费马商与安肯尼-阿廷-乔拉猜想

NicFellini M. Ram Murty*Queen's University 女王
大学n.fellini@queensu.ca murty@queensu.ca

arXiv:2304.02789v1 [math.NT] 5 Apr 2023

摘要

本文给出了 Ankeny、Artin 和 Chowla 关于素数 $p \equiv 1$ 满足（mod 4）时实二次域 $\mathbb{Q}(\sqrt{p})$ 的基本单位的结果的简洁证明，并对他们的猜想作了推广。利用这一推广，我们将二次非剩余（mod p）的费马商与调和数之和联系起来。

1 引言

1951 年，Ankeny、Artin 和 Chowla [AAC51] 推导出了实二次域 $\mathbb{Q}(\sqrt{p})$ 的类数的四个同余关系，其中 p 是素数。在一篇后来的论文中，[AAC52]，他们只发表了其中三个关系的证明，也许无意中遗漏了第四个关系的证明。Carlitz [Car53] 补上了这一缺漏，给出了证明，但同样没有写出证明中的几个关键步骤。缺失的步骤涉及使用 p-进对数；这一深刻思想由 [AAC52] 提出，后来由 Iwasawa [Was82] 加以发展。回顾 Ankeny、Artin 和 Chowla 的论文，不难看出数论中两个基本概念的诞生：其一是 p-进对数，其二是利用群环研究分圆域；二者都对二十世纪数论产生了变革性影响。

在本文中，我们将进一步拓展这一思路，为 [AAC51] 和[AAC52]中的结果给出简化的证明。同时，我们还将推广这些结果，并研究 Ankeny、Artin 和 Chowla 在下一节中阐述的一个猜想。

2 Ankeny-Artin-Chowla 同余式的推广 e

Let p 是一个素数 $\equiv 1$(模 4)。$\mathbb{Q}(\sqrt{p})$ 的基本单位可写为

$$\varepsilon = \frac{t + u\sqrt{p}}{2} \tag{1}$$

对于正整数 t 和 u。Ankeny、Artin 和 Chowla [AAC51] 陈述了该结果。

$$\frac{2hu}{t} \equiv \frac{A+B}{p} \pmod{p} \tag{2}$$

其中 h 是 $\mathbb{Q}(\sqrt{p})$ 的类数，A 是模 p 的二次剩余位于$[1,p]$ 中的乘积且 B 是模 p 的二次非剩余位于 $[1,p]$ 中的乘积。这是 [AAC51] 中陈述的四个结果之一，且这四个结果中的三个在 [AAC52] 中得到了证明。Carlitz[Car53] 注意到了这一空白并提供了一个证明，但在几个关键步骤上含糊不清。推导 (2) 所需的 p-adic 对数的基本要素在 [Car53] 或[AAC52]中没有清楚地阐明。我们将在下面的讨论中填补这一空白。我们也将借此机会给出 [AAC51] 和 [AAC52]中结果的精简证明。

*研究 部分由 NSERC Discovery 资助 资助

在他们的论文中，Ankeny、Artin 和Chowla猜想，对于 $p \equiv 1$ （模4）素数，我们总有 $p \nmid u$。当 $p \equiv 5$ （模 8 ）且 $p < 2000$ 时，他们验证了这一猜想。Van derPoorten 、 te Riele 和 Williams [vdPtRW01] [VDPtRW03] 验证了这一猜想对所有素数 $p < 2 \cdot 10^{11}$均成立。这一猜想之所以受到关注，在于以下观察。1960年，Ankeny 和Chowla [AC60]证明了 $h < p$。对于任意给定的素数 p，量 A、 B 和 ε 都很容易计算（在 ε 的情况下，使用 $\sqrt{p}$ 的连分数），因此，（ 2 ）给出了 h （模 p ）的一个同余式。但由于 $h < p$，只要 u 不被 p 整除，既约剩余就给出了 h 的确切值。

我们简要讨论 Ankeny 和 Chowla [AC60] 关于 $h < p$所作的评论。他们在论文中写道，这个估计并不广为人知，并引用了 Carlitz [Car53] 的一条评论来说明这一点。随后，他们给出了更强估计 $h = O(\sqrt{p})$ 的证明。在论文的附录中，他们还给出了莫德尔提出的较弱估计 $h = O(p^{1/2+\varepsilon})$ 的另一种证明，该证明运用了约化二元二次型理论。 [AC60] 给出的证明使用了狄利克雷类数公式，尽管作者从未明言。事实上，第 146 页上方的公式是凭空从“狄利克雷的帽子”里掏出来的。

相对来　　说，利用狄利克雷公式的如下形式，给出 $h = O(\sqrt{p})$ 的证明并不费力

$$\frac{2h \log \varepsilon}{\sqrt{|d_K|}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}, \tag{3}$$

其中 $\chi(n) = (d_K/n)$ 是克罗内克符号， d_K 是 $K = \mathbb{Q}(\sqrt{p})$ 的判别式。由 (1) 可知， $\varepsilon \gg \sqrt{p}$ 因此 (3) 的左边为

$$\gg \frac{h \log p}{\sqrt{p}}.$$

另一方面，(3) 的右侧可以（通过分部求和）改写为

$$\sum_{n=1}^{p-1} \frac{\chi(n)}{n} + \int_p^{\infty} \frac{S(x)}{x^2} dx,$$

其中 $S(x) = \sum_{n<x} \chi(n)$。由于 $S(x) = O(p)$，我们看到 (3) 的右端被 $O(\log p)$ 所界定，结论遂即得证。我们指出，同样的证明表明， D 为基本判别式的 $\mathbb{Q}(\sqrt{D})$ 的类数 $h(D)$ 也为 $O(\sqrt{|D|})$。我们将在后文中用到这一事实。

一个自然产生的问题是：如果我们将（2）中的 A 和 B 分别替换为二次剩余和非二次剩余的完备集合 $\{a_s\}_{s=1}^{(p-1)/2}$ 、 $\{b_s\}_{s=1}^{(p-1)/2}$ （但不一定属于 $[1, p]$），那么会得到什么结果。我们将假设 a_s、 b_s 均为正数。这个问题很容易回答如下。

写作

$$a_s = \langle a_s \rangle + p \left[\frac{a_s}{p} \right]$$
$$b_s = \langle b_s \rangle + p \left[\frac{b_s}{p} \right]$$

其中，$\langle x\rangle$ 表示 x（模 p）的既约剩余。然后，

$$A=\prod_{s=1}^{(p-1)/2}\left(a_s-p\left[\frac{a_s}{p}\right]\right)$$
$$B=\prod_{s=1}^{(p-1)/2}\left(b_s-p\left[\frac{b_s}{p}\right]\right).$$

我们很容易看出，

$$A\equiv A^*-pA^*\sum_{s=1}^{(p-1)/2}\left[\frac{a_s}{p}\right]\frac{1}{a_s}\pmod{p^2}$$
$$B\equiv B^*-pB^*\sum_{s=1}^{(p-1)/2}\left[\frac{b_s}{p}\right]\frac{1}{b_s}\pmod{p^2}$$

其中

$$A^*=\prod_{s=1}^{(p-1)/2}a_s\quad\text{and}\quad B^*=\prod_{s=1}^{(p-1)/2}b_s.$$

因此，

$$A+B\equiv A^*+B^*-p\left(A^*\sum_{s=1}^{(p-1)/2}\left[\frac{a_s}{p}\right]\frac{1}{a_s}+B^*\sum_{s=1}^{(p-1)/2}\left[\frac{b_s}{p}\right]\frac{1}{b_s}\right)\pmod{p^2}.$$

因此，

$$\frac{A+B}{p}\equiv\frac{A^*+B^*}{p}-\left(A^*\sum_{s=1}^{(p-1)/2}\left[\frac{a_s}{p}\right]\frac{1}{a_s}+B^*\sum_{s=1}^{(p-1)/2}\left[\frac{b_s}{p}\right]\frac{1}{b_s}\right)\pmod{p}.$$

这就得到了 (2) 的以下变体。

定理 2.1。令 $p\equiv 1$（模4）为素数，且 $\{a_s\}$、$\{b_s\}$ 为分别表示一组完整的二次剩余和非剩余的正数（模 p）。令 A^* 和 B^* 分别为 a_s 和 b_s 的乘积。如果 $\varepsilon=\frac{1}{2}(t+u\sqrt{p})$ 是 $\mathbb{Q}(\sqrt{p})$ 的基本单位，则

$$\frac{A^*+B^*}{p}\equiv\frac{2hu}{t}+\left(A^*\sum_{s=1}^{(p-1)/2}\left[\frac{a_s}{p}\right]\frac{1}{a_s}+B^*\sum_{s=1}^{(p-1)/2}\left[\frac{b_s}{p}\right]\frac{1}{b_s}\right)\pmod{p}.$$

注：如果 $1\le a_s$、$b_s\le p$，那么上述同余式中的两个和恒等为零，我们便得到 Ankeny、Artin 和 Chowla 同余式 (2)。

3 与费马商和调和数的关系

设 R 是一组完整的二次剩余（模 p），且全部位于 $[1,p-1]$ 中；设 N 是一组完整的二次非剩余（模 p），且全部位于 $[1,p-1]$中。则 $A^*=A$ 和 $A\equiv -1$（模 p）。此外，$B^*=B$ 和 $B\equiv 1$（模 p）。现在我们固定一个二次非剩余 m（模 p），并定义以下两个数列

$$b_r=mr\ \ (r\in R)\quad\text{and}\quad a_n=mn\ \ (n\in N).$$

在这一设定下，定理 2.1 表述为

$$\frac{A+B^*}{p} \equiv \frac{2hu}{t} + B^* \sum_{r\in R} \left[\frac{mr}{p}\right] \frac{1}{mr} \pmod{p}$$

and

$$\frac{A^*+B}{p} \equiv \frac{2hu}{t} + A^* \sum_{n\in N} \left[\frac{mn}{p}\right] \frac{1}{mn} \pmod{p}$$

分别地。注意到 $B^* = m^{(p-1)/2}A$ 和 $A^* = m^{(p-1)/2}B$ 分别成立，并且 $m^{(p-1)/2} \equiv -1$（模 p），我们推得

$$A\left(\frac{m^{\frac{p-1}{2}}+1}{p}\right) \equiv \frac{2hu}{t} - A\sum_{r\in R} \left[\frac{mr}{p}\right] \frac{1}{mr} \pmod{p} \tag{4}$$

$$B\left(\frac{m^{\frac{p-1}{2}}+1}{p}\right) \equiv \frac{2hu}{t} - B\sum_{n\in N} \left[\frac{mn}{p}\right] \frac{1}{mn} \pmod{p} \tag{5}$$

这随即导出了对 [AAC51] 的改进：

定理 3.1. 设 p 是一个模 4 $\equiv 1$ 的素数，并令 R 为包含于 $[1, p-1]$ 中的二次剩余的完全集合， N 为包含于 $[1, p-1]$ 中的二次非剩余的完全集合，

$$\varepsilon = \frac{t+u\sqrt{p}}{2}$$

是 $\mathbb{Q}(\sqrt{p})$ 的基本单位，而 h 是 $\mathbb{Q}(\sqrt{p})$ 的类数。则对于任意模 p 的二次非剩余 m,

$$\frac{m^{p-1}-1}{p} \equiv \frac{4hu}{t} + 2\sum_{r\in R} \left[\frac{mr}{p}\right] \frac{1}{mr} \pmod{p} \tag{6}$$

$$\frac{m^{p-1}-1}{p} \equiv -\frac{4hu}{t} + 2\sum_{n\in N} \left[\frac{mn}{p}\right] \frac{1}{mn} \pmod{p} \tag{7}$$

证明。根据上述讨论，只需注意到 $A \equiv -1$（模 p）以及 $B \equiv 1$（模 p），再将方程 (4) 和 (5) 分别乘以 $m^{(p-1)/2} - 1 \equiv -2$（模 p），定理便立即得证。 □

定义。对于 p 素数，底数为 a 的费马商定义为

$$F(a) = \frac{a^{p-1}-1}{p}.$$

将定理 3.1 中的两个同余式相加，我们得到：

推论 3.2. 假设 $p \equiv 1$（模 4），且 m 是（模 p）二次非剩余。那么 ，

$$mF(m) \equiv 2\sum_{k=1}^{p-1} \left[\frac{mk}{p}\right] \frac{1}{k}$$

其中 $F(m)$ 是费马商。

注：我们注意到，关于费马商的这一同余关系并不以安肯尼-阿廷-乔拉猜想为条件。如果 $p \mid u$，定理3.1中涉及类数的项就会消失。如果 $p \nmid u$，这两项在相加时会相互抵消。

定义。 k阶调和数 H_k 定义为

$$H_k = \sum_{j=1}^{k} \frac{1}{j}$$

其中我们约定 $H_0 = 0$。

引理 3.3。对于任意奇素数 p， $H_{p-1} \equiv 0$（模 p）。

证明。这只需将加法逆元两两配对即可。当 k 遍历 $\{1, \ldots, \frac{p-1}{2}\}$时，$p-k$ 将遍历 $\{p-1, \ldots, \frac{p+1}{2}\}$。因此，

$$H_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k} \equiv \sum_{k=1}^{\frac{p-1}{2}} \left(\frac{1}{k} + \frac{1}{p-k} \right) \equiv \sum_{k=1}^{\frac{p-1}{2}} \left(\frac{1}{k} - \frac{1}{k} \right) \equiv 0 \, (\mathrm{mod}\ p) \, .$$

□

引理 3.3 的一个直接推论如下：

推论 3.4。 假设 p 是素数，且 $a < b$ 是正整数，使得 $a + b = p - 1$，该 n

$$H_a \equiv H_b \, (\mathrm{mod}\ p) \, .$$

证明。根据引理 3.3，我们有

$$0 \equiv H_{p-1} \equiv \sum_{j=1}^{a} \frac{1}{j} + \sum_{j=a+1}^{p-1} \frac{1}{j} \, (\mathrm{mod}\ p) \, .$$

根据假设， $a + 1 = p - b$ 从而

$$H_a \equiv - \sum_{j=p-b}^{p-1} \frac{1}{j} \, (\mathrm{mod}\ p) \, .$$

进行变量替换， $j \to p - j$ 我们得到，

$$H_a \equiv \sum_{j=1}^{b} \frac{1}{j} \equiv H_b \, (\mathrm{mod}\ p) \, .$$

□

令 $x_k = H_{k-1}$，推论 3.2 可表述为

$$mF(m) \equiv \sum_{k=1}^{p-1} \left[\frac{mk}{p} \right] (x_{k+1} - x_k) \, (\mathrm{mod}\ p) \, .$$

使用分部求和后，这变为

$$mF(m) \equiv x_p \left[\frac{m(p-1)}{p} \right] - \sum_{k=2}^{p-1} x_k \left(\left[\frac{mk}{p} \right] - \left[\frac{m(k-1)}{p} \right] \right) (\mathrm{mod}\ p) \, .$$

右侧的第一项由引理 3.3 得出为零。现在，在求和项中，我们利用以下引理简化地板函数之差：

引理3.5。假设 p是素数，且 M 是模 p 的正既约剩余 m 的任意正陪集代表元。那么，

$$\left[\frac{Mk}{p}\right]-\left[\frac{M(k-1)}{p}\right]=\left[\frac{M}{p}\right]+\left[\frac{mk}{p}\right]-\left[\frac{m(k-1)}{p}\right]$$

对于所有 $1\le k\le p-1$。特别是，如果 $M=m$ 则

$$\left[\frac{mk}{p}\right]-\left[\frac{m(k-1)}{p}\right]=\begin{cases}1 & if\ k=\left[\frac{p\ell}{m}\right]+1\ for\ some\ \ell\in[0,m-1]\\ 0 & otherwise.\end{cases}$$

证明。写作 $M=m+p\left[\frac{M}{p}\right]$。然后，

$$\left[\frac{Mk}{p}\right]-\left[\frac{M(k-1)}{p}\right]=\left[\frac{mk}{p}+k\left[\frac{M}{p}\right]\right]-\left[\frac{m(k-1)}{p}+(k-1)\left[\frac{M}{p}\right]\right].$$

作为 $[x+n]=[x]+n$ 对于任意正整数 n，我们可推出该陈述的第一部分 t.

对于第二个陈述，我们注意到 $\left[\frac{mk}{p}\right]-\left[\frac{m(k-1}{p}\right]\neq 0$ 当且仅当存在某个正整数 $\ell\le m-1$ 使得

$$\frac{m(k-1)}{p}<\ell\le\frac{mk}{p}.$$

重新整理这个不等式，我们得到】【。

$$k-1<\frac{p\ell}{m}\le k$$

因此 $k-1=\left[\frac{p\ell}{m}\right]$。对于 k 的这些取值，我们希望将其简化为:

$$\left[\frac{m}{p}\left(\left[\frac{p\ell}{m}\right]+1\right)\right]-\left[\frac{m}{p}\left[\frac{p\ell}{m}\right]\right].$$

写作 $p\ell=\theta+m\left[\frac{p\ell}{m}\right]$， $0<\theta<m$，我们可得

$$\frac{m}{p}\left[\frac{p\ell}{m}\right]=\ell-\frac{\theta}{p}.$$

利用这一关系，我们得到:

$$\left[\frac{m}{p}\left(\left[\frac{p\ell}{m}\right]+1\right)\right]-\left[\frac{m}{p}\left[\frac{p\ell}{m}\right]\right]=\left[\ell-\frac{\theta}{p}+\frac{m}{p}\right]-\left[\ell-\frac{\theta}{p}\right]=\left[\frac{m-\theta}{p}\right]-\left[-\frac{\theta}{p}\right]$$

由于 $0<\theta<m$，右侧的第一个取整函数为零，因为 $0<m-\theta<p$。第二项为–1 ，因为 $-1<-\theta/p<0$。结果随即得出。 □

引理 3.6. 固定 p 和某个 $q<p$. 那么对于所有 $1\le k\le q-1$ 我们有

$$\left[\frac{pk}{q}\right]+\left[\frac{p(q-k)}{q}\right]=p-1.$$

证明。假设 $\left[\frac{pk}{q}\right]=\ell$。那么我们有

$$\left[\frac{p(q-k)}{q}\right]=p+\left[\frac{-pk}{q}\right]$$

且由于 $\left[\frac{pk}{q}\right]=\ell$我们可推出 $\left[\frac{-pk}{q}\right]=-\ell-1$。因此，

$$\left[\frac{pk}{q}\right]+\left[\frac{p(q-k)}{q}\right]=\ell+(p-\ell-1)=p-1.$$

□

因此，由引理 3.5 以及部分求和法，我们推得：

定理3.7.若 $p\equiv 1$(模 4)是素数，且 M 是二次非剩余 m(模 p) 的任意正陪集代表元，那么

$$-MF(M)\equiv\left[\frac{M}{p}\right]+\sum_{j=1}^{m-1}H_{\left[\frac{pj}{m}\right]}.$$

备注。通过应用推论 3.4和引理3.6，可以缩短定理3.7 中右侧的求和式。所得求和式的长度仅取决于 m 的奇偶性。

注记。注意，如果 $p\equiv 5$(模 8)，那么 2 是二次非剩余，定理 3.7 得出

$$-2F(2)\equiv H_{\left[\frac{p}{2}\right]}\pmod p$$

由于该和仅包含一项。此外，由于 p为奇数，因此 $\left[\frac{p}{2}\right]=\frac{p-1}{2}$。实际上，我们得到了艾森斯坦同余。

$$-2F(2)\equiv H_{\frac{p-1}{2}}\pmod p$$

对于所有素数 $p\equiv 5$(mod 8) [Eis50]。事实上，我们得到了该结果的一个轻微推广。假设 $1<m<p$ 是一个奇数二次非剩余，满足 $p\equiv 1$(mod m)。根据前面的注记、定理 3.7，以及 $\left[\frac{pj}{m}\right]=(p-1)_m{}^j$ 这一事实，我们推出

$$-mF(m)\equiv 2\sum_{j=1}^{(m-1)/2}H_{\left(\frac{p-1}{m}\right)j}\pmod p.$$

注记。Th e 费马商 $F(a)=\frac{a^{p-1}-1}{p}$ 满足“对数”函数方程 n

$$F(ab)=F(a)+F(b)\pmod p$$

对于与 p 互素的 a 和 b。事实上，$a^{p-1}=1+pF(a)$ 从而

$$1+pF(ab)=(ab)^{p-1}=a^{p-1}b^{p-1}=(1+pF(a))(1+pF(b))\equiv 1+p(F(a)+F(b))\left(\mathrm{mod}\ p^2\right)$$

由此即可立即得到所需的加法同余关系。需要注意的是，费马商是一个从 $(\mathbb{Z}/p^2\mathbb{Z})^\times\to\mathbb{Z}/p\mathbb{Z}$ 到.....的函数。

定理 3.8. 假设 $p \equiv 1 (\text{mod } 4)$ 是素数。那么，任意二次剩余 (mod p) 的费马商都可以写成若干个二次非剩余 (mod p) 的费马商的线性组合。具体而言，若 r is a quadratic residue (mod p) 且 $r \equiv \overline{a}\overline{b} \left(\text{mod } p^2\right)$ for 二次非剩余 $\overline{a}, \overline{b} \left(\text{mod } p^2\right)$ such that $\overline{a} \equiv a (\text{mod } p)$ and $\overline{b} \equiv b (\text{mod } p)$，则，

$$-rF(r) \equiv \overline{b} \left[\frac{\overline{a}}{p}\right] + \overline{a} \left[\frac{\overline{b}}{p}\right] + \overline{b} \sum_{j=1}^{a-1} H_{\left[\frac{pj}{a}\right]} + \overline{a} \sum_{k=1}^{b-1} H_{\left[\frac{pk}{b}\right]} (\text{mod } p).$$

证明。这由定理 3.7和费马商的对数性质得出。 □

4 一个广义的安肯尼-阿廷-乔拉猜想

在一篇近期的论文中， [YF18], Yang和 Fu 对安肯尼-阿廷-乔拉猜想作出了如下推广。设 D 为一个不是完全平方数的正整数。考虑婆罗摩笈多-佩尔方程的所有解的集合

$$u^2 - Dv^2 = 1,$$

其中 u、 v 为自然数。令(u_1, v_1)为该集合中的最小正整数解，并记 $h(4D)$为判别式为 $4D$ 的原始二元二次型的类数。对于奇数 D ，他们猜想

$$v_1 h(4D) \not\equiv 0 \pmod{D}.$$

我们将其称为广义安肯尼-阿廷-乔拉猜想（GAAC）。假设这一猜想成立，Fu 和 Yang 证明方程

$$x^y + y^x = z^2, \quad \min(x, y) > 1, \quad (x, y) = 1, \quad 2 \nmid xy, \quad x, y, z \in \mathbb{N}$$

无解。然而，他们的猜想似乎提出得过早。事实上，在 [YY98] 中列出了六个正的无平方因子 $D < 10^8$ ，满足 $v_1 \equiv 0$（模 D）。这六个反例中，只有 $D = 23 \cdot 79$、$3 \cdot 69997$ 和 $41 \cdot 79 \cdot 541$ 是奇数。这三个 D 均是 GACC 的反例。

我们将使用一个初等筛法论证和基础代数数论，证明 GAAC 对无穷多个判别式 D成立。首先给出一个非常简单的集合论筛法不等式:

引理 4.1（简单筛法）。设 S 为一个有限非空集合， I 为一个有限指标集。对每个 $i \in I$，指定一个集合 $A_i \subset S$。若 $J \subseteq I$，则

$$\left| S \setminus \bigcup_{i \in I} A_i \right| \geq \left| S \setminus \bigcup_{j \in J} A_j \right| - \sum_{i \in I \setminus J} |A_i|.$$

A应用简单筛法并结合一个初等计数论证，可得:

引理 4.2。小于 x 且满足 $n^2 - 1$ 为无平方因子的 $n \in \mathbb{N}$ 的个数为

$$|\{n \leq x : n^2 - 1 \text{ is square free}\}| = Ax + O\left(\frac{x}{\log\log x}\right)$$

其中

$$A = \prod_{p \leq \log\log x} \left(1 - \frac{2}{p^2}\right).$$

证明。设 x 足够大。对于每个素数 $p \le x$，我们定义：

$$A_p = \{n \le x : p^2 \mid (n^2 - 1)\}.$$

然后我们的目标是估计

$$\left| \{n \le x\} \setminus \bigcup_{p \le x} A_p \right|.$$

简单筛法的直接应用给出了下界

$$\left| \{n \le x\} \setminus \bigcup_{p \le x} A_p \right| \ge \left| \{n \le x\} \setminus \bigcup_{p \le z} A_p \right| - \sum_{z \le p \le x} |A_p|.$$

其中 z 是我们稍后将选择的某个参数。

我们观察到，如果 $n \in A_p$，则 $p^2 \mid (n^2 - 1)$，特别地，p^2 只能整除 $n - 1$ 或 $n + 1$ 中的一个。因此，A_p 将是约化为 $1 \pmod{p^2}$ 或 $-1 \pmod{p^2}$ 的 $n \le x$ 的个数。由此我们推断出

$$|A_p| = \frac{2x}{p^2} + O(1).$$

因此，

$$\sum_{z \le p \le x} |A_p| = 2x \sum_{z \le p \le x} \frac{1}{p^2} + O(\pi(x)).$$

通过积分判别法，我们看到该和被 $1/z$ 上界，因此我们可以将该和界定为

$$\sum_{z \le p \le x} |A_p| \ll \frac{x}{z} + O(\pi(x)).$$

令 $P_z = \prod_{p \le z} p$。则有

$$|\{n \le x : n \notin A_p \text{ for any } p \le z\}| = \sum_{n \le x} \sum_{\substack{d^2 \mid (n^2-1) \\ d \mid P_z}} \mu(d).$$

交换求和顺序，我们得到

$$\sum_{n \le x} \sum_{\substack{d^2 \mid (n^2-1) \\ d \mid P_z}} \mu(d) = \sum_{d \mid P_z} \mu(d) \sum_{\substack{n \le x \\ n^2 \equiv 1 (d^2)}} 1.$$

i 内层求和为 $\frac{x 2^{\omega(d)}}{d^2} + O(2^{\omega(d)})$。将其代入上述等式，我们得到 t

$$\sum_{n \le x} \sum_{\substack{d^2 \mid (n^2-1) \\ d \mid P_z}} \mu(d) = x \sum_{d \mid P_z} \frac{\mu(d) 2^{\omega(d)}}{d^2} + O\left(\sum_{d \mid P_z} 2^{\omega(d)} \right).$$

注意到 $\mu(a) 2^{\omega(a)} a^{-2}$ 和 $2^{\omega(a)}$ 都是积性函数，我们可以将这两个和式写成对所有小于 z 的素数的乘积，即，

$$\sum_{n \le x} \sum_{\substack{d^2 \mid (n^2-1) \\ d \mid P_z}} \mu(d) = x \prod_{p \le z} \left(1 - \frac{2}{p^2}\right) + O\left(\prod_{p \le z} (1 + 2) \right).$$

第一个乘积收敛于一个非零常数，误差项中的乘积可估计为 $3^{\pi(z)}$。总之，我们推得

$$|\{n \le x : n^2 - 1 \text{ is square free}\}| = Ax + O\left(3^{\pi(z)}\right) + O\left(\frac{x}{z} + \pi(x)\right)$$

对于某个绝对非零常数 A。取 $z = \log\log x$，我们可以将第一个大-O 项界定为 $O((\log x)^B)$，其中 B为某个绝对常数；第二项则界定为 $O(^{x}{\log\log x})$。总之，

$$|\{n \le x : n^2 - 1 \text{ is square free}\}| = Ax + O\left(\frac{x}{\log\log x}\right)$$

□

对于二次函数 $f(n) = n^2 + c$ 的无平方因子值的更详细分析，请读者参阅 [Mur99] 的第二节。

定理4.3.如果 $D = n^2 - 1$ 是平方自由的，那么$\varepsilon = n + \sqrt{n^2 - 1}$ 是$\mathbb{Q}(\sqrt{D})$ 的基本单位。对于这样的 D，当 D 足够大时，GAAC 成立。

证明。 ε 是 $\mathbb{Q}(\sqrt{D})$的基本单位这一事实是 [ME05] 中的一个练习（见第115页的练习8.3.1）。按照猜想GAAC的记号，我们有 $v_1 = 1$。如前所述，$h(D) = O(\sqrt{|D|})$，由引理4.2可立即得出该断言。

□

5 p-进对数

可以利用幂级数定义 p-进对数

$$-\log(1 - x) = \sum_{n=1}^{\infty} \frac{x^n}{n}.$$

设 $v_p(n)$ 是整除 n 的 p 的最高次幂。我们用 $|\cdot|_p$ 表示 $\mathbb{Q}$ 上的标准 p-进度量。因此，若 $x = a/b$、a、$b \in \mathbb{Z}$，且 $\gcd(a, b) = 1$ 并且 $b \neq 0$，则

$$|x|_p = p^{v_p(b) - v_p(a)}.$$

由于对给定的素数 p，$v_p(n) \le [\log n / \log p]$，我们知道若 $|x|_p = \lambda < 1$，则

$$-\log(1 - x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

在 p-进意义下收敛，因为

$$\left|\frac{x^n}{n}\right|_p \le \lambda^n p^{v_p(n)} \to 0$$

当 $n \to \infty$ 时。

和通常一样，我们用 $\mathbb{Q}_p$ 表示关于 $|\cdot|_p$的 $\mathbb{Q}$ 的完备化。给定 $\mathbb{Q}_p$，取其代数闭包 $\overline{\mathbb{Q}_p}$，再将其完备化，从而得到 p-进复数类比，记作 $\mathbb{C}_p$。这个域是代数闭的（例如参见 [Was82] 的命题 5.2）。

p 进对数　上文为 $|x|_p < 1$ 定义的对数现在可以扩展到 $\mathbb{C}_p^{\times}$ 的全部元素，使得　t

$$\log xy = \log x + \log y$$

以及$\log p = 0$。为避免与通常的对数混淆，我们将 p-进对数记作$\log_p$。称 $|x|_p < 1$ 等价于称$v_p(x) > 0$。如果 $v_p(x) \geq 1/(p-1)$，那么在级数中

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n},$$

我们看到

$$v_p\left(\frac{x^{rp^v}}{p^v}\right) \geq \frac{rp^v - v(p-1)}{p-1} = \frac{r((p-1)+1)^v - v(p-1)}{p-1} \geq \frac{r\binom{v}{2}(p-1)^2}{p-1} \geq 1$$

如果 $v \geq 2, r \geq 1$ 或者如果 $v = 1, r \geq 2$ 或者如果 $v = 0$ 并且 $r \geq p-1$。因此，我们有

$$\left|\log(1-x) - \sum_{j=1}^{p} \frac{x^j}{j}\right|_p < \frac{1}{p}.$$

换句话说，

$$\log(1-x) = -\sum_{j=1}^{p} \frac{x^j}{j} \pmod{p}.$$

威尔逊定理的一个简单推广表明，对于 $1 \leq j \leq p-1$，

$$\frac{1}{p}\binom{p}{j} \equiv \frac{(-1)^{j-1}}{j} \pmod{p}.$$

因此，

$$\begin{aligned}\log(1-x) &\equiv \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j}(-1)^j x^j + \frac{1}{p}(-1)^p x^p \pmod{p} \\ &\equiv \frac{1}{p}\left((1-x)^p - 1\right) \pmod{p}.\end{aligned}$$

这证明了：

定理 5.1（Ankeny、Artin、Chowla，1952）。如果 $v_p(x-1) \geq 1/(p-1)$，那么

$$\log_p(x) \equiv \frac{x^p - 1}{p} \pmod{p}.$$

我们可以将此与费马商联系起来

$$F(a) = \frac{a^{p-1} - 1}{p}$$

对于 $(a, p) = 1$，如下所示。写作 $a^{p-1} = 1 + pF(a)$，我们有

$$\log_p(a) = \frac{1}{p-1}\log_p a^{p-1} = \frac{1}{p-1}\log_p(1 + pF(a)).$$

另一方面，我们有 p-进级数

$$\frac{1}{p-1} = -1 - p - p^2 - \cdots$$

and

$$-\log_p(1+x) = -x + \frac{x^2}{2} - \cdots$$

从而

$$\begin{aligned}\log_p(a) &= (-1-p-p^2-\cdots)\left(pF(a) - \frac{p^2F(a)^2}{2} + \cdots\right)\\ &\equiv -pF(a) \pmod{p^2}.\end{aligned}$$

因此，我们有：

定理 5.2. 如果 $(a,p) = 1$，那么

$$F(a) \equiv -\frac{\log_p(a)}{p} \pmod{p}.$$

特别是，如果我们有整数集合 $\{a_s\}_{s=1}^{(p-1)/2}$ 和 $\{b_s\}_{s=1}^{(p-1)/2}$，使得

$$\prod_{s=1}^{(p-1)/2} a_s = -1 + p\Omega$$

and

$$\prod_{s=1}^{(p-1)/2} b_s = 1 + p\Omega^*,$$

然后取 p-adic 对数，便得到 *[*Car*53]* 的公式 (3.2 ff)：

$$\begin{aligned}\Omega &\equiv \sum_{s=1}^{(p-1)/2} F(a_s) \pmod{p}\\ \Omega^* &\equiv \sum_{s=1}^{(p-1)/2} F(b_s) \pmod{p}\end{aligned}$$

备注。它是　　关于 p-进对数的这一关键讨论在 [Car53] 中缺失。　　.

6 群环、高斯和与同余

另一个重要思想 [AAC52] 是使用与伽罗瓦群 Γ 相关联的群环，以及它如何作用于域元素。更准确地说，设 $K/\mathbb{Q}$ 是一个有限伽罗瓦扩张，其伽罗瓦群为 Γ。群环 $\mathbb{Q}[\Gamma]$ 由元素组成

$$\sum_{g\in\Gamma} a_g g, \quad a_g \in \mathbb{Q}$$

并且我们通过

$$\left(\sum_{g\in\Gamma} a_g g\right)\left(\sum_{h\in\Gamma} b_h h\right) = \sum_{z\in\Gamma}\left(\sum_{gh=z} a_g b_h\right) z.$$

如果 Γ是阿贝尔的，那么 $\mathbb{Q}[\Gamma]$ 也是阿贝尔的。

显然，可以将 Γ 对域元素 K 的作用扩展为 $\mathbb{Q}[\Gamma]$ 的作用：对于 $\alpha \in K$，

$$\left(\sum_{g\in\Gamma} a_g g\right)(\alpha) := \sum_{g\in\Gamma} a_g g(\alpha).$$

对于分圆域 $\mathbb{Q}(\zeta_m)$，其中 ζ_m 表示一个本原的 m 次单位根， $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ 的伽罗瓦群 Γ 为 $\Gamma \cong (\mathbb{Z}/m\mathbb{Z})^\times$，其中对应于互素剩余类 a(模 m) 的自同构 σ_a 定义为

$$\sigma_a(\zeta_m) = \zeta_m^a.$$

若 $m = p$ 是素数，令 $\zeta = \zeta_p$，并按照 [AAC52], , 记为

$$G = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \sigma_j$$

群环 $\mathbb{Q}[(\mathbb{Z}/p\mathbb{Z})^\times]$ 中的元素。这里 $\left(\frac{\cdot}{p}\right)$ 表示勒让德符号。此元素可以视为一个“高斯和”。准确地说，我们有：

引理 6.1. 设 $p \equiv 1$(模 4) 是一个素数。假设 ζ 是一个本原的 p 次单位根。那么对于任意 $1 \le a \le p-1$,

$$G(\zeta^a) \equiv \sqrt{p}\left(\frac{a}{p}\right)$$

其中 $\left(\frac{\cdot}{p}\right)$ 是勒让德符号。

证明。根据定义，我们有

$$G(\zeta^a) = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^{aj}.$$

进行变量替换后， $k = aj$ 我们有

$$G(\zeta^a) = \sum_{k=1}^{p-1} \left(\frac{a^{-1}k}{p}\right) \zeta^k.$$

由勒让德符号的乘法性以及 (a/p) =(a^{-1}/p)，我们有

$$G(\zeta^a) = \left(\frac{a^{-1}}{p}\right)\tau$$

其中

$$\tau = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$$

根据 [Was82]的推论 4.6， τ 的值为

$$\tau = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p}, & \text{if } p \equiv 3 \pmod 4 . \end{cases}$$

结果得证。 □

给定元素 $\alpha \in K$ 和 $\beta = \sum_{g\in\Gamma} a_g g \in \mathbb{Q}[\Gamma]$，我们将使用如下记号

$$\alpha^\beta := \prod_{g\in\Gamma} g(\alpha)^{a_g}.$$

我们注意到，给定 $x \in \mathbb{Q}$,

$$x^G = 1$$

由于特征和为零，并且 x 被每个群元素固定。

于是，狄利克雷类数公式可用群环形式写成如下形式。若 $p \equiv 1$(模 4)， ε 是 $\mathbb{Q}(\sqrt{p})$ 的基本单位，而 h 是类数，则有熟知的公式

$$2h \log \varepsilon = -\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \log(1-\zeta^j). \tag{8}$$

这里，我们关键地利用了 $p \equiv 1$(模 4) 这一条件，来计算推导式 (8) 时出现的高斯和。将式 (8) 两边取指数，得到

$$\varepsilon^{2h} = (1-\zeta)^{-G},$$

使用我们的群环形式。正如上文所述，对任意 $x \in \mathbb{Q}$，都有 $x^G = 1$ ，因此

$$\varepsilon^{2h} = (1-\zeta)^{-G} = (\zeta-1)^{-G}.$$

若 n 是模 p 的二次非剩余，则在定义 G 的和中作变量替换，将 $j \mapsto nj$ 映为。经过这一变量替换，我们有

$$G = \sum_{j=1}^{p-1} \left(\frac{nj}{p}\right) \sigma_{nj} = -\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \sigma_{nj}.$$

因此,

$$(1-\zeta)^{-G} = (1-\zeta^n)^G$$

由此可得

$$\varepsilon^{2h} = (\zeta^n - 1)^G.$$

结合关于 ε^{2h} 的两个公式可得

$$\varepsilon^{4h} = \left(\frac{\zeta^n - 1}{\zeta - 1}\right)^G = \left(\frac{\zeta^n - 1}{n(\zeta-1)}\right)^G \tag{9}$$

因为 $n^G = 1$。

于是得到以下引理:

引理 6.2. 设 ζ 是 p 为有理素数时的一个原始 p 次单位根。对于一个模 p 的二次非剩余，令

$$\alpha_j = \frac{\zeta^{nj} - 1}{n(\zeta^j - 1)}.$$

然后 $v_p(\alpha_j - 1) \geq 1/(p-1)$。

证明。写作 $\omega = \zeta^j$，我们有

$$\alpha_j = \frac{1-\omega^n}{1-\omega} = \sum_{k=0}^{n-1} \omega^k.$$

由于 $\zeta \equiv 1$(模 $1-\zeta$)，我们推得对于所有 $1 \le k \le n-1$，$\omega^k \equiv 1$(模 $1-\zeta$)。因此，$\alpha_j \equiv 1$(模 $1-\zeta$)。所以，$(1-\zeta)^{p-1}$ 整除 $(\alpha_j - 1)^{p-1}$。我们有 $(p) = (1-\zeta)^{p-1}$。因此，

$$(\alpha_j - 1)^{p-1} \equiv 0 \pmod{p}.$$

特别地，由于 $v_p(x)$ 是乘法性的，我们有

$$(p-1)v_p(\alpha_j - 1) \ge 1.$$

由此即可得到所需的结论。 □

注意到

$$\left(\frac{\zeta^n - 1}{n(\zeta - 1)}\right)^G = \prod_{j=1}^{p-1} \left(\frac{\zeta^{nj} - 1}{n(\zeta^j - 1)}\right)^{\left(\frac{j}{p}\right)}$$

并对（9）两边取 p-进对数，可得

$$4h \log_p \varepsilon \equiv \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \log_p \left(\frac{\zeta^{nj} - 1}{n(\zeta^j - 1)}\right) \pmod{p}.$$

由定理 5.1 和引理 6.2 可得同余式

$$4h \log_p \varepsilon \equiv \frac{1}{p} \sum_{j=1}^{p} \left(\frac{j}{p}\right) \left(\left(\frac{\zeta^{nj} - 1}{n(\zeta^j - 1)}\right)^p - 1\right) \equiv \frac{1}{n^p} G \left(\frac{\left(\frac{\zeta^n - 1}{\zeta - 1}\right)^p - n}{p}\right) \pmod{p}.$$

这等价于

$$4h \log_p(\varepsilon) \equiv \frac{1}{n} G(f(\zeta)) \pmod{p} \tag{10}$$

其中

$$f(x) = \frac{1}{p} \left\{ \left(\frac{x^n - 1}{x - 1}\right)^p - \left(\frac{x^{np} - 1}{x^p - 1}\right) \right\}.$$

注意到我们可以将 $f(x)$ 定义中的两个有理函数分解因式，由此可得 $f(x)$ 是 x 中的一个多项式：

$$f(x) = \frac{1}{p} \left(\left(\sum_{k=0}^{n-1} x^k \right)^p - \sum_{j=0}^{n-1} x^{kp} \right). \tag{11}$$

此外，由于 $\zeta^p = 1$，我们看到，式 (11)中的第二个和在 ζ 处取值时等于 n。因此，$f(\zeta) = \frac{1}{p}\left(\left(\frac{\zeta^n - 1}{\zeta - 1}\right)^p - n\right)$。按照 [AAC52]，我们希望将 $f(x)$（模 p）化简。特别地：

引理 6.3。对于如上定义的 $f(x)$,

$$f(x) \equiv -\sum_{k=1}^{p-1} \sum_{j=0}^{\infty} \frac{1}{k} x^{nk+pj} + \sum_{k=1}^{p-1} \sum_{j=0}^{n-1} \frac{j+1}{k} x^{k+pj} \pmod{p}$$

其中第一个求和是对 $nk + pj < pn$ 进行的。

证明。我们将 $f(x)$ 写作

$$f(x)=\frac{(x^n-1)^p(x^p-1)-(x^{pn}-1)(x-1)^p}{p}\cdot\frac{1}{(x-1)^p(x^p-1)}.$$

注意到 $\frac{1}{p}\binom{p}{k}\equiv(-1)_k^{k-1}$（模 p）对于 $1\le k\le p-1$ 我们有

$$\frac{(x-1)^p}{p}\equiv\frac{x^p-1}{p}-\sum_{k=1}^{p-1}\frac{x^{p-k}}{k}\,(\mathrm{mod}\ p)\,.$$

写作 $\ell=p-k$，上面的展开式 $f(x)$ 可写为

$$f(x)\equiv\sum_{\ell=1}^{p-1}\frac{x^{n\ell}}{\ell(x^p-1)}-\sum_{\ell=1}^{p-1}\frac{x^\ell}{\ell}\cdot\frac{x^{pn}-1}{(x^p-1)^2}\,(\mathrm{mod}\ p)\,.$$

写作

$$\frac{1}{1-x^p}=\sum_{j=0}^{\infty}x^{pj}\quad\text{and}\quad\frac{1}{(1-x^p)^2}=\sum_{j=0}^{\infty}(j+1)x^{pj},$$

$$f(x)\equiv-\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty}\frac{x^{n\ell+pj}}{\ell}+\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty}\frac{j+1}{\ell}x^{pj+\ell}-\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty}\frac{j+1}{\ell}x^{pj+pn+\ell}\,(\mathrm{mod}\ p)\,.$$

Ch在上面的最后一个求和式中更换求和指标，从 $j\mapsto j-n$ 开始，我们有

$$f(x)\equiv-\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty}\frac{x^{n\ell+pj}}{\ell}+\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty}\frac{j+1}{\ell}x^{pj+\ell}-\sum_{\ell=1}^{p-1}\sum_{j=n}^{\infty}\frac{j+1}{\ell}x^{pj+\ell}+\sum_{\ell=1}^{p-1}\sum_{j=n}^{\infty}\frac{n}{\ell}x^{pj+\ell}\,(\mathrm{mod}\ p)\,.$$

两个中间的和相消，得到一个有限和。接下来，我们注意到，最后一个和中的指数遍历大于 pn 且与 p 互素的数。因此，我们可以将指数写成 $u=nv+pj$，其中 $v\in\{1,\dots,p-1\}$ 为某个量。因此，

$$u=nv+pj>pn\Rightarrow pj>n(p-v)>0.$$

因此，指数 u 也出现在第一个和中。对 $\ell\mapsto n\ell$ 的第一个和进行变量替换后，我们看到，第一个和中对应于指数 u 的项的系数为$-n/u$。因此，最后一个和完全消失了。实际上，

$$f(x)\equiv-\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty}\frac{1}{\ell}x^{n\ell+pj}+\sum_{\ell=1}^{p-1}\sum_{j=0}^{n-1}\frac{j+1}{\ell}x^{pj+\ell}\,(\mathrm{mod}\ p)$$

其中第一个求和遍历所有 $n\ell+pj<pn$。 □

最后，我们还需要一个计算工具。

引理 6.4。假设 $p\equiv1$(模 4)。

$$S=\sum_{k=1}^{p-1}\frac{1}{k}\left(\frac{k}{p}\right)\equiv0\,(\mathrm{mod}\ p)\,.$$

证明。我们注意到】【。

$$S \equiv \sum_{k=1}^{p-1} \frac{1}{p-k} \left(\frac{p-k}{p} \right) \equiv -\sum_{k=1}^{p-1} \frac{1}{k} \left(\frac{-k}{p} \right) \pmod{p}.$$

由于 $p \equiv 1$（模 4），$(-1/p) = 1$。将 S 的两种表示相加，我们推得

$$2S \equiv 0 \pmod{p}.$$

因此，$S \equiv 0$（模 p）。 □

定理 6.5（Ankeny、Artin、Chowla，1952）。设 $p \equiv 1$（模 4）。令 h 表示 $\mathbb{Q}(\sqrt{p})$ 的类数，并令 $\varepsilon = (t + u\sqrt{p})/2$ 为基本单位。则

$$4h\frac{u}{t} \equiv -\frac{1}{n} \sum_{k=1}^{p-1} \frac{1}{k} \left[\frac{nk}{p} \right] \left(\frac{k}{p} \right) \pmod{p}$$

对于任意二次非剩余 n（模 p）。

证明。假设 ζ 是一个本原的 p 次单位根。那么根据引理 6.3,

$$f(\zeta) = -\sum_{\ell=1}^{p-1} \sum_{j=0}^{\infty} \frac{1}{\ell} \zeta^{n\ell} + \sum_{\ell=1}^{p-1} \frac{1}{\ell} (j+1) \zeta^{\ell} \pmod{p}$$

其中第一个求和对所有 $n\ell + pj < pn$ 进行。特别地，第一个求和中有 $1 + [n\ell/p]$ 个这样的 j。将第一个求和中的求和指标从 $\ell \mapsto p - \ell$ 改为，我们得到

$$f(\zeta) \equiv \sum_{\ell=1}^{p-1} \frac{1 + \left[\frac{n\ell}{p} \right]}{\ell} \zeta^{-n\ell} + \frac{n(n+1)}{2} \sum_{\ell=1}^{p-1} \frac{1}{\ell} \zeta^{\ell} \pmod{p}.$$

然后，应用式 (10) 中定义的元素 G，并利用 G 的线性性，可得

$$G(f(\zeta)) \equiv \sum_{\ell=1}^{p-1} \frac{1 + \left[\frac{n\ell}{p} \right]}{\ell} G(\zeta^{-n\ell}) + \frac{n(n+1)}{2} \sum_{\ell=1}^{p-1} \frac{1}{\ell} G(\zeta^{\ell}) \pmod{p}.$$

由引理 6.1，可化简为

$$G(f(\zeta)) \equiv \sqrt{p} \sum_{\ell=1}^{p-1} \left(\frac{-n\ell}{p} \right) \frac{1 + \left[\frac{n\ell}{p} \right]}{\ell} + \frac{n(n+1)}{2} \sqrt{p} \sum_{\ell=1}^{p-1} \frac{1}{\ell} \left(\frac{\ell}{p} \right) \pmod{p}$$

展开第一个求和式，应用引理 6.4，并注意到 $-n$ 是模 p 的二次非剩余，可推出

$$G(f(\zeta)) \equiv -\sqrt{p} \sum_{\ell=1}^{p-1} \frac{1}{\ell} \left[\frac{n\ell}{p} \right] \left(\frac{\ell}{p} \right) \pmod{p}.$$

因此,

$$4h \log_p(\varepsilon) \equiv -\sqrt{p} \sum_{\ell=1}^{p-1} \frac{1}{\ell} \left[\frac{n\ell}{p} \right] \left(\frac{\ell}{p} \right) \pmod{p}.$$

注意到

$$\log_p(\varepsilon) \equiv \frac{u\sqrt{p}}{t} \pmod{p},$$

我们得出这一结果。 □

7 总结

我们对 [AAC52] 和 [Car53] 中的一些结果进行了完整而自成体系的论述。我们在定理 2.1 中推广了 AAC 猜想，从而将 AAC 猜想与费马商的一个同余关系联系起来。这一推广使我们得以推广艾森斯坦的一项结果，该结果将费马商与调和数之和联系起来。

Yu 和 Yu [YY98]研究了安肯尼-阿廷-乔拉猜想在函数域中的类比情形。Mordell [Mor60] 研究了 $p \equiv 3 \pmod 4$ 的情形， [Mor61] 并提出了一个类似的猜想。在所有这些情形中，我们都能看到与伯努利数之间有趣的联系。特别是，若存在无穷多个正则素数（即不整除 p 次分圆域类数的素数 p），那么安肯尼-阿廷-乔拉猜想和莫德尔猜想对这些素数 p 都成立。目前尚不清楚正则素数是否有无穷多个，不过猜想认为这类素数具有正密度。斯拉武茨基 [Sla04]的一篇相关综述值得仔细研读。

参考文献

[AAC51] N.C.Ankeny、E. Artin 和S. Chowla。实二次域的类数。美国国家科学院院刊，37(8)：524–525，1951。[AAC52] N.C. Ankeny、E.Artin 和 S. Chowla。实二次数域的类数。数学年刊，56(3)：479–493，1952。[AC60] N. C.Ankeny 和 S. Chowla。关于实二次域类数的一注。算术学报，6：145–147，1960。[Car53] L. Carlitz。关于实二次域类数的注记。美国数学会会刊，4(4)：535–537，1953。[Eis50] F.Eisenstein。一类新的数论函数：它依赖于两个元素，并由某些线性函数方程定义。K ¨onigl. Preuß. Akad 报告，15：36–42，1850。[ME05] M. Ram Murty和 J. Esmonde。代数数论问题，数学研究生教材第190卷。Springer-Verlag，纽约，第二版，2005年。[Mor60] L. J. Mordell。关于一个佩尔方程猜想。算术学报，6：137–144，1960。[Mor61] L.J. Mordell。关于一个佩尔方程猜想。II。伦敦数学会杂志，36：282–288，1961。[Mur99] M.Ram.Murty。二次域类群的指数。梅塔数学与数学物理研究所，印度阿拉哈巴德：1999年。[Sla04] I.Sh. Slavutskii。实二次域与安肯尼–阿廷–乔拉猜想。数学科学杂志，122(6)：3673–3678，2004。[vdPtRW01] A. J. van der Poorten、H.J. J. teRiele 和H. C.Williams。对所有小于100 000000 000的素数验证安肯尼-阿廷-乔拉猜想。数学计算，70(235)：1311–1328，2001。

[VDPtRW03] A. J. Van Der Poorten、H. J. J. te Riele 和 H. C. Williams。《关于“对所有小于 100 000 000 000 的素数进行安肯尼-阿廷-乔拉猜想的计算机验证”的勘误和补充》 [数学计算 70 (2001)，第 235 期，1311–1328；MR1709160 (2001j:11125)]。数学计算，72(241):521–523，2003 年。[Was82] L. Washington。《分圆域导论》，数学研究生教材第 83 卷。Springer-Verlag，纽约，1982 年。[YF18] H. Yang 和 R. Fu。通过安肯尼-阿廷-乔拉猜想的推广研究指数丢番图方程 $x^y + y^x = z^2$ 。国际数论杂志，14(5):1223–1228，2018 年。[YY98] J. Yu 和 J-K. Yu。关于安肯尼-阿廷-乔拉猜想几何类比的注记。当代数学，210:101–105，1998 年。