 \\ 162 &= 63 * 2 + 36 \\ 63 &= 36 + 27 \\ 36 &= 27 + 9 \\ 27 &= 9 * 3 + 0 \end{aligned}$$

  значи $\text{nzd}(549, 387) = 9$. Низ дељења који чини Еулидов алгоритам се користи за представљање НЗД-а у облику линеарне комбинације тих бројева:

$$\begin{aligned} 9 &= 36 - 27 \\ &= 36 - (63 - 36) \\ &= -63 + 36 * 2 \\ &= -63 + (162 - 63 * 2) * 2 \\ &= 162 * 2 - 63 * 5 \\ &= 162 * 2 - (387 - 162 * 2) * 5 \\ &= -387 * 5 + 162 * 12 \\ &= -387 * 5 + (549 - 387) * 12 \\ &= 549 * 12 - 387 * 17 \end{aligned}$$

- На сличан начин се добија да је $\text{nzd}(589, 343) = 1$ и $589 * 99 - 343 * 170 = 1$, $\text{nzd}(12606, 6494) = 382$ и $-12606 + 6494 * 2 = 382$, $\text{nzd}(6188, 4709) = 17$ и $6188 * 121 - 4709 * 159 = 17$.

Задатак 9 *Одредити* $160^{-1} \pmod{841}$.

Решење: За израчунавање инверза користимо Еуклидов алгоритам. Применом Еуклидовог алгоритма добијамо да је $\text{nzd}(160, 841) = 1$ што значи да постоји инверз. Када изразимо НЗД у облику линеарне комбинације тих бројева добијамо да је $1 = -39 * 841 + 205 * 160$, па је $160^{-1} \pmod{841} = 205$.

Задатак 10 *Колико чинилаца има број* 945*?*

Решење: Када се број 945 растави на факторе добија се $945 = 3^3 * 5 * 7$. Фактори броја 945 могу бити само бројеви облика $3^{\alpha_1} * 5^{\alpha_2} * 7^{\alpha_3}$, где $\alpha_1 \in \{0, 1, 2, 3\}$, $\alpha_2 \in \{0, 1\}$, $\alpha_3 \in \{0, 1\}$ што значи да их има $4 * 2 * 2 = 16$.

Задатак 11 *Одредити* $2^{1000000} \bmod 7$.

Решење: Како је $2^3 \bmod 7 = 1$ важи да је $2^{1000000} = 2^{999999+1} = 2^{3*333333+1} = 2^{3*333333} * 2 = 2^{3^{333333}} * 2 = 1 * 2 = 2$.

Задатак 12 *Одредити сва решења конгруенција*

а) $3x \equiv 4 \pmod{7}$

б) $3x \equiv 4 \pmod{12}$

в) $9x \equiv 12 \pmod{21}$

г) $27x \equiv 25 \pmod{256}$

д) $27x \equiv 72 \pmod{900}$

ђ) $103x \equiv 612 \pmod{676}$

Решење:

а) $3x \equiv 4 \pmod{7}$

Када се на обе стране једначине дода број 3, добија се $3(x+1) \equiv 0 \pmod{7}$, односно $x+1 \equiv 0 \pmod{7}$ (пошто је $\text{nzd}(3,7)=1$). Одатле следи да је $x \equiv -1 \pmod{7}$, тј. $x = 7k-1, k \in \mathbb{Z}$.

б) $3x \equiv 4 \pmod{12}$

Једначина се може записати у облику $12|3x-4$. Како $3|12$ то значи да мора да важи и да $3|3x-4$, тј. $3|3(x-2)+2$ што никако није испуњено па смо добили контрадикцију. Нема решења.

в) $9x \equiv 12 \pmod{21}$

Ова једначина се може скратити са 3. Када се то уради добија се једначина $3x \equiv 4 \pmod{7}$ што је задатак под (a), што значи да је решење $x = 7k-1, k \in \mathbb{Z}$.

г) $27x \equiv 25 \pmod{256}$

Једначина се може записати у облику $256|27x-25$, што значи да постоји y тако да важи $27x-25 = 256y$, односно $27x-256y = 25$.

Применом Еуклидовог алгоритма добија се да је $\text{nzd}(27,256)=1$ и да важи $1 = 27*19 - 256*2$. Када се та једначина помножи са 25 добија се $25 = 27*950 - 256*50$. Када се ова једначина одузме од иницијалне једначине добија се да важи $27(x-950) - 256(y-50) = 0$, тј. $27(x-950) = 256(y-50)$. Како су 27 и 256 узајамно прости важи да је $x-950 = 256k, k \in \mathbb{Z}$, тј. $x = 950+256k, k \in \mathbb{Z}$.

д) $27x \equiv 72 \pmod{900}$

Ова једначина се може скратити са 9 након чега се добија $3x \equiv 8 \pmod{100}$. То значи да важи $100|3x-8$, тј. постоји y тако да важи $3x-8 = 100y$. Како су бројеви 8 и 100 дељиви са 4, а број 3 није дељив са 4 то значи да x мора бити дељиво са 4 па постоји променљива z тако да важи $x = 4z$. Када се то убаци у почетну једначину добија се $12z-100y = 8$. Када се та једначина подели са 4 добија се $3z-25y = 2$.

Применом Еуклидовог алгоритма добија се $\text{nzd}(3,25)=1$ и $1 = 1*25 - 3*8$, тј. $2 = 2*25 - 3*16$ што је једно решење једначине. Да би нашли опште решење треба одузети једначине чиме се добија $25(2+y) - 3(z+16) = 0$, тј. $25(2+y) = 3(z+16)$ одакле следи да је $z+16 = 25k, k \in \mathbb{Z}$, односно $x = 4z = 4(25k-16) = 100k-64, k \in \mathbb{Z}$.

ђ) $103x \equiv 612 \pmod{676}$

Једначина се може записати у облику $676|103x-612$. Како је $\text{nzd}(676,612)=4$ и 4 не дели 103, то значи да $4|x$ па постоји цео број z тако да је $x = 4z$. Када се то убаци у почетну једначину добије се

$676|103*4z-612$. Када се та једначина подели са 4 добија се да важи $169|103z-153$, односно постоји y тако да важи $103z-169y=153$.

Применом Еуклидовог алгоритма добија се да је $\text{nzd}(169,103)=1$ и да важи $103*64-169*39=1$. Када се та једначина помножи са 153 добије се да важи $103*9792-169*5967=153$. Када се та једначина одузме од почетне добије се да важи $103*(z-9792)=169*(y-5967)$, односно $z=9792+169k_1=159+169*k$, тј. $x=636+676k, k\in\mathbb{Z}$.

Задатак 13 *Одредити* $\varphi(n)$ *за* $n=90,91,\ldots,100$.

Решење: Решење ће бити приказано у табели. Прво ће сви бројеви бити факторисани па ће онда бити приказане вредности Ојлерове функције.

n	90	91	92	93	94	95	96	97	98	99	100
фактори	$2*3^2*5$	$7*13$	2^2*23	$3*31$	$2*47$	$5*19$	2^5*3	97	$2*7^2$	3^2*11	2^2*5^2
$\varphi(n)$	24	72	44	60	46	72	32	96	42	60	40

Задатак 14 *Доказати: број* m *је прост ако и само ако је* $\varphi(m)=m-1$.

Решење: Ако је број прост онда су сви бројеви мањи од њега узајамно прости са њим, а њих има $m-1$ па мора да важи да је $\varphi(m)=m-1$. Са друге стране, ако важи да је $\varphi(m)=m-1$ онда сви бројеви мањи од њега морају бити узајамно прости са њим па тај број мора бити прост (пошто га не дели ни један број мањи од њега).

Задатак 15 *Раставити на просте чиниоце бројеве* 82798848, 81057226635.

Решење: Добија се да је $82798848=2^8*3^5*11^3$ и да је $81057226635=3^3*5*7^3*11^2*17*23*37$.

Задатак 16 *Раставити на просте чиниоце бројеве* 10!, 15!, 20!, 30!.

Решење: Ови бројеви се лако факторису тако што се факторишу њихови чиниоци. На тај начин се добија да је $10!=2^8*3^4*5^2*7^1$,
$15!=10!*2^3*3^2*5*7*11*13=2^11*3^6*5^3*7^2*11*13$,
$20!=15!*2^7*3^2*5=2^18*3^8*5^4*7*2*11*13*17*19$
$30!=20!*2^8*3^6*5^3*7^2*11*13*23*29=2^26*3^14*5^7*7^4*11^2*13^2*17*19*23*29$.

Задатак 17 *Са колико нула се завршавају бројеви* 50!, 100!*?*

Решење: Број нула на крају броја ће одговарати степену броја 5 приликом факторисања датих бројева. Како се број 5 налази на сваком 5-том месту, и додатно на сваком 25 месту се налази 5^2 може се закључити да се број 50! завршава са $50/5+50/25=12$ нула, а да се број 100! завршава са $100/5+100/25=24$ нуле.

Задатак 18 *Одредити* $\varphi(n)$ *за* $n=375,720,957,988,1200,4320$.

Решење: Решење ће бити приказано у табели:

n	375	720	957	988	1200	4320
$\varphi(n)$	200	192	560	432	320	1152

Задатак 19 *Колико има бројева од* 1 *до* 120 *који нису узајамно прости са* 30*?*

Решење: Како је $30 = 2 * 3 * 5$ и $120 = 2^3 * 3 * 5$, бројеви који нису узајамно прости са 30 морају бити облика $2^{\alpha_1} * 3^{\alpha_2} * 5^{\alpha_3}$, где је $\alpha_1 \in \{0, 1, 2, 3\}$, $\alpha_2 \in \{0, 1\}$, $\alpha_3 \in \{0, 1\}$ (искључујући јединицу), па их има укупно $4 * 2 * 2 - 1 = 15$.

Задатак 20 *Зна се да је* $\varphi(a) = 120$ *и да је* $a = pq$*, где су* p*,* q *прости бројеви. Одредити* a*, ако је* $p - q = 2$*.*

Решење: Како су p и q прости бројеви, и како важи да је $p - q = 2$ онда важи да је $120 = \varphi(a) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = q^2 - 1$, односно $q = 11$, $p = 13$ па је $a = 143$.

Задатак 21 *Доказати да збир квадрата пет узастопних целих бројева не може бити потпуни квадрат.*

Решење:

Збир квадрата пет узастопних целих бројева може се представити као: $(n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2$. Број n се може представити као $n = 5k + r$, $r = 0, \pm 1, \pm 2$. Онда је вредност суме једнака $5 * ((5k + r)^2 + 2)$. Да би ова сума била квадрат онда број 5 мора делити израз $(5k + r)^2 + 2$.

Како r може бити $0, \pm 1, \pm 2$, добија се да је вредност овог израза по модулу 5 редом $2, 3, 1$, што значи да почетна сума никако не мозе бити квадрат целог броја.

Задатак 22 *Одредити сва целобројна решења једначина* $53x + 47y = 1$*,* $22x + 32y = 18$*.*

Решење:

- $53x + 47y = 1$.

  Применом Еуклидовог алгоритма добија се да је $1 = \text{nzd}\{53, 47\}$ и да важи $8 * 53 - 9 * 47 = 1$ чиме добијамо једно решење дате једначине. Када се ова једначина одузме од почетне добија се да је $53(x - 8) = -47(y + 9)$. Како су 53 и 47 узајамно прости то значи да мора постојати цео број k тако да важи да је $x = 8 + 47k$, $y = -53k - 9$, што је решење почетне једначине.

- $22x + 32y = 18$.

  Након дељења са 2 једначина постаје $11x + 16y = 9$. Применом Еуклидовог алгоритма добија се да је $1 = \text{nzd}\{11, 16\}$ и да важи

$11 * 3 - 16 * 2 = 1$. Након множења последње једначине са 9 добија се $11 * 27 + 16 * (-18) = 9$. Када се ова једначина одузме од почетне добија се да је $-11(x - 27) = 16(18 + y)$. Како су 11 и 16 узајамно прости, то значи да постоји цео број k тако да важи да је $x = 16k + 27$, $y = 11k - 18$, што је решење почетне једначине.

Задатак 23 *Направити табелу индекса по модулу* 29 *са основом* 2 *и табелу индекса по модулу* 23 *са основом* 3.

Решење:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2^n (\text{mod} 29)$	1	2	4	8	16	3	6	12	24	19	9	18	7	14	28
n	15	16	17	18	19	20	21	22	23	24	25	26	27	28	
$2^n (\text{mod} 29)$	27	25	21	13	26	23	17	5	10	20	11	22	15	1	

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$5^n (\text{mod} 23)$	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13
n	15	16	17	18	19	20	21	22							
$5^n (\text{mod} 23)$	19	3	15	6	7	12	14	1							

Задатак 24 *Ако је* $\text{nzd}(a, n) = 1$, *доказати да је* $a^{-1} \equiv a^{\varphi(n)-2} \pmod{n}$.

Решење:

Задатак 25 *Решити једначине* $52^x \equiv 38 \pmod{29}$, $23^x \equiv 9 \pmod{29}$, $3^x \equiv 7 \pmod{23}$, $3^x \equiv 6 \pmod{23}$.

Решење:

(а) $52^x \equiv 38 \pmod{29}$

након свођења по модулу 29, овај проблем се своди на $23^x \equiv 9 \pmod{29}$ што је други део овог задатка.

(б) $23^x \equiv 9 \pmod{29}$

Из табле добијене у једном од претходних задатака може се видети да је $9 \equiv 2^{10} \pmod{29}$, $23 \equiv 2^{20} \pmod{29}$ па добијамо да је $2^{20x} \equiv 2^{10} \pmod{29}$ односно $29 | 2^{20x} - 2^{10} = 2^{10} * (2^{20x-10} - 1)$. Како број 2^{10} није дељив са 29 то значи да је $2^{20x-10} \equiv 1 \pmod{29}$. Из табеле добијамо да је $1 = 2^{28} \pmod{29}$ што значи да постоји цео број n тако да важи $20x - 10 = 28n$, тј. $28 | 20x - 10 = 2(10x - 5)$. Број 28 је дељив са 4, а вредност са десне стране није дељива са 4 јер је израз $10x - 5$ увек непаран. Отуда следи да овај задатак нема решења.

(ц) $3^x \equiv 7 \pmod{23}$

Из табле добијене у једном од претходних задатака може се видети да је $3 \equiv 2^5 \pmod{29}$ и да је $7 \equiv 2^{12} \pmod{29}$. Отуда добијамо да је $29 | 2^{12}(2^{5x-12} - 1)$. Како 29 не дели 2^{12} добија се да је $29 | 2^{5x-12} - 1$. Из табеле се добија да је $1 = 2^{28} \pmod{29}$ што значи да постоји цео

број n тако да важи $5x - 12 = 28n$. Како 4 дели и број 12 и број 28 онда постоји цео број z тако да је $x = 4z$. Отуда следи да је $20z - 12 = 28n$, тј. $5z - 3 = 7n$. Отуда следи да $7|5z - 3 = 5z - 3 - 7 = 5z - 10 = 5(z - 2)$, односно $7|z - 2$ па постоји цео број k тако да важи $z = 7k + 2$. Отуда добијамо да је $x = 4z = 4(7k + 2) = 28k + 8$ што је решење нашег задатка.

(д) $3^x \equiv 6 \pmod{23}$

Из табеле добијене у једном од претходних задатака може се видети да је $3 \equiv 5^{16} \pmod{23}$, $6 \equiv 5^{18}$. Отуда добијамо да важи $23|5^{18}(5^{16x-18} - 1)$. Како 23 не дели 5^{18} то значи да мора да важи $23|5^{16x-18} - 1$. Из табеле видимо да је $1 \equiv 5^{22} \pmod{23}$ што значи да важи да $22|16x - 18$. Отуда добијамо $11|8x - 9 = 8x - 9 + 11 = 8x + 2 = 2(4x + 1)$ што значи да важи $11|4x + 1 = 4x + 1 + 11 = 4x + 12 = 4(x + 3)$. Отуда добијамо да постоји цео број n тако да је $x = 11n - 3 = 11n + 8$ па је решење наше једначине $x \equiv 8 \pmod{11}$.

Задатак 26 *Одредити све генераторе* $\mathbf{Z}/n\mathbf{Z}^*$ *за* $n = 23, 29$.

Решење:
За прост број p важи, ако је g генератор цикличне групе F_p^* онда је и g^k генератор те групе акко $\text{nzd}(k, p - 1) = 1$.
За $n = 23$ генератор је број 5 па је онда и свака вредност облика 5^k генератор те групе акко $\text{nzd}(k, 22) = 1$. Како је скуп бројева који су узајамно прости са 22: $\{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$ то значи да је скуп генератора: $\{5, 10, 20, 17, 11, 21, 19, 15, 7, 14\}$.
За $n = 29$ генератор је број 2 па је и свака вредност облика 2^k генератор те групе акко $\text{nzd}(k, 28) = 1$. Како је скуп бројева који су узајамно прости са 28: $\{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$ то значи да је скуп генератора: $\{2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15\}$.

Задатак 27 *Израчунати* $5^{-1} \pmod{29}$, $7^{-1} \pmod{29}$, $21^{-1} \pmod{29}$, $39^{-1} \pmod{23}$, $(-1)^{-1} \pmod{23}$.

Решење:

(а) $5^{-1} \pmod{29}$

Тражимо решење једначине $5 * x \equiv 1 \pmod{29}$. Из табеле видимо да је $1 \equiv 2^{28} \pmod{29}$ и да је $5 \equiv 2^{22} \pmod{29}$. Отуда добијамо да је $x \equiv 2^{28-22}$, тј. $x \equiv 2^6 \equiv 6 \pmod{29}$.

(б) $7^{-1} \pmod{29}$

Из табеле видимо да је $7 \equiv 2^{12} \pmod{29}$, па је $x \equiv 2^{16} \equiv 25$.

(ц) $21^{-1} \pmod{29}$

Из табеле видимо да је $21 \equiv 2^{17} \pmod{29}$ па је $x \equiv 2^{11} \equiv 18 \pmod{29}$.

(д) $39^{-1} \pmod{23}$

$39^{-1} \equiv 16^{-1} \equiv (5^8)^{-1} \equiv 5^{-8} \equiv 5^{22-8} \equiv 5^{14} \equiv 13 \pmod{23}$.

(е) $(-1)^{-1} \pmod{23}$

$(-1)^{-1} \equiv 22^{-1} \equiv (5^{11})^{-1} \equiv 5^{-11} \equiv 5^{22-11} \equiv 5^{11} \equiv 22 \equiv -1$.

Задатак 28 *Одредити све несводљиве полиноме степена* ≤ 3 *у* $\mathbf{F}_2[x]$.

Решење: Сви полиноми степена ≤ 3 су:
1, x, $x+1$, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+x^2, x^3+x, x^3+1, x^3+x^2+x, x^3+x^2+1, x^3+x+1, x^3+x^2+x+1.
Полиноми степена 2 који су сводљиви се могу добити као производ полинома степена 1. Таквих комбинација имамо 3:
$x*x = x^2$, $x*(x+1) = x^2+x$, $(x+1)*(x+1) = x^2+1$.
Преостали полином степена 2 који се не налази у овом скупу је несвољив: x^2+x+1.
Сада посматрамо полиноме чији је степен 3. Полиноми који су дељиви са x сигурно нису несводљиви па проверавамо да ли су несводљиви само полиноми који при дељењу са x дају остатак 1.
Полином x^3+1 се може раставити на $(x+1)*(x^2+x+1)$, па он није несводљив.
Полином
$x^3+x^2+x+1 = x^3+1+x^2+x = (x+1)(x^2+x+1)+x(x+1) = (x+1)(x^2+1)$
није несводљив.
Полином x^3+x+1 је несводљив јер је његов остатак при дељењу са x и $x+1$ једнак 1:
$x^3+x+1 \equiv_{x+1} x^3 \equiv x^3+1+1 \equiv 1$.
Полином x^3+x^2+1 је несводљив јер је његов остатак при дељењу са x и $x+1$ једнак 1:
$x^3+x+1 \equiv_{x+1} x^3+1+x^2 \equiv x^2 \equiv x^2+1+1 \equiv 1$.
Отуда видимо да је скуп несводљивих полинома:
$\{1, x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1\}$.

Задатак 29 *Да ли је несводљив полином* $x^4+x^3+x^2+x+1$ *у* $\mathbf{F}_2[x]$*?*

Решење: Да би проверили да ли је полином несводљив прво проверавамо да ли је дељив са неким полиномом степена 1:
$x^4+x^3+x^2+x+1 \equiv_x 1$, па није дељив са x.
$x^4+x^3+x^2+x+1 \equiv_{x+1} x^3(x+1)+x^2+x+1 \equiv x^2 \equiv x^2+1+1 \equiv 1$, па није дељив ни са $x+1$.
Што значи да ако је овај полином сводљив онда мора бити дељив са неким несводљивим полиномом степена 2. Једини такав полином је полином x^2+x+1, што значи да овај полином евентуално може бити квадрат тог полинома.
$(x^2+x+1)(x^2+x+1) = x^4+x^2+1$.
Како нисмо добили тражени полином то значи да је он несводљив.

Задатак 30 *Направити таблицу множења у а)* $\mathbf{F}_2[x]/(x^2+x+1)^*$*; б)* $\mathbf{F}_2[x]/(x^3+x^2+1)^*$.

Решење:

(а)

	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

(б)

	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	x^2+1	x^2+x+1	1	$x+1$
$x+1$	$x+1$	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	x^2	x^2+1	1	x^2+x+1	$x+1$	x	x^2+x
x^2+1	x^2+1	x^2+x+1	x	$x+1$	x^2+x	x^2	1
x^2+x	x^2+x	1	x^2+x+1	x	x^2	$x+1$	x^2+1
x^2+x+1	x^2+x+1	$x+1$	x^2	x^2+x	1	x^2+1	x

Задатак 31 *Помоћу Еуклидовог алгоритма одредити* $(x^4)^{-1}$ *у пољу* $\mathbf{F}_2[x]/(x^5+x^2+1)$.

Решење: На основу Еуклидовог алгоритма добијамо да је:

$$\begin{aligned} x^5+x^2+1 &= x*x^4+(x^2+1) \\ x^4 &= (x^2+1)*(x^2+1)+1 \end{aligned}$$

Овај низ дељења се користи за представљање НЗД-а у облику линеарне комбинације тих полинома:

$$\begin{aligned} 1 &= x^4+(x^2)(x^2+1) \\ &= x^4+(x^2+1)(x^5+x^2+1+x*x^4) \\ &= x^4+(x^2+1)*(x^5+x^2+1)+x*(x^2+1)*x^4 \\ &= x^4*(x^3+x+1)+(x^2+1)*(x^5+x^2+1) \end{aligned}$$

Одакле се добија да је $(x^4)^{-1}=x^3+x+1$ у пољу $\mathbf{F}_2[x]/(x^5+x^2+1)$.

Задатак 32 *Одредити матрице* A*,* B*, такве да се друга компонента пресликавања* S *у алгоритму* §AES *може представити у облику* $AY+B$*, где је* Y *вектор–колона — нибл добијен из прве компоненте* S *(инверзије).*

Решење: Колона нибл Y се може записати као $Y = [b_0, b_1, b_2, b_3]^T$, односно нибл који она представља као $N(Y) = b_0y^3 + b_1y^2 + b_2y + b_3$. Друга компонента пресликавања се може записати као $T(N) = a(y) * N(Y) + b(y)$, где је $a(y) = y^3 + y^2 + 1$, $b(y) = y^3 + 1$.

$$\begin{aligned} T(N) &= (y^3 + y^2 + 1)(b_0y^3 + b_1y^2 + b_2y + b_3) + (y^3 + 1) \\ &= y^3(b_0 + b_2 + b_3 + 1) + \\ &\quad y^2(b_0 + b_1 + b_3) + \\ &\quad y(b_0 + b_1 + b_2) + \\ &\quad 1(b_1 + b_2 + b_3 + 1) \end{aligned}$$

Одавде се могу директно извући две матрице A и B:

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Задатак 33 *Представити проширивање кључа у SAES (односно AES — већим дијаграмом) дијаграмом са шест чворова, три реда по два чвора, тако да у i-том реду буду чворови $W[2i]$, $W[2i + 1]$, $i = 0, 1, 2$.*

Решење:

Задатак 34 *Ако се погрешно пренесе један бит шифрата, колико ће то изазвати грешака у дешифрованој поруци ако се користи*

а) *синхрона проточна шифра;*

а) *самосинхронишућа проточна шифра код које c_i зависи од p_{i-k}, $p_{i-k+1}, \ldots, p_i$?*

Решење:

Задатак 35 *Колики највећи период може имати излазни низ из алгоритма RC4 (одговор треба да зависи од параметра n)?*

Решење:

Задатак 36 *Користећи чињеницу да функције MC у SAES трансформише колону* $\begin{array}{|c|}\hline b_0b_1b_2b_3 \\ \hline b_4b_5b_6b_7 \\ \hline \end{array}$ *у колону* $\begin{array}{|cccc|}\hline b_0 \oplus b_6 & b_1 \oplus b_4 \oplus b_7 & b_2 \oplus b_4 \oplus b_5 & b_3 \oplus b_5 \\ \hline b_2 \oplus b_4 & b_0 \oplus b_3 \oplus b_5 & b_0 \oplus b_1 \oplus b_6 & b_1 \oplus b_7 \\ \hline \end{array}$ $=$ $\begin{array}{|c|}\hline b'_0b'_1b'_2b'_3 \\ \hline b'_4b'_5b'_6b'_7 \\ \hline \end{array}$ *Одредити матрицу A која вектор $b = [b_0\ b_1\ \ldots b_7]^T$ пресликава у $b' = [b'_0\ b'_1\ \ldots b'_7]^T = Ab$*

Решење:

Задатак 37 *Од колико најмање бита стања алгоритма AES зависи неки бит стања после*

а) *функције ByteSub;*

б) *функције ShiftRow;*

в) *функције MixColumn;*

г) *функције AddRoundKey;*

д) *једне рунде?*

Решење:

Задатак 38 *Колико бита је погрешно после дешифровања поруке ако је шифровање извршено алгоритмом AES у режиму ECB, CBC, CFB, OFB?*

Решење:

Задатак 39 *Користећи табелу која описује функцију S у SAES написати изразе за четири излазна бита e, f, g, h преко улазних бита a, b, c, d.*

Решење: На основу табеле која описује S функцију, излазне битове можемо изразити преко улазних битова на следећи начин (увек ће само један од ових сабирака бити различит од нуле и то управо онај који ће бити једнак потребној вредности):

$$\sum_{\begin{pmatrix} k_0 \\ k_1 \\ k_2 \\ k_3 \end{pmatrix} \in \{0,1\}^4} S\begin{pmatrix} k_0 \\ k_1 \\ k_2 \\ k_3 \end{pmatrix} (a+k_0+1)(b+k_1+1)(c+k_2+1)(d+k_3+1)$$

Један начин да се ова функција израчуна је да се распише за свих 16 комбинација. Други начин је да вредности које се налазе уз конкретне комбинације записујемо кроз матрицу. Може се приметити да је довољно да посматрамо "десну" половину S табеле па ћемо из S таблице издвојити само излазне вредности:

$$S = \begin{bmatrix} 1001 & 0110 \\ 0100 & 0010 \\ 1010 & 0000 \\ 1011 & 0011 \\ 1101 & 1100 \\ 0001 & 1110 \\ 1000 & 1111 \\ 0101 & 0111 \end{bmatrix}$$

У изразу за функцију можемо издвојити комбинације које имају уз себе умножак a и оне које имају уз себе умножак $a+1$, па се функција може записати у облику:
$f = (a+1) * f_1(b,c,d) + a * f_2(b,c,d) = f_1(b,c,d) + a * (f_1 + f_2)(b,c,d)$.
Функције f_1 и f_2 можемо прочитати из S таблице (f_1 одговара левој половини S таблице, а f_2 одговара десној половини S таблице) па преко таблице сличне конструкције можемо израчунати и вредности функције $f_1 + f_2$. Њу ћемо добити тако што леву половину (излазних вредности) S таблице додамо на десну половину S таблице. Вредности функција f_1 и $f_1 + f_2$ ћемо представити исто преко матрице:

$$S' = \begin{bmatrix} 1001 & 1111 \\ 0100 & 0110 \\ 1010 & 1010 \\ 1011 & 1000 \\ 1101 & 0001 \\ 0001 & 1111 \\ 1000 & 0111 \\ 0101 & 0010 \end{bmatrix}$$

Након тога сличан поступак можемо поновити за комбинације које имају уз себе умножак b и оне које имају уз себе умножак $b+1$. Те комбинације ће бити сачуване у горњој, односно доњој половини таблице S', па на сличан начин добијамо табелу S'':

$$S'' = \begin{bmatrix} 1001 & 1111 \\ 0100 & 0110 \\ 1010 & 1010 \\ 1011 & 1000 \\ 0100 & 1110 \\ 0101 & 1001 \\ 0010 & 1101 \\ 1110 & 1010 \end{bmatrix}$$

Сада понављамо исту ствар за комбинације које имају уз себе умножак c и оне које имају уз себе умножак $c+1$. Те комбинације ће бити сачуване у редовима $1, 2, 5, 6$, односно у редовима $3, 4, 7, 8$. Табела S''' ће изгледати:

$$S''' = \begin{bmatrix} 1001 & 1111 \\ 0100 & 0110 \\ 0011 & 0101 \\ 1111 & 1110 \\ 0100 & 1110 \\ 0101 & 1001 \\ 0110 & 0011 \\ 1011 & 0011 \end{bmatrix}$$

И на крају понављамо исту ствар за комбинације које имају уз себе умножак d и оне које имају уз себе умножак $d+1$. Те комбинације ће бити сачуване у непарним, односно у парним редовима. Коначна верзија табеле је:

$$\begin{bmatrix} 1001 & 1111 \\ 1101 & 1001 \\ 0011 & 0101 \\ 1100 & 1011 \\ 0100 & 1110 \\ 0001 & 0111 \\ 0110 & 0011 \\ 1101 & 0000 \end{bmatrix}$$

И из ње сада можемо да прочитамо коефицијете наше функције:

$$\begin{aligned} (e,f,g,h) &= (1,0,0,1) + (1,1,0,1)d + (0,0,1,1)c + (1,1,0,0)cd + \\ &\quad (0,1,0,0)b + (0,0,0,1)bd + (0,1,1,0)bc + (1,1,0,1)bcd + \\ &\quad (1,1,1,1)a + (1,0,0,1)ad + (0,1,0,1)ac + (1,0,1,1)acd + \\ &\quad (1,1,1,0)ab + (0,1,1,1)abd + (0,0,1,1)abc + (0,0,0,0)abcd \\ &= (1+d+cd+bcd+a+ad+acd+ab, d+cd+b+bc+bcd+a+ac+ab+abd, \\ &\quad c+bc+a+acd+ab+abd+abc, 1+d+c+bd+bcd+a+ad+ac+acd+abd+abc). \end{aligned}$$

Задатак 40 *Израчунати* $57^{1616} \pmod{97}$.

Решење: Како је 97 прост број и $\text{nzd}(57,97) = 1$ онда се може применити Мала Фермаова теорема па важи $57^9 6 \equiv 1 \pmod{97}$. Отуда добијамо да је: $57^{1616} \equiv (57^{96})^{16} * 57^{80} \equiv 57^{80} \equiv (-40)^{2*40} \equiv 1600^{40} \equiv 48^{40} \equiv (48^2)^{20} \equiv (24*96)^{20} \equiv (-24)^{20} \equiv ((-24)^2)^{10} \equiv 576^{10} \equiv (6*96)^{10} \equiv 6^{10} \equiv 2^{10} * 3^{10} \equiv 96^2 * 3^8 \equiv 3^8 \equiv 81^2 \equiv (-16)^2 \equiv 356 \equiv 62.$

Задатак 41 *Оценити сложеност израчунавања* B^N*; факторизације* N *дељењем са бројевима мањим од* $\sqrt{N}$.

Решење:

Задатак 42 *Направити таблицу степенова, односно логаритама, у* $\mathbf{F}_2[x]/(x^3+x^2+1)^*$ *ако је генератор* x*. Користећи ове табеле израчунати* $(x^2+1)(x^2+x+1)$.

Решење:

n	0	1	2	3	4	5	6
x^n	1	x	x^2	x^2+1	x^2+x+1	$x+1$	x^2+x

На основу ове табеле $x^2+1=x^3$, $x^2+x+1=x^4$; па је
$(x^2+1)(x^2+x+1)=x^3*x^4=x^7=1$.

Задатак 43 *Нека је n производ различитих простих бројева. Нека су бројеви $d,e\in N$ такви да за сваки прост $p|n$ важи $p-1|de-1$. Доказати да је $a^{de}\equiv a \pmod n$ за свако a, чак и ако је* $\mathrm{nzd}(a,n)>1$.

Решење: Треба доказати да је $a^{de}\equiv a \pmod n$, односно да $n|a^{de}-a=a(a^{de-1}-1)$. Како је $n=p_1*p_2*...p_k$, за неке просте бројеве p_i, довољно је да докажемо да за сваки број p_i који дели n важи $p_i|a(a^{de-1}-1)$.
У наставку задатка ћемо са p означавати произвољан прост број $p_i|n$. Разликујемо два случаја:

- $\mathrm{nzd}(p,a)=p$

  Тада је израз тривијално испуњен.

- $\mathrm{nzd}(p,a)=1$

  Тада важи Мала Фермаова теорема: $a^{p-1}\equiv 1 \pmod p$, тј. важи да $p|a^{p-1}-1$.

  На основу претпоставке задатка важи $p-1|de-1$ па онда постоји m тако да је $de-1=m(p-1)$. Онда се десни део израза може записати као

  $a^{de-1}-1=a^{m(p-1)}-1=(a^{p-1})^m-1^m$,

  што је дељиво са $a^{p-1}-1$ а то је дељиво са p, чиме је показано жељено тврђење.

Задатак 44 *Доказати да у пољу $\mathbf{F}_q$, ако је $q=p^k$, p – прост број, важи $(a+b)^p=a^p+b^p$.*

Решење: Како је $q=p^k$, довољно је показати да тврђење важи по модулу p. Односно довољно је показати да важи да $p|(a+b)^p-a^p-b^p$. Како је $(a+b)^p=\sum_{k=0}^{p}\binom{p}{k}a^{p-k}b^k$, онда је $(a+b)^p-a^p-b^p=\sum_{k=1}^{p-1}\binom{p}{k}$ што је једнако нули по модулу p јер је сваки сабирак једнак нули по модулу p. Наиме, како је $\binom{p}{k}=\frac{p!}{k!(p-k)!}=\frac{p*(p-1)...(p-k+1)}{k!}$, онда за $1\le k\le p-1$ важи да $p|\binom{p}{k}$, чиме је доказано наше тврђење.

Задатак 45 *На елиптичкој кривој $y^2=x^3-36^2$ нека је $P=(-3,9)$ и $Q=(-2,8)$. Одредити $P+Q$ и $2P$.*

Решење:

Задатак 46 *Колико решења има једначина $x^m\equiv 1 \pmod n$ за различите вредности m, $m<n$?*

Решење:

Задатак 47 *Ако је корисник грешком у систему RSA изабрао $n = p$ (p – прост), доказати да је систем лако разбити.*

Решење:

Задатак 48 *Показати да ако $x^2 \equiv d \pmod{n}$ има решење, и $n = pq$ (p, q – прости), онда ова конгруенција има 4 решења.*

Решење: Ако постоји једно решење x_0 такво да је $x_0^2 \equiv d \pmod{p}q$ онда је друго решење $x_1 = pq - x_0$. Наиме,
$x_1^2 \equiv (pq - x_0)^2 \equiv (pq)^2 - 2pqx_0 + x_0^2 \equiv x_0^2 \equiv d \pmod{p}q$.
Треће и четврто решење тражимо тако да задовољавају једначину
$pq|x^2 - d \equiv x^2 - x_0^2 \equiv (x - x_0)(x + x_0)$. Како су p и q прости бројеви то значи да мора да важи $p|x - x_0$ и $q|x + x_0$ (или обратно).
То значи да важи $x \equiv x_0 p mod p$ и $x \equiv -x_0 p mod q$, односно да постоје цели бројеви m_1 и m_2 такви да важи $x - x_0 = p * m_1$ и $x + x_0 = q * m_2$. Када одузмемо другу једначину од прве добијамо $2x_0 = q * m_2 - p * m_1$.
Како су p и q прости бројеви, они су и узајамно прости бројеви па на основу Еуклидовог алгоритма важи да постоје јединствени цели бројеви a и b такви да важи $a * p + b * q = 1$. Након множења ове једначине са $2x_0$ добијамо да важи $2a * p * x_0 + 2b * q * x_0 = 2x_0$, односно добијамо да је $m_2 = 2b * x_0$ и $m_1 = -2q * x_0$, тј. $x = x_0 + p * m_1 = x_0 - 2a * p * x_0 \pmod{p}$.
Четврто решење се добија на исти начин за случај када $q|x - x_0$ и $p|x + x_0$.

Задатак 49 *Број x, $1 \leq x \leq n-1$ је непокретна тачка за RSA систем са модулом n ако се пресликава у самог себе. Доказати: ако је x непокретна тачка, онда је и $n - x$ непокретна тачка.*

Решење:

Задатак 50 *Показати да у систему RSA са параметрима p, q, e, d има $r+s+rs$ непокретних тачака, где је $r = \text{nzd}(p-1, e-1)$, $s = \text{nzd}(q-1, e-1)$*

Решење:

Задатак 51 *Претпоставимо да сваки корисник A има тајни пар трансформација $f_A : \mathcal{P} \to \mathcal{P}$ где је $\mathcal{P}$ фиксирани скуп могућих отворених текстова. Алиса жели да Бобану сигурно пренесе поруку применом Меси–Омура поступка, тј. Алиса шаље $f_A(P)$ Бобану, који јој затим шаље $f_B(f_A(P))$, итд. Описати услове које треба да задовољи систем функција f_A да би систем функционисао.*

Решење:

Задатак 52 *За елиптичку криву $E : y^2 = x^3 + Ax + B$ извести изразе за збир две тачке $P + Q$, односно $P + P$.*

Решење: Нека су координате тачака $P(x_1, y_1)$ и $Q(x_2, y_2)$. За рачунање збира различитих тачака потребно је одредити једначину праве која их садржи:
$y = k * x + n$, где је $k = \frac{y_2 - y_1}{x_2 - x_1}$, $n = -k * x_1 + y_1$.
Након тога је потребно израчунати пресек ове праве са елиптичком кривом:
$(kx + n)^2 = x^3 + Ax + B$, након чега се добије једначина трећег степена:
$x^3 - k^2x^2 + (A - 2kn)x + B - n^2 = 0$ која мора имати три решења (од којих су нам два већ позната: x_1 и x_2) па се може записати и у облику
$(x - x_1)(x - x_2)(x - x_3) = 0$. Када се ова једначина распише добија се
$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3 = 0$.
Након изједначавања коефицијената уз одговарајуће степене од x добија се координата треће пресечне тачке: $x_1 + x_2 + x_3 = k^2$, тј.
$x_3 = k^2 - x_1 - x_2$, и одговарајућа y координата $y_3 = k * x_3 + n$.
Тачка која је једнака збиру тачака P и Q има координате $(x_3, -y_3)$.
Да би се израчунао збир $P + P$ потребно је одредити једначину тангенте на елиптичку криву у тој тачки. Коефицијент тангенте се добија помоћу одређивања извода, тј. $2y(x) * k = 3x^2 + A$, одакле се добија да је
$k = \frac{3x_1^2 + A}{2y_1}$. Надаље је процес рачунања исти као у претходном случају с тим што је $x_2 = x_1$ па се добија да је $x_3 = k^2 - 2 * x_1$ и $y_3 = k * x_3 + n$. Па тачка која је једнака збиру тачке P са самом собом има координате $(x_3, -y_3)$.

Задатак 53 *Доказати да елиптичка крива над пољем* $\mathbf{F}_q$ *има највише* $2q+1$ *тачку.*

Решење: Све тачке елиптичке криве могу бити представљене у облику (x, y), где $x, y \in F_q$. То значи да могућих вредности за x координату има највише q. За сваку x координату могу постојати највише две тацке (са једнаким y координатама по апсолутној вредности) које јој одговарају. Укупно то је $2q$ тачака. Осим тих тачака и бесконачно далека тачка увек припада елиптичкој кривој што укупно даје $2q + 1$ тачака.

Задатак 54 *За елиптичку криву* $E : y^2 = x^3 + 3x + 8$ *над пољем* $\mathbf{F}_{13}$

а) *показати да је скуп тачака криве*

$$E(\mathbf{F}_{13}) = \{\oslash, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\};$$

б) *израчунати* $(1,8) + (9,7)$, $2(9,7)$*;*

в) *показати да* $(1,5)$ *генерише криву, а затим направити табелу умножака те тачке и табелу логаритама;*

г) *користећи ову табелу израчунати* $(12,11)+(2,3)$, $(12,2)+(9,6)$, $25(9,7)$.

Решење:

а) Могуће вредности за x координате су $\{0, 1, \ldots, 12\}$. Проверавамо за које вредности може да се нађе решење једначине. Потребне су нам и све могуће вредности за y и вредности квадрата:

y	0	±1	±2	±3	±4	±5	±6
y^2	0	1	4	9	3	12	10

За $x = 0$, нема решења јер важи да је $x^3 + 3x + 8 = 8$, што није једна од могућих вредности квадрата.

За $x = 1$, $x^3 + 3x + 8 = 12 = (\pm5)^2$, што значи да су тачке $(1, 5)$ и $(1, 8)$ решења једначине.

За $x = 2$, $x^3 + 3x + 8 = 9 = (\pm3)^2$, што значи да су тачке $(2, 3)$ и $(2, 10)$ решења једначине.

За $x = 9$, $x^3 + 3x + 8 = 10 = (\pm6)^2$, што значи да су тачке $(9, 6)$ и $(9, 7)$ решења једнахине.

За $x = 12$, $x^3 + 3x + 8 = 4 = (\pm2)^2$, што значи да су тачке $(12, 2)$ и $(12, 11)$ решења једначине.

За вредности $x = 3, 4, 5, 6, 7, 8, 10, 11$ добијају се редом вредности $x^3 + 3x + 8 = 5, 6, 7, 8, 8, 11, 11, 7$ што нису квадрати па нема више решења дате једначине.

Скуп тачака криве је значи:

$$E(\mathbf{F}_{13}) = \{\oslash, (1, 5), (1, 8), (2, 3), (2, 10), (9, 6), (9, 7), (12, 2), (12, 11)\};$$

б) За рачунање збира тачака $(1, 8)$ и $(9, 7)$ потребно је прво одредити једначину праве која их садржи. На основу формула изведених у једном од претходних задатака добија се да је та права одређена једначином $y = 8x$ (односно $k = 8$, $n = 0$) и да тачка која представља збир одређена једначином
$(x_3, -y_3) = (k^2 - x_1 - x_2, -(k * x_3 + n)) = (2, 10)$.

За рачунање вредности $2(9, 7) = (9, 7) + (9, 7)$ потребно је одредити једнахину тангенте на дату елиптичку криву у тачки $(9, 7)$. На основу раније изведених формула добијамо да је једначина те тангенте $y = 12x + 3$, (односно $k = 12$, $n = 3$) па је тачка која представља овај збир одређена једначином
$(x_3, -y_3) = (k^2 - x_1 - x_1, -(k * x_3 + n)) = (9, 6)$.

в) Да би показали да је тачка $G = (1, 5)$ генератор ове криве потребно је израчунати вредности $2G, 3G, \ldots, 8G$. На основу формула изведених у једном од претходних задатака лако се добија следећа табела:

n	0	1	2	3	4	5	6	7	8
nG	$\oslash$	$(1, 5)$	$(2, 10)$	$(9, 7)$	$(12, 2)$	$(12, 11)$	$(9, 6)$	$(2, 3)$	$(1, 8)$

г) На основу табеле све тачке можемо изразити преко генератора. Тај скуп чини цикличну групу која има 9 тачака.

$(12,11)+(2,3)=5G+7G=12G=3G=(9,7)$

$(12,2)+(9,6)=4G+6G=10G=G=(1,5)$

$25(9,7)=25*3G=75G=3G=(9,7).$

Задатак 55 *За ПУКДХ користи се елиптичка крива из претходног задатка. Ако се користи генератор* $(2,3)$*, а тајни кључеви су* $e_A=4$*,* $e_B=5$*, одредити тачку која се добија као резултат усаглашавања.*

Решење: Нека је $G(2,3)$. Јавни кључеви су
$G^{e_A}=4*G=4*7*(1,5)=28(1,5)=(1,5)$ и
$G^{e_B}=5*G=5*7*(1,5)=35(1,5)=8(1,5)=(1,8)$.
Тачка која се добија као резултат усаглашавања је
$((G^{e_A})^{e_B}=e_B*G^{e_A}=5(1,5)=(12,11)$.

Задатак 56 *За систем ЕлГамал користи се елиптичка крива из претпретходног задатка, а генератор из претходног задатка. Ако су тајни кључеви* $e_A=5$*,* $e_B=3$*, приказати поступак шифровања поруке* $M=(12,11)$ *(користи се случајни број* $k=4$*), а затим поступак дешифровања шифрата.*

Решење: У систему ЕлГамал јавно се објављује пар $(G^k, M*(G^{e_B})^k)$.
Израчунавамо $G^k=4G=4(2,3)=4*7*(1,5)=(1,5)$,
$G^{e_B}=3G=3(2,3)=3*7*(1,5)=21(1,5)=3(1,5)=(9,7)$,
$(G^{e_B})^k=4*(9,7)=4*3*(1,5)=12(1,5)=3(1,5)=(9,7)$,
$M*(G^{e_B})^k=(12,11)+(9,7)=5(1,5)+3(1,5)=8(1,5)=(1,8)$, и добијамо
$(G^k, M*(G^{e_B})^k)=((1,5),(1,8))$.
Поступак дешифровања се састоји у израчунавању поруке M на основу објављеног пара тачака: $M=[M*(G^{e_B})^k]*[(G^{e_B})^k]^{-1}$.
На основу објављеног пара тачака рачуна се:
$(G^k)^{e_B}=e_B*(1,5)=3(1,5)=(9,7)$,
$[(G^{e_B})^k]^{-1}=((G^k)^{e_B})^{-1}=-(9,7)=-3(1,5)=6(1,5)=(9,6)$,
$M=[M*(G^{e_B})^k]*[(G^{e_B})^k]^{-1}=(1,8)+(9,6)=8(1,5)+6(1,5)=14(1,5)=5(1,5)=(12,11)$.

Задатак 57 *У систему аутентикације заснованом на RSA корисник A изабрао је јавни кључ* $e=7$ *и* $n=77$*. Ако је он од B добио број* 23*, како треба да гласи његов одговор, да би саговорника убедио у свој идентитет?*

Решење: Јавни подаци су (n,e), а тајни подаци су (d,p,q), где је $n=pq$, а d се добија преко једначине $d\equiv e^{-1} \pmod{\phi)n}$ где је e број за који важи $\mathrm{nzd}(e,\phi n)=1$.
У овом случају $p=7$, $q=11$, $e=7$, $d=43$. Тада је порука која се шаље једнака $M^d=23^43 \pmod 7)7=23$.

Задатак 58 *За дигиталне потписе засноване на систему RSA корисници A иB имају јавне кључеве* $e_A=3$*,* $n_A=15$*, односно* $e_B=7$*,* $n_B=77$*. B жели да пошаље поруку* $M=4$ *као потпис неког текста. Који цели број он треба да пошаље?*

Решење: Корисник A има свој пар јавних кључева (n_A, e_A) и тајни кључ d_A, B има свој пар јавних кључева (n_B, e_B) и тајни кључ d_B. Ако корисник B шаље поруку као потпис он ће израчунати вредност $M^{d_B} \pmod{n)_B}$. Како је $d_B = e_B^{-1} \pmod{n)_B} = 7^{-1} \pmod{7)7} = 43$, вредност која се шаље је $M^{d_B} \pmod{n)_B} = 4^{43} \pmod{7)7} = 53$.

Задатак 59 *Доказати да за дигиталне потписе засноване на RSA важи следеће тврђење: ако је S_1 потпис поруке m_1, а S_2 потпис поруке m_2, онда је S_1S_2 потпис поруке m_1m_2.*

Решење: Потпис поруке m_1 је вредност $S_1 = m_1^d$, потпис поруке m_2 је вредност $S_2 = m_2^d$. Потпис поруке m_1m_2 ће бити вредност $S = (m_1m_2)^d = m_1^d m_2^d = S_1S_2$.

Задатак 60 *Корисник A има јавни кључ $e = 11$, $n = 899$. Како гласи његов RSA дигитални потпис поруке 876?*

Решење: Како је $n = 899$, $\phi n = \phi 29 * 31 = 840$. Након тога рачуна се $d = e^{-1} \pmod{\phi)n} = 11^{-1} \pmod{8)40} = 611 \pmod{8)40}$. Дигитални потпис поруке $M = 876$ је $M^d \pmod{n} \equiv 876^{611} \pmod{8)99} \equiv 225$.

Задатак 61 *ЕлГамал дигитални потпис. Особа A бира прост број $p = 21739$ и примитивни корен $g = 7$, а затим тајни кључ $a_A = 15140$.*

а) *Који је њен јавни кључ?*

б) *Шта је потпис поруке $S = 5331$ ако се користи кључ сесије $k = 10727$?*

б) *Како прималац B проверава потпис?*

Решење:

а) Јавни кључ је $g^{a_A} \pmod{21739} = 17702$.

б) Потпис поруке $S = 5331$ се рачуна уз помоћ $r = g^k \pmod{21739} = 15755$, $x = (S - a_A r)k^{-1} \pmod{21738} = (5331 - 15140 \cdot 15775) \cdot 6353 \equiv 791 \pmod{21738}$ и гласи $(r, x, S) = (15755, 791, 5331)$.

б) Да би прималац B проверио потпис он мора да израчуна и упореди $(g^{a_A})^r r^x = 17702^{15775} \cdot 15775^{791} \equiv 13897 \pmod{21739}$ и $g^S = 7^{5331} \equiv 13897 \pmod{21739}$, што су исте вредности.

Задатак 62 *Одредити верижни развој бројева $\sqrt{3}$, $\sqrt{5}$, $\sqrt{7}$, $\frac{7}{23}$, π и одредити првих 8 парцијалних разломака.*

Решење: Верижни развој броја $\sqrt{3}$ је $[1, 1, 2, 1, 2, ...]$, а првих 8 парцијалних разломака се налазе у наредној табели:

n	-1	0	1	2	3	4	5	6	7
a_n		1	1	2	1	2	1	2	1
P_n	1	1	2	5	7	19	26	71	97
Q_n	0	1	1	3	4	11	15	41	56

Верижни развој броја $\sqrt{5}$ је $[2, 4, 4, 4, 4...]$, а првих 8 парцијалних разломака се налазе у наредној табели:

n	-1	0	1	2	3	4	5	6	7
a_n		2	4	4	4	4	4	4	4
P_n	1	2	9	38	161	682	2889	12238	51841
Q_n	0	1	4	17	72	305	1292	5473	23184

Верижни развој броја $\sqrt{7}$ је $[2, 1, 1, 1, 4, 1, 1, 1, 4, ...]$, а првих 8 парцијалних разломака се налазе у наредној табели:

n	-1	0	1	2	3	4	5	6	7
a_n		2	1	1	1	4	1	1	1
P_n	1	2	3	5	8	37	45	82	127
Q_n	0	1	1	2	3	14	17	31	48

Верижни развој броја $\frac{7}{23}$ је $[0, 3, 3, 2]$. Како је у питању рационалан број, и верижни развој и број парцијалних разломака је коначан:

n	-1	0	1	2	3
a_n		0	3	3	2
P_n	1	0	1	3	7
Q_n	0	1	3	10	23

Верижни развој броја π је $[3; 7, 15, 1, 292, 1, 1, 1, 2, ...]$, а првих 8 парцијалних разломака се налази у наредној табели:

n	-1	0	1	2	3	4	5	6	7
a_n		3 7 15 1 292 1 1 1							
P_n	1	3	22	333	355	103993	104348	208341	312689
Q_n	0	1	7	106	113	33102	33215	66317	99532

Задатак 63 *Одредити орбите за линеарне померачке регистре:* $1 + x^2 + x^3 + x^4$, $1 + x + x^5$, $1 + x + x^6$.

Решење:

- Ако је линеарни померачки регистар задат полиномом $P(x) = 1 + x^2 + x^3 + x^4$, то значи да је функција која даје последњи бит наредног стања дефинисана са $(b_0, b_1, b_2, b_3) = (1, 0, 1, 1)$, тј. $f(s_0, s_1, s_2, s_3) = s_0 + s_2 + s_3$.

  Како је $n = 4$ то значи да укупно имамо $2^4 = 16$ стања. Приликом одређивања орбита крећемо од произвољног стања, на пример $(1, 0, 0, 0)$ и добијамо прву орбиту (која има 7 елемената):

1000
0001
0011
0110
1101
1010
0100

За одређивање наредне орбите бирамо стање које се не налази у претходној орбити, на пример $(1, 1, 1, 0)$ и добијамо другу орбиту (која има исто 7 елемената):

1110
1100
1001
0010
0101
1011
0111

Трећу орбиту одређује само једно стање $(0, 0, 0, 0)$ и четврту орбиту такође одређује само једно стање $(1, 1, 1, 1)$.

- Ако је линеарни померачки регистар задат полиномом $P(x) = 1 + x + x^5$, то значи да је функција која даје последњи бит наредног стања дефинисана са $(b_0, b_1, b_2, b_3, b_4) = (1, 1, 0, 0, 0)$, тј. $f(s_0, s_1, s_2, s_3, s_4) = s_0 + s_1$.

  Како је $n = 5$ то значи да укупно имамо $2^5 = 32$ стања. Приликом одређивања прве орбите узимамо произвољно стање, приликом одређивања друге орбите узимамо произвољно стање које се не налази у првој орбити и тако даље. На тај начин добијамо 4 орбите приказане у наредној табели:

Прва орбита	00001 00010 00100 01000 10001 00011 00110 01100 11001 10010 00101 01010 10101 01011 10111 01111 11111 11110 11100 11000 10000
Друга орбита	01110 11101 11010 10100 01001 10011 00111
Трећа орбита	01101 11011 10110
Четврта орбита	0000

- Ако је линеарни померачки регистар задат полиномом $P(x) = 1 + x + x^6$, можемо одредити орбите померачког регистра на начин описан у претходном примеру.

  Други начин да проверимо да ли овај померачки регистар даје орбиту максималне дужине је да проверимо да ли је полином $P(x)$ примитиван. Односно, да проверимо да ли је полином $P(x)$ несводљив и да ли је x генератор групе $F_{2^n}^* = F_2[x]/P(x)$. Уколико је $2^n - 1$ прост број онда је довољно проверити да ли је $P(x)$ несводљив.

Да би проверили да ли је полином $P(x) = 1 + x + x^6$ несводљив, потребно је за почетак одредити остатак при дељењу са x, и остатак при дељењу са $x + 1$. Добијају се остаци, редом, 1 и x. То значи да су потенцијални делиоци овог полинома само несводљиви полиноми степена 2 или 3.

Како постоји само један несвођив полином степена 2 и како је вредност $(1 + x_x^2)^3 = 1 + x + x^3 + x^5 + x^6$ то значи да га тај полином не дели.

Остало је још да проверимо да ли је дељив полиномом степена 3. Постоје два несводљива полинома степена 3: $1 + x + x^3$ и $1 + x^2 + x^3$ па проверавамо да ли је почетни полином једнак квадрату једног од ова два полинома или да ли је једнак њиховом производу. Како је $(1 + x + x^3) * (1 + x^2 + x^3) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$, $(1 + x + x^3)^2 = 1 + x^2 + x^6$ и $(1 + x^2 + x^3)^{=}1 + x^4 + x^6$, то значи да је полином $P(x)$ несводљив.

Сада треба проверити да ли је x генератор цикличне групе остатака по модулу $P(x)$. Један начин је да одредимо све вредности $x^0, x^1, x^2, \ldots, x^{63}$. Други, мало бржи начин, је да проверимо да ли је $x^{63} = 1$ и да ли неки делилац броја 63 можда генерише цикличну групу, тј. треба да проверимо да ли је $x^d! = 1$, за $d \in \{3, 7, 9, 21, 27\}$.

На начин описан у претходним задацима лако се проверава да је $x^{63} = 1$ и да је $x^3 = x^3! = 1$, $x^7 = x^2 + x! = 1$, $x^9 = x^4 + x^3! = 1$, $x^{21} = x^5 + x^4 + x^3 + x + 1! = 1$ и $x^{27} = x^3 + x^2 + x + 1! = 1$, што значи да x јесте генератор те групе па постоји орбита максималне дужине.

Задатак 64 *Одредити повратне спреге линеарног померачког регистра дужине* 5 *на основу отвореног и шифрованог текста:* $OT = [4, 0] = [00100, 00000]$, $ST = [17, 30] = [10001, 11110]$.

Решење:

Задатак 65 *Одредити линеарне комбинације улаза и излаза најближе константи за табелу* S *у SAES , и за sbox-ове* $S1$ *и* $S4$ *за DES .*

Решење: Решење се може наћи у оквиру `Е7ел` фајла у фолдеру `Криптографија`.

Задатак 66 *Раставити на чиниоце* 14873 *поступком који користи случајно лутање по модулу* 14873.

Решење: Поступак који користи случајно лутање се састоји од израчунавања елемената низа a који је дефинисан са $a_0 = 0$, $a_{m+1} = a_m^2 + 1$ и одређивању у сваком кораку вредности $\mathrm{nzd}(a_{2i} - ai, n)$. Када добијемо број различит од 1 нашли смо један делиоц броја n. Тај поступак може бити приказан наредном табелом:

и	a_i	a_{2i-1}	a_{2i}	$\mathrm{nzd}(a_{2i}-a_i, n)$
1	1	1	2	1
2	2	5	26	1
3	5	677	12140	1
4	26	3044	58	1
5	677	3365	4873	1
6	12140	8822	12149	1
7	3044	13423	5408	1
8	58	6147	8190	107

Што значи да су делиоци броја n бројеви 107 и $n/107 = 139$.

Задатак 67 *Применити Фермаов поступак факторизације на број* 21079.

Решење: Фермаов поступак факторизације се састоји прво од рачунања вредности $k = \lceil \sqrt{n} \rceil = 146$, па затим рачунања вредности $\sqrt{k^2 - n}$ и повећавања броја k док се не добије целобројна вредност корена.
Поступак је приказан у наредној табели:

k	$\sqrt{k^2-n}$
146	15,39
147	23,02
148	28,72
149	33,49
150	37,69
151	41,49
152	45

Након тога се делиоци броја n добијају захваљујући томе што смо нашли два броја који задовољавају једначину $x^2 - n = y^2$, тј.
$n = x^2 - y^2 = (x-y)(x+y) = 107 * 197$.

Задатак 68 *Доказати да су у пољу* $\mathbf{Q}(\sqrt{-5})$ *алгебарски цели бројеви облика* $a + b\sqrt{-5}$, $a, b \in \mathbf{Z}$.

Решење: Број је алгебарски ако је најстарији коефицијент његовог минималног полинома једнак 1. Одредимо $f(x)$ минимални полином за број $\alpha = a + b\sqrt{-5}$. Ако је α корен тог полинома онда $x - \alpha | f(x)$, али такође и $x - \bar{\alpha} | f(x)$ па се минимални полином може добити као:
$f(x) = (x-\alpha)(x-\bar{\alpha}) = (x - a - b\sqrt{-5})(x - a + b\sqrt{-5}) = x^2 - 2ax + a^2 + 5b^2$.
Како коефицијенти минималног полинома морају бити целобројни, одатле можемо закључити да ако су a или b рационални бројеви онда ће најмањи коефицијент бити различит од 1, па одатле следи да a и b морају бити цели бројеви.

Задатак 69 *Доказати да се у пољу* $\mathbf{Q}(\sqrt{-5})$ *број* 2 *не може раставити у нетривијални производ алгебарских целих бројева.*

Решење: Треба доказати да је једини начин да се број 2 растави на производ алгебарских целих бројева један од следећих:

$2 = 1 * 2 = 2 * 1 = (-1) * (-2) = (-2) * (-1)$ (њих сматрамо тривијалним производима).
Претпоставимо супротно: постоје алгебарски цели бројеви $a + b\sqrt{-5}$ и $c + d\sqrt{-5}$, $a, b, c, d \in \mathbb{Z}$, тако да важи
$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}$.
Покушавамо да решимо систем од следеће две једначине:
$ac - 5bd = 2$
$ad + bc = 0$
Разматраћемо два случаја, када је $b = 0$ и када је $b! = 0$.
У случају $b = 0$ добија се да је $d = 0$ и да је $ac = 2$, што значи да добијамо тривијални производ.
У случају $b! = 0$ поново разматрамо два случаја, када је $d = 0$ и када је $d! = 0$. Ако је $d = 0$ онда мора да важи и $c = 0$ што не може да важи, па нам остаје још само случај када је $d! = 0$. У том случају увешћемо променљиву $t = \frac{a}{b} = -\frac{c}{d}$, односно изразићемо променљиве a и c преко променљивих b, d и t на следећи начин:
$a = bt$, $c = -dt$.
Када ове једначине убацимо у почетну једначину добијамо:
$2 = ac - 5bd = bt(-dt) - 5db = -bd(5 + t^2)$. Како је t цео број, мора да важи да је $t^2 > 0$ па је вредност $5 + t^2 > 5 > 2$ што је у контрадикцији са претпоставком да тај број дели број 2, чиме смо доказали да се број 2 не може раставити у нетривијални производ.

Задатак 70 *У скупу* $\mathbf{Z}(i)$ *раставити на чиниоце бројеве* $11 - 3i$, $5 + 3i$.

Решење:

- Да би раставили број $11 - 3i$ на чиниоце, прво израчунавамо вредност $N(11 - 3i) = 11^2 + 3^2 = 130 = 2 * 5 * 13$. Што значи да је скуп могућих делиоца једнак $1 + i$, i, $2 \pm i$ и $3 \pm 2i$.

  Како је $\frac{11-3i}{2+i} = \frac{25-17i}{5}$, то значи да број $2 + i$ није један од делиоца па покушавамо са неким другим делиоцем.

  $\frac{11-3i}{2-i} = 5 + i$, па $2 - i$ јесте један од делиоца. Да би нашли остале делиоце настављамо са бројем $5 + i$ и преосталим делиоцима из скупа могућих делиоца:

  $\frac{5+i}{1+i} = 3 - 2i$, што значи да је $1 + i$ такође један од делиоца, а како смо као резултат добили број $3 - 2i$ који се налази у скупу могућих делиоца, то значи да факторизација изгледа овако
  $11 - 3i = (2 - i)(1 + i)(3 - 2i)$.

- $N(5 + 3i) = 34 = 2 * 17$, па је скуп могућих делиоца једнак i, $1 + i$, $4 \pm i$.

  Како је $\frac{5+3i}{4+i} = \frac{23+7i}{17}$, то значи да број $4 + i$ није један од делиоца па покушавамо са неким другим.

  $\frac{5+3i}{4-i} = 1 + i$, што значи да је $5 + 3i = (1 + i)(4 - i)$.