二次剩余笔记

BY AYANAMISTS

1 二次剩余的定义

定义 1. 一个整数p是另一个整数q的二次剩余， 当且仅当

$$\exists x, x^2 \equiv p \pmod q$$

在这个定义中， *0*作为代表元的剩余类是被包括的。但为方便起见，*我们下面的讨论均排除0作为代表元的剩余类。*

这里的x是需要进一步解释的。我们有

$$(x+kq)^2 = x^2 + 2kqx + q^2$$

所以

$$(x+kq)^2 \equiv x^2 \pmod q$$

这也就是说， 我们真正要找到的x是一个*剩余类的代表元*， 只要这个代表元不与p同余于q， 那么整个剩余类中的元素都不与p同余于q， 反之亦然。

2 对奇素数的二次剩余

2.1 判断是否二次剩余的方法

考虑这个同余方程

$$x^2 \equiv p \pmod q$$

我们如果想知道， 对于给定的q和p，p是不是q的二次剩余， 该怎么做呢？

首先， 在之前的学习中我们多次使用了**唯一分解定理**， 知道把问题a变成「对素数的情况」是非常有用的， 而且由于**唯一分解定理**的存在， 我们往往最终可以得到一般的情况。所以， 对于这个问题，我们首先要研究q是素数的情况。

一个很有意思的问题是， 上面的二次同余方程『为什么』会没有解。没有解， 也就是说，

$$\forall x, x^2 \not\equiv p \pmod q$$

显然地，$[p \pmod q]$是一个模q的**剩余类**， 自然存在x属于这个剩余类。但是， 却不一定存在x^2属于这个剩余类， 这说明下面这个函数

$$\operatorname{square}(x) = x^2 \bmod q, x \in [0, q-1]$$

有两个特性：

- 它的值域是定义域的**真子集**
- 它不是一个**单射**， 也就是说， 存在$x_1 \neq x_2, \operatorname{square}(x_1) = \operatorname{square}(x_2)$

实际上， 我们立刻就会联系到二次函数的特征：

$$f(x)=f(-x)$$

上面的square函数没有x为负时的定义， 但这是我们强行限制的， 可以搞一个新函数：

$$\text{square}'(x)=x^2 \bmod q, x\in Z$$

当$x\in[0,q-1]$时， 有：

$$\text{square}(x)=\text{square}'(x)$$

对于这个square$'$函数， 注意到一个事实：

$$\begin{aligned}\text{square}'(-1) &= \text{square}'(1)\\ \text{square}'(-1) &= \text{square}'(q-1)\end{aligned}$$

这就会导致

$$\text{square}'(1)=\text{square}(q-1)$$

也就是

$$\text{square}(1)=\text{square}(q-1)$$

类似地， 我们有

$$\begin{aligned}\text{square}(2) &= \text{square}(q-2)\\ \text{square}(3) &= \text{square}(q-3)\\ &\cdots\\ \text{square}\left(\frac{q-1}{2}\right) &= \text{square}\left(\frac{q+1}{2}\right)\end{aligned}$$

因为q是奇素数， 所以$\frac{q-1}{2}$一定是一个整数， 这也就是说， 从1到$q-1$的集合可以分为两个交集为$\varnothing$的集合：

$$\begin{aligned}A &= \left\{a|1\leqslant a\leqslant\frac{q-1}{2}\right\}\\ B &= \left\{b|\frac{q+1}{2}\leqslant b\leqslant q-1\right\}\end{aligned}$$

它们的元素数为：

$$\begin{aligned}|A| &= \frac{q-1}{2}\\ |B| &= \frac{q-1}{2}\end{aligned}$$

把A和B按从小到大的顺序排序， 记从0开始的第i个元素为：

$$\begin{gathered}a_i\\ b_i\end{gathered}$$

我们有：

$$\text{square}(a_i)=\text{square}(b_i)$$

考虑所有的$\text{square}(x)$的值构成的集合S， 我们有：

$$S=\left\{x|x=\text{square}(a_i),i\in\left[1,\frac{q-1}{2}\right]\right\}$$

这说明：

$$|S|\leqslant|A|=\frac{q-1}{2}$$

而集合S， 正是**所有对q二次剩余的p构成的集合。**

这样一来， 我们就真正地想明白了『为什么』会存在二次非剩余。因为集合S最多有$\frac{q-1}{2}$个元素， 所有的剩余类却有$q-1$个， 所以至少有$\frac{q-1}{2}$个元素是二次非剩余q的。

那么， 能不能进一步找到所有的二次剩余与二次非剩余构成的集合呢？

现在真正的问题是， 在$\text{square}(1),\text{square}(2),\text{square}(3)\ldots\text{square}\left(\frac{q-1}{2}\right)$中， 有多少**相同**的元素。

这时使用q是奇素数的条件。考虑$i\in\left[1,\frac{q-1}{2}\right],j\in\left[1,\frac{q-1}{2}\right],i\neq j$:

假设有

$$\text{square}(i)=\text{square}(j)$$

即

$$i^2\equiv j^2\ (\text{mod}\ q)$$

学过一点数论的人都会知道这是不成立的。

所以， 对于奇素数q而言， 集合S的元素数为$\frac{q-1}{2}$. 这就得到了定理2.

定理 2. *设q是奇素数， 在模q的简化剩余系中， 恰有$\frac{q-1}{2}$个模q二次剩余，$\frac{q-1}{2}$个模p非剩余， 如果p是q的二次剩余，则$x^2\equiv p\ (\text{mod}\ q)$的解数为2*

这样一来， 我们就得到了模q的二次剩余集合S的元素数量。我们也知道它就是$\text{square}(1),\text{square}(2),\text{square}(3)\ldots\text{square}\left(\frac{q-1}{2}\right)$这些值。可是， 对于一个确定的$p$， 我们只能遍历集合$S$来查找它是否在集合$S$中吗？ 答案是否定的。

费马小定理告诉我们， 如果$x\nmid q$， 那么：

$$x^{q-1}\equiv 1\ (\text{mod}\ q)$$

所以对于任意的$i\in\left[1,\frac{q-1}{2}\right]$,有：

$$(\text{square}(i))^{\frac{q-1}{2}}\equiv 1\ (\text{mod}\ q)$$

这也就是说， 如果p是模q的二次剩余， 那么一定有：

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

问题是， 如果有$p^{\frac{q-1}{2}}\equiv 1\ (\text{mod}\ q)$，那么$p$是否一定是模$q$的二次剩余呢？

用形式化的语言叙述一下， 就会是这样：

$$\exists p,\left(p^{\frac{q-1}{2}}\equiv 1\ (\text{mod}\ q)\right)\wedge(\forall x,x^2\not\equiv p\ (\text{mod}\ q))$$

要回答这个问题， 我们就不得不考察一下$p^{\frac{q-1}{2}}$这个式子。我们实际地计算一下：

对于$q=5$的情况：

$$\begin{aligned}1^2 &= 1 \pmod 5\\ 2^2 &= -1 \pmod 5\\ 3^2 &= -1 \pmod 5\\ 4^2 &= 1 \pmod 5\end{aligned}$$

这不由得让人猜测，$p^{\frac{q-1}{2}}$这个式子， 是否只会属于两个模q的剩余类， 即$[1]$和$[-1]$呢？ 再次考虑一下费马小定理：

$$p^{q-1}\equiv 1 \pmod q$$

我们发现：

$$p^{\frac{q-1}{2}}\equiv \pm\sqrt{p^{q-1} \pmod q} = \pm 1 \pmod q$$

所以它的确只会属于代表元为1和-1的这两个模q的剩余类。不过， 这只是说明了它确实可以与-1同余， 没有给出它与-1同余的『理由』， 或者说， 有什么结构使得它与-1同余。

刚刚我们已经得出了一个结论， 那就是：

$$p\text{是模}q\text{的二次剩余}\rightarrow p^{\frac{q-1}{2}}\equiv 1 \pmod q$$

能不能类似地给出这个结论呢：

$$p\text{是模}q\text{的二次非剩余}\rightarrow p^{\frac{q-1}{2}}\equiv -1 \pmod q$$

Wilson定理告诉我们：

$$(q-1)!\equiv -1 \pmod q$$

如果上面的构造是成立的， 那么就会有这个构造：

$$p\text{是模}q\text{的二次非剩余}\rightarrow p^{\frac{q-1}{2}}\equiv (q-1)! \pmod q$$

我们就尝试构造一下

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

要构造这种结构， 一般来说都是要构造

$$a_i a_j\equiv p \pmod q$$

其中$i\neq j, i\in[1,q-1], j\in[1,q-1]$

而这个构造是不难的， 因为我们可以将上式看作一个线性同余方程， 其中

$$\begin{aligned}a &= a_i\\ x &= a_j\\ ax &\equiv p \pmod q\end{aligned}$$

这个方程是有解的， 因为

$$a_i \nmid q$$

这个方程的解可能是$x\equiv a \pmod q$吗？

如果可能的话， 我们有

$$a^2\equiv p \pmod q$$

恰恰就是二次剩余的形式！

我们假设p是模q的二次非剩余， 那么上面对方程的讨论就可以表示为这样的逻辑语言：

$$\forall a_i, \exists a_j, i\neq j, a_i a_j\equiv p \pmod q$$

我们任取$\frac{q-1}{2}$个a_i， 放在集合I中， 对应的$\frac{q-1}{2}$个a_j放在集合J中。如果我们可以证明

$$|I\cup J| = q-1$$

那么证明就完成了。

现在我们有：

$$\begin{aligned} |I| &= \frac{q-1}{2} \\ I\cap J &= \varnothing \end{aligned}$$

所以我们需要证明：

$$|J| = \frac{q-1}{2}$$

也就是说要证明J中没有重复元素。

形式化地写出：

$$\forall a_i, a_k, a_j, a_j a_i\equiv p \pmod q \rightarrow a_j a_k \not\equiv p \pmod q$$

而这是显然的， 因为以下两个同余方程会有相同的解：

$$\begin{aligned} ax &= p \pmod q \\ ax' &= p \pmod q \end{aligned}$$

所以， 我们可以证明，

$$p\text{是模}q\text{的二次非剩余} \rightarrow p^{\frac{q-1}{2}} \equiv (q-1)! \pmod q \equiv -1 \pmod q$$

这实际上是

$$p^{\frac{q-1}{2}} \equiv 1 \pmod q \rightarrow p\text{是模}q\text{的二次剩余}$$

的逆反命题。

至此， 我们已经得到了著名的**欧拉判别法**：

定理 3. (欧拉) 对于任意的奇整数q， 任意的整数p，

如果有

$$p^{\frac{q-1}{2}} \equiv 1 \pmod q$$

那么， p是q的二次剩余。

如果有

$$p^{\frac{q-1}{2}} \equiv -1 \pmod q$$

那么，p是q的二次非剩余。

2.2 勒让德符号

我们之前一直在用『p是q的二次剩余』,『p是q的二次非剩余』这种自然语言来描述二次剩余，但实际上，用符号描述会更好一点。如果我设计的话，我会设计成s表达式的样子：

```
(quad-res p q)
```

但是，数学家们喜欢用各种奇奇怪怪的符号描述这些东西。我们不得不遵循这些数学家的习惯。勒让德符号就是这些数学家用来描述二次剩余的符号：

$$\left(\frac{p}{q}\right) = \begin{cases} 1\text{，如果}p\text{是}q\text{的二次剩余} \\ -1\text{，如果}p\text{是}q\text{的二次非剩余} \\ 0\text{，如果}p \mid q \end{cases}$$

或者说：

$$\left(\frac{p}{q}\right) = p^{\frac{q-1}{2}} \pmod q$$

有人可能会问了，提出这种套皮符号，究竟有什么意义？我们会在接下来的学习中解决这个问题。

2.3 勒让德符号的约化

1. $\left(\frac{p+q}{q}\right) = \left(\frac{p}{q}\right)$

2. $\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$，这是因为 $(ab)^{\frac{q-1}{2}} = (a)^{\frac{q-1}{2}}(b)^{\frac{q-1}{2}}$

3. $\left(\frac{a^2}{q}\right) = \left(\frac{a}{q}\right)^2$

2.4 高斯引理

2.4.1 定理与证明

我们能不能对

$$p^{\frac{q-1}{2}} \pmod q$$

这个式子作进一步约化？

能不能找到一个$a = f(p, q)$，使得

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

高斯引理告诉我们，这样的寻找是可能的。

引理 4. (高斯) 考虑一个$N^2 \to N$的函数$count$， 定义如下:

$$\operatorname{count}(p,q) = \left| \left\{ x \middle| \left(x = pi \bmod q, i \in \left[1, \frac{q-1}{2}\right], i \in N \right) \wedge \left(x \geqslant \frac{q+1}{2} \right) \right\} \right|$$

我们有

$$p^{\frac{q-1}{2}} \pmod q \equiv (-1)^{\operatorname{count}(p,q)}$$

同样地， 我们给出一个$p=3, q=5$时的例子：

$$\begin{aligned} 3 \bmod 5 &= 3 \geqslant 3 \\ (3 \times 2) \bmod 5 &= 1 < 3 \end{aligned}$$

这样会有

$$\operatorname{count}(3,5) = 1$$

而

$$3^2 \equiv (-1)^1 \pmod 5$$

要搞清楚这个引理究竟在讲什么、 如何证明它， 我们需要仔细考察一下这个集合：

$$C = \left\{ x | x = pi \bmod q, i \in \left[1, \frac{q-1}{2}\right], i \in N \right\}$$

或者说

$$C = \left\{ p \bmod q, 2p \bmod q, 3p \bmod q, 4p \bmod q, \ldots, \frac{q-1}{2} p \bmod q \right\}$$

第一个问题是， 它的元素个数是多少个？

如果没有重复， 那么显然有

$$|C| = \frac{q-1}{2}$$

要证明没有重复是很简单的， 因为q是奇素数， 如果$p \nmid q$， 那么就有$(p,q)=1$. 而如果存在i,j使得$i \neq j$且

$$ip \equiv jp \pmod q$$

两边乘以p的逆元， 有

$$i \equiv j \pmod q$$

这显然不成立。

我们记

$$D = \left\{ x \middle| \left(x = pi \bmod q, i \in \left[1, \frac{q-1}{2}\right], i \in N \right) \wedge \left(x \geqslant \frac{q+1}{2} \right) \right\}$$

显然有$D \subset C$， 构造一个新集合E， 满足

$$E = \left\{ x | x = \left\{ \begin{array}{l} t, t \in C, t \notin D \\ q - t, t \in D \end{array} \right. \right\}$$

这个集合会有一些有趣的性质。

首先， 它仍然是无重复的。要证明这一点并不难， 假设存在$t_1 \in C-D, t_2 \in D$， 使得

$$t_1 \equiv q - t_2 \pmod q$$

我们知道

$$\begin{aligned} t_1 &\equiv ip \pmod q \\ t_2 &\equiv jp \pmod q \end{aligned}$$

带入上式， 可以得到：

$$\begin{aligned} ip &\equiv q - jp \pmod q \\ p\,(i+j) &\equiv q \pmod q \\ p\,(i+j) &\equiv 0 \pmod q \\ (i+j) &\equiv 0 \pmod q \\ q &\mid i+j \end{aligned}$$

而这是不可能的， 因为$i \in \left[1, \frac{q-1}{2}\right], j \in \left[1, \frac{q-1}{2}\right], i+j \in [2, q-1]$

所以有

$$|E| = \frac{q-1}{2}$$

实际上，E这个集合有：

$$\forall x \in E, x \leqslant \frac{q-1}{2}$$

所以E这个集合就是$\left\{1, 2, 3, 4, \ldots, \frac{q-1}{2}\right\}$.

记

$$\begin{aligned} c_i &\in C - D \\ d_i &\in D \end{aligned}$$

把E中所有的元素乘起来并模q， 我们会得到：

$$\begin{aligned} \Pi c_i \Pi (q - d_i) &\equiv \left(\frac{q-1}{2}\right)! \pmod q \\ \Pi c_i \Pi (-d_i) &\equiv \left(\frac{q-1}{2}\right)! \pmod q \\ (-1)^{|D|} \Pi c_i \Pi d_i &\equiv \left(\frac{q-1}{2}\right)! \pmod q \\ (-1)^{|D|} \Pi p i &\equiv \left(\frac{q-1}{2}\right)! \pmod q \\ (-1)^{|D|} p^{|C|} \left(\frac{q-1}{2}\right)! &\equiv \left(\frac{q-1}{2}\right)! \pmod q \\ (-1)^{|D|} p^{\frac{q-1}{2}} &\equiv 1 \pmod q \\ p^{\frac{q-1}{2}} &\equiv (-1)^{|D|} \pmod q \\ p^{\frac{q-1}{2}} &\equiv (-1)^{\operatorname{count}(p,q)} \pmod q \end{aligned}$$

这样一来， 我们就得到了**高斯引理**。

2.4.2 count函数的解析形式

count函数的形式为

$$\mathrm{count}\,(p,q)=\left|\,\left\{x\middle|\left(x=pi \bmod q, i\in\left[1,\frac{q-1}{2}\right], i\in N\right)\wedge\left(x\geqslant\frac{q+1}{2}\right)\right\}\,\right|$$

能否找到一个解析形式， 使得count被表示出来呢？

要研究这个问题， 我们就必须研究pi这个『值』在没有取模之前到底落在哪里。

如果它落在

$$\left[k,\frac{q-1}{2}k\right], k\in N$$

这个区间里， 那么它不会属于之前提到的集合D；

如果它落在

$$\left[\frac{q+1}{2}k,(q-1)\,k\right], k\in N$$

这个区间里， 那么它会属于集合D， 构成了$\mathrm{count}\,(p,q)$里的「1」。

如何表征