arXiv:2301.02951v1 [math.NT] 8 Jan 2023

虚二次域的类数与二次剩余恒等式

Jorge Garcia

2023年1月10日

摘要

本文研究模素数$p = 4n - 1$ 的二次剩余和公式。我们将该公式中的若干项与二次方程的根联系起来，并基于这些根对新概念进行了全面分析。我们得到了若干关于二次剩余和的公式。最后，本文推导出若干涉及虚二次域类数 $h(-p)$的恒等式，其中虚二次域为 $\mathbb{Q}(\sqrt{-p})$。

1 引言

考虑一个素数 $p = 4n - 1$和 $1 \leq k \leq p - 1$. 根据 $r_p(k^2)$，我们将 k^2 除以 p所得的余数记作 $r_p(k^2)$，并称其为模 p. 下 k^2 的二次剩余。当我们将所有这些余数相加时，就得到相对于素数 p的二次剩余之和。这个和有一个复杂的公式，

$$\sum_{k=1}^{p-1} r_p\left(k^2\right) = \binom{p}{2} - p \cdot h(-p), \tag{1.1}$$

其中， $h(-p)$ 是虚二次域 $\mathbb{Q}(\sqrt{-p})$ 的类数。当素数的形式为 $p = 4n - 1 > 3$ 时，类数的重要公式包括狄利克雷类数公式

$$h(-p) \;=\; \frac{\sqrt{p}}{2\pi}\sum_{r=1}^{\infty}\frac{\chi(r)}{r}, \tag{1.2}$$

其中， χ 是狄利克雷特征。

公式1.2 可见于 [2]。另一个涉及克罗内克符号 $\left(\frac{p}{r}\right)$ 的公式可见于 [5]（第 428 页推论1）。最后，Cohen 提出的公式 [1] [推论 5.3。16] 也给出了类数。

本文的主要目的是通过以不同方式计算二次剩余，得到该数 h（$-p$）的一些恒等式。

这里总结了本文得出的主要公式。这里，
$Q_k = \left(1+\sqrt{4kp+12n-7}\right)/2$、 $M = \lfloor n^2/p \rfloor$ 和 J_n 表示跳跃数（见第2节）。

$$\begin{aligned}
\sum_{k=1}^{M}\left\lfloor\sqrt{kp}\right\rfloor - \sum_{k=0}^{M-1}\lfloor Q_k\rfloor &= J_n - M - 1.\\
\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor + \sum_{k=0}^{M-1}\lfloor Q_k\rfloor &= (M-1)n.
\end{aligned}$$

$$\begin{aligned}
\sum_{k=1}^{p-1} r_p\left(k^2-k+2-3n\right) &= \sum_{k=1}^{p-1} r_p\left(k^2\right) + 3n - 2.\\
\sum_{k=1}^{2n} r_p\left(k^2-k+2-3n\right) &= \sum_{k=1}^{2n} r_p\left(k^2\right) + n.\\
\sum_{k=1}^{n} r_p\left(k^2-k+2-3n\right) &= \sum_{k=1}^{n} r_p\left(k^2\right) + \frac{n(n+1)}{2} - p(J_n - 1 - M).\\
\sum_{k=1}^{p-1}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{p(p-5)+6-n}{3} - \frac{1}{p}\sum_{k=1}^{p-1} r_p\left(k^2\right).\\
\sum_{k=1}^{2n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{n(2n-1)(4n-7)}{3p} - \frac{1}{p}\sum_{k=1}^{2n} r_p\left(k^2\right).\\
\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{(n+1)(2n^2-23n+6)}{3p} - \frac{1}{p}\sum_{k=1}^{n} r_p\left(k^2\right) + J_n - M.
\end{aligned}$$

这里总结了本文中涉及类数 $h=h$（$-p$）的恒等式。

$$\begin{aligned}
\frac{J_n}{2}+M(n-1) &= \frac{h}{4}+\sum_{k=1}^{M}\left\lfloor\sqrt{kp}\right\rfloor+\frac{n^2-5n+9}{12}.\\
-\frac{J_n}{2}+Mn &= \frac{h}{4}+\sum_{k=0}^{M-1}\lfloor Q_k\rfloor+\frac{n^2-5n-3}{12}.\\
\frac{J_n}{2}+\sum_{k=1}^{n-1}\left\lfloor\frac{k^2}{p}\right\rfloor &= \frac{h}{4}+\frac{n^2-5n+9}{12}.
\end{aligned}$$

$$\begin{aligned}
\sum_{k=1}^{p-1} r_p\left(k^2-k+2-3n\right) &= p\cdot(2n-h)-n-1.\\
\sum_{k=1}^{2n} r_p\left(k^2-k+2-3n\right) &= \frac{p\cdot(2n-h)+1}{2}.\\
\sum_{k=1}^{n} r_p\left(k^2-k+2-3n\right) &= \frac{p}{4}(3n+2-2J_n-h)-\frac{(n+1)(n-1)}{4}.
\end{aligned}$$

$$\sum_{k=1}^{n} r_p\left(k^2\right) = \frac{p}{4}(2J_n+2n-3-4M-h)+\frac{n(n+1)}{4}.$$

$$\begin{aligned}
\sum_{k=1}^{p-1}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= h+\frac{16n^2-35n+15}{3}.\\
\sum_{k=1}^{2n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{h}{2}+\frac{4n^2-14n+9}{6}.\\
\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{h}{4}+\frac{J_n}{2}+\frac{n^2-17n-3}{12}.\\
\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{h}{2}+M(1-n)+\frac{n^2-11n+3}{6}+\sum_{k=1}^{M}\left\lfloor\sqrt{kp}\right\rfloor.
\end{aligned}$$

在第2节中，我们给出全文所使用的主要定义和符号。在此，我们阐述跳跃和总余数的概念，并指出这些跳跃何时发生。在第3节中，我们将跳跃归入六个不同的集合，并陈述若干主要引理，以便在第4节中统计跳跃。我们还在此定义不同集合对之间的双射函数，以计算它们的基数。在第5节中，我们求形如$k^2 - k + 2 - 3n$ 的项的二次剩余之和，其中 k 在不同区间 $[1, 4n-2]$、$[1, 2n]$或 $[1, n]$. 中取值。本节还统计跳跃的总数。最后，在第6节中，我们建立若干涉及虚二次域 $\mathbb{Q}(\sqrt{-p})$的类数 $h(-p)$的恒等式。这些恒等式基于前几节所得的和，其中一些恒等式还涉及跳跃的数量。

在 [4] 中，我们计算了 $p = 4n + 1$ 时的几个二次剩余和；而在本文中，我们对 $p = 4n - 1$. 时的情形进行类似但不同的分析。本文涉及类数。有时，为了便于比较，我们会同时给出两个公式（$p = 4n - 1$ 和 $p = 4n + 1$）。

2 二次剩余和与跳跃

设 $p = 4n - 1$ 为素数。约定，当我们写 n 时，表示一个自然数 $n \geq 1$.

定义2.1 设 q 为正整数，且 $x \in \mathbb{Z}$。我们用 $r_q(x)$ 表示 x 除以 q 所得的余数。因此，$r_q(x) \in \{0, 1, 2, ..., q-1\}$ 满足

$$x = m \cdot q + r_q(x),$$

对于某个 $m \in \mathbb{Z}$。显然，$m = \lfloor x/q \rfloor$.

以下记号在本文中将会一直用到： [3]

记号 2.2 对于 $m \in \mathbb{Z}$、 $p = 4n-1$ 素数以及 $m \geq 0$，我们记

$$Q_m = \frac{1}{2} + \frac{1}{2}\sqrt{1 + 4\left[(m+1)p - n - 1\right]} = \frac{1}{2} + \frac{1}{2}\sqrt{4mp + 3p - 4},$$

$$R_m = \sqrt{mp},$$

$$M = \left\lfloor \frac{n^2}{p} \right\rfloor.$$

在 [3], 中，我们得到了一个涉及 $p = 4n-1$时二次剩余之和的定理。为便于参考，我们在此写出该定理。

定理 2.3 设 $p = 4n-1$ 为素数。使用记号 2.2，我们有

$$\frac{1}{2}\sum_{k=1}^{p-1} r_p\left(k^2\right) = p\left(\sum_{m=1}^{M}\lfloor R_m\rfloor + \sum_{m=0}^{M-1}\lfloor Q_m\rfloor\right) - Mp(2n-1) + \frac{p\cdot(n^2+n)}{6}.$$

当我们研究项 Q_m时，自然会出现一个概念。该项是二次多项式 $x^2 - x + 2 - 3n - mp$ 的正根，它与 $(x-1)^2 + x + 1 - 3n - mp$.相同

定义 2.4 设 $p = 4n-1$ 为素数且 $0 \leq k \leq p$。 k 的总余数定义为，并记作

$$\Gamma(k) = r_p\left((k-1)^2\right) + r_p\left(k + 1 - 3n\right).$$

我们还称 k 是一个跳跃，如果其总余数为 p 或更大，即当

$$\Gamma(k) \geq p.$$

跳跃的重要性是什么？首先，在定理 2.3 的证明中（见 [3]），一个关键技巧是将 $r_p(k^2)$ 与 $r_p((2n-k)^2)$ 相加。事实证明，当 $k \in (R_m, Q_m]$ 时，这个和是常数；但一旦 k 超过 Q_m，我们就需要减去 p. 。因此，了解何时需要减去 p，是更好地理解定理 2.3 中公式的关键。其次，区间 $[2, n+2]$ 中的跳跃数将使我们能够建立一个公式，用于计算项 $\sum_{m=0}^{M-1}\lfloor Q_m\rfloor$、 $\sum_{m=1}^{M}\lfloor R_m\rfloor$ 以及作为 n、 $h(-p)$ 和跳跃数的函数的 $\sum_{k=0}^{n} r_p(k^2)$。这在推论 6.2 和 6.4 中得以实现。

以下三个引理使我们能够确定一些跳跃及其发生的时机。为方便记号，我们定义 $\mathbb{Z}_0 = \{0, 1, 2, ...\}$.

引理 2.5 设 $p = 4n - 1$ 为素数，且 $m \in \mathbb{Z}_0$. 。则

$$\lfloor Q_m \rfloor < Q_m.$$

证明。假设存在 $j \in \mathbb{Z}$ 使得 $j = \left(1 + \sqrt{4mp + 12n - 7}\right)/2$.那么 $j^2 - j + 2 - 3n = mp$. 取 $x_0 = 2n - j$ 可得

$$x_0^2 = 4n^2 - n + mp + j - 4nj + n + 3n - 2 = (n + m - j + 1)p - 1,$$

因此 $x_0^2 \equiv -1$ (模 p)，这与费马小定理矛盾，因为 $p = 4n - 1$. □

注 2.6 采用相同的论证可知，不存在满足 $k^2 - 3k + 4 - 3n = mp$ 的整数 k ，否则取 $k - 1 = j$ 可得 $j^2 - j + 2 - 3n = mp$，这将导致矛盾。

引理 2.7 设 $p = 4n - 1$ 是满足 $n \geq 3$. 的素数。设 $m \in \mathbb{Z}_0$ 满足

$$0 \leq m \leq \left\lfloor \frac{n^2 - 4n + 5}{p} \right\rfloor \quad and \quad k_m = 1 + \left\lfloor \frac{1 + \sqrt{4mp + 12n - 7}}{2} \right\rfloor.$$

Then

(i) $3 \leq k_m \leq n + 2$.(ii) $1 + \sqrt{4mp + 12n - 7} < 2k_m < 3 + \sqrt{4mp + 12n - 7}$.(iii) k_m 是一个跳跃，并且

(iv) $3n - k_m - 1 < r_p\left((k_m - 1)^2\right) = (k_m - 1)^2 - mp \leq 3n + k_m - 4.$

证明。

(i) 注意到 $4mp + 12n - 7 \leq 4n^2 + 4n + 1$，因此 $k_m \leq n + 2$. 。由于 $2 \leq n$, $9 \leq 4mp + 12n - 7$. 。因此 $3 \leq k_m$.

(ii) 注意， k_m 严格大于 $x^2 - x + 2 - 3n - mp$的正根，因此

$$k_m^2 - k_m + 2 - 3n > mp. \tag{2.3}$$

现在，由 $k_m \le n+2 \le 3n$ 和 $2 \le n$ 可得

$$(k_m-1)^2 - mp = k_m^2 - k_m + 2 - 3n - mp + 3n - k_m - 1 \ge 3n - k_m. \quad (2.4)$$

由引理 2.5，$k_m < \left(3+\sqrt{4mp+12n-7}\right)/2$. 另一个不等式显然成立。

(iii) 由 (ii)，k_m 小于 $x^2 - 3x + 4 - mp - 3n$ 的正根，因此 $k_m^2 - 3k_m + 4 - mp - 3n \le -1$. 于是

$$(k_m-1)^2 - mp \le 3n + k_m - 4 \le 4n. \quad (2.5)$$

不可能有 $(k_m-1)^2 - mp = 4n$，否则 $(k_m-1)^2 - 1 = (m+1)p$，因此 p 会整除 $(k_m-2)k_m$，这迫使 $k_m = 0$ 或 $k_m = 2$，与 $k_m \ge 3$. 矛盾。因此 $(k_m-1)^2 - mp \le 4n-1$。然而，若 $(k_m-1)^2 - mp = 4n-1$，则 $k_m = 1$，这同样不可能。于是 $(k_m-1)^2 - mp < p$，因此 $r_p((k_m-1)^2) = (k_m-1)^2 - mp$.

现在 $\Gamma(k_m) = r_p((k_m-1)^2) + r_p(k_m+1-3n) = (k_m-1)^2 - mp + k_m + 1 - 3n - p$ 当 $k_m \le n+2 \le 3n-2$. 现在不等式 2.3 推出 $\Gamma(k_m) = k_m^2 - k_m + 2 - 3n - mp + p \ge p$，因此 k_m 是一个跳跃。

(iv) 为完成证明，我们注意到由不等式 2.4 和 2.5 可得

$$3n - k_m \le r_p\left((k_m-1)^2\right) = (k_m-1)^2 - mp \le 3n + k_m - 4.$$

□

下面的引理使我们能够基于引理 2.7 中找到的跳跃，找到更多跳跃。

引理 2.8 设 k_m 为引理 2.7 中的跳跃，且 $k \le n+2$. 若 $k_m < k \le 1 + \left\lfloor\sqrt{mp+p-1}\right\rfloor$ 则 k 是一个跳跃，并且

$$3n + k - 3 < r_p\left((k-1)^2\right) = (k-1)^2 - mp.$$

证明。显然，$k_m < k$ 推出 $mp \le (k_m-1)^2 < (k-1)^2$.。由于 $k \le \left\lfloor\sqrt{mp+p-1}\right\rfloor$，$(k-1)^2 \le mp+p-1$.。因此 $r_p((k-1)^2) = (k-1)^2 - mp$.

由于 $k \leq n+2$, $r_p(k+1-3n) = k+1-3n-p.$。我们知道， k 严格大于 $x^2-x+2-3n-mp$ 的正根，因此 $k^2-k+2-3n > mp.$。这意味着

$$\begin{aligned}\Gamma(k) =& r_p\left((k-1)^2\right) + r_p\left(k+1-3n\right) = (k-1)^2 - mp + k + 1 - 3n + p \\ =& k^2 - k + 2 - 3n - mp + p \geq p.\end{aligned}$$

于是 k 是一个跳跃。
由引理 2.7， $\left(1+\sqrt{4mp+12n-7}\right)/2 < k_m \leq k-1$，因此 $\left(3+\sqrt{4mp+12n-7}\right)/2 < k.$
所以 $0 < k^2-3k+4-mp-3n$，然后

$$3n+k-3 < (k-1)^2 - mp = r_p\left((k-1)^2\right).$$

□

注 2.9 注意，由引理 2.7，跳跃 k_m 满足 $3n-k_m-1 < r_p((k-1)^2) \leq 3n+k_m-4$；由引理 2.8，跳跃 $k > k_m$ 满足 $3n+k-3 < r_p((k-1)^2)$。现在，如果 k 不是跳跃且 $2 \leq k \leq n+2$，那么必然有 $r_p((k-1)^2) < 3n-k-1$，如下一个引理所示。

下面两个引理讨论总剩余，并将帮助我们计算区间 $[1, 4n].$ 内跳跃的总次数。我们只证明第一个引理，因为第二个引理的证明类似。

引理 2.10 设 $n \geq 2$、 $2 \leq k \leq n+2$ 和 $p = 4n-1$ 为素数。

(a) 若 $r_p((k-1)^2) < 3n-k-1$，则 $\Gamma(k) < p$ 且 $\Gamma(p+2-k) < p$。
(b) 若 $3n-k-1 \leq r_p((k-1)^2) < 3n+k-3$，则 $\Gamma(p+2-k) < p \leq \Gamma(k)$。
(c) 若 $3n+k-3 \leq r_p((k-1)^2)$，则 $p \leq \Gamma(p+2-k)$ 且 $p \leq \Gamma(k)$。

证明。
注意， $-(4n-1) \leq k+1-3n \leq -1$，因此 $r_p(k+1-3n) = k+1-3n+p.$ 类似地， $k \leq n+2$ 意味着 $0 \leq p+3-k-3n \leq p-1$，从而 $r_p(k^2)\, p+3-k-3n = p+3-k-3n.$

(a) 显然

$$\begin{aligned}\Gamma(k) =& r_p\left((k-1)^2\right) + r_p\left(k+1-3n\right),\\ =& r_p\left((k-1)^2\right) + p + k + 1 - 3n < p.\\ \Gamma(p+2-k) =& r_p\left((p-(k-1))^2\right) + r_p\left(p+3-k-3n\right),\\ =& r_p\left((k-1)^2\right) + p + 3 - k - 3n < p.\end{aligned}$$

(b) 此处 $\Gamma(k) = r_p((k-1)^2) + p + k + 1 - 3n \geq p$ 且 $\Gamma(p+2-k) = r_p((k-1)^2) + p + 3 - k - 3n < p.$

(c) 最后 $\Gamma(k) = r_p((k-1)^2) + p + k + 1 - 3n \geq p$ 且 $\Gamma(p+2-k) = r_p((k-1)^2) + p + 3 - k - 3n \geq p.$

注意，$2 \leq k \leq n+2$ 意味着 $0 \leq p+2-k \leq p$，因此 $\Gamma(p+2-k)$ 有定义。另外，当 $k = 0$ 或 $k = 1$时，$r_p(k^2) < 3n-k-1$ 且 $\Gamma(k) < p$。于是 $\Gamma(p+2-k)$ 没有定义，因为 $p+2-k > p.$ □

引理 2.11 设 $n \geq 2$、$p = 4n-1$ 为素数，且 $n+3 \leq k \leq 2n.$

(a) 若 $r_p((k-1)^2) < k-n-2$，则 $\Gamma(k) < p$，且 $\Gamma(p+2-k) < p$.(b) 若 $k-n-2 \leq r_p((k-1)^2) < 3n-k-1$，则 $\Gamma(k) < p \leq \Gamma(p+2-k)$。
(c) 若 $3n-k-1 \leq r_p((k-1)^2)$，则 $p \leq \Gamma(k)$，且 $\Gamma(p+2-k)$。

证明。（与引理 2.10 的证明非常相似。） □

3 跳跃分解

为便于后文引用，我们定义以下集合。

记号 3.1 对于 $p=4n-1$ 素数，记

$$\begin{aligned}
C_{<} &= \left\{k\in\{2,...,n+2\} \ : \ r_p\left((k-1)^2\right)<3n-k-1\right\},\\
C_{\vdash} &= \left\{k\in\{2,...,n+2\} \ : \ r_p\left((k-1)^2\right)\in[3n-k-1,3n+k-3)\right\},\\
C_{\geq} &= \left\{k\in\{2,...,n+2\} \ : \ r_p\left((k-1)^2\right)\geq 3n+k-3\right\},\\
D_{<} &= \left\{k\in\{n+3,...,2n\} \ : \ r_p\left((k-1)^2\right)<k-n-2\right\},\\
D_{\vdash} &= \left\{k\in\{n+3,...,2n\} \ : \ r_p\left((k-1)^2\right)\in[k-n-2,3n-k-1)\right\},\\
D_{\geq} &= \left\{k\in\{n+3,...,2n\} \ : \ r_p\left((k-1)^2\right)\geq 3n-k-1\right\}.
\end{aligned}$$

引理 3.2 设 $\ell\in\mathbb{Z}$ 和 $p=4n-1$ 为素数。

(a) 设 $\ell\geq 6$。若 $n=4\ell+2$ 或 $n=4\ell+3$，则 $n-3,n-1,n+1\in C_{\vdash}$和 $n-2,n,n+2\in C_{<}$.

(b) 设 $\ell\geq 4$。若 $n=4\ell+1$ 或 $n=4\ell+4$，则 $n-3,n-1,n+1\in C_{<}$ 和$n-2,n,n+2\in C_{\vdash}$.

证明。表 1 总结了在 n 的四种不同情形（分别为 $4\ell+1,4\ell+2,4\ell+3$ 和 $4\ell+4$, $\ell\geq 4$.）下，$(k-1)^2$ 对于 $k=n-3,n-2,n-1,n,n+1$ 和 $n+2$ 的剩余。

我们只验证表 1 的第一列，也就是说，我们将计算当 $k=n-3.$ 时 $(k-1)^2$ 的剩余

$$\begin{aligned}
(4\ell-3)^2 &= (16\ell+3)(\ell-2)+5\ell+15, \quad 0\leq 5\ell+15\leq 16\ell+2,\\
(4\ell-2)^2 &= (16\ell+7)(\ell-2)+9\ell+18, \quad 0\leq 9\ell+18\leq 16\ell+6,\\
(4\ell-1)^2 &= (16\ell+11)(\ell-2)+13\ell+23, \quad 0\leq 13\ell+23\leq 16\ell+10,\\
(4\ell)^2 &= (16\ell+15)(\ell-1)+\ell+15, \quad 0\leq \ell+15\leq 16\ell+14.
\end{aligned}$$

给定 n、k，记 $I_n^k=[3n-k-1,3n+k-3)$ 和 $\Delta_n^k=r_p((k-1)^2)$。

(a) 考虑 $n=4\ell+2$ 和 $k=n-3$，则 $I_n^k=[8\ell+6,16\ell+2)$。根据表 1，$\Delta_n^k=9\ell+18.$ 我们观察到，如果 $\ell\geq 3$, $\Delta_n^k\in I_n^k.$ 同样地，如果 $k=n-1$, $I_n^k=[8\ell+4,16\ell+4)$ 且 $\Delta_n^k=9\ell+7\in I_n^k$ 对于 $\ell\geq 1.$ 如果 $k=n+1$, $I_n^k=[8\ell+2,16\ell+6)$ 且 $\Delta_n^k=9\ell+4\in I_n^k$ 对于 $\ell\geq 0.$ 因此，对于 $\ell\geq 6$, $n-3$, $n-1$, $n+1\in C_{\vdash}$.

注意，当 $\ell\geq 1.$ 时，若 $k=n-2,\Delta_n^k=\ell+8\notin[8\ell+5,16\ell+3)=I_n^k$。
同样，当 $\ell\geq 0.$ 时，若 $k=n,\Delta_n^k=\ell+1\notin[8\ell+3,16\ell+5)=I_n^k$

	k					
	$n-3$	$n-2$	$n-1$	n	$n+1$	$n+2$
$n=4\ell+1$ $p=16\ell+3$	$5\ell+15$	$13\ell+10$	$5\ell+4$	$13\ell+3$	$5\ell+1$	$13\ell+4$
$n=4\ell+2$ $p=16\ell+7$	$9\ell+18$	$\ell+8$	$9\ell+7$	$\ell+1$	$9\ell+4$	$\ell+2$
$n=4\ell+3$ $p=16\ell+11$	$13\ell+23$	$5\ell+11$	$13\ell+12$	$5\ell+4$	$13\ell+9$	$5\ell+5$
$n=4\ell+4$ $p=16\ell+15$	$\ell+15$	$9\ell+16$	$\ell+4$	$9\ell+9$	$\ell+1$	$9\ell+10$

表 1：当 $k=n-3,n-2,...,n+2$ 时， $n.$的不同情形下 $(k-1)^2$ 的剩余

最后，如果 $k=n+2,\Delta_n^k=\ell+2\notin[8\ell+1,16\ell+7)=I_n^k$当 $\ell\geq 1$.因此 $n-2,n,n+2\notin C_{\vdash)}$当 $\ell\geq 1$，事实上， $n-2,n,n+2\in C_<$对于 $\ell\geq 1.$情形 $n=4\ell+3$ 类似。

(b) 此情形的证明类似。

□

注3.3 如果 $n>3$ 要么 $\Gamma(n+2)<p\leq\Gamma(n+1)$，要么 $\Gamma(n+1)<p\leq\Gamma(n+2)$。

证明。由引理 3.2，若 $n=4\ell+2$ 或 $n=4\ell+3$ 且 $\ell\geq 6$，则$n+1\in C_{\vdash)}$ 且 $n+2\in C_<.$。由引理 2.10， $\Gamma(n+2)<p\leq\Gamma(n+1)$。由引理 3.2，若 $n=4\ell+1$ 或 $n=4\ell+4$ 且 $\ell\geq 4$，则 $n+1\in C_<$且 $n+2\in C_{\vdash)}.$。由引理 2.10， $\Gamma(n+1)<p\leq\Gamma(n+2)$。

我们只需验证情形 $n=5$、6、8、11、12、15 和 18，因为情形 $n=4$、7、9、10、13、16 和 19 得不到素数。

(i) 如果 $n=5$，那么 $n+2\in C_{\vdash)}=\{5,7\}$ 且 $n+1\in C_<=\{2,3,4,6\}.$

(ii) 若 $n=6$，则 $n+1\in C_{\vdash)}=\{5,7\}$ 且 $n+2\in C_<=\{2,3,4,6,8\}.$

(iii) 若 $n=8$，则 $n+2\in C_{\vdash}=\{6,8,10\}$ 且 $n+1\in C_{<}=\{2,3,4,5,7,9\}$.
(iv) 若 $n=11$，则 $n+1\in C_{\vdash}=\{7,10,12\}$ 且 $n+2\in C_{<}$.(v) 若 $n=12$，则 $n+2\in C_{\vdash}=\{7,10,12,14\}$ 且 $n+1\in C_{<}$.

(vi) 若 $n=15$，则 $n+1\in C_{\vdash}=\{8,11,14,16\}$ 且 $n+2\in C_{<}$.

(vii) 若 $n=18$，则 $n+1\in C_{\vdash}=\{8,12,15,17,19\}$ 且 $n+2\in C_{<}$.

应用引理 2.10 即可得到该结果。

注意，当 $n=3$、$C_{\vdash}=\{4,5\}$、$C_{<}=\{2,3\}$ 时，在这种情况下，$\Gamma(n+1)=16$ 和 $\Gamma(n+2)=13$ 均大于 $p=11$. □

下面两个引理使我们能够具体计算 $C_{\geq}$. 的基数

引理 3.4 设 $n>3$、$p=4n-1$ 为素数，且 $M_0=\lfloor(n^2-4n+5)/p\rfloor$。定义 $\ell_m=1+\lfloor\sqrt{mp+p-1}\rfloor$，并考虑按引理 2.7 中所述定义的 k_m。设 $2\leq k\leq n+2$ 和 $0\leq m\leq M_0-1$.

如果 $k<k_0$、$k>\ell_{M_0}$ 或 $\ell_m<k\leq k_{m+1}$，那么 $k\notin C_{\geq}$. 。另外，如果 $k<k_0$ 或 $\ell_m<k<k_{m+1}$，那么 k 不是跳跃。

证明。考虑 $k<k_0=1+\lfloor(1+\sqrt{12n-7})/2\rfloor$。于是 $(2k-1)^2<12n-7$，由此可得 $(k-1)^2<3n-k-1\leq 4n-1$.。因此 $r_p((k-1)^2)=(k-1)^2<3n-k-1$.。由引理 2.10，$k\in C_{<}$，且 k 不是跳跃。

考虑 $k>\ell_{M_0}$.。注意到 $\ell_{M_0}=1+\lfloor\sqrt{Mp}\rfloor\geq n-1$.。由引理 3.2，$k\in C_{\vdash}$ 或 $k\in C_{<}$. 。若 $k=k_{m+1}$，根据引理 2.7 (iv)，$k\in C_{\vdash}$.

最后考虑 $\ell_m<k<k_{m+1}$.，于是

$$1+\sqrt{(m+1)p}<k<\frac{1+\sqrt{4(m+1)p+12n-7}}{2}.$$

因此

$$(m+1)p<(k-1)^2<(m+1)p+3n-k-1.$$

因此 $r_p((k-1)^2)=(k-1)^2-(m+1)p<3n-k-1$. 根据引理 2.10 和 3.2，$k$ 不是跳跃，且 $k\in C_{<}$. □

引理 3.5 设 n、p 和 M_0 如引理 2.7 中所述。那么 $k \in C_{\geq}$ 当且仅当存在 $m \in \{0, 1, ..., M_0\}$ 使得 $k_m < k \leq 1 + \left\lfloor \sqrt{mp + p - 1} \right\rfloor$.

证明。
由引理 2.8，若 $k_m < k \leq \ell_m$，则 k 是一个跳跃，且 $r_p((k-1)^2) > 3n + k - 3$. 注意到 $2 \leq k_0 < k.$。由于 $m \leq M_0$，我们有 $\ell_m \leq n + 2$，因此$2 \leq k \leq n + 2.$。所以 $k \in C_{\geq}$.

反过来，设 $k \in C_{\geq}.$。那么 $2 \leq k \leq n+2$，并且 $r_p((k-1)^2) \geq 3n+k-3$。注意到

$$[2, n+2] = [2, k_0] \cup (k_0, \ell_0] \cup (\ell_0, k_1] \cup (k_1, \ell_1] \cup \cdots \cup (k_{M_0}, \ell_{M_0}] \cup (\ell_{M_0}, n+2].$$

若 $k < k_0$、$k > \ell_{M_0}$ 或 $\ell_m < k \leq k_{m+1}$，由引理 3.4，$k \notin C_{\geq}$.

这就迫使 k 属于 $(k_m, \ell_m]$，其中某个 $m \in \{0, ..., M_0\}$，这正是我们想要的。□

4 跳跃的计数

本节将说明不同集合 $C_<$、$C_{\vdash)}$、$C_{\geq}$、$D_<$、$D_{\vdash)}$ 和 $D_{\geq}.$ 中的跳跃之间的关系。在可能的情况下，我们将计算不同的基数。本节中，我们考虑 $n > 3$ 和 $p = 4n - 1$，其中 $p = 4n - 1$ 是一个素数。

定理 4.1 函数 $f : C_{\geq} \longrightarrow D_<$ 定义如下

$$f(k) = 2n + 2 - k,$$

是良定义的且为双射。

证明。
考虑 $k \in C_{\geq}.$ 根据引理 2.8、3.5 和观察 2.9，存在$m \in \{0, 1, ..., M_0\}$，满足 $M_0 = \lfloor (n^2 - 4n + 5)/p \rfloor$，使得 $k_m < k \leq 1 + \left\lfloor \sqrt{mp + p - 1} \right\rfloor$ 且 $3n + k - 3 \leq (k-1)^2 - mp = r_p((k-1)^2)$，其中 k_m 是引理 2.10 中给出的跳跃。因此

$$0 \leq k^2 - 3k - 3n + 4 - mp, \tag{4.6}$$
$$k^2 - 2k + 1 - mp \leq 4n - 2. \tag{4.7}$$

令 $k_f = f(k) = 2n + 2 - k$. 我们先证明 $k_f \in D_<$. 现在

$$(k_f - 1)^2 = (n - k + m + 2)p + (k - 1)^2 - mp + n - k + 1 - p.$$

由不等式 4.6，令 $w = (k-1)^2 - mp + n - k + 1 - p.$ $w \geq -1.$；由注 2.6，$k^2 - 3k + 4 - 3n - mp \neq 0$，因此 $w \geq 0.$

注意，若不等式 4.7 取等号，则有 $(k-1)^2 = mp + p - 1$，因此同余式 $x^2 \equiv -1 \pmod{p}$ 有解，这不可能。因此

$$k^2 - 2k + 1 - mp < 4n - 2. \tag{4.8}$$

由不等式 4.7,

$$w = k^2 - 2k + 1 - mp + 2 - k - 3n < n - k. \tag{4.9}$$

显然 $n - k \leq 4n - 2$，因此 $w < p - 1.$。所以 $r_p((k_f - 1)^2) = w.$。由不等式 4.9，$0 \leq w < n - k$，这迫使 $k \leq n - 1$。此外，由不等式 4.9，因 $k_f - n - 2 = n - k$，我们得出 $r_p((k_f - 1)^2) = w < k_f - n - 2.$

最后，$2 \leq k \leq n - 1$ 推出 $n + 3 \leq k_f \leq 2n$，因此 f 可定义为 $k_f \in D_<$.

$\widehat{\ }$ $\widehat{\ }$显然，f 是单射。现在取 $k \in D_<.$，则 $n + 3 \leq k \leq 2n$ 且

$$r_p\left((\widehat{k} - 1)^2\right) < \widehat{k} - n - 2. \tag{4.10}$$

$\widehat{\ }$考虑 $k = 2n + 2 - k$ 和 $\widehat{m} \in \mathbb{Z}$，其中

$$\widehat{m} \leq (\widehat{k} - 1)^2 < \widehat{m} \cdot p + p. \tag{4.11}$$

于是 $2 \leq k \leq n - 1$ 且

$$(k - 1)^2 = (n - \widehat{k} + \widehat{m}) \cdot p + (\widehat{k} - 1)^2 - \widehat{m}p + n - \widehat{k} + 1 - p.$$

考虑 $m = n - \widehat{k} + \widehat{m}$ 和 $u = (\widehat{k} - 1)^2 - \widehat{m}p + n - \widehat{k} + 1 - p.$

$\widehat{\ }$由于 $k \leq 5n$，不等式 4.11 推出

$$0 \leq n - \widehat{k} + 1 - p \leq (k - 1)^2 - \widehat{m}p + n - \widehat{k} + 1 - p. \tag{4.12}$$

同样根据不等式 4.10，有 $(k-1)^2 - \widehat{m}p + n - \widehat{k} + 1 - p < p - 1$，因此 $0 \leq u < p - 1.$ 所以 $r_p((k - 1)^2) = (k - 1)^2 - mp = u.$

最后，不等式 4.12 推出 $u \geq 5n - \widehat{k} \geq 5n - 1 - \widehat{\ }$ $k = 3n + k - 3.$因此 $r_p((k - 1)^2) \geq 3n + k - 3$，即 $k \in C_\geq.$ 显然 $f(k) = \widehat{k}$，那么 f是双射的。 □

引理 4.2 设 y, z 为 $C_{\vdash}$. 中的最后两个元素。若 $k \in C_{\vdash} - \{y, z\}$，则

$$mp + p \leq (n-2)^2 + 1, \tag{4.13}$$

其中 $m = m(k) = \lfloor (k-1)^2/p \rfloor$.

证明。

（a）情形 $n = 4\ell + 2$ 或 $n = 4\ell + 3$, $\ell \geq 6$. 由引理 3.2, $k \in C_{\vdash} - \{y, z\}$ 蕴含 $k \leq n - 3$. 因此 $m \leq \ell - 2 = \lfloor (n-4)^2/p \rfloor$. 若 $n = 4\ell + 2$ 则$mp + p \leq (\ell - 1)(16\ell + 7) \leq 16\ell^2 + 1 = (n-2)^2 + 1$.若 $n = 4\ell+3$ 则 $mp+p \leq (\ell-1)(16\ell+11) \leq 16\ell^2+8\ell+2 = (n-2)^2+1$。

（b）情形 $n = 4\ell + 1$ 或 $n = 4\ell + 4$, $\ell \geq 4$. 由引理 3.2, $k \in C_{\vdash} - \{y, z\}$ 蕴含 $k \leq n - 2$. 若 $n = 4\ell + 1$ 则 $m \leq \lfloor (n-3)^2/p \rfloor = \ell - 2$. 因此$mp + p \leq (\ell - 1)(16\ell + 3) \leq 16\ell^2 - 8\ell + 2 = (n-2)^2 + 1$.若 $n = 4\ell+4$则 $m \leq \lfloor (n-3)^2/p \rfloor = \ell-1$. 因此 $mp+p \leq \ell\cdot(16\ell+15) \leq 16\ell^2 + 16\ell + 5 = (n-2)^2 + 1$.

（c）剩下的情形只有 $n = 5$、6、8、11、12、15 和 18，因为候选项 $n =$ 4、7、9、10、13、14、16、19、22、23 并不提供素数。

(i) 若 $n = 5$ 或 6，则 $C_{\vdash}$ 只有两个元素。因此，不等式 4.13 显然成立。(ii) 若 $n = 8$ ，则 $C_{\vdash} = \{6, 8, 10\}$ 且 $k = 6$. 因此 $m(k) = 0 = \lfloor (k-1)^2/p \rfloor = \lfloor 25/31 \rfloor$ 显然满足不等式 4.13。(iii) 若 $n = 11$ ，则 $C_{\vdash} = \{7, 10, 12\}$ 且 $k = 7$. 因此 $m(k) = 0$显然满足不等式 4.13。(iv) 若 $n = 12$ ，则 $C_{\vdash} = \{7, 10, 12, 14\}$. 若 $k = 10$，则 $m(k) = 1 = \lfloor (k-1)^2/p \rfloor = \lfloor 81/47 \rfloor$ 显然满足不等式 4.13，因为 $94 \leq 101$。显然， $m(7)$ 也满足。(v) 若 $n = 15$ ，则 $C_{\vdash} = \{8, 11, 14, 16\}$. 若 $k = 11$，则 $m = 1 = \lfloor (k-1)^2/p \rfloor = \lfloor 100/59 \rfloor$ 显然满足不等式 4.13，因为 $118 \leq 169$。显然， $m(8)$ 也满足。(vi) 若 $n = 18$ ，则 $n + 1 \in C_{\vdash} = \{8, 12, 15, 17, 19\}$. 若 $k = 15$，则$m(k) = 2 = \lfloor (k-1)^2/p \rfloor = \lfloor 196/71 \rfloor$ 显然满足不等式 4.13，因为 $213 \leq 256$。显然， $m(8)$ $m(12)$ 也满足不等式 4.13。

□

引理 **4.3** $k \in D_{\vdash}$ 当且仅当存在一个整数 m，使得 $1 \le m \le \lfloor (n^2-4n+5)/p \rfloor$ 且

$$k = 2n - \left\lfloor \sqrt{mp-1} \right\rfloor .$$

证明。

⇒) 令 $k \in D_{\vdash}$，并定义 $\alpha = 2n+1-k.$。于是 $1 \le \alpha \le n-2$，且

$$(k-1)^2 = 4n^2 + \alpha^2 - 4n\alpha = (n-\alpha+m)p + \alpha^2 + n - \alpha - mp,$$

其中 m 满足 $mp \le \alpha^2+n-\alpha < (m+1)p.$。因此 $r_p((k-1)^2) = \alpha^2+n-\alpha-mp.$。由于 $k-n-2 \le r_p((k-1)^2) < 3n-k-1$，$mp-1 \le \alpha^2$ 且 $(\alpha-1)^2 < mp-1.$

于是 $\sqrt{mp-1} \le \alpha < \sqrt{mp-1}+1.$。由于 $x^2 \equiv -1$ (模 p) 无解，$\sqrt{mp-1}$ 不是整数。因此 $\alpha = \lfloor \sqrt{mp-1} \rfloor + 1.$

那么 $k = 2n - \lfloor \sqrt{mp-1} \rfloor$。

由于 $0 \le \alpha^2 + n - \alpha$，$m \ge 0.$ 现在 $(\alpha-1)^2 < mp-1$ 意味着 $1 \le m$.显然 $mp \le \alpha^2+1 \le (n-2)^2+1.$ 因此 $m \le (n^2-4n+5)/p.$

⇐) 取一个整数 m，满足 $1 \le m \le (n^2-4n+5)/p$ 且 $k = 2n - \lfloor \sqrt{mp-1} \rfloor$.

由于 $mp-1 \le (n-2)^2$，$n+2 \le k.$ 显然，$n+2=k$ 使我们得到 $x^2 \equiv -1$ (模 p) 的一个整数解，因此 $n+3 \le k.$ 此外 $1 \le m$意味着 $k \le 2n.$

考虑 $\alpha = \lfloor \sqrt{mp-1} \rfloor + 1.$。那么 $\sqrt{mp-1} \le \alpha < \sqrt{mp-1}+1.$ 显然 $\alpha \ne \sqrt{mp-1}+1$（否则 $x^2 \equiv -1$ (模 p) 有一个整数解），于是 $\sqrt{mp-1} < \alpha < \sqrt{mp-1}+1$。

因此 $mp-1 < \alpha^2$ 且 $(\alpha-1)^2 < mp-1.$ 由于 $\alpha < n-1$，$mp \le \alpha^2 \le \alpha^2+n-\alpha < n+\alpha-2+mp < mp+p.$ 由于

$$(k-1)^2 = (2n-\alpha)^2 = (n-\alpha+m)p + \alpha^2 + n - \alpha - mp,$$

$r_p((k-1)^2) = \alpha^2+n-\alpha-mp.$ 最后，由 $k-n-2 = n-\alpha-1 < r_p((k-1)^2) < n+\alpha-2 = 3n-k-1$，我们得出 $k \in D_{\vdash}$. □

定理 4.4 设 y, z 为 $C_{\vdash}$. 的最后两个元素。对于 $k \in C_{\vdash} - \{y, z\}$，考虑 $m = \lfloor (k-1)^2/p \rfloor$ 和 $u_0 = u_0(k)$，其中第一个不大于 $n+2$ 且满足 $x = u_0$ 的整数

$$(m+1)\, p \leq (k+x-1)^2 + 1. \tag{4.14}$$

那么，由下式定义的函数 $f:\ C_{\vdash} - \{y, z\} \longrightarrow D_{\vdash}$

$$f(k) = k_f = 2n + 2 - u_0 - k,$$

是良定义的且为双射。

证明。首先，我们将证明 f 是良定义的。不难验证 $u_0 = \left\lfloor \sqrt{(m+1)p} \right\rfloor + 2 - k$。根据 u_0 的定义，u_0、u_0+1.....满足不等式 4.14，但 $u_0 - 1$ 不满足。因此 u_0 满足

$$4n + mp \leq k^2 + 2k(u_0 - 1) + u_0^2 - 2u_0 + 3, \tag{4.15}$$

$$k^2 + 2k(u_0 - 2) + u_0^2 - 4u_0 + 6 < 4n + mp. \tag{4.16}$$

若 $k^2 = mp + 3n + 3k - 2$ 对于 $2 \leq k \leq n+2$ 成立，且我们定义 $x_0 = 2n - k + 1$，那么 $x_0^2 = (n+m-k+2)p + 1.$。因此 p 整除 $(x_0 - 1)(x_0 + 1)$，然而由于 $n \geq 3$ 且 $2 \leq k \leq n+2$，我们有

$$1 \leq 2n - k = x_0 - 1 < x_0 + 1 = 2n + 2 - k \leq 4n - 2,$$

这是不可能的。因此

$$k^2 \neq mp + 3n + 3k - 2. \tag{4.17}$$

注意，$u_0 \geq 1$ 由于 $x = 0$ 不满足不等式 4.14。另外，$u_0 \leq n+2$由于 $(k+n+1)^2 \geq (k-1)^2 + (n+2)^2 \geq mp + p - 1.$

为简化记号，定义

$$\begin{cases} m_f &= n + 2 - k - u_0 + m, \\ \Delta &= r_p\left((k-1)^2\right), \\ \Delta_f &= r_p\left((k_f - 1)^2\right), \\ w_f &= \Delta + k(2u_0 - 1) - p + n + u_0^2 - 3u_0 + 1. \end{cases}$$

为了检验 f 是否良定义，我们需要验证 $n + 3 \leq k_f \leq 2n$和 $k_f - n - 2 \leq \Delta_f < 3n - k_f - 1.$。不难验证

$$(k_f - 1)^2 = m_f \cdot p + w_f.$$

注意，$\Delta = r_p((k-1)^2) = (k-1)^2 - mp \le 3n-k-1$. 根据不等式 4.17, $\Delta \ge 3n-k$. 因此,

$$\begin{aligned} w_f &\ge 3n-k++k(2u_0-1)-p+n+u_0^2-3u_0+1, \\ &= k(2u_0-2)+u_0^2-3u_0+2, \\ &\ge u_0^2-3u_0+2=(u_0-2)(u_0-1)\ge 0. \end{aligned}$$

由不等式 4.16,

$$\begin{aligned} w_f &= k^2+2k(u_0-2)+u_0^2-4u_0+6-4n-mp+k+u_0+n-3, \\ &< k+u_0+n-3\le 4n-1. \end{aligned}$$

这表明 $w_f = r_p((k_f-1)^2)$。由于 $3n-k_f-1 = n-3+u_0+k$, $w_f < 3n-k_f-1$. 由于 $k_f-n-2 = n-u_0-k$, 不等式 4.15 推出 $w_f \ge k_f-n-2$. 因此 $k_f-n-2 \le r_p((k_f-1)^2) < 3n-k_f-1$. 根据引理 4.2, $x = n-k-1$ 满足不等式 4.14, 因此 $1 \le u_0 \le n-k-1$.因此 $n+3 \le k_f \le 2n$. 这证明了 $k_f \in D_{\vdash}$, 从而 f 是良定义的。

考虑 k_0 和 k_1, 使得 $k_f = f(k_0) = f(k_1)$。取 u_0, u_1, m_0 和 m_1, 使得 $m_0 = \lfloor (k_0-1)^2/p \rfloor$, $m_1 = \lfloor (k_1-1)^2/p \rfloor$, 并且 u_0, u_1 是使不等式 4.14 分别对 $k=k_0$ 和 $k=k_1$ 成立的第一个整数。

现在, $f(k_0) = f(k_1)$ 意味着 $u_0+k_0 = u_1+k_1$。由于

$$m_f = n+2-k_0-u_0+m_0 = n+2-k_1-u_1+m_1,$$

我们得出 $m_0 = m_1$. 由于

$$w_f = (k_0+u_0-1)^2-u_0-m_0p-p+n+1 = (k_1+u_1-1)^2-u_1-m_1p-p+n+1,$$

$u_0 = u_1$ 因此 $k_0 = k_1$. 所以 f 是单射。

现在取 $k_f \in D_{\vdash}$. 设 $m_f = \lfloor (k_f-1)^2/p \rfloor$。那么 $k_f-n-2 \le \Delta_f < 3n-k_f-1$. 注意到 $x=0$ 满足不等式

$$0 \le (k_f+x-1)^2+1-m_fp-px. \tag{4.18}$$

令 v_0 为大于或等于 1 且使得 $x = v_0$ 不满足不等式 4.18 的第一个整数。因此, $v_0 = x$ 满足等价不等式

$$\begin{aligned} (k_f+x-1)^2+1-m_fp-px<0, \\ \Delta_f+2k_fx+(x-1)^2-px<0. \end{aligned} \tag{4.19}$$

考虑 $k = 2n + 2 - v_0 - k_f$、 $m = n - k_f + m_f$和 $w = \Delta_f + k_f$（$2v_0 - 1$）$+ n +$ （$v_0^2 - 3v_0 + 1$） $- v_0 p + p$. 那么

$$\begin{aligned}(k-1)^2 &= (n+1-k_f+m_f)p + k_f^2 + k_f(2v_0-3) + n + 2 + v_0^2 - 3v_0 - v_0 p - mp, \\ &= (n-k_f+m_f)p + \Delta_f + k_f(2v_0-1) + n + (v_0^2 - 3v_0 + 1) - v_0 p + p, \\ &= mp + w.\end{aligned}$$

由引理 4.3，存在一个整数 $m, 1 \le m \le (n^2 - 4n + 5)/p$ 使得$k_f = 2n - \lfloor \sqrt{mp-1} \rfloor$. 此外，根据引理 4.3 的证明，若 $\alpha = 2n - k_f + 1$，则 $m_f = n - \alpha + m$. 取 $x_0 = \alpha - 1 = 2n - k_f$. 注意到 $x_0 \ge 1$ ，因为$\sqrt{mp-1} \ge 1$. 将 $x = x_0$代入（$k_f + x - 1$）$^2 + 1 - m_f p - px$，得到

$$(2n-1)^2 + 1 - (n - \alpha + m)p - p(\alpha - 1) = n + 3 - mp.$$

由于 $m \ge 1$, $n + 3 - mp < 0$. 那么 $x = x_0$满足不等式 4.19，因此v_0存在，且 $v_0 \le 2n - k_f$. 由于 $x = v_0 - 1$ 满足不等式 4.18，我们有

$$0 \le \Delta_f + k_f(2v_0 - 2) + (v_0 - 2)^2 + p - v_0 p.$$

因此 $w \ge k_f + n + v_0 - 3 = 3n - k - 1$. 由于 $k_f \ge n + 3$ 且 $v_0 \ge 1$ 我们得出 $w \ge 0$ 和 $2 \le k \le n - 2$.
由于 v_0 满足不等式 4.19，

$$w < n - k_f - v_0 + p = 5n - k_f - v_0 - 1 = 3n + k - 3 \le 4n - 1.$$

因此 $0 \le w < p$ 且 $3n - k - 1 \le w < 3n + k - 3$. 这意味着$w = r_p$ $((k-1)^2)$ $m = \lfloor (k-1)^2/p \rfloor$ 因此 $k \in C_{\vdash)}$. 引理 3.2 和引理 4.2 的证明表明， $\{y, z\}$ 是 $\{n-1, n, n+1, n+2\}$的子集，于是 $k \in C_{\vdash)} - \{y, z\}$.

现在我们来求 $u_0 = u_0(k)$。由于 $\Delta_f \ge k_f - n - 2$,

$$\begin{aligned}(k + v_0 - 1)^2 + 1 &= (2n + 1 - k_f)^2 + 1, \\ &= (n - k_f + m_f + 1)p + \Delta_f + n - k_f + 2, \\ &= (m+1)p + \Delta_f + n - k_f + 2 \ge (m+1)p.\end{aligned}$$

由 $\Delta_f < 3n - k_f - 1 = p - n - k_f$，我们得到

$$\begin{aligned}(k + v_0 - 2)^2 + 1 &= (2n - k_f)^2 + 1, \\ &= (n - k_f + m_f + 1)p + \Delta_f + k_f + n - p, \\ &= (m+1)p + \Delta_f + k_f + n - p < (m+1)p.\end{aligned}$$

因此 $u_0 = v_0$和 $f(k) = k_f$. 于是 f是满射，因而是双射。□

推论 4.5 $\left|D_{\vdash\rightarrow}\right| = \lfloor (n^2 - 4n + 5)/2 \rfloor$ 和

$$\left|C_{\geq}\right| = \left|D_{<}\right|, \quad \left|C_{\vdash\rightarrow}\right| = \left|D_{\vdash\rightarrow}\right| + 2, \quad \left|C_{<}\right| = \left|D_{\geq}\right| + 1.$$

证明。从引理 4.1 $|C_{\geq}| = |D_{<}|$. 4.4 $|C_{\vdash\rightarrow}| = |D_{\vdash\rightarrow}| +$.，从定理 .，由于 2. $n + 1 = |C_{<}| + |C_{\vdash\rightarrow}| + |C_{\geq}|$ 和 $n - 2 = |D_{<}| + |D_{\vdash\rightarrow}| + |D_{\geq}|$，我们有

$$n + 1 = \left|C_{<}\right| + \left|D_{<}\right| + \left|D_{\vdash\rightarrow}\right| + 2 = \left|C_{<}\right| + n - \left|D_{\geq}\right|,$$

因此，要证明 $|C_{<}| = |D_{\geq}| + 1$. To see that $|D_{\vdash\rightarrow}| = \lfloor (n^2 - 4n + 5)/2 \rfloor$，只需证明引理 4.3 中由每个 m 给出的所有 $k's$ 彼此不同，而这确实成立，因为

$$\sqrt{mp - 1} + 1 < \sqrt{(m+1)p - 1}.$$

□

定理 4.6 在定理 4.4 的假设下,

$$\left|\{k \in \mathbb{Z} \mid 2 \leq k \leq 4n - 1,\ \Gamma(k) \geq p\}\right| = 2n - 2.$$

证明。令 $J_\Gamma = \{k \in \mathbb{Z} : \quad 2 \leq k \leq 4n - 2, \ \Gamma(k) \geq p\}$。由引理 2.10 和引理 2.11,

$$\begin{aligned}J_\Gamma \cap [2, n+2] &= C_{\vdash\rightarrow} \cup C_{\geq}, \\ J_\Gamma \cap [n+3, 2n] &= D_{\geq}.\end{aligned}$$

$$
\begin{aligned}
&\big|J_\Gamma \cap [2n+1, 3n-2]\big| \\
&\qquad = \Big|\{2n+1 \le k \le 3n-2 \ \mid \ \Gamma(k) \ge p\}\Big|, \\
&\qquad = \Big|\{2n+1 \le p+2-k \le 3n-2 \ \mid \ \Gamma(p+2-k) \ge p\}\Big|, \\
&\qquad = \Big|\{n+3 \le k \le 2n \ \mid \ \Gamma(p+2-k) \ge p\}\Big| = \big|D_{\vdash\!\rightarrow}\big| + \big|D_{\ge}\big|.
\end{aligned}
$$

$$
\begin{aligned}
&\big|J_\Gamma \cap [3n-1, 4n-1]\big| \\
&\qquad = \Big|\{3n-1 \le k \le 4n-1 \ \mid \ \Gamma(k) \ge p\}\Big|, \\
&\qquad = \Big|\{3n-1 \le p+2-k \le 4n-1 \ \mid \ \Gamma(p+2-k) \ge p\}\Big|, \\
&\qquad = \Big|\{2 \le k \le n+2 \ \mid \ \Gamma(p+2-k) \ge p\}\Big| = \big|C_{\ge}\big|.
\end{aligned}
$$

利用这些恒等式和推论 4.5，我们得到

$$
\begin{aligned}
\big|J_\Gamma\big| &= \big|C_{\vdash\!\rightarrow}\big| + 2\big|C_{\ge}\big| + \big|D_{\vdash\!\rightarrow}\big| + 2\big|D_{\ge}\big|, \\
&= \big|C_{\vdash\!\rightarrow}\big| + 2\big|C_{\ge}\big| + \big|C_{\vdash\!\rightarrow}\big| - 2 + 2\left(\big|C_{<}\big| - 1\right), \\
&= 2\left(\big|C_{<}\big| + \big|C_{\vdash\!\rightarrow}\big| + \big|C_{\ge}\big|\right) - 4, \\
&= 2 \cdot \Big|\mathbb{Z} \cap [2, n+2]\Big| - 4 = 2n-2.
\end{aligned}
$$

□

下面的推论由前一个定理的证明得出。

推论 4.7 在定理 4.4 的假设下，

$$
\Big|\,\{k \in \mathbb{Z} \ : \ 2 \le k \le 2n, \ \ \Gamma(k) \ge p\}\,\Big| = n,
$$

$$
\Big|\,\{k \in \mathbb{Z} \ : \ 2n+1 \le k \le 4n, \ \ \Gamma(k) \ge p\}\,\Big| = n-2.
$$

5 个和，涉及 $r_p\left(k^2-k+2-3n\right)$.

考虑 $J_n=\left|\{k\in\mathbb{Z}:\quad 2\le k\le n+2,\ \Gamma(k)\ \ge p\}\right|$，我们将 J_n 简称为跳跃数。现在我们将推导公式，建立 $k^2-k+2-3n$ 模 p.下各项的剩余之间的关系

定理 5.1 若 $n>3$ 且 $p=4n-1$ 是素数，则

$$\begin{aligned}
\sum_{k=1}^{p-1} r_p\left(k^2-k+2-3n\right) &= \sum_{k=1}^{p-1} r_p\left(k^2\right)+3n-2.\\
\sum_{k=1}^{2n} r_p\left(k^2-k+2-3n\right) &= \sum_{k=1}^{2n} r_p\left(k^2\right)+n.\\
\sum_{k=1}^{n} r_p\left(k^2-k+2-3n\right) &= \sum_{k=1}^{n} r_p\left(k^2\right)+\frac{n(n+1)}{2}-p(J_n-1-M).
\end{aligned}$$

证明。注意到

$$r_p(x+y)=\begin{cases} r_p(x)+r_p(y) & \text{if } r_p(x)+r_p(y)<p,\\ r_p(x)+r_p(y)-p & \text{if } r_p(x)+r_p(y)\ge p.\end{cases}$$

回忆一下，我们将 k 定义为跳跃，当 $\Gamma(k)\ =r_p((k-1)^2)+r_p(k+1-3n)\ \ge p.$ 根据定理 4.6,

$$
\begin{aligned}
&\sum_{k=2}^{4n-1} r_p\left(k^2-k+2-3n\right)\\
&\quad= \sum_{k:\Gamma(k)\geq p}\left(r_p\left((k-1)^2\right)+r_p\left(k+1-3n\right)-p\right)\\
&\qquad\qquad + \sum_{k:\Gamma(k)<p}\left(r_p\left((k-1)^2\right)+r_p\left(k+1-3n\right)\right),\\
&\quad= -p|J_\Gamma|+\sum_{k=2}^{p} r_p\left((k-1)^2\right)+\sum_{k=2}^{3n-2} r_p\left(k+1-3n\right)+\sum_{k=3n-1}^{4n-1} r_p\left(k+1-3n\right),\\
&\quad= -p(2n-2)+\sum_{k=1}^{p-1} r_p\left(k^2\right)+\sum_{k=2}^{3n-2}(k+1-3n+p)+\sum_{k=3n-1}^{4n-1}(k+1-3n),\\
&\quad= \sum_{k=1}^{p-1} r_p\left(k^2\right)+\sum_{k=2}^{4n-1}(k+1-3n)\ +\ p(2-2n+3n-3),\\
&\quad= \sum_{k=1}^{p-1} r_p\left(k^2\right)+3n-2.
\end{aligned}
$$

由于 $r_p\left(k^2-k+2-3n\right)=2-3n+p$ 对于 $k=0,p$ 结论得证。注意,

$$
\sum_{k=0}^{p-1} r_p\left(k^2-k+2-3n\right)=\sum_{k=1}^{p-1} r_p\left(k^2\right)+p.
$$

另外两个公式的推导类似。 □

将此结果与 [4] when $p=4n+1$ 中的定理 5.1 进行比较,

$$
\sum_{k=0}^{p-1} r_p\left(k^2+k+1-n\right)=\sum_{k=1}^{p-1} r_p\left(k^2\right)-p=p(2n-1).
$$

注 5.2 定理 5.1 中的前两个公式实际上对任意 n 均成立，但第三个公式仅对 $n>3.$ 成立。图表 2 和 3 给出了该定理排除的特殊情形下剩余 $r_p\left(k^2-k+2-3n\right)$ 的总和。

推论 5.3 若 $n>3$ 且 $p=4n-1$ 是素数，则

n	$\sum_{k=0}^{p-1} r_p\left(k^2-k+2-3n\right)$	$\sum_{k=0}^{p-1} r_p\left(k^2\right)+p$
1	5	5
2	21	21
3	55	55

表2：特殊情形下剩余 $r_p(k^2-k+2-3n)$ 的和。

n	$\sum_{k=0}^{2n} r_p\left(k^2-k+2-3n\right)$	$\sum_{k=0}^{2n} r_p\left(k^2\right)+2n+1$
1	5	5
2	14	14
3	32	32

表3：特殊情形下剩余 $r_p(k^2-k+2-3n)$ 的和。

$$\begin{aligned}
\sum_{k=1}^{p-1}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{p(p-5)+6-n}{3}-\frac{1}{p}\sum_{k=1}^{p-1} r_p\left(k^2\right).\\
\sum_{k=1}^{2n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{n(2n-1)(4n-7)}{3p}-\frac{1}{p}\sum_{k=1}^{2n} r_p\left(k^2\right).\\
\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{(n+1)(2n^2-23n+6)}{3p}-\frac{1}{p}\sum_{k=1}^{n} r_p\left(k^2\right)+J_n-M.
\end{aligned}$$

证明。由 $x=p\left\lfloor\frac{x}{p}\right\rfloor+r_p(x)$，可得若 $y=\sum_{k=1}^{p-1}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor$，则

$$\sum_{k=1}^{p-1}\left(k^2-k+2-3n\right)=py+\sum_{k=1}^{p-1} r_p\left(k^2-k+2-3n\right).$$

由定理 5.1,

$$\frac{(p-1)p(2p-1)}{6}-\frac{(p-1)p}{2}+(p-1)(2-3n)=py+\sum_{k=1}^{p-1} r_p\left(k^2\right)+3n-2,$$

then

$$p\cdot\frac{p\cdot(p-5)+6-n}{3}=py+\sum_{k=1}^{p-1} r_p\left(k^2\right).$$

结论得证。其余两个求和式的证明方法类似。 □

下面的引理和备注旨在找出一个公式，用于$\sum_{k=0}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor$.

引理 5.4 设 $Q_m=\dfrac{1+\sqrt{4mp+12n-7}}{2}$如记号 2.2 所述。则

$$\lfloor Q_m\rfloor=\max\{k\in\mathbb{N}\ :\ k^2-k+2-3n\le mp\}.$$

证明。显然，$\lfloor Q_m\rfloor\le Q_m<\lfloor Q_m\rfloor+1$，并且由于 Q_m是$x^2-x+2-3n=mp$的非负根，$k_0=\lfloor Q_m\rfloor$满足 $0\le k_0\le Q_m$，且 $k_0^2-k_0+2-3n\le mp.$。因此，$k_1=\lfloor Q_m\rfloor+1$ 满足 $0\le k_1$，且 $k_1^2-k_1+2-3n>mp.$。若$k_0=0$，则 $k_1=1$，从而 $p\le mp<2-3n$，这是不可能的，因此
$k_0\in\mathbb{N}$. □

观察 5.5 由引理 2.5，不存在整数 k,m,n 使得$\lfloor Q_m\rfloor=Q_m$，即 $k^2-k+2-3n\ne mp$，无论 k,m,n.为何

定理 5.6 设 $n>3$ 和 $p=4n-1$ 为素数。那么

$$\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor=(M-1)n-\sum_{m=0}^{M-1}\lfloor Q_m\rfloor.$$

证明。由于 $n>3,1\le M.$ 定义，$t_m=\lfloor Q_m\rfloor$ 且

$$H_m=\begin{cases}\{1,...,t_0\} & \text{if } m=0,\\ \{t_{m-1}+1,t_{m-1}+2,...,t_m\} & \text{if } 1\le m\le M-1,\\ \{t_{M-1}+1,t_{M-1}+2,...,n\} & \text{if } m=M.\end{cases}$$

由引理 5.4，$k=\lfloor Q_m\rfloor$ 满足 $k^2-k+2-3n\le mp$；又由观察 5.5，$k^2-k+2-3n<mp.$。因此，由引理 5.4，对于 $k\in H_m$，我们有

$$(m-1)p<k^2-k+2-3n<mp.$$

对于这样的 k，必然有 $\lfloor(k^2-k+2-3n)/p\rfloor=m-1.$

注意，$\{H_0, H_1, ..., H_M\}$ 是 $\{1, 2..., n\}$ 的一个划分，因为 $Q_{M-1} < n < Q_M$ （见 [3] 中的引理 2.5）。因此

$$\begin{aligned}\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \sum_{m=0}^{M}\sum_{\substack{k=0\\k\in H_m}}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor,\\ &= \sum_{m=0}^{M}(m-1)|H_m|,\\ &= -t_0+0(t_1-t_0)+1(t_2-t_1)+\cdots,\\ &\quad +(M-2)(t_{M-1}-t_{M-2})+(M-1)(n-t_{M-1}),\\ &= -\sum_{m=0}^{M-1}\lfloor Q_m\rfloor+(M-1)n.\end{aligned}$$

□

推论 5.7 若 $n > 3$ 和 $p = 4n - 1$ 是素数，则

$$\sum_{k=0}^{n}\left\lfloor\frac{k^2}{p}\right\rfloor+\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor=\frac{n(n-5)}{6}+M-\frac{1}{2p}\sum_{k=1}^{p-1}r_p\left(k^2\right).$$

证明。由 [6] （第 253 页）可得

$$\sum_{m=1}^{M}\lfloor R_m\rfloor = Mn-\sum_{k=0}^{n}\left\lfloor\frac{k^2}{p}\right\rfloor. \tag{5.20}$$

[3]中的推论 2 指出

$$\frac{1}{2}\sum_{k=1}^{p-1}r_p\left(k^2\right)=p\left(\sum_{m=1}^{M}\lfloor R_m\rfloor+\sum_{m=0}^{M-1}\lfloor Q_m\rfloor\right)-Mp(2n-1)+\frac{p\cdot(n^2+n)}{6}. \tag{5.21}$$

将定理 5.6 和方程 5.20 代入方程 5.21，可得

$$\begin{aligned}\frac{1}{2}\sum_{k=1}^{p-1}r_p\left(k^2\right) &= p\left((2M-1)n-\sum_{k=1}^{n}\left\lfloor\frac{k^2}{p}\right\rfloor-\sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor\right)\\ &\quad -Mp(2n-1)+\frac{p\cdot(n^2+n)}{6}.\end{aligned}$$

结果由此得出。 □

将推论 5.7 与定理 2.2（情形 $p = 4n + 1$）进行比较，在 [4] 中可将其改写为

$$\sum_{k=0}^{n} \left\lfloor \frac{k^2}{p} \right\rfloor + \sum_{k=1}^{n} \left\lfloor \frac{k^2 + k + 1 - n}{p} \right\rfloor = \frac{(n+3)(n+2)}{6} + M - \frac{1}{2p} \sum_{k=1}^{p-1} r_p\left(k^2\right) + u_n.$$

推论 5.8 若 $n > 3$ 且 $p = 4n - 1$ 是素数，则

$$\sum_{m=1}^{M} \lfloor R_m \rfloor - \sum_{m=0}^{M-1} \lfloor Q_m \rfloor = J_n - M - 1.$$

证明。由引理 2.10、4.3 和 3.5 可得

$$\begin{aligned} J_n &= |C_{[\mapsto)}| + |C_{\geq}| = |D_{[\mapsto)}| + 2 + |C_{\geq}|, \\ &= M_0 + 2 + \sum_{m=0}^{M_0} (\ell_m - k_m), \\ &= M + 1 + \sum_{m=0}^{M_0} (\lfloor R_{m+1} \rfloor - \lfloor Q_m \rfloor), \\ &= M + 1 + \sum_{m=1}^{M} \lfloor R_m \rfloor - \sum_{m=0}^{M-1} \lfloor Q_m \rfloor. \end{aligned}$$

□

比较 [4] 中的推论 5.8 与定理 5.3（情形 $p = 4n + 1$）

$$\sum_{m=1}^{M} \lfloor R_m \rfloor - \sum_{m=0}^{M} \lfloor S_m \rfloor = j_n + 2 - n - u_n.$$

6 类数恒等式

本节将建立一些恒等式，涉及当 p 具有 $p=4n-1.$ 的形式时，虚二次域 $\mathbb{Q}(\sqrt{-p})$ 的类数 $h=h(-p)$。这些恒等式基于我们在前几节推导出的公式。

在 [3], 中，我们有

$$\begin{aligned} h &= (2M+1)(2n-1)-2\left(\sum_{m=1}^{M}\lfloor R_m\rfloor-\sum_{m=0}^{M-1}\lfloor Q_m\rfloor\right)-\frac{n^2+n}{3}. \\ h &= \frac{p-1}{2}-\frac{1}{p}\sum_{k=1}^{p-1}r_p\left(k^2\right). \end{aligned}$$

由推论 5.3、5.7 以及 $\sum_{k=1}^{p-1}r_p(k^2)=2\sum_{k=1}^{2n}r_p(k^2)-2n$，我们得到

推论 6.1

$$\begin{aligned} \sum_{k=1}^{p-1}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= h+\frac{16n^2-35n+15}{3}. \\ \sum_{k=1}^{2n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{h}{2}+\frac{4n^2-14n+9}{6}. \\ \sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{h}{4}+\frac{J_n}{2}+\frac{n^2-17n-3}{12}. \\ \sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{h}{2}+M+\frac{n^2-11n+3}{6}-\sum_{k=1}^{n}\left\lfloor\frac{k^2}{p}\right\rfloor. \\ \sum_{k=1}^{n}\left\lfloor\frac{k^2-k+2-3n}{p}\right\rfloor &= \frac{h}{2}+\sum_{m=1}^{M}\lfloor R_m\rfloor+M(1-n)+\frac{n^2-11n+3}{6}. \end{aligned}$$

由推论 5.8 可得

推论 6.2

$$\begin{aligned}\frac{J_n}{2}+M(n-1) &= \frac{h}{4}+\sum_{m=1}^{M}\lfloor R_m\rfloor+\frac{n^2-5n+9}{12}.\\ -\frac{J_n}{2}+Mn &= \frac{h}{4}+\sum_{m=0}^{M-1}\lfloor Q_m\rfloor+\frac{n^2-5n-3}{12}.\\ \frac{J_n}{2}+\sum_{k=1}^{n-1}\left\lfloor\frac{k^2}{p}\right\rfloor &= \frac{h}{4}+\frac{n^2-5n+9}{12}.\end{aligned}$$

由定理 5.1 可知

推论 6.3

$$\begin{aligned}\sum_{k=1}^{p-1} r_p\left(k^2-k+2-3n\right) &= p\cdot(2n-h)-n-1.\\ \sum_{k=1}^{2n} r_p\left(k^2-k+2-3n\right) &= \frac{p\cdot(2n-h)+1}{2}.\\ \sum_{k=1}^{n} r_p\left(k^2-k+2-3n\right) &= \frac{p}{4}(3n+2-2J_n-h)-\frac{(n+1)(n-1)}{4}.\end{aligned}$$

最后，将这个公式与定理 5.1 结合起来，我们得到

推论 6.4

$$\sum_{k=1}^{n} r_p\left(k^2\right)=\frac{p}{4}(2J_n+2n-3-4M-h)+\frac{n(n+1)}{4}.$$

我们得到的数值数据使我们可以提出以下

猜想 6.5 考虑所有满足 $p=4n-1$ 为素数的 n。那么

$$\lim_{n\to\infty}\frac{J_n}{n}=\frac{3}{8}.$$

猜想 6.6 考虑所有满足 $p = 4n - 1$ 为素数的 n。那么

$$\lim_{n\to\infty} \frac{\sum_{m=1}^{M} \lfloor R_m \rfloor + \sum_{m=0}^{M-1} \lfloor Q_m \rfloor}{Mp + 2n} = \frac{1}{3}.$$

此外， $\sum_{m=1}^{M} \lfloor R_m \rfloor + \sum_{m=0}^{M-1} \lfloor Q_m \rfloor$ 的一个良好估计是 $\lfloor (Mp + 2n)/3 \rfloor$.

参考文献

[1] H. Cohen, 《计算代数数论教程》, 数学研究生教材第138卷, 施普林格出版社, 纽约, 1993年。

[2] P. G. L. Dirichlet, 定理的证明: 每个首项和公差互素且均为整数的无限算术级数, 都包含无穷多个素数。普鲁士皇家科学院论丛, 《普鲁士皇家科学院论丛》, （1837）, 第45—81页。

[3] J. Garcia, 虚二次域 $\mathbb{Q}(\sqrt{-p})$ $p = 4n - 1$类数的一个可计算公式, 《电子研究档案》, 29（2021）, 第3853–3865页。

[4] ——, 模形如$p = 4n + 1$的素数的二次剩余和, 2022。

[5] W. Narkiewicz, 《代数数论的初等与解析理论》, 施普林格, 2004。[6] C. Zeller, 关于算术级数中最大整数的和, 《哥廷根皇家科学学会及乔治-奥古斯特大学通讯》, 1879年5月14日。