原根的概念、性质及其存在性

小圆滚滚

上一篇文章我们证明了欧拉定理，其中提到了除以m的余数里有$\phi(m)$个与m互质，当a与m互质时，我们有$a^{\phi(m)} \equiv 1 \pmod{m}$。在证明威尔逊定理时，我们引出了可逆元的概念，这些与m互质的余数（实为同余类）刚好就是模m的可逆元，构成一个有限乘法群，其中余数1为恒等元，余数m-1的平方等于恒等元。

1 原根的概念和性质

如果a与m不互质，那么我们把满足$a^k \equiv 1 \pmod{m}$的最小正整数k称为a的模m的**阶**。

事实1：如果$a^n \equiv 1 \pmod{m}$，那么a的阶k整除n.

用带余除法可得n=kq+r，其中$0 \leq r \leq k-1$.

由阶的定义可知k满足$a^k \equiv 1 \pmod{m}$，用乘方的性质可得$a^{kq} \equiv (a^k)^q \equiv 1 \pmod{m}$.

直接计算可得$a^r \equiv a^{n-kq} \equiv a^{n-kq}a^{kq} \equiv a^n \equiv 1 \pmod{m}$.

因为k是满足同余式的最小正整数，只能有r=0，也就是k整除n.

由欧拉定理我们有当a与m互质时，$a^{\phi(m)} \equiv 1 \pmod{m}$，因此a的模m的阶一定是$\phi(m)$的因数。

我们把阶刚好等于$\phi(m)$的余数（同余类）称为模m的原根(primitive root)。

当m=2时，可逆元只有$\phi(2)=1$个，其阶为1，所以1是模2的原根；

当m=3时，可逆元有1和2共$\phi(3)=2$个，其中2的阶为2，所以2是模3的原根；

当m=4时，可逆元是1和3共$\phi(4)=2$个，其中3的阶是2，所以3是模4的原根；

当m=6时，可逆元是1和5共$\phi(6)=2$个，其中5的阶是2，所以5是模6的原根；

原根可能不止一个，比如

当m=5时，可逆元是1, 2, 3, 4共$\phi(5)=4$个，其中2和3的阶都是4，而4的阶是2，所以2和3都是模5的原根，而4不是。

之所以称之为根，是因为它是同余方程的一个解$x^{\phi(m)} \equiv 1 \pmod{m}$。而称之为“原”根，是因为是方程解集（乘法群）的生成元，解集是$\phi(m)$阶循环群。原根有如下性质：

事实2：g是模m的原根当且仅当g可以生成所有的可逆元，也就是说任何与m互质的整数a，都可以找到正整数k使得$a \equiv g^k \pmod{m}$.

证明：如果g不是模m的原根，那么其阶小于$\phi(m)$，不同余的q的次方就少于$\phi(m)$个，而可逆元有$\phi(m)$个，故不可能生成所有可逆元。

如果g是模m的原根g的前$\phi(m)$个正整数次方$g,\ g^2, \cdots,\ g^{\phi(m)}$，我们说明这些整数除以m后余数不同。否则设$g^i \equiv g^j \pmod{m}$，$1 \leq i < j \leq \phi(m)$，利用同余的除法性质，由g与m互质，同余式两边消去公因数g^i可得$g^{j-i} \equiv 1 \pmod{m}$，得到比$\phi(m)$还小的正整数指数j-i，与g为原根，$\phi(m)$为其阶矛盾。

这$\phi(m)$个g的次方除以m得到的余数正好是与m互质的$\phi(m)$个余数（可逆元）的重新排列，

其中$g^{\phi(m)} \equiv 1 \pmod{m}$.

在模5的所有$\phi(5)=4$个可逆元中，2的阶是4，是一个原根，$4\equiv 2^2 \pmod 5$，$3\equiv 2^3 \pmod 5$。同样地，3的阶也是4，也是一个原根，$4\equiv 3^2 \pmod 5$，$2\equiv 3^3 \pmod 5$.

如果模m的可逆元存在原根，根据**事实2**，所有可逆元都可以通过这个原根的次方表示出来，我们可以根据指数来判断得到的次方是否是也是原根。

事实3：设g是模m的一个原根，那么g^k是原根，当且仅当k与$\phi(m)$互质。

证明：当k与$\phi(m)$互质时，可以找到整数s和t，使得$sk+t\phi(m)=1$。对任意次方g^i都有

$g^i \equiv g^{j(sk+t\phi(m))} \equiv (g^k)^{js} \pmod m$

也就是g^i在同余意义下可以表示成g^k的js次方，说明g^k可以生成所有可逆元，故为模m的原根。

比如当m=7时，$3^2\equiv 2 \pmod 7$，$3^3\equiv 6 \pmod 7$，$3^4\equiv 4 \pmod 7$，$3^5\equiv 5 \pmod 7$

可知，3是模7的一个原根，与$\phi(7)=6$互质的另一个指数是5，

因此还有一个原根是$5\equiv 3^5 \pmod 7$.

这个事实说明，如果原根存在，那么原根的数量为$\phi(\phi(m))$.

并不是对所有的整数m都有原根。

例如当$m=8=2^3$时，$3^2\equiv 4^2\equiv 5^2\equiv 7^2\equiv 1 \pmod{}$，除恒等元1外，其他可逆元的阶都为2，没有阶为$\phi(8)=4$的可逆元，因此模8没有原根。

2 模p原根的存在性

原根存在性定理：对于质数p，模p的原根存在，且有$\phi(\phi(p))=\phi(p-1)$个。

为证明这个定理，我们需要几个引理，第一个引理实为**事实3**的一个推广：

引理1：如果整数a模m的阶是t，那么a^k的阶是t当且仅当k和t互质。

证明：设k和t的最大公因数是d，记$k'=k/d$和"$t'=t/d$.

一方面，$(a^k)^{t\ss}\equiv (a^t)^{k'}\equiv 1 \pmod m$，根据**事实1**可得$a^k$的阶s一定整除$t'$.

如果s=t，那么一定有t整除t'，可以推出$t=t'$，也就是d=1，k和t互质。

另一方面，$(a^k)^s\equiv a^{ks}\equiv 1 \pmod m$，根据**事实1**可得a的阶t一定整除ks.

如果k与t互质，那么t一定整除s，又因为s整除t，所以一定有s=t.

例如当$m=9=3^2$时，共有$\phi(9)=6$个可逆元，其中2和5是原根，阶为6，4和7的阶为3，这里正好有关系$4^2\equiv 7 \pmod 9$和$7^2\equiv 4 \pmod 9$.

代数基本定理告诉我们n次复系数多项式f在复数域内至少有一个复根，通过数学归纳法可以证明恰好有n个复根（重数计算在内）。但这对同余方程不一定成立：

比如二次同余式$x^2+x\equiv 0 \pmod 6$在模6的6个余数中有4个根，分别是0, 2, 3, 5.

但如果模m是一个质数，那么结论成立。具体地，我们有

引理2：对于n次同余方程$f(x)\equiv 0 \pmod p$最多有n个根。

证明：用数学归纳法，一次同余方程有$ax+b\equiv 0 \pmod p$最多一个根。

假设n-1次同余方程最多n-1个根，考虑n次同余方程$f(x)\equiv 0 \pmod p$.

如果方程没有根，结论成立。

如果方程有根，不妨设r是一个根。记n次整系数多项式f为

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$

代入x=r得

$f(r)=a_nr^n+a_{n-1}r^{n-1}+\cdots+a_1r+a_0$

两式相减得

$f(x)=f(x)-f(r)=a_n(x^n-r^n)+a_{n-1}(x^{n-1}-r^{n-1}+\cdots+a_1(x-r))$

每一项因式分解后提取公因式x-r可得

$f(x)=(x-r)g(x)$

其中$g(x)$是n-1次整系数多项式。

因为p是质数，p整除(x-r)g(x)等价于p整除x-r或p整除g(x)，也就是

$(x-r)g(x)\equiv 0 \pmod p$等价于$x-r\equiv 0 \pmod p$或者$g(x)\equiv 0 \pmod p$.

根据归纳假设$g(x)\equiv 0 \pmod p$最多n-1个根，所以加上r这个根，$f(x)\equiv 0 \pmod p$最多n个根。

引理3：如果d整除p-1 ，那么$x^d\equiv 1 \pmod p$恰好有d个根。

证明：由费马小定理知同余方程$x^{p-1}\equiv 1 \pmod p$在同余意义下有p-1个根。

如果d整除p-1，不妨记p-1=qd，由代数恒等式可知

$x^{p-1}-1=(x^d)^q-1=(x^q-1)(x^{(q-1)d}+x^{(q-2)d}+\cdots+x^d+1)$

$x^{p-1}-1\equiv 0 \pmod 0$就等价于$x^d-1\equiv 0 \pmod p$或$g(x)\equiv 0 \pmod p$

其中$g(x)=x^{(q-1)d}+\cdots+x^d+1$是(q-1)d次整系数多项式，对应的同余方程最多(q-1)d个根。

由此可得$x^d-1\equiv 0 \pmod p$至少有$(p-1)-(q-1)d=qd-(q-1)d=d$个根。但由**引理2**我们知道同余方程$x^d\equiv 1 \pmod p$最多有d个根，因此恰好有d个根。

下面证明模p的原根有$\phi(p-1)$个。这里的想法是把p-1个可逆元按照阶来分类。

在模p的$1,\ 2,\cdots,\ p-1$个可逆元中，每一个的阶都是p-1的因数。

记n(t)为以t阶的可逆元个数，显然有n(1)=1和n(2)=1.

把所有可能的阶对应的可逆元个数加起来就等于可逆元的总数$\sum\limits_{t|p-1} n(t)=p-1.$

另外，与p-1的最大公因数为t的可逆元个数有$\phi((p-1)/t)$个，这些可能的最大公因数对应的可逆元全部加起来也是可逆元的总数$\sum\limits_{t|p-1}\phi((p-1)/t)=\sum\limits_{t|p-1}\phi(t)=p-1.$

因此可以得到$\sum\limits_{t|p-1} n(t)=\sum\limits_{t|p-1}\phi(t).$

对任意$t\mid p-1$，分两种情况：

一、没有阶为t的可逆元，也就是$n(t)=0<\phi(t)$；

二、存在阶为t的可逆元，不妨设为a，那么根据**引理3**，同余方程$x^t\equiv 1 \pmod p$恰好有t个解，正好就是t个的a的次方$a,\ a^2,\cdots,\ a^t$。

阶为t的可逆元一定是同余方程的解，也就一定是$a,\ a^2,\cdots,\ a^t$中的一个。

再根据**引理1**，这其中a^k的阶为t当且仅当k与t互质，这样的指数共有$\phi(t)$个；也就是在这种情形下，刚好有$n(t)=\phi(t)$。

但$\sum\limits_{t|p-1} n(t)=\sum\limits_{t|p-1}\phi(t)$，因此不可能有第一种情况发生，只能是对任意$t\mid p-1$，都有$n(t)=\phi(t)$，

特别地，原根的个数$n(p-1)=\phi(p-1).$

以p=13为例，一共有12个可逆元，其中阶为$\phi(1)=1$的有1个，即恒等元1；阶为2的有$\phi(2)=1$个，即12；阶为3的有$\phi(3)=2$个，为3和9；阶为4的有$\phi(4)=2$个，为5和8；阶为6的有$\phi(6)=2$个，为4和10；最后阶为12的本原根有$\phi(12)=4$个，为2, 6, 7, 11.

下一篇文章讨论什么样的合数m有原根，结论是只有m=4，$m=p^a$或$2p^a$，其中p是奇质数。