A COMPLETE DETERMINATION OF THE COMPLEX QUADRATIC FIELDS OF CLASS-NUMBER ONE

H. M. Stark

1. INTRODUCTION

Let h(d) be the class-number of the quadratic extension of the rationals of discriminant d. In the case of complex quadratic fields, it has long been known that

$$h(-p) = 1 \qquad \text{for } p = 3,\ 4,\ 7,\ 8,\ 11,\ 19,\ 43,\ 67,\ 163\,.$$

Heilbronn and Linfoot [5] have shown that there is at most one more value of p for which h(-p) = 1, and the author has shown [7] that if such an additional value p exists, then $p > \exp(2.2 \cdot 10^7)$. Heegner [3] attempted to show that the above nine values of p give the only complex quadratic fields of class-number 1. Unfortunately, it is thought that there is a gap in Heegner's proof, possibly traceable to one of his references, Weber [8]. Nevertheless, it will be instructive to examine briefly Heegner's method.

Put

$$f(\omega) = q^{-1/24} \prod_{\nu=1}^{\infty} (1 + q^{2\nu-1}),$$

where $q = e^{\pi i \omega}$ and $\Im\omega > 0$. Also, put $\gamma_2(\omega) = f(\omega)^{16} - 16\, f(\omega)^{-8}$. It is known [8, Section 125] that when $p \equiv 3 \pmod 4$ and h(-p) = 1, $\gamma_2\left(\frac{-3+\sqrt{-p}}{2}\right)$ is a rational integer. Thus for $p \equiv 3 \pmod 4$ and h(-p) = 1, $f\left(\frac{-3+\sqrt{-p}}{2}\right)$ satisfies an equation of degree 24 with integral coefficients,

$$x^{24} - \gamma_2 x^8 - 16 = 0\,.$$

Heegner reduces this equation to one of degree 12,

$$x^{12} + 2\zeta x^8 + 2\zeta^2 x^4 - 4 = 0,$$

with the relation

$$-4\zeta(\zeta^3 + 4) = \gamma_2\,.$$

This equation in turn is reduced to an equation of degree 6,

$$x^6 + 2\alpha x^4 + 2\beta x^2 - 2 = 0,$$

with the relations

$$\zeta = 2(\beta - \alpha^2), \qquad \zeta^2 = 2(\beta^2 + 2\alpha)\,.$$

These relations can be combined to give the equation

Received November 25, 1966.

$$(1) \qquad (\beta - 2\alpha^2)^2 = 2\alpha(\alpha^3 + 1).$$

The surprising thing about all this is that for p = 3, 11, 19, 43, 67, and 163, α and β turn out to be rational integers. Heegner in fact claims that when $p \equiv 3 \pmod 8$ and h(-p) = 1, α and β must be rational integers (this is the point where the gap, if one exists, must occur). He then proceeds to find all integral solutions to (1). There are exactly six solutions to (1), corresponding to the six values of p listed above.

We should mention that if the numbers α and β satisfying (1) were not integers, but merely exceptionally close to integers, then equation (1) would still be satisfied by the integers nearest to α and β. In this paper, we describe a technique for producing numbers which, if not integers, are sufficiently close to integers to yield Diophantine equations that can be solved. As a result, we prove the following theorem:

THEOREM. *If* h(-p) = 1, *then* $p < 200$.

In view of the remarks at the end of the first paragraph, I have deemed it advisable not to introduce elliptic functions into this paper. However, the reader familiar with Kronecker's limit formula will see elliptic functions lurking in the background.

2. NOTATION AND NECESSARY LEMMAS

From this point on, the letter p will denote an integer ($p \geq 19$) such that h(-p) = 1. As a result [1, Vol. 3, p. 184], p is a prime $\equiv 3 \pmod 8$, and 3 is a nonresidue of p. Thus $p \equiv 19 \pmod{24}$. We set

$$Q(x, y) = x^2 + xy + \frac{p+1}{4} y^2.$$

Throughout, the letter k is reserved to be either k = 8 or k = 12, and $\chi(n) = \left(\frac{k}{n}\right)$ (Kronecker symbol) is a real character modulo k. By $\zeta(s)$ we denote the Riemann zeta function, and if d is the discriminant of a quadratic field, we put

$$L_d(s) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-s}.$$

For convenience, we write $e(x) = e^{2\pi i x}$.

LEMMA 1. *For* $s > 1$,

$$(2) \qquad \sum_{y=1}^{\infty} y^{1-2s} \sum_{j=0}^{k-1} \chi(Q(j, y)) = \begin{cases} 4^{2-2s}\zeta(2s-1)(-1+2^{2-2s}) & \text{if } k = 8, \\ 2^{2-2s}\zeta(2s-1)(-1+2^{2-2s})(-1+3^{2-2s}) & \text{if } k = 12. \end{cases}$$

Proof. Put $S(y) = \sum_{j=0}^{k-1} \chi(Q(j, y))$. From Table 1, we see that $\chi\left(n + \frac{k}{2}\right) = -\chi(n)$, both for k = 8 and k = 12. Thus, if y is odd,

$$\chi\left(Q\left(j + \frac{k}{2}, y\right)\right) = \chi\left(Q(j, y) + \frac{k}{2} y\right) = -\chi(Q(j, y)),$$

and hence $S(y) = 0$. If y is even, then

$$\chi(Q(j,\, y)) = \chi\left(\left(j + \frac{y}{2}\right)^2 + p\left(\frac{y}{2}\right)^2\right),$$

and therefore $S(y) = \sum_{j=0}^{k-1} \chi\left(j^2 + p\left(\frac{y}{2}\right)^2\right)$.

Making use of Table 1, we see that for $k = 8$,

$$\begin{aligned} S(2) = S(6) &= 2\chi(3) + 4\chi(4) + 2\chi(7) = 0\,, \\ S(4) &= 2\chi(4) + 4\chi(5) + 2\chi(0) = -4\,, \\ S(0) &= 2\chi(0) + 4\chi(1) + 2\chi(4) = 4\,. \end{aligned}$$

Thus for $k = 8$ and $s > 1$,

$$\begin{aligned} \sum_{y=1}^{\infty} y^{1-2s} \sum_{j=0}^{k-1} \chi(Q(j,\, y)) &= 4 \cdot 4^{1-2s} \sum_{n=1}^{\infty} \frac{(-1)^n}{n^{2s-1}} \\ &= 4^{2-2s}\left[-\sum_{n=1}^{\infty} n^{1-2s} + 2 \sum_{n=1}^{\infty} (2n)^{1-2s} \right] \\ &= 4^{2-2s}\, \zeta(2s - 1)(-1 + 2^{2-2s})\,. \end{aligned}$$

<u>k = 8</u>

$n =$	0	1	2	3	4	5	6	7
$\chi(n) =$	0	1	0	-1	0	-1	0	1

$n =$	0	1	4
$R_8(n) =$	2	4	2

<u>k = 12</u>

$n =$	0	1	2	3	4	5	6	7	8	9	10	11
$\chi(n) =$	0	1	0	0	0	-1	0	-1	0	0	0	1

$n =$	0	1	4	9
$R_{12}(n) =$	2	4	4	2

TABLE 1. $R_k(n)$ is the number of solutions of $x^2 \equiv n \pmod{k}$ $(0 \leq x < k)$.

From Table 1, we see that for $k = 12$,

$$\begin{aligned} S(2) = S(10) &= 2\chi(7) + 4\chi(8) + 4\chi(11) + 2\chi(4) = 2\,, \\ S(4) = S(8) &= 2\chi(4) + 4\chi(5) + 4\chi(8) + 2\chi(1) = -2\,, \\ S(6) &= 2\chi(3) + 4\chi(4) + 4\chi(7) + 2\chi(0) = -4\,, \\ S(0) &= 2\chi(0) + 4\chi(1) + 4\chi(4) + 2\chi(9) = 4\,. \end{aligned}$$

Thus, for $k = 12$ and $s > 1$,

$$\sum_{y=1}^{\infty} y^{1-2s} \sum_{j=0}^{k-1} \chi(Q(j, y)) = 2^{2-2s} \sum_{n=1}^{\infty} n^{1-2s} . \frac{S(2n)}{2}$$

$$= 2^{2-2s} \left\{ \sum_{n=1}^{\infty} n^{1-2s} - 2 \sum_{n=1}^{\infty} (2n)^{1-2s} - 3 \sum_{n=1}^{\infty} (3n)^{1-2s} + 6 \sum_{n=1}^{\infty} (6n)^{1-2s} \right\}$$

$$= 2^{2-2s} \zeta(2s - 1)(1 - 2^{2-2s} - 3^{2-2s} + 6^{2-2s})$$

$$= 2^{2-2s} \zeta(2s - 1)(-1 + 2^{2-2s})(-1 + 3^{2-2s}).$$

LEMMA 2. *Let* $I(s) = \int_{-\infty}^{\infty} \frac{e^{-iwv}}{(v^2 + 1)^s} dv$. *For* $1 \leq s \leq 2$ *and* $w \geq w_0 > 0$, *there exists a constant* c *such that* $|I(s)| < cwe^{-w}$.

Proof. We shorten the proof by appealing to known formulae involving Bessel functions [2, pp. 50-52]. For $1 \leq s \leq 2$ and $w \geq w_0 > 0$, we have the identities,

$$I(s) = 2 \int_0^{\infty} \frac{\cos wv}{(v^2 + 1)^s} dv = 2w^{2s-1} \int_0^{\infty} \frac{\cos v}{(v^2 + w^2)^s} dv$$

$$= \frac{2\sqrt{\pi}}{\Gamma(s)} \left(\frac{w}{2}\right)^{s-\frac{1}{2}} K_{s-\frac{1}{2}}(w) = \frac{\pi}{\Gamma(s)^2 \cdot 2^{s-1}} w^{s-1} e^{-w} \int_0^{\infty} e^{-v} v^{s-1} \left(1 + \frac{v}{2w}\right) dv,$$

where $K_{s-1/2}(w)$ is a modified Bessel function of the second kind and $\Gamma(s)$ is the Gamma function. But now, for $1 \leq s \leq 2$ and $w \geq w_0 > 0$, it is easy to see that there exist constants c_1 and c such that

$$|I(s)| < c_1 we^{-w} \left[\int_0^1 e^{-v} \left(1 + \frac{v}{2w_0}\right) dv + \int_1^{\infty} ve^{-v} \left(1 + \frac{v}{2w_0}\right) dv \right] < cwe^{-w}.$$

LEMMA 3. $h(-8p) \equiv 2 \pmod 4$, $h(-12p) \equiv 4 \pmod 8$. (Thus, there exist nonnegative integers M and N such that $h(-12p) = 8M + 4$ and $h(-8p) = 4N + 2$.)

Proof. We recall the formula for the class-number of a quadratic field of discriminant $d < 0$ [6, Satz 897],

$$h(d) = \frac{w}{2\left[2 - \left(\frac{d}{2}\right)\right]} \sum_{1 \leq j \leq \frac{|d|}{2}} \left(\frac{d}{j}\right), \tag{3}$$

where $w = 6$ if $d = -3$, $w = 4$ if $d = -4$, $w = 2$ if $d < -4$. Put $p = 8r + 3$. Then

(4) {the relations in the upper half of the next page constitute equation (4)}

$$h(-8p) = \frac{1}{2} \sum_{m=1}^{4p} \left(\frac{-8p}{m} \right)$$

$$= \frac{1}{2} \left\{ \sum_{\substack{m=1 \\ m\equiv 1 \ (\mathrm{mod}\ 8)}}^{4p} - \sum_{\substack{m=1 \\ m\equiv 3 \ (\mathrm{mod}\ 8)}}^{4p} - \sum_{\substack{m=1 \\ m\equiv 5 \ (\mathrm{mod}\ 8)}}^{4p} + \sum_{\substack{m=1 \\ m\equiv 7 \ (\mathrm{mod}\ 8)}}^{4p} \right\} \left(\frac{m}{p} \right)$$

$$= \frac{1}{2} \left\{ \sum_{\substack{m=1 \\ m\equiv 1,6,3,0 (\mathrm{mod}\ 8)}}^{p} - \sum_{\substack{m=1 \\ m\equiv 3,0,5,2 (\mathrm{mod}\ 8)}}^{p} - \sum_{\substack{m=1 \\ m\equiv 5,2,7,4 (\mathrm{mod}\ 8)}}^{p} + \sum_{\substack{m=1 \\ m\equiv 7,4,1,6 (\mathrm{mod}\ 8)}}^{p} \right\} \left(\frac{m}{p} \right)$$

$$= \sum_{\substack{m=1 \\ m\equiv 1,6 \ (\mathrm{mod}\ 8)}}^{p} \left(\frac{m}{p} \right) - \sum_{\substack{m=1 \\ m\equiv 2,5 \ (\mathrm{mod}\ 8)}}^{p} \left(\frac{m}{p} \right)$$

$$= \sum_{\substack{m=1 \\ m\equiv 1,6 \ (\mathrm{mod}\ 8)}}^{p} \left(\frac{m}{p} \right) - \sum_{\substack{m=1 \\ m\equiv 1,6 \ (\mathrm{mod}\ 8)}}^{p} \left(\frac{p-m}{p} \right) = 2 \cdot \sum_{\substack{m=1 \\ m\equiv 1,6 \ (\mathrm{mod}\ 8)}}^{p} \left(\frac{m}{p} \right).$$

The last sum contains $2r + 1$ numbers, each odd. Therefore $h(-8p) \equiv 2 \ (\mathrm{mod}\ 4)$.

Now put $p = 24r + 19$. In particular, $p \equiv 3 \ (\mathrm{mod}\ 8)$ and $p \equiv 7 \ (\mathrm{mod}\ 12)$. Thus,

$$h(-12p) = \frac{1}{2} \sum_{m=1}^{6p} \left(\frac{-12p}{m} \right)$$

$$= \frac{1}{2} \left\{ \sum_{\substack{m=1 \\ m\equiv 1 \ (\mathrm{mod}\ 12)}}^{6p} - \sum_{\substack{m=1 \\ m\equiv 5 \ (\mathrm{mod}\ 12)}}^{6p} - \sum_{\substack{m=1 \\ m\equiv 7 \ (\mathrm{mod}\ 12)}}^{6p} + \sum_{\substack{m=1 \\ m\equiv 11 \ (\mathrm{mod}\ 12)}}^{6p} \right\} \left(\frac{m}{p} \right)$$

$$= \frac{1}{2} \left\{ \sum_{\substack{m=1 \\ m\equiv 1, 6, 11, 4, 9, 2 \ (\mathrm{mod}\ 12)}}^{p} - \sum_{\substack{m=1 \\ m\equiv 5, 10, 3, 8, 1, 6 \ (\mathrm{mod}\ 12)}}^{p} \right.$$

$$\left. - \sum_{\substack{m=1 \\ m\equiv 7, 0, 5, 10, 3, 8 \ (\mathrm{mod}\ 12)}}^{p} + \sum_{\substack{m=1 \\ m\equiv 11, 4, 9, 2, 7, 0 \ (\mathrm{mod}\ 12)}}^{p} \right\} \left(\frac{m}{p} \right)$$

$$= \left\{ \sum_{\substack{m=1 \\ m\equiv 2, 4, 9, 11 \ (\mathrm{mod}\ 12)}}^{p} - \sum_{\substack{m=1 \\ m\equiv 3, 5, 8, 10 \ (\mathrm{mod}\ 12)}}^{p} \right\} \left(\frac{m}{p} \right)$$

$$= \sum_{\substack{m=1 \\ m\equiv 2,\,4,\,9,\,11 \pmod{12}}}^{p} \left\{\left(\frac{m}{p}\right) - \left(\frac{p-m}{p}\right)\right\} = 2 \cdot \sum_{\substack{m=1 \\ m\equiv 2,\,4,\,9,\,11 \pmod{12}}}^{p} \left(\frac{m}{p}\right).$$

Now

$$\sum_{\substack{m=1 \\ m\equiv 4,9 \pmod{12}}}^{p} \left(\frac{m}{p}\right) = \sum_{\substack{m=1 \\ m\equiv 4 \pmod{12}}}^{p} \left(\frac{m}{p}\right) + \sum_{\substack{m=1 \\ m\equiv 9 \pmod{12}}}^{p} \left(\frac{m+p}{p}\right)$$

$$= \sum_{\substack{m=1 \\ m\equiv 4 \pmod{12}}}^{2p} \left(\frac{m}{p}\right) = \sum_{\substack{m=1 \\ m\equiv 2,8 \pmod{12}}}^{p} \left(\frac{2m}{p}\right) = - \sum_{\substack{m=1 \\ m\equiv 2,8 \pmod{12}}}^{p} \left(\frac{m}{p}\right)$$

$$= - \sum_{\substack{m=1 \\ m\equiv 2 \pmod{12}}}^{p} \left(\frac{m}{p}\right) - \sum_{\substack{m=1 \\ m\equiv 11 \pmod{12}}}^{p} \left(\frac{p-m}{p}\right)$$

$$= - \sum_{\substack{m=1 \\ m\equiv 2 \pmod{12}}}^{p} \left(\frac{m}{p}\right) + \sum_{\substack{m=1 \\ m\equiv 11 \pmod{12}}}^{p} \left(\frac{m}{p}\right).$$

Thus,

$$h(-12p) = 4 \cdot \sum_{\substack{m=1 \\ m\equiv 11 \pmod{12}}}^{p} \left(\frac{m}{p}\right). \tag{5}$$

There are $2r + 1$ terms in this sum, each odd. Therefore $h(-12p) \equiv 4 \pmod 8$.

LEMMA 4. *Put*

$$B_r = \frac{2\pi}{k\sqrt{p}}\, e^{-\frac{\pi r\sqrt{p}}{k}} \cdot e\left(\frac{r}{2k}\right) \sum_{y\,|\,r} \frac{1}{y} \sum_{j=0}^{k-1} \chi(Q(j,\, y))\, e\left(\frac{jr/y}{k}\right). \tag{6}$$

i) *When* $k = 12$ *and* $\frac{p+1}{4} \equiv 1 \pmod 4$, *then*

$$B_1 = -\frac{2\pi\sqrt{2}}{3\sqrt{p}}\, e^{-\frac{\pi\sqrt{p}}{12}}, \quad B_2 = 0, \quad B_3 = -\frac{4\pi\sqrt{2}}{9\sqrt{p}}\, e^{-\frac{\pi\sqrt{p}}{4}}.$$

When $k = 12$ *and* $\frac{p+1}{4} \equiv 3 \pmod 4$, *then*

$$B_1 = \frac{2\pi\sqrt{2}}{3\sqrt{p}}\, e^{-\frac{\pi\sqrt{p}}{12}}, \quad B_2 = 0, \quad B_3 = \frac{4\pi\sqrt{2}}{9\sqrt{p}}\, e^{-\frac{\pi\sqrt{p}}{4}}.$$

ii) *When* $k = 8$ *and* $\frac{p+1}{4} \equiv 1 \pmod 8$, $B_1 = \frac{\pi}{\sqrt{p}\sqrt{2+\sqrt{2}}} e^{-\frac{\pi\sqrt{p}}{8}}$, $B_2 = 0$.

When $k = 8$ *and* $\frac{p+1}{4} \equiv 5 \pmod 8$, $B_1 = -\frac{\pi}{\sqrt{p}\sqrt{2+\sqrt{2}}} e^{-\frac{\pi\sqrt{p}}{8}}$, $B_2 = 0$.

When $k = 8$ *and* $\frac{p+1}{4} \equiv 3 \pmod 8$, $B_1 = -\frac{\pi\sqrt{2}\sqrt{2+\sqrt{2}}}{2\sqrt{p}} e^{-\frac{\pi\sqrt{p}}{8}}$, $B_2 = 0$.

When $k = 8$ *and* $\frac{p+1}{4} \equiv 7 \pmod 8$, $B_1 = \frac{\pi\sqrt{2}\sqrt{2+\sqrt{2}}}{2\sqrt{p}} e^{-\frac{\pi\sqrt{p}}{8}}$, $B_2 = 0$.

Proof. We show first that $B_2 = 0$ for both $k = 8$ and $k = 12$. We recall that $\chi\left(n+\frac{k}{2}\right) = -\chi(n)$. Thus,

$$\chi\left(j^2+j+\frac{p+1}{4}\right) e\left(\frac{2j}{k}\right) + \chi\left(\left[j+\frac{k}{2}\right]^2 + \left[j+\frac{k}{2}\right] + \frac{p+1}{4}\right) e\left(\frac{2\left[j+\frac{k}{2}\right]}{k}\right) = 0.$$

Therefore

$$\sum_{j=0}^{k-1} \chi(Q(j, 1)) e\left(\frac{2j}{k}\right) = 0. \tag{7}$$

Likewise,

$$\chi(j^2+2j+p+1) e\left(\frac{j}{k}\right) + \chi\left(\left[j+\frac{k}{2}\right]^2 + 2\left[j+\frac{k}{2}\right] + p + 1\right) e\left(\frac{\left[j+\frac{k}{2}\right]}{k}\right) = 0,$$

and hence

$$\sum_{j=0}^{k-1} \chi(Q(j, 2)) e\left(\frac{j}{k}\right) = 0. \tag{8}$$

From (7) and (8) we see immediately that $B_2 = 0$.

We may cut the remainder of our job in half. Consider first the case $k = 12$. In this case, $\frac{p+1}{4} \equiv 1 \pmod 4$ implies $\frac{p+1}{4} \equiv 5 \pmod{12}$, and hence

$$Q(j, 1) \equiv j^2 + j + 5 \pmod{12}, \qquad Q(j, 3) \equiv j^2 + 3j + 9 \pmod{12}.$$

On the other hand, $\frac{p+1}{4} \equiv 3 \pmod 4$ implies $\frac{p+1}{4} \equiv 11 \pmod{12}$, and hence

$$Q(j, 1) \equiv j^2 + j + 11 \pmod{12}, \qquad Q(j, 3) \equiv j^2 + 3j + 3 \pmod{12}.$$

Consequently, as we go from $\frac{p+1}{4} \equiv 1 \pmod 4$ to $\frac{p+1}{4} \equiv 3 \pmod 4$, $\chi(Q(j, 1))$ merely changes sign for every value of j, and the same is true of $\chi(Q(j, 3))$. As a result, the same is true for B_1 and B_3. For $k = 8$, a similar situation arises as we go from

$$\frac{p+1}{4} \equiv 1 \pmod 8 \quad \text{and} \quad Q(j, 1) \equiv j^2 + j + 1 \pmod 8$$

to

$$\frac{p+1}{4} \equiv 5 \pmod 8 \quad \text{and} \quad Q(j, 1) \equiv j^2 + j + 5 \pmod 8 .$$

Here again, B_1 merely changes sign. This is again clearly the case when we go from

$$\frac{p+1}{4} \equiv 3 \pmod 8 \quad \text{and} \quad Q(j, 1) \equiv j^2 + j + 3 \pmod 8$$

to

$$\frac{p+1}{4} \equiv 7 \pmod 8 \quad \text{and} \quad Q(j, 1) \equiv j^2 + j + 7 \pmod 8 .$$

It remains to verify the values of B_1 and B_3 for $k = 12$, $\frac{p+1}{4} \equiv 1 \pmod 4$ and the values of B_1 for $k = 8$, $\frac{p+1}{4} \equiv 1, 3 \pmod 8$. Table 2 will aid the reader in checking the arithmetic. Simplified values of $e\left(\frac{1}{2k}\right)$ may also be useful:

$$e\left(\frac{1}{16}\right) = \frac{1}{2}\left(\sqrt{2+\sqrt{2}} + i\sqrt{2-\sqrt{2}}\right),$$

$$e\left(\frac{1}{24}\right) = \frac{1}{2\sqrt{2}}\left[(\sqrt{3}+1) + i(\sqrt{3}-1)\right].$$

LEMMA 5. *The only solutions in integers of* $8x^6 \pm 1 = y^2$ *are*

$$x = 0,\ y = \pm 1, \qquad |x| = 1,\ |y| = 3 .$$

The only solutions in integers of $x^6 \pm 1 = 2y^2$ *are* $|x| = 1$, $|y| = 0, 1$.

Proof. The first equation is classical. Euler [1, Vol. 2, pp. 533-534] solved the equation $x^3 \pm 1 = y^2$ and found that $x = -1, 0, 1, 2$ give the only solutions. I am unable to find a complete solution of the second equation in the literature; but Dickson [1, Vol. 2, p. 538] notes that L. Aubry and E. Fauquembergue proved that $x^3 + 1 = 2y^2$ has solutions only for $x = -1, 1, 23$. We therefore solve the second equation here. The same techniques work for the first equation with the plus sign; the first equation with the minus sign has no solutions (mod 4). We first treat the equation $x^6 = 1 + 2y^2$. Here

$$(x^2)^3 = (1 + y\sqrt{-2})(1 - y\sqrt{-2}). \tag{9}$$

The field $Q(\sqrt{-2})$ has unique factorization of integers. Further, the units of $Q(\sqrt{-2})$ are ± 1 and thus are cubes in $Q(\sqrt{-2})$. Finally, if $\pi \in Q(\sqrt{-2})$ is a prime and divides both factors, then π divides their sum and thus $\pi = \pm\sqrt{-2}$. But $\pm\sqrt{-2}$ does not divide

$$k = 12,\ \frac{p+1}{4} \equiv 1 \pmod 4$$

j	Q(j, 1) (mod 12)	χ(Q(j, 1))	Q(j, 3) (mod 12)	χ(Q(j, 3))
0	5	-1	9	0
1	7	-1	1	1
2	11	1	7	-1
3	5	-1	3	0
4	1	1	1	1
5	11	1	1	1
6	11	1	3	0
7	1	1	7	-1
8	5	-1	1	1
9	11	1	9	0
10	7	-1	7	-1
11	5	-1	7	-1

$Q(j, 1) \equiv j^2 + j + 5 \pmod{12}$, $\quad Q(j, 3) \equiv j^2 + 3j + 9 \pmod{12}$

$$k = 8,\ \frac{p+1}{4} \equiv 1 \pmod 8$$

j	Q(j, 1) (mod 8)	χ(Q(j, 1))
0	1	1
1	3	-1
2	7	1
3	5	-1
4	5	-1
5	7	1
6	3	-1
7	1	1

$Q(j, 1) \equiv j^2 + j + 1 \pmod 8$

$$k = 8,\ \frac{p+1}{4} \equiv 3 \pmod 8$$

j	Q(j, 1) (mod 8)	χ(Q(j, 1))
0	3	-1
1	5	-1
2	1	1
3	7	1
4	7	1
5	1	1
6	5	-1
7	3	-1

$Q(j, 1) \equiv j^2 + j + 3 \pmod 8$

TABLE 2

either factor. Thus there are rational integers a and b such that

$$1 + y\sqrt{-2} = (a + b\sqrt{-2})^3 .$$

Therefore

$$1 = a(a^2 - 6b^2), \qquad y = b(3a^2 - 2b^2).$$

Consequently, $a = 1$, $b = 0$, $y = 0$, $x = \pm 1$.

Now consider the equation $x^6 + 1 = 2y^2$. Here

$$(x^2 + 1)(x^4 - x^2 + 1) = 2y^2. \tag{10}$$

We note that the first factor must be even and the second odd. Also, since

$$x^4 - x^2 + 1 = (x^2 + 1)^2 - 3(x^2 + 1) + 3\,,$$

$x^2 + 1$ and $x^4 - x^2 + 1$ can have no common factor other than 3; but this can not occur, since 3 never divides $x^2 + 1$. Finally, $x^4 - x^2 + 1$ is positive, and thus it follows that there exists an integer z such that

$$x^4 - x^2 + 1 = z^2\,. \tag{11}$$

We note that for $x^2 > 1$,

$$(x^2 - 1)^2 < x^4 - x^2 + 1 < (x^2)^2\,.$$

Hence, the only solutions to (11) are $x = 0, \pm 1$. Of these, only $x = \pm 1$ gives solutions to $x^6 + 1 = 2y^2$.

3. DERIVATION OF DIOPHANTINE EQUATIONS FOR SUFFICIENTLY LARGE p

For $s > 1$,

$$\begin{aligned} L_k(s)\,L_{-kp}(s) &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\left(\frac{k}{n}\right)\left(\frac{-kp}{m}\right) n^{-s}\, m^{-s} \\ &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\left(\frac{k}{mn}\right)\left(\frac{-p}{m}\right)(mn)^{-s} = \sum_{d=1}^{\infty}\left(\frac{k}{d}\right) d^{-s} \sum_{m\mid d}\left(\frac{-p}{m}\right). \end{aligned} \tag{12}$$

Let $e_{d,Q}$ denote the number of representations of d by the form Q. Heilbronn [4, p. 156] showed that if $h(-p) = 1$, then

$$\sum_{m\mid d}\left(\frac{-p}{m}\right) = \frac{1}{2}\, e_{d,Q}\,. \tag{13}$$

Landau [6, Satz 204] proves (13) under the additional hypothesis that $(d, p) = 1$. It should be noted that (13) contains the assumption that $h(-p) = 1$, since ordinarily the right-hand side of (13) would be summed over all forms belonging to a complete representative system of forms of discriminant $-p$. In fact, this is the last point where we need to use the assumption that $h(-p) = 1$.

From (12) and (13), we get (at $z = 1/2$) the relation

$$\begin{aligned} L_k(s)\,L_{-kp}(s) &= \frac{1}{2}\sum_{x,y}{}' \frac{\chi(Q(x, y))}{Q(x, y)^s} \\ &= \frac{1}{2}\sum_{x\neq 0}\frac{\chi(x^2)}{(x^2)^s} + \frac{1}{2}\sum_{y\neq 0}\sum_{x}\frac{\chi(Q(x, y))}{Q(x, y)^s} \\ &= \zeta(2s) \prod_{\substack{q\mid k \\ q \text{ prime}}} (1 - q^{-2s}) + \sum_{y=1}^{\infty}\sum_{x}\frac{\chi(Q(x, y))}{\left[(x + zy)^2 + \frac{p}{4}\, y^2\right]^s}\,. \end{aligned} \tag{14}$$

The symbol $\sum'$ in the first line means that $(x, y) = (0, 0)$ is to be excluded from the summation. For fixed $s > 1$, the last function is continuously differentiable in z and periodic in z with period k, and we therefore expand it in a Fourier series. For $s > 1$ and $z = 1/2$,

$$L_k(s)L_{-kp}(s) - \zeta(2s) \prod_{\substack{q \mid k \\ q \text{ prime}}} (1 - q^{-2s}) = \sum_{r=-\infty}^{\infty} A_r(s) e\left(\frac{rz}{k}\right) \tag{15}$$

$$= A_0(s) + 2\Re \sum_{r=1}^{\infty} A_r(s) e\left(\frac{r}{2k}\right),$$

where

$$A_r(s) = \frac{1}{k}\int_0^k \sum_{y=1}^{\infty} \sum_{x} \frac{\chi(Q(x, y))}{\left[(x + zy)^2 + \frac{p}{4}y^2\right]^s} e\left(\frac{-rz}{k}\right) dz \tag{16}$$

$$= \frac{1}{k} \sum_{y=1}^{\infty} \sum_{x} \chi(Q(x, y)) \int_0^k \frac{e\left(-\frac{rz}{k}\right)}{\left[(x + zy)^2 + \frac{p}{4}y^2\right]^s} dz .$$

The interchange of the integral and summation signs is justified by the absolute and uniform convergence in z of the double series. We change variables in (16) by putting $x + zy = \frac{y\sqrt{p}}{2} u$; this gives the equation

$$A_r(s) = \frac{1}{k}\left(\frac{\sqrt{p}}{2}\right)^{1-2s} \sum_{y=1}^{\infty} y^{-2s} \sum_{x} \chi(Q(x, y)) e\left(\frac{rx}{ky}\right) \int_{\frac{2x}{y\sqrt{p}}}^{\frac{2(x+ky)}{y\sqrt{p}}} \frac{e\left(-\frac{r\sqrt{p}u}{2k}\right)}{(u^2 + 1)^s} du .$$

Now replace x by $m + kyn$ $(0 \leq m \leq ky - 1)$; then

$$A_r(s) = \frac{1}{k}\left(\frac{\sqrt{p}}{2}\right)^{1-2s} \sum_{y=1}^{\infty} y^{-2s} \sum_{m=0}^{ky-1} \chi(Q(m, y)) e\left(\frac{rm}{ky}\right) \sum_{n} \int_{\frac{2(m+kyn)}{y\sqrt{p}}}^{\frac{2[m+ky(n+1)]}{y\sqrt{p}}} \frac{e\left(-\frac{r\sqrt{p}u}{2k}\right)}{(u^2 + 1)^s} du \tag{17}$$

$$= \frac{1}{k}\left(\frac{\sqrt{p}}{2}\right)^{1-2s} \int_{-\infty}^{\infty} \frac{e\left(-\frac{r\sqrt{p}u}{2k}\right)}{(u^2 + 1)^s} du \sum_{y=1}^{\infty} y^{-2s} \sum_{m=0}^{ky-1} \chi(Q(m, y)) e\left(\frac{rm}{ky}\right) .$$

If we put $m = g + kj$ $(0 \leq g \leq k - 1)$, then we see that

$$\sum_{m=0}^{ky-1} \chi(Q(m, y)) e\left(\frac{rm}{ky}\right) = \sum_{g=0}^{k-1} \chi(Q(g, y)) e\left(\frac{rg}{ky}\right) \sum_{j=0}^{y-1} e\left(\frac{rj}{y}\right)$$

$$(18)\qquad = \begin{cases} y \sum\limits_{g=0}^{k-1} \chi(Q(g, y))\, e\left(\frac{gr/y}{k}\right) & \text{if } y \mid r, \\ 0 & \text{if } y \nmid r. \end{cases}$$

It follows from (17) and (18) that

$$(19)\qquad A_r(s) = \frac{1}{k}\left(\frac{\sqrt{p}}{2}\right)^{1-2s} \int_{-\infty}^{\infty} \frac{e\left(-\frac{r\sqrt{p}\,u}{2k}\right)}{(u^2+1)^s}\, du \sum_{\substack{y \mid r \\ y>0}} y^{1-2s} \sum_{g=0}^{k-1} \chi(Q(g, y))\, e\left(\frac{gr/y}{k}\right).$$

When $r > 0$, this last formula has meaning even for $s = 1$. For $r > 0$, we write

$$(20)\qquad A_r = A_r(1).$$

By elementary residue theory,

$$\int_{-\infty}^{\infty} \frac{e\left(-\frac{r\sqrt{p}\,u}{2k}\right)}{u^2+1}\, du = -2\pi i \lim_{u \to -i} \frac{e\left(-\frac{r\sqrt{p}\,u}{2k}\right)}{u - i} = \pi e^{-\frac{\pi r\sqrt{p}}{k}} \qquad (r > 0).$$

Thus, for $r > 0$,

$$(21)\qquad A_r = \frac{2\pi}{k\sqrt{p}}\, e^{-\frac{\pi r\sqrt{p}}{k}} \sum_{\substack{y \mid r \\ y>0}} \frac{1}{y} \sum_{j=0}^{k-1} \chi(Q(j, y))\, e\left(\frac{jr/y}{k}\right).$$

By (19) and Lemma 1, when $s > 1$,

$$A_0(s) = \frac{1}{k}\left(\frac{\sqrt{p}}{2}\right)^{1-2s} \int_{-\infty}^{\infty} \frac{du}{(u^2+1)^s} \begin{cases} 4^{2-2s}\zeta(2s-1)(-1+2^{2-2s}) & (k = 8), \\ 2^{2-2s}\zeta(2s-1)(-1+2^{2-2s})(-1+3^{2-2s}) & (k = 12). \end{cases}$$

Thus we may define

$$(22)\qquad A_0 = \lim_{s \to 1^+} A_0(s) = \frac{2\pi}{k\sqrt{p}} \cdot \begin{cases} -\log 2 & (k = 8), \\ 0 & (k = 12). \end{cases}$$

From (19) and Lemma 2, we see that $\sum_{r=1}^{\infty} A_r(s)\, e\left(\frac{r}{2k}\right)$ converges uniformly for $1 \leq s \leq 2$ and hence is continuous from the right at $s = 1$. Thus, combining (15) and (22), we see that

$$(23)\qquad L_8(1)L_{-8p}(1) = \frac{\pi^2}{8} - \frac{\pi \log 2}{4\sqrt{p}} + 2\Re \sum_{r=1}^{\infty} A_r e\left(\frac{r}{16}\right),$$

$$L_{12}(1)L_{-12p}(1) = \frac{\pi^2}{9} + 2\,\Re \sum_{r=1}^{\infty} A_r e\left(\frac{r}{24}\right) . \tag{24}$$

We shall evaluate the left-hand sides of (23) and (24) by Dirichlet's formula ([6, Satz 209]; here Landau is speaking of class-numbers for quadratic forms and units of norm +1; he makes the connection with class-numbers for quadratic fields and fundamental units in Teil XI, Kap. 3). Dirichlet found that

$$L_8(1) = \frac{\log(1+\sqrt{2})}{\sqrt{2}}, \qquad L_{12}(1) = \frac{\log(2+\sqrt{3})}{\sqrt{3}}, \qquad L_{-kp}(1) = \frac{\pi h(-kp)}{\sqrt{kp}} .$$

We therefore see from (23) and (24) that

$$\frac{h(-8p)\log(1+\sqrt{2})}{4} + \frac{1}{4}\log 2 = \frac{\pi\sqrt{p}}{8} + \frac{2\sqrt{p}}{\pi}\,\Re\left\{\sum_{r=1}^{\infty} A_r e\left(\frac{r}{16}\right)\right\} \qquad (k = 8), \tag{25}$$

$$\frac{h(-12p)\log(2+\sqrt{3})}{8} = \frac{\pi\sqrt{p}}{12} + \frac{3\sqrt{p}}{2\pi}\,\Re\left\{\sum_{r=1}^{\infty} A_r e\left(\frac{r}{24}\right)\right\} \qquad (k = 12). \tag{26}$$

It will be necessary to consider equation (26) in the cases $\frac{p+1}{4} \equiv 1, 3 \pmod 4$, and equation (25) in the cases

$$\frac{p+1}{4} \equiv 1, 5 \pmod 8 \qquad \text{and} \qquad \frac{p+1}{4} \equiv 3, 7 \pmod 8 .$$

For each of these three pairs, it will turn out that the values of A_r differ in sign only, for the two cases in the pair. In this section, we shall consider in detail only the first case from each grouping, and we shall state the result for the second case. In Section 4, when we consider the error terms, we shall consider the second case from each grouping. Thus the reader will ultimately see each of the Diophantine equations (51) to (54) completely derived; but at first he will not need to worry about the error terms.

Put

$$q = e^{\pi\sqrt{p}} , \tag{27}$$

and

$$r_1 = 2 + \sqrt{3}, \qquad r_2 = 2 - \sqrt{3} . \tag{28}$$

Further, let

$$w_n = \frac{1+\sqrt{3}}{2} r_1^n + \frac{1-\sqrt{3}}{2} r_2^n, \tag{29}$$

so that w_n is an integer and satisfies the recursion relation

$$x_{n+2} = 4x_{n+1} - x_n . \tag{30}$$

We now assume that $k = 12$ and $\frac{p+1}{4} \equiv 1 \pmod 4$. By (26), (21), and Lemmas 3 and 4,

$$\left(M + \frac{1}{2}\right) \log r_1 = \frac{\pi\sqrt{p}}{12} - \sqrt{2}q^{-1/12} - \frac{2\sqrt{2}}{3} q^{-1/4} + O(q^{-1/3}). \tag{31}$$

Thus,

$$\begin{aligned} r_1^M \frac{1+\sqrt{3}}{2} &= r_1^M \sqrt{\frac{2+\sqrt{3}}{2}} = \frac{1}{\sqrt{2}} r_1^{M+\frac{1}{2}} \\ &= \frac{1}{\sqrt{2}} q^{1/12}[1 - \sqrt{2}q^{-1/12} + q^{-1/6} - \sqrt{2}q^{-1/4} + O(q^{-1/3})]. \end{aligned} \tag{32}$$

As a result,

$$r_2^M(\sqrt{3} - 1) = \left(r_1^M \frac{1+\sqrt{3}}{2}\right)^{-1} = \sqrt{2}q^{-1/12}[1 + \sqrt{2}q^{-1/12} + O(q^{-1/6})],$$

and therefore

$$r_2^M \frac{1-\sqrt{3}}{2} = -\frac{1}{\sqrt{2}} q^{-1/12}[1 + \sqrt{2}q^{-1/12} + O(q^{-1/6})]. \tag{33}$$

In view of (29), we are led to combine (32) and (33); in the case of $\frac{p+1}{4} \equiv 1 \pmod 4$, we therefore define the integer

$$\begin{aligned} a = w_M + 1 &= r_1^M \frac{1+\sqrt{3}}{2} + r_2^M \frac{1-\sqrt{3}}{2} + 1 \\ &= \frac{1}{\sqrt{2}} q^{1/12}[1 - 2\sqrt{2}q^{-1/4} + O(q^{-1/3})]. \end{aligned} \tag{34}$$

In particular,

$$a^3 = \frac{1}{2\sqrt{2}} q^{1/4}[1 - 6\sqrt{2}q^{-1/4} + O(q^{-1/3})],$$

and hence

$$a^3 + 3 = \frac{1}{2\sqrt{2}} q^{1/4} + O(q^{-1/12}). \tag{35}$$

In the case that $\frac{p+1}{4} \equiv 3 \pmod 4$, we get (31) with two sign changes,

$$\left(M + \frac{1}{2}\right) \log r_1 = \frac{\pi\sqrt{p}}{12} + \sqrt{2}q^{-1/12} + \frac{2\sqrt{2}}{3} q^{-1/4} + O(q^{-1/3}).$$

We then define the integer a in the case of $\frac{p+1}{4} \equiv 3 \pmod 4$ as

$$a = w_M - 1 = \frac{1}{\sqrt{2}} q^{1/12}[1 + 2\sqrt{2}q^{-1/4} + O(q^{-1/3})]. \tag{36}$$

We then see that

$$a^3 - 3 = \frac{1}{2\sqrt{2}} q^{1/4} + O(q^{-1/12}). \tag{37}$$

Put

$$R_1 = 1 + \sqrt{2}, \qquad R_2 = 1 - \sqrt{2}, \tag{38}$$

and let

$$y_n = \frac{1}{2\sqrt{2}} (R_1^n - R_2^n), \qquad z_n = \frac{1}{2} (R_1^n + R_2^n). \tag{39}$$

We see that y_n and z_n are integers and satisfy the recursion relation

$$x_{n+2} = 2x_{n+1} + x_n. \tag{40}$$

We now assume that $k = 8$ and $\frac{p+1}{4} \equiv 1 \pmod 8$. By (25), (21), and Lemmas 3 and 4,

$$\left(N + \frac{1}{2}\right) \log R_1 + \frac{1}{4} \log 2 = \frac{\pi\sqrt{p}}{8} + \frac{2}{\sqrt{R_1\sqrt{2}}} q^{-1/8} + O(q^{-3/8}). \tag{41}$$

Therefore,

$$\sqrt{R_1\sqrt{2}}\, R_1^N = q^{1/8}\left[1 + \frac{2}{\sqrt{R_1\sqrt{2}}} q^{-1/8} + O(q^{-1/4}) \right]. \tag{42}$$

Together, equations (41) and (42) imply that

$$\begin{aligned} \sqrt{2} R_1^{2N+1} &= q^{1/4}\left[1 + \frac{4}{\sqrt{R_1\sqrt{2}}} q^{-1/8} + \frac{8}{R_1\sqrt{2}} q^{-1/4} + O(q^{-3/8}) \right] \\ &= q^{1/4} + 4R_1^N + O(q^{-1/8}). \end{aligned} \tag{43}$$

Thus

$$\frac{1}{2} R_1^{2N+1} - \sqrt{2} R_1^N = \frac{1}{2\sqrt{2}} q^{1/4} + O(q^{-1/8}),$$

and since $R_2^N = O(q^{-1/8})$ by (42), we see from definition (39) that

$$z_{2N+1} - 4y_N = \frac{1}{2\sqrt{2}} q^{1/4} + O(q^{-1/8}) \qquad \left[\frac{p+1}{4} \equiv 1 \pmod 8 \right]. \tag{44}$$

In the case $\frac{p+1}{4} \equiv 5 \pmod 8$, we get equation (41) with a sign change:

$$\left(N + \frac{1}{2}\right) \log R_1 + \frac{1}{4} \log 2 = \frac{\pi\sqrt{p}}{8} - \frac{2}{\sqrt{R_1\sqrt{2}}} q^{-1/8} + O(q^{-3/8}),$$

and we are then led to the analogue of (44):

$$z_{2N+1} + 4y_N = \frac{1}{2\sqrt{2}} q^{1/4} + O(q^{-1/8}) \qquad \left[\frac{p+1}{4} \equiv 5 \pmod 8 \right]. \tag{45}$$

Now we consider the case $\frac{p+1}{4} \equiv 3 \pmod 8$. By (25), (21), and Lemmas 3 and 4,

$$\left(N+\frac{1}{2}\right)\log R_1+\frac{1}{4}\log 2 = \frac{\pi\sqrt{p}}{8} - \sqrt{2R_1\sqrt{2}}\,q^{-1/8}+O(q^{-3/8}). \tag{46}$$

Therefore

$$\sqrt{R_1\sqrt{2}}\,R_1^N = q^{1/8}[1-\sqrt{2R_1\sqrt{2}}\,q^{-1/8}+O(q^{-1/4})]. \tag{47}$$

Combining equations (46) and (47), we find that

$$\begin{aligned}\sqrt{2}R_1^{2N+1} &= q^{1/4}[1-2\sqrt{2R_1\sqrt{2}}\,q^{-1/8}+4R_1\sqrt{2}q^{-1/4}+O(q^{-3/8})]\\ &= q^{1/4}-4R_1^{N+1}+O(q^{-1/8}).\end{aligned} \tag{48}$$

Thus

$$\frac{1}{2}R_1^{2N+1}+\sqrt{2}R_1^{N+1} = \frac{1}{2\sqrt{2}}q^{1/4}+O(q^{-1/8}),$$

and as a result,

$$z_{2N+1}+4y_{N+1} = \frac{1}{2\sqrt{2}}q^{1/4}+O(q^{-1/8}) \qquad \left[\frac{p+1}{4}\equiv 3 \pmod 8\right]. \tag{49}$$

In the case $\frac{p+1}{4} \equiv 7 \pmod 8$, we get (46) with a sign change:

$$\left(N+\frac{1}{2}\right)\log R_1+\frac{1}{4}\log 2 = \frac{\pi\sqrt{p}}{8}+\sqrt{2R_1\sqrt{2}}\,q^{-1/8}+O(q^{-3/8}),$$

and we are then led to the analogue of (49):

$$z_{2N+1}-4y_{N+1} = \frac{1}{2\sqrt{2}}q^{1/4}+O(q^{-1/8}) \qquad \left[\frac{p+1}{4}\equiv 7 \pmod 8\right]. \tag{50}$$

Combining equations (35), (37), (44), (45), (49), and (50), we see that if p is sufficiently large, then one of the following equations is satisfied:

$$z_{2N+1}-4y_N = a^3+3 \qquad \left[\frac{p+1}{4}\equiv 1 \pmod 8\right], \tag{51}$$

$$z_{2N+1}+4y_N = a^3+3 \qquad \left[\frac{p+1}{4}\equiv 5 \pmod 8\right], \tag{52}$$

$$z_{2N+1}+4y_{N+1} = a^3-3 \qquad \left[\frac{p+1}{4}\equiv 3 \pmod 8\right], \tag{53}$$

$$z_{2N+1}-4y_{N+1} = a^3-3 \qquad \left[\frac{p+1}{4}\equiv 7 \pmod 8\right]. \tag{54}$$

In (51) and (52), a is defined by (34); in (53) and (54), a is defined by (36).

Equations (51) to (54) have been derived under the assumptions that $h(-p) = 1$, $p \equiv 19 \pmod{24}$, and p is sufficiently large. Except for this last condition, the values p = 19, 43, 67, and 163 satisfy these assumptions. For each of these values of p, the corresponding equation is actually satisfied; for example, when p = 163, both sides of (51) are equal to 8,003. We present the pertinent numbers:

For $p = 19$,	$h(-12p) = 4$,	$h(-8p) = 6$,	$M = 0$,	$N = 1$,	$a = 2$,	$z_3 = 7$,	$y_1 = 1$.
For $p = 43$,	$h(-12p) = 12$,	$h(-8p) = 10$,	$M = 1$,	$N = 2$,	$a = 4$,	$z_5 = 41$,	$y_3 = 5$.
For $p = 67$,	$h(-12p) = 12$,	$h(-8p) = 14$,	$M = 1$,	$N = 3$,	$a = 6$,	$z_7 = 239$,	$y_3 = 5$.
For $p = 163$,	$h(-12p) = 20$,	$h(-8p) = 22$,	$M = 2$,	$N = 5$,	$a = 20$,	$z_{11} = 8119$,	$y_5 = 29$.

4. PROOF THAT $p \geq 200$ IS SUFFICIENTLY LARGE

The results of this section are that if $p \geq 200$, then equations (51) to (54) are valid and $a > 20$. This estimate on a will be crucial, since we show, in Section 5, that there exist no solutions to equations (51) to (54) with $a > 20$. We shall assume throughout this section that $p \geq 200$. With the exceptions of the estimates (56) and (57) on $q^{-1/k}$, all of the estimates in the section will be sufficiently relaxed so that the reader can verify them without recourse to tables or calculating devices. We shall use the following four relations: for $|x| < 1$,

$$\sum_{n=r}^{\infty} nx^n = \frac{x^r}{(1-x)^2}[r - (r-1)x]; \tag{55}$$

for $p \geq 200$,

$$q^{-1/12} \leq e^{-\pi\sqrt{200}/12} < e^{-3.7} < \frac{1}{40}, \tag{56}$$

and

$$q^{-1/8} \leq e^{-\pi\sqrt{200}/8} < e^{-5.5} < \frac{1}{240}; \tag{57}$$

for $r > 0$, it follows from (21) that

$$|A_r| \leq \frac{2\pi r}{\sqrt{p}} e^{-\frac{\pi r\sqrt{p}}{k}} . \tag{58}$$

We let θ denote a number (not necessarily the same each time it occurs) such that $|\theta| \leq 1$.

Assume that $k = 12$ and $\frac{p+1}{4} \equiv 3 \pmod 4$. By (58), (26), (21), Lemmas 3 and 4, and then (55) and (56),

$$\begin{aligned}\left(M + \frac{1}{2}\right) \log r_1 &= \frac{\pi\sqrt{p}}{12} + \sqrt{2}q^{-1/12} + \frac{2\sqrt{2}}{3}q^{-1/4} + 3\theta \sum_{r=4}^{\infty} r(q^{-1/12})^r \\ &= \frac{\pi\sqrt{p}}{12} + \sqrt{2}q^{-1/12} + \frac{2\sqrt{2}}{3}q^{-1/4} + 15\,\theta\, q^{-1/3} .\end{aligned} \tag{59}$$

Note that

$$\sqrt{2}\,q^{-1/12} + \frac{2\sqrt{2}}{3}q^{-1/4} + 15\,\theta\,q^{-1/3} = \sqrt{2}\,q^{-1/12}(1 + \theta\,q^{-1/6})$$

and therefore

$$\left|\sqrt{2}\,q^{-1/12} + \frac{2\sqrt{2}}{3}q^{-1/4} + 15\,\theta\,q^{-1/3}\right| < 2q^{-1/12}\,.$$

These relations imply that

$$\begin{aligned}
r_1^M\frac{1+\sqrt{3}}{2} &= r_1^M\sqrt{\frac{2+\sqrt{3}}{2}} = \frac{1}{\sqrt{2}}\,r_1^{M+\frac{1}{2}} \\
&= \frac{1}{\sqrt{2}}q^{1/12}\Bigg\{1 + \left(\sqrt{2}\,q^{-1/12} + \frac{2\sqrt{2}}{3}q^{-1/4} + 15\,\theta\,q^{-1/3}\right) + q^{-1/6}(1+\theta\,q^{-1/6})^2 \\
&\qquad + \frac{\sqrt{2}}{3}q^{-1/4}(1+\theta\,q^{-1/6})^3 + \theta\sum_{n=4}^{\infty}\frac{(2q^{-1/12})^n}{n!}\Bigg\} \qquad (60) \\
&= \frac{1}{\sqrt{2}}q^{1/12}\left\{1 + \sqrt{2}\,q^{-1/12} + q^{-1/6} + \sqrt{2}\,q^{-1/4} + 18\,\theta\,q^{-1/3} + \frac{\theta}{24}\,\frac{(2q^{-1/12})^4}{1-2q^{-1/12}}\right\} \\
&= \frac{1}{\sqrt{2}}q^{1/12}\left\{1 + \sqrt{2}\,q^{-1/12} + q^{-1/6} + \sqrt{2}\,q^{-1/4} + 19\,\theta\,q^{-1/3}\right\}.
\end{aligned}$$

Since

$$\left|q^{-1/6} + \sqrt{2}\,q^{-1/4} + 19\,\theta\,q^{-1/3}\right| < 2q^{-1/6}$$

and

$$\left|\sqrt{2}\,q^{-1/12} + q^{-1/6} + \sqrt{2}\,q^{-1/4} + 19\theta q^{-1/3}\right| < 2q^{-1/12}\,,$$

it follows from (60) that

$$\begin{aligned}
r_2^M(\sqrt{3}-1) &= \left(r_1^M\frac{1+\sqrt{3}}{2}\right)^{-1} \\
&= \sqrt{2}\,q^{-1/12}\left\{1 - \sqrt{2}\,q^{-1/12} + 2\,\theta\,q^{-1/6} + \theta\sum_{n=2}^{\infty}(2q^{-1/12})^n\right\} \\
&= \sqrt{2}\,q^{-1/12}\left\{1 - \sqrt{2}\,q^{-1/12} + 7\,\theta\,q^{-1/6}\right\};
\end{aligned}$$

in other words,

$$r_2^M\frac{1-\sqrt{3}}{2} = -\frac{1}{\sqrt{2}}q^{-1/12}\left\{1 - \sqrt{2}\,q^{-1/12} + 7\,\theta\,q^{-1/6}\right\}. \tag{61}$$

If we combine (60) and (61) and apply the definition of a in (36), along with (29), we find that

$$a = w_M - 1 = r_1^M\frac{1+\sqrt{3}}{2} + r_2^M\frac{1-\sqrt{3}}{2} - 1 = \frac{1}{\sqrt{2}}q^{1/12}\left\{1 + 2\sqrt{2}\,q^{-1/4} + 26\,\theta\,q^{-1/3}\right\}. \tag{62}$$

Using the inequality

$$|2\sqrt{2}q^{-1/4} + 26\,\theta\, q^{-1/3}| < 4q^{-1/4},$$

we see from (62) that

$$a^3 = \frac{1}{2\sqrt{2}} q^{1/4}\{1 + 6\sqrt{2}q^{-1/4} + 78\,\theta\, q^{-1/3} + 3\,\theta\,(4q^{-1/4})^2 + \theta\,(4q^{-1/4})^3\}$$

$$= \frac{1}{2\sqrt{2}} q^{1/4}\{1 + 6\sqrt{2}q^{-1/4} + 79\,\theta\, q^{-1/3}\},$$

and thus

$$a^3 - 3 = \frac{1}{2\sqrt{2}} q^{1/4}(1 + 79\,\theta\, q^{-1/3}).$$

Since $\frac{1}{2\sqrt{2}} \cdot 79 = \frac{2\sqrt{2}}{8} \cdot 79 < \frac{3}{8} \cdot 80 = 30,.$

$$|a^3 - 3 - \frac{1}{2\sqrt{2}} q^{1/4}| < 30q^{-1/12} < \frac{3}{4}, \tag{63}$$

which incidentally verifies (37).

In the case $\frac{p+1}{4} \equiv 1 \pmod 4$, there are occasional changes of sign in the main terms; but the error terms (those containing the factor θ) are identical with the above. Thus we have a more exact statement of (34) and (35):

$$a = \frac{1}{\sqrt{2}} q^{1/12}\{1 - 2\sqrt{2}q^{-1/4} + 26\,\theta\, q^{-1/3}\}, \tag{64}$$

$$|a^3 + 3 - \frac{1}{2\sqrt{2}} q^{1/4}| < 30q^{-1/12} < \frac{3}{4}. \tag{65}$$

Since $1 \pm 2\sqrt{2}q^{-1/4} + 26\,\theta\, q^{-1/3} > \frac{1}{\sqrt{2}}$, we see from (62) and (64) that in all cases

$$a > \frac{1}{2} q^{1/12} > 20 \qquad (p \geq 200). \tag{66}$$

Assume that k = 8 and $\frac{p+1}{4} \equiv 5 \pmod 8$. By (58), (25), (21), Lemmas 3 and 4, and then (55) and (57),

$$\begin{aligned}\left(N + \tfrac{1}{2}\right) \log R_1 + \tfrac{1}{4} \log 2 &= \frac{\pi\sqrt{p}}{8} - \frac{2}{\sqrt{R_1\sqrt{2}}} q^{-1/8} + 4\,\theta \sum_{r=3}^{\infty} r(q^{-1/8})^r \\ &= \frac{\pi\sqrt{p}}{8} - \frac{2}{\sqrt{R_1\sqrt{2}}} q^{-1/8} + 13\,\theta\, q^{-3/8}.\end{aligned} \tag{67}$$

Since $\sqrt{R_1\sqrt{2}} = \sqrt{2 + \sqrt{2}}$, we see that

$$\sqrt{2} < \sqrt{R_1\sqrt{2}} < 2, \qquad \text{that is,} \qquad 1 < \frac{2}{\sqrt{R_1\sqrt{2}}} < \sqrt{2}, \tag{68}$$

and thus

$$-\frac{2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}+13\,\theta\,q^{-3/8} = -\frac{2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}\,(1+13\,\theta\,q^{-1/4}),$$

$$\left|-\frac{2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}+13\,\theta\,q^{-3/8}\right| < 2q^{-1/8}.$$

It follows from (67) and (68) that

$$\begin{aligned}\sqrt{R_1\sqrt{2}}\,R_1^N &= q^{1/8}\left\{1+\left(\frac{-2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}+13\,\theta\,q^{-3/8}\right)+\frac{2}{R_1\sqrt{2}}\,q^{-1/4}\right.\\ &\qquad\left.\cdot\,(1+13\,\theta\,q^{-1/4})^2+\theta\sum_{n=3}^{\infty}\frac{(2q^{-1/8})^n}{n!}\right\}\\ &= q^{1/8}\left\{1-\frac{2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}+\frac{2}{R_1\sqrt{2}}\,q^{-1/4}+14\,\theta\,q^{-3/8}+\frac{\theta}{6}\,\frac{(2q^{-1/8})^3}{1-(2q^{-1/8})}\right\}\\ &= q^{1/8}\left\{1-\frac{2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}+\frac{2}{R_1\sqrt{2}}\,q^{-1/4}+16\,\theta\,q^{-3/8}\right\}.\end{aligned}\tag{69}$$

Since

$$-\frac{2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}+\frac{2}{R_1\sqrt{2}}\,q^{-1/4}+16\,\theta\,q^{-3/8} = -\frac{2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}(1+\theta\,q^{-1/8}),$$

we see, after squaring (69) and then using (69) again, that

$$\begin{aligned}\sqrt{2}R_1^{2N+1} &= q^{1/4}\left\{1-\frac{4}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}+\frac{4}{R_1\sqrt{2}}\,q^{-1/4}+32\,\theta\,q^{-3/8}\right.\\ &\qquad\left.+\frac{4}{R_1\sqrt{2}}\,q^{-1/4}(1+\theta\,q^{-1/8})^2\right\}\\ &= q^{1/4}\left\{1-\frac{4}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}+\frac{8}{R_1\sqrt{2}}\,q^{-1/4}+37\,\theta\,q^{-3/8}\right\}\\ &= q^{1/4}(1+37\,\theta\,q^{-3/8})-\frac{4}{\sqrt{R_1\sqrt{2}}}\,q^{1/8}\left(1-\frac{2}{\sqrt{R_1\sqrt{2}}}\,q^{-1/8}\right)\\ &= q^{1/4}(1+37\,\theta\,q^{-3/8})-\frac{4}{\sqrt{R_1\sqrt{2}}}\left(\sqrt{R_1\sqrt{2}}R_1^N+2\,\theta\,q^{-1/8}\right)\\ &= q^{1/4}-4R_1^N+45\,\theta\,q^{-1/8}.\end{aligned}\tag{70}$$

As a result,

$$\frac{1}{2}\,R_1^{2N+1}+\sqrt{2}R_1^N = \frac{1}{2\sqrt{2}}\,q^{1/4}+23\,\theta\,q^{-1/8}.\tag{71}$$

By (68), (69), and (70),

$$|\sqrt{2}R_2^N| = \sqrt{2}\,\frac{\sqrt{R_1\sqrt{2}}}{\sqrt{R_1\sqrt{2}R_1^N}} < \sqrt{2}\cdot 2\cdot 2q^{-1/8} < 6q^{-1/8}$$

and

$$\left|\frac{1}{2}R_2^{2N+1}\right| = \frac{1}{\sqrt{2}}\,\frac{1}{\sqrt{2}R_1^{2N+1}} < 2q^{-1/4}.$$

Combining these inequalities with (71) and using (39), we see that

$$z_{2N+1} + 4y_N = \frac{1}{2\sqrt{2}}\,q^{1/4} + 30\,\theta\,q^{-1/8},$$

that is,

$$\left|z_{2N+1} + 4y_N - \frac{1}{2\sqrt{2}}\,q^{1/4}\right| \le 30q^{-1/8} < \frac{1}{4}\,. \tag{72}$$

This also verifies (45).

In the case $\frac{p+1}{4} \equiv 1 \pmod 8$, there are occasional changes in sign of the main terms from the case $\frac{p+1}{4} \equiv 5 \pmod 8$; but the error terms are identical. Thus we get an improvement of (44):

$$\left|z_{2N+1} - 4y_N - \frac{1}{2\sqrt{2}}\,q^{1/4}\right| \le 30q^{-1/8} < \frac{1}{4}\,. \tag{73}$$

Assume that $k = 8$ and $\frac{p+1}{4} \equiv 7 \pmod 8$. By (58), (25), (21), Lemmas 3 and 4, and then (55) and (57),

$$\begin{aligned}\left(N+\frac{1}{2}\right)\log R_1 + \frac{1}{4}\log 2 &= \frac{\pi\sqrt{p}}{8} + \sqrt{2R_1\sqrt{2}}\,q^{-1/8} + 4\,\theta\sum_{r=3}^{\infty} r\,(q^{-1/8})^r \\ &= \frac{\pi\sqrt{p}}{8} + \sqrt{2R_1\sqrt{2}}\,q^{-1/8} + 13\,\theta\,q^{-3/8}.\end{aligned} \tag{74}$$

Since $\sqrt{2R_1\sqrt{2}} = \sqrt{4+2\sqrt{2}}$, we have the inequalities

$$2 < \sqrt{2R_1\sqrt{2}} < \sqrt{7} < 3\,, \tag{75}$$

and thus

$$\sqrt{2R_1\sqrt{2}}\,q^{-1/8} + 13\,\theta\,q^{-3/8} = \sqrt{2R_1\sqrt{2}}\,q^{-1/8}(1 + 7\,\theta\,q^{-1/4}),$$

$$|\sqrt{2R_1\sqrt{2}}\,q^{-1/8} + 13\,\theta\,q^{-3/8}| < 3q^{-1/8}.$$

It follows from (74) and (68) that

$$\begin{aligned}\sqrt{R_1\sqrt{2}}\,R_1^N &= q^{1/8}\left\{1 + (\sqrt{2R_1\sqrt{2}}\,q^{-1/8} + 13\,\theta\,q^{-3/8}) + R_1\sqrt{2}q^{-1/4}(1 + 7\,\theta\,q^{-1/4})^2 \right.\\ &\qquad\left. + \,\theta\sum_{n=3}^{\infty}\frac{(3\,q^{-1/8})^n}{n!}\right\}\\ &= q^{1/8}\left\{1 + \sqrt{2R_1\sqrt{2}}q^{-1/8} + R_1\sqrt{2}q^{-1/4} + 14\,\theta\,q^{-3/8} + \frac{\theta}{6}\,\frac{(3\,q^{-1/8})^3}{1-(3\,q^{-1/8})}\right\}\\ &= q^{1/8}\,\{1 + \sqrt{2R_1\sqrt{2}}q^{-1/8} + R_1\sqrt{2}q^{-1/4} + 19\,\theta\,q^{-3/8}\}\,.\end{aligned}\tag{76}$$

Since

$$\sqrt{2\,R_1\sqrt{2}}q^{-1/8} + R_1\sqrt{2}q^{-1/4} + 19\,\theta\,q^{-3/8} = \sqrt{2R_1\sqrt{2}}q^{-1/8}(1 + 2\,\theta\,q^{-1/8}),$$

we see, after squaring (76) and then using (76) again, that

$$\begin{aligned}\sqrt{2}R_1^{2N+1} &= q^{1/4}\{1 + 2\sqrt{2R_1\sqrt{2}}q^{-1/8} + 2R_1\sqrt{2}q^{-1/4} + 38\,\theta\,q^{-3/8}\\ &\qquad + 2R_1\sqrt{2}q^{-1/4}(1 + 2\,\theta\,q^{-1/8})^2\}\\ &= q^{1/4}\{1 + 2\sqrt{2R_1\sqrt{2}}q^{-1/8} + 4R_1\sqrt{2}q^{-1/4} + 67\,\theta\,q^{-3/8}\}\\ &= q^{1/4}\{1 + 67\,\theta\,q^{-3/8}\} + 2\sqrt{2R_1\sqrt{2}}q^{1/8}\,\{1 + \sqrt{2R_1\sqrt{2}}q^{-1/8}\}\\ &= q^{1/4}\{1 + 67\,\theta\,q^{-3/8}\} + 2\sqrt{2R_1\sqrt{2}}\,\{\sqrt{R_1\sqrt{2}}R_1^N + 4\,\theta\,q^{-1/8}\}\\ &= q^{1/4} + 4R_1^{N+1} + 91\,\theta\,q^{-1/8}\,.\end{aligned}\tag{77}$$

As a result,

$$\frac{1}{2}R_1^{2N+1} - \sqrt{2}R_1^{N+1} = \frac{1}{2\sqrt{2}}q^{1/4} + 47\,\theta\,q^{-1/8}\,.\tag{78}$$

From (75), (76), and (77), we get the inequalities

$$|\sqrt{2}R_2^{N+1}| = \frac{\sqrt{2R_1\sqrt{2}}}{R_1}\cdot\frac{1}{\sqrt{R_1\sqrt{2}R_1^N}} < \frac{3}{2}\cdot\frac{4}{3}q^{-1/8} \le 2q^{-1/8},$$

and

$$\left|\frac{1}{2}R_2^{2N+1}\right| = \frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}R_1^{2N+1}} < 2q^{-1/4}\,.$$

Combining this with (78) and using (39), we see that

$$z_{2N+1} - 4y_{N+1} = \frac{1}{2\sqrt{2}}q^{1/4} + 50\,\theta\,q^{-1/8},$$

or

$$\left|z_{2N+1} - 4y_{N+1} - \frac{1}{2\sqrt{2}}q^{1/4}\right| \le 50q^{-1/8} < \frac{1}{4}\,.\tag{79}$$

This verifies (50).

In the case $\frac{p+1}{4} \equiv 3 \pmod 8$, there are occasional changes in sign from the case $\frac{p+1}{4} \equiv 7 \pmod 8$, but the error terms are identical. Thus we get an improvement over (49):

(80) $$\left| z_{2N+1} + 4y_{N+1} - \frac{1}{2\sqrt{2}} q^{1/4} \right| \leq 50 q^{-1/8} < \frac{1}{4}.$$

We are now in a position to verify (51) to (54) for $p \geq 200$: equation (51) follows from (65) and (73); equation (52) follows from (65) and (72); equation (53) follows from (63) and (80); equation (54) follows from (63) and (79).

5. SOLUTIONS OF EQUATIONS (51) TO (54)

The following relations will be useful: for all integral values of n,

(81) $$z_{2n+1} = 4y_n y_{n+1} + (-1)^n,$$

(82) $$y_{2n} = 2y_n z_n,$$

(83) $$y_{2n-1} = 4y_n^2 - 2y_n z_n + (-1)^n = 2z_n^2 - 2y_n z_n - (-1)^n,$$

(84) $$z_n^2 = 2y_n^2 + (-1)^n,$$

(85) $$z_{-n} = (-1)^n z_n,$$

(86) $$y_{-n} = (-1)^{n+1} y_n,$$

(87) $$y_{n-1} = z_n - y_n,$$

(88) $$z_{n-1} = 2y_n - z_n.$$

These relations follow immediately from the definitions (38) and (39). The linear relations (85) to (88) also follow from the recursion relation (40), by induction. In addition, the relations are not independent; for example, (84) follows from (83). Define N' and a' by

(89) $$N' = \begin{cases} N & \text{if } \frac{p+1}{4} \equiv 1,\ 5 \pmod 8, \\ -N-1 & \text{if } \frac{p+1}{4} \equiv 3,\ 7 \pmod 8, \end{cases}$$

(90) $$a' = \begin{cases} a & \text{if } \frac{p+1}{4} \equiv 1,\ 5 \pmod 8, \\ -a & \text{if } \frac{p+1}{4} \equiv 3,\ 7 \pmod 8. \end{cases}$$

The definition of N in Lemma 3 shows that

(91)
$$\begin{aligned} N' &\geq 0 \quad \left[\frac{p+1}{4} \equiv 1,\ 5 \pmod 8\right], \\ N' &< 0 \quad \left[\frac{p+1}{4} \equiv 3,\ 7 \pmod 8\right]. \end{aligned}$$

From (85), (86), and (89), it follows that if $\frac{p+1}{4} \equiv 3,\ 7 \pmod 8$, then

$$\begin{aligned} z_{2N+1} \pm 4y_{N+1} &= z_{-(2N'+1)} \pm 4y_{-N'} = -z_{2N'+1} \pm 4(-1)^{N'+1} y_{N'} \\ &= -(z_{2N'+1} \pm 4(-1)^{N'} y_{N'}) \end{aligned}$$

and thus all of equations (51) to (54) can be put into the form

(92)
$$(a')^3 + 3 = z_{2N'+1} + 4\varepsilon y_{N'},$$

where

(93)
$$\varepsilon = \begin{cases} -1 & \text{if } \frac{p+1}{4} \equiv 1 \pmod 8, \\ 1 & \text{if } \frac{p+1}{4} \equiv 5 \pmod 8, \\ (-1)^{N'} & \text{if } \frac{p+1}{4} \equiv 3 \pmod 8, \\ -(-1)^{N'} & \text{if } \frac{p+1}{4} \equiv 7 \pmod 8. \end{cases}$$

By (81) and (92),

(94)
$$(a')^3 + 3 - (-1)^{N'} = z_{2N'+1} - (-1)^{N'} + 4\varepsilon y_{N'} = 4y_{N'}(y_{N'+1} + \varepsilon).$$

This shows that a' is even, say

(95)
$$a' = 2b,$$

and as a result, N' is odd, say

(96)
$$N' = 2N'' - 1.$$

Things now simplify considerably. Since N' is odd, (93) becomes

(97)
$$\varepsilon = \begin{cases} -1 & \text{if } \frac{p+1}{4} \equiv 1,\ 3 \pmod 8, \\ 1 & \text{if } \frac{p+1}{4} \equiv 5,\ 7 \pmod 8. \end{cases}$$

Also, (91) and (96) show that

$$\text{(98)}\qquad \begin{aligned} N'' &> 0 \quad \left[\frac{p+1}{4} \equiv 1,\ 5 \pmod 8\right], \\ N'' &\leq 0 \quad \left[\frac{p+1}{4} \equiv 3,\ 7 \pmod 8\right]. \end{aligned}$$

Equations (94) to (96) yield the equation

$$2b^3 + 1 = y_{2N''-1}(y_{2N''} + \varepsilon),$$

and in view of (82) and (83), this becomes

$$\text{(99)}\qquad 2b^3 + 1 = (4y_{N''}^2 - 2y_{N''}z_{N''} + (-1)^{N''})(2y_{N''}z_{N''} + \varepsilon),$$

or equivalently,

$$\text{(100)}\qquad 2b^3 + 1 = (2z_{N''}^2 - 2y_{N''}z_{N''} - (-1)^{N''})(2y_{N''}z_{N''} + \varepsilon).$$

When $\frac{p+1}{4} \equiv 1,\ 3 \pmod 8$ and N" is odd, or when $\frac{p+1}{4} \equiv 5,\ 7 \pmod 8$ and N" is even (in other words, by (97), when $\varepsilon = (-1)^{N''}$), we see from (99) in conjunction with (84) and (87) that

$$\text{(101)}\qquad \begin{aligned} b^3 &= 4y_{N''}^3 z_{N''} - 2y_{N''}^2 z_{N''}^2 + 2\varepsilon y_{N''}^2 = 4y_{N''}^3 z_{N''} - 2y_{N''}^2(z_{N''}^2 - (-1)^{N''}) \\ &= 4y_{N''}^3 z_{N''} - 4y_{N''}^4 = 4y_{N''}^3(z_{N''} - y_{N''}) = 4y_{N''}^3 y_{N''-1}. \end{aligned}$$

When $\frac{p+1}{4} \equiv 1,\ 3 \pmod 8$ and N" is even, or when $\frac{p+1}{4} \equiv 5,\ 7 \pmod 8$ and N" is odd (in other words, by (97), when $\varepsilon = -(-1)^{N''}$), we see from (100) in conjunction with (84) and (88) that

$$\text{(102)}\qquad \begin{aligned} b^3 &= 2y_{N''}z_{N''}^3 - 2y_{N''}^2 z_{N''}^2 + \varepsilon z_{N''}^2 = 2y_{N''}z_{N''}^3 - z_{N''}^2(2y_{N''}^2 + (-1)^{N''}) \\ &= 2y_{N''}z_{N''}^3 - z_{N''}^4 = z_{N''}^3(2y_{N''} - z_{N''}) = z_{N''}^3 z_{N''-1}. \end{aligned}$$

Since $|R_1| \neq |R_2|$, we see from (39) that $y_n = 0$ if and only if $n = 0$. Thus, except when N" = 0, equation (101) leads us to solve the equation

$$\text{(103)}\qquad y_n = 2c^3,$$

where n = N" - 1. Equation (84) shows us that

$$8c^6 + (-1)^n = z_n^2.$$

By Lemma 5, this happens if and only if c = - 1, 0, 1. Since $|y_{-n}| = y_n > 2$ for $n > 2$ (by (86) and induction on the recursion relation (40)), the only solutions to (103) are

$$y_{-2} = 2(-1)^3, \qquad y_0 = 2(0)^3, \qquad y_2 = 2(1)^3.$$

Thus, recalling that the case N" = 0 had to be handled separately, we see that the only solutions to (101) are

(104) $N'' = -1,\ b = -2;\quad N'' = 0,\ b = 0;\quad N'' = 1,\ b = 0;\quad N'' = 3,\ b = 10$

(see Table 3 for values of y_n with $|n| \leq 3$).

We proceed to equation (102). Since $|R_1| \neq |R_2|$ and $z_0 \neq 0$, we see from (39) that $z_n \neq 0$ for all n. Thus in solving (102) we are led to solve

(105) $$z_n = d^3,$$

where $n = N'' - 1$. Equation (84) shows that

$$d^6 - (-1)^n = 2y_n^2.$$

Thus, by Lemma 5, $d = \pm 1$. Since $|z_{-n}| = z_n > 1$ for $n > 1$ (by (85) and induction from (40)), the only solutions to (105) are

$$z_{-1} = (-1)^3,\quad z_0 = (1)^3,\quad z_1 = (1)^3.$$

Hence the only solutions to (102) are

(106) $N'' = 0,\ b = -1;\quad N'' = 1,\ b = 1;\quad N'' = 2,\ b = 3,$

as can be seen from Table 3.

n	-3	-2	-1	0	1	2	3
y_n	5	-2	1	0	1	2	5
z_n	-7	3	-1	1	1	3	7

TABLE 3

We have now completely solved equations (101) and (102), the solutions being exhibited in (104) and (106), respectively. From the two sets of conditions on N" in (101) or (102) and in (98), given a solution to (101) or (102), we can tell exactly to which of the cases $\frac{p+1}{4} \equiv 1, 3, 5, 7 \pmod 8$ it corresponds. For example, by (104), $N'' = -1$ gives a solution to (101). Since N" is odd, we see from the conditions for (101) that we must have $\frac{p+1}{4} \equiv 1$ or $3 \pmod 8$. Also, by (98), $\frac{p+1}{4} \equiv 3$ or $7 \pmod 8$. Therefore $\frac{p+1}{4} \equiv 3 \pmod 8$, and we are dealing with equation (53). We then determine N from N" by (96) and (89) and a from b by (95) and (90). In this way we see that for $N \geq 0$

the only solutions to (51) are $N = 1,\ a = 0;\ N = 3,\ a = 6;\ N = 5,\ a = 20;$

the only solution to (52) is $N = 1,\ a = 2;$

the only solutions to (53) are $N = 0,\ a = 2;\ N = 2,\ a = 4;$

the only solution to (54) is $N = 0,\ a = 0$.

(In solving (51) to (54) we introduced the assumption that $N \geq 0$ in (91). This is sufficient for our purposes, since $N \geq 0$ by its definition in Lemma 3.) Note that the largest value of a listed above is $a = 20$.

6. PROOF OF THE THEOREM, AND CONCLUSION

In Section 4, we proved that if $p \geq 200$ and $h(-p) = 1$, then one of equations (51) to (54) must hold with $a > 20$ (equation (66)), and $N \geq 0$ (definition of N in Lemma 3). But we have just seen in Section 5 that no such solution exists. Thus the hypothesis that $p \geq 200$ and $h(-p) = 1$ is untënable. This proves the theorem.

We noted at the beginning of Section 2 that if $p \geq 19$ and $h(-p) = 1$, then p is a prime and $p \equiv 19 \pmod{24}$. The only primes congruent to 19 (mod 24) in the range from 1 to 200 are 19, 43, 67, 139, and 163. The only maverick among this list is 139, which can easily be eliminated. For example, $x^2 + xy + 35y^2$ and $5x^2 + xy + 7y^2$ are two inequivalent quadratic forms of discriminant -139. Thus we see that the list of possible values of $p > 0$ for which $h(-p) = 1$ may be quickly reduced to the nine values given in the introduction.

REFERENCES

1. L. E. Dickson, *History of the theory of numbers*, 3 volumes, Stechert, New York, 1934.
2. A. Gray, G. B. Mathews, and F. M. Macrobert, *A treatise on Bessel functions and their applications to physics*, Second Edition, Macmillan, London, 1952.
3. K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. 56 (1952), 227-253.
4. H. Heilbronn, *On the class-number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. 5 (1934), 150-160.
5. H. Heilbronn and E. H. Linfoot, *On the imaginary quadratic corpora of class-number one*, Quart. J. Math. Oxford Ser. 5 (1934), 293-301.
6. E. Landau, *Vorlesungen über Zahlentheorie*, 3 Volumes, Chelsea, New York, 1947.
7. H. M. Stark, *On complex quadratic fields with class number equal to one*, Trans. Amer. Math. Soc. 122 (1966), 112-119.
8. H. Weber, *Lehrbuch der Algebra*, Vol. 3, Third edition, Chelsea, New York, 1961.

Addenda. A. Baker has recently established another method of finding, in principle, an upper bound for the numbers p such that $h(-p) = 1$. See his paper, *Linear forms in the logarithms of algebraic numbers*, Mathematika 13 (1966), 204-216.

It should also be noted that a result similar to Lemma 1 can be established for any k such that either $k \equiv 1 \pmod 4$ and k is square-free or $k \equiv 0 \pmod 4$ and $k/4$ is square-free. Further, most of the arithmetic in Lemma 4 can be eliminated. For details see my paper, *L-functions for quadratic forms* (to be published).

The University of Michigan, Dearborn Campus