量子コンピューティング

スタディー・ガイド

（構成中）

作　　成：松原　　望
作成補助：森本　栄一

2024/1/25

＜予定内容*＞

確率論基礎レベルを前提とします。

「量子コンピュータ」とは直接のかかわりはありません。

0．量子力学と量子論

　　付：ボーア対アインスタイン（コペンハーゲン解釈）

1．重ね合わせの原理のベイズ確率論**

　　付：Dirac の「ブラ」と「ケット」

2．Q ビットと量子状態

3．多重 Q ビット系と「量子もつれ」

　　付：確率論で量子もつれ早わかり

4．量子ゲートと量子回路

　　付：制御 NOT ゲート、アダマールゲート、ベル回路

5．量子コンピューティング入門

　　付：ドイッチェ・アルゴリズム、サイモン検索

6．応用 I　RSA 暗号解読、ショア・アルゴリズム、量子フーリエ変換

7．応用 II　化学量子コンピューテイング、量子誤り訂正、量子機械学習

8．量子データ分析 Quantum Data Analysis, QDA©への招待

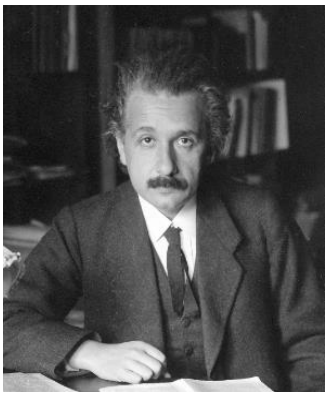
*おおむね 2024 年 2 月末より、各月末 1 節宛て登載予定

**参照『入門　確率過程』『入門　ベイズ統計学改訂版』東京図書

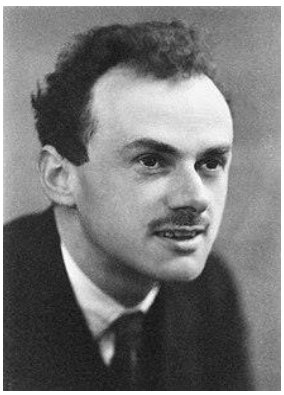
「コペンハーゲン解釈」にかかわった量子力学の創設者

Niels Bohr

Werner Heisenberg



Albert Einstein



Paul Dirac

以下のページは現在作業中で未完です。

RSA 暗号（公開鍵暗号）

① 私は大きい素数p, qを選び$N = pq$とする。

② 私は暗号化鍵$K < N$を

— $K, (p-1)(q-1)$が互いに素（1 以外の公約数はない）

ように選び、K, Nを新たに送る（秘案でよくてよいー公開鍵）

③ あなたはVm（デジタル化）を私に、鍵Kを用いてメッセージ

$$c \equiv m^k \ mod\ N$$

として送る。

④ 私は次の準備をしておく。解読のため整数d

$$Kd \equiv 1 \mod (p-1)(q-1)$$

のように選ぶ。これにはp, qを知る必要がある。

⑤ 私は

$$m \equiv c^d \ mod\ N$$

として、あなたが送ったmを解読できる。

シェアの因数分解アルゴリズム

① ランダムに$a < N$を選ぶ。Nがaで割り切れるようなaがNの約数となる。
（実際にはほとんどありえない）。そうでない場合は次へ進む

② $1 \equiv a^r \ mod\ N$となる最小のrを見出せ。すなわち$a^r - 1$がNで割り切れるrを探索する。

③ もしrが偶数なら、④へ進む。奇数なら①へ戻り、aを選び出す。

④ $S \equiv a^{r/2} \ mod\ N$を計算する。（③によりこれは可能）

⑤ 素数*

$$p = GCD(s-1, N), q = GCD(s+1, N)$$

を求めれば

$$N = pq$$

を得る。

*GCD：最大公約数

量子フーリエ解析（図参照）

① 変換 $|\psi_0\rangle \rightarrow |\psi_1\rangle$

$$|\psi_1\rangle = H^{\otimes n}|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle|0\rangle_n$$

上レジスタ　下レジスタ

$\sum$ ：$0 \sim 2^n - 1$（以下同）

②変換 $|\psi_1\rangle \rightarrow |\psi_2\rangle$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle|f(x)\rangle$$

上レジスタ　下レジスタ

ここで、入力は

$$f(x) \equiv a^x \ mod\ N$$

注）$2^n = N$

③ 上レジスタに量子フーリエ変換 QFT を演算

$$U_{QFT}|x\rangle = \frac{1}{\sqrt{N}}\sum_y U_F(x,y)|y\rangle \quad (def.)$$

ここで、U_Fはサンプリング関数で、各kに対し

$$U_F(j,k) = \cos(2\pi jk/N),\ \ j = 1,2,\cdots,N-1$$

で定義される。しかして

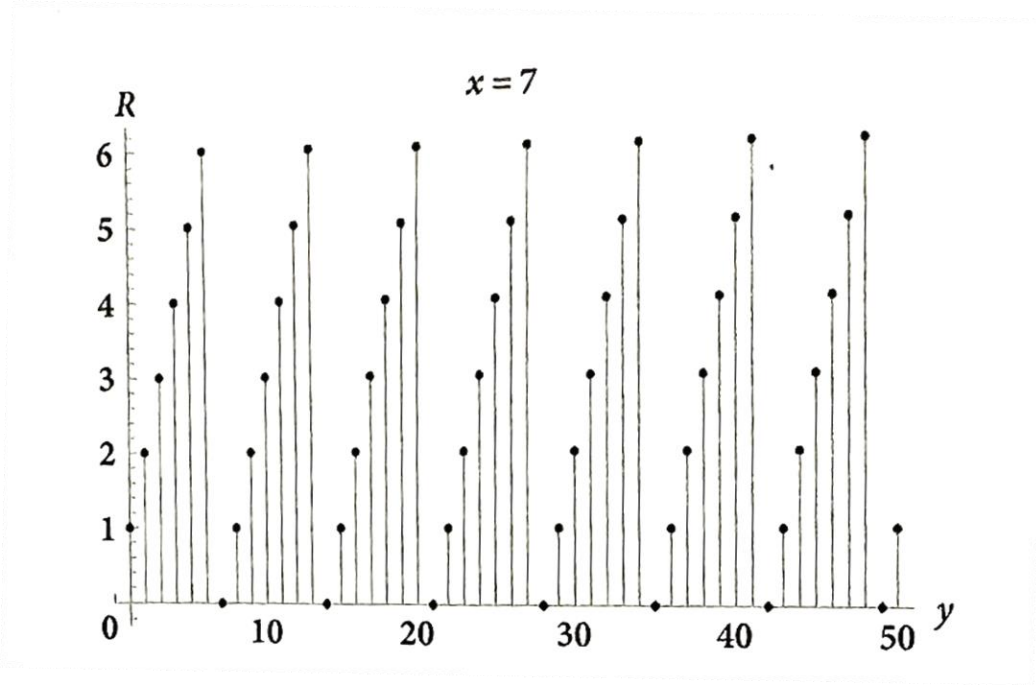
$$|\psi_3\rangle = U_{QFT}|\psi_2\rangle$$

④ 観測装置

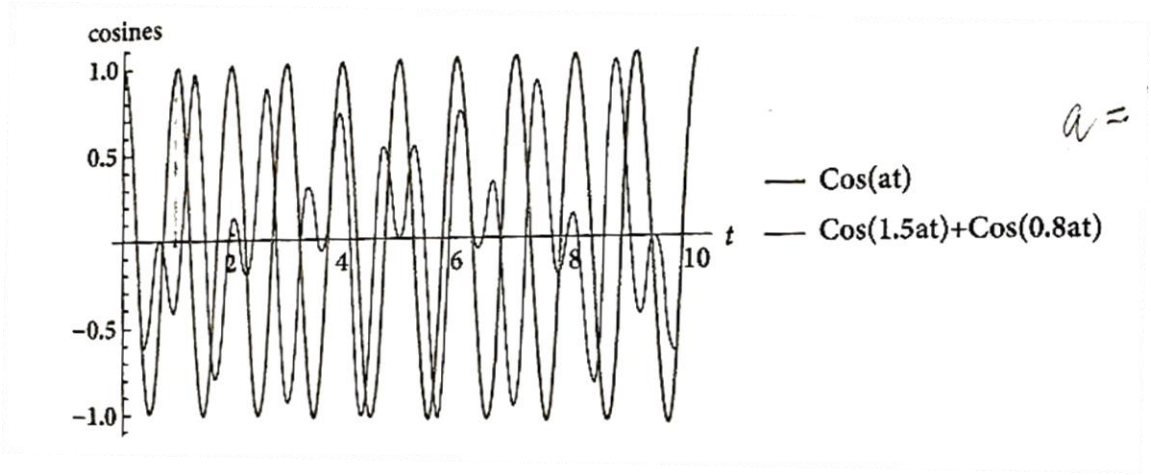
上レジスタ―の最大値$y = N/r$から

$$r = N/y$$

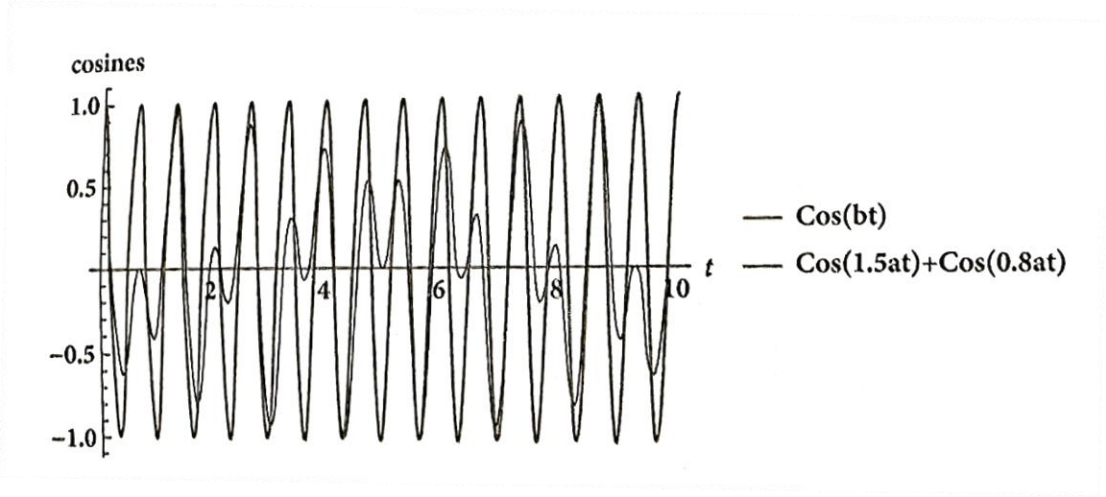
でrを特定。



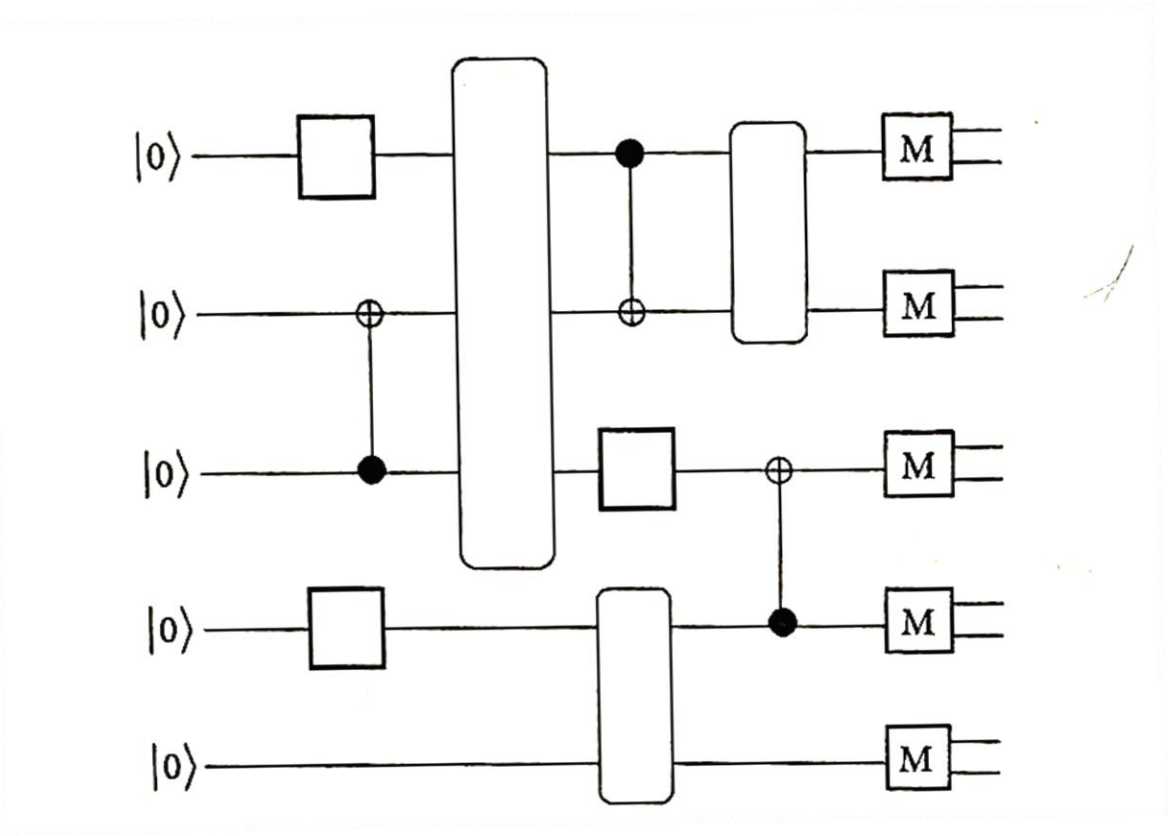
① 剰余計算から得られる周期が、素因数の発見に通じる



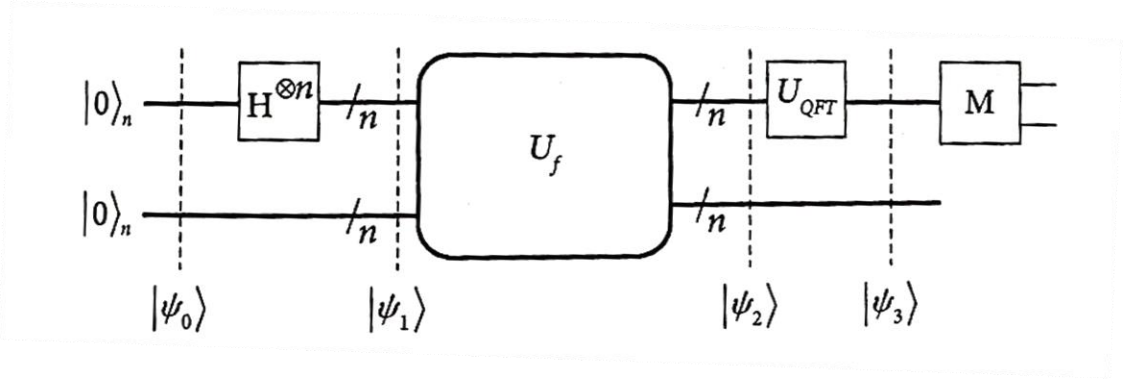
② 周期を発見できていない例（ cos at ）



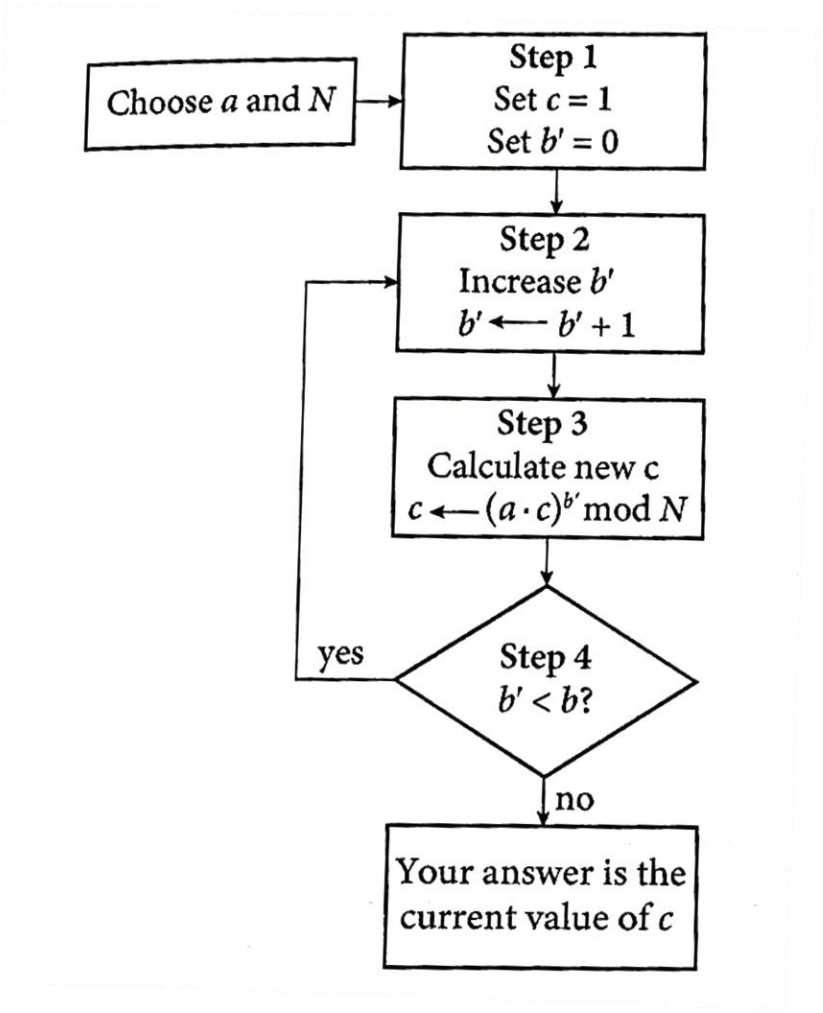
③ 周期を発見できた例 （cos at ）



④ 量子ゲートの例



⑤ n 重 qbit でフーリエ解析を行う量子回路



⑥ 量子回路で Shor アルゴリズムを実装