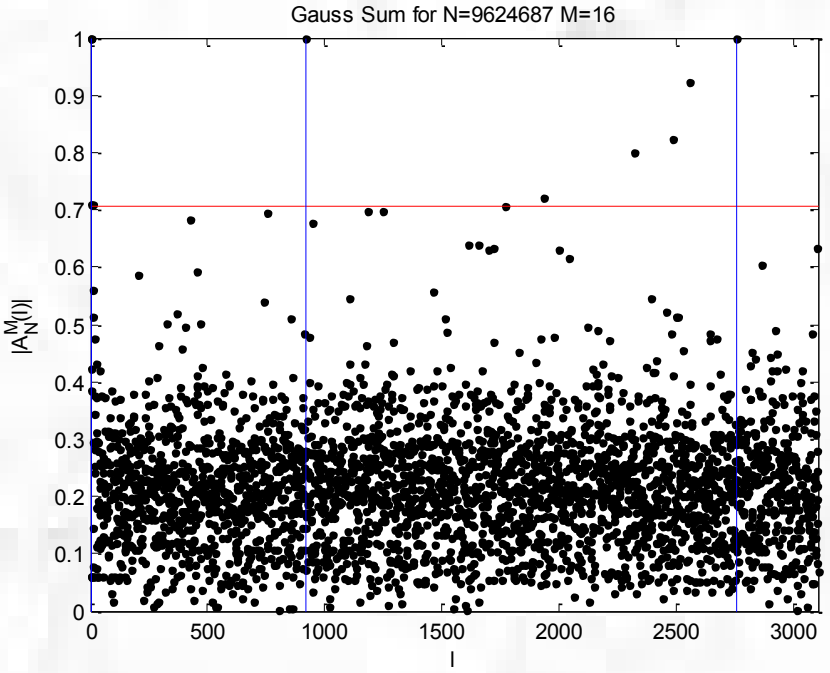
Factorization with Gauss Sums: Scaling Properties of Ghost Factors

M. Stefanak, W. Merkel, W. P. Schleich, D. Haase, and H. Maier

New Journal of Physics 9 (2007) 370



Paper Presentation

Math 475

Ron Caplan

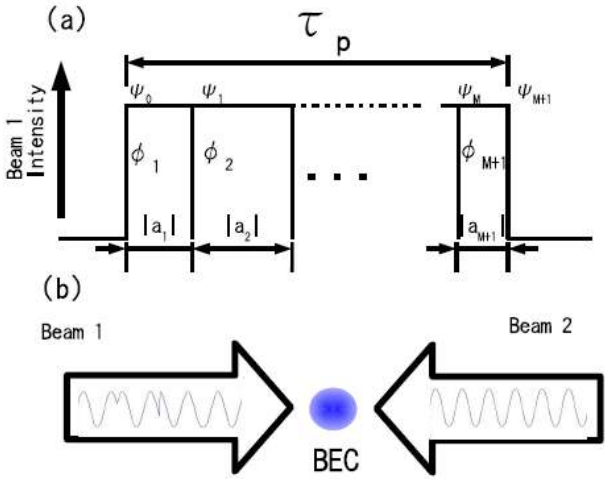
March 23, 2009

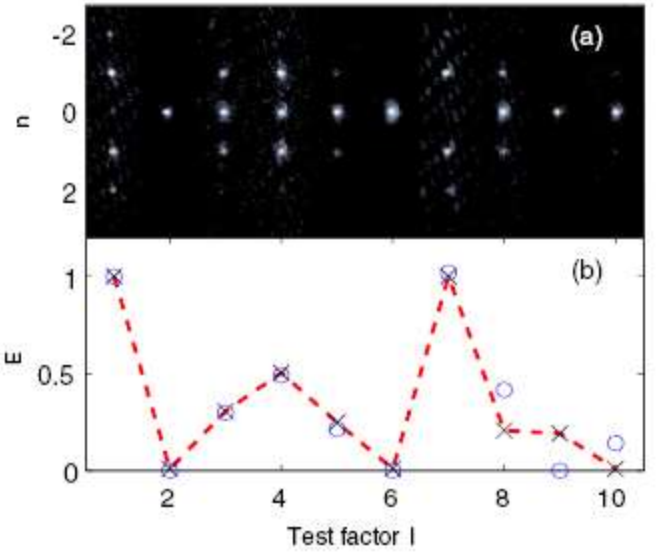
Outline

- Introduction
- Factoring with Gauss Sums: Ghost Factors
- 4 Classes of Trial Factors
- Truncation Parameter for Complete Suppression of Ghost Factors
- Scaling of Ghost Factors with Counting Function
  - Uniform distribution of fractional part
  - Non-uniform distribution of fractional part
- Optimal scaling law
- Summery of Results
- Friendly Ghost Factors?
- Conclusion

Introduction

- Gauss sums are prevalent in descriptions of various physical systems including optics and quantum mechanics.
- Can be used to factor large numbers, an important task for cryptography etc.
- Full vs. Truncated: Lower number of terms in sum better for experiments, but ghost factors appear.
- Want to know how ghost factors scale with number of summation terms, to find min terms necessary





Factoring with Gauss Sums

Complete Gauss Sum:

$$\mathcal{A}_N^{(\ell-1)}(\ell) = \frac{1}{\ell}\sum_{m=0}^{\ell-1} \exp\left(2\pi i m^2 \frac{N}{\ell}\right)$$

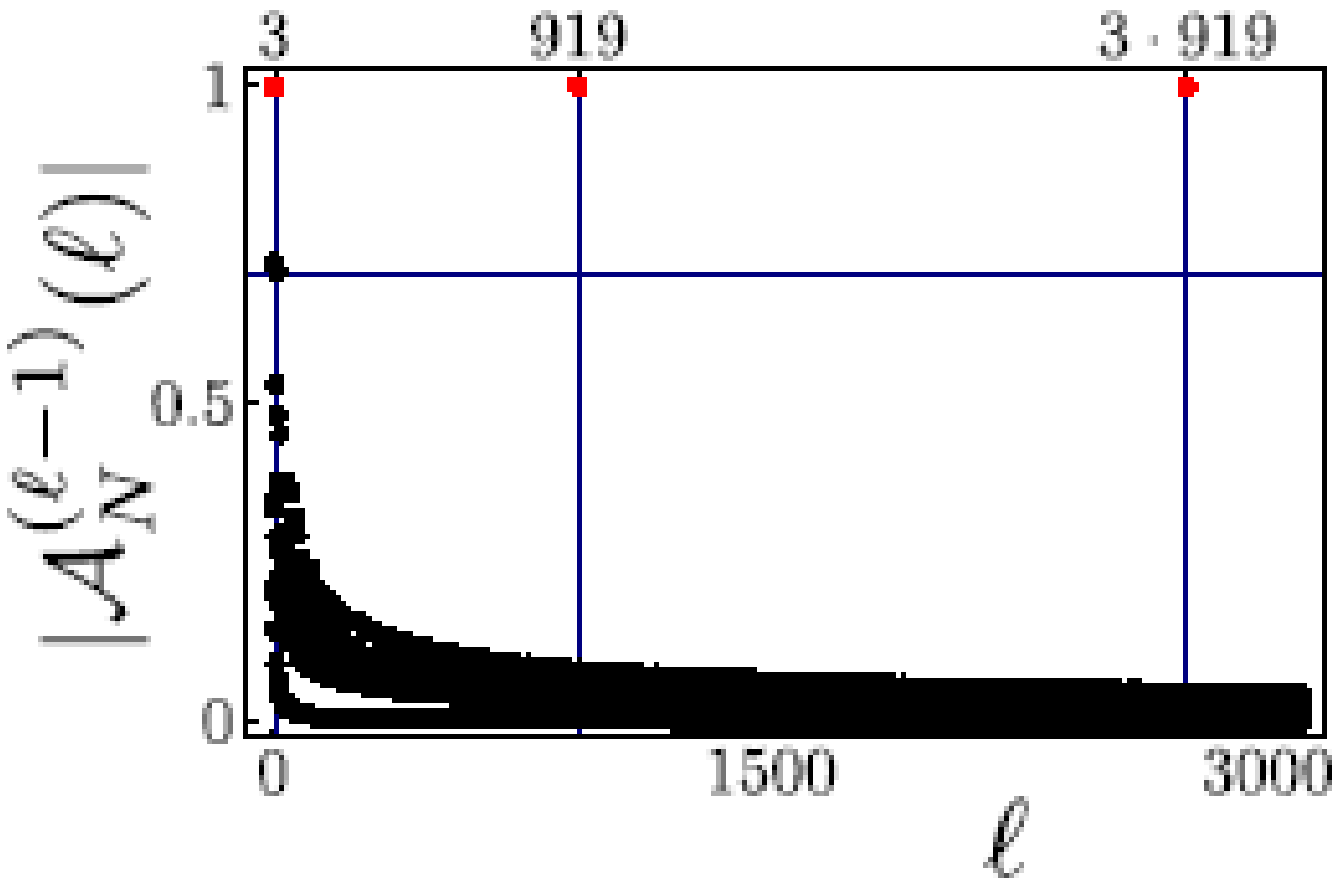
Total # of Terms to Sum:

$$\sum_{\ell=1}^{\sqrt{N}} \ell = \frac{1}{2}\sqrt{N}(\sqrt{N}-1) \approx \frac{1}{2}N$$

$l : 1 \rightarrow \lfloor \sqrt{N} \rfloor$

Example:

$N = 9\,624\,687$



Factoring with Gauss Sums

Truncated Gauss Sum:

$$\mathcal{A}_N^{(M)}(\ell) = \frac{1}{M+1} \sum_{m=0}^{M} \exp\left(2\pi i m^2 \frac{N}{\ell}\right)$$

Total # of Terms to Sum:

$$\sum_{\ell=1}^{\sqrt{N}} M = M\sqrt{N}$$

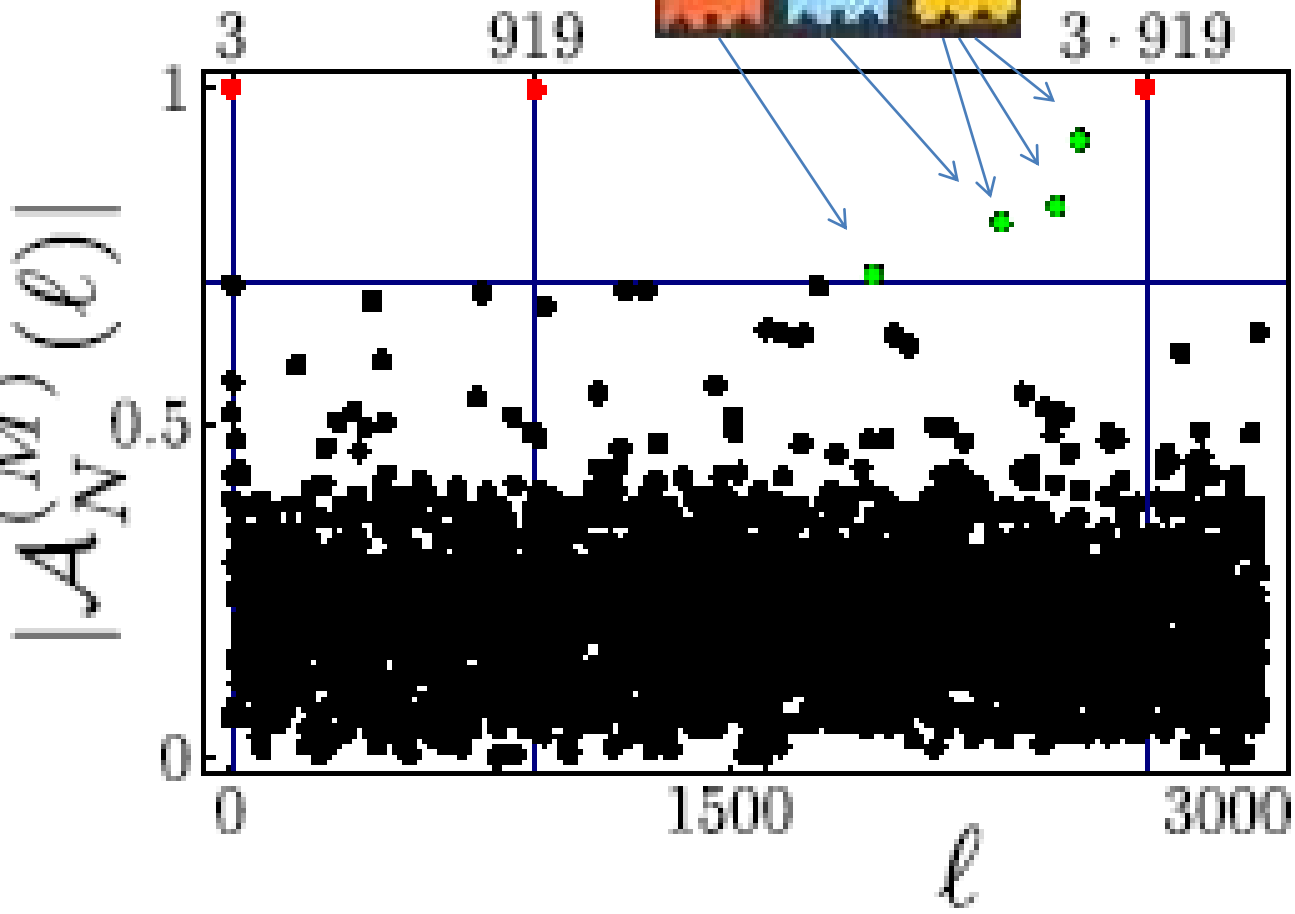
Ghosts!

$l : 1 \to \lfloor \sqrt{N} \rfloor$

Example:

$N = 9\,624\,687$

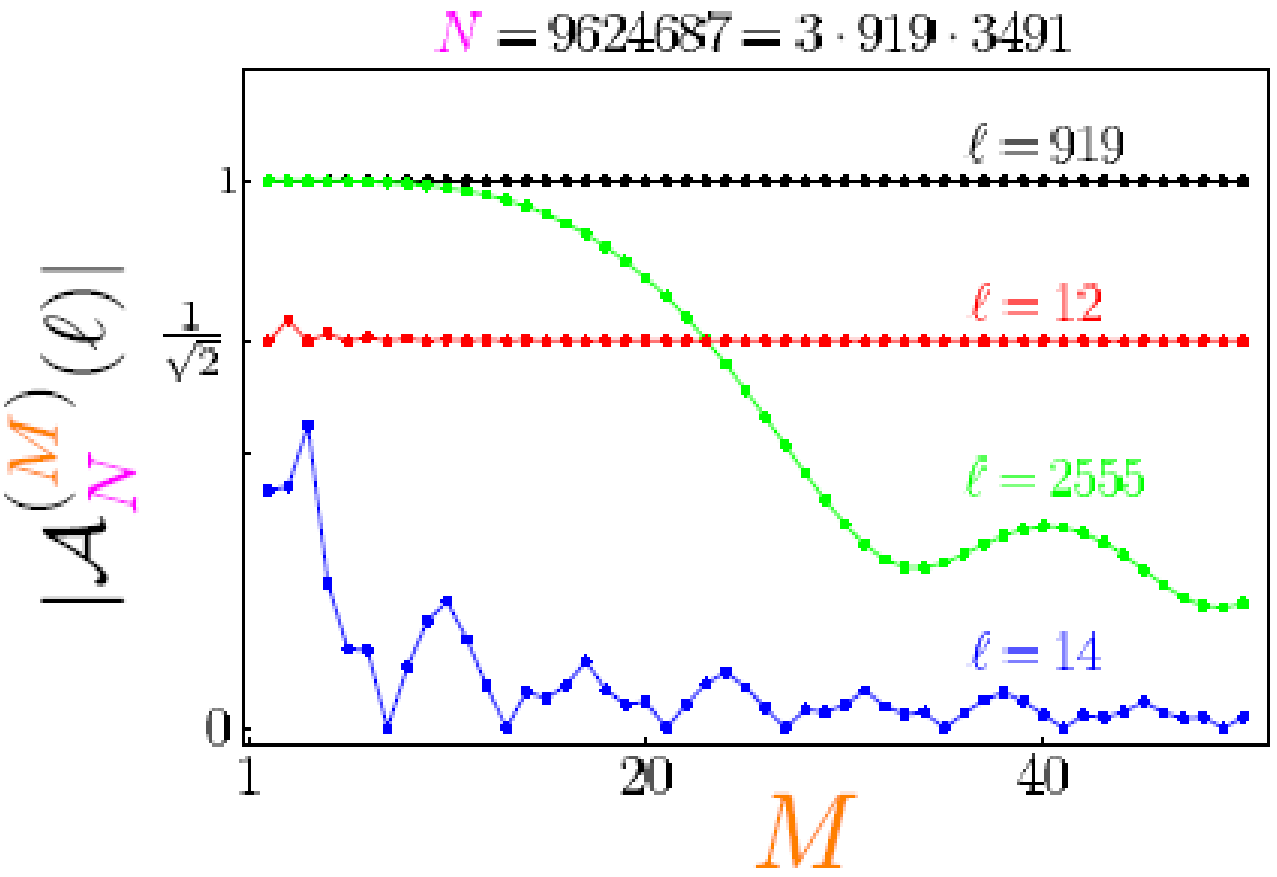
$M = \lfloor \ln N \rfloor = 16$



Classification of Trial Factors

1) Actual factors – constant value of 1 for all M
2) Non-factors that decay quickly with higher M
3) Ghost factors which require large M to decay
4) Threshold non-factors that do not decay with larger M

$$\frac{2N}{\ell}$$



1) Even integer
2) Close to odd integer
3) Close to even integer
4) Midpoint between even and odd integer

New Form for Gauss Sum

- Since 2N/l determines the class of trial factors, useful to re-write the Gauss sum

$$\frac{2N}{l} = 2k + \frac{p}{q}$$

Fractional part:

$$\rho(N,l) = \frac{2N}{l} - 2k = \frac{p}{q}$$

$$\rho(N,l) \in [-1,1]$$

Define normalized curlicue function:

$$s_M(\tau) \equiv \frac{1}{M+1} \sum_{m=0}^{M} \exp\left(\mathrm{i}\pi\, m^2 \tau\right)$$

$$\tau \in [-1,1]$$

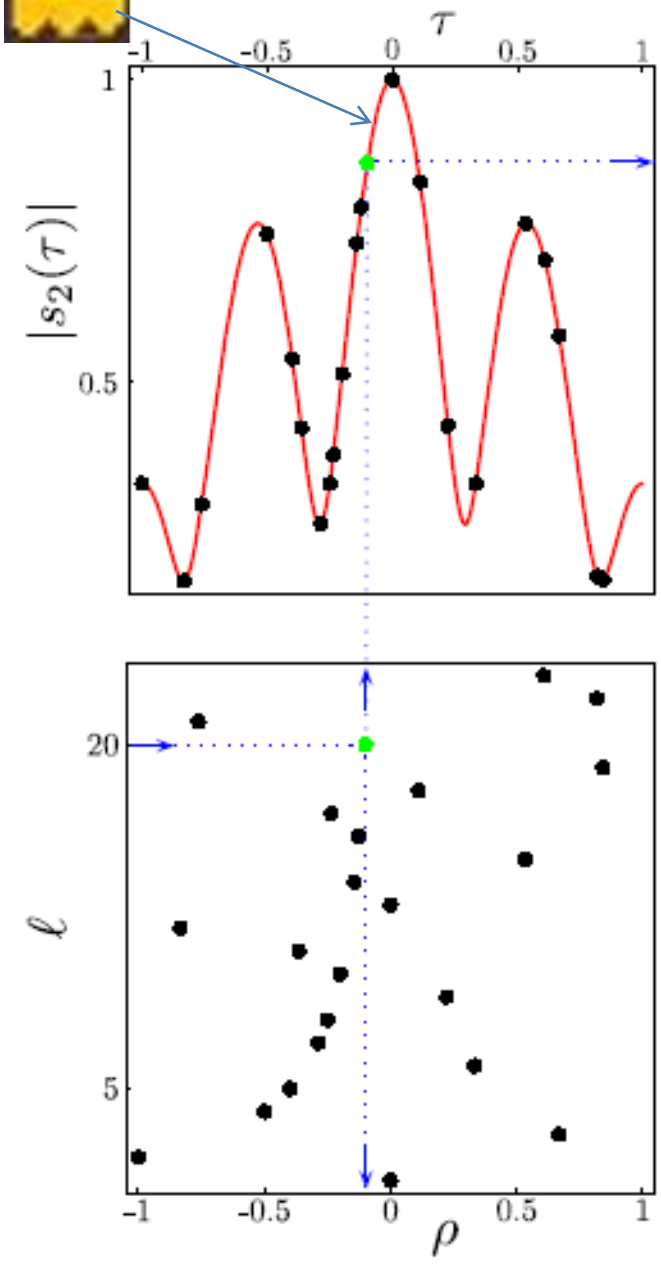
Can now write Gauss sum as:

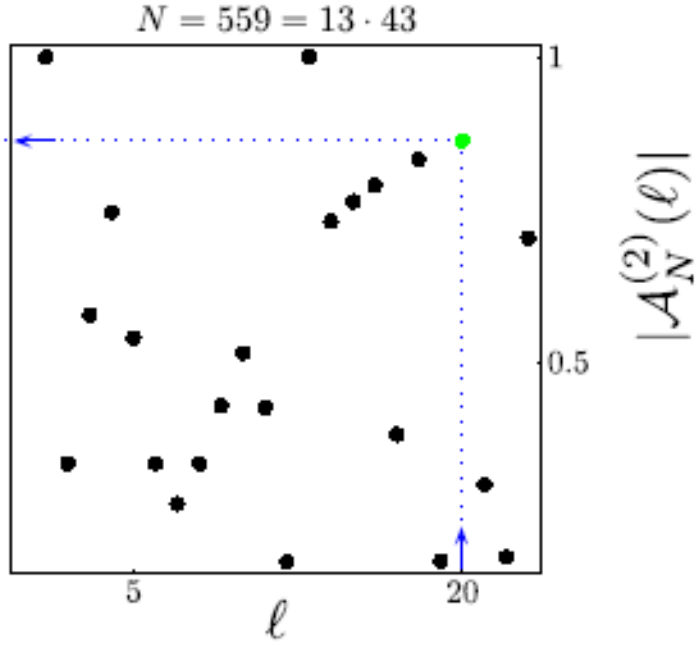
$$\mathcal{A}_N^{(M)}(\ell) = s_M\left(\rho(N,\ell)\right)$$

$\rho(N,l) = 0$ corresponds to factors, ρ close to 0, to ghost factors.

$|s_M|$ is even about tau because: $s_M(-\tau) = s_M^*(\tau)$

New Form of Gauss Sum





$$N = 559 = 13 \times 43$$

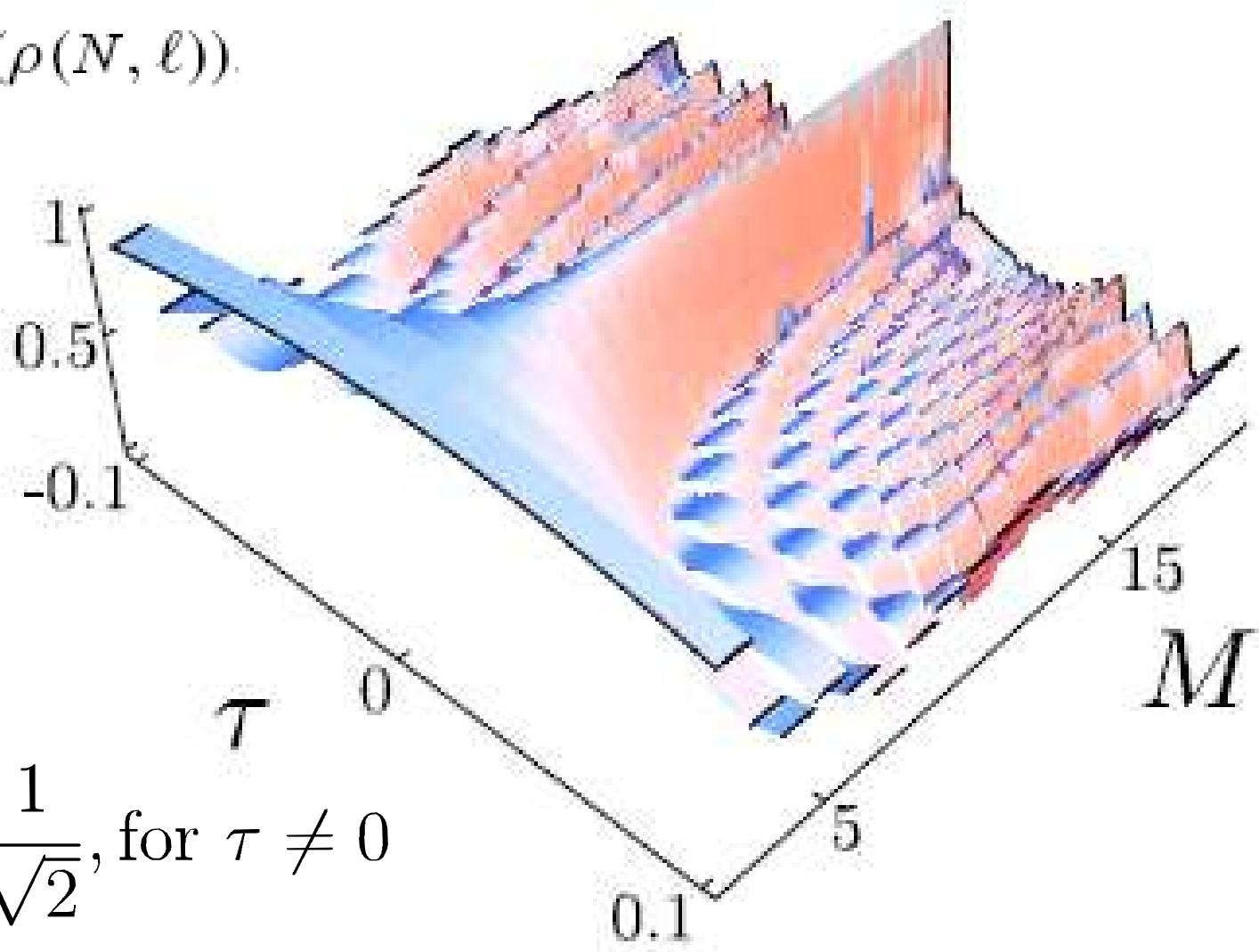
$$M = 2$$

$$\rho(N,l) = \frac{2N}{l} - 2k = \frac{p}{q}$$

$$\mathcal{A}_N^{(M)}(\ell) = s_M\left(\rho(N,\ell)\right)$$

New Form of Gauss Sum

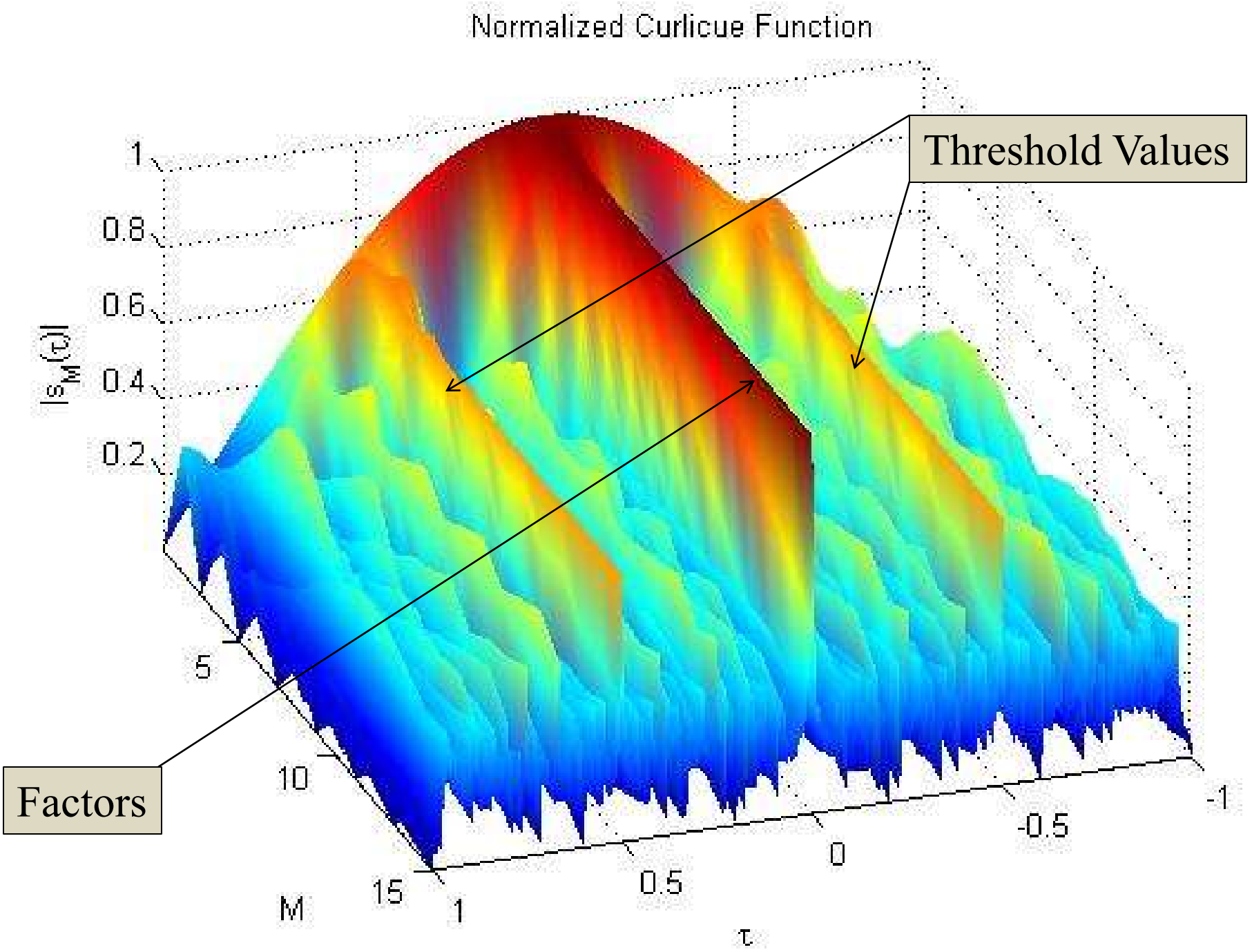
$$\mathcal{A}_N^{(M)}(\ell) = s_M\left(\rho(N,\ell)\right)$$



For large M:

$$|s_M(\tau)| \le \frac{1}{\sqrt{2}}, \text{for } \tau \neq 0$$

Define: of N is $\{l : |s_M(\rho(N,l))| \in (1/\sqrt{2}, 1)\}$


Normalized Curlicue Function
Threshold Values
Factors
$|s_M(\tau)|$
1
0.8
0.6
0.4
0.2
5
10
15
M
1
0.5
0
-0.5
-1
τ

Truncation Parameter

- Need to determine truncation parameter M_0 that will suppress all ghost factors below threshold
- Since ghost factors occur for very small values of τ we can replace summation with an approximate integral

$$s_M(\tau) \equiv \frac{1}{M+1} \sum_{m=0}^{M} \exp\left(\mathrm{i}\pi\, m^2 \tau\right)$$

Note

Substitute:

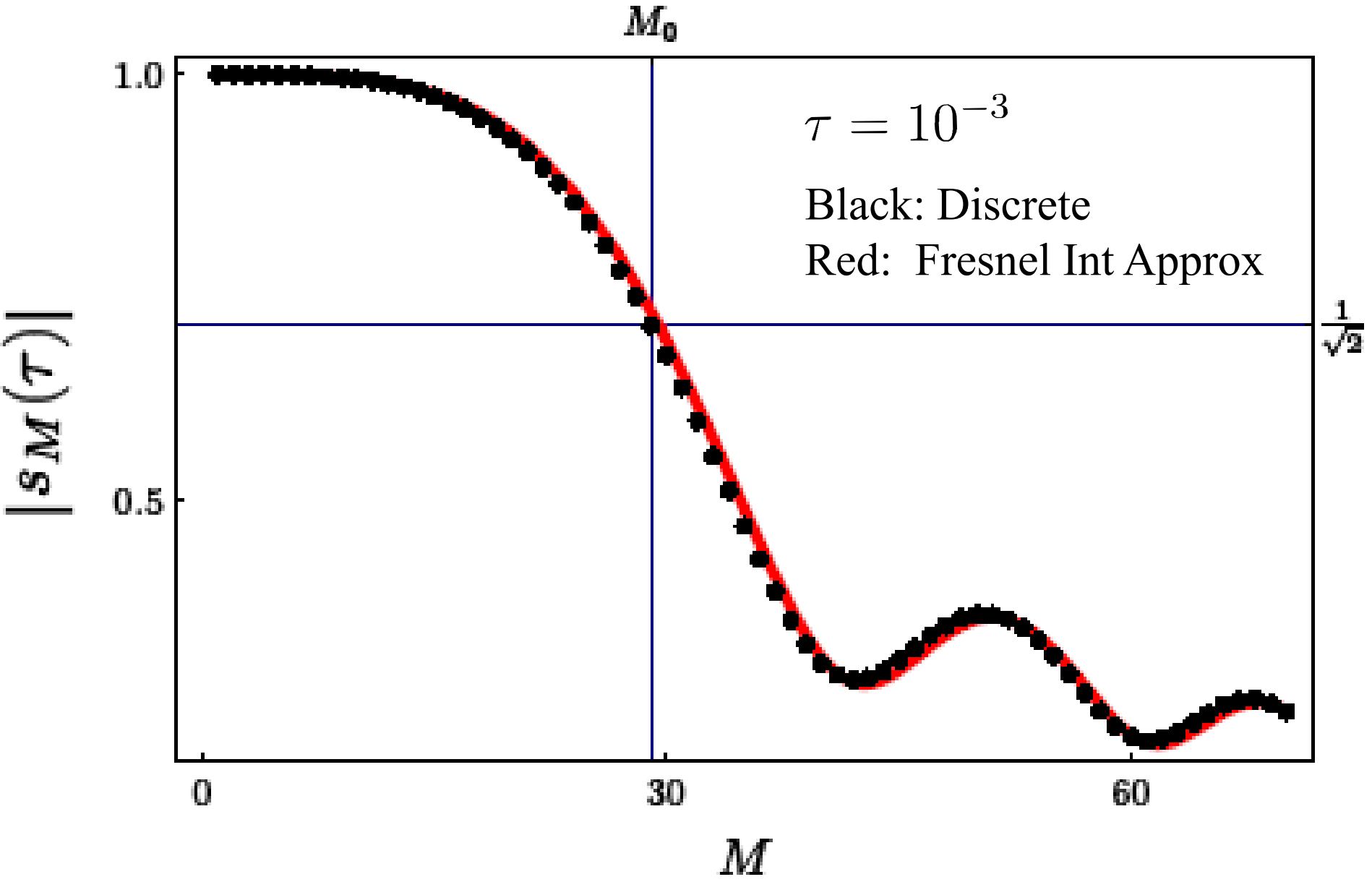
$$u = \sqrt{2\tau}\, m$$

$$du = \sqrt{2\tau}\, dm$$

$$s_M(\tau) \approx \frac{1}{M} \int_0^M \mathrm{d}u\ \exp\left(\mathrm{i}\,\pi m^2 \tau\right) = \frac{F(M\sqrt{2\tau})}{M\sqrt{2\tau}}$$

Fresnel integral: $F(x) = \int_0^x \mathrm{d}u\ \exp\left(\mathrm{i}\,\frac{\pi}{2}u^2\right)$

Truncation Parameter



Truncation Parameter

$$\mathcal{A}_N^{(M)}(\ell) = s_M\left(\rho(N,\ell)\right)$$

$$s_M(\tau) \approx \frac{1}{M}\int_0^M \mathrm{d}u\ \exp\left(\mathrm{i}\,\pi m^2\tau\right) = \frac{F(M\sqrt{2\tau})}{M\sqrt{2\tau}}$$

$\alpha(\xi)$ sol of $\dfrac{|F(\alpha)|}{\alpha} = \xi$

$$\alpha(\xi) = M_0\sqrt{2\tau}.$$

ℓ is varied within the interval $[1, \sqrt{N}]$

$$\rho(N,l) = \frac{2N}{l} - 2k = \frac{p}{q}$$

Minimum value at largest l:

$$\rho_{\min}(N) \sim \frac{2}{\sqrt{N}}$$

$$M_0 \approx \frac{\alpha(\xi)}{\sqrt{2\rho_{\min}(N)}} \approx \frac{\alpha(\xi)}{2}\sqrt[4]{N}.$$

Natural threshold:

$\xi = 1/\sqrt{2}$

$\alpha(\xi) \approx 1.318$ (numeric)

$$M_0 \approx 0.659\sqrt[4]{N}$$

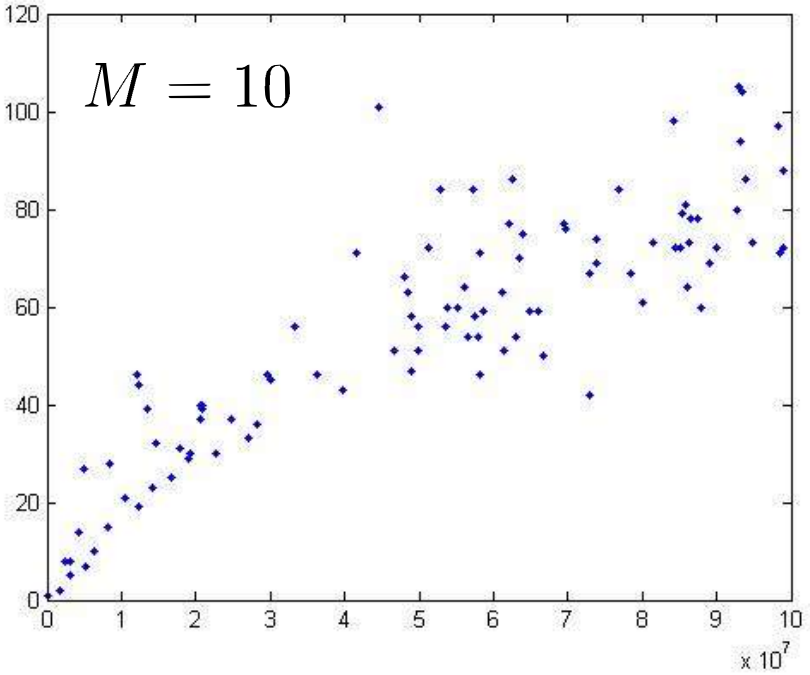
Scaling unchanged by threshold value – only pre-factor changes!

Ghost Factor Counting

- Have found *sufficient* condition to suppress ghosts
- Now, want to find *necessary* condition

Ghost factor counting function:

$$g(N, M) \equiv \#\left\{\ell = 1, \ldots, \lfloor\sqrt{N}\rfloor \text{with } \frac{1}{\sqrt{2}} < |\mathcal{A}_N^{(M)}(\ell)| < 1\right\}$$



Ghost Factor Counting

Ghost factors occur in region of s: $[-\tau_0, \tau_0]$

From Fresnel: $\alpha(\xi) = M_0\sqrt{2\tau}.$ $\Rightarrow$ $\tau_0 = \tau_0(M) \approx \dfrac{\alpha^2}{2M^2}$

Total width of s with values larger than $1/\sqrt{2}$: $2\tau_0 \approx \dfrac{\alpha^2}{M^2}$

Now want to relate g(N.M) to width via distribution of τ for a given N

2 Cases: Uniform Distribution
Non-uniform Distribution

Ghost Factor Counting

Uniform Distribution

Remember: $\tau \in [-1, 1]$

So # of ghosts directly proportional to width:

$$\frac{g(N, M)}{\sqrt{N}} \approx \frac{2\tau_0}{2};$$

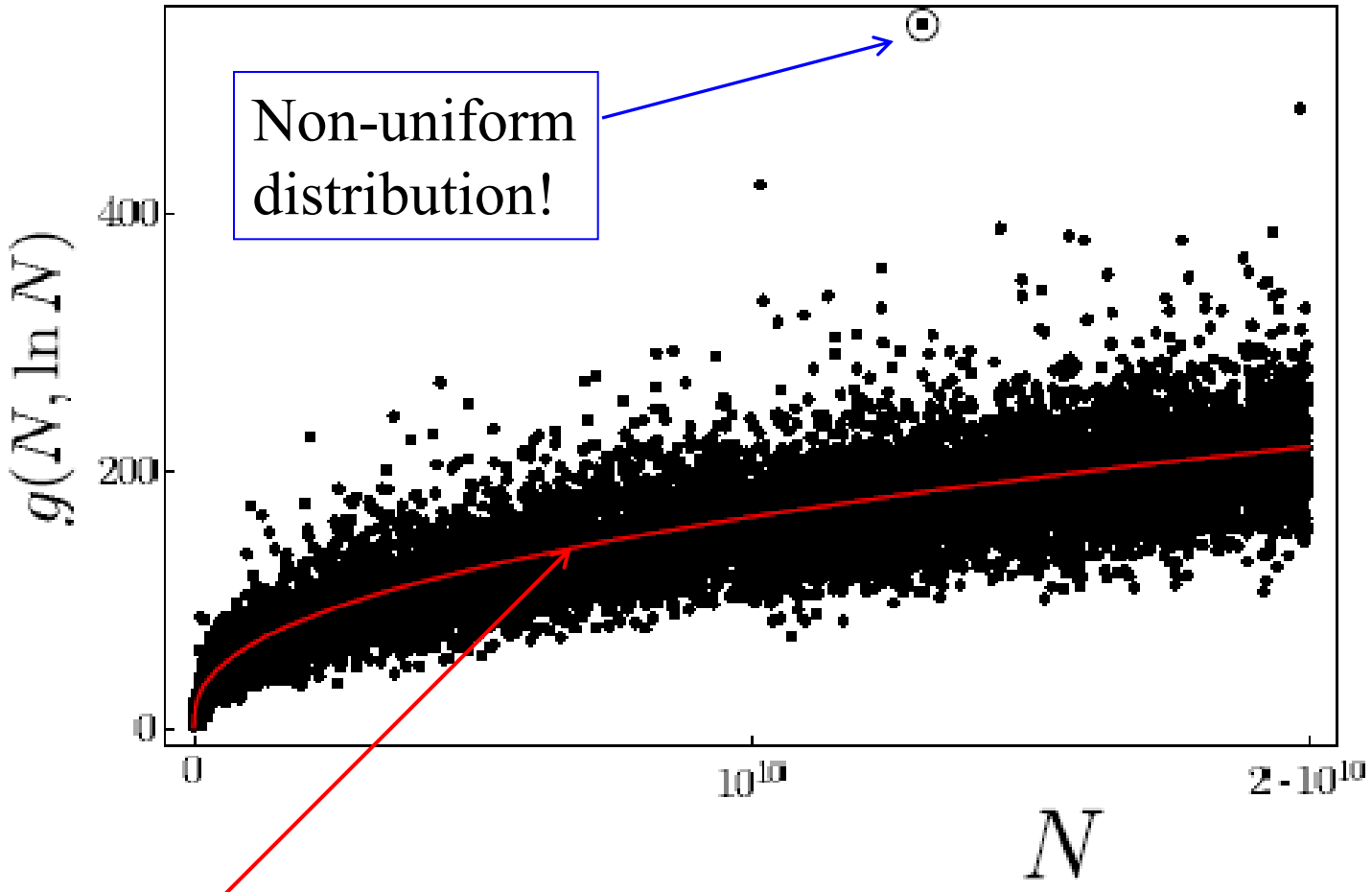
$$\tau_0 = \tau_0(M) \approx \frac{\alpha^2}{2M^2} \quad \Rightarrow \quad g(N, M) \approx \frac{1}{2}\left(\frac{\alpha}{M}\right)^2 \sqrt{N}$$

Inverse power law

Example: M = ln N:

$$g(N, \ln N) \approx \frac{1}{2}\left(\frac{\alpha}{\ln N}\right)^2 \sqrt{N}$$

Ghost Factor Counting



10,000 random numbers from

$[1, 2\text{x}10^{10}]$

M = ln N

$$g(N, \ln N) \approx \frac{1}{2}\left(\frac{\alpha}{\ln N}\right)^2 \sqrt{N}$$

Ghost Factor Counting

Non-uniform Distribution

Happens when N has few divisors, but nearby number N+k has many.

$$|k| << N$$

Example: $N = 13\,064\,029\,441 = 21647 \times 603\,503$

$$N' = N - 1 = 2^8 \times 3 \times 5 \times 11 \times 17 \times 23 \times 113$$

Let us consider ℓ' which is a divisor of $N' = N + k$ but not of N.

$$\rho(N, l) = \frac{2N}{l} - 2k = \frac{p}{q}$$

if $\ell' > 2k$ $\longrightarrow$ $\rho(N, l') = \left[\frac{2N'}{l'} - 2k\right] - \frac{2k}{l'} = -\frac{2k}{l'}$

$N = N' + k$

Ghost Factor Counting

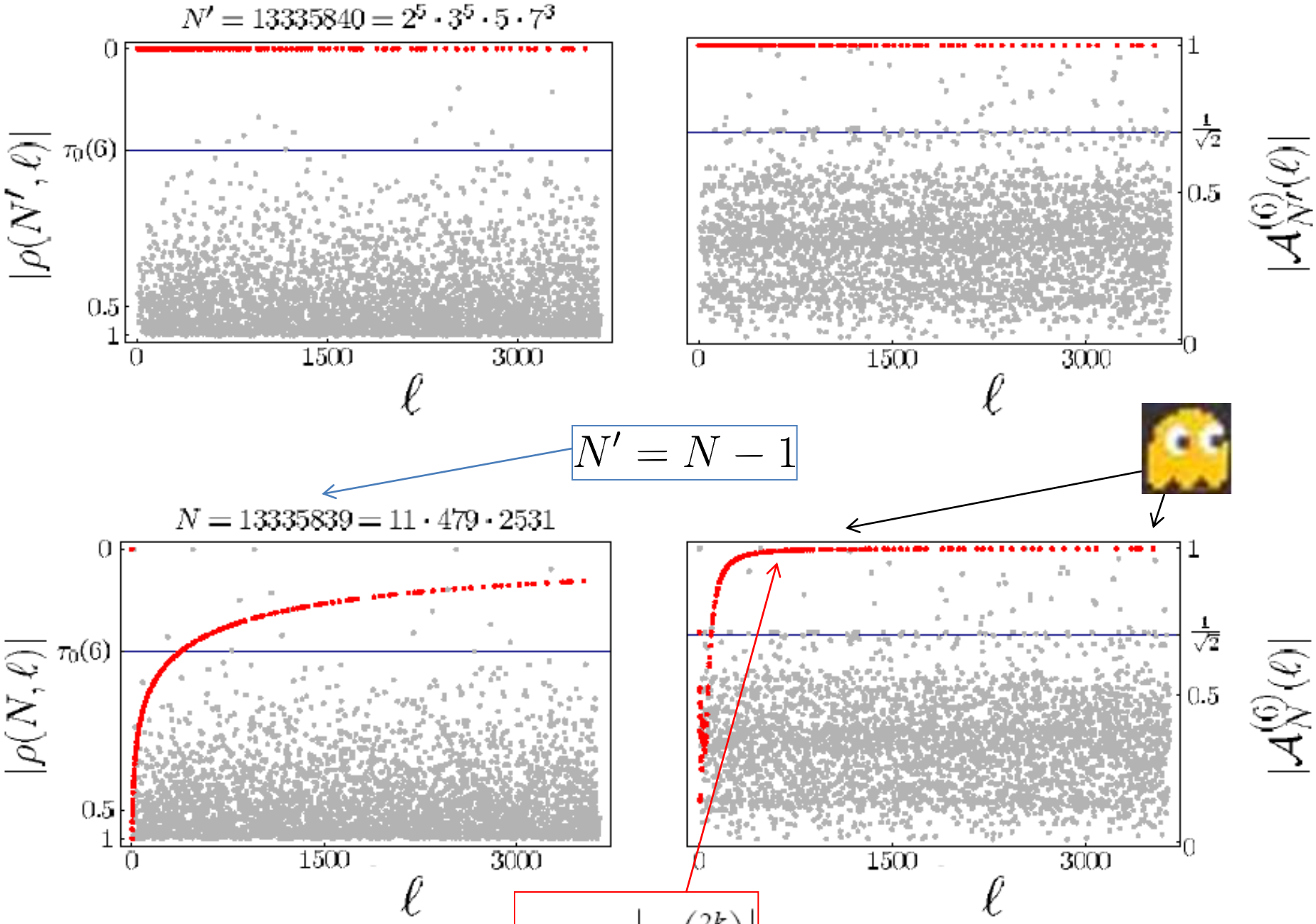
Non-uniform Distribution

l' data points (factors of N') in interference pattern of N follow curve:

$$\gamma_k^{(M)}(l) \equiv \left| s_M\left(\frac{2k}{\ell}\right) \right|$$

Tends to 0 for large l', so becomes ghost factor:

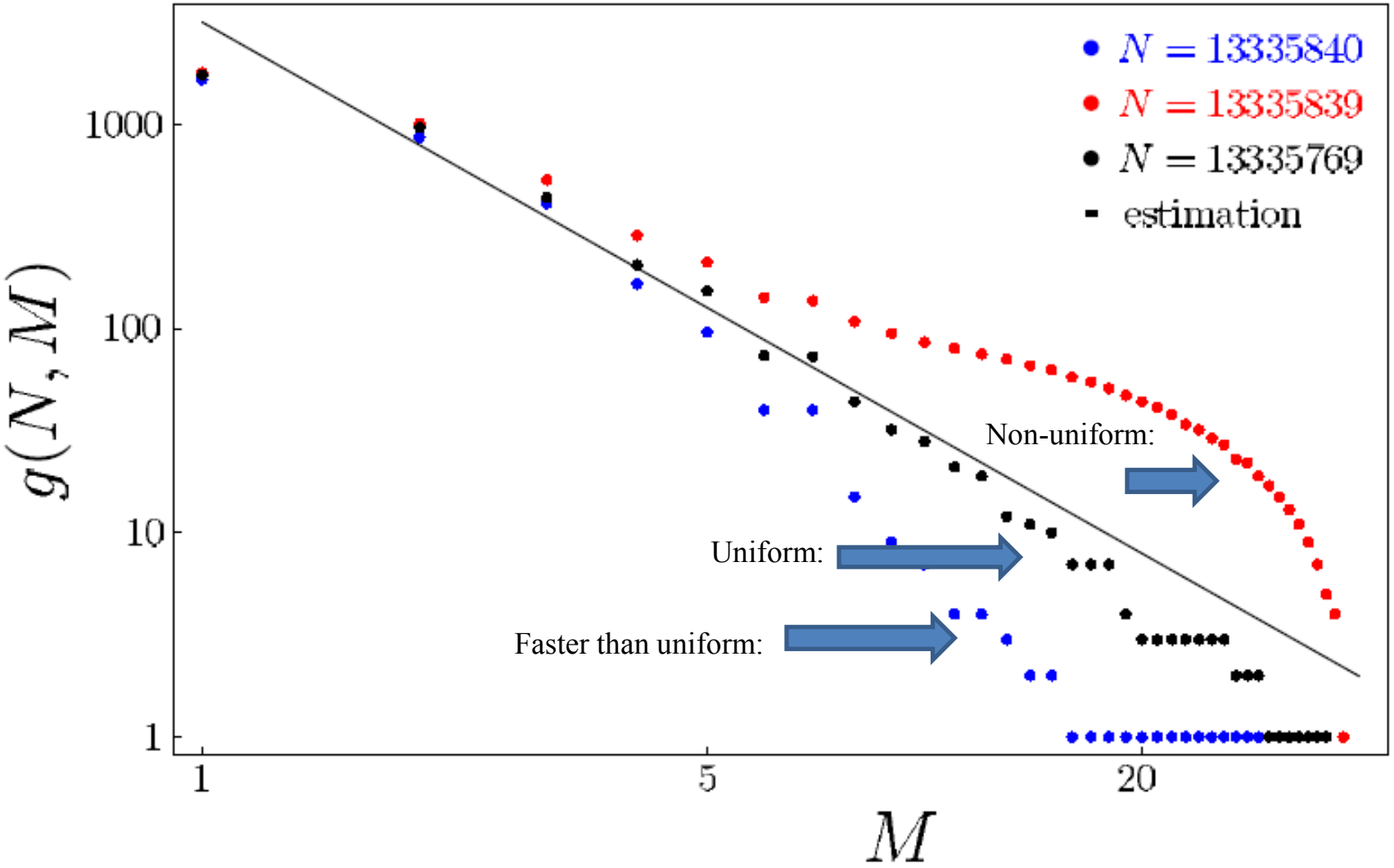
$$\mathcal{A}_N^{(M)}(\ell) = s_M\left(\rho(N,\ell)\right) \qquad s_M(0) = 1$$


$N' = 13335840 = 2^5 \cdot 3^5 \cdot 5 \cdot 7^3$
$|\rho(N', \ell)|$
$\tau_0(6)$
ℓ
$|A^{(6)}_{N'}(\ell)|$
$\frac{1}{\sqrt{2}}$
$N' = N - 1$
$N = 13335839 = 11 \cdot 479 \cdot 2531$
$|\rho(N, \ell)|$
$|A^{(6)}_{N}(\ell)|$
$\gamma_k^{(M)}(l) \equiv \left| s_M\left(\frac{2k}{\ell}\right) \right|$

Optimality of 4th root Law

Remember for uniform distribution we have:

$$g(N, M) \approx \frac{1}{2}\left(\frac{\alpha}{M}\right)^2 \sqrt{N}$$



Optimality of 4th root Law

Idea! Since g(N.M) decays fast at first, why not allow K ghosts:

$$g(N, M) \approx \frac{1}{2}\left(\frac{\alpha}{M}\right)^2 \sqrt{N} = K$$

$$M_K \approx \frac{\alpha}{\sqrt{2K}} \sqrt[4]{N}$$

Only used uniform distribution, non-uniform cases, Mk may even be larger!

Compare with: $$M_0 \approx \frac{\alpha(\xi)}{\sqrt{2\rho_{\min}(N)}} \approx \frac{\alpha(\xi)}{2} \sqrt[4]{N}$$

So, even if we tolerate K ghosts, we cannot do better then a $\sqrt[4]{N}$ scaling for required M

So, 4th root scaling is both sufficient and necessary!

Results

To eliminate all ghost factors for ANY N, need: $M_0 \sim \sqrt[4]{N}$

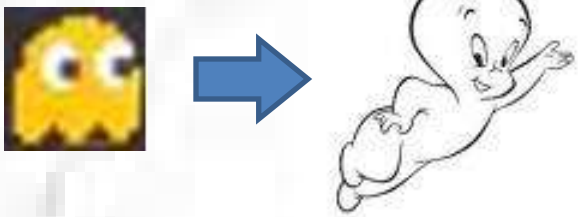
Number of terms to sum: $\sum_{\ell=1}^{\sqrt{N}} M = M\sqrt{N} \sim N^{3/4}$

Full Gauss sum requires $\sim N$ terms, so we save a bit

[For some N, need less M … what percentages?]

Are ghost factors really that bad? ……

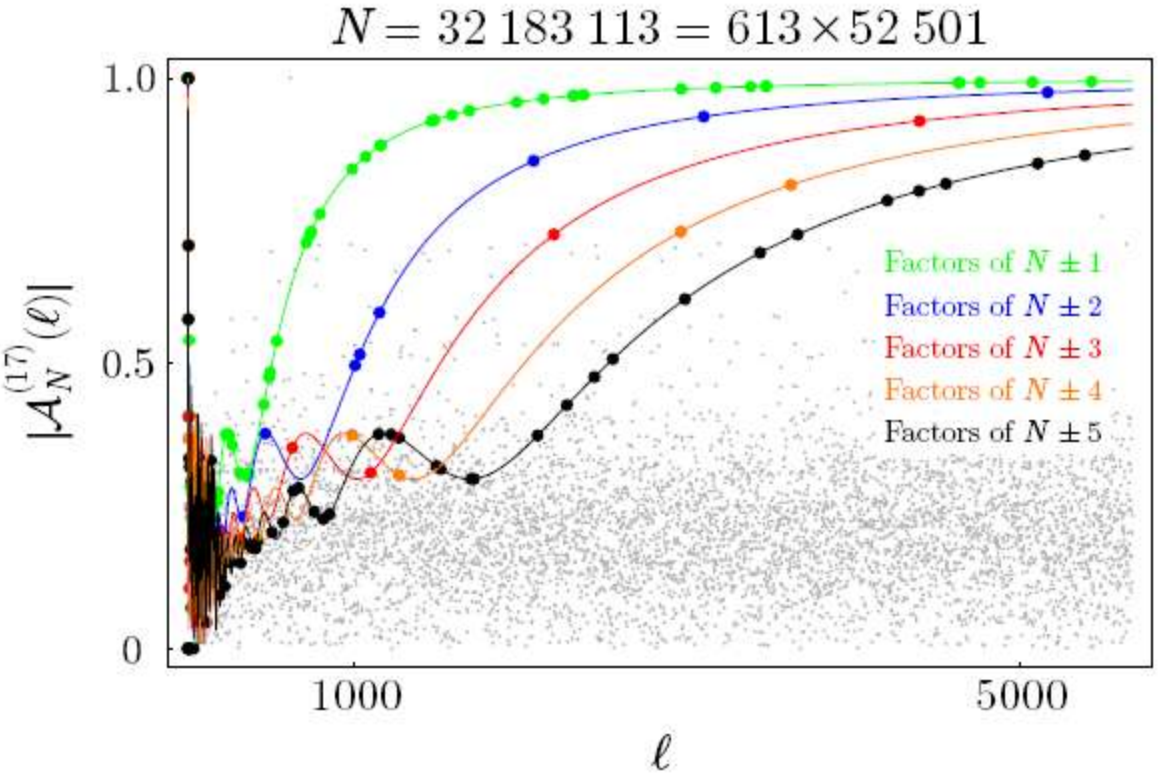
Results: Friendly Ghost Factors



We now know that ghost factors are actually real factors of a nearby number N + k

May be possible to exploit this fact to factor numbers more efficiently

$$l' \text{ of } N \pm k \text{ are on the curve } \gamma_k^{(M)}(l)$$



M=17 not good to suppress ghosts, but we can fit them to curves of factors of different N-primes

Can possibly come up with new scheme taking advantage of this…(?)

Conclusion

- Ghost factors are factors of neighboring numbers
- Using 4^{th} root law, can eliminate all ghost factors

Outlook

- Ghost factors may be helpful in forming new algorithms to factor numbers.
- Some experiments (like BEC diffraction) seem to compute higher power Gauss sums (like cubic) which can help the scaling for M0.