Ex#1 Using Cipolla's algorithm, find the square root of 13 mod 43 if exists.

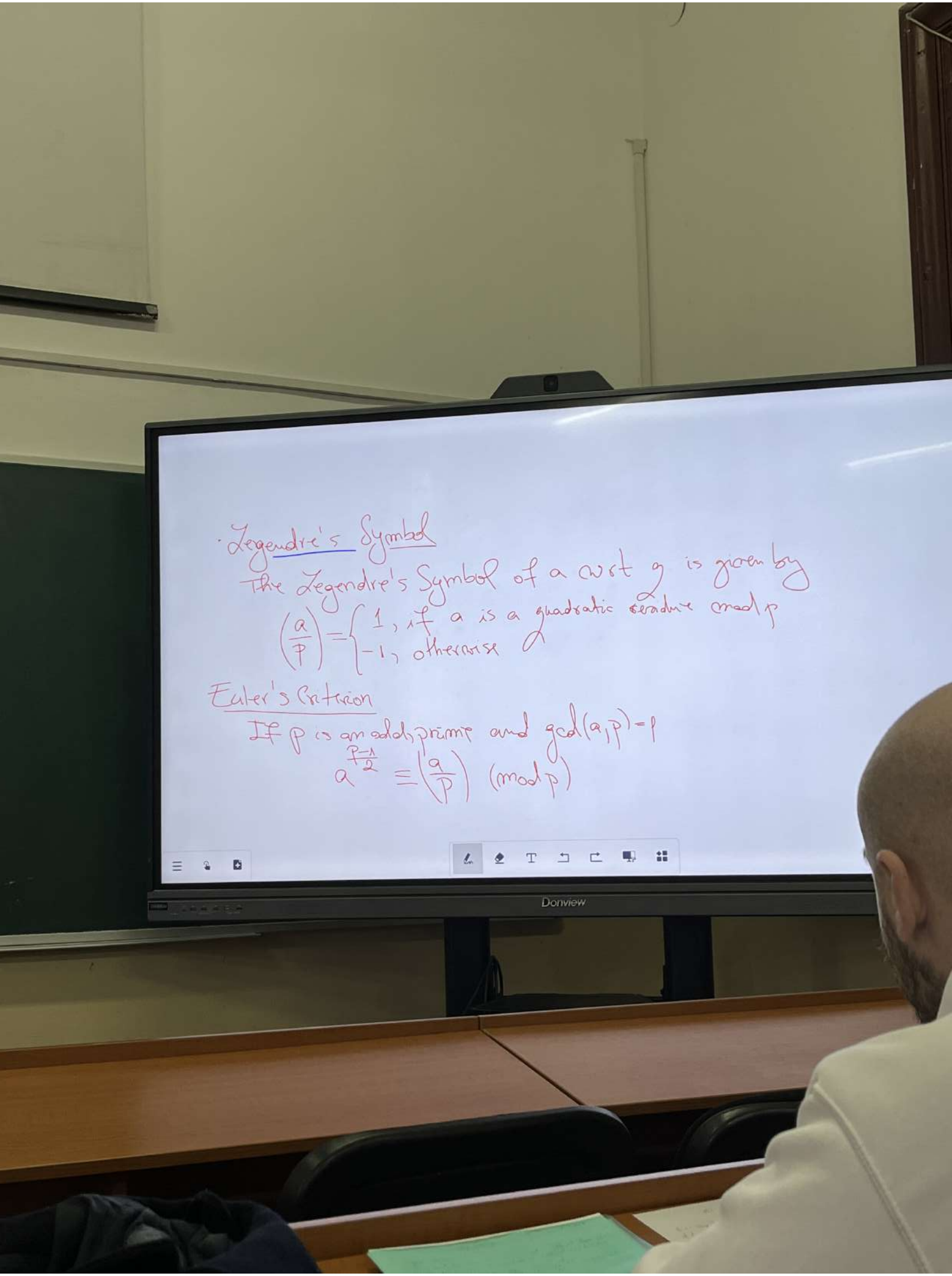
R: Cipolla's algorithm (used to compute the square root $\pmod p$)

- Given $n \in sq(U(\mathbb{Z}_q))$
- Want $a \in U(\mathbb{Z}_q)$ st $a^2 - n \notin sq(U(\mathbb{Z}_q))$

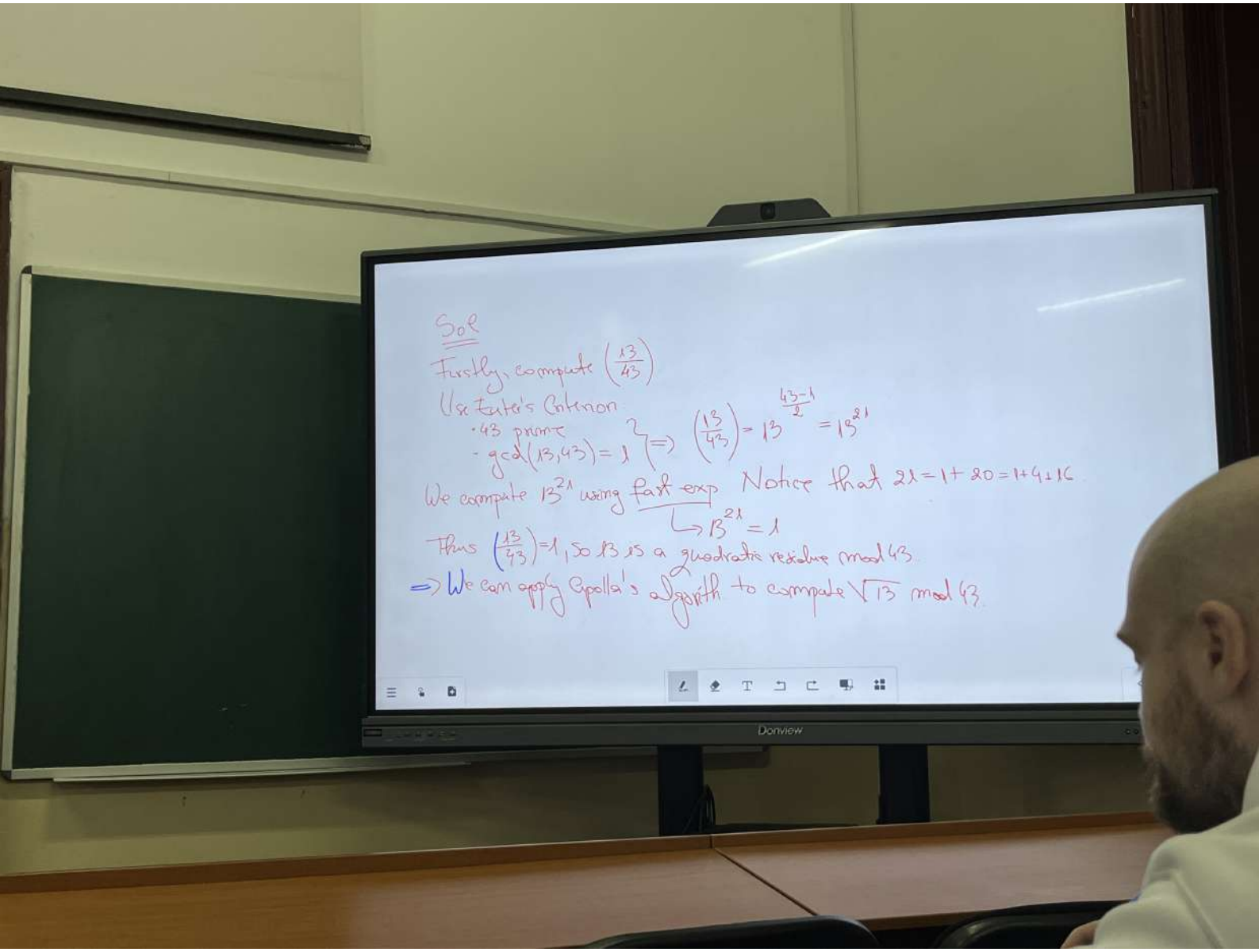
  $w = \sqrt{a^2 - n} \notin \mathbb{F}_q$

  $x = (a + w)^{(q+1)/2}$
- Output x

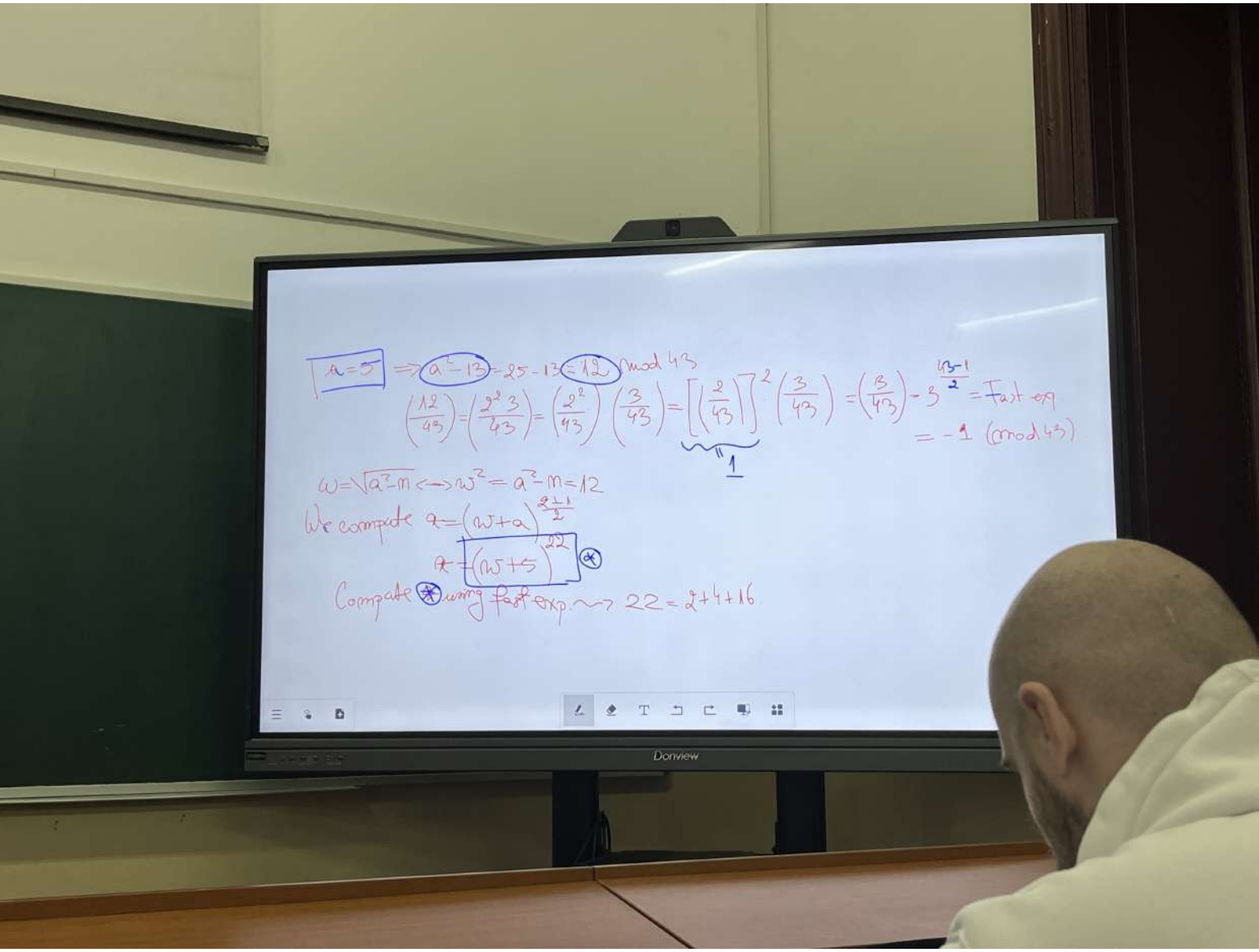
□

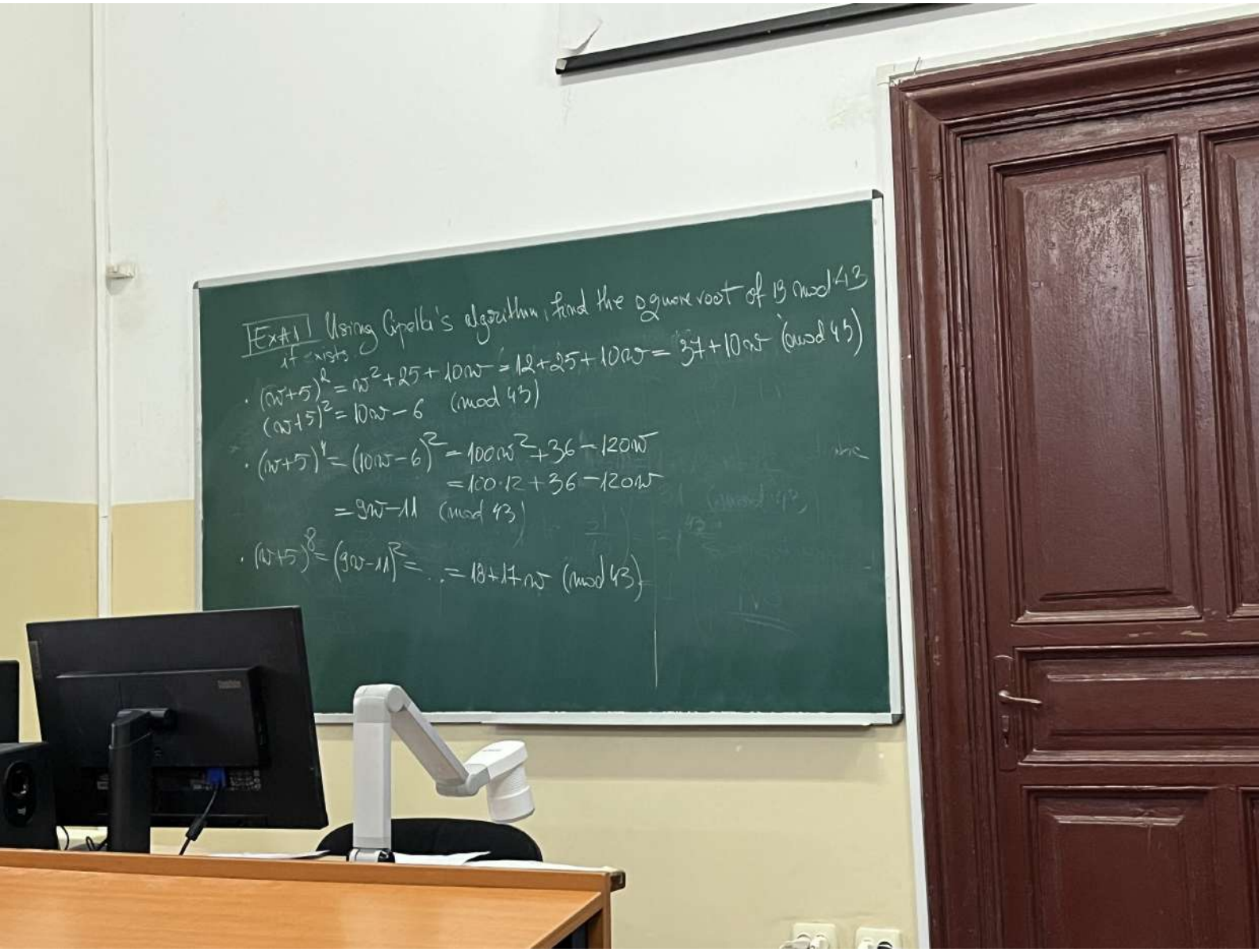

· Legendre's Symbol
The Legendre's Symbol of a wrt p is given by
$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue mod } p \\ -1, & \text{otherwise} \end{cases}$
Euler's Criterion
If p is an odd, prime and $\gcd(a,p)=1$
$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$
Donview

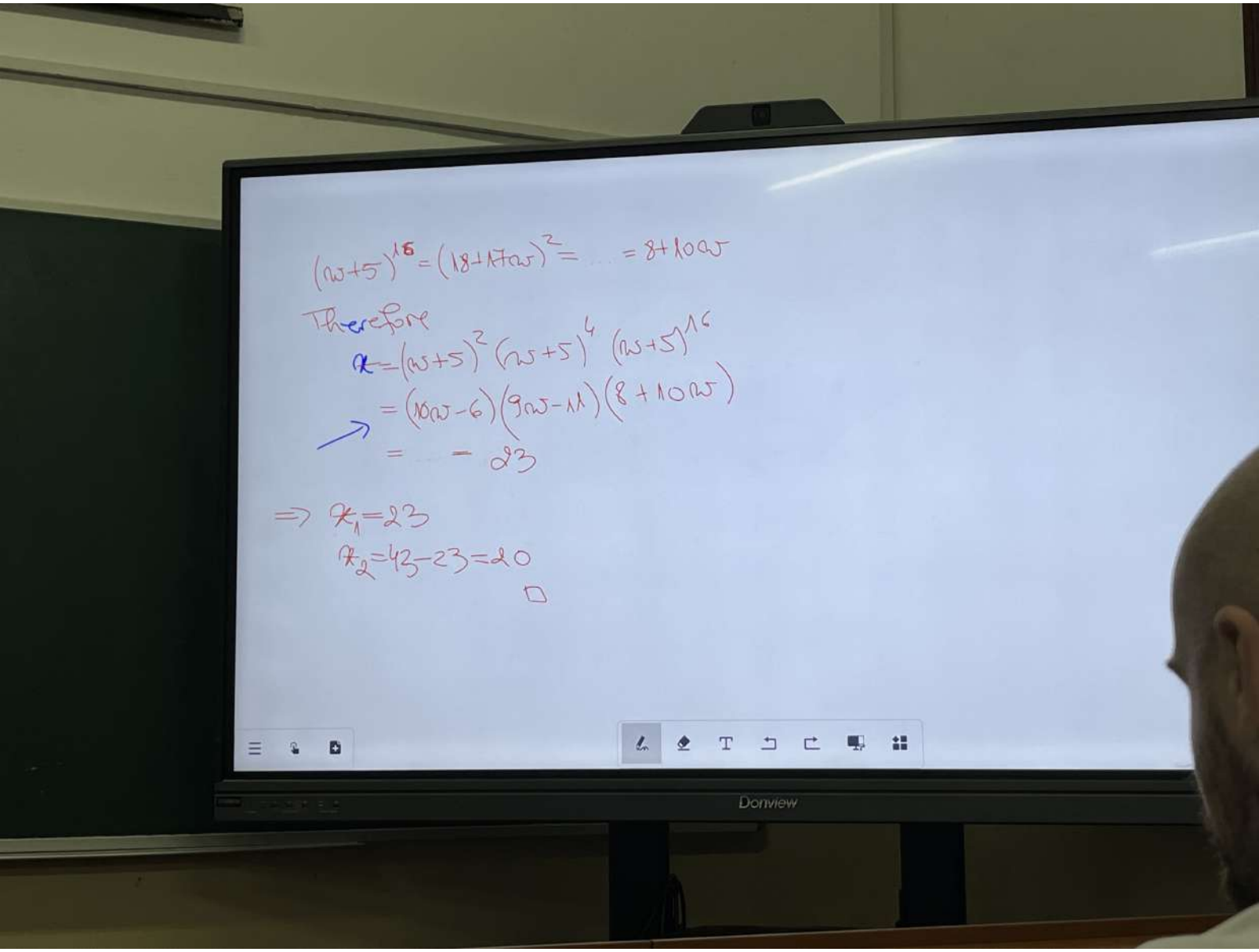

Ex#1 Using Cipolla's algorithm, find the square root of 13 mod 43 if exists.
Properties
1) If $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2) $\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$
3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
Theorem
$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
The law of quadratic reciprocity
$p \neq q$ primes, odd
$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

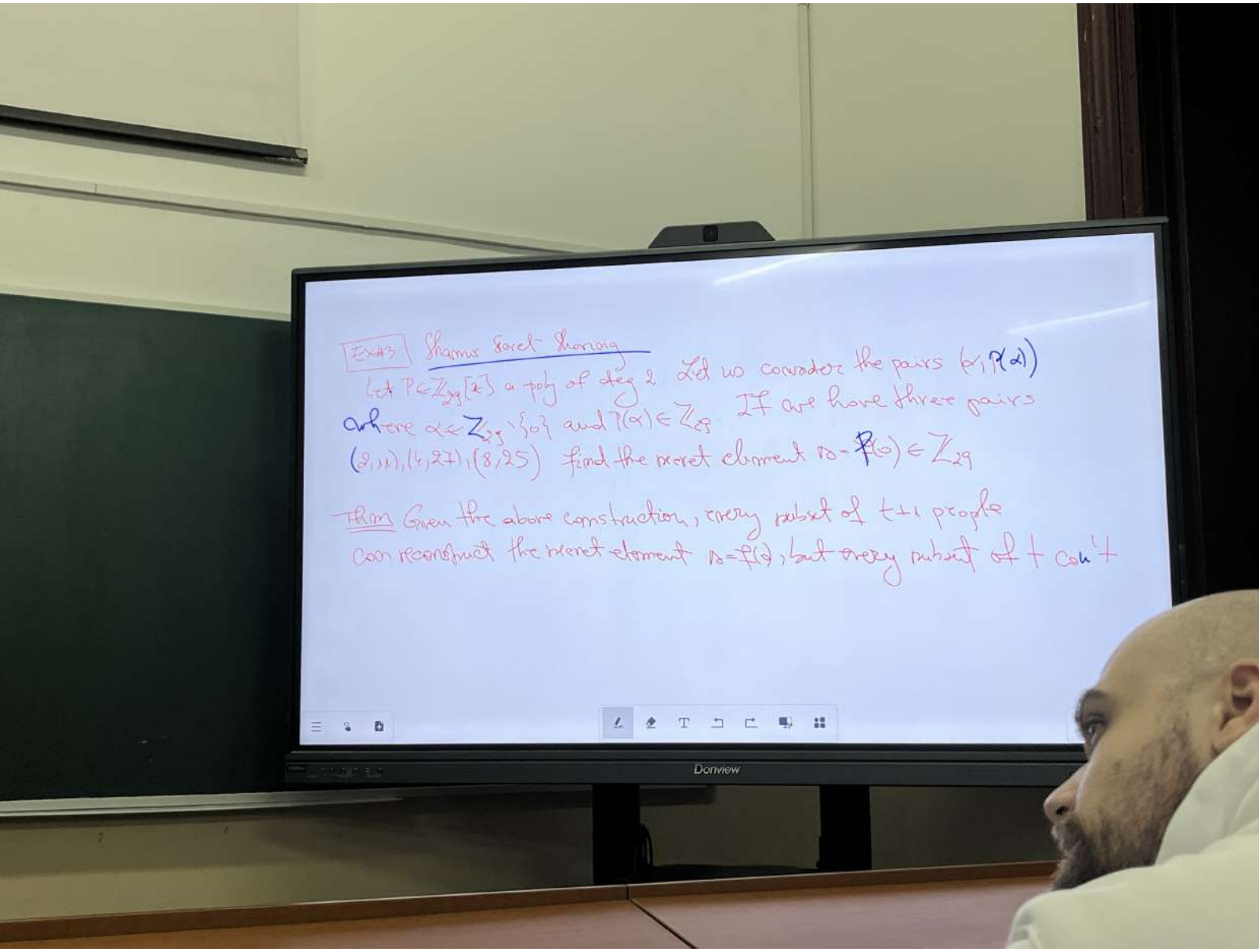

Sol
Firstly, compute $\left(\frac{13}{43}\right)$
Use Euler's Criterion
· 43 prime
· $\gcd(13,43)=1$ $\Rightarrow \left(\frac{13}{43}\right) = 13^{\frac{43-1}{2}} = 13^{21}$
We compute 13^{21} using fast exp Notice that $21 = 1+20 = 1+4+16$
$\hookrightarrow 13^{21} = 1$
Thus $\left(\frac{13}{43}\right)=1$, so 13 is a quadratic residue mod 43
$\Rightarrow$ We can apply Cipolla's algorith to compute $\sqrt{13}$ mod 43
Donview

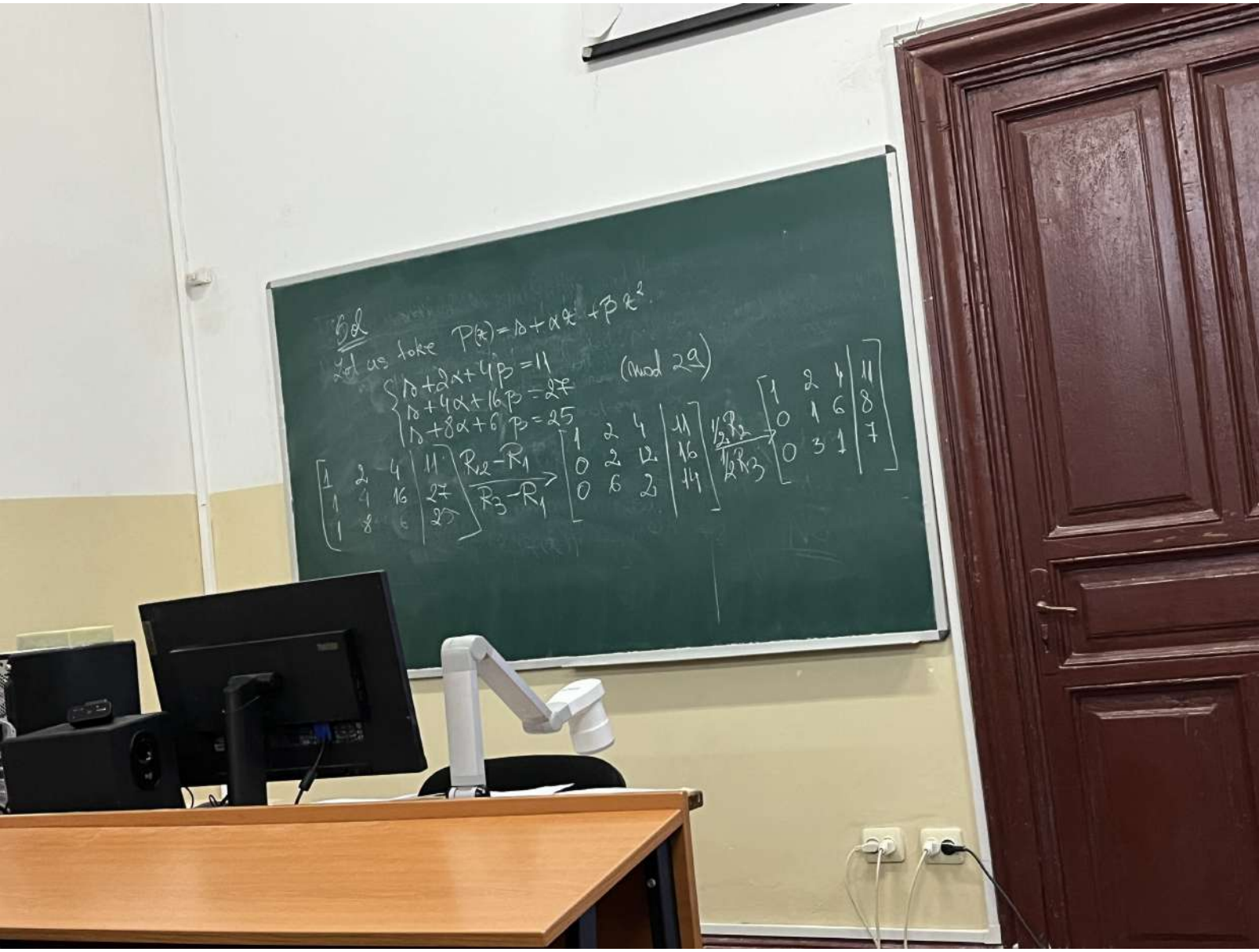

Ex#1 Using Cipolla's algorithm, find the square root of 13 mod 43
if exists
We want to find a s.t. $a^2 - n \in SQ((\mathbb{Z}/43\mathbb{Z})^*)$.
If $a=0 \Rightarrow a^2 - n = -13 = 30$.
Compute $\left(\frac{30}{43}\right)$
In the alg.
I said $a \in (\mathbb{Z}/43)$
If $a=1 \to a^2 - n = 1 - 13 = -12$
$= 31 \pmod{43}$
Compute $\left(\frac{31}{43}\right) = 31^{\frac{43-1}{2}}$ = Fast exp
Euler
$= 1$ No

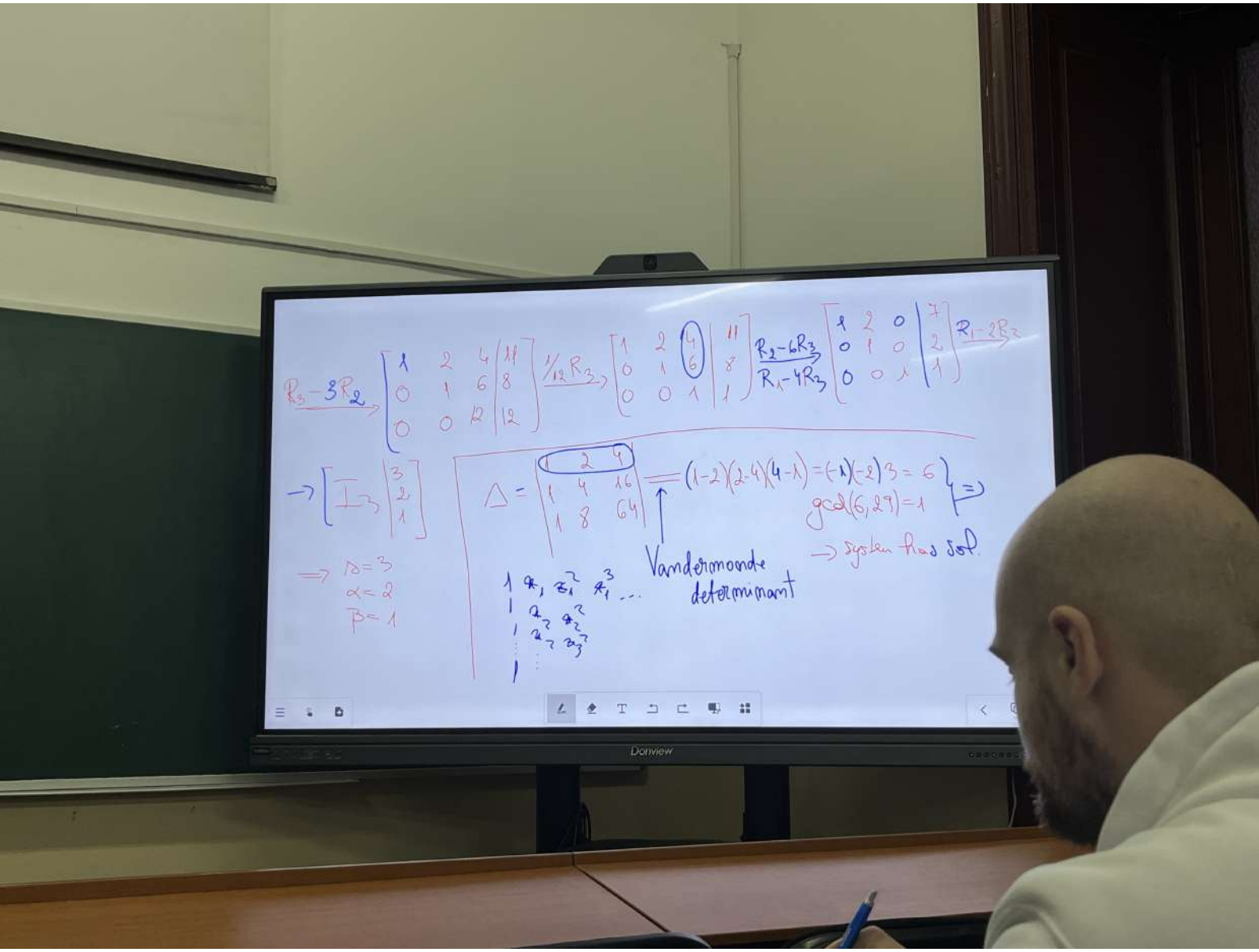

a=5 ⇒ a²−13 = 25−13 = 12 mod 43
(12/43) = (2²·3/43) = (2²/43)(3/43) = [(2/43)]²(3/43) = (3/43) = 3^((43−1)/2) = Fast exp
= −1 (mod 43)
= 1
ω = √(a²−n) ⟷ ω² = a²−n = 12
We compute A = (ω+a)^((q+1)/2)
A = (ω+5)^22 (*)
Compute (*) using fast exp. ⇝ 22 = 2+4+16
Donview

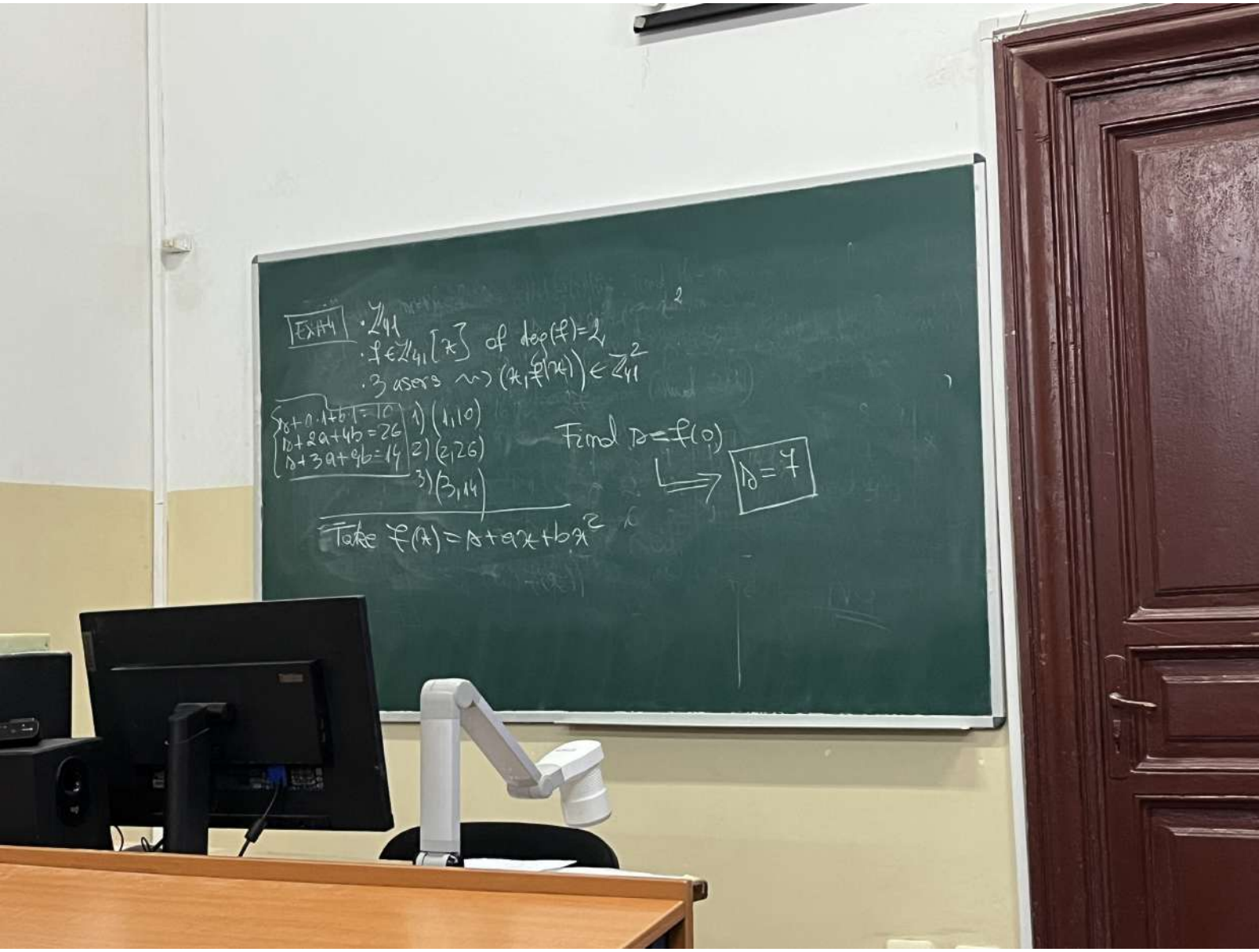

Ex#1 Using Cipolla's algorithm, find the square root of 13 mod 43
if exists
$(w+5)^2 = w^2+25+10w = 12+25+10w = 37+10w \pmod{43}$
$(w+5)^2 = 10w-6 \pmod{43}$
$(w+5)^4 = (10w-6)^2 = 100w^2+36-120w$
$= 100\cdot 12+36-120w$
$= 9w-11 \pmod{43}$
$(w+5)^8 = (9w-11)^2 = \ldots = 18+17w \pmod{43}$

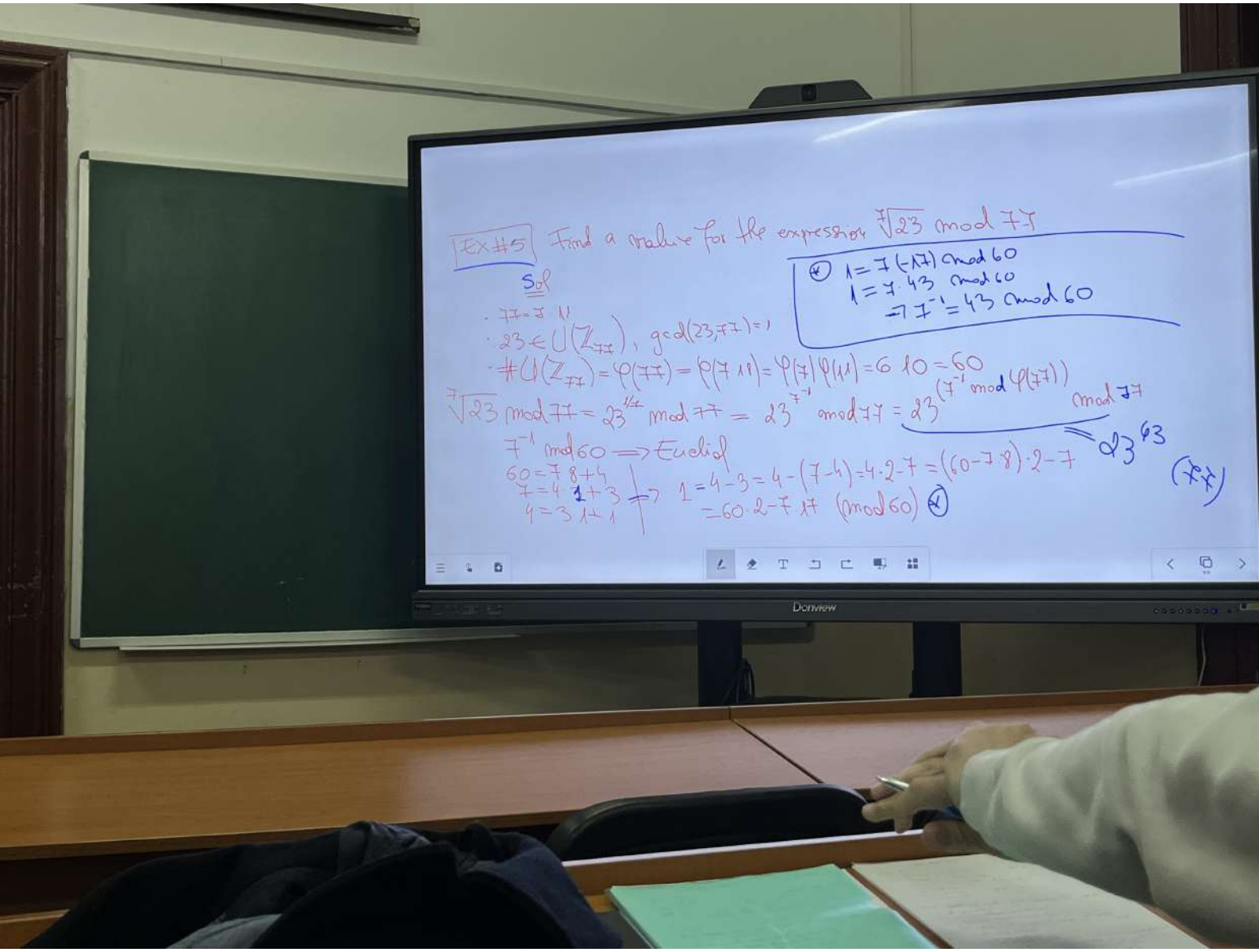

$(w+5)^{16} = (18+17w)^2 = \ldots = 8+10w$
Therefore
$\alpha = (w+5)^2 (w+5)^4 (w+5)^{16}$
$= (10w-6)(9w-11)(8+10w)$
$= \ldots = 23$
$\Rightarrow x_1 = 23$
$x_2 = 43-23 = 20$
Donview

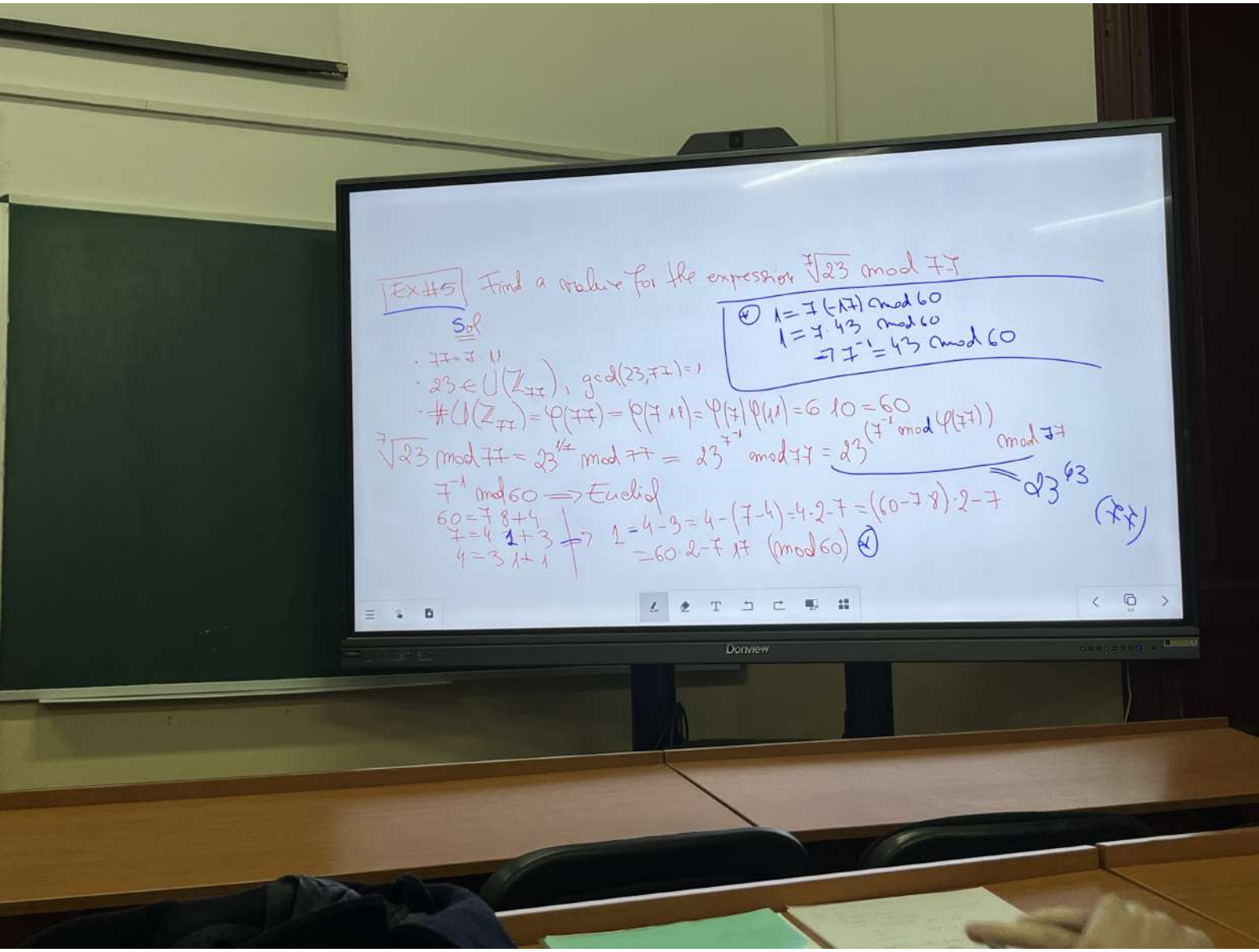

Ex#3 Shamir Secret Sharing
Let $P \in \mathbb{Z}_{29}[x]$ a poly of deg 2. Let us consider the pairs $(\alpha, P(\alpha))$
where $\alpha \in \mathbb{Z}_{29} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{29}$. If we have three pairs
$(2,11), (4,27), (8,25)$ find the secret element $s = P(0) \in \mathbb{Z}_{29}$
Thm Given the above construction, every subset of $t+1$ people
can reconstruct the secret element $s = P(0)$, but every subset of t can't
Donview


Let us take $P(x) = a + \alpha x + \beta x^2$
$a + 2\alpha + 4\beta = 11$
$a + 4\alpha + 16\beta = 27$
$a + 8\alpha + 6\beta = 25$
(mod 29)
$R_2 - R_1$
$R_3 - R_1$
$\frac{1}{2}R_2$
$2R_3$


Vandermonde determinant
gcd(6,29)=1
→ system has sol.
Donview


EXAM
$\mathbb{Z}_{41}$
$f \in \mathbb{Z}_{41}[x]$ of $\deg(f) = 2$
3 users $\rightsquigarrow (x, f(x)) \in \mathbb{Z}_{41}^2$
$\begin{cases} a + a \cdot 1 + b \cdot 1 = 10 \\ a + 2a + 4b = 26 \\ a + 3a + 9b = 14 \end{cases}$
1) (1,10)
2) (2,26)
3) (3,14)
Find $a = f(0)$
$a = 7$
Take $f(x) = a + ax + bx^2$


Ex #5 Find a value for the expression $\sqrt[7]{23} \bmod 77$
Sol
$77 = 7 \cdot 11$
$23 \in U(\mathbb{Z}_{77})$, $\gcd(23,77)=1$
$\#U(\mathbb{Z}_{77}) = \varphi(77) = \varphi(7\cdot 11) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$
$\sqrt[7]{23} \bmod 77 = 23^{1/7} \bmod 77 = 23^{7^{-1}} \bmod 77 = 23^{(7^{-1} \bmod \varphi(77))} \bmod 77$
$= 23^{43}$
$7^{-1} \bmod 60 \Rightarrow$ Euclid
$60 = 7 \cdot 8 + 4$
$7 = 4 \cdot 1 + 3$
$4 = 3 \cdot 1 + 1$
$1 = 4 - 3 = 4 - (7-4) = 4 \cdot 2 - 7 = (60 - 7 \cdot 8) \cdot 2 - 7$
$= 60 \cdot 2 - 7 \cdot 17 \pmod{60}$
$1 = 7(-17) \bmod 60$
$1 = 7 \cdot 43 \bmod 60$
$7^{-1} = 43 \bmod 60$
Donview


Ex #5 Find a value for the expression $\sqrt[7]{23} \bmod 77$
Sol
$\cdot 77 = 7 \cdot 11$
$\cdot 23 \in U(\mathbb{Z}_{77})$, $\gcd(23,77)=1$
$\cdot \#U(\mathbb{Z}_{77}) = \varphi(77) = \varphi(7\cdot 11) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$
$\sqrt[7]{23} \bmod 77 = 23^{1/7} \bmod 77 = 23^{7^{-1}} \bmod 77 = 23^{(7^{-1} \bmod \varphi(77))} \bmod 77$
$= 23^{43}$ (**)
$7^{-1} \bmod 60 \Rightarrow$ Euclid
$60 = 7\cdot 8 + 4$
$7 = 4\cdot 1 + 3$
$4 = 3\cdot 1 + 1$
$1 = 4 - 3 = 4 - (7-4) = 4\cdot 2 - 7 = (60 - 7\cdot 8)\cdot 2 - 7$
$= 60\cdot 2 - 7\cdot 17 \pmod{60}$ (*)
(*) $1 = 7(-17) \bmod 60$
$1 = 7 \cdot 43 \bmod 60$
$\Rightarrow 7^{-1} = 43 \bmod 60$
Donview