

# 理论上讲拥有多少个量子比特 $de=1\pmod{n}$ (n)是什么意思-股识吧

## 一、 $de=1\pmod{n}$ (n)是什么意思

在RSA算法中， $de=1\pmod{n}$ 是指 $de$ 与1关于 $n$ 同余。

对极大整数做因数分解的难度决定了RSA算法的可靠性。

对一极大整数做因数分解愈困难，RSA算法愈可靠。

假如有人找到一种快速因数分解的算法的话，那么用RSA加密的信息的可靠性就肯定会极度下降。

但找到这样的算法的可能性是非常小的。

只有短的RSA钥匙才可能被强力方式解破。

世界上还没有任何可靠的攻击RSA算法的方式。

只要其钥匙的长度足够长，用RSA加密的信息实际上是不能被解破的。

扩展资料：由于RSA算法基于大数分解（无法抵抗穷举攻击），因此在未来量子计算能对RSA算法构成较大的威胁。

一个拥有 $N$ 量子比特的量子计算机，每次可进行 $2^N$ 次运算，理论上讲，密钥为1024位长的RSA算法，用一台512量子比特位的量子计算机在1秒内即可破解。

1983年麻省理工学院在美国为RSA算法申请了专利。

这个专利2000年9月21日失效。

由于该算法在申请专利前就已经被发表了，在世界上大多数其它地区这个专利权不被承认。

参考资料来源：股票百科-RSA算法

## 二、量子计算机基本原理是什么，又长什么样

这东西现在还是傻大黑粗的原始形态，你估计也不想看见。

现在比最早的计算机艾尼亚克快10-100倍，根本没法用。

艾尼亚克是个三十吨的大家伙。

它的原理倒是比较简单，就是用光子代替了电子传输信息，用电子只有两种状态，高电平代表1，低电平代表0.用光子就好很多了，一个光子可以传递几个甚至几十个状态。

计算速度就从 $2^n$ 变成了 $10^n$ 或者 $100^n$ ，同样的传输单位传达的信息和计算的信息增大多少应该很明显吧。

这种计算机的原理和算法已经研究很多年了，都是虚拟研究，现在才有了象点样的

实物，应该会发展很快的。

### 三、人的超能力是随意掌控四大基本力，会怎么样

四大基本力是宇宙内万物间的作用力，一切都遵守著物理定律四大基本力，依强弱次序分别为：1强作用力-核子中的结合力-有效范围 $10^{-12}$ 公分2电磁力（强作用力的 $1/137$ -精细结构常数）-有效范围：远程力

；

-原子中的结合力及分子中的结合力(分子间还有凡得瓦力)3弱作用力（约强作用力的 $1/100,000$ ）-有效范围 $10^{-16}$ 公分-太阳辐射光的能力4万有引力（约强作用力的 $10^{-40}$ 分之1）-太阳系的结合力-有效范围：远程力。

这四种作用力分别由四种玻色子来传递（见下四图）：1传递强核作用力的粒子：胶子内部结构模型图2传递电磁力的粒子：光子内部结构模型图3传递弱核作用力的粒子：W及Z玻色子内部结构模型图4传递万有引力的粒子：引(重)力子内部结构模型图图中+ - 号代表不可分割的最小正负电磁信息单位-

量子比特（qubit）（名物理学家约翰.惠勒John

Wheeler曾有句名言：万物源于比特

；

from

bit量子信息研究兴盛后，此概念升华为，万物源于量子比特）注：位元即比特

### 四、中国量子计算机领先世界多少

这东西现在还是傻大黑粗的原始形态，你估计也不想看见。

现在比最早的计算机艾尼亚克快10-100倍，根本没法用。

艾尼亚克是个三十吨的大家伙。

它的原理倒是比较简单，就是用光子代替了电子传输信息，用电子只有两种状态，高电平代表1，低电平代表0.用光子就好很多了，一个光子可以传递几个甚至几十个状态。

计算速度就从 $2^n$ 变成了 $10^n$ 或者 $100^n$ ，同样的传输单位传达的信息和计算的信息增大多少应该很明显吧。

这种计算机的原理和算法已经研究很多年了，都是虚拟研究，现在才有了象点样的实物，应该会发展很快的。

## 五、量子比特与经典比特有什么区别

通俗模式：

前面的回答已经很精彩了，我再稍微补充一点，因为关于量子纠缠的比喻有很多。中科大量子信息实验室的老大郭光灿院士曾经打过一个比方比喻量子通信，说在美国的女儿生下孩子那一瞬间，远在中国的母亲就变成了姥姥

## 六、理论上，量子计算机最多能有多少个量子单元？为什么？

展开全部问题1：在可预见的将来不会有，也就是说，我们根本无法预计什么时候会有，量子计算机虽然概念已经被提出来了，却还没有具体实施的理论，全世界目前没有任何一个科学家知道该怎么制造量子计算机。

基本上，在当前的科技水平上，量子计算机和科幻没有多少区别。

问题2：一台量子计算机可供全世界所有人同时玩最极品的游戏无压力，还顺便把全世界的天气预报搞定。

问题3：现在的计算机是二进制的，这是因为存储单元是用电压来表示数据，电压只有高和低两个状态；

而量子却有近乎无限个状态，所以一个存储单元就可以存储近乎无限的数据，处理完一个单元的数据就完成了近乎无限条代码的计算（理论上，量子的状态是无限的，但受空间尺寸及测量的分辨率限制，我们无法利用到无限多的状态，但比起电子计算机来说，近乎无限了）。

顺便提一下，不要因为中国发射了量子实验卫星就认为量子计算机快要诞生了。中国这个量子实验卫星，实验的是量子通信，跟你所说的量子计算机是完全不同的两个东西。

## 参考文档

[下载：理论上讲拥有多少个量子比特.pdf](#)

[《股票开通融资要多久》](#)

[《股票卖出多久可以转账出来》](#)

[《委托股票多久时间会不成功》](#)

[《股票抽签多久确定中签》](#)

[下载：理论上讲拥有多少个量子比特.doc](#)

[更多关于《理论上讲拥有多少个量子比特》的文档...](#)

声明：

本文来自网络，不代表

【股识吧】立场，转载请注明出处：

<https://www.gupiaozhishiba.com/chapter/39695350.html>