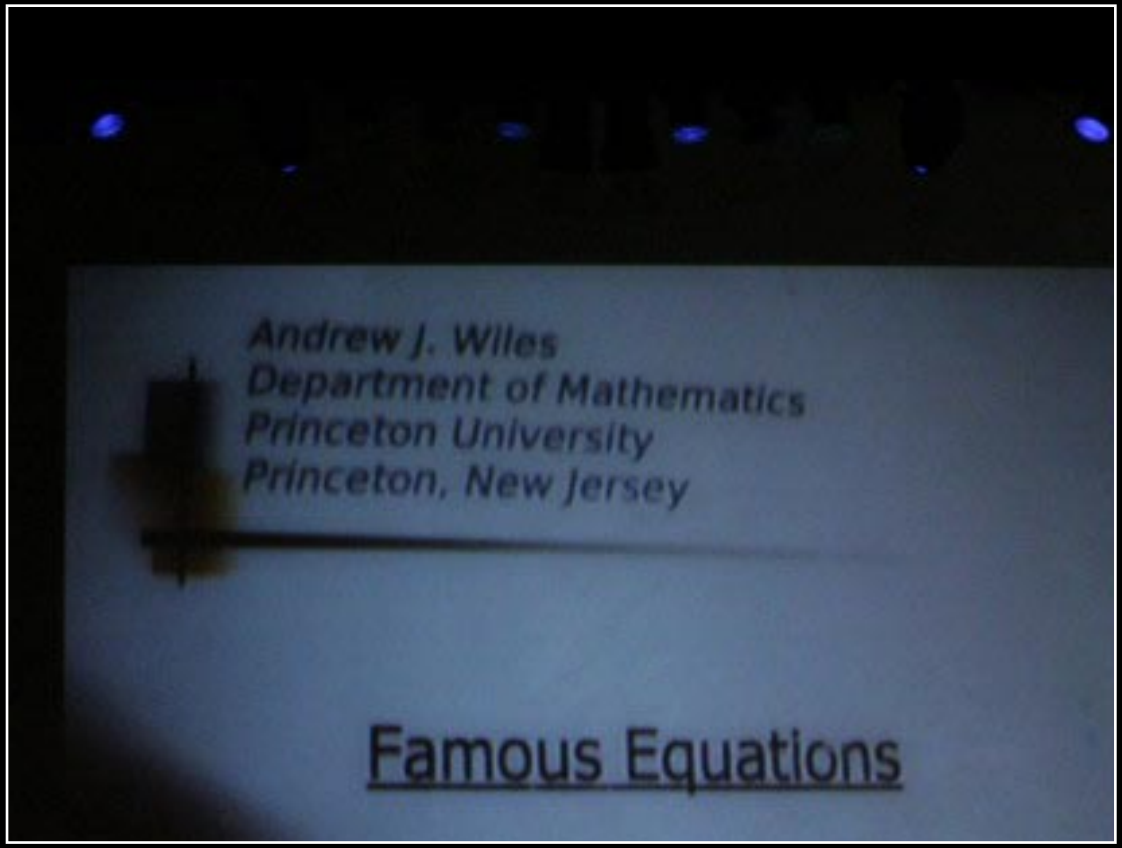
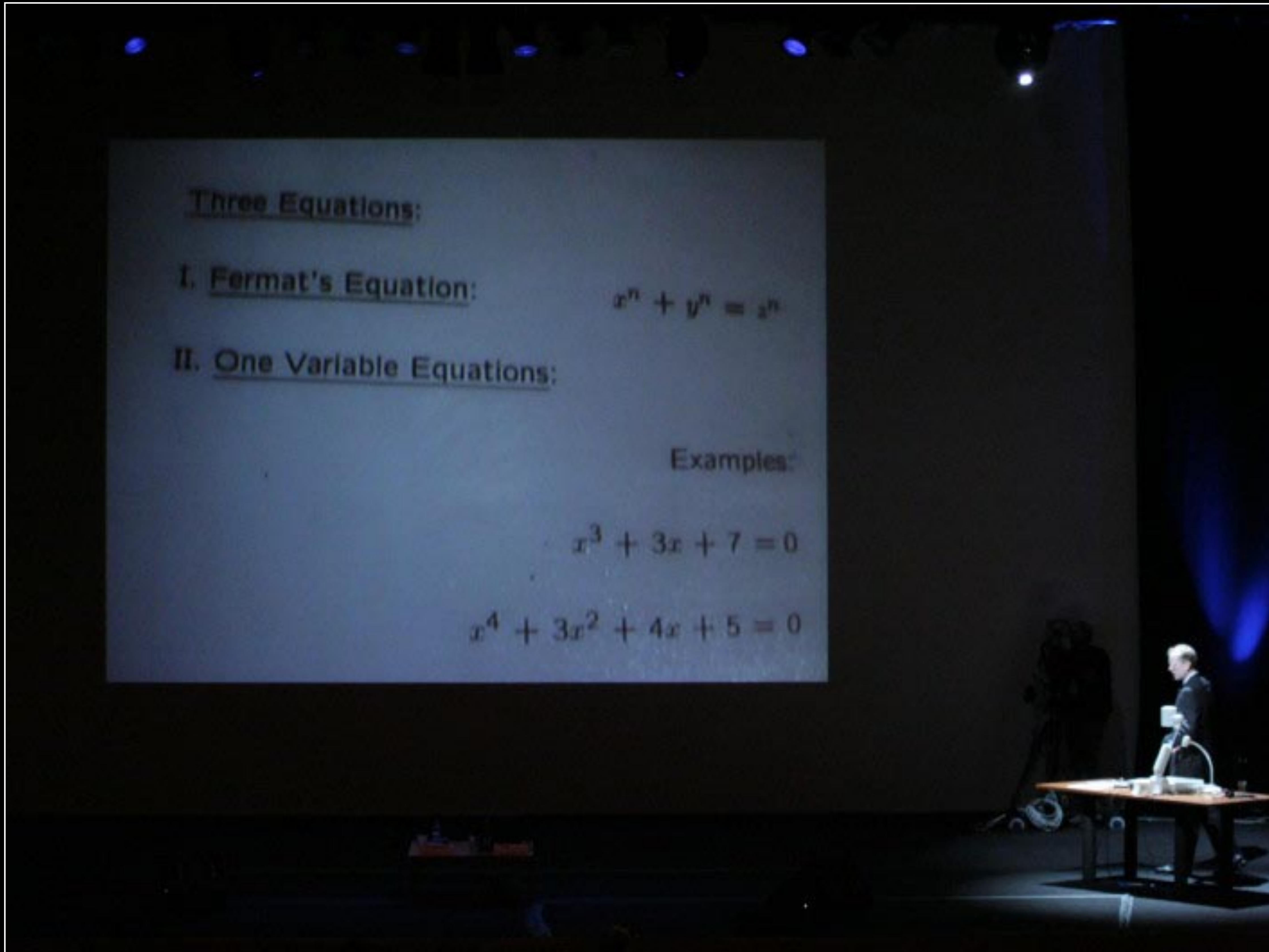
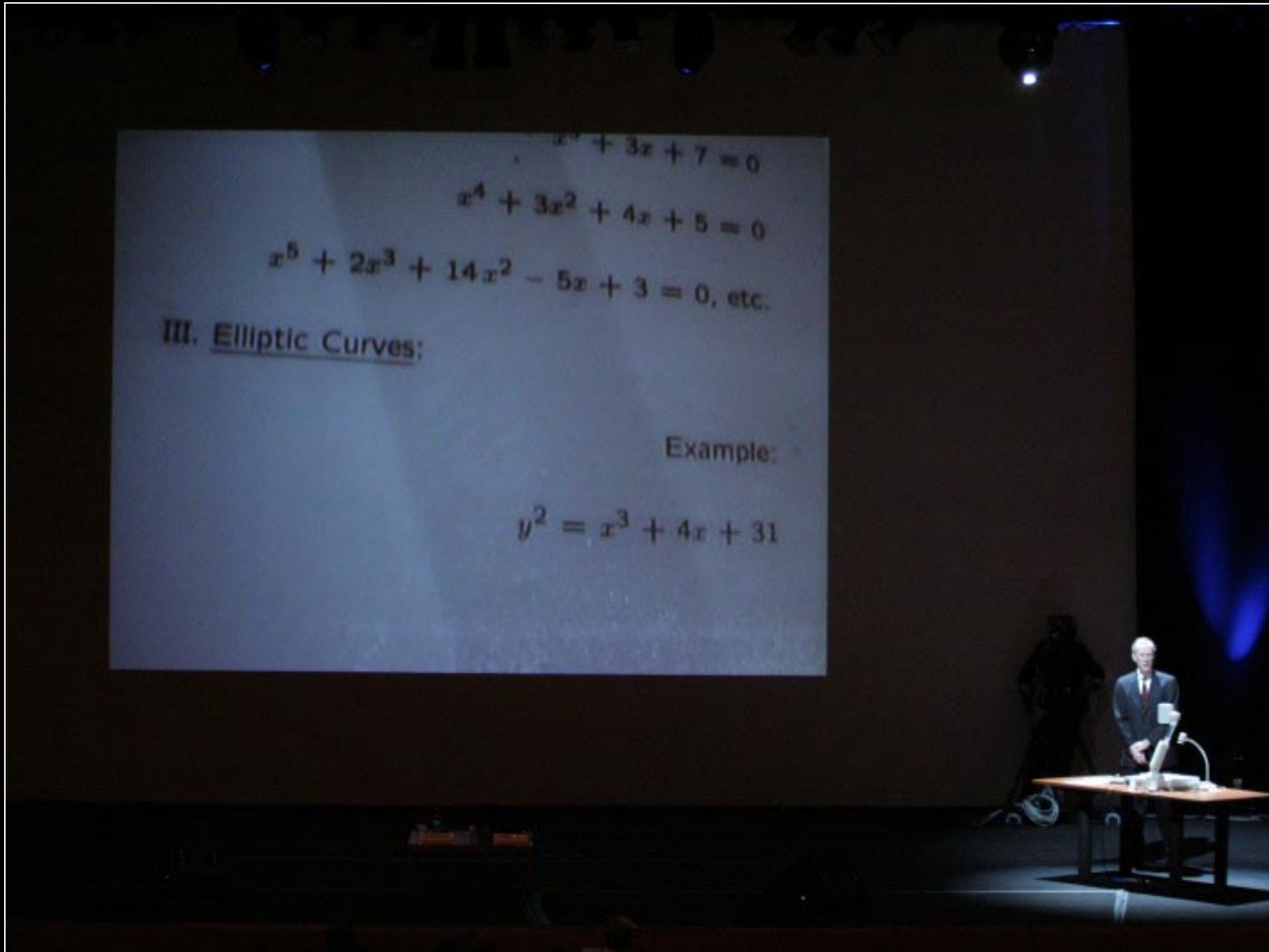
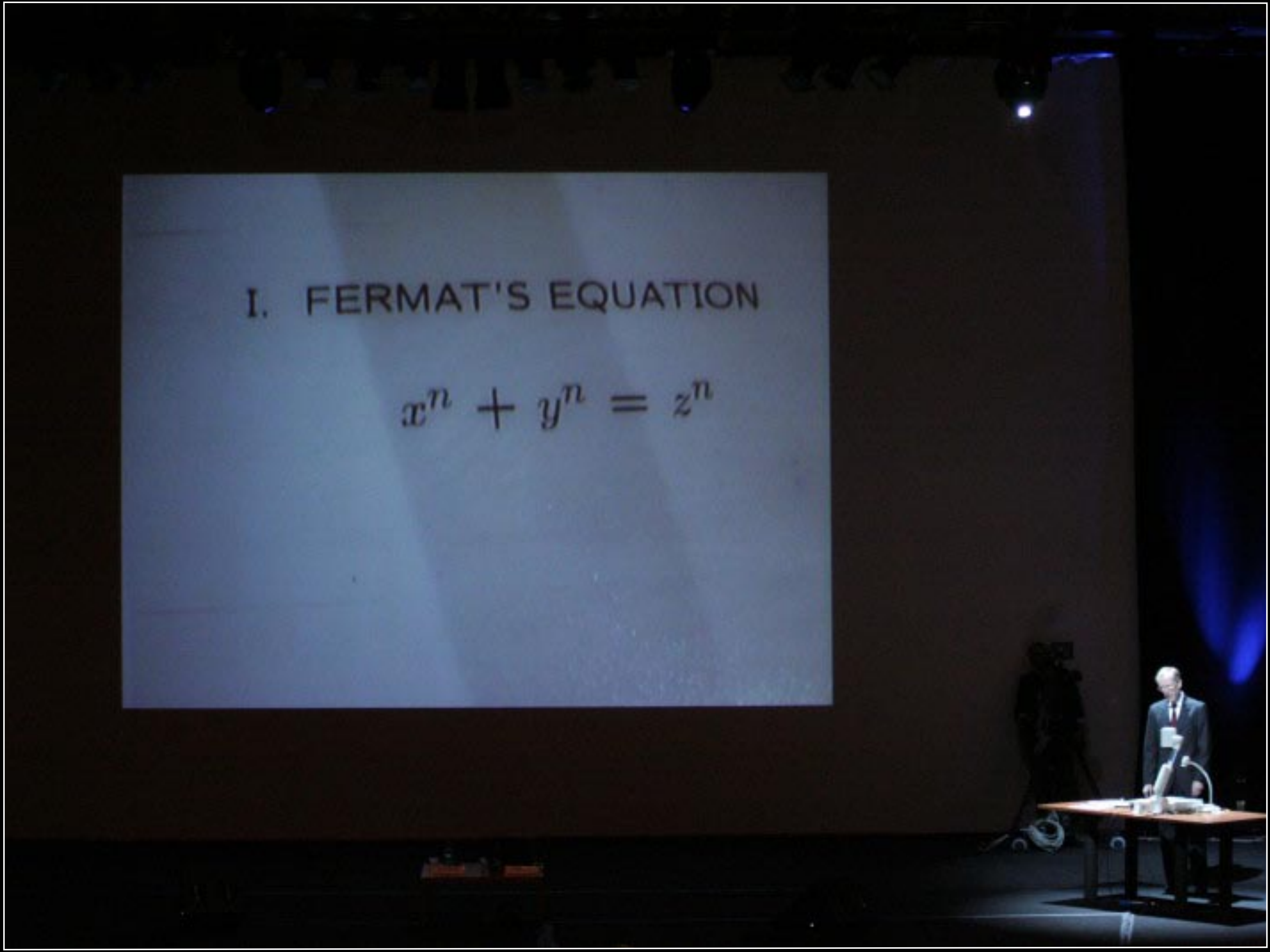


I lucidi di Andrew Wiles


Three Equations:
I. Fermat's Equation:
$x^n + y^n = z^n$
II. One Variable Equations:
Examples:
$x^3 + 3x + 7 = 0$
$x^4 + 3x^2 + 4x + 5 = 0$


$+ 3x + 7 = 0$
$x^4 + 3x^2 + 4x + 5 = 0$
$x^5 + 2x^3 + 14x^2 - 5x + 3 = 0$, etc.
III. Elliptic Curves:
Example:
$y^2 = x^3 + 4x + 31$


I. FERMAT'S EQUATION
$x^n + y^n = z^n$

$$
\begin{aligned}
3^2 &+ 4^2 &= 5^2 \\
65^2 &+ 72^2 &= 97^2 \\
&\vdots \\
12,709^2 &+ 13,500^2 &= 18,541^2 .
\end{aligned}
$$

Plimpton 322 had 15 solutions in integers including these (1900-1600 B.C.)

Fermat's Last Theorem

The equation $x^n + y^n = z^n$ has no solutions [in] non-zero integers for $n \geq 3$.

Special cases

$n = 3$ (Euler gave first proof)

[illegible]
Parte. [illegible]

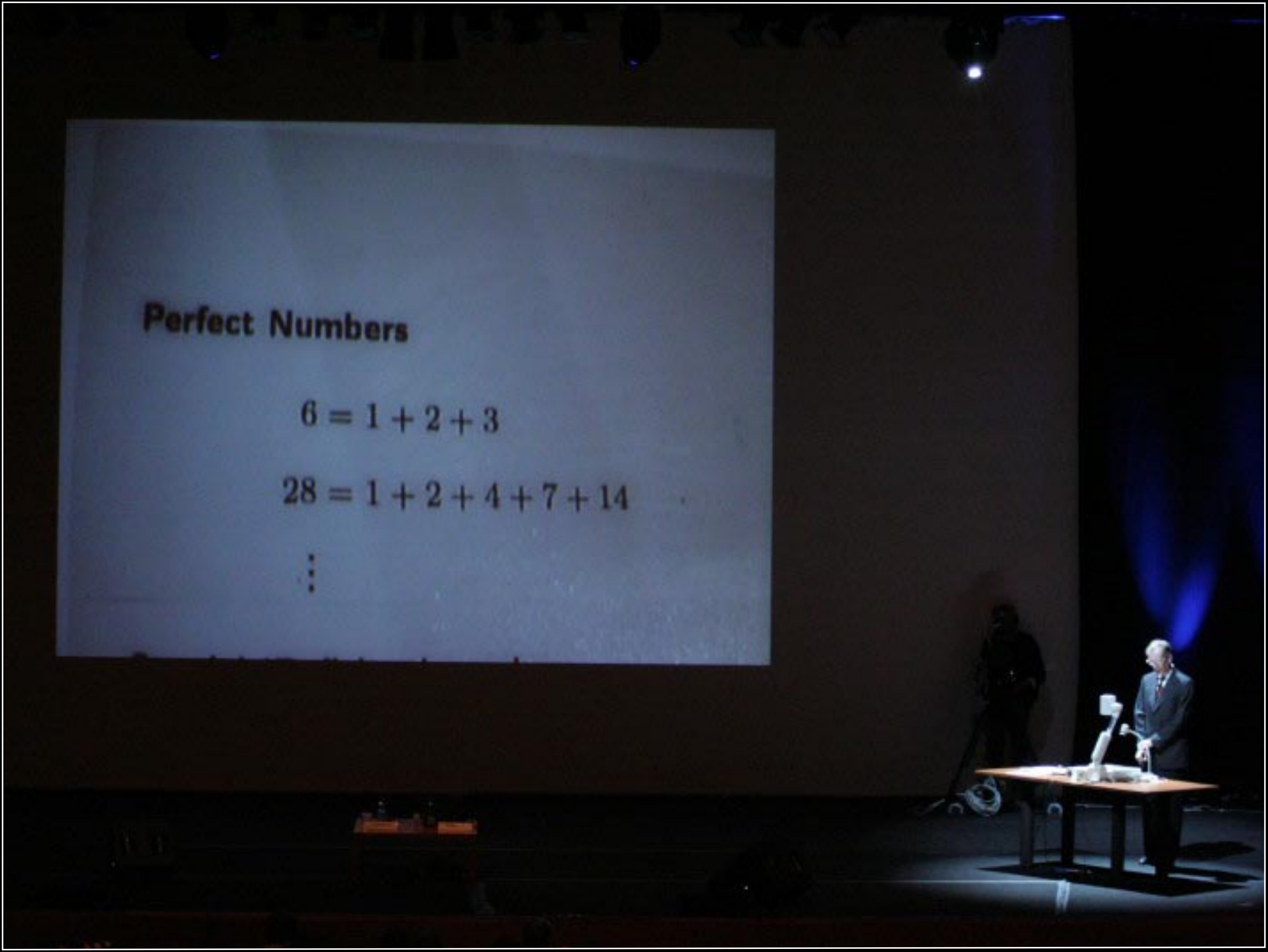
QVÆSTIO VIII.

Propositum quadratum dividere in duos quadratos. Imperatum sit ut 16. dividatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 - 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot unitatum quot continet latus ipsius 16. esto à 2 N - 4. ipse igitur quadratus erit 4 Q. + 16 - 16 N. hæc æqua-

[illegible]

QVÆSTIO VIII.

QVÆSTIO IX.


Perfect Numbers
6 = 1 + 2 + 3
28 = 1 + 2 + 4 + 7 + 14
⋮

$$28 = 1 + 2 + 4 + 7 + 14$$

$$\vdots$$

Special 'Deficient' numbers

672 : **Sum of divisors** $= 2 \times 672$.

Amicable numbers

$$284 = 1 + 2 + 4 + 5 + 10 + 11 + \cdots$$

$$220 = 1 + 2 + 4 + 71 + 142$$

Amicable numbers

$$284 = 1 + 2 + 4 + 5 + 10 + 11 + \cdots$$

$$220 = 1 + 2 + 4 + 71 + 142$$

Also 17,296 and 18,416.

First Phase (1637 - 1847)

Fermat's method of descent

$n = 3, 4$:	Fermat	
$n = 3, 4$:	Euler	(1753)
$n = 5$:	Dirichlet, Legendre	(1825)
$n = 7$:	Lamé	(1839)

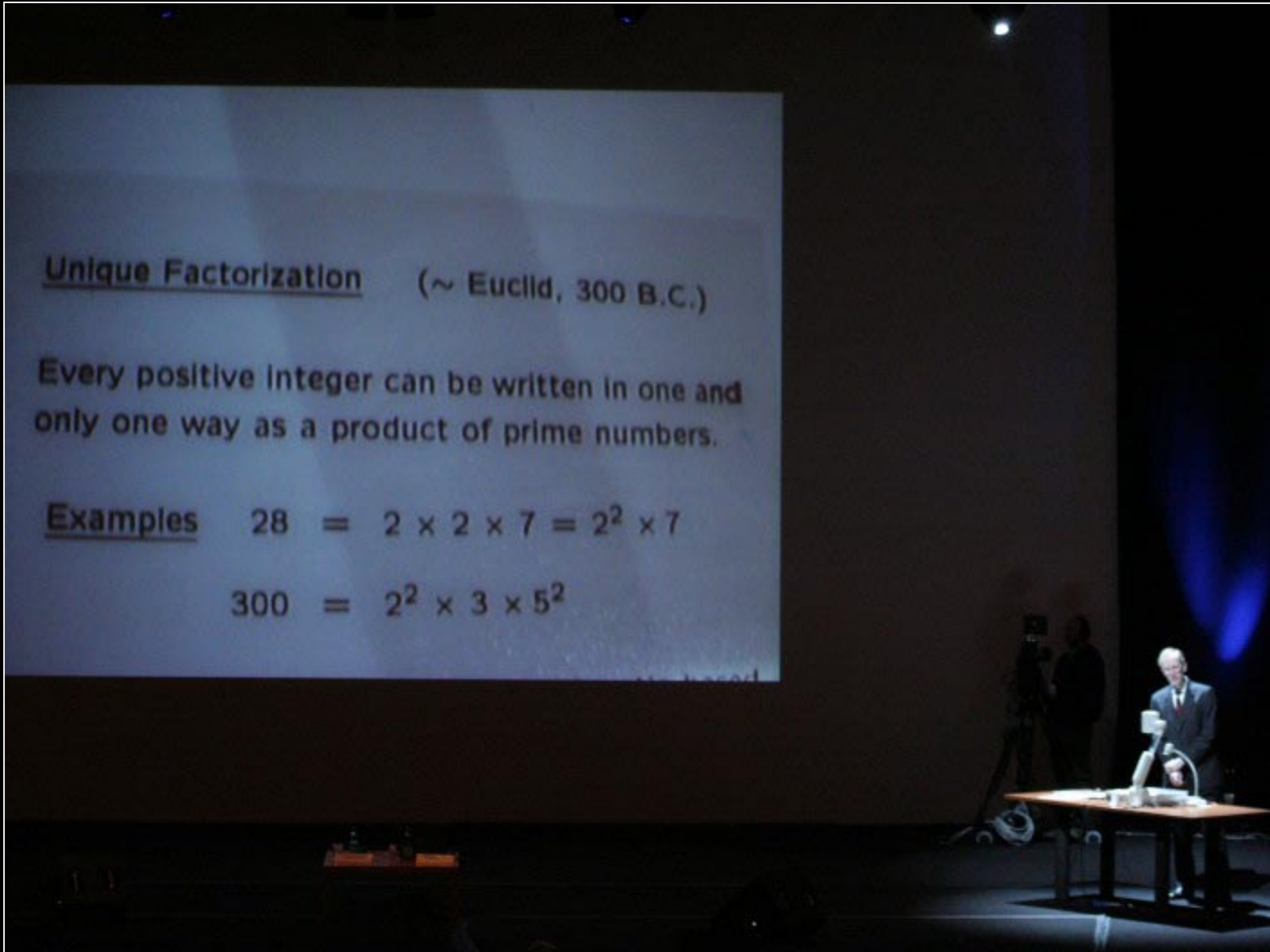
$n = 3,4$: Fermat

$n = 3,4$: Euler (1753)

$n = 5$: Dirichlet, (1825)
Legendre

$n = 7$: Lamé (1839)

Method of infinite descent: if there were a solution in positive integers then Fermat proposes to show that one can deduce from it a second and smaller solution; from the second solution one deduces a third and still smaller solution, descending ad infinitum. But there can not be infinitely many positive integers less than a given one.


Unique Factorization (~ Euclid, 300 B.C.)
Every positive integer can be written in one and only one way as a product of prime numbers.
Examples 28 = 2 × 2 × 7 = 2^2 × 7
300 = 2^2 × 3 × 5^2

$300 = 2^2 \times 3 \times 5^2$

Fails to hold for more general arithmetic based on other number systems

<u>example</u> if we base arithmetic on $\sqrt{-5}$:

$$(1+\sqrt{-5}) \times (1-\sqrt{-5}) = 2 \times 3$$

(Fermat noticed this in another form:
$6 = 1^2 + 5.1^2$, but we can not write 2 or 3 in the form $a^2 + 5b^2$)

Second Phase (1847 - 1985)

Kummer's method:

$$x^p + y^p = z^p \qquad (p > 3 \text{ and prime})$$

write as:

$$(x + y)(x + (\sqrt[p]{1})\, y) \ldots (x + (\sqrt[p]{1})^{p-1} y) = z^p$$

Unique factorization fails in arithmetic which uses $\sqrt[p]{1}$.

$$(x+y)(x+(\sqrt[p]{1})y)\dots(x+(\sqrt[p]{1})^{p-1}y)=z^p$$

Unique factorization fails in arithmetic which uses $\sqrt[p]{1}$.

Kummer introduced a theory that sometimes bypasses this problem.

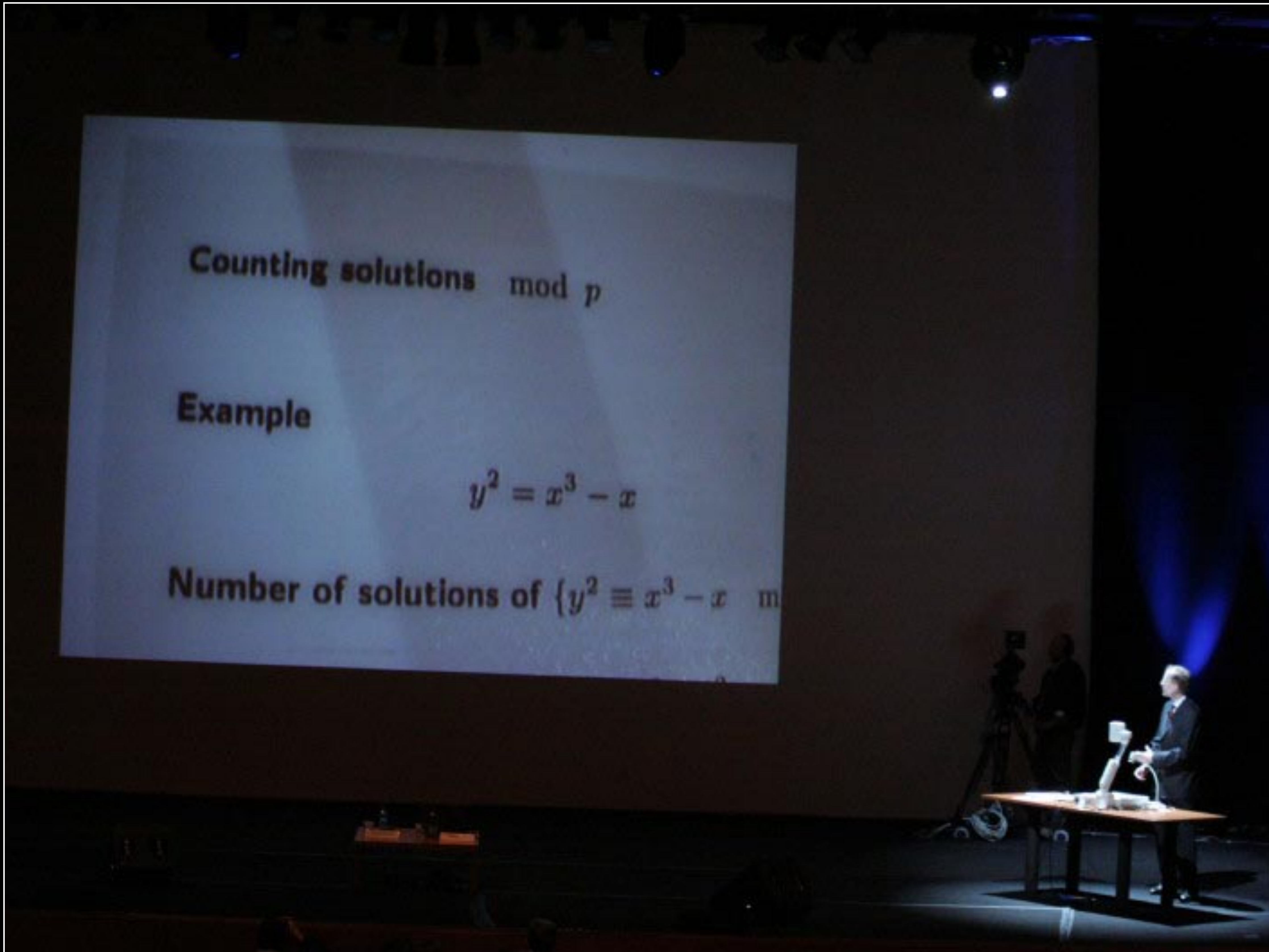
* * * * *

But fails for $p = 37, 59, 67, \dots$

Mod p arithmetic

Example

Mod 7: $0, 1, 2, 3, 4, 5, 6.$


Counting solutions mod p
Example
$y^2 = x^3 - x$
Number of solutions of $\{y^2 \equiv x^3 - x$

Counting solutions mod p

Example

$$y^2 = x^3 - x$$

Number of solutions of $\{y^2 \equiv x^3 - x \mod$

$$\begin{cases} p & \text{if } p \neq a^2 + b^2 \\ p - 2a & \text{if } p = a^2 + b^2 \end{cases}$$

Example

$$y^2 = x^3 - x$$

Number of solutions of $\{y^2 \equiv x^3 - x \mod p\}$

$$\begin{cases} p & \text{if } p \neq a^2 + b^2 \\ p - 2a & \text{if } p = a^2 + b^2 \end{cases}$$

Example $p = 13$; $3^2 + 2^2 = 13$; pick $a = 3$.

Theorem: There is a general formula for counting solutions mod p for equations of the form

$$y^2 = x(x-u)(x+v)$$

Theorem: Fermat's Last Theorem is true.

Further Developments and Diophantine Problems

(I) $x^p + y^p = cz^p$ (Serre)
no solutions for certain small values of c.

(II) $x^p + y^p = z^r$ (Darmon, Granville, Merel).

$r = 2$: no primitive solutions

$r = 2$: no primitive solutions

$r = 3$: no primitive solutions

(iii) $x^p + y^q = z^r$

(iv) $A + B = C$

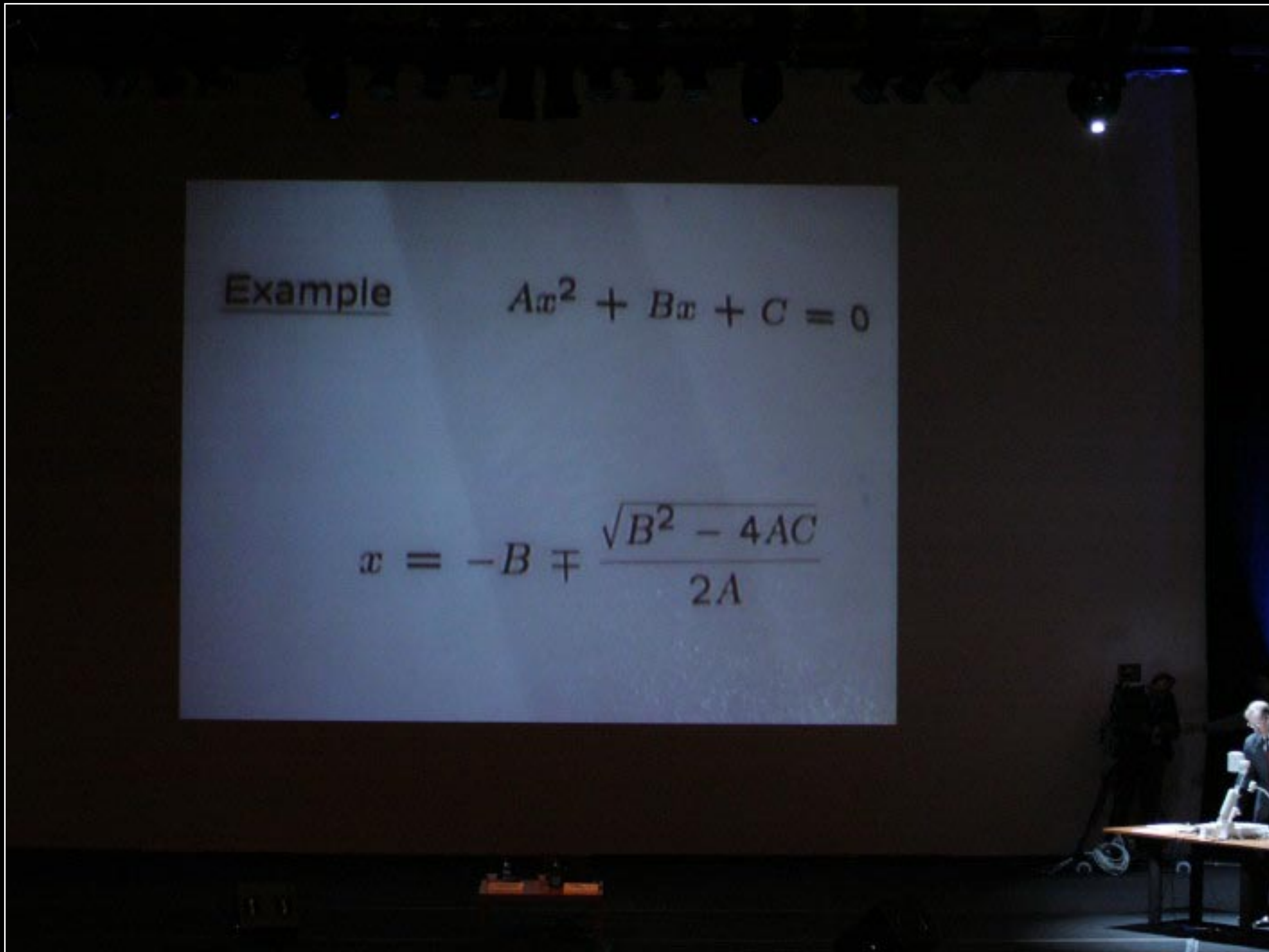
II. Polynomial Equations

$$Ax^2 + Bx + C = 0 \qquad \text{(quadratic)}$$

$$x^3 + Ax + B = 0 \qquad \text{(cubic)}$$

$$x^4 + Ax^2 + Bx + C = 0 \qquad \text{(quartic)}$$

......


Example
$Ax^2 + Bx + C = 0$
$x = -B \mp \frac{\sqrt{B^2 - 4AC}}{2A}$

7 Complete Cubic Equations (All Powers Represented)

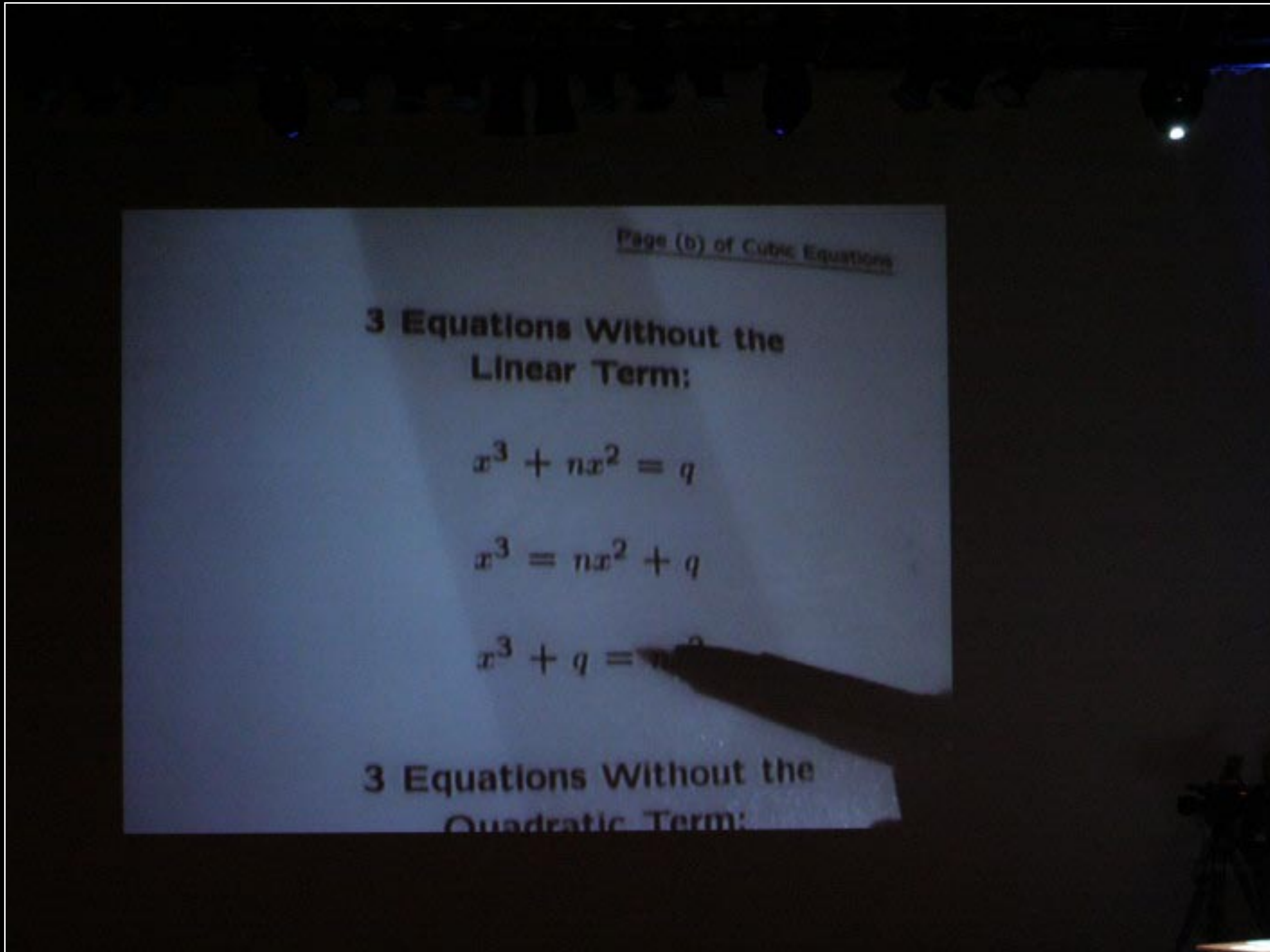
$$x^3 + nx^2 + px = q$$

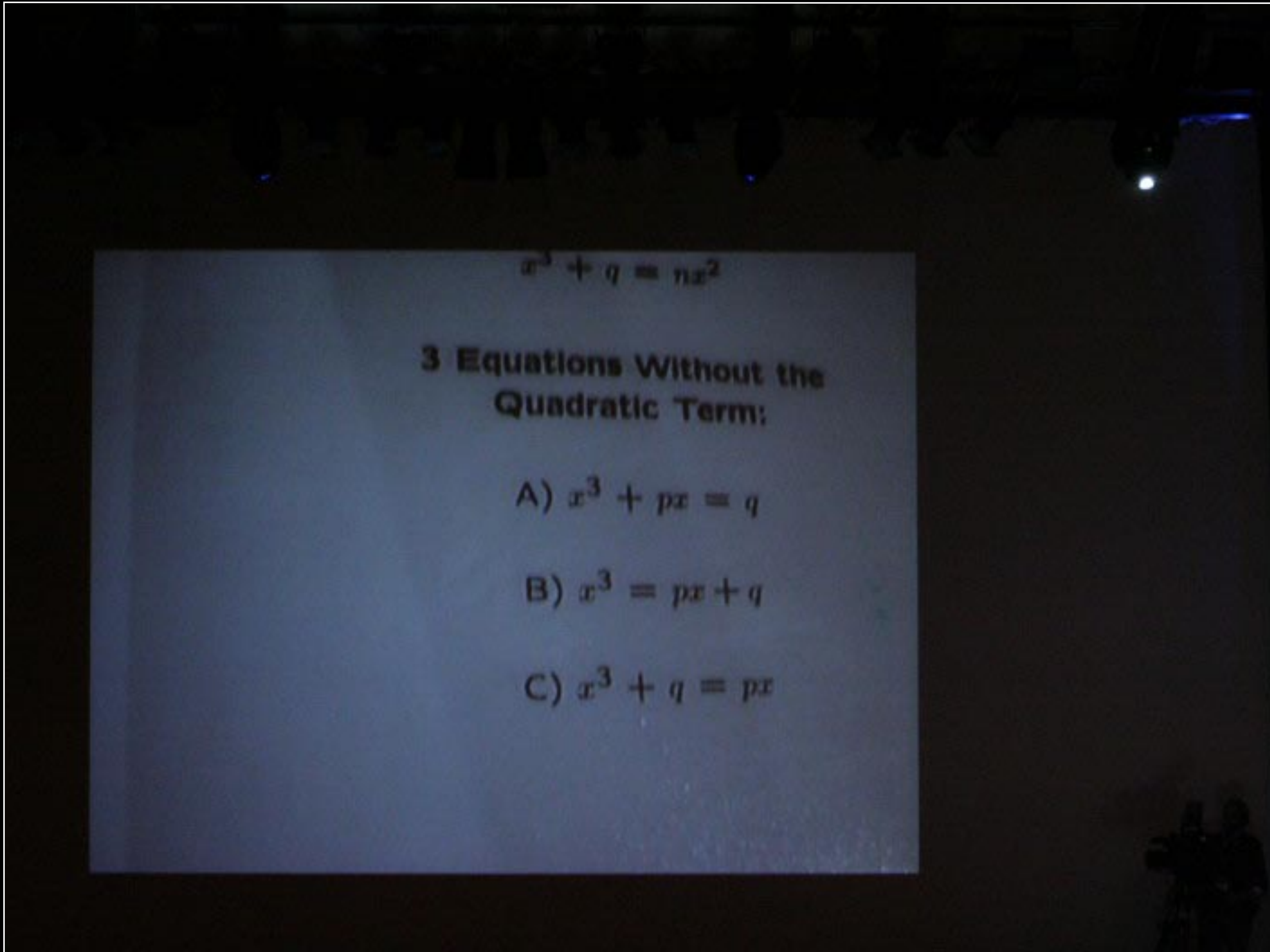
$$x^3 + nx^2 + q = px$$

$$x^3 + px + q = nx^2$$

$$x^3 + nx^2 = px + q$$

$$x^3 + px = nx^2 + q$$


Page (b) of Cubic Equations
3 Equations Without the Linear Term:
$x^3 + nx^2 = q$
$x^3 = nx^2 + q$
3 Equations Without the
Quadratic Term:


$x^3 + q = nx^2$
3 Equations Without the Quadratic Term:
A) $x^3 + px = q$
B) $x^3 = px + q$
C) $x^3 + q = px$

Equations in One Variable

Cubic Equations: del Ferro, Tartaglia, Cardan (16^{th} century) $x^3 + ax = b$; solution

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

Tartaglia's Original Poem - 1539

Quando che'l cubo con le cose appresso
Se agguaglia a qualche numero discreto
Trouan dui altri differenti in esso.

Dapoi terrai questo per consueto
Che'l lor produtto sempre sia eguale
Al terzo cubo delle cose netto,

El residuo poi suo generale
Delli lor lati cubi ben sottr atti
Varrà la tua cosa principale.

Original Poem (Cont'd.)

Del numer farai due tal part'a uolo
Che l'una in l'altra si produca schietto
El terzo cubo delle cose in stolo

Delle qual poi, per commun precetto
Torrai li lati cubi insieme gionti
Et cotal somma sara il tuo concetto.

El terzo poi de questi nostri conti
Se solue col secondo se ben guardi
Che per natura son quasi congionti.

El terzo cubo delle cose in stolo

Delle qual poi, per commun precetto
Torrai li lati cubi insieme gionti
Et cotal somma sara il tuo concetto.

El terzo poi de questi nostri conti
Se solue col secondo se ben guardi
Che per natura son quasi congionti.

Questi trouai, & non con passi tardi
Nel mille cinquecent'e quattro trenta
Con fondamenti ben sald'e gagliardi

Poem Translation

When the cube with the cose [unknowns] beside it $[x^3 + px]$

quates itself to some other whole number, $[= q]$

ind two other [numbers], of which it is the difference. $[u - v = q]$

ereafter you will consider this customarily

hat their product always will be equal $[uv =]$

o the third of the cube of the cose net. [wrong: $p^3/3$, instead of $(p/3)^3$]

s general remainder [the difference] then

f their cube sides [cube roots], well subtracted, $[\sqrt[3]{u} - \sqrt[3]{v}]$

ill be the value of your principal unknown. $[= x]$

the second of these acts,

hen the cube remains solo [on one side of the equation], $[x^3 = px + q]$

u will observe these other arrangements:

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

<u>Quartic Equations</u>: Ferrari (1545)

<u>Quintic Equations</u>: Ruffini (1797), Abel (1826), Galois (1832): <u>no</u> solution by radicals for general quintic

Open Problem

Can one solve any equations in two variables using radicals?

Example: $ax^n + by^n = c$

Solution: $x = \sqrt[n]{\frac{1}{a}},\ y = \sqrt[n]{\frac{c-1}{b}}$

But:

$$x^7 + ax^6y + bx^5y^2 + \cdots + gy^7 = 1$$

Example: $ax^n + by^n = c$

Solution: $x = \sqrt[n]{\frac{1}{a}},\ y = \sqrt[n]{\frac{c-1}{b}}$

But:

$$x^7 + ax^6y + bx^5y^2 + \cdots + gy^7 = 1$$

Does this ha[illegible] solution in radicals for any $a, b, \ldots, g$?

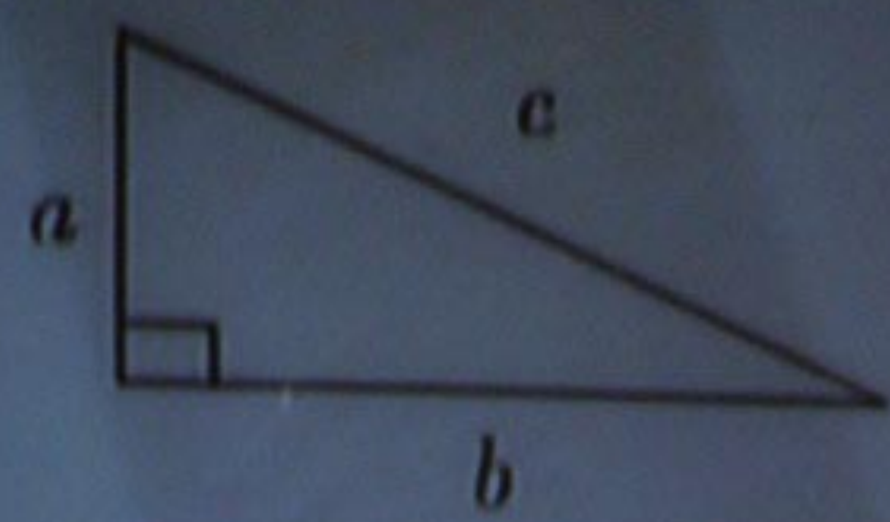
III. Elliptic Curves

$$y^2 = x^3 + Ax + B$$

Example $y^2 = x^3 - x$

Only solution is $x = 1,\ y = 0$ (Fermat).

In general there is no known method for finding the solutions. There is no known method to say whether solutions exist.



Question: Does $\exists$ a triangle as shown with a, b, c equal to rational numbers and area $=$ given integer n ?

$n = 1, 2, 3, 4$ no

$n = 5, 6, 7$ yes

example $3 - 4 - 5$ **triangle**

$$\text{area} = \frac{1}{2}.3.4 = 6.$$

For $n = 1$ Fermat solved an equi

problem.

Relation to elliptic curves:

$$\begin{cases} b^2 + a^2 = c^2 \\ \frac{1}{2}ab = n \end{cases}$$

$$\Longrightarrow \begin{cases} c^2 + 4n = (b+a)^2 \\ c^2 - 4n = (b-a)^2 \end{cases}$$

$$\Longrightarrow (b^2 - a^2)^2 = c^4 - 16n^2$$

$$\Longrightarrow c^2.(b^2 - a^2)^2 = c^6 - 16n^2c^2$$

Relation to elliptic curves:

$$\begin{cases} b^2 + a^2 = c^2 \\ \frac{1}{2}ab = n \end{cases}$$

$$\Longrightarrow \begin{cases} c^2 + 4n = (b \ldots \\ c^2 - 4n = (b - a) \ldots \end{cases}$$

$$\Longrightarrow (b^2 - a^2)^2 = c^4 - 16n^2$$

$$\Longrightarrow c^2.(b^2 - a^2)^2 = c^6 - 16n^2 \ldots$$

$\Longrightarrow \exists$ solution of elliptic cu...

$$\Longrightarrow (b^2 - a^2)^2 = c^4 - 16n^2$$

$$\Longrightarrow c^2.(b^2 - a^2)^2 = c^6 - 16n^2c^2$$

$\Longrightarrow \exists$ **solution of elliptic curve**

$$y^2 = x^3 - n^2x$$

In fact:

n **is a congruent number**

$\Longleftrightarrow y^2 = x^3 - n^2x$ **has infinitely**

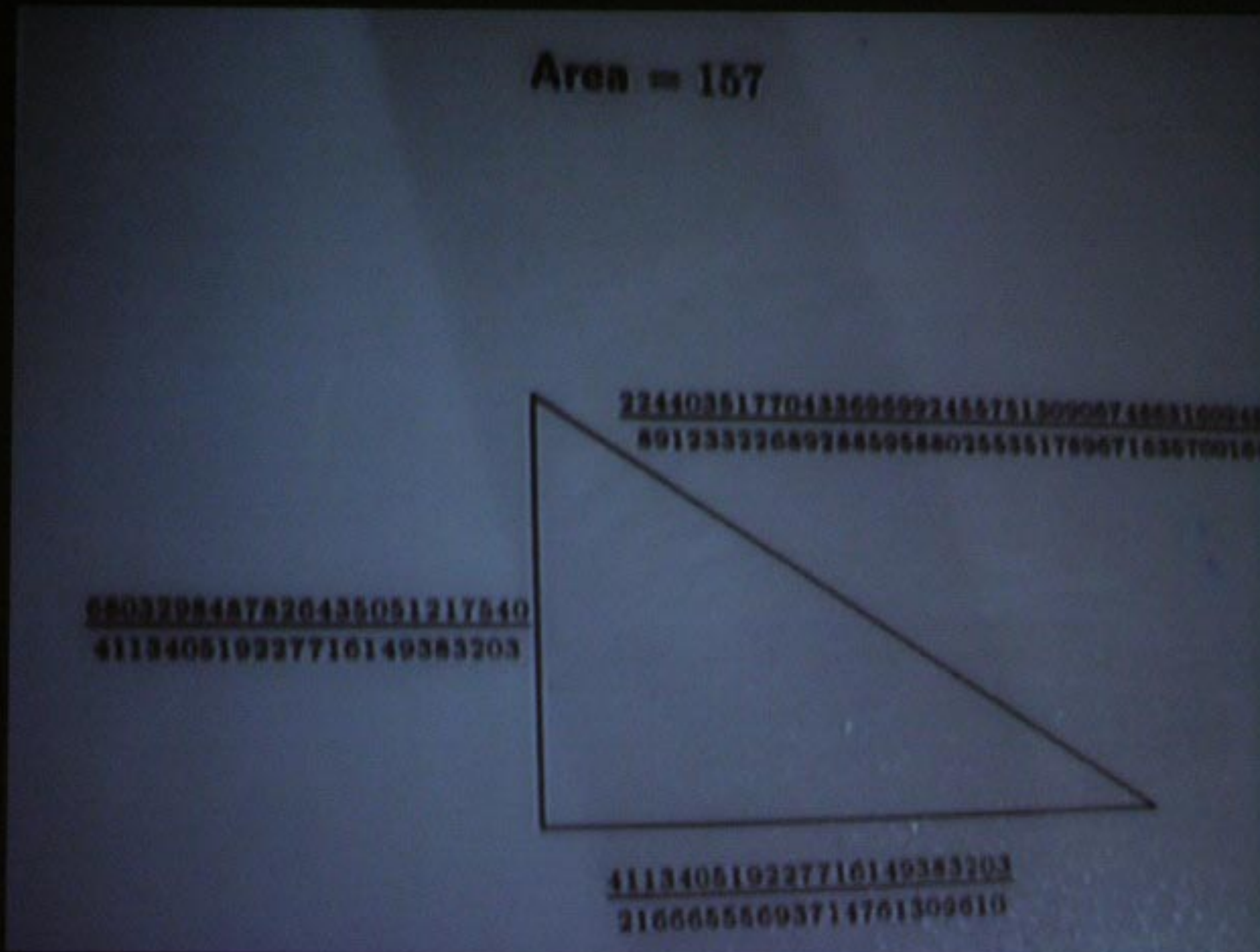
Question When does n occur as the area of a right-angled triangle with rational length sides?

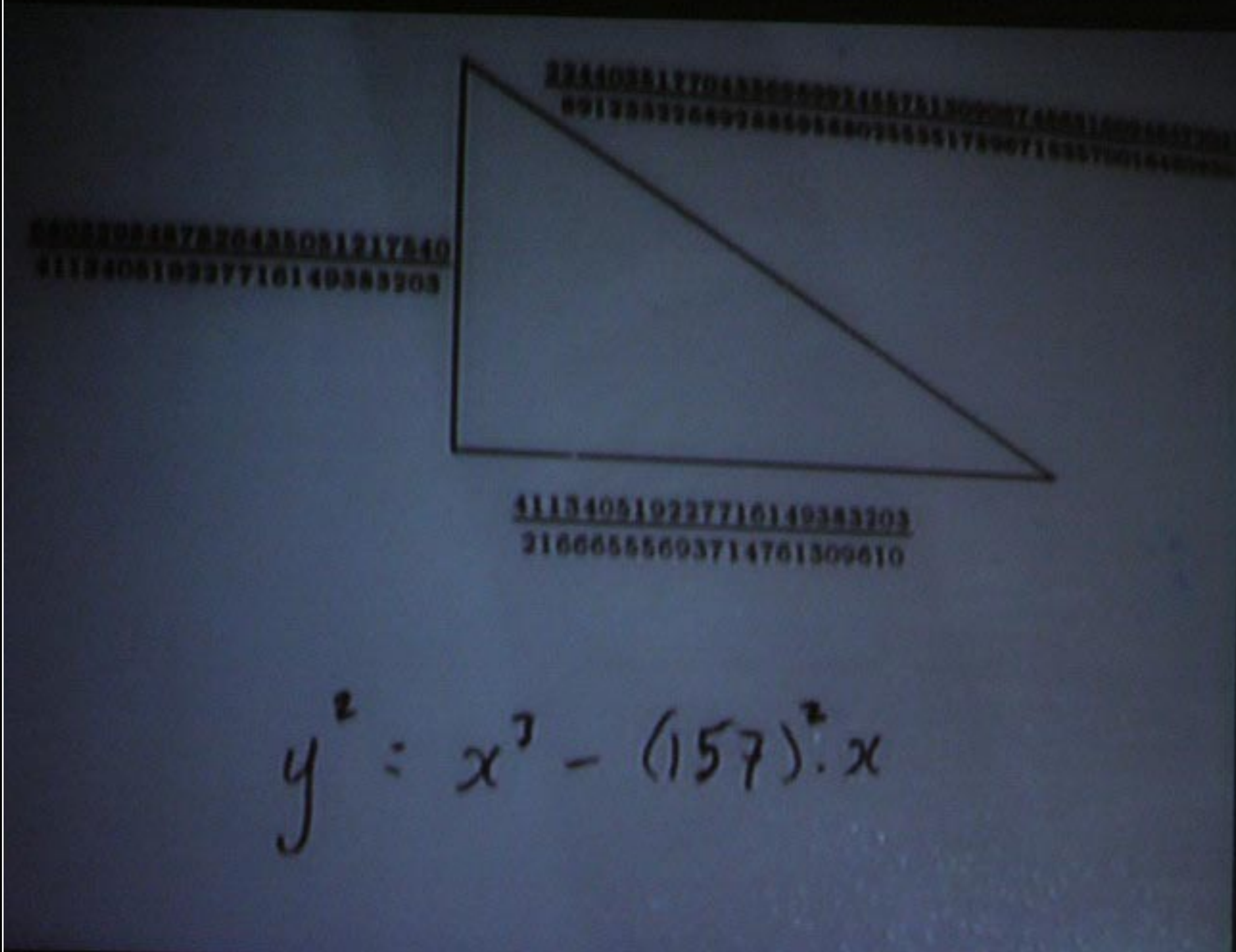
Conjectured answer (for n odd)

Yes — if and only if

$$\left\{\begin{matrix}\text{number of solutions}\\ \text{of } 2x^2+y^2+8z^2=n\end{matrix}\right\} = 2\times\left\{\begin{matrix}\text{number of solutions}\\ \text{of } 2x^2+y^2+32z^2=n\end{matrix}\right\}$$

n	$2x^2 + y^2 + 8z^2 = n$		$2x^2 + y^2 + 32z^2 = n$	
	#sol^{ns}	sol^{ns}	#sol^{ns}	sol^{ns}
1	2	$(0, \pm 1, 0)$	2	$(0, \pm 1, 0)$
3	4	$(\pm 1, \pm 1, 0)$	4	$(\pm 1, \pm 1, 0)$
5, 7	0		0	


Area = 157
6803298487826435051217540
411340519227716149383203
411340519227716149383203
21666555693714761309610


$y^2 = x^3 - (157)^2 \cdot x$