# 原根到底在做什么?

> 编写人：王原龙
>
> 2021.04.01

写一点自己的粗浅理解，未必全对，希望对大家理解原根与指数部分的知识有所帮助

大家愿意看就看，不愿看就算了，看到错误可以选择跟我交（dui）流（xian）或者暗地里嘲笑我。~~虽然考试不一定会考这里的内容，但是依然~~希望大家加深对这部分知识的理解。

注：为方便叙述起见，后面会将模$m$完系和缩系的元素限定在$[0,m]$当中，且除非特殊声明，否则变量均为非负整数，不讨论负数。

首先从整体上说，在我们所学的范围内理解，通过原根实现了**从缩系到完系的映射**。进一步来说，对于有原根的数$m$，模$m$缩系$\{m_0,m_1,\cdots,m_{\phi(m)-1}\}$到模$\phi(m)$完系$\{0,1,\cdots,\phi(m)-1\}$之间存在一个一一对应的映射（即双射），准确地说，随着以后的学习大家会明白，这一双射实际上还是一个**同构映射**。而通过这一同构映射，研究指数的问题就完全转化成了一个研究系数的问题（也就是将$a^b$转化成了$ab$）。

而这一部分之所以略难理解，就是因为课本的叙述对于这个同构只字未提，且不区分在完系和缩系两个不同系统里对应的操作，所以在一边很容易理解的一些东西到了原根与指数这里就转化成了一个看起来很怪异的结论。

那么我们从头讲起：

# 从完系开始

相信在这一节一开始，很多同学就被书上给出的定义直接搞晕，首先我们之前几乎没有考虑过在同余背景下讨论“指数函数”的经历，另外$a^n\equiv 1\ (mod\ m)$这种莫名其妙的式子也让人摸不着头脑，因为除一个数余数是1好像并没啥特殊的，为什么令这种式子成立的最小$n$反倒成了一个让人感兴趣的话题？

为理解这一定义，我们先来观察一些现象，它出现在$a$对自己不断进行**模$m$加法**的迭代过程中：$a$不断加自己，产生一个$0a,a,2a,3a,\cdots,ma$的序列，这时候发现$0a$和$ma$在模$m$的意义下好像是相同的啊！那么此后的加法结果也就是循环的了，也就是说这个序列是一个周期序列，而且因为它是离散的，所以是肯定具有所谓最小正周期的吧？这一最小正周期当然不一定是$m$，而显而易见$\frac{m}{(a,m)}a=[a,m]$是$m$的倍数，且不存在比$\frac{m}{(a,m)}$更小的正整数了，否则与最小公倍数的定义矛盾！于是我们能不能捕捉到这样的周期特性呢？

我们看看下面这个简单到极点的定义：

- 定义$a$模$m$的**加阶**为$n$，当它们满足

$$n=\min_x\{x\mid xa\equiv 0(mod\ m),x>0\}$$

  即$n$是使$na\equiv 0(mod\ m)$成立的最小正整数。

首先，这个线性同余方程一定有解（我们学过其判定法），所以$n$是存在的。且容易看到，由于$n$有最小性，所以$a,2a,\cdots,(n-1)a$都不是$m$的倍数。另外，我们知道一个周期可以从周期中任一个点开始，那么为什么同余0就那么特殊呢？其实不管对于任何整数都是一样，当$ka\equiv sa(mod\ m)$时，$|k-s|a\equiv 0(mod\ m)$就成立，而且同余0还可以避免同余方程无解的问题，而且由于对任意数$a$，有$a\equiv a+0(mod\ m)$，所以 0 是模$m$加法的**单位元**，显然更好理解，也就是对$m$完系里面随便什么数，每步走$a$这么长，每连走$n$步就会回到原点，相当于走了0步（加了单位元）。

那么若$a$的加阶为$n$，$ka$的加阶如何呢？首先我们知道$a$的倍数模$m$时每走$n$步余数就会循环，而$ka$每次走$k$步，所以实际上当走的步数达到$[k,n]$步的时候实际第一次回到原点，仔细想想其实这个问题相当于在问$k$模$n$的加阶！从前面的叙述中就可以知道是$\frac{n}{(n,k)}$了。

十分特殊的是，我们首先观察到1的模$m$加阶显然是$m$，另外由上一段的结论得知$k=k\times 1$模$m$的阶为$m$当且仅当$(k,m)=1$。于是知道$m$缩系中的元素的加阶**都是**$m$。所以通过迭代地加这个特殊的元素$m$次可以得到一个完系，而且$m$缩系中的元素均具有此性质。

# 从加法到乘法

啰嗦这么多，我们又发现这个定义跟书上阶定义好像很相似，而且看起来简单多了。我们做一步大胆的变换：将加法换成乘法，将加法单位元0换成乘法单位元1，会发生什么？**(注：下面的定义与部分性质目前只是单纯做替换，还缺少一个关键条件，即a与m互素，将在后面叙述)**

- 定义$a$模$m$的**阶**为$n$，当它们满足
$$n=\min_x\{x\mid a^x\equiv 1(mod\ m),x>0\}$$
即$n$是使$a^n\equiv 1(mod\ m)$成立的最小正整数。
- 由于$n$有最小性，所以$a,a^2,\cdots,a^{n-1}$模$m$非1。
- 当$a^k\equiv a^s(mod\ m)$时，$a^{|k-s|}\equiv 1(mod\ m)$就成立
- 对任意$a$，$a\equiv a\times 1(mod\ m)$——乘法单位元
- 若$a$的阶为$n$，$a^k$的阶为$\frac{n}{(n,k)}$

而关于这个替换成乘法的新系统，这个类比1的特殊元素是什么呢？答案已经呼之欲出了——原根

那么这一切跟$\phi(m)$有什么关系呢？我们回顾加阶的定义

$$n=\min_x\{x\mid xa\equiv 0(mod\ m),x>0\}$$

这里我们显然看到这个方程是有解的，而从加法扩展到乘法后，我们遇到的第一个问题就是——$a^x\equiv 1(mod\ m)$这种东西，真的有解吗？

一般情况下，当然是不一定有解，但是伟大的**欧拉定理**告诉我们——只要有$(a,m)=1$，那么$a^{\phi(m)}\equiv 1(mod\ m)$成立！于是上面的方程至少有显然的解$\phi(m)$，于是阶的存在性就有了保证，并且一定有阶$l\mid\phi(m)$成立。这也就是为什么上面的定义和性质**几乎**都需要$(a,m)=1$作为保证。于是我们的视野就从完系转换到了缩系中。

那么回到特殊元素的问题，是否存在这样一个$g$，使得其阶达到这个最大的值$\phi(m)$呢？于是定义：

- 若$(g,m)=1$且$g$模$m$的阶为$\phi(m)$，则称$g$为模$m$的原根。

并且经验证我们得到了一些原根的存在，说明这个定义完全是合理的。那么完全类似上一段的讨论，就可以知道$\{g^0,g^1,\cdots,g^{\phi(m)-1}\}$是一个模$m$的缩系。

# 从完系到缩系的映射

在上一部分的讨论中我们看到，纵使我们进行了一些替换如把加法替换成乘法，乘法替换成乘方，0替换成1等等，但是还是有一些技巧是我们没有替换的，比如说“特殊元”的思想，“单位元”的思想，以及最重要的“用特殊元生成讨论的集合中所有元素”这一思想。

尽管运算变了，表示变了，但是对“特殊元”进行与自己的迭代运算这一点并没有变化，于是我们就可以看到，给定$m$的原根$g$，则在$m$的缩系中任意一个元素可以由$g$迭代若干步得到，而这个迭代过程是以$\phi(m)$为周期。而且我们小学二年级就学过，乘法搬到指数上就变成了加法。所以如果从$g$的指数来看，这一过程其实是在模$\phi(m)$的完系之中进行的迭代加法，这就给我们一个启发，如果我们定义一个映射

$$f(x):\{g^0,g^1,\cdots,g^{\phi(m)-1}\}\to\{0,1,\cdots,\phi(m)-1\}$$
$$f(g^t)=t,0\le t<\phi(m)$$
$$f(g^x\times g^y)=f(g^x)+f(g^y)=x+y\ mod\ m$$

那么将在模$m$缩系到模$\phi(m)$完系$\{0,1,\cdots,\phi(m)-1\}$之间建立一个双射，这个映射保持了各自的运算，那么在缩系里面研究乘法就完全等价于在完系中研究加法了，所以迁移有关加阶的性质，我们就知道$m$的缩系中对于模$m$阶是$\phi(m)$的元素$g^t$有$(t,\phi(m))=1$，于是（当$m$有原根时）$m$的原根有$\phi(\phi(m))$个。

如果上面的说法比较绕，那我们再来换一个更简单一点的说法：实质上通过这个映射我们将缩系的乘法转换成了完系的加法，将缩系的指数换成了数乘，也就是说在$m$有原根$g$的情形下我们实际上定义出了$m$缩系中的元素对于原根的**对数**，而这就是所谓的**离散对数**，它是我们解决形如$x^n\equiv c\ (mod\ m),(c,m)=1$的方程的有力工具，因为这时我们在两边取对于$m$的原根$g$的离散对数（映射到缩系），就可以得到$n\ log_gx\equiv log_gc(mod\ \phi(m))$，由于$c$在$m$的缩系中，所以$log_gc$存在，所以可以解出这个关于$log_gx$的线性同余方程，于是就解出了$x$。而由于$m$可以进行质因数分解，且形如$p^k,2p^k$的数存在原根，所以我们就可以解决很多这样的方程了（当然，$m=8$的情形尚不能解决）。这就是原根与指数部分的核心思想。

# 杂谈

至此，这一部分的核心思想就讲解完了。我个人认为这一部分之所以略难理解，有一大原因是增1，加法，乘法，乘方四个运算等级是逐级提升的，并且是通过下层运算的迭代形成上层运算，也就是我们二年级就懂的反复自增形成加法，反复加形成乘，反复乘形成乘方。而在完系中我们把加法视为核心运算，研究加法和迭代加——即乘法；而在缩系中我们把乘法视为核心运算，研究乘法和迭代乘——即乘方。所以这中间乘法是在两个系统中都出现的，但是其意义——从我们研究的思路来看——是不同的，所以若不试着区分的话很容易把自己绕进去。

而这一部分体现了相当精彩的类比思想，也把代数结构的最精华的部分给大家揭开了一角。从本质上说，代数结构所研究的核心问题是一个集合以及在集合元素上定义的运算，我们并不关心集合元素的真面目，而只关心其上运算的性质，也就是说这个代数系统的性质就体现在其运算上，这是一个上层的抽象。而在实际的应用中，只要某个研究的问题中有这样性质的运算，不管这个运算是对谁做的，不管这个运算具体怎样实现的，这个集合和这个运算都会体现出这些性质。就好比所有满足线性空间公理的空间都可以转化成向量进行研究一样，不管是多项式也好，向量本身也好，线性变换空间也好，因为它们都是线性空间，所以必定会有基，而其中的任意元素一定可以分解成基的线性组合。