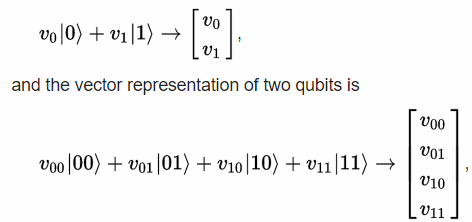
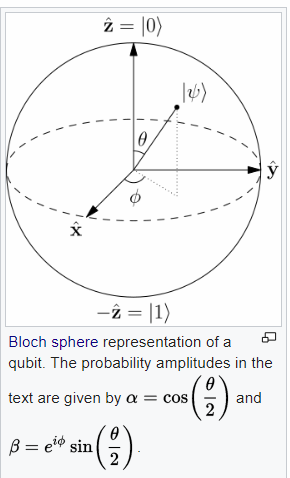
Bra ket, also called dirac notation is convenient notation used, to represent Qubit state,

**Write:**



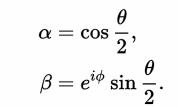
Where one ket or zero ket is a base state.

**Example:** one over square root of two: 1/sqrt2 \* a\*|0> b\*|1> ; plane(not bloh sphere yet) for real a,b on blackboard, add that a,b could be complex, so we couldn’t show every state on simple plane. For this reason, we could illustrate quntum state of qubit on bloh sphere.



Have to follow this formula:





**Write: inner product <a|b>**

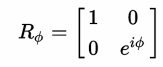
**Write: outer product |a><b|**

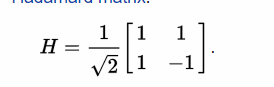
Photon could represent qubit, **example:** bloh sphere with linear polarity as theta. circular as phi. by linear and circular polarization. referred as elliptical polarization.

outer product

Gates:

NOT (pauli x gate) , **example**

Controled rotation gate. **Example:**  it adds angle phi to base vector one.

Hadamard gate  here is special cases that are worth to mention 0> = 0>+1>/sqrt2 , 1> = 0> - 1>/sqrt2, H(H)

preservationn inner product, reversible

We couldn’t use any kind of matrix, because quantum rules limited us that transformation have to preserve norm. so the matrices which we are using, are unitary matrices which could be used to represent realizable transformation.

The matrices looks quiet easy, but of course not every simple matrix could be implemented as quantum gate. It should preserve norm, it is just a simple quantum rule Unitary matrices meet the requirement.

Here is definition: U is an unitary matrix if: UU\* = U\*U = I. I will explain it. Hermitian conjugate identity matrix.

It could be proved that linear transformation U full fill norm preservation requirement.

**example:** unitary unitary transform is also unitary transform - H\*(CRG\*(CRG(H)) , it is a linear transform and thus behave as linear transform.

There is also another quantum rule which should be mentioned, it is no cloning theorem, which states that it is impossible to create an identical copy of an arbitrary unknown [quantum state](https://en.wikipedia.org/wiki/Quantum_state).

**Example:** it is because measurement could destroy quantum state of particle. For example: if we pass photon through polarizer, polarizer is our measurement, we could lost or retrieve photon it depends on particular situation,

Uncomputing…?

Grover search:

Here is Grover database search algorithm

Ok we are ready to look at quantum algorithms now, here is grover database search algorithm, which can find an element in unsorted set with square root complexity. Note that conventional algorithm need linear time.

**Example:** quantum bits and quantum secrets, page 97, show inversion on blackboard,

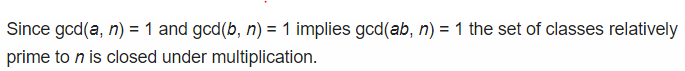
The optimal numer of iterations asumptoticaly goes to sqrt(N), higher count will decrease the probability peak.

Before we attempt to shor algorithm I would like to present some group theory:

Look at **multiplicative group of integers modulo n**, N =9, coprimes 1,2, 4, 5, 7, 8

This kind of groups have special properties:

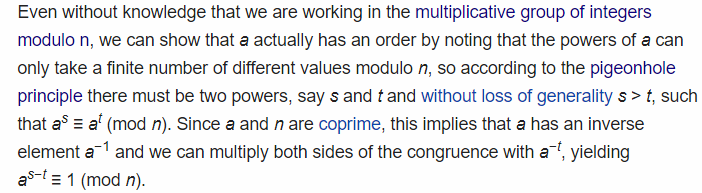
is closed, because if



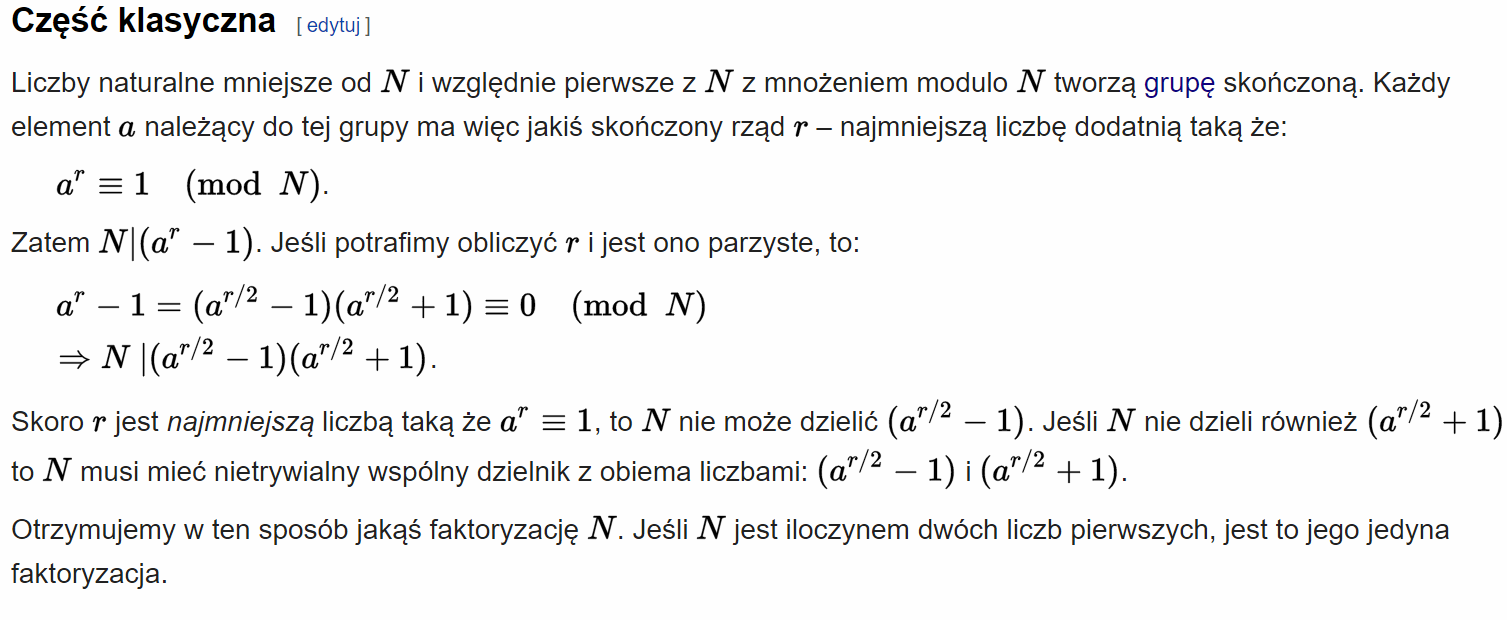
Look at the intuition behind this equation:

a = a1\*a2 , b = b1 \* b1, n = n1\* n2\*n3

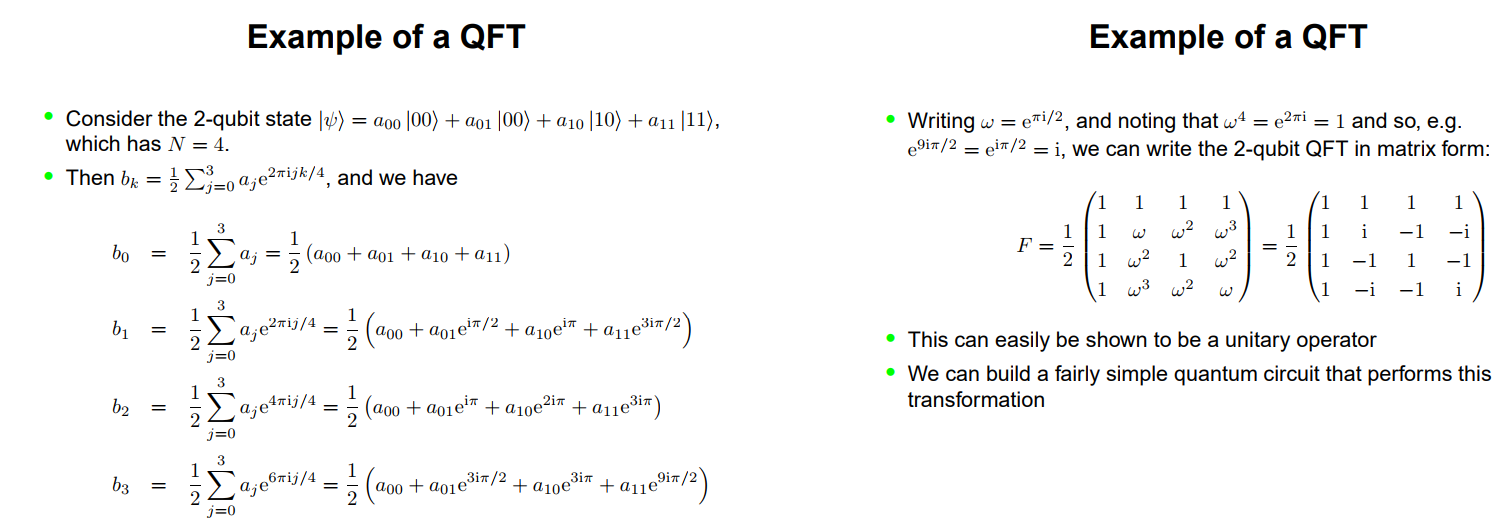
And second important theory about multiplicative group:

We know that multiplicative group of integers modulo n is finite, because it is closed, and the number of elements is lower than n.   


Shor:



qft:



P74 computing devices, applying fourier2.7.5 and get result