多重スリット干渉を利用したガウス和計算による素因数分解

岩下・小林研究室　1170036　乙成　隆仁

1.　研究背景・目的

近年、コンピュータの回路等の部品の小型化が進み、電子機器の映像や処理速度等の性能が急激な進歩を遂げている。しかし、今後回路等の部品の小型化が物理的に困難になり、電子機器の性能の向上が難しくなることが予想されている。その中で、現在のコンピュータとは全く異なる方法で計算を行うために可視光線あるいはその他の光線に関連した物理現象により情報処理を実現する光計算がある。光計算の中でも、本研究では、光学的干渉における、明線の条件に注目する。光路差δが波長λの整数倍、つまり、光路差δを波長λで割った値が整数になったときに干渉の明線が現れるが、逆に言えば、明線を測定できればδがλで割り切れるか調べることができる。この割り算は素因数分解に応用できる。素因数分解を様々なアルゴリズムが考えられてはいるが基本的に素因数の組み合わせの計算を逐次行なうため、計算量が膨大になり、計算に多くの時間を要してしまう。そこで、本研究では、多数の波長を持つ光波の光学的干渉という物理現象を用いて、素因数分解を並列的に効率よく計算できるのではないかと考え研究を行った。

2.　多重スリット干渉を利用したガウス和計算

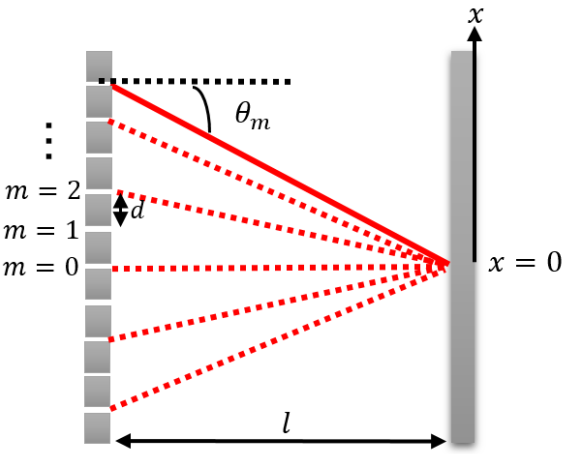

図 1　多重スリット干渉概要

多重スリット干渉について概要を図 1 に示す。M番目のスリットからスクリーン上の原点x = 0までの長さl_mを求め、x = 0での干渉光強度を計算する。

光強度をIとし、m = 0からM番目のスリットの和をとると

$$I = \left| \sum_{m=0}^{M} A \exp\left(-2\pi \ im^2 \frac{d^2}{2l\lambda} \right) \right|^2 \qquad (1)$$

と表せる。ここで、Aは光波の振幅、 dはスリットの間隔、lはスリットとスクリーンの距離、λは波長である。(1)式のように位相項に和の変数 m の 2 乗が含まれた式は「ガウス和」と呼ばれる。ガウス和Iは$\frac{d^2}{2l\lambda}$が整数となるとき最大値をとるため、多数のλを用いることで並列に割り算が計算できる。

3.　ガウス和計算による素因数分解

一般的にガウス和hは以下で定義される。

$$h(Z, M, 2, L) = \left| \frac{1}{M+1} \sum_{m=0}^{M} \exp(2\pi i m^2 \frac{Z}{L}) \right| \qquad (2)$$

ここで、素因数分解したい数をZ、Zの素因数の候補Lとする。(2)の計算例を図 2 に示す。$Z = 40001$、$M = 20$のとき、素因数の候補Lを 1～$\sqrt{40001}$まで変化させたときのガウス和の値の変化である。LがZの素因数であれば$h = 1$となるが、図 2 より40001の素因数 13、17、181 で$h = 1$となり、ガウス和を用いて素因数分解を行うことが可能となる。

4.　Ghost Factor(GF)

測定を進めていく中でガウス和の値が$h = 1$となるLの値の測定を行いたいが、なかにはガウス和hの値が 1 に近いLの値が存在する。本研究では、このhが 1 に近いときのLを Ghost Factor と呼ぶ。図 2 の点線は Ghost Factor を表している。測定を行うときは Ghost Factor の値をできるだけ小さくする必要がある。

5.　まとめ

多重スリット干渉を利用したガウス和計算による素因数分解は可能であると考える。

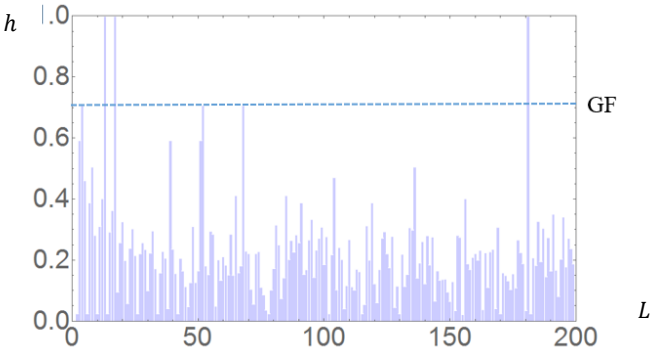

図 2　Z = 40001のときのガウス和計算例