剩余类环的单位群

2020 年 12 月 4 日

设N是正整数,求$(\mathbb{Z}/N\mathbb{Z})^{\times}$的结构。设$N=p_1^{a_1}\cdots p_r^{a_r}$,由中国剩余定理

$$(\mathbb{Z}/N\mathbb{Z})^{\times}=(\mathbb{Z}/(p_1^{a_1}\cdots p_r^{a_r}\mathbb{Z}))^{\times}\cong\prod_{i=1}^{r}(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^{\times}.$$

于是我们只需算出$N=p^a$时$(\mathbb{Z}/N\mathbb{Z})^{\times}$的结构。

定理1：当p是奇素数,或者当$p=2,a=1$,或2时,有限Abel群$(\mathbb{Z}/p^a\mathbb{Z})^{\times}$是循环群.若$a\geq 3$,则

$$(\mathbb{Z}/2^a\mathbb{Z})^{\times}\cong(\mathbb{Z}_2,+)\oplus(\mathbb{Z}_{2^{a-2}},+).$$

证明:首先，易知$(\mathbb{Z}/p\mathbb{Z})^{\times}$是$p-1$阶循环群。取$(\mathbb{Z}/p\mathbb{Z})^{\times}$的一个生成元$g$,则$g$在$(\mathbb{Z}/p^a\mathbb{Z})^{\times}$中阶必被$p-1$整除.事实上,设$g^k\equiv 1(modp^a)$则$p^a|g^k-1$,从而$p|g^k-1$,于是$g^k\equiv 1(modp)$,但$p$是$(\mathbb{Z}/p\mathbb{Z})^{\times}$的一个生成元,从而$g$的阶为$p-1$,于是$p-1|k$.由$g^{p^{a-1}(p-1)}\equiv 1(modp^a)$知$g$在$(\mathbb{Z}/p^a\mathbb{Z})^{\times}$中阶数为$p^{a-1}(p-1)$的因数，从而设为$p^k(p-1),0\leq k\leq a-1$,于是$g^{'}=g^{p^k}$的阶数为$p-1$,令$z=1+p$,我们下面说明$z$的阶为$p^{a-1}$.

引理：设p是奇素数,$z\in Z,z\equiv 1(mod\quad p)$,若$z$有素数分解$z=p_1^{a_1}\cdots p_r^{a_r}$，定义$ord_{p_i}(z)=a_i$,即$ord_p(z)$表示$z$的素数分解中素数$p$出现的次数。

则$a)ord_p(z^p-1)=ord_p(z-1)+1$.

$b)\forall k\in\mathbb{Z}^+,ord_p(z^{p^k}-1)=ord_p(z-1)+k$.

证明：令$z=1+xp,x\in Z$,那么$ord_p(z-1)=1+ord_p(x)$,二项展开

$$z^p-1=(1+xp)^p-1=\binom{p}{1}(xp)+\binom{p}{2}(xp)^2+\cdots+\binom{p}{p-1}(xp)^{p-1}+(xp)^p.$$

由此易看出

$$ord_p(z^p-1)=ord_p(\binom{p}{1}(xp))=2+ord_p(x)=ord_p(z-1)+1.$$

$b)$用$a)$和归纳法。

应用上述引理到$z=1+p$,则$ord_p(z^{p^{k-1}}-1)=k,\forall k\in\mathbb{Z}^+$.因此$z^{p^{a-2}}\neq 1(mod\quad p^a),z^{p^{a-1}}\equiv 1(mod\quad p^a)$：即$z$在$(\mathbb{Z}/p^a\mathbb{Z})^{\times}$中的阶为$p^{a-1}$,由于$(p^{a-1},p-1)=1$,$g^{'}z$的阶为$p^{a-1}(p-1)=|(\mathbb{Z}/p^a\mathbb{Z})^{\times}|$,这就说明$(\mathbb{Z}/p^a\mathbb{Z})^{\times}$是循环群.

若$p=2$,首先易证$(\mathbb{Z}/2\mathbb{Z})^{\times},(\mathbb{Z}/4\mathbb{Z})^{\times}$是循环群。若$a\geq 3$,类似上述引理，设$z=1+2x$,则

$$z^2-1=4x^2+4x=4x(x+1)$$

若x是偶数，则

$$ord_2(z^2-1)=ord_2(4x(x+1))=ord_2(4x)=1+ord_2(2x)=1+ord_2(z-1)$$

注意到$z^2=1+2(2x(x+1))$,因此

$$ord_2((z^2)^2-1)=ord_2(z^2-1)+1=ord_2(z-1)+2$$

由此归纳下去便得到

$$ord_2(z^{2^k}-1)=ord_2(z-1)+k$$

特别地，取$x=2$,则$z=5$,于是$ord_2(5^{2^k}-1)=k+2$,因此若$a\geq 2$，则5在$(\mathbb{Z}/2^a\mathbb{Z})^\times$中阶为$2^{a-2}$。易证 2^a-1在$(\mathbb{Z}/2^a\mathbb{Z})^\times$中阶为2.注意到在$\mathbb{Z}/2^a\mathbb{Z}$中$2^a-1\equiv -1(mod 2^a)$且$5^k\equiv 1(mod 4)$对任意正整数$k$成立，因此$5^k\neq -1(mod 2^a)$,用$<5>$表示5在$(\mathbb{Z}/2^a\mathbb{Z})^\times$中生成的循环群，$<2^a-1>$表示$2^a-1$在$(\mathbb{Z}/2^a\mathbb{Z})^\times$生成的循环群,则$<5>\cap<2^a-1>=0, |<5>||<2^a-1>|=2^a$,于是

$$(\mathbb{Z}/2^a\mathbb{Z})^\times=<5>\times<2^a-1>$$

推论：$(\mathbb{Z}/N\mathbb{Z})^\times$是循环群，当且仅当$N$满足下列条件
$(i)N=1,2,4.$
$(ii)N=p^a$,这里p是奇素数.
$(iii)N=2p^a$,这里p是奇素数.
证明: 当N满足(i)或(ii)中的条件时，由上一定理知$(\mathbb{Z}/N\mathbb{Z})^\times$是循环群。
若p是奇素数，则

$$(\mathbb{Z}/2p^a\mathbb{Z})^\times\cong(\mathbb{Z}/2\mathbb{Z})^\times\times(\mathbb{Z}/p^a\mathbb{Z})^\times\cong(\mathbb{Z}/p^a\mathbb{Z})^\times$$

即$(\mathbb{Z}/2p^a\mathbb{Z})^\times$是循环群。反过来：若$N$不是上述形式,则$N$被8整除或$N$有两个不同的素数,对于第一种情形 ,$N$可以写成$N=2^aM,(2,M)=1,a\geq 3$.于是

$$(\mathbb{Z}/N\mathbb{Z})^\times\cong(\mathbb{Z}/2^a\mathbb{Z})^\times\times(\mathbb{Z}/M\mathbb{Z})^\times$$

$(\mathbb{Z}/2^a\mathbb{Z})^\times$不是循环群，因此$(\mathbb{Z}/N\mathbb{Z})^\times$不是循环群。对于第二种情形，$N$可以写成$N=p^aq^bM$,于是

$$(\mathbb{Z}/N\mathbb{Z})^\times\cong(\mathbb{Z}/p^a\mathbb{Z})^\times\times(\mathbb{Z}/q^b\mathbb{Z})^\times\times(\mathbb{Z}/M\mathbb{Z})^\times$$

由于$(\mathbb{Z}/p^a\mathbb{Z})^\times,(\mathbb{Z}/q^b\mathbb{Z})^\times$的阶都是偶数,它们的阶不是互素的,从而它们的直积不是循环群, $(\mathbb{Z}/N\mathbb{Z})^\times$不是循环群.