Factoring numbers with periodic optical interferograms

Vincenzo Tamma

with **Heyi Zhang, Xuehua He,**

Augusto Garuccio, Wolfgang Schleich, and Yanhua Shih

University of Maryland, Baltimore County
University of Bari, Italy

QAMF Workshop – Vancouver, 24th July 2010

Outline

- Factorization and the hyperbolic function
- Novel analogue algorithm
  for prime number decomposition
- Experimental results:
  Factorization of large integers
  with an optical computer
- Further developments

Why factoring large numbers is important?

Security of government information, our credit card information, emails, …

⇩

RSA encryption:

an encrypted message can be decipher only by knowing the factors of a given large number N

⇩

Our security is based on the actual impossibility of factoring large numbers in a reasonable time

Why factoring large numbers is difficult?

Determination of the factors of a large number N by dividing N for each trial factor l

↓

In the worst case we need to try each trial factor l from 1 to $\sqrt{N}$

↓

$$\sqrt{N} \quad divisions \qquad :$$

A lot of division operations for large numbers, costly processes for a digital computer

↓

10^{10} years (~ age of the universe) necessary to factor a 100-digit number (~333 bits)!

Factorization and the hyperbolic function

Hyperbolic function $$f(\xi) \equiv \frac{1}{\xi} \qquad 0 < \xi \leq 1$$

$$\Updownarrow \quad \xi_N \equiv N\xi$$

Complete knowledge about divisions for any given integer N

$$f(\xi) \equiv \frac{1}{\xi} = \frac{N}{N\xi} \equiv \frac{N}{\xi_N} \equiv f_N(\xi_N)$$

p,q factors of N $\Leftrightarrow$ $f_N(p) = q$

Towards a complete knowledge of the hyperbolic function

- **Number theory:**

  Read-out of the hyperbolic function by exploiting the periodicity of continuous truncated Gauss sums (CTGS)

- **Physics:**

  Interference as a tool to measure such a periodicity

Towards an analogue algorithm for factorization

Shor's idea: factorization of N by periodicity measurement of the function

$g_N(j) = a^j \bmod N$

15 is the largest number factored!

⇩

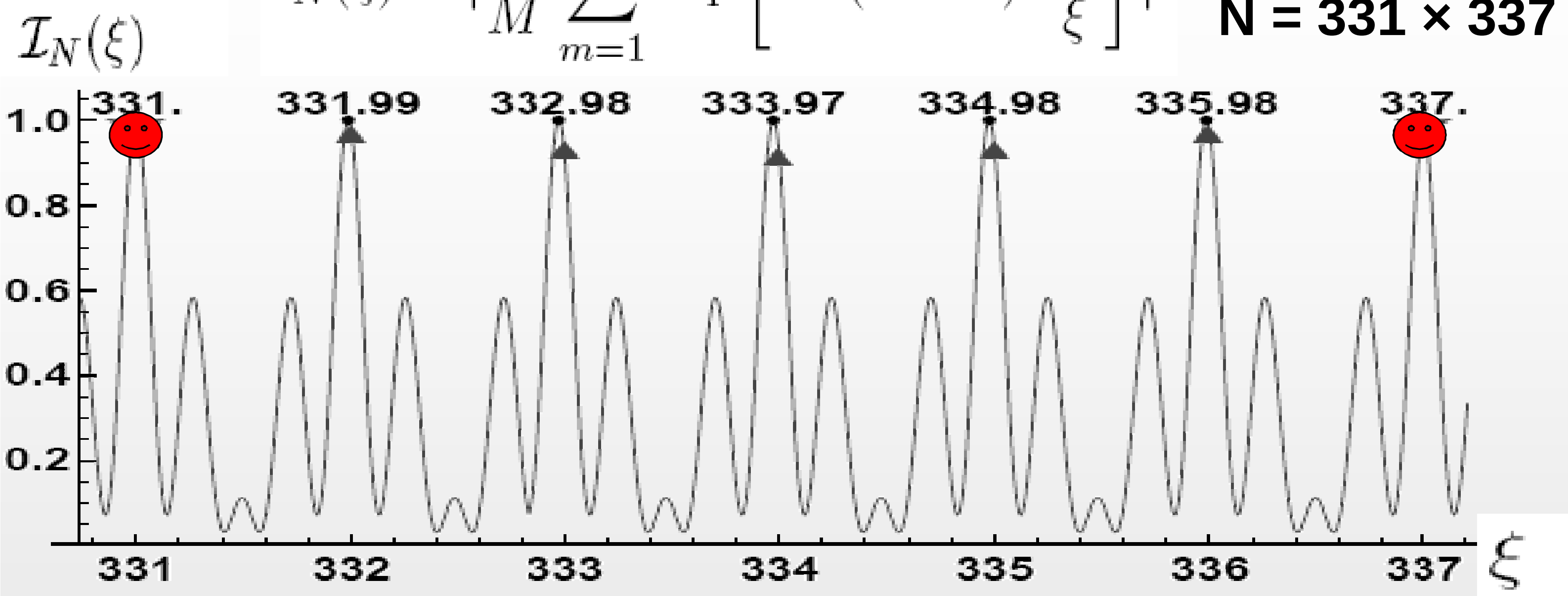
Is there a periodic "factoring" function other than Shor's function?

If yes, is the periodicity of such a function physically measurable with an analogue computer?

Continuous Truncated Gauss Sum (CTGS) function

$$\mathcal{I}_N(\xi) = |\frac{1}{M}\sum_{m=1}^{M}\exp\left[2\pi i(m-1)^2\frac{N}{\xi}\right]|^2$$

N = 331 × 337



Factors **ξ = 331, 337** ⟺ Interference Maxima

Non factors **ξ = 332,…,336** ⟺ Non maxima

Factoring numbers by measuring the periodicity of the CTGS function!

Optical computation: basic idea

Polychromatic waves of optical phases $\dfrac{x}{\lambda}$

x = length travelled by the waves
λ = continuous values of the wavelengths

x ≡ N nm
λ ≡ ξ nm

$$\frac{x}{\lambda} \equiv \frac{N}{\xi}$$

Nature makes division for us!

Optical computation: "factoring" optical interference

- Polychromatic source
- M optical paths $x_m \equiv (m-1)^2 x$

  with m=1,2,…,M

$\lambda \equiv \xi$ nm

$x \equiv N$ nm

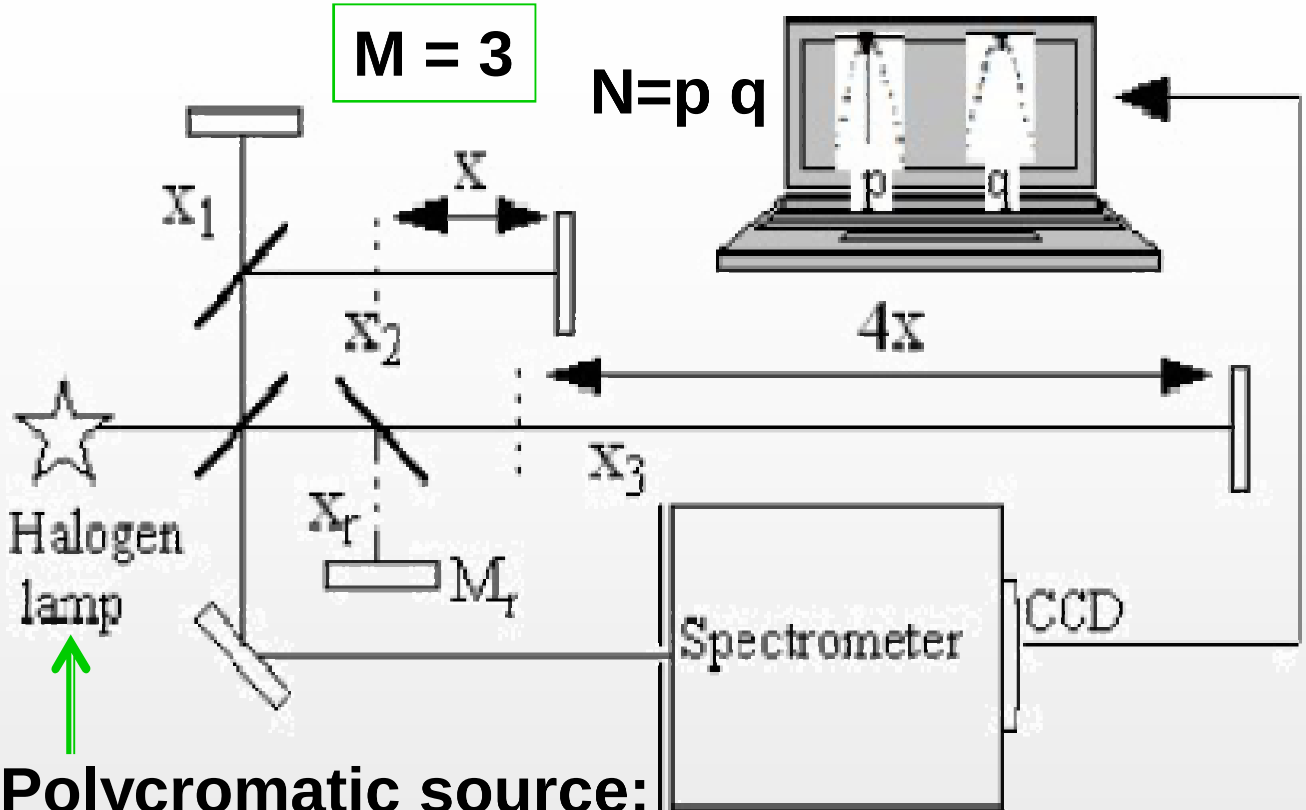
$$\frac{x}{\lambda} \equiv \frac{N}{\xi}$$

$$I_x(\lambda) \equiv \mathcal{I}_N(\xi) = \left| \frac{1}{M} \sum_{m=1}^{M} \exp\left[2\pi i (m-1)^2 \frac{N}{\xi}\right] \right|^2$$

The factors of N are the integer wavelengths corresponding to maxima

Connection between Physics and Number Theory

Optical computer



$x_m \equiv x_r + (m-1)^2\, x$

m=1,2,3

x = N nm

λ ≡ ξ nm

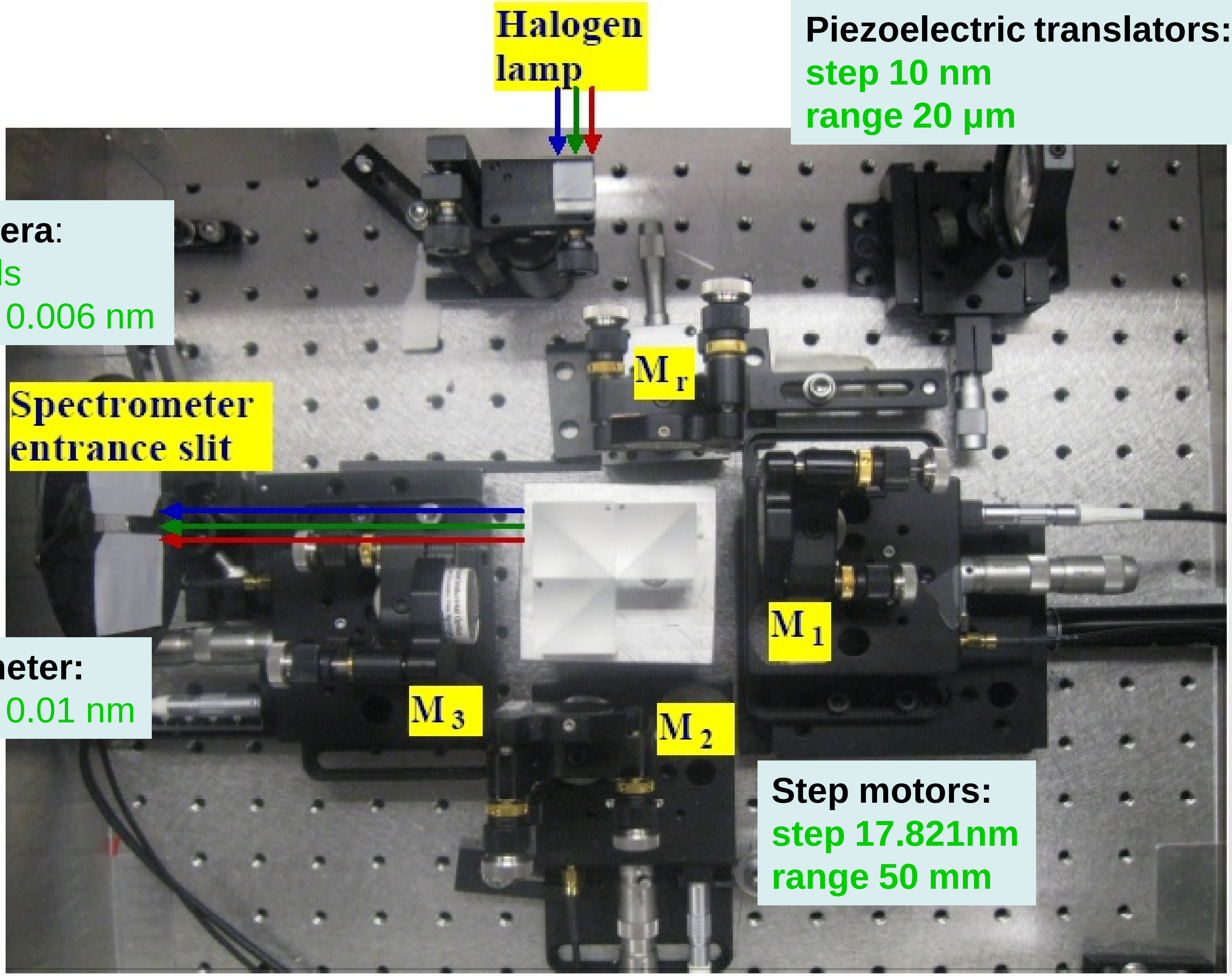
Polycromatic source:

all integer wavelengths- trial factors at the same time

Normalized interference spectrum:

$$I_x(\lambda) \equiv \mathcal{I}_N(\xi) = \left| \frac{1}{M} \sum_{m=1}^{M} \exp\left[2\pi i (m-1)^2 \frac{N}{\xi}\right] \right|^2$$

Picture of the optical computer



Piezoelectric translators:
step 10 nm
range 20 μm

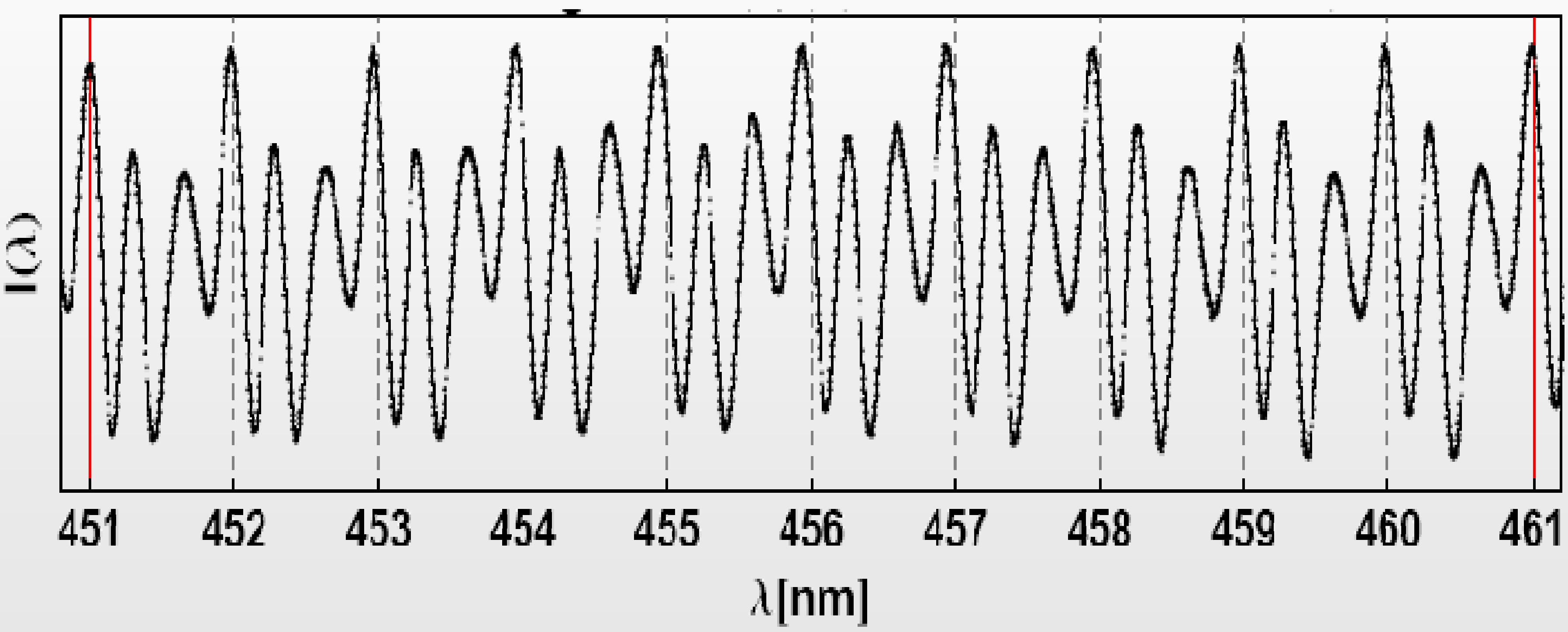
CCD camera:
2048 pixels
resolution 0.006 nm

Spectrometer:
resolution 0.01 nm

Step motors:
step 17.821nm
range 50 mm

Experiment for x=207911 nm=451×461nm

M=3 interfering terms



Factoring several numbers with the same analogue function

Several N encoded by **rescaling the wavelengths**

M optical paths

$x_m \equiv (m-1)^2 x$

m=1,2,…,M

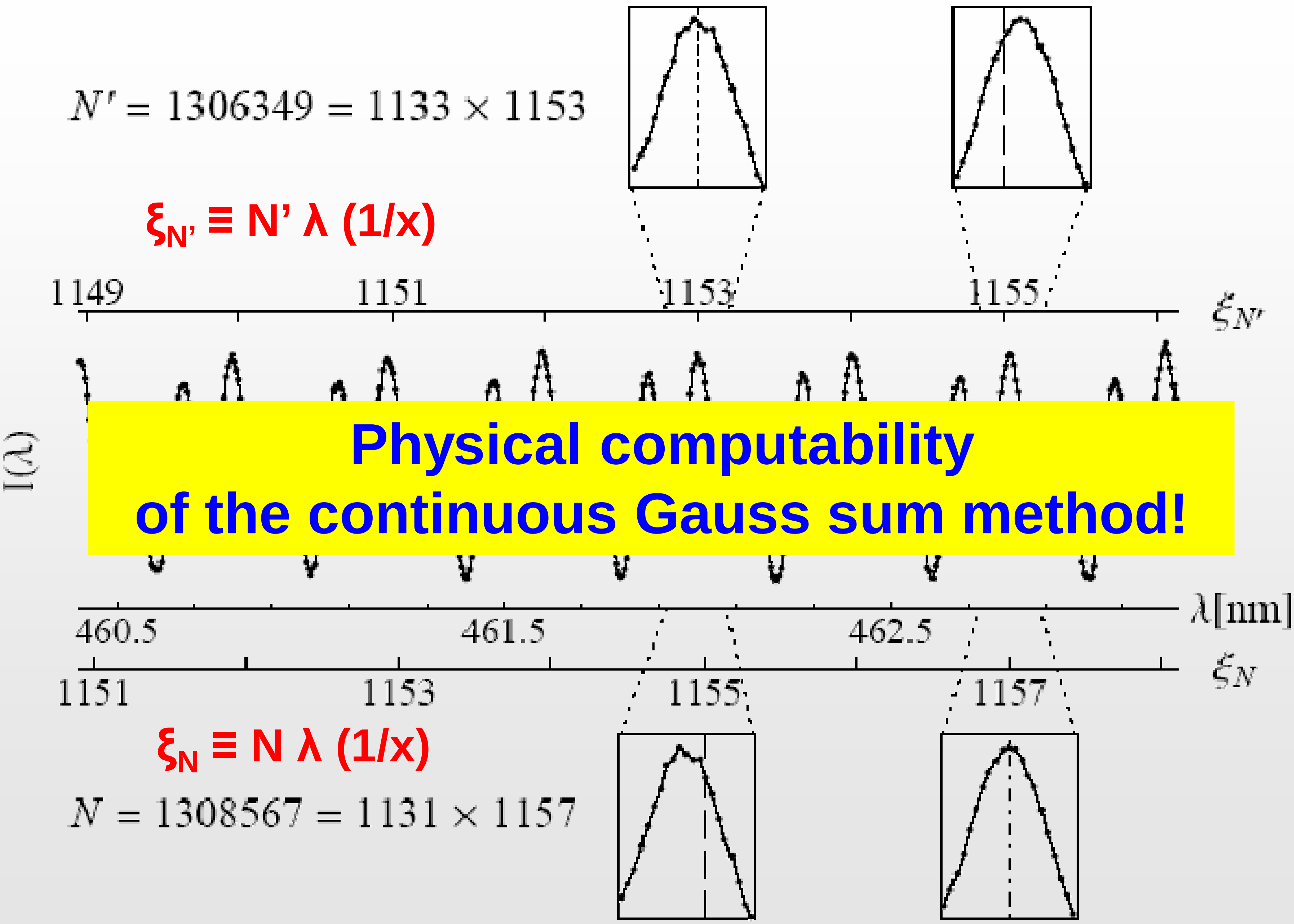
$\lambda \equiv (\xi_N/N)\ x$

$$\frac{x_m}{\lambda} \equiv \frac{(m-1)^2 N}{\xi_N}$$

$$I_x(\lambda) \equiv \mathcal{I}(\xi_N) = \left| \frac{1}{M} \sum_{m=1}^{M} \exp\left[2\pi i (m-1)^2 \frac{N}{\xi_N}\right] \right|^2$$

The ratios N/ξ_N are stored for several numbers N at the same time!

Experiment for x = 523426.8 nm



$\xi_{N'} \equiv N' \lambda (1/x)$

$\xi_{N} \equiv N \lambda (1/x)$

Physical computability
of the continuous Gauss sum method!

Prior art: Discrete Gauss sums

$$\mathcal{A}_N(l) = \frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i (m-1)^2 \frac{N}{l}\right]$$

Mehring et al., PRL 98,120502 (2007); Gilowsky et al., PRL 100, 030201 (2008); Bigourd et al., PRL 100, 030202 (2008); Sadgrove et al., PRL 101, 180502 (2008)

- **Ratio N/l pre-calculated before the experiment is run**

Jones, Phys. Lett. A 372, 5758 (2008)

- **No periodicity measurement: independent experimental runs for each trial factor**

CTGS method:

- **The wave nature of light performs the divisions N/l**
- **Periodicity measurement: parallel experimental evaluation of the CTGS function for trial factors of several integers N**

CTGS optical algorithm

For a **fixed unit of displacement x:**

$$I_x(\lambda) = |\frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i(m-1)^2 \frac{x}{\lambda}\right]|^2$$

Scaling property: $\xi_N = \frac{N}{x}\lambda$

Interval of trial factors: $[\xi_N^{(min)}, \xi_N^{(max)}] = [\frac{N}{x}\lambda_{min}, \frac{N}{x}\lambda_{max}]$

If the factors of N are outside of such a range…

We can vary x to cover all the trial factors in the range:

$$3 \leq \xi_N < \sqrt{N}$$

CTGS optical algorithm

$$I(\lambda; x_i) = |\frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i(m-1)^2\frac{x_i}{\lambda}\right]|^2$$

Parameter x not fixed anymore!

$x=x_i$ with i=0,1,…,n-1

$$\xi_N = \xi_{N,i} = \frac{N}{x_i}\lambda$$

Visible range:
400nm=$\lambda_{min} \leq \lambda \leq \lambda_{max}$=800nm

$$[\xi_{N,i}, \xi_{N,i+1}] = [\frac{N}{x_i}\lambda_{min}, \frac{N}{x_i}\lambda_{max}].$$

Number n of interferograms:

$$n < 1 + log_c\sqrt{N}$$

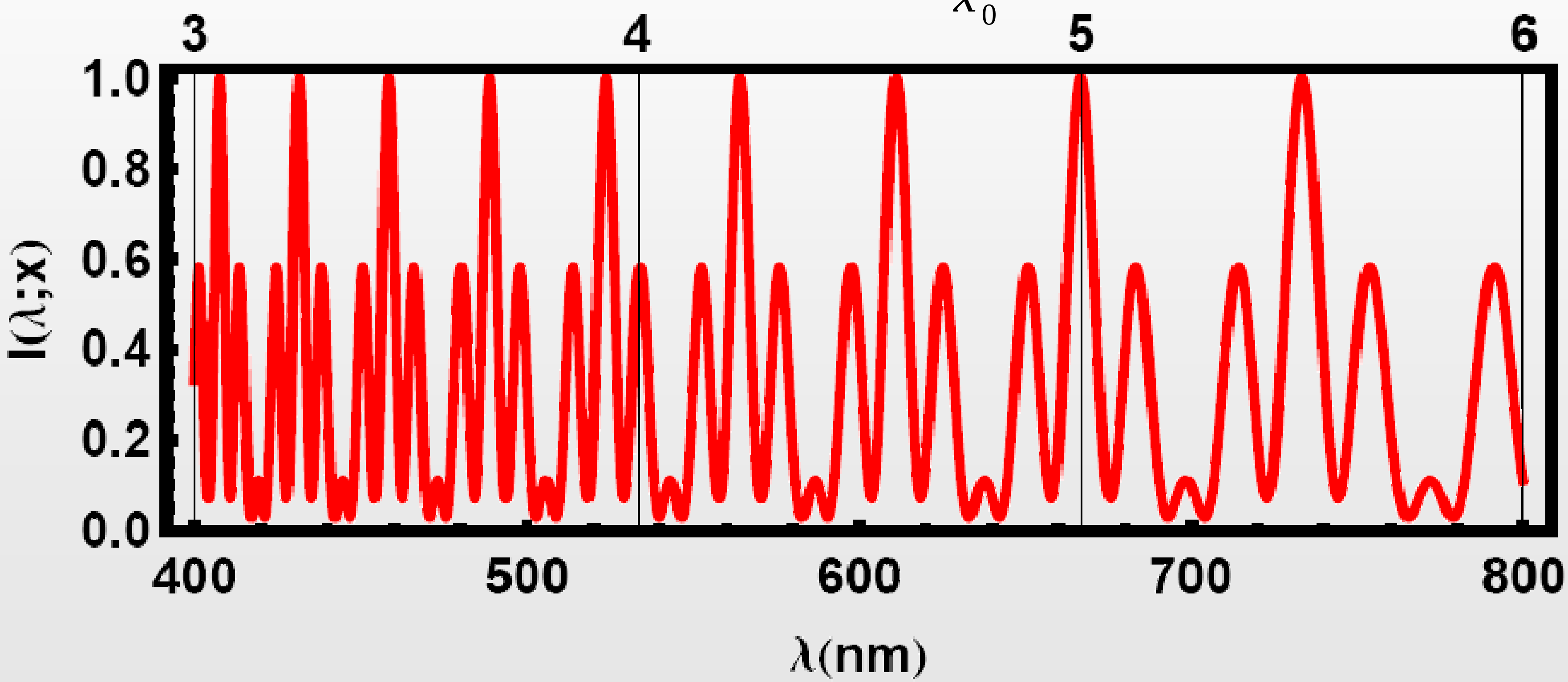
$$c = \frac{\lambda_{max}}{\lambda_{min}} > 1$$

c=2 in the visible range:
400nm$\leq \lambda \leq$ 800nm

Example for N=55 $3 \le \xi_N < \sqrt{N}$

$$x = x_0 \equiv N \frac{\lambda_{min}}{3}$$

$$\xi_{N,0} = \frac{N}{x_0} \lambda$$



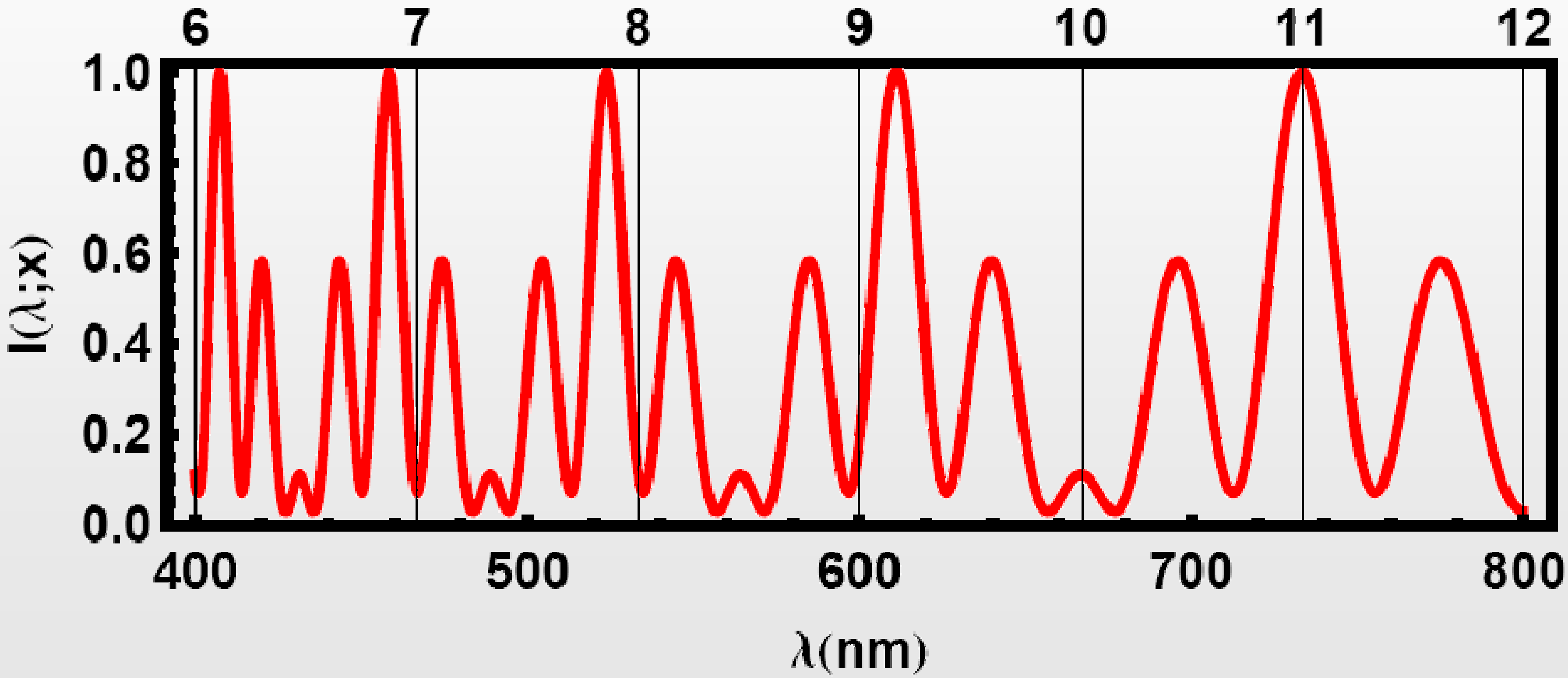
5 is a factor!

Example for N=55

$$3 \leq \xi_N < \sqrt{N}$$

$$x_1 = \frac{\lambda_{min}}{\lambda_{max}} x_0 < x_0$$

$$\xi_{N,1} = \frac{N}{x_1} \lambda$$



11 is a factor!

CTGS analogue algorithm

Algorithm principle:

- **Measurement of the periodicity of the CTGS "factoring" function**
  (connection with Shor's method)

- **Factors of several numbers by rescaling the measured periodicity**

CTGS analogue algorithm

Optical implementation:

- Optical computer able to physically compute the CTGS algorithm

- Factors of two seven-digit numbers exploiting only three interfering paths (pending patent)

- Generalization to higher order non linear optical paths: "continuous truncated exponential sums" (CTES)

$$I(\lambda; x) \equiv I(\xi_N; N) = \left|\frac{1}{M}\sum_{m=1}^{M}\exp\left[2\pi i (m-1)^j \frac{N}{\xi_N}\right]\right|^2 \qquad j>2$$

Further developments

➢Use of other physical systems (liquid crystal grating, neutrons, BEC, ions, etc.)

➢Digital implementation of the CTGS algorithm

➢Polynomial scaling with entangled systems as multi-photon entangled states

Acknowledgements

J. Franson, T. Pittman and T. Worchesky

M. Fitelson, M. Genovese, K. McCann, R. E. Meyers,

S. Pascazio, A. Pittenger, M. H. Rubin, and H. Winsor

"The theory of computation has traditionally been studied almost entirely in the abstract, as a topic in pure mathematics. This is to miss the point of it. Computers are physical objects, and computations are physical processes. What computers can or cannot compute is determined by the laws of physics alone, and not by pure mathematics."

David Deutsch

Thank you for your attention!

Single generic number N

$$n < 1 + log_c\sqrt{N}$$

$$c_= \frac{\lambda_{max}}{\lambda_{min}} > 1$$

$$N = (\frac{x_0}{\lambda_{min}})^2$$

Range of numbers $N_{min} \leq N \leq N_{max}$

$$n < 1 + log_{c'}\sqrt{N_{max}}$$

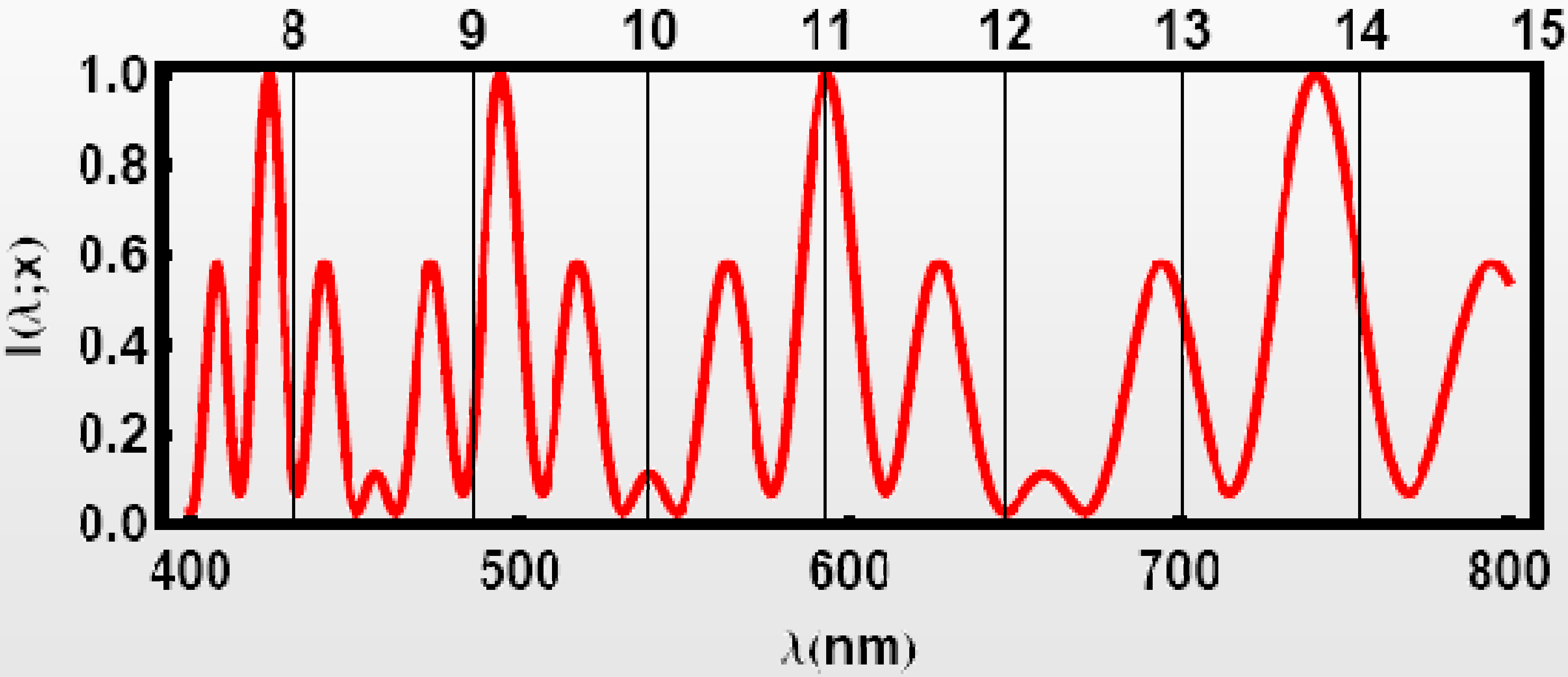
$$c' = \frac{N_{min}\lambda_{max}}{N_{max}\lambda_{min}} > 1$$

$$N_{max} \equiv x_0\frac{\sqrt{N_{min}}}{\lambda_{min}}$$

$$N_{min} > N_{max}\frac{\lambda_{min}}{\lambda_{max}}$$

Example for N=55 $\sqrt{N} < \xi_N < N$

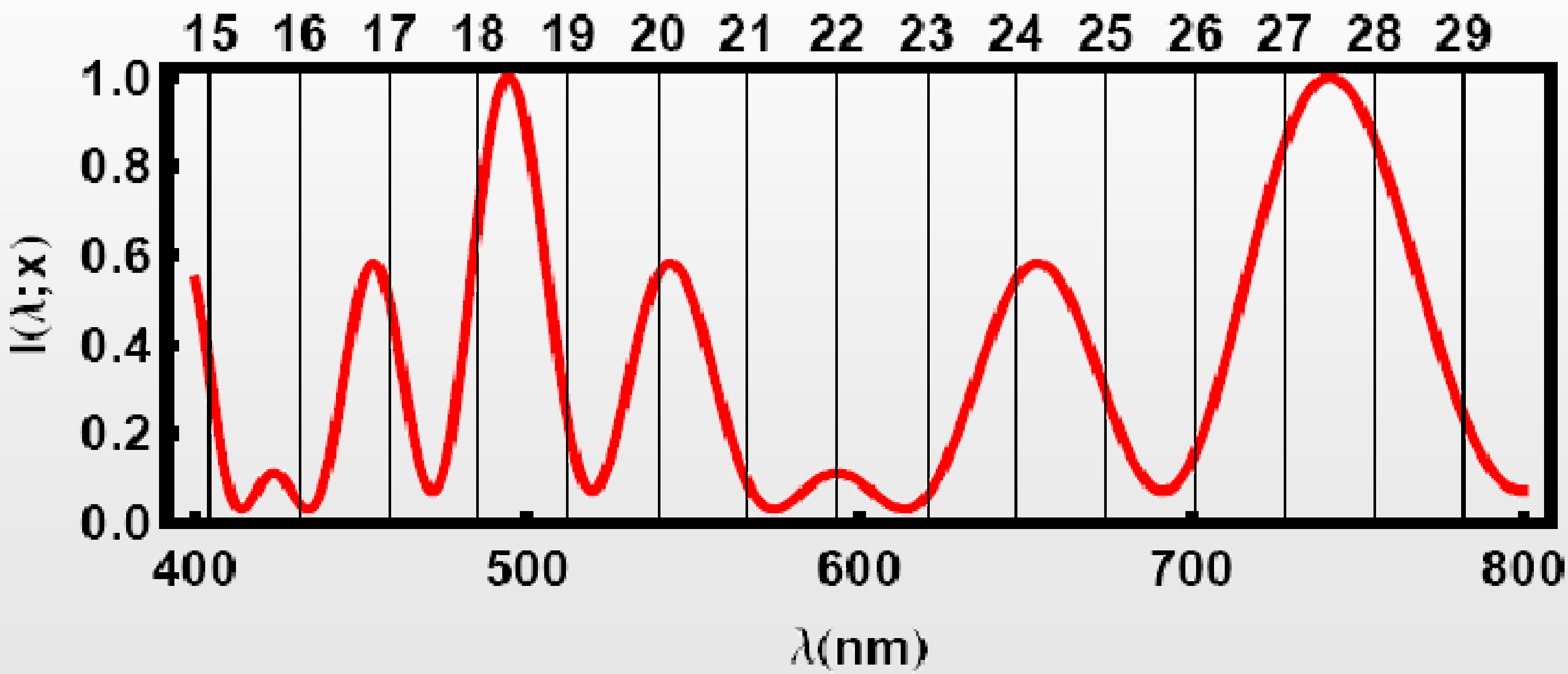
$$x = x_0 \equiv N\frac{\lambda_{min}}{\sqrt{N}} = \sqrt{N}\lambda_{min}$$



11 is a factor!

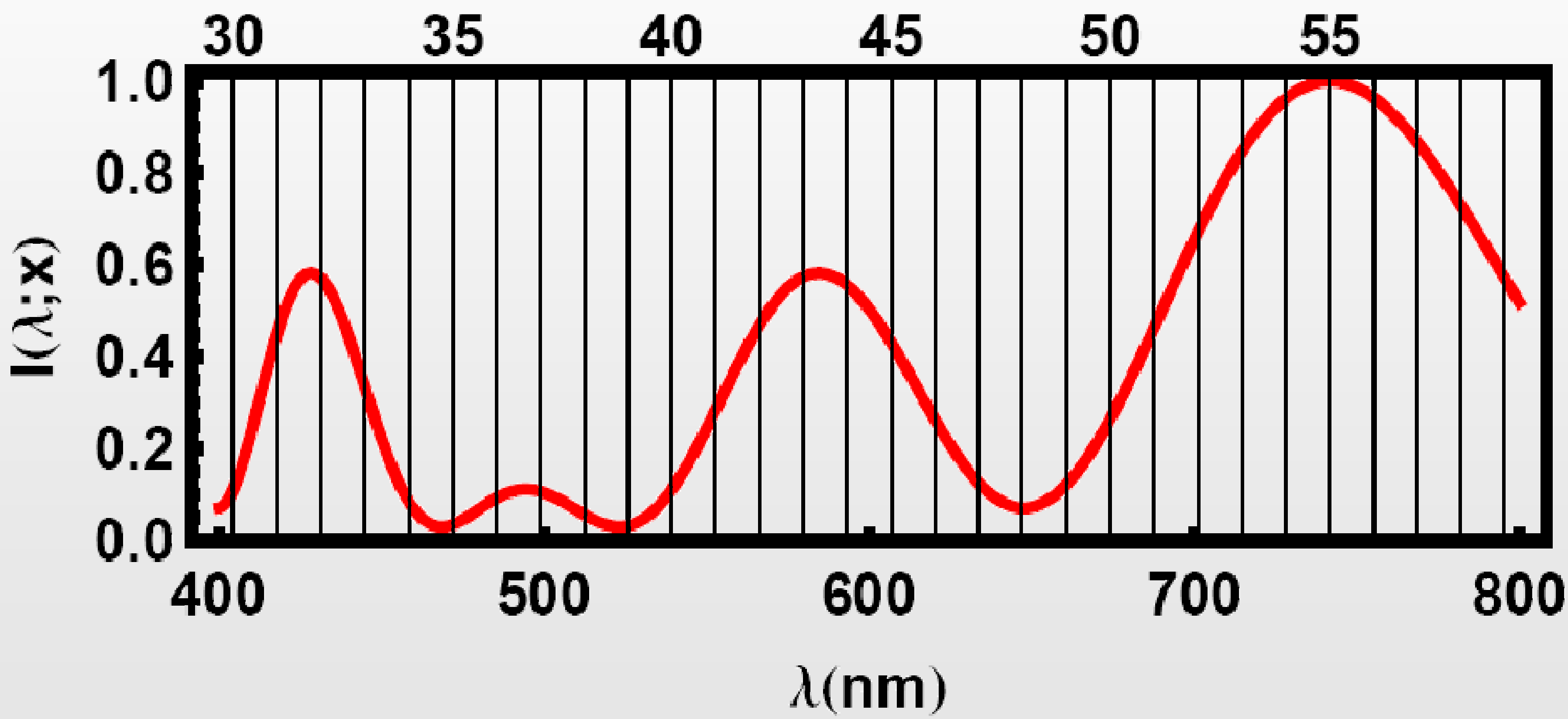
Example for N=55 $\sqrt{N} < \xi_N < N$

$$x_1 - \frac{\lambda_{min}}{\lambda_{max}} x_0 < x_0$$

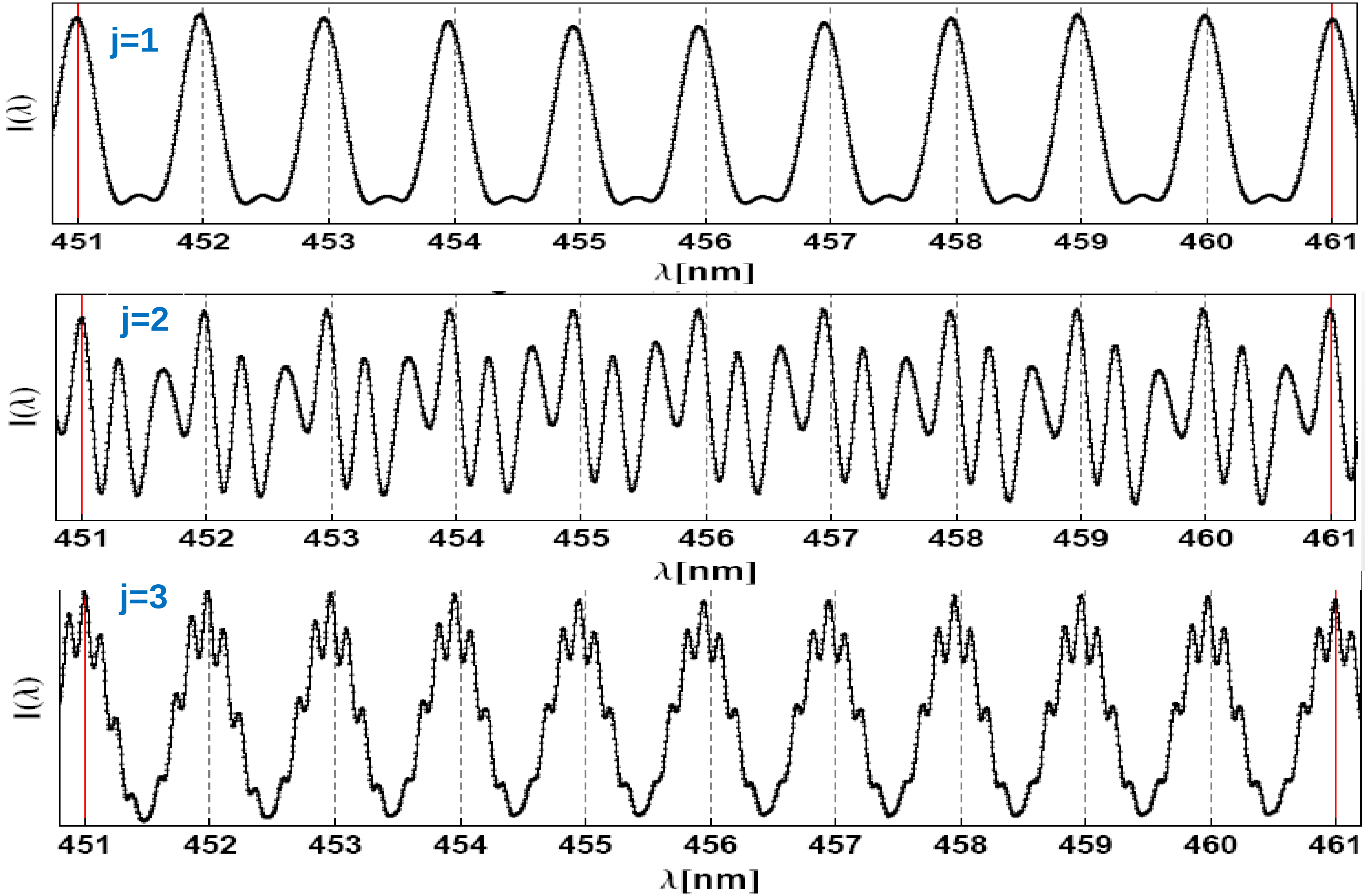


Example for N=55 $\sqrt{N} < \xi_N < N$

$$x_2 = \frac{\lambda_{min}}{\lambda_{max}} x_1 < x_1 < x_0$$



Experiments with displacement unit x = 451×461 nm for different orders j=1,2,3



Maximum factorable number with a single interferogram in perfect conditions

$$I(\lambda) = |\frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i (m-1)^2 \frac{x}{\lambda}\right]|^2$$

x fixed

$\xi_N \equiv N\lambda/x$

For a give spectrum $\lambda_{min} \leq \lambda \leq \lambda_{max}$

For a given number N in order to cover all the trial factors $\xi_N \in [1, \sqrt{N}]$

$$x \leq \frac{\lambda_{max}^2}{\lambda_{min}}$$

$$(\frac{x}{\lambda_{max}})^2 \leq N \leq \frac{x}{\lambda_{min}}$$

$$x = x_{max} = \frac{\lambda_{max}^2}{\lambda_{min}}$$

$$N_{max} = \frac{x}{\lambda_{min}} = (\frac{\lambda_{max}}{\lambda_{min}})^2$$

The necessary wavelength bandwidth increases as the maximum number to be factored

Maximum factorable number in given experimental conditions

$$\xi_N \in \left[1, \sqrt{N}\right]$$

$$\sqrt{\frac{x}{|\Delta\lambda|}} \leq N_{max} < \frac{x}{|\Delta\lambda|}$$

$$|\Delta\lambda| \doteq |\Delta\lambda_{op}| + |\Delta\lambda_{eff}|$$

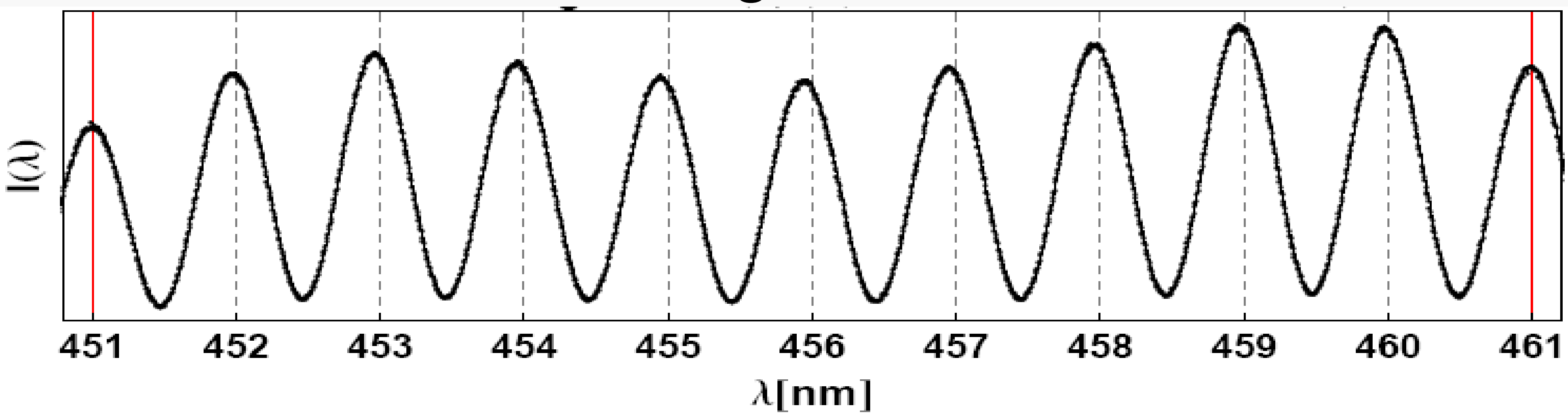
$$\Updownarrow$$

$$\frac{\lambda}{|\Delta\lambda|} \leq N_{max} < \left(\frac{\lambda}{|\Delta\lambda|}\right)^2$$

The maximum achievable value of x together with the resolution in the wavelengths associated with our experimental device affect the largest factorable number

Experiment for x = 207911 nm = 451×461 nm

M=2 interfering terms (one mirror blocked)



Generalization to continuous exponential sums

Continuous Gauss sum interferogram:

$$I(\lambda) \equiv \mathcal{I}(\xi_N; N) = |\frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i(m-1)^2 \frac{N}{\xi_N}\right]|^2$$

M optical paths
$x_m \equiv (m\text{-}1)^2\ x$
with m=1,2,…,M

↓

Continuous exponential sum interferogram of order j>2:

$$I(\lambda) \equiv \mathcal{I}_j(\xi_N; N) = |\frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i(m-1)^j \frac{N}{\xi_N}\right]|^2$$

M optical paths
$x_m \equiv (m\text{-}1)^j\ x$
with m=1,2,…,M

Liquid crystal grating analog computer

Experimental conditions for a generic optical analog computer:

$op_m = n_m x_m \equiv (m-1)^2 x$

(m=1,2,…,M)

$\lambda \equiv (\xi_N/N)\ x$

⟺

$$I(\lambda) \equiv \mathcal{I}(\xi_N; N) = \left|\frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i (m-1)^2 \frac{N}{\xi_N}\right]\right|^2$$

First solution

↓

Knob for the lengths x_m ($n_m = 1$)

↓

Symmetric multi-path Michelson interferometer

Second solution

↓

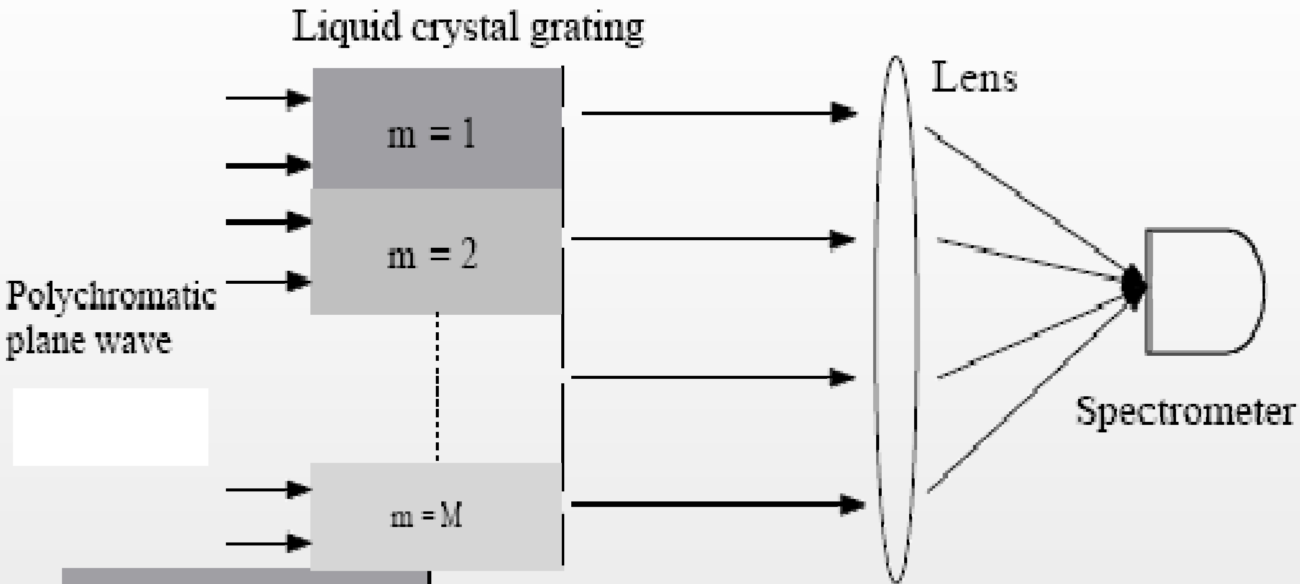
Knob for the refraction indexes n_m ($x_m = d$)

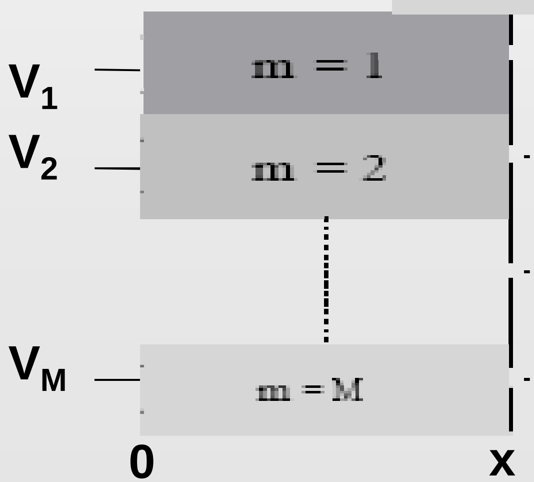
↓

Liquid crystal grating

Liquid crystal grating analog computer

M-term continuous Gauss sum ⇨ M different regions in a liquid crystal grating

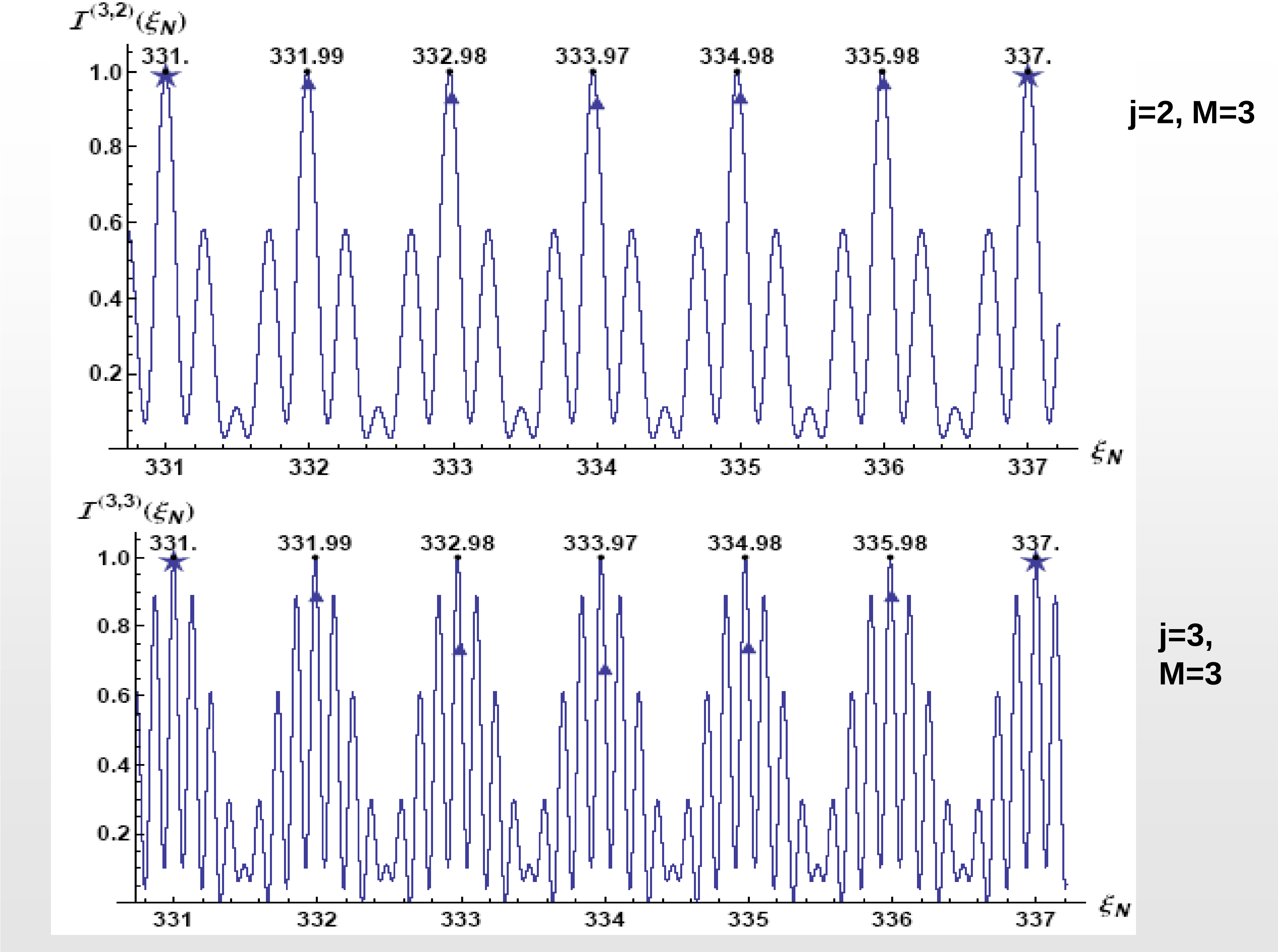




We apply the potentials V_m such that:

$$op_m(V_m)=n_m(V_m)\, d= (m-1)^2\, x$$

x unit of displacement in the optical paths



$\mathcal{I}^{(3,2)}(\xi_N)$
331.
331.99
332.98
333.97
334.98
335.98
337.
1.0
0.8
0.6
0.4
0.2
331
332
333
334
335
336
337
ξ_N
j=2, M=3
$\mathcal{I}^{(3,3)}(\xi_N)$
331.
331.99
332.98
333.97
334.98
335.98
337.
1.0
0.8
0.6
0.4
0.2
331
332
333
334
335
336
337
ξ_N
j=3,
M=3

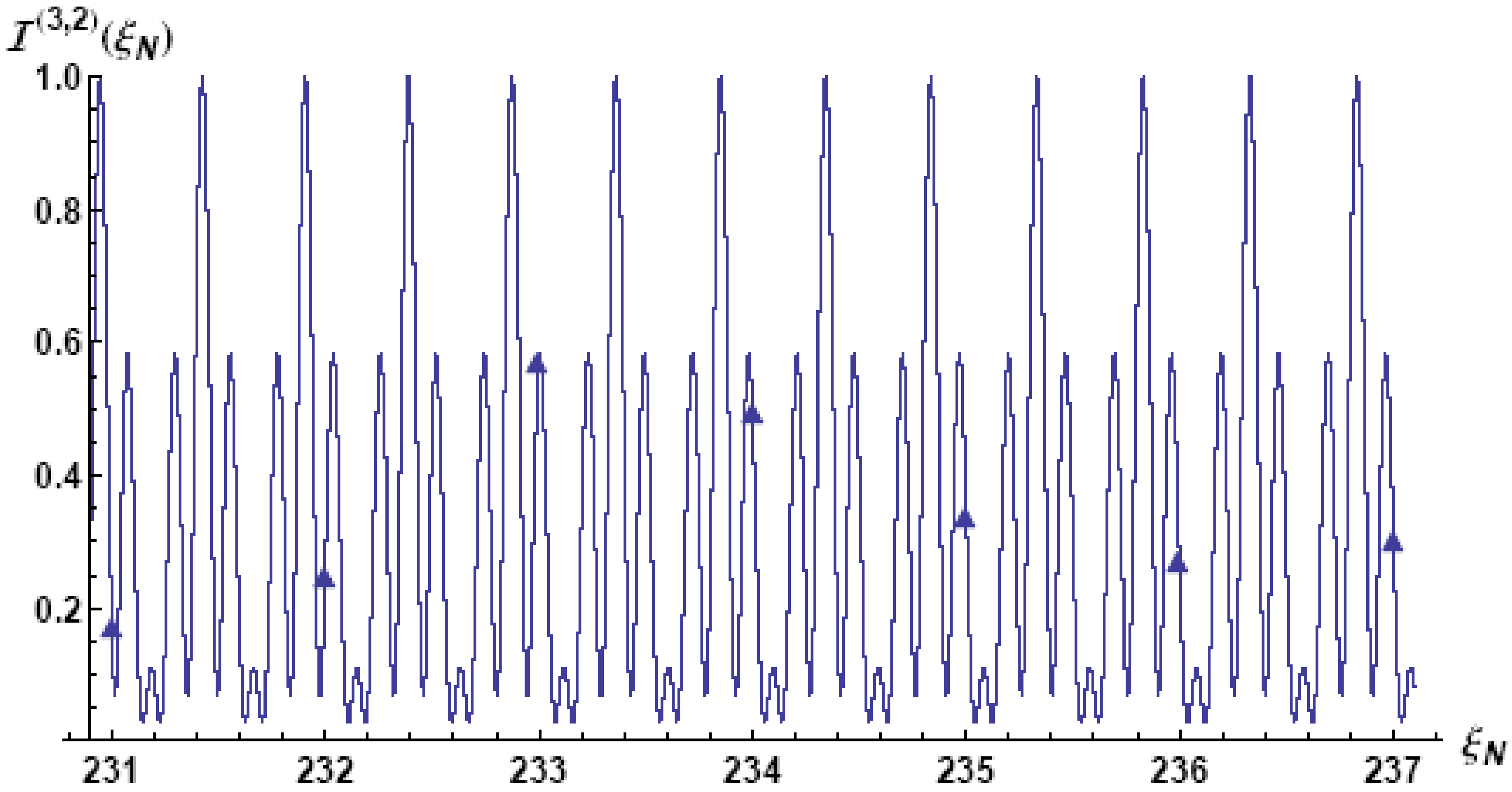
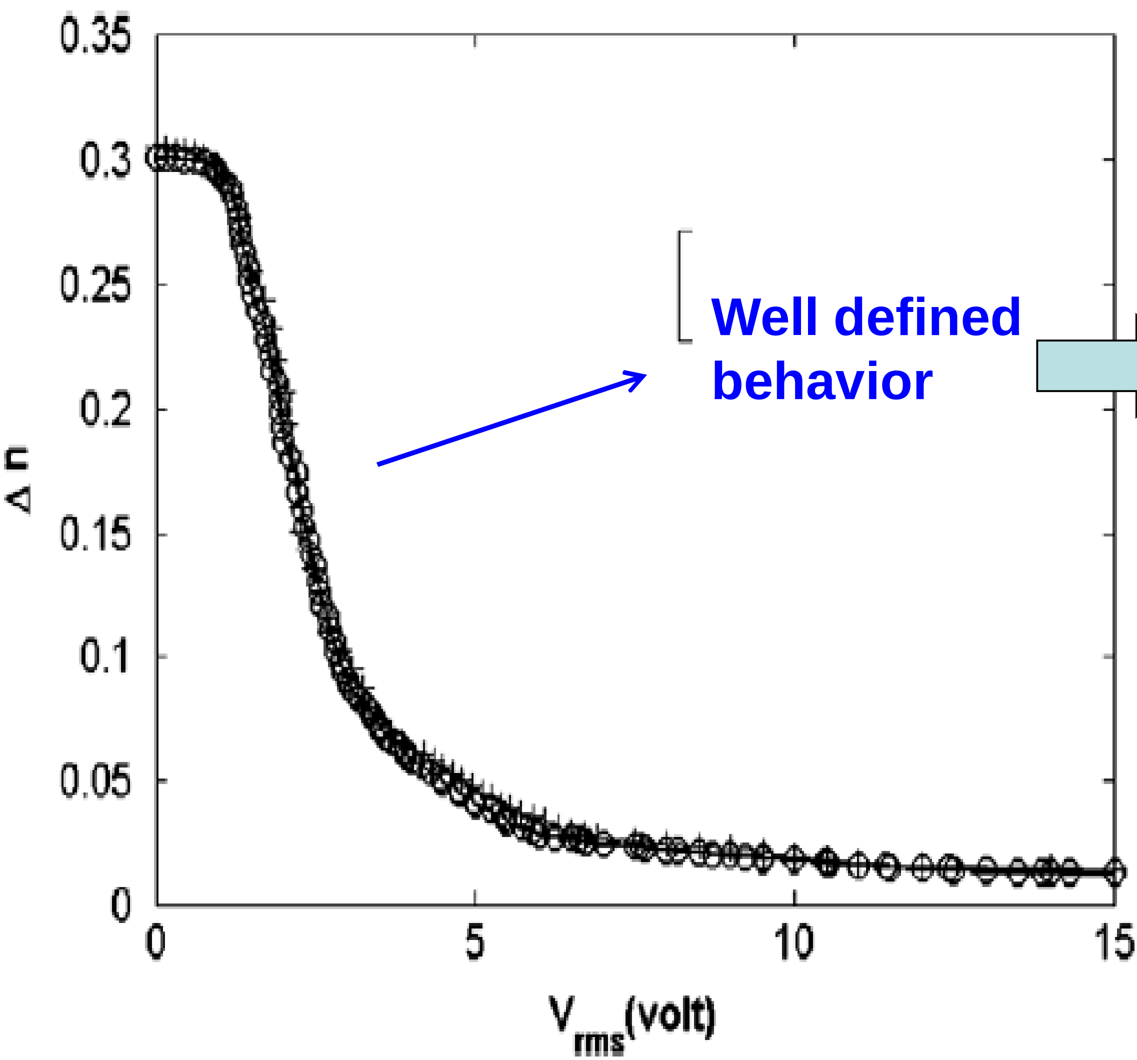


Figure 2.3: Rescaled CTES interferogram $\mathcal{I}^{(M,j)}(\xi_N; N)$ in Eq. (2.11) for $N = 111547$, with $M = 3$ and $j = 2$, as a function of the variable ξ_N in Eq. (2.2) in the interval $[230.9, 237.1]$. We can clearly see that all the trial factors in such a range, represented by triangles, have a relatively limited value of intensity so that they can be easily disregarded as possible factors.

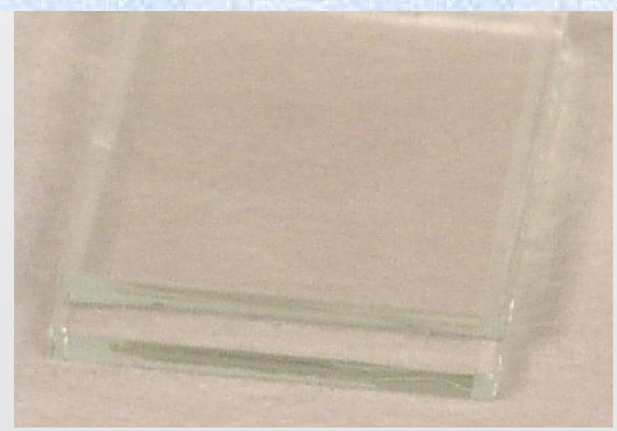
Liquid crystal cells: an interesting behavior…



A. Jafari et al. ,
Optics Communications
266, 207-213 (2006)

Index of refraction, for radiation in the ordinary mode, fixed by the applied voltage V:

n = n(V)



Basic ideas in the past realizations of:

$$A_N^{(M,j)}(\ell) = \frac{1}{M}\sum_{m=1}^{M} \exp\left[-2\pi i\,(m-1)^j \frac{N}{\ell}\right]$$

Interaction of M laser pulses with two level systems

↓

Occupation probability of the excited state given by the truncated Gauss sum

1) Nuclear magnetic Resonance
(Mehring et al., PRL 98,120502 (2007)
Mahesh et al., PRA 75,062303 (2007)
Peng and Suter, EPL 84, 40006 (2008))

2) Cold atoms
(Gilowsky et al., PRL 100, 030201 (2008))

3) Sequence of shaped ultrashort pulses (Bigourd et al., PRL 100, 030202 (2008)
Weber et al., EPL 83, 34008 (2008))

↓

Gauss sum reproduced by the interference produced by the M pulses

4) Bose Enstein Condensate in an optical lattice
(Sadgrove et al., PRL 101, 180502 (2008))

↓

Gauss sum reproduced by the energy of the atomic ensemble

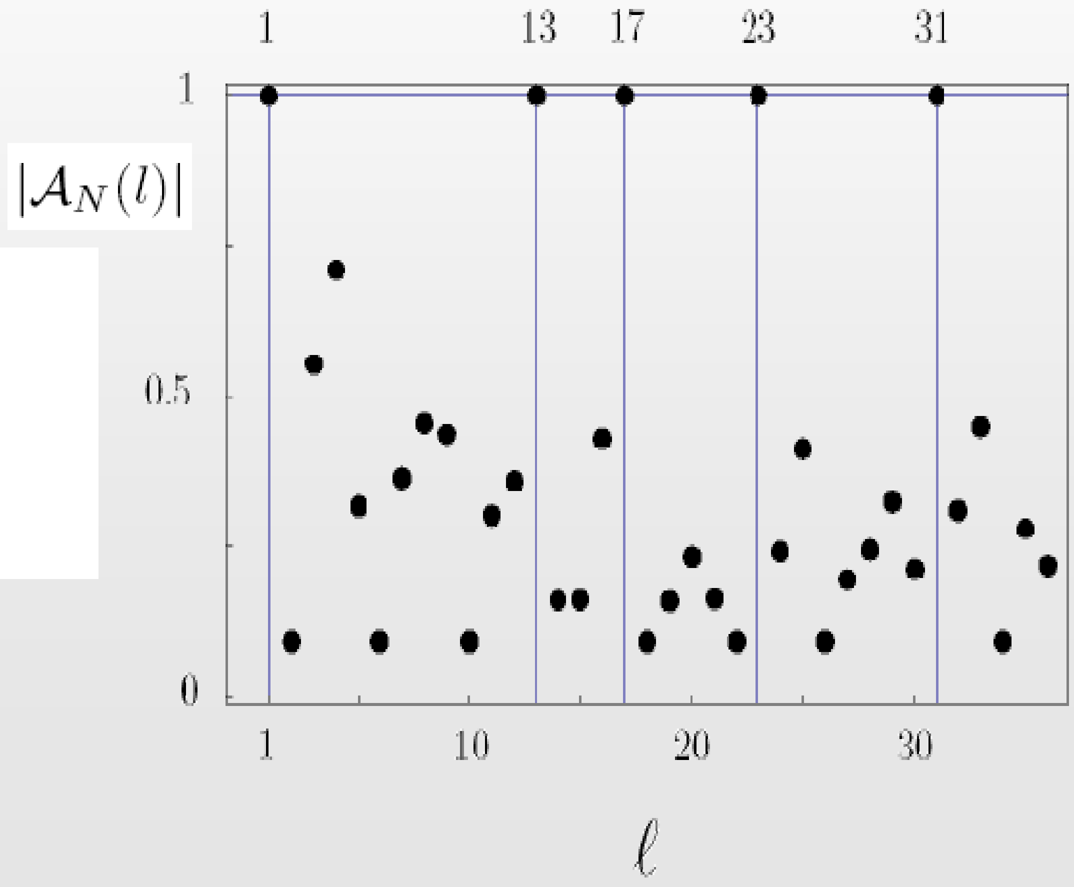
Effective factorization with a discrete Gauss sum approach

For a given value of N

Input of the experiment: l

Output of the experiment: $|\mathcal{A}_N(l)|$

$$\mathcal{A}_N(l) = \frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i (m-1)^2 \frac{N}{l}\right]$$



The experiment performs the ratio N/l

Is "l" a factor?

$|\mathcal{A}_N(l)| = 1$ ⇒ **Yes!**

$|\mathcal{A}_N(l)| < 1$ ⇒ **No!**