组合数学第十一讲

授课时间: 2017年11月27日 授课教师: 孙晓明 记录人: 李奉治 万之凡

1 二次剩余(Quadratic Residue)

上节课在证明$4k+1$型素数无穷时，我们引入了二次剩余的概念.

二次剩余 对于一个素数p，称a是模p的一个二次剩余，当且仅当存在一个b，使得:

$$b^2 \equiv a \pmod p \quad a, b \in \mathbb{Z}_p$$

为了方便表示，我们引入勒让德符号(Legendre Symbol):

勒让德符号 对于一个素数p，a为$\mathbb{Z}_p$中的元素，则记号$(\frac{a}{p})$定义为:

$$(\frac{a}{p}) = \begin{cases} 1 & \text{if} \quad a \not\equiv 0 \pmod p, \ \exists b \in \mathbb{Z}_p, \ s.t. \ b^2 \equiv a \pmod p \\ -1 & \text{if} \quad a \not\equiv 0 \pmod p, \ \nexists b \in \mathbb{Z}_p, \ s.t. \ b^2 \equiv a \pmod p \\ 0 & \text{if} \quad a \equiv 0 \pmod p \end{cases}$$

在上节课证明$4k+1$型素数无穷的过程中，最关键的一步即为证明，对于$4k+3$型素数，不存在x，使得$x^2+1 \equiv 0 \pmod p$. 利用勒让德符号重述，即需证明$(\frac{-1}{p}) = -1$.

证明 使用反证法，假设$(\frac{-1}{p}) = 1$，即可推出$\exists b \in \mathbb{Z}_p$，满足$b^2 \equiv -1 \pmod p$.将等式两侧同取$\frac{p-1}{2}$ 次方(素数p为$4k+3$型保证了$\frac{p-1}{2}$ 是整数)，可以得到：

$$(b^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

等式左侧由费马小定理可得：

$$(b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p$$

而等式右侧：

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{4k+3-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

等式两侧$1 \not\equiv -1 \pmod p$，矛盾，原假设失效，$(\frac{-1}{p}) = -1$.证毕. □

由此，即可完成$4k+1$型素数无穷的证明过程.

2 欧拉判别准则(Euler Criterion)

上述的证明过程提醒我们，$(\frac{a}{p})$有其他的计算方法.这里我们给出欧拉判别准则：

定理 1. 对于一个奇素数p，$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod p \quad (a \not\equiv 0 \pmod p))$.

在进行证明之前值得思考，我们已知上述等式左侧的值为1或-1，那么等式右侧$a^{\frac{p-1}{2}}$的值是否也为1或-1 呢？

由费马小定理可知，$a^{p-1} \equiv 1 \pmod p$，故$p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1)$. 其中$p$为奇素数，则$\frac{p-1}{2}$是整数，$p \mid a^{\frac{p-1}{2}} + 1$或$p \mid a^{\frac{p-1}{2}} - 1$.因此，当$p \mid a^{\frac{p-1}{2}} + 1$ 时，$a^{\frac{p-1}{2}} \equiv -1 \pmod p$；当$p \mid a^{\frac{p-1}{2}} - 1$时，$a^{\frac{p-1}{2}} \equiv 1 \pmod p$。这说明$a^{\frac{p-1}{2}}$的值也为1或$-1$.

为了证明欧拉判别准则，我们先简述两个引理：

引理2. 如果$(\frac{a}{p})=1$，$(\frac{b}{p})=1$，则$(\frac{ab}{p})=1$.

证明 $(\frac{a}{p})=1$说明存在$x\in\mathbb{Z}_p$，满足$x^2\equiv a \pmod p$. $(\frac{b}{p})=1$说明存在$y\in\mathbb{Z}_p$，满足$y^2\equiv b \pmod p$. 此时$x^2y^2\equiv(xy)^2\equiv ab \pmod p$，这说明$(\frac{ab}{p})=1$. □

引理3. 如果$(\frac{a}{p})=1$，$(\frac{b}{p})=-1$，则$(\frac{ab}{p})=-1$.

证明 使用反证法.若$(\frac{ab}{p})=1$，即存在$x\in\mathbb{Z}_p$，满足$x^2\equiv ab \pmod p$. 而$(\frac{a}{p})=1$说明存在$y\in\mathbb{Z}_p$，满足$y^2\equiv a \pmod p$. 因此$b\equiv x^2\cdot a^{-1}\equiv x^2\cdot(y^2)^{-1}\equiv(x\cdot y^{-1}) \pmod p$，即$(\frac{b}{p})\equiv -1 \pmod p$，矛盾，原假设失效，$(\frac{ab}{p})=-1$. □

使用上述两个引理，我们对欧拉判别准则进行证明：

证明

Case 1: 如果$(\frac{a}{p})=1$，则说明存在$x\in\mathbb{Z}_p$，满足$a\equiv x^2 \pmod p$. 因此$a^{\frac{p-1}{2}}\equiv b^{p-1}\equiv 1 \pmod p$.即可证得当前情况下$(\frac{a}{p})\equiv a^{\frac{p-1}{2}} \pmod p$.

Case 2: 如果$(\frac{b}{p})=-1$，我们需证明$(\frac{b}{p})\equiv -1 \pmod p$.

定义二次剩余的集合$A=\{a\mid(\frac{a}{p})=1\}$，如果存在某个$b\in\mathbb{Z}_p$，则用$b$乘上$A$中的每个元素，利用引理2，得到一个二次非剩余的集合$bA=\{ab\mid(\frac{a}{p})=1\}$，这个集合的大小与$A$ 的大小相等.这说明二次非剩余集合$B=\{b\mid(\frac{b}{p})=-1\}$ 的大小应大于A 的大小.更进一步，应为A集合大小的整数倍.

为考察二次剩余集合的具体大小，对于一个奇素数p，我们考察1到$p-1$.

可以证明，$1^2,2^2,\cdots,(\frac{p-1}{2})^2$都是互不相同的$p$的二次剩余.这是因为$\forall i,j\in 1,2,\cdots,\frac{p-1}{2}$，若$i\neq j$，不妨令$j>i$，则$j^2-i^2=(j-i)(j+i)$，其中$j-i>0$，$(j+i)<p-1$，故$j^2-i^2\neq 0$，$i^2\neq j^2$.

继续考察$\frac{p+1}{2},\frac{p+3}{2},\cdots,p-1$，易知

$$(\frac{p+1}{2})^2\equiv(p-\frac{p-1}{2})^2\equiv(\frac{p-1}{2})^2 \pmod p$$
$$(\frac{p+3}{2})^2\equiv(p-\frac{p-3}{2})^2\equiv(\frac{p-3}{2})^2 \pmod p$$
$$\cdots$$
$$(p-1)^2\equiv 1^2 \pmod p$$

这说明$|A|=\frac{p-1}{2}$，因此$|B|=\frac{p-1}{2}$，$|A|=|B|$.这样我们就可以得到$b\cdot A\equiv B \pmod p$，将等式两侧集合中的元素求积，得到等式：

$$b^{\frac{p-1}{2}}\cdot\sum_{x\in A}x\equiv\sum_{y\in B}y \pmod p$$

而$A\cup B$恰为1至$p-1$的所有元素，利用定理$(p-1)!\equiv -1 \pmod p$(留作作业自证)，可得：

$$b^{\frac{p-1}{2}}\equiv(\sum_{x\in A}x)^{-1}\cdot(\sum_{y\in B}y)\equiv\sum_{x\in A}x\cdot\sum_{y\in B}y\equiv(p-1)!\equiv -1 \pmod p$$

Case 2得证

综合**Case 1**和**Case 2**，命题得证，$(\frac{a}{p})\equiv a^{\frac{p-1}{2}} \pmod p \quad (a\not\equiv 0 \pmod p)$. □

3 对$(\frac{2}{p})$求解

先用一个例子进行计算

例1 求$(\frac{2}{19})$.

解 模仿上一部分的证明，我们计算$2\times4\times6\times8\times10\times12\times14\times16\times18\equiv2^9\cdot9! \pmod{19}$ 而$10\equiv-9 \pmod{19}, 12\equiv-7 \pmod{19}, 14\equiv-5 \pmod{19}, 16\equiv-3 \pmod{19}, 18\equiv-1 \pmod{19}$，故可以得到：

$$2\times4\times6\times8\times10\times12\times14\times16\times18\equiv2\times4\times6\times8\times(-9)\times(-7)\times(-5)\times(-3)\times(-1)\equiv(-1)^5\cdot9! \pmod{19}$$

因此$2^9\cdot9!\equiv(-1)^5\cdot9!$，进而得出$(\frac{2}{19})\equiv2^9\equiv-1 \pmod{p}$

类似的，我们为下述定理给出证明：

定理 4. 对于一个奇素数p,$k\in\mathbb{N}$

$$(\frac{2}{p})=\begin{cases}1 & if \quad p=8k+1\ or\ 8k+7,\ k\in\mathbb{N}\\ -1 & if \quad p=8k+3\ or\ 8k+5,\ k\in\mathbb{N}\end{cases}$$

证明 模仿例1，进行计算:

$$2\times4\times\cdots\times(2(\frac{p-1}{2}))=2^{\frac{p-1}{2}}\cdot(\frac{p-1}{2})!$$

同时

$$2\times4\times\cdots\times(2(\frac{p-1}{2}))=(\sum_{i:2i<\frac{p}{2}}2i)\cdot(\sum_{j:2j>\frac{p}{2}}(p-2j))=(\frac{p-1}{2})!\cdot(-1)^{\#\{j|2j>\frac{p}{2}\}}$$

比较两个结果可得：

$$2^{\frac{p-1}{2}}\equiv(-1)^{\#\{j|2j>\frac{p}{2}\}} \pmod{p},\ 1\leq j\leq\frac{p-1}{2}$$

单独讨论-1的指数：

$$\#\{j\mid 2j>\frac{p}{2}\}=\frac{p-1}{2}-\#\{j\mid 2j\leq\frac{p}{2}\}=\frac{p-1}{2}-\#\{j\mid j\leq\frac{p}{4}\}=\frac{p-1}{2}-[\frac{p}{4}]$$

因此

$$(\frac{2}{p})\equiv2^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}-[\frac{p}{4}]}\equiv\begin{cases}1 & \text{if} \quad p=8k+1\ or\ 8k+7,\ k\in\mathbb{N}\\ -1 & \text{if} \quad p=8k+3\ or\ 8k+5,\ k\in\mathbb{N}\end{cases}$$

定理证毕. □