Planetcalc

nicoleta.dumitru@my.fmi.unibuc.ro

for modulo comp.

Ex#1 (Examen 31 Mai 2024)

Rings of Remainders Rezolvați

$$x^{256}=1$$

în inelul $(\mathbb{Z}_{1024}, +, \times, 0, 1)$. Câte soluții avem și care este forma lor.

Dem

- Știm că $\#U(\mathbb{Z}_{1024}) = \varphi(1024) = \varphi(2^{10}) = 2^9 = 512$.
- Observăm că 512 este nr. de elem. impare din $\mathbb{Z}_{1024}$
- $U(\mathbb{Z}_{1024})$ nu este ciclic.

$\cdot\ (2^n-1)^2 = 2^{2n}+1-2^{n+1} = 1 \mod 2^n$

$\cdot\ (2^{n-1}+1)^2 = 2^{2n-2}+1+2^n = 1 \mod 2^n$

$\square$

$\Rightarrow$ ordinul elementelor din $U(\mathbb{Z}_{1024})$ este mereu un divizor de-al lui 512, mai mic ca 512.

$512 = 2 \cdot 256$

Deci toți divizorii lui 256.

Prin urmare, orice x impar satisface $x^{256} = 1 \mod 2^{10}$

$\boxed{\text{Planetcalc}}$ ← for modulo comp.

nicoleta.dumitru@my.fmi.unibuc.ro

$\boxed{\text{Ex\#1}}$ (Examen 31 Mai 2022)

Rings of Remainders Rezolvați

$x^{256}-1$

este formula lor.

Evident, x par nu satisface.

Fie $k \in \mathbb{Z}$ a.î. $x = 2k$.

$x^{256} = (2k)^{256} = 2^{256} k^{256} = \underline{2^{10}} \cdot 2^{246} k^{256} = 0 \mod 2^{10}$

$\Rightarrow$ Avem 512 soluții.

$\square$

Ex#2 (Examen 24 noiem. 2021)

RSA: O pers. criptează mesajul m mod 85 folosind cheia publică $e = 11$ și obț. $c = 12$.
Decriptați folosind $\lambda(N)$.

RSA → clasică $\varphi(N)$
RSA → modif. $\lambda(N)$

Planetcalc

nicoleta.dumitru@my.fmi.unibuc.ro

for modulo comp.

$N = 85$ fol. $\lambda(N)$.

$e = 11$

$c = 12$

Obs. că $N = 85 = 5 \cdot 17$.

Calc. $\lambda(N) = \lambda(85) = \lambda(5 \cdot 17) = \mathrm{lcm}(5-1, 17-1) = \mathrm{lcm}(4, 16) = 16$

Știm $de \equiv 1 \bmod \lambda(N)$

$11d \equiv 1 \bmod 16 \Rightarrow d = 11^{-1} \bmod 16$

Aplicăm Euclid extins:

$$16 = 11 \cdot 1 + 5$$
$$11 = 5 \cdot 2 + 1 \Rightarrow 1 = 11 - 5 \cdot 2$$
$$= 11 - (16 - 11) \cdot 2 = 11 \cdot 3 - 16 \cdot 2 \pmod{16}$$

$1 = 11 \cdot 3 \mod 16$

$11^{-1} = 3 \mod 16$

$\Rightarrow \boxed{d = 3}$

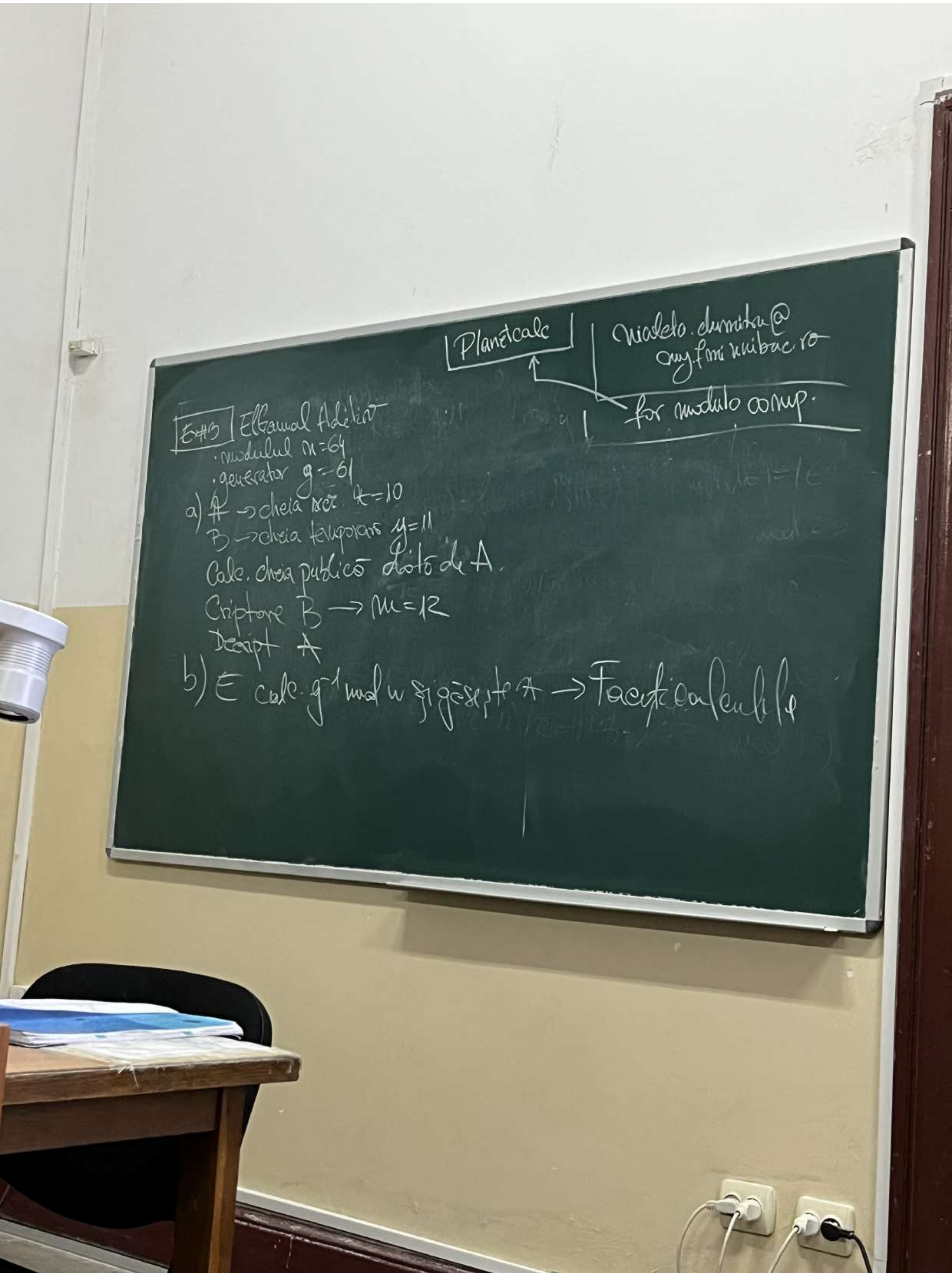
Calculăm $m = c^{d} \mod N$

$m = 12^{3} \mod 85$

$m = 12^{2} \cdot 12 \mod 85$

$m = 28 \mod 85$

$\square$


Planetcalc
nicoleta.dumitru@
my.fmi.unibuc.ro
for modulo comp.
Ex#3 ElGamal Aditiv
· modulul n=64
· generator g=61
a) A → cheia secr. x=10
B → cheia temporară y=11
Calc. cheia publică dată de A.
Criptare B → m=12
Decript A
b) E calc. g-1 mod n şi găseşte A →

Obs

Lucrăm în $(\mathbb{Z}_{64}, +)$

a). Cheia publică $h = g x \bmod 64$

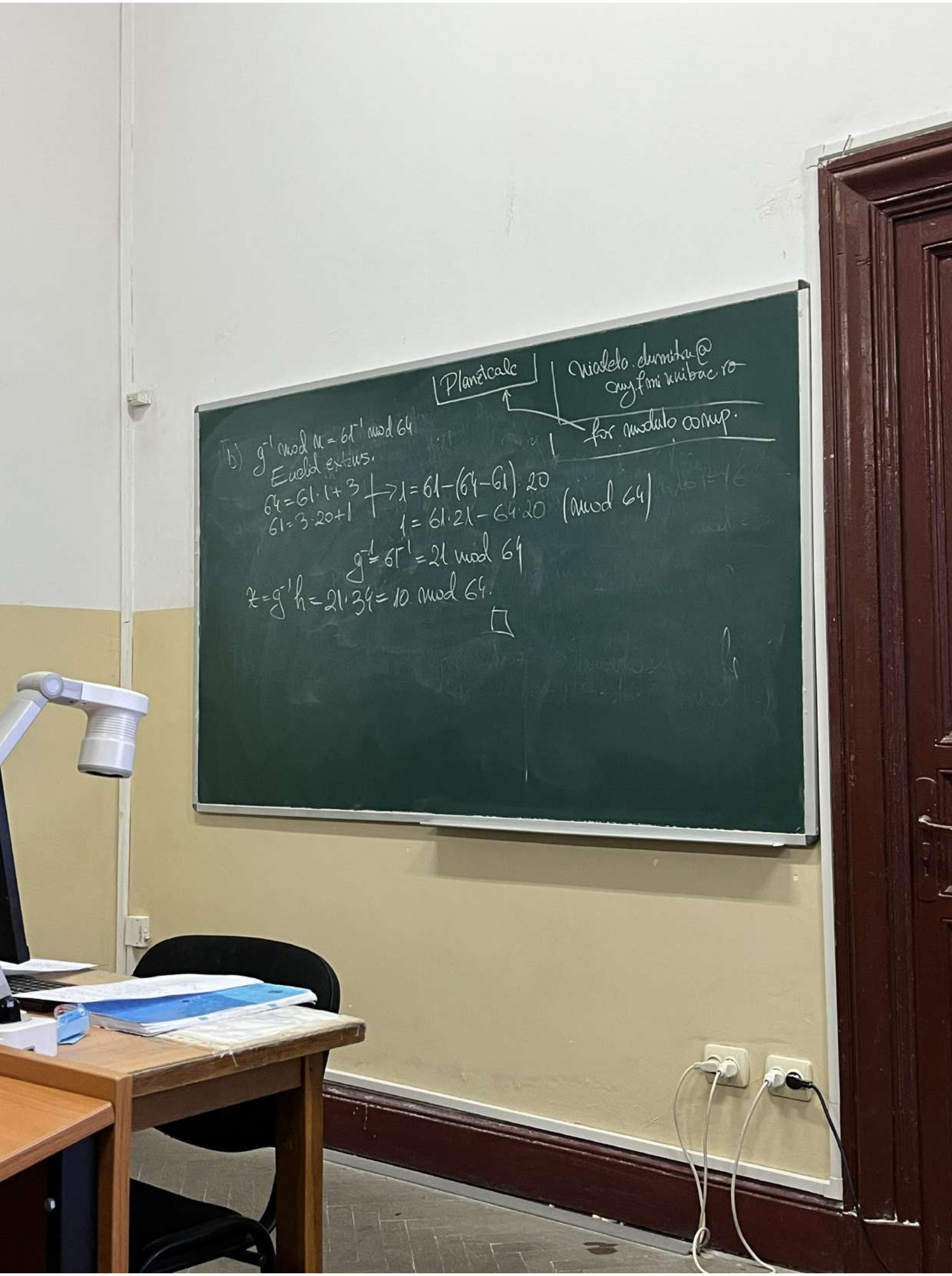
$h = 61 \cdot 10 = 34 \bmod 64$

· Criptare Bob

$(c_1, c_2) = (gy, hy + m) = (61 \cdot 11, 34 \cdot 11 + 12) = (31, 2) \bmod 64$

· Decriptarea Alice

$m = c_2 - c_1 x = 2 - 31 \cdot 10 = 12 \pmod{64}$


Planetcalc
nicoleta.dumitru@
my.fmi.unibuc.ro
for modulo comp.
b) $g^{-1} \bmod n = 61^{-1} \bmod 64$
Euclid extins.
$64 = 61 \cdot 1 + 3$
$61 = 3 \cdot 20 + 1$
$\Rightarrow 1 = 61 - (64 - 61) \cdot 20$
$1 = 61 \cdot 21 - 64 \cdot 20 \pmod{64}$
$g^{-1} = 61^{-1} = 21 \bmod 64$
$x = g^{-1} h = 21 \cdot 34 = 10 \bmod 64.$
$\square$

Ex#4 ElGamal

- mod $p = 23$
- generator $g = 2$
- cheie publică $h = 18$
- $B \to (c_1, c_2) = (3, 10)$

Decriptați mesajul

Sol

Lucrăm în $(\mathbb{Z}_{23}, \cdot)$

Cheia publică $h = g^x \bmod p$

$$18 = 2^x \bmod 23$$

Rezolvăm prin forță brută

$2^1 =$

$2^2 =$

$\vdots$

$2^6 = 18 \bmod 23$

$\Rightarrow \boxed{x = 6}$

Planetcalc

nicoleta.dumitru@my.fmi.unibuc.ro

for modulo comp.

Calculăm $m = c_2 c_1^{-x} = 10 \cdot (g^6)^{-1} \mod 23$

Apl. exp. rapidă $6 = 2+4$

$g^2 = 12 \pmod{23}$

$g^4 = 6$ (—"—)

Deci $g^6 = 12 \cdot 6 = 3 \pmod{23}$

- Calc $3^{-1} \mod 23$ folosind Euclid
- Obs. că $3 \cdot 8 = 24 = 1 \pmod{23}$

$\Rightarrow 3^{-1} = 8 \mod 23$

$\Rightarrow m = 10 \cdot 8 = 11 \mod 23.$

$\blacksquare$

$\boxed{\text{Ex\#5}}$ Shamir's Secret Sharing

Fie $P \in \mathbb{Z}_{23}[x]$, $\deg(P) = 2$

Considerăm perechi de forma $(\alpha, P(\alpha))$, $\alpha \in \mathbb{Z}_{23} \setminus \{0\}$ şi $P(\alpha) \in \mathbb{Z}_{23}$

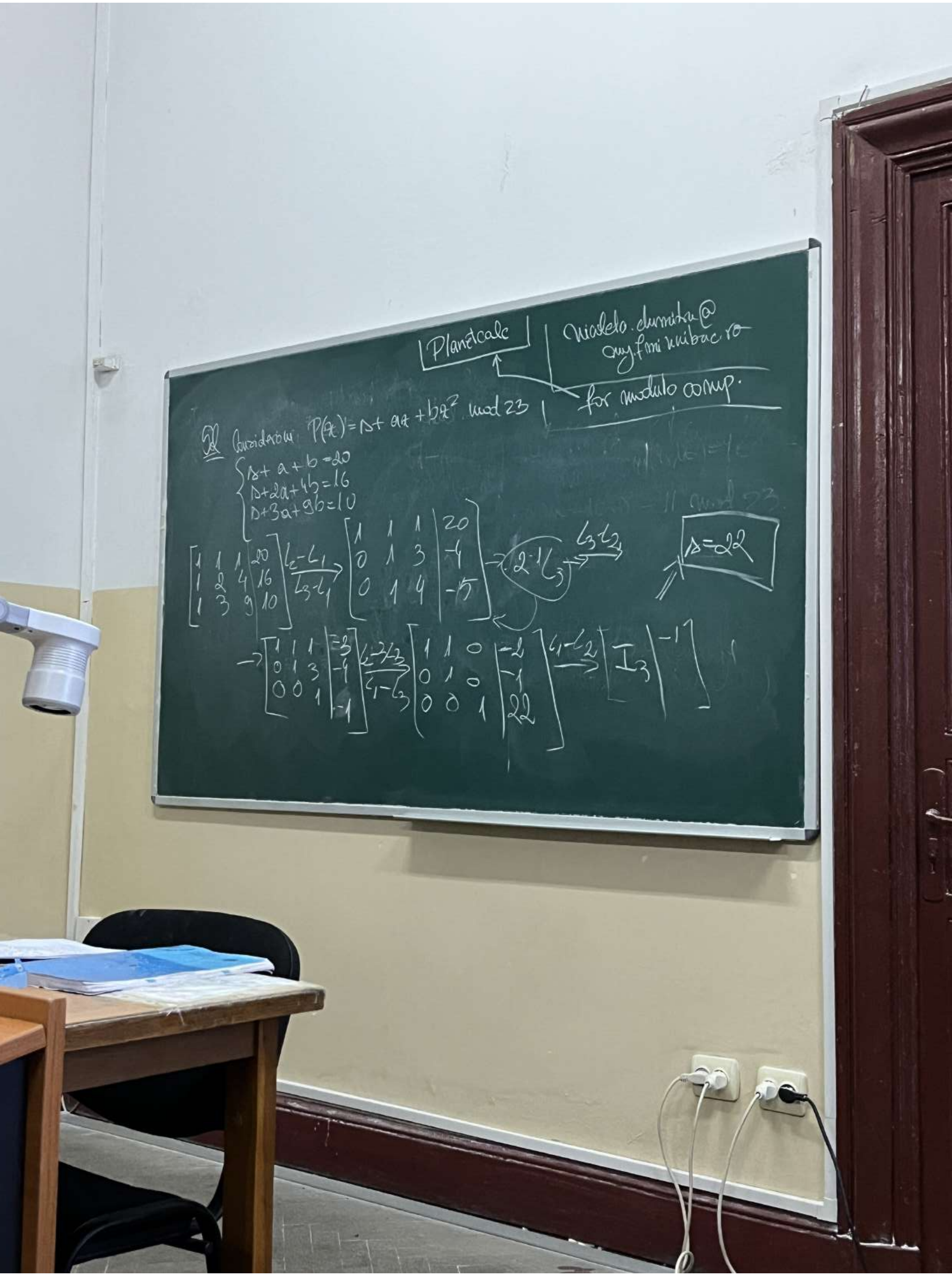
$U(\mathbb{Z}_p) = \mathbb{Z}_p^*$

Trei astfel de perechi $(1, 20)$

$(2, 16)$

$(3, 10)$

Deduceţi ~~[illegible]~~ elementul secret $s = P(0)$


Planetcalc
nicoleta.dumitru@
my.fmi.unibuc.ro
for modulo comp.
Ex Consider $P(x) = s + ax + bx^2$ mod 23
$s + a + b = 20$
$s + 2a + 4b = 16$
$s + 3a + 9b = 10$
$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 20 \\ 1 & 2 & 4 & 16 \\ 1 & 3 & 9 & 10 \end{array}\right] \xrightarrow[L_3 - L_1]{L_2 - L_1} \left[\begin{array}{ccc|c} 1 & 1 & 1 & 20 \\ 0 & 1 & 3 & -4 \\ 0 & 1 & 4 & -5 \end{array}\right] \to 2^{-1} L_3 \xrightarrow{L_3 - L_2}$
$\to \left[\begin{array}{ccc|c} 1 & 1 & 1 & -3 \\ 0 & 1 & 3 & -4 \\ 0 & 0 & 1 & -1 \end{array}\right] \xrightarrow[L_1 - L_3]{L_2 - 3L_3} \left[\begin{array}{ccc|c} 1 & 1 & 0 & -2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 22 \end{array}\right] \xrightarrow{L_1 - L_2} \left[\begin{array}{c|c} I_3 & -1 \end{array}\right]$
$\boxed{s = 22}$

Examen 23 Ian 2021

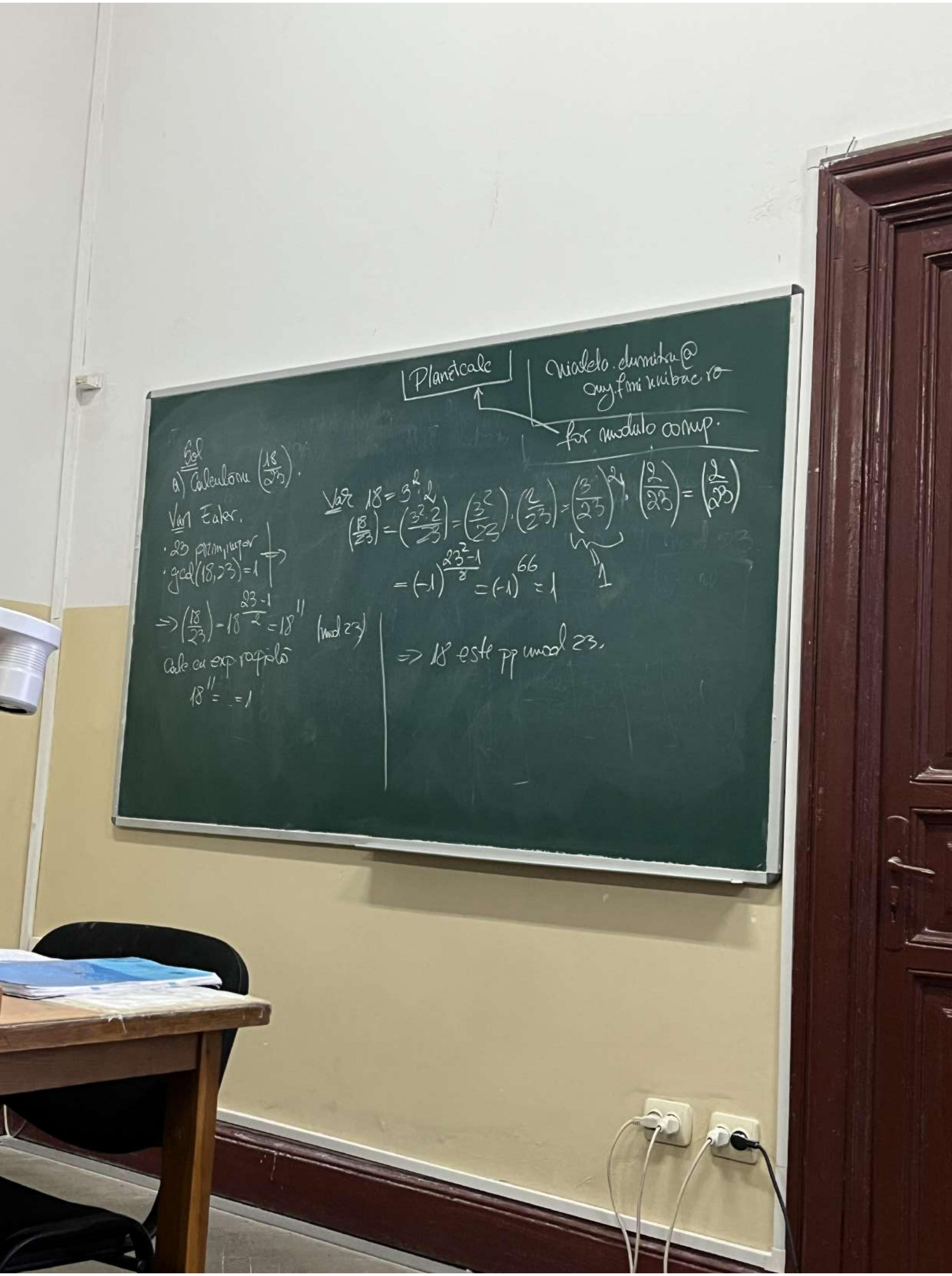
$\boxed{\text{Ex\#6}}$ Cipolla

a) Arătați că 18 este rest pătratic mod 23

b) Calculați $\sqrt{18}$ mod 23. Arătați întâi că

$a=3$ este o bună alegere ai a^2-18 nu este pădrat mod 23.

Calculați în $\mathbb{Z}_{23}[\sqrt{14}]$


Planetcalc
nicoleta.dumitru@
my.fmi.unibuc.ro
for modulo comp.
Sol
a) Calculam $\left(\frac{18}{23}\right)$.
Var Euler.
· 23 prim, impar
· gcd(18,23)=1
$\Rightarrow \left(\frac{18}{23}\right) = 18^{\frac{23-1}{2}} = 18^{11}$ (mod 23)
Calc. cu exp rapida
$18^{11} = \ldots = 1$
Var $18 = 3^2 \cdot 2$
$\left(\frac{18}{23}\right) = \left(\frac{3^2 \cdot 2}{23}\right) = \left(\frac{3^2}{23}\right) \cdot \left(\frac{2}{23}\right) = \left(\frac{3}{23}\right)^2 \cdot \left(\frac{2}{23}\right) = \left(\frac{2}{23}\right)$
1
$= (-1)^{\frac{23^2-1}{8}} = (-1)^{66} = 1$
$\Rightarrow$ 18 este pp mod 23.

Examen 23 Ian 2021

$\boxed{\text{Ex\#6}}$ Cipolla

a) Arătați că 18 este rest pătratic mod 23

b) Calculați $\sqrt{18}$ mod 23. Arătați întâi că

$a=3$ este o bună alegere ai a^2-18 nu este pătrat mod 23.

Calculați în $\mathbb{Z}_{23}[\sqrt{14}]$

---

b) $a=3$

$a^2-18=9-18=14 \pmod{23}$

Calc $\left(\frac{14}{23}\right) \equiv 14^{11} = \ldots = -1$

Euler

$\Downarrow$

14 e [illegible]

Deci $a=3$ este o bună alegere și putem aplica Cipolla.

Considerăm $\omega^2=a^2-18=14$

Calculăm $x=(\omega+a)^{\frac{23+1}{2}}=(\omega+3)^{12}$

$\boxed{\text{Planetcalc}}$ ← for modulo comp.

nicoleta.dumitru@my.fmi.unibuc.ro

Folosind exp. rapida calc.

$(w+3)^{12}$; $12 = 4+8$

$\cdot\ (w+3)^2 = w^2 + 9 + 6w = 14 + 9 + 6w \overset{23}{=} 6w$

$\cdot\ (w+3)^4 = (6w)^2 = 36w^2 = 13 \cdot 14 \overset{23}{=} 21$

$\cdot\ (w+3)^8 = 21^2 = 4 \mod 23$

$\Rightarrow x_1 = (w+3)^{12} = 21 \cdot 4 = 15 \pmod{23}$

$x_2 = 23 - 15 \overset{23}{=} 8$

$\square$