第六讲 初等数论

6

本讲提要

- 原根

1.1 整数的次数

定义1 设$m>0,(m,a)=1$，l是使

$$a^l\equiv 1(\bmod m)$$

成立的最小正整数，则 l叫做a对模m的次数。

定理1 设a对模m的次数为l，如有$a^n\equiv 1(\bmod m)$，$n>0$，则$l\mid n$。

定理1证明.

若$l\mid n$不成立，有：

$n=ql+r,0<r<l$，而$1\equiv a^n\equiv a^{ql+r}\equiv a^{ql}a^r\equiv a^r(\bmod m)$。这违反了定义1。

推论1 设a对模m的次数为l，则$l\mid\varphi(m)$。

根据第三讲的欧拉定理，推论1是显然的。

2 缩系(续)

定理5（欧拉定理）设$m>1,(a,m)=1$，则

$$a^{\varphi(m)}\equiv 1(\bmod m)。$$

定理5证明.

设r_1，$r_2,\cdots$，$r_{\varphi(m)}$为模m的一组缩系，由 定理4知

ar_1，$ar_2,\cdots$，$ar_{\varphi(m)}$亦是模m的缩系。

因此,$(ar_1)(ar_2)\cdots(ar_{\varphi(m)})\equiv r_1r_2\cdots r_{\varphi(m)}(\bmod m)$,

即$a^{\varphi(m)}r_1r_2\cdots r_{\varphi(m)}\equiv r_1r_2\cdots r_{\varphi(m)}(\bmod m)$。

因为r_1，$r_2,\cdots$，$r_{\varphi(m)}$为模m的一组缩系，所以$(r_1r_2\cdots r_{\varphi(m)},m)=1$。

由上讲定理8知$a^{\varphi(m)}\equiv 1(\bmod m)$。

1.1 整数的次数(续)

定理2 设a对模m的次数为 l，则

$$1，a，a^2,\cdots，a^{l-1}$$

对模m两两互不同余。

定理2 证明.

若结论不成，有 j和k,$0 \le j < k \le l-1$，使的

$a^k \equiv a^j \pmod{m}$，有 $a^{k-j} \equiv 1 \pmod{m}$，

而$0 \le k-j \le l-1$，这与 l是a模m的次数矛盾。

1.1 整数的次数(续)

定理3　设a对模m的次数是l，$\lambda>0$，a^{λ}对模m的次数为l_1，

则$l_1=\dfrac{l}{(\lambda,l)}$。

定理3 证明.

由l_1为a^{λ}的次数，有$a^{\lambda l_1}\equiv 1(\bmod m)\overset{\text{定理1}}{\Rightarrow} l\mid \lambda l_1$即$\dfrac{l}{(\lambda,l)}\Bigg|\dfrac{\lambda}{(\lambda,l)}l_1$，

由于$\left(\dfrac{l}{(\lambda,l)},\dfrac{\lambda}{(\lambda,l)}\right)=1$，得$\dfrac{l}{(\lambda,l)}\Bigg|l_1$。

另$\left(a^{\lambda}\right)^{\frac{l}{(\lambda,l)}}\equiv\left(a^{l}\right)^{\frac{\lambda}{(\lambda,l)}}\equiv 1(\bmod m)$，有$l_1\Bigg|\dfrac{l}{(\lambda,l)}$，因此，$l_1=\dfrac{l}{(\lambda,l)}$。

1.1 整数的次数(续)

推论2 设a对模m的次数是l，则$\varphi(l)$个数

$$a^{\lambda}，(\lambda, l) = 1，0 < \lambda \le l,$$

对模m的次数均为l。

由定理2、3知推论2显然成立。

1.1 整数的次数(续)

定理4 设p是一个素数，如果存在 整数a，它对模p的次数为l，则恰有 $\varphi(l)$个对模p两两不同余的整数，它 们对模p的次数都为l。

定理4证明.

a对模p的次数为l。定理2说明

a，$a^2,\cdots a^{l-1}$，a^l模p两两互不同余，因此， 根据第三讲的定理12，其是

$x^l \equiv 1(\bmod p)$的全部解。

而次数为l的整数必包含于其中。

由推论2知$a^{\lambda},(\lambda,l)=1,0<\lambda\leq l$的次数为$l$。因此，恰有$\varphi(l)$个。

4 模是素数的同余式

定理12（拉格朗日定理）设p是素数，$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，$n>0$，$a_n\not\equiv 0 \pmod p$，是一个整系数多项式，则同余式

$$f(x)\equiv 0 \pmod p$$

最多有n个解。

定理12 证明.

归纳法。

当$n=1$时，$a_1x+a_0\equiv 0 \pmod p$，$p\nmid a_1$，恰有一解。

假定$n-1$时为真，即最多有 $n-1$个解，需证明 n时最多只有n个解。如果 $n\geq p$结论立即成立。

1.1 整数的次数(续)

定理5 设$l \mid p-1$，则次数是l的，模素数p互不同余的整数的个数是$\varphi(l)$个。

定理5证明.

ψ代表$1,2,\cdots$，$p-1$中对p次数为l的个数。因为次数l只能为$p-1$的因数，故

$\sum\limits_{l \mid p-1} \psi(l) = p-1$，另$\sum\limits_{l \mid p-1} \varphi(l) = p-1$。

定理4说明$\psi(l)=0$或$\varphi(l)$有$\psi(l) \le \varphi(l)$，上两式做差

$\sum\limits_{l \mid p-1} (\varphi(l)-\psi(l)) = 0$。

因此，$\varphi(l)=\psi(l)$。

1.1 整数的次数(续)

定理5证明.（续）

把正整数

$1,2,\cdots$，$j,\cdots$，m按其与m的最大公约数分类，即相同分一类。

这种子集为：

$(j,m)=d, 1\le j\le m$(为对全体数的一个不相交划分)。

设$j=dh$，有

$$\left(h,\frac{m}{d}\right)=1, 1\le h\le\frac{m}{d},$$

因此，这样的h的个数为$\varphi\left(\frac{m}{d}\right)$，即

$$m=\sum_{d|m}\varphi\left(\frac{m}{d}\right)=\sum_{d|m}\varphi(d)。$$

1.2 原根

定义2 设整数$m>0,(g,m)=1$，如果整数g对m的次数为$\varphi(m)$，则g叫模m的一个原根。

定理6 设$(g,m)=1$，$m>0$，则g是m的一个原根的充分必要条件是

$$g，g^2,\cdots，g^{\varphi(m)}$$

组成模m的一组缩系。

1.2 原根(续)

定理6证明.

$\rightarrow$ g是m的一个原根，次数为 $\varphi(m)$。

根据定理2知g，$g^2,\cdots$，$g^{\varphi(m)}$中任意

两个互不同余。又因为$(g,m)=1$,

所以$g^2,\cdots$，$g^{\varphi(m)}$都与m互素，因此，

g，$g^2,\cdots$，$g^{\varphi(m)}$构成模m的一组缩系。

$\leftarrow$ $(g,m)=1$，由欧拉定理$g^{\varphi(m)}\equiv 1(\bmod m)$。

所以任意$1\le s<\varphi(m)$，有$g^s\not\equiv 1(\bmod m)$,

故g是m的一个原根。

1.2 原根(续)

定理7　$m=2,4$，$p^l, 2p^l(l\geq 1$，p为奇素数$)$时，m 有原根，其他$m>1$情况无原根。

定理8　设$m>2$，$\varphi(m)$的所有不同素因子是q_1，$q_2, \cdots$，$q_s, (g,m)=1$，则g是m的一个原根的充分必要条件是

$$g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 (\bmod m) \qquad (i=1,2,\cdots, s)。$$

1.2 原根(续)

定理8证明.

$\rightarrow$因为g是原根，次数为$\varphi(m)$，而任意$1 \le i \le s$，

有$0 < \dfrac{\varphi(m)}{q_i} < \varphi(m)$。因此，不等同余式成立。

$\leftarrow$若不等同余式成立，假设g模m次数为$f < \varphi(m)$，

因根据推论1知$f \mid \varphi(m)$，所以$\dfrac{\varphi(m)}{f}$为大于1的整数，

故有某个素数$q_i \left| \dfrac{\varphi(m)}{f} \right.$，即$\dfrac{\varphi(m)}{f} = q_i u \Rightarrow \dfrac{\varphi(m)}{q_i} = fu$，而

$g^{\frac{\varphi(m)}{q_i}} \equiv g^{fu} \equiv 1(\bmod m)$，这与式$g^{\frac{\varphi(m)}{q_i}} \not\equiv 1(\bmod m)$矛盾。

故只能有$f = \varphi(m)$。

1.2 原根(续)

例子1 12是41的一个原根。

设$m=41$，$\varphi(41)=40=2^3 5$，$q_1=2$，

$q_2=5, 12^{20}\equiv 40\not\equiv 1(\bmod 41), 12^8\equiv 18\not\equiv 1(\bmod 41)$，

故由定理8知12是41的一个原根。

定理9 设a对模奇素数p的次数是d，$d<p-1$则

$$a^\lambda，\lambda=1,2,\cdots，d$$

都不是p的原根。

1.2 原根(续)

例子2 求出41的原根。

列出

$$1,2,\cdots,40。$$

因为2对模41的次数小于40，故在以上序列去除

2,4,8,16,32,23,5,10,20,40,39,37,33,25,9,18,36,31,21,1,

其次取3，因为3对模41的次数小于40，所以在序列中去除

3,9,27,40,38,32,14,1,

其中1,9,32,40已经去除，剩下的数的 个数刚好是$\varphi(40)$个，因此，全是原根。它们 是

6,7,11,12,13,15,17,19,22,24,26,28,29,30,34,35。

谢谢！