天道数学

太乙真人

1 道可道，非常道

开篇第一章无名有欲是我们立天地间的兴趣、希望、探索使然。

第五章天地不仁，以万物为刍狗。总揽。他是道教宇宙观中的重要神祇，负责主宰宇宙的运行和创造，同时也是天地万物的创世之主。述明了平等对于怜悯悲悯的态度。

后世不管随机还是概率叠加态，都应秉持商增混乱平均匀称。

老子思想起源于对万物变化中永恒不变事物的思考，他用“天地” 概括经验世界万事万物，认为其皆在变化，只有“道” 永恒不变。“道” 是事物依循的规律规则，超越天地万物，先天地生，是形而上的规则性存在，但又运行于每个事物中，持续存在，如“周行而不殆”“可以为天下母”，老子将其称为“道”，这也是《道德经》的起点。

迷茫和冥想不一样，有欲望的人才会迷茫，放弃欲望的人才会进入冥想。而万籁俱寂就是死人。融入和凝聚，也正如此。当你抄袭和学习之后如果不能进入积累。那么就没有创造。当你体验之后如果不能进入创新，那么此生覆盖cover毫无意义。如果穷其一生都不能找到那条路，那么一辈子蹉跎分不清主次大小，何去何从。择路、铺路才是人间正道。

2 形而上学

形而上学的定义：预设任何实体或概念必然有一种存在方式，且有一种实体或概念是以精神性、规则性的方式存在，证明这类实体或概念如何可能的学说即为形而上学，如宗教的上帝、柏拉图的理念。同时，马哲认为形而上学是孤立、静止、片面的，因其强调独立存在和自身属性，忽略环境等因素相互作用，超越时空、忽略发展变化，且从单一角度论述，缺乏辩证。

3 光

光传的到底是什么？信息、因果、变化、能量。因果变化结合在一起不可逆。时间距离均可缩短。能量变化最小份的量子就是变化本身。

速度的基本单位是怎么确定的？

速度是描述物体运动快慢的物理量，等于位移和发生这个位移所用时间的比值。

在国际单位制中，长度的基本单位是米（m），时间的基本单位是秒（s）。速度等于位移（长度）除以时间，所以速度的基本单位是米每秒（m/s），它是由长度单位和时间单位组合确定的。

米是怎么确定的？

米的定义经历了不断的演变。

最初，1米被定义为通过巴黎的子午线上从地球赤道到北极点的距离的千万分之一。

后来，为了更精准的测量，米的定义基于光在真空中于1/299792458秒内行进的距离，这样的定义使得长度单位米更加精确、稳定，并且便于复现，不依赖于地球子午线的长度测量这种相对不太方便的方式。

299792458这个数字是怎么确定的？

真空中的光速是一个基本物理常数，约为299792458米/秒。这个数值是科学家们通过大量高精度的实验测量得到的。

历史上，科学家们用各种方法来测量光速。例如，通过测量光在已知距离内往返的时间，早期的实验包括斐索实验、迈克尔逊 - 莫雷实验等，随着测量技术的不断进步，对光速的测量越来越精确。

当国际计量大会确定了以光在真空中传播的速度来定义米之后，就把1米定义为光在真空中

1/299792458秒内所经过的距离，从而使长度单位和时间单位建立起更精确的联系。

为什么不用整数？

光速的数值299792458米/秒不是为了刻意不用整数而确定的。

这个数值是基于科学测量的精确结果。长度单位“米”的定义与光速紧密相关，在确定以光在真空中行进的距离来定义米时，要确保这个定义与之前米的定义能够平滑衔接，并且和其他物理量的关系也保持连贯。这样可以保证整个度量衡体系在更新定义的过程中，不会因为数值的随意改变而对科学研究、工程应用等诸多领域造成混乱。

之前米的长度是怎么定义的？

在以光速定义米之前，“米”的定义主要有以下阶段：

最开始，1米被定义为通过巴黎的子午线上从地球赤道到北极点距离的千万分之一。这是基于地球尺寸的一种定义，方便当时的人们以地球的尺度作为参考来确定长度标准。但这种定义方式会受到地球形状不规则、测量误差等因素的影响。

千万分之一是怎么量出来的？

18世纪末，法国科学家为了建立一个统一的长度标准，着手测量子午线长度。

他们组织了大规模的测量活动，使用当时先进的三角测量法。科学家在法国境内沿着子午线方向设置一系列观测点，通过测量角度和已知的基线长度（在相对平坦、可精确测量的短距离地段确定的长度基准），利用三角几何关系计算出各个点之间的距离，逐步构建起一个覆盖较长子午线范围的距离测量网络。

经过复杂的测量和计算后，将从地球赤道到北极点的子午线长度测量出来，然后取其千万分之一来定义“米”这个长度单位。这种方式使得“米”有了基于地球尺寸的、较为客观的定义基础。

4 线性同余与随机数

为什么线性同余能产生随机数？

线性同余法（LCG）能产生看似随机的数，是因为它有以下特点：

线性同余法通过公式 $X_{n+1} = (aX_n + c) \bmod m$ 来生成数列，其中 X_n 是第 n 个随机数，a 是乘子，c 是增量，m 是模数。

首先，对于不了解该公式和初始值（种子）的人来说，生成的数列中的数字在一定范围内（0到$m-1$）看起来是没有明显规律的。因为每次计算都是对前一个值进行乘、加、取模运算的组合。

其次，当参数 a、c、m 选择合适时，这个数列可以覆盖$[0, m-1]$整个区间，而且数字出现的顺序比较杂乱，能在一定程度上模拟随机的分布。不过，严格来说，线性同余生成器产生的是伪随机数。因为它是通过确定性的算法产生的，如果知道种子值和参数，就可以准确地预测后续的数字。

线性同余随机数的参数如何选择？

选择线性同余法（LCG）的参数要考虑以下几点：

4.1 模数 m

- **取值范围**：m 应该是一个较大的正整数。通常选择 2 的幂次方（如 $2^{31}-1$）或者是一个大质数，这样可以让生成的随机数序列覆盖更广泛的范围。例如，在一些应用场景中，使用 $m=2^{32}$ 能产生一个在 0 到 $2^{32}-1$ 之间的整数序列。 - **周期影响**：m 的大小直接影响随机数序列的周期长度。较大的 m 值有可能增加周期长度，理想情况下周期可以达到 m，但这还取决于其他参数的选择。

4.2 乘子 a

- **与模数关系**：a 一般要满足 $2 \leq a < m$。它与 m 最好是互质的（即最大公约数为 1），这样可以使生成的随机数序列有更好的统计特性和更长的周期。例如，若 $m=10$，$a=3$ 时，生成的序列可能比 $a=2$ 时（因为 2 和 10 不互质）更随机。 - **避免不良取值**：某些 a 的取值可能会导致生成的序列出现短周期或明显的规律。例如，当 $a=1$ 时，序列几乎是等差序列，不具备随机性。

4.3 增量 c

- **取值范围**：c 是一个整数，通常 $0 \leq c < m$。 - **对随机性的影响**：当 $c=0$ 且 a 满足一些特殊条件（如 a 是模 m 的原根）时，生成的序列仍可以有较长周期，但可能会出现一些不太理想的统计特性。非零的 c 可以在一定程度上增加序列的复杂性和随机性。

在实际应用中，一些经过验证的参数组合可以产生较好的随机数序列。例如，经典的参数组合 $m=2147483647$（$2^{31}-1$，是一个质数）、$a=16807$、$c=0$，这组参数被广泛应用于早期的伪随机数生成场景。

原根是什么，为什么选16807？

原根的定义：设$m>1$，$(a,m)=1$（即a与m互质），

t是使$a^t \equiv 1 \pmod{m}$成立的最小正整数，

则称t为a关于模m的阶数。若a关于模m的阶数是$\varphi(m)$（其中$\varphi(m)$是欧拉函数，表示小于等于m且与m互质的正整数的个数），就称a为模m的一个原根。

为什么选择 16807 作为线性同余法中的参数： - **理论基础方面**： - **保证较好的随机性**：线性同余法生成的随机数序列的质量与所选取的参数有很大关系。当使用原根作为乘子时，能够使得生成的随机数序列具有更好的随机性和更长的周期。16807 这个数作为乘子，在特定的模数下能够满足原根的条件，使得随机数生成器的性能较好。 - **满足数学性质**：原根具有一定的数学性质，使得基于原根的线性同余法生成的随机数序列能够更好地满足均匀分布等随机性的要求。对于特定的模数，选择合适的原根作为乘子可以确保生成的随机数在统计上更接近真正的随机数。 - **实践验证方面**： - **长期的实践经验**：在计算机科学和数学的发展过程中，人们经过大量的实验和实践，发现 16807 作为乘子在很多情况下能够生成质量较高的随机数序列。经过长时间的使用和验证，它被证明是一个比较可靠的选择。 - **与其他参数的配合**：16807 与特定的模数（如 $2^{31}-1$）配合使用时，能够产生具有较好随机性和较长周期的随机数序列。这种参数组合在实际应用中表现出了较好的效果，因此被广泛采用。

总的来说，选择 16807 作为线性同余法的乘子是基于数学理论和长期实践经验的综合考虑，它能够为线性同余法提供较好的随机性和较长的周期，从而满足很多应用场景对随机数的需求。

素数原根定理？

素数原根定理是数论中的一个重要定理。

1. **定义** - 对于一个素数p，原根是指一个整数g（$1 < g < p$），

使得g的幂次g^k（$k = 1, 2, \cdots, p-1$）在模p下产生$p-1$个不同的余数。也就是说，这些余数正好遍历从1到$p-1$的所有整数。 2. **定理内容** - 对于素数p，原根是存在的。而且原根的个数为$\varphi(p-1)$，其中$\varphi(n)$是欧拉函数，表示小于等于n且与n互质的正整数的个数。例如，对于素数$p = 7$，$\varphi(6) = 2$，它有两个原根，经过计算可以发现是3和5。 - 对于整数m，如果它有原根，那么原根的个数为$\varphi(\varphi(m))$。不过这个情况相对复杂一些，因为不是所有的整数都有原根，只有$m = 2, 4, p^k, 2p^k$（其中p是奇素数，k是正整数）这些形式的整数才有原根。 3. **应用意义** - 在密码学中，原根被广泛应用。例如在Diffie - Hellman密钥交换协议中，原根的性质被用来在不安全的通信信道上安全地交换密钥。双方可以基于一个公开的素数和它的原根来生成共享的密钥，由于原根的幂次在模素数下的特殊性质，使得攻击者很难破解出这个密钥。 - 在伪随机数生成方面，如前面提到的线性同余法中，选择素数的原根作为乘子可以帮助生成具有更好随机性和更长周期的伪随机数序列。因为原根的幂次模素数的结果分布较为均匀，符合随机数生成的一些要求。

欧拉函数？

1. **定义** - 对于正整数n，欧拉函数$\varphi(n)$表示小于等于n且与n互质（即最大公约数为1）的正整数的个数。例如，$\varphi(6)$，小于等于6且与6互质的数有1、5，所以$\varphi(6) = 2$。 2. **计算方法** - 若n是素数，那么$\varphi(n) = n - 1$。因为素数与小于它的所有正整数都互质。例如，$n = 7$，小于等于7且与7互质的正整数有1、2、3、4、5、6，共6个，所以$\varphi(7) = 6$。 - 若$n = p^k$（p是素数，k是正整数），则$\varphi(n) = p^k - p^{k-1}$。例如，$n = 2^3 = 8$，根据公式$\varphi(8) = 2^3 - 2^2 = 4$，实际上小于等于8且与8互质的数是1、3、5、7，正好是4个。 - 对于一般的n，如果$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$（$p_i$是不同的素数，$k_i$是正整数），那么$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right)$。例如，$n = 12 = 2^2 \times 3$，则$\varphi(12) = 12 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 4$，小于等于12且与12互质的数是1、5、7、11，共4个。 3. **性质和应用** - 欧拉函数是乘法函数，即如果m和n互质，那么$\varphi(mn) = \varphi(m)\varphi(n)$。这一性质在数论计算和一些数学证明中非常有用。 - 在密码学中，特别是在RSA公钥加密算法中，欧拉函数起着关键的作用。RSA算法的安全性基于分解大整数的困难性以及欧拉函数的性质，通过巧妙地利用欧拉定理（$a^{\varphi(n)} \equiv 1 \pmod{n}$，其中$a$与$n$互质）来实现加密和解密的过程。

有原根的整数为什么满足条件？

1. **$m = 2$的情况** - 当$m = 2$时，1是它的原根。因为$1^1 \equiv 1 \pmod{2}$，在模2下遍历了所有与2互质的数（其实只有1）。 2. **$m = 4$的情况** - 对于$m = 4$，3是原根。因为$3^1 \equiv 3 \pmod{4}$，$3^2 \equiv 1 \pmod{4}$，在模4下，3的幂次遍历了1和3，这是所有小于等于4且与4互质的数。 3. **$m = p^k$（p是奇素数，k是正整数）的情况** - 从群论的角度来看，整数模m的乘法群$Z_m^\times$是一个循环群，其生成元就是原根。对于$m = p^k$，这个乘法群的阶数（元素个数）是$\varphi(p^k) = p^k - p^{k-1}$。 - 由于这个群是循环群，所以存在生成元（原根），其幂次可以遍历群中的所有元素，也就是生成所有小于等于m且与m互质的余数。 4. **$m = 2p^k$（p是奇素数，k是正整数）的情况** - 可以证明，在这种情况下整数模m的乘法群$Z_m^\times$也是循环群，所以存在原根。 - 具体的证明过程涉及到群论和数论的一些比较复杂的知识，简单来说，是通过分析群的结构和元素之间的关系，发现存在一个元素（原根），其幂次能够遍历群中的所有元素。