# 组合数学第十二讲

授课时间: 2017年12月5日 授课教师: 孙晓明 记录人: 姚依航

## 1 二次互反律的证明

**证明** 由欧拉判别准则得

$$(\frac{p}{q}) \equiv p^{\frac{q-1}{2}}(modp)$$

上节课已经证明

$$\begin{aligned}(\frac{p}{q}) &\equiv p^{\frac{q-1}{2}} \\ &\equiv (-1)^{|1\geq j\leq \frac{q-1}{2}|j\frac{p}{q}>\frac{1}{2}|} \\ &\equiv (-1)^{\sum_{j=1}^{\frac{q-1}{2}}[j\frac{p}{q}]}(modp)\end{aligned}$$

其中，{}是高斯符号，表示取符号内该数的小数部分,则

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}}[j\frac{p}{q}]+\sum_{i=1}^{\frac{p-1}{2}}[i\frac{p}{q}]}$$

下证：

$$\sum_{j=1}^{\frac{q-1}{2}}[j\frac{p}{q}] + \sum_{i=1}^{\frac{p-1}{2}}[i\frac{p}{q}] = \frac{(p-1)(q-1)}{4}$$

□

## 2 费马素数定理

**定理 1.** 对于一个素数$p$，$\exists x, y \in \mathbb{Z}$,使得$p = x^2 + y^2 \iff p$是$4k + 1$型素数.
例：3不满足，5=$1^2 + 2^2$,且5是$4k + 1$型素数，7不满足，11不满足，$13 = 2^2 + 3^2$

**证明** $1^o$若

$$p = x^2 + y^2$$

则

$$x^2 + y^2 \equiv 0(modp)$$

即

$$x^2 \equiv -y^2(modp)$$

由$y \neq 0$得$y$可逆,则

$$x^2y^{-2} \equiv -1(modp)$$

故

$$(xy^{-1})^2 \equiv -1(modp)$$

即$-1$是p的二次剩余

即

$$(\frac{-1}{p})=1$$

由上节课证明的定理p是$4k+1$型素数$\Longleftrightarrow (\frac{-1}{p})=1$得，

p是$4k+1$型素数 □

**例1** 什么样的素数$p$, 能够写成两个整数$x,y$的平方和, 即$p=x^2+y^2$的形式?

首先, 考虑几个简单的例子:

$p=3$时, 不存在满足条件的$x,y$.

$p=5$时, $5=1^2+2^2$.

$p=7$时, 不存在满足条件的$x,y$.

$p=11$时, 不存在满足条件的$x,y$.

$p=13$时, $13=2^2+3^2$.

...

通过上面的例子我们可以不完全归纳出: $4k+1$型素数能够写成两个整数的平方和, $4k+3$型素数不能够写成两个整数的平方和.

为什么$4k+3$型素数不能写成两个整数的平方和?

**证明** $p$是$4k+3$型素数, 若$p$能写成两个整数的平方和的形式, 则$\exists x,y$

$$x^2+y^2\equiv 0(modp)$$

即

$$x^2\equiv -y^2(modp)$$

在素域$mathbbZ_p$上, $y$有逆. 因此

$$(xy^{-1})^2\equiv -1(modp)$$

但由勒让德符号

$$(\frac{-1}{p})=-1$$

即$-1$不是$p$的二次剩余, 与$(xy^{-1})^2\equiv -1(modp)$矛盾, 故$p=4k+3$型素数不满足条件. □

为什么$4k+1$型素数一定能写成两个整数的平方和?

**证明** $p$是$4k+1$型素数, 由勒让德符号

$$(\frac{-1}{p})=1$$

得: $\exists z\in\mathbb{N}$, 使$z^2\equiv -1(modp)$ 考虑集合$A=(a,b)|a\le a,b\le[\sqrt{p}]$ 得

$$|A|=([\sqrt{p}]+1)^2>(\sqrt{p})^2=p$$

对$\forall(a,b)\in A$, 考虑$a+bz(modp)$ 因为$|\mathbb{Z}_p|=p-1$, 而$(a,b)$有$p$组, 所以

$$\exists(a_1,b_1),(a_2,b_2)\in A, a_1+b_1z\equiv a_2+b_2z(modp)$$

即$(a_1-a_2)\equiv z(b_2-b_1)(modp)$, 对等式两边同时平方由$z^2\equiv -1(modp)$得到

$$(a_1-a_2)^2\equiv -(b_1-b_2)^2(modp)$$

即

$$(a_1-a_2)^2+(b_1-b_2)^2\equiv 0(modp)$$

即

$$p|(a_1-a_2)^2+(b_1-b_2)^2$$

由$(a_1,b_1),(a_2,b_2)$的选取可得

$$(a_1-a_2)_{max}=(b_1-b_2)_{max}=[\sqrt{p}]$$

$$0<(a_1-a_2)^2+(b_1-b_2)^2\leq([\sqrt{p}])^2+([\sqrt{p}])^2<2p$$

在0到$2p$之间能够被$p$整除的整数只有$p$, 所以

$$(a_1-a_2)^2+(b_1-b_2)^2=p$$

即对$4k+1$型素数, 一定能写成两个整数的平方和. □

**例2** 类似的, 我们可以考虑什么样的素数$p$能够写成$x^2+2y^2$的形式?

首先, 考虑几个简单的例子: $p=3$时, $3=1^2+2\cdot 1^2$.

$p=5$时, 不存在满足条件的$x,y$.

$p=7$时, 不存在满足条件的$x,y$.

$p=11$时, $11=3^2+2\cdot 1^2$.

...

通过上面的例子我们可以推断$8k+3$型素数可以写成$x^2+2y^2$的形式. 接下来我们进行证明.

**证明** $p$是$8k+3$型素数, 由勒让德符号

$$(\frac{-2}{p})=1$$

得: $\exists z\in\mathbb{N}$, 使$z^2\equiv -2(modp)$ 考虑集合$A=(a,b)|a\leq a,b\leq[\sqrt{p}]$ 得

$$|A|=([\sqrt{p}]+1)^2>(\sqrt{p})^2=p$$

对$\forall(a,b)\in A$, 考虑$a+bz(modp)$ 因为$|\mathbb{Z}_p|=p-1$, 而$(a,b)$有$p$组, 所以

$$\exists(a_1,b_1),(a_2,b_2)\in A, a_1+b_1z\equiv a_2+b_2z(modp)$$

即$(a_1-a_2)\equiv z(b_2-b_1)(modp)$, 对等式两边同时平方由$z^2\equiv -2(modp)$得到

$$(a_1-a_2)^2\equiv -2(b_1-b_2)^2(modp)$$

即

$$(a_1-a_2)^2+2(b_1-b_2)^2\equiv 0(modp)$$

即

$$p|(a_1-a_2)^2+2(b_1-b_2)^2$$

由$(a_1,b_1),(a_2,b_2)$的选取可得

$$(a_1-a_2)_{max}=(b_1-b_2)_{max}=[\sqrt{p}]$$

$$0 < (a_1 - a_2)^2 + 2(b_1 - b_2)^2 \leq ([\sqrt{p}])^2 + 2([\sqrt{p}])^2 < 3p$$

在0到$3p$之间能够被$p$整除的整数只有$p$和$2p$. $1^o$若$(a_1 - a_2)^2 + 2(b_1 - b_2)^2 = p$, 则命题得证. $2^o$若$(a_1 - a_2)^2 + 2(b_1 - b_2)^2 = 2p$, 将该等式模2得

$$(a_1 - a_2)^2 \equiv 0(modp)$$

所以, $a_1 - a_2$能被2整除, 则

$$(b_1 - b_2)^2 + a(\frac{a_1 - a_2}{2})^2 = p$$

命题得证. □

## 3 抽屉原理/鸽巢原理(Pigeonhole's Principle)/Dirichlet's Principle

**定理 2.** *原理1：把多于n+1个的物体放到n个抽屉里，则至少有一个抽屉里的东西不少于两件*

*原理2：把多于mn(m乘n)+1（n不为0）个的物体放到n个抽屉里，则至少有一个抽屉里有不少于（m+1）个物体。*

**例3** S=1,2,3...100,从中取51个数,则$\exists a, b \in S$,使得$gcd(a, b) = 1$

**证明** 把相邻的两个数$1, 2, 3, 4...99, 100$看作一个抽屉，共50组

取了51个数，则一定存在两个数在同一个组里，则这两个数相邻

又相邻两数互素，故$\exists a, b \in S$,使得

$$gcd(a, b) = 1$$

又，51是满足此条件的最小的数字

反例：取50个数,若取的是$2, 4, 6, ...100$,不符合条件. □

**例4** $n$个人中一定两个人具有相同的朋友个数

图论的语言：对于图$G(V, E)$, $\exists u, v \in V$,,使得$deg(u) = deg(v)$

**证明** 每个人可能有的朋友个数：$0, 1, 2...n - 1$,将每个人可能有的朋友个数看作抽屉.

若一个人有0个朋友，则该人是一个孤立的点，剩下的人都不可能有$n - 1$个朋友,即$n - 1$和0不能同时出现

相当于共有$n - 1$个抽屉，共n个人，

故一定有两个人有相同的朋友数

□

**例5** 对于$a_1, a_2, a_3...a_n \in \mathbb{Z}$，一定存在子集$a_{i_1}, a_{i_2}...a_{i_k}$,使得$n|(a_{i_1} + a_{i_2} + ... + a_{i_k})$

**证明** 考虑前缀和$S_1 = a_1, S_2 = a_1 + a_2, ...S_j = a_1 + a_2 + ...a_j, ...$ 考虑$n = 100$

$$S_1, S_2...S_100(mod100) \in 0, 1, 2..., 99$$

若余数为0,则显然成立

若余数不为0,100个前缀和模100的余数至少有99种可能，则$\exists i < j$使得

$$S_i \equiv S_j(mod100)$$

$$100|(S_i - S_j)$$

其中

$$S_i - S_j = a_{i_1} + a_{i_2} + ... + a_{i_k}$$

故存在子集$a_{i_1}, a_{i_2}...a_{i_k}$,使得

$$n|(a_{i_1} + a_{i_2} + ... + a_{i_k})$$

证明100是满足此条件的最小数字反例：5若$n$是99,取99个1,不符合条件 □

**例6** 设$a_i$表示第$i$天做$n$道题, 连续做60天, 做的题数满足$\forall i, a_i \geq 1$, 且$\sum_{i=1}^{30} a_i \leq 50, \sum_{i=31}^{60} a_i \leq 50$, 证明: 一定存在若干天, 在这些天做的总题数为19道.

**证明** 考虑前缀和序列$S_i, 1 \leq i \leq 60, S_i = \sum_{k=1}^{i} a_i$, 由$\forall i, a_i \geq 1$, 且$\sum_{i=1}^{30} a_i \leq 50, \sum_{i=31}^{60} a_i \leq 50$, 可以得到

$$1 \leq S_1 < S_2 < \cdots < S_{60} \leq 100$$

对前缀和序列的每一项加上19, 可以得到

$$20 \leq S_1 + 19 < s_2 + 19 < \cdots < S_{60} + 19 \leq 119$$

则$S_i$和$S_i + 19$两个序列共有120项, 但最多有119个不同的数字, 由鸽巢原理

$$\exists i, j, i > j, S_i = S_j + 19$$

即

$$S_i - S_j = \sum_{k=1}^{i} a_i - \sum_{k=1}^{j} a_i = \sum_{k=i+1}^{j} a_i = 19$$

因此一定存在若干天, 即第$i+1$天到第$j$天, 在这些天做的总题数为19道. □

事实上, 我们证明的是一个更强的结果, 即一定存在连续的若干天, 在这些天做的总题数为19道.

接下来我们考虑一个有趣的问题.

**例7** 一定可以从50名身高互不相同的同学中找到8名同学, 随学号增大, 他们的身高逐渐增加或者逐渐减小.

**证明** 将这50个同学按学号递增的顺序进行排序, 第$i$个学生学号为$N_i$, 对应的身高为$h_i$, 则有$N_1 < N_2 < \cdots < N_50$. 设$L_i$表示从第$i$个同学开始的最大身高递增列的长度, 则$L_i \geq 1$.

若存在$L_i] \geq 8$, 则找到了8名学生满足条件.

若不存在$L_i] \geq 8$, 则$\forall i, 1 \leq L_i < 8$. 由鸽巢原理, 一定存在8名学生, 从他们开始最大的身高递增列长度相等. 即

$$\exists k_1, k_2, \cdots, k_8, k_1 < k_2 < \cdots < k_8, L_{k_1} = L_{k_2} = \cdots = L_{k_8}$$

可以断言

$$h_{k_1} > h_{k_2} > \cdots > h_{k_8}$$

否则, 存在$k_i$和$k_j$,$k_i < k_j$, $h_{k_i} < h_{k_j}$.

则从第$k_i$个同学开始, 将第$k_i$个同学和从第$k_j$个同学开始的最大升高递增列相连可以获得一个长度大于$L_{k_i}$的身高递增列, 这与$L_{k_i}$的选取矛盾. 因此, 我们找到了一个满足条件的身高递减序列.

命题得证. □