Osaka University Knowledge Archive

Title	A construction for irregular discriminants
Author(s)	Craig, Maurice
Citation	Osaka Journal of Mathematics. 1977, 14(2), p. 365-402
Version Type	VoR
URL	https://doi.org/10.18910/10250
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

Craig, M.
Osaka J. Math.
14 (1977), 365–402

A CONSTRUCTION FOR IRREGULAR DISCRIMINANTS

MAURICE CRAIG

(Received January 26, 1976)

1. Introduction

By the 3-rank of a number field is meant the rank of the 3-primary component of the ideal class group. For example, the field $\boldsymbol{Q}(\sqrt{-3299})$, with class group $\boldsymbol{C}(3)\times\boldsymbol{C}(9)$, has 3-rank two. No quadratic field presently known has 3-rank exceeding four.

In [3] (q.v. for notation), I showed the existence of infinitely many imaginary quadratic fields with 3-rank three (or larger). Extending this earlier work, the present article provides the following:

Theorem. *Infinitely many imaginary quadratic fields have* 3*-rank at least four.*

This result will be approached by way of:

Proposition (Cf. [3, Prop. 3]). *Suppose that for* $1\leqslant i\leqslant 4$:

(i) *The integers* A_i, B_i *are coprime*;

(ii) *The quantities* $B_i^2-4A_i^3$ *have a common value* D, *such that* $\boldsymbol{Q}(\sqrt{D})$ *is an imaginary quadratic field of discriminant* <-4;

(iii) *There is a prime* l_i *dividing* A_i *for which* B_i *is not a cubic residue*;

(iv) $\frac{1}{2}(B_i+B_j)$ *is a non-zero cubic residue of* l_j *whenever* $1\leqslant i<j\leqslant 4$.

Then with f_i *denoting the class determined by the ideal* $(A_i, \frac{1}{2}(B_i+\sqrt{D})$ *of the field* $\boldsymbol{Q}(\sqrt{D})$, *we have*

$$\langle f_1, f_2, f_3, f_4\rangle\cong\boldsymbol{C}(3)^4\,. \tag{1}$$

For the proof of the Proposition, refer to [16].

The work falls naturally into two main divisions. Parts 2-6 (cf. (ii) above) are concerned with constructing a polynomial D possessing suitably many decompositions in the form B^2-4A^3, where A, B denote polynomials with rational integer coefficients. The remainder is devoted to verifying the premises of the Proposition, for certain values of this expression D.

More specifically, in Part 2 the problem of forming an appropriate function D is reduced to that of obtaining a rational parametric solution to a

certain pair of simultaneous diophantine equations. The latter are best treated by means of *circulants* (taking the place of factorizations using cube roots of unity, in an earlier version). Part 3 accordingly furnishes a treatment of these determinants and in Part 4 the notation is applied in effecting a resolution of the equations in Part 2. The remaining difficulties are then of a computational nature, the statement of the Proposition serving to guide this later division of the work. A number of supplementary matters receive attention in notes at the end.

This article is based on the author's dissertation [4]. I take the opportunity to express my deep gratitude to Professor D.J. Lewis for his sympathetic guidance and unfailing support as my advisor. Thanks are tendered also to Dr W. Ellison, who jointly suggested the topic of the investigation, to Dr P.J. Weinberger for sharing his expertise in the course of many profitable discussions, and to Professor D.H. Lehmer, to whom are due the factorizations of the larger numbers in formulae (60) below.

2. The simultaneous equations

We begin as in [3] from the observation that the polynomial

$$D(X_0,\ Y_0,\ Z_0) = (-X_0+Y_0+Z_0)^2-4Y_0Z_0$$

is a symmetric function of the three variables. This can be turned to advantage by writing $X_0=x_0^3$ and so on, thereby producing a polynomial $D(x_0^3,\ y_0^3,\ z_0^3)$ with three different arrangements in the form B^2-4A^3. To enrich the supply still further, we admit additional variables $x_1, \cdots, z_2$ which are to be such that

$$D(x_0^3,\ y_0^3,\ z_0^3) = D(x_1^3,\ y_1^3,\ z_1^3) = D(x_2^3,\ y_2^3,\ z_2^3)\,.$$

These requirements will be met provided

$$x_1z_1 = x_0z_0\,, \quad x_2y_2 = x_0y_0 \tag{2-a}$$

$$\begin{cases} x_1^3-y_1^3+z_1^3 = -(x_0^3-y_0^3+z_0^3) \\ x_2^3+y_2^3-z_2^3 = -(x_0^3+y_0^3-z_0^3)\,. \end{cases} \tag{2-b}$$

Equations (2-a) are evidently satisfied by the assignments

$$\begin{bmatrix} x_0 & y_0 & z_0 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{bmatrix} = \begin{bmatrix} \lambda a & \mu b & \nu c \\ \lambda c & \mu b_1 & \nu a \\ \lambda b & \mu a & \nu c_1 \end{bmatrix}. \tag{3}$$

Substituting these values in (2-b) produces

$$\begin{cases} \mu^3(b^3+b_1^3) = (\lambda^3+\nu^3)(a^3+c^3) \\ \nu^3(c^3+c_1^3) = (\lambda^3+\mu^3)(a^3+b^3), \end{cases} \tag{4}$$

this being the diophantine system alluded to in the Introduction.

The system is separately homogeneous in both Greek and Roman letters, so that every solution amounts in fact to a doubly infinite solution set. It will be clear however, that since

$$D((\lambda a)^3, (\mu b)^3, (\nu c)^3) = ((\lambda a)^3+(\mu b)^3-(\nu c)^3)^2-4(\lambda a \mu b)^3 \tag{5}$$

is likewise bi-homogeneous, this feature does not lead to a proliferation of fields $\boldsymbol{Q}(\sqrt{D})$. The various integer values of D so obtained will all be sixth-power multiples of a common, least integer value.

3. Circulants

Let σ denote a generator of the cyclic group $\boldsymbol{C}(3)$. The regular representation of $\boldsymbol{C}(3)$ maps σ to the matrix

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

The element $p\mathbf{1}+q\sigma+r\sigma^2$ $(\sigma^3=\mathbf{1})$ of the rational group algebra $\boldsymbol{QC}(3)$ is carried to the matrix

$$\Gamma(p,q,r) = \begin{bmatrix} p & r & q \\ q & p & r \\ r & q & p \end{bmatrix},$$

known as a cyclic matrix of the third order. The determinant

$$\Delta(p, q, r) = \det \Gamma(p, q, r)$$

is called a cyclic determinant, or circulant. Since $\boldsymbol{QC}(3)$ is a commutative ring, multiplication of cyclic matrices is commutative and the products are again cyclic matrices. We note that

$$\Gamma(p, q, r)^T = \Gamma(p, r, q)$$

and

$$\operatorname{adj} \Gamma(p, q, r) = \Gamma(p^2-qr, r^2-pq, q^2-rp)\,.$$

Thus the transpose of a cyclic matrix and the inverse of a nonsingular cyclic matrix are both cyclic.

Unit circulants

The diophantine equation

$$\Delta(p, q, r) = 1 \tag{6}$$

can be solved completely (in rational numbers p, q, r) with the aid of a change of variables. We set

$$\text{(7–a)} \qquad \begin{cases} [p, q, r] = [\alpha+s, \beta+s, \gamma+s] \\ \text{where} \quad \alpha+\beta+\gamma = 0 . \end{cases}$$

The inverse transformation is given by

$$\text{(7-b)} \qquad \begin{cases} 3s = p+q+r \\ [\alpha, \beta, \gamma] = [p-s, q-s, r-s] . \end{cases}$$

By means of (7-a) (ii), it is possible to write (7-a) (i) in terms of only three new variables (say α, β, s), but it is better to preserve symmetry.

In view of the identity

$$\begin{vmatrix} p & r & q \\ q & p & r \\ r & q & p \end{vmatrix} = (p+q+r) \begin{vmatrix} p-q & r-p \\ q-r & p-q \end{vmatrix},$$

equation (6) assumes the form

$$(8) \qquad 3s \begin{vmatrix} \alpha-\beta & \gamma-\alpha \\ \beta-\gamma & \alpha-\beta \end{vmatrix} = 1 .$$

As this is linear in s, however, it serves to determine the latter in terms of the other new variables.

Equations (7) and (8) express in parametric form the complete solution of (6). The letters α, β, γ (possibly accented) will be standard notation for three rational-valued parameters (not all zero) subject to the single restraint (7-a) (ii). Further, we shall write

$$\text{(9-a)} \qquad \phi = \phi(\alpha, \beta, \gamma) = \begin{vmatrix} \alpha-\beta & \gamma-\alpha \\ \beta-\gamma & \alpha-\beta \end{vmatrix},$$

$$\text{(9-b)} \qquad [L, M, N] = [\alpha+1/3\phi, \beta+1/3\phi, \gamma+1/3\phi]$$

(where $L=L(\alpha, \beta, \gamma)$ and so on).

In summary,

$$[p, q, r] = [L, M, N]$$

gives the general solution of equation (6). The values of α, β, γ are recoverable from those of p, q, r by use of relations (7-b), and in fact it follows directly from (9) that

$$\text{(10)} \qquad \begin{cases} [\alpha, \beta, \gamma] = [L-s, M-s, N-s] \\ \text{where} \qquad 3s = L+M+N . \end{cases}$$

Three further functions U, V, W of α, β, γ are defined by

$$[U, V, W] = [L^2-MN, M^2-NL, N^2-LM]. \tag{11}$$

Thus $\Gamma(U, V, W)$ is the matrix of cofactors for $\Gamma(L, M, N)$. We have $\Delta(L, M, N)=1$, hence

$$\Gamma(L, M, N)^{-1} = \operatorname{adj} \Gamma(L, M, N) = \Gamma(U, V, W)^T = \Gamma(U, W, V).$$

Writing I for the identity matrix $\Gamma(1, 0, 0)$, we obtain the relation

$$\Gamma(L, M, N)\Gamma(U, V, W)^T = I, \tag{12}$$

by transposition of which it follows that

$$\Gamma(U, V, W)\Gamma(L, M, N)^T = I.$$

The transformation (11) is therefore involutory, that is,

$$[L, M, N] = [U^2-VW, V^2-WU, W^2-UV].$$

(To save repeated back-reference, the reader is asked to memorize both (11) and these inverse formulae. They will be needed constantly.) Thence

$$L(L^2-MN) = LU = (U^2-VW)U$$

or

$$L^3-U^3 = LMN-UVW.$$

This extends by symmetry of the right side to yield the relations

$$L^3-U^3=M^3-V^3=N^3-W^3 = LMN-UVW. \tag{13}$$

The expanded form of (12) provides the identities

$$\begin{cases} LV+MW+NU = 0 \\ LW+MU+NV = 0. \end{cases} \tag{14}$$

On solving these as a pair of linear equations to determine M, V we find the expressions

$$M = \frac{N^2U-L^2W}{LU-NW}, \quad V = \frac{LW^2-NU^2}{LU-NW}. \tag{15}$$

Lastly, (7-a) (ii) shows that

$$\alpha^2-\beta\gamma=\beta^2-\gamma\alpha=\gamma^2-\alpha\beta.$$

The common value of these three quantities will be one third of their sum, hence $\frac{1}{3}\phi$. By (9-b) and (11) however,

$$U=\left(\alpha+\frac{1}{3\phi}\right)^2-\left(\beta+\frac{1}{3\phi}\right)\left(\gamma+\frac{1}{3\phi}\right)$$
$$=\alpha^2-\beta\gamma+\frac{\alpha}{\phi}, \qquad \text{by (7-a) (ii).}$$

Writing

$$\begin{bmatrix} \boldsymbol{L} & \boldsymbol{U} \\ \boldsymbol{M} & \boldsymbol{V} \\ \boldsymbol{N} & \boldsymbol{W} \end{bmatrix} = 3\phi \begin{bmatrix} L & U \\ M & V \\ N & W \end{bmatrix}, \tag{16}$$

we have therefore the formulae

$$\begin{bmatrix} \boldsymbol{L} & \boldsymbol{U} \\ \boldsymbol{M} & \boldsymbol{V} \\ \boldsymbol{N} & \boldsymbol{W} \end{bmatrix} = \begin{bmatrix} 1+3\alpha\phi & \phi^2+3\alpha \\ 1+3\beta\phi & \phi^2+3\beta \\ 1+3\gamma\phi & \phi^2+3\gamma \end{bmatrix}. \tag{17}$$

These polynomial functions $\boldsymbol{L}, \cdots, \boldsymbol{W}$ are ultimately better suited to express the solution of equations (4). We shall find it easier however, to work with the rational functions $L, \cdots, W$, using (16) to translate the results as required.

Carmichael's and Vieta's equations

The complete solution of the diophantine equation

$$\Delta(p'', q'', r'') = \Delta(p', q', r') \tag{18}$$

was given by Carmichael [2]. Assuming that neither side vanishes (N.B. $2\Delta\,(p, q, r)=\sum p \sum (q-r)^2$), we can write the equation as

$$\det\{\Gamma(p'', q'', r'')\Gamma(p', q', r')^{-1}\} = 1\,.$$

From our earlier remarks, it follows that the expression in braces is a cyclic matrix. We conclude that

$$\Gamma(p'', q'', r'') = \Gamma(p, q, r)\Gamma(p', q', r')$$

where (6) holds. In other words

$$\begin{bmatrix} p'' \\ q'' \\ r'' \end{bmatrix} = \Gamma(L, M, N) \begin{bmatrix} p' \\ q' \\ r' \end{bmatrix}.$$

Consider next the diophantine equation

$$x^3+y^3 = z^3+w^3\,, \tag{19}$$

first solved in full generality by Euler [2, 5, 9]. It is clear from (13) that

$$x:y:z:w = L:-U:N:-W \tag{20}$$

affords a parametric solution. Apart from solutions of the form $[x, y, x, y]$, this is in fact the general solution. For equation (19) may be put in the form

$$\Delta(x, 0, -z) = \Delta(-y, w, 0),$$

showing it to be a restricted case of (18). (A distribution of symbols has been chosen which leads to (20). There are evidently many solutions of (19) inherent in (13), all of them forms of the general solution.) Thus

$$\Gamma(L, M, N)\Gamma(x, 0, -z) = \Gamma(-y, w, 0)$$

or

$$\begin{bmatrix} -y \\ w \\ 0 \end{bmatrix} = \begin{bmatrix} Lx-Mz \\ Mx-Nz \\ Nx-Lz \end{bmatrix},$$

in agreement with (20).

Lemma. *Let $L'=L(\alpha', \beta', \gamma')$ and so on. Then α', β', γ' can be chosen rationally in terms of α, β, γ so as to produce*

$$\frac{L}{L'} = \frac{U}{N'} = \frac{N}{U'} = \frac{W}{W'} \qquad (set=J). \tag{21}$$

Proof. Equation (19) may be put in the alternative form

$$\Delta(x, 0, y) = \Delta(z, w, 0),$$

and then for suitable values of α', β', γ' we shall have

$$\Gamma(L', M', N')\Gamma(x, 0, y) = \Gamma(z, w, 0) \tag{22}$$

hence

$$x:y:z:w=L':-N':U':-W'.$$

A comparison with (20) yields (21). Q.E.D.

To obtain α', β', γ' explicitly in terms of α, β, γ, write (22) in the form

$$\begin{bmatrix} L' \\ M' \\ N' \end{bmatrix} = \Gamma(x, 0, y)^{-1} \begin{bmatrix} z \\ w \\ 0 \end{bmatrix}.$$

Since

$$\operatorname{adj} \Gamma(x, 0, y) = \Gamma(x^2, y^2, -xy),$$

the right side becomes

$$(x^3+y^3)^{-1} \begin{bmatrix} x(xz-yw) \\ y^2z+x^2w \\ -y(xz-yw) \end{bmatrix}.$$

Thus from (20) we obtain

$$\begin{bmatrix} L' \\ M' \\ N' \end{bmatrix} = (L^3-U^3)^{-1} \begin{bmatrix} L(LN-UW) \\ NU^2-L^2W \\ U(LN-UW) \end{bmatrix} \tag{23}$$

where the factor $(L^3-U^3)^{-1}$ may be replaced by $(LMN-UVW)^{-1}$, in accordance with (13). We find that

$$L'+M'+N' = \frac{N-W}{L-U}$$

and then α', β', γ' can be obtained at once from (10′) (denoting the primed-notation analogue of (10)). Moreover, (23) gives for the common value of the ratios in (21),

$$J = \frac{LMN-UVW}{LN-UW}. \tag{24}$$

Finally, we can supplement (21) by relations which allow M' and V' to be expressed in terms of L, U, N, W. Thus by (21), the equations

$$M' = \frac{N'^2U'-L'^2W'}{L'U'-N'W'}, \quad V' = \frac{L'W'^2-N'U'^2}{L'U'-N'W'} \tag{15′}$$

take the form

$$JM' = \frac{NU^2-L^2W}{LN-UW}, \quad JV' = \frac{LW^2-N^2U}{LN-UW}. \tag{25}$$

Combining (25) (i) with (24) gives, of course, the same expression for M' as lent already by (23).

REMARK. Although no use will be made of it, the following property of the functions L, M, N seems worth mentioning. Suppose that

$$\Gamma(L'', M'', N'') = \Gamma(L, M, N)\Gamma(L', M', N').$$

Then the associated parameters are related by the equation

$$\Gamma(\alpha'', \beta'', \gamma'') = \Gamma(\alpha, \beta, \gamma)\Gamma(\alpha', \beta', \gamma').$$

For on multiplying the former equation by $\Gamma(1, 1, 1)$, we obtain

$$L''+M''+N'' = (L+M+N)(L'+M'+N'),$$

while from (10),

$$\Gamma(L, M, N) = \Gamma(\alpha, \beta, \gamma)+\frac{1}{3}(L+M+N)\Gamma(1, 1, 1).$$

The result then follows directly.

4. The rational parametric solution

A solution in the field $\boldsymbol{Q}(\alpha, \beta, \gamma)$ will be obtained for the system (4). Taking the equations separately, we may write (4) (i) in the form

$$\Delta(\mu b, \mu b_1, 0) = \Delta(\lambda, 0, \nu)\Delta(a, 0, c)$$

and so obtain a parametric solution by setting

$$\Gamma(L, M, N)\Gamma(\mu b, \mu b_1, 0) = \Gamma(\lambda, 0, \nu)\Gamma(a, 0, c)$$

or
$$\begin{bmatrix} \mu b \\ \mu b_1 \\ 0 \end{bmatrix} = \Gamma(U, W, V)\begin{bmatrix} \lambda a \\ \nu c \\ \nu a+\lambda c \end{bmatrix} = \begin{bmatrix} (\lambda U+\nu W)a+(\lambda W+\nu V)c \\ (\lambda W+\nu V)a+(\lambda V+\nu U)c \\ (\lambda V+\nu U)a+(\lambda U+\nu W)c \end{bmatrix}.$$

This yields the formulae

$$\begin{cases} \dfrac{c}{a} = -\dfrac{\lambda V+\nu U}{\lambda U+\nu W} \\ \dfrac{\mu b}{a} = \dfrac{\lambda^2 L-\lambda\nu M+\nu^2 N}{\lambda U+\nu W} \\ \dfrac{\mu b_1}{a} = -\dfrac{\lambda^2 M-\lambda\nu N+\nu^2 L}{\lambda U+\nu W}. \end{cases}$$

A solution of (4) (ii) can be read off by symmetry. With $L'=L(\alpha', \beta', \gamma')$ and so on, we have

$$\begin{cases} \dfrac{b}{a} = -\dfrac{\lambda V'+\mu U'}{\lambda U'+\mu W'} \\ \dfrac{\nu c}{a} = \dfrac{\lambda^2 L'-\lambda\mu M'+\mu^2 N'}{\lambda U'+\mu W'} \\ \dfrac{\nu c_1}{a} = -\dfrac{\lambda^2 M'-\lambda\mu N'+\mu^2 L'}{\lambda U'+\mu W'}. \end{cases}$$

A simultaneous solution of equations (4) will be achieved by showing how α', β', γ' may be chosen in terms of α, β, γ so as to reconcile the disparate expressions for b/a and c/a afforded by the two sets of formulae above. For this we require

$$(26) \qquad \begin{cases} \dfrac{\lambda^2 L-\lambda\nu M+\nu^2 N}{\lambda U+\nu W} = -\mu\dfrac{\lambda V'+\mu U'}{\lambda U'+\mu W'} & \left(=\dfrac{\mu b}{a}\right) \\ -\nu\dfrac{\lambda V+\nu U}{\lambda U+\nu W} = \dfrac{\lambda^2 L'-\lambda\mu M'+\mu^2 N'}{\lambda U'+\mu W'} & \left(=\dfrac{\nu c}{a}\right). \end{cases}$$

Now from (14) (ii),

$$U(\lambda^2 L-\lambda\nu M+\nu^2 N)=\lambda L(\lambda U+\nu W)+\nu N(\lambda V+\nu U)\,.$$

There is an analogous identity in the primed notation. If we write

$$\mu^*=-\mu\frac{\lambda V'+\mu U'}{\lambda U'+\mu W'}\,,\quad \nu^*=-\nu\frac{\lambda V+\nu U}{\lambda U+\nu W}\,,$$

equations (26) will therefore assume the form

$$\begin{cases}\lambda L=\mu^* U+\nu^* N\\ \lambda L'=\mu^* N'+\nu^* U'\,.\end{cases}$$

Let α', β', γ' now be chosen, as the Lemma shows may be done, so that (21) is satisfied. Then the relations just written, regarded as a pair of linear equations to determine the ratios λ: μ^*: ν^*, are seen to be linearly dependent. (Conversely, if they are dependent, then (21) must hold. For

$$\frac{L}{L'}=\frac{U}{N'}=\frac{N}{U'}$$

and the cube of each ratio will equal

$$\frac{L^3-U^3-N^3}{L'^3-N'^3-U'^3}=\frac{W^3}{W'^3}\,,$$

by (13), (13′).) Returning to the earlier form (26) of these relations, we need therefore only solve the single equation obtained by subtracting corresponding sides, namely

$$\frac{\lambda^2 L-\lambda\nu(M-V)+\nu^2(N+U)}{\lambda U+\nu W}+\frac{\lambda^2 L'-\lambda\mu(M'-V')+\mu^2(N'+U')}{\lambda U'+\mu W'}=0\,. \tag{27}$$

This can be accomplished as follows. Set

$$k=\frac{U}{W}+\frac{U'}{W'}\,. \tag{28}$$

From (21),

$$k=\frac{N+U}{W}=\frac{N'+U'}{W'}\,. \tag{29}$$

The choice

$$\mu+\nu=-k\lambda \tag{30}$$

reduces (27) to a mere linear equation, which may then be solved simultaneously with (30) itself to yield the ratios μ/λ, ν/λ.

In fact, eliminating k between (28) and (30) produces

$$\frac{\lambda U+\nu W}{W}+\frac{\lambda U'+\mu W'}{W'}=0\,, \tag{31}$$

which simplifies (27) to the form

$$\frac{\lambda^2 L-\lambda\nu(M-V)+\nu^2(N+U)}{W}=\frac{\lambda^2 L'-\lambda\mu(M'-V')+\mu^2(N'+U')}{W'}\,.$$

By (21), $\lambda^2 L/W=\lambda^2 L'/W'$. Subtracting this quantity from both sides and using (29), we are left with the equation

$$k\nu^2-\frac{M-V}{W}\lambda\nu=k\mu^2-\frac{M'-V'}{W'}\lambda\mu\,.$$

This gives upon rearrangement

$$\begin{aligned}\lambda\left(\frac{M-V}{W}\nu-\frac{M'-V'}{W'}\mu\right)&=k(\nu^2-\mu^2)\\&=k^2\lambda(\mu-\nu)\,,\qquad\text{by (30).}\end{aligned}$$

Hence

$$\left(k^2+\frac{M'-V'}{W'}\right)\mu=\left(k^2+\frac{M-V}{W}\right)\nu\,. \tag{32}$$

A mental check now suffices to show the solution of the linear system (30)-(32) to be

$$\left\{\begin{aligned}\frac{\mu}{\lambda}&=\frac{-k\left(k^2+\dfrac{M-V}{W}\right)}{2k^2+\dfrac{M-V}{W}+\dfrac{M'-V'}{W'}}\,,\\[2ex]\frac{\nu}{\lambda}&=\frac{-k\left(k^2+\dfrac{M'-V'}{W'}\right)}{2k^2+\dfrac{M-V}{W}+\dfrac{M'-V'}{W'}}\,.\end{aligned}\right. \tag{33}$$

In summary, the solution obtained for the bi-homogeneous system (4) is the following:

$$\left\{\begin{aligned}&\mu/\lambda,\ \nu/\lambda \text{ given by equations (33);}\\[1ex]&\frac{b}{a}=\frac{1}{\mu}\,\frac{\lambda^2 L-\lambda\nu M+\nu^2 N}{\lambda U+\nu W}=-\frac{\lambda V'+\mu U'}{\lambda U'+\mu W'}\\[2ex]&\frac{c}{a}=-\frac{\lambda V+\nu U}{\lambda U+\nu W}=\frac{1}{\nu}\,\frac{\lambda^2 L'-\lambda\mu M'+\mu^2 N'}{\lambda U'+\mu W'}\end{aligned}\right. \tag{34}$$

$$\left|\begin{array}{l} \dfrac{b_1}{a} = -\dfrac{1}{\mu}\,\dfrac{\lambda^2 M-\lambda\nu N+\nu^2 L}{\lambda U+\nu W} \\ \dfrac{c_1}{a} = -\dfrac{1}{\nu}\,\dfrac{\lambda^2 M'-\lambda\mu N'+\mu^2 L'}{\lambda U'+\mu W'}\,. \end{array}\right.$$

The values of α', β', γ' for these formulae are to be determined from those of α, β, γ as described at the end of the preceding section (they will not be needed explicitly), while (in (33)) $k=(N+U)/W$. (See also Note A.)

5. Identities

From equation (31) we see that

$$\lambda U'+\mu W' = -J^{-1}(\lambda U+\nu W)\,.$$

By formulae (34), the system (4) thus has a solution in which

$$\text{(35-a)} \qquad \left\{\begin{array}{r} a = -(\lambda U+\nu W) \\ c = \lambda V+\nu U \\ \mu b = -(\lambda^2 L-\lambda\nu M+\nu^2 N) \\ \mu b_1 = \lambda^2 M-\lambda\nu N+\nu^2 L\,, \end{array}\right.$$

$$\text{(35-b)} \qquad \left\{\begin{array}{r} -J^{-1}a = -(\lambda U'+\mu W') \\ -J^{-1}b = \lambda V'+\mu U' \\ -J^{-1}\nu c = -(\lambda^2 L'-\lambda\mu M'+\mu^2 N') \\ -J^{-1}\nu c_1 = \lambda^2 M'-\lambda\mu N'+\mu^2 L'\,. \end{array}\right.$$

Several useful relations connecting the variables on the left side in (3) follow from the above. The first of these are

$$\text{(36-a)} \qquad \left\{\begin{array}{l} x_0 = Ly_0+Ny_1 \\ z_0 = My_0+Ly_1\,, \end{array}\right.$$

$$\text{(36-b)} \qquad \left\{\begin{array}{l} x_0 = L'z_0+N'z_2 \\ y_0 = M'z_0+L'z_2\,. \end{array}\right.$$

In fact,

$$-x_0+Ly_0+Ny_1 = -\lambda a+L\mu b+N\mu b_1$$

and (36-a) (i) results immediately on substituting the values given by (35-a). The other three relations are obtained similarly.

Further identities can be deduced by elimination (that is, by solving). Thus we find

$$\text{(37-a)} \qquad \begin{cases} Lx_0 - Uy_0 - Nz_0 = 0 \\ Mx_0 + Uy_1 - Lz_0 = 0\,, \end{cases}$$

$$\text{(37-b)} \qquad \begin{cases} L'x_0 - N'y_0 - U'z_0 = 0 \\ M'x_0 - L'y_0 + U'z_2 = 0\,. \end{cases}$$

Application of (21) to (37-b) (i) yields (37-a) (i) again, while applying (21) to (37-b) (ii) produces

$$JM'x_0 - Ly_0 + Nz_2 = 0\,.$$

Eliminating y_0 between this equation and (36-a) (i), we get

$$\text{(38)} \qquad N(y_1 + z_2) = (1 - JM')x_0\,.$$

In addition to these linear relations, there are also quadratic identities connecting the triplets of subscripted variables. Indeed (35-a) gives

$$\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} = \begin{bmatrix} \lambda c \\ \mu b_1 \\ \nu a \end{bmatrix} = \begin{bmatrix} V & U & 0 \\ M & -N & L \\ 0 & -U & -W \end{bmatrix} \begin{bmatrix} \lambda^2 \\ \lambda\nu \\ \nu^2 \end{bmatrix}.$$

Inverting the matrix and making use of (14), we find

$$-LN \begin{bmatrix} \lambda^2 \\ \lambda\nu \\ \nu^2 \end{bmatrix} = \begin{bmatrix} LU + NW & UW & LU \\ MW & -VW & -LV \\ -MU & UV & LW \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix},$$

so that by elimination of λ, ν,

$$\begin{aligned} &(MWx_1 - VWy_1 - LVz_1)^2 \\ &\quad = ((LU + NW)x_1 + UWy_1 + LUz_1)(-MUx_1 + UVy_1 + LWz_1)\,, \end{aligned}$$

or finally (by application of (14) and after division by L)

$$\text{(39-a)} \qquad LM(x_1 + z_1)^2 - N^2 x_1 z_1 = VWy_1^2 + (LV - MW)(x_1 + z_1)y_1\,.$$

The analogous identity satisfied by x_2, y_2, z_2 is

$$\text{(39-b)} \qquad L'M'(x_2 + y_2)^2 - N'^2 x_2 y_2 = V'W'z_2^2 + (L'V' - M'W')(x_2 + y_2)z_2\,.$$

It is to be noted that although not every solution of (4) given by (34) will satisfy (35), the relations obtained in Part 5 will be valid anyway. For the bi-homogeneity of these relations leaves them free of the added restriction on the value of a/λ imposed by the parent equations (35).

6. The simplified solution

The values used for the Greek letters in (35) must satisfy (33). Hence

$$[\lambda, \mu, \nu] = \delta[\bar{\lambda}, \bar{\mu}, \bar{\nu}]$$

where

$$(40) \qquad \begin{cases} \bar{\lambda} = -2k - \dfrac{1}{k}\left(\dfrac{M-V}{W} + \dfrac{M'-V'}{W'}\right) \\ \bar{\mu} = k^2 + \dfrac{M-V}{W} \\ \bar{\nu} = k^2 + \dfrac{M'-V'}{W'}, \end{cases}$$

while is δ arbitrary. We shall next simplify certain of formulae (35)-(40), assigning δ a particular value chosen to help achieve this end.

Set

$$(41) \qquad K = M+V+1 .$$

We have

$$\begin{aligned} K(M-V) &= M^2-V^2+(V^2-UW)-(M^2-LN) \\ &= LN-UW . \end{aligned}$$

Again, by (13),

$$L^3+W^3 = N^3+U^3 ,$$

giving

$$\frac{L^2-LW+W^2}{N+U} = \frac{N^2-NU+U^2}{L+W} ,$$

where the common value of the two members will be shared also by the ratio

$$\frac{NU(L^2-LW+W^2)-LW(N^2-NU+U^2)}{NU(N+U)-LW(L+W)} .$$

The numerator in this expression simplifies to $(LU-NW)(LN-UW)$, while as regards the denominator, (15) gives

$$M-V = \frac{NU(N+U)-LW(L+W)}{LU-NW} .$$

This serves to establish the formulae

$$(42) \qquad \frac{L^2-LW+W^2}{N+U} = \frac{N^2-NU+U^2}{L+W} = \frac{LN-UW}{M-V} = K .$$

We may use (29) and (42) to write

$$k=\frac{N+U}{W}=\frac{L^2-LW+W^2}{KW}. \tag{43}$$

And from (42), (24) and (13),

$$JK=M^2+MV+V^2. \tag{44}$$

By (42) and (44), we see that it is appropriate to define

$$\boldsymbol{J}=3\phi J, \quad \boldsymbol{K}=3\phi K.$$

Formulae containing the letters J, K and homogeneous in $L, \cdots, W$ will then remain valid on replacing the latter by $\boldsymbol{L}, \cdots, \boldsymbol{W}$, provided we also change J to $\boldsymbol{J}$ and K to $\boldsymbol{K}$.

Next, for the numerators in (25), we have

$$\begin{aligned} NU^2-L^2W &= N(U^2-VW)-(L^2-MN)W-NW(M-V) \\ &= (LN-UW)-NW(M-V) \end{aligned}$$

and likewise

$$LW^2-N^2U=(LN-UW)-LU(M-V).$$

So by (42),

$$JM'=1-NW/K, \quad JV'=1-LU/K \tag{45}$$

whence on subtraction (*N.B.* $W'=W/J$)

$$\frac{M'-V'}{W'}=\frac{LU-NW}{KW}. \tag{46}$$

Moreover,

$$(LU-NW)+(LN-UW)=(L-W)(N+U), \tag{47}$$

so with the help of (29) we derive

$$\frac{1}{k}\left(\frac{M-V}{W}+\frac{M'-V'}{W'}\right)=\frac{L-W}{K}. \tag{48}$$

When the values given by (43), (46) and (48) are introduced in equations (40), we find

$$\begin{cases} \bar{\lambda}=-2\dfrac{L^2-LW+W^2}{KW}-\dfrac{L-W}{K} \\ \bar{\mu}=\left(\dfrac{N+U}{W}\right)^2+\dfrac{M-V}{W} \\ \bar{\nu}=\dfrac{N+U}{W}\,\dfrac{L^2-LW+W^2}{KW}+\dfrac{LU-NW}{KW}. \end{cases}$$

By (47), we can write

$$(N+U)(L^2-LW+W^2)+W(LU-NW)=$$
$$(N+U)[(L^2-LW+W^2)+W(L-W)]-W(LN-UW),$$

which by (42) reduces simply to $L^2(N+NU)-KW(M-V)$.

Consideration of the denominators in the expressions thus obtained for $\bar{\lambda}$, $\bar{\mu}$, $\bar{\nu}$ leads to the choice $\delta=KW^2$. We have then the formulae

$$\text{(49)}\qquad \begin{cases} \lambda = -W[2(L^2-LW+W^2)+W(L-W)] \\ \quad = -W(2L^2-LW+W^2) \\ \mu = K[(N+U)^2+W(M-V)] \\ \nu = (N+U)(L^2-LW+W^2)+W(LU-NW) \\ \quad = L^2(N+U)-KW(M-V). \end{cases}$$

Equations (45) in conjunction with (21) permit the reduction of several other formulae also. Thus (35-b) (ii) gives

$$\text{(50)}\qquad b=-(1-LU/K)\lambda-N\mu$$

while (36-b) (ii), (38) and (39-b) yield in turn

$$\text{(51)}\qquad Jy_0=(1-NW/K)z_0+Lz_2$$

$$\text{(52)}\qquad Wx_0=K(y_1+z_2)$$

$$\text{(53)}\qquad L(1-NW/K)(x_2+y_2)^2-U^2x_2y_2=$$
$$W(1-LU/K)z_2^2+[(L-W)+(NW^2-L^2U)/K](x_2+y_2)z_2.$$

Proceeding with the simplification of (35-a) (i), we have by (49)

$$\begin{aligned} -a/W &= U(\lambda/W)+\nu \\ &= -U[2(L^2-LW+W^2)+W(L-W)] \\ &\quad +(N+U)(L^2-LW+W^2)+W(LU-NW) \\ &= (N-U)(L^2-LW+W^2)-W^2(N-U). \end{aligned}$$

Hence

$$\text{(54)}\qquad a=-LW(L-W)(N-U).$$

And by elimination of ν between (35-a) (i) and (ii),

$$\text{(55)}\qquad Wc=-L\lambda-Ua.$$

The equations (54), (50), (55), (36-a) (i) and (52) can now be assembled to read as follows:

$$
(56)\qquad \begin{cases} a = -LW(L-W)(N-U) \\ b = -(1-LU/K)\lambda - N\mu \\ c = L(-\lambda/W) + U(-a/W) \\ N\mu b_1 = \lambda a - L\mu b \\ K\nu c_1 = W\lambda a - K\mu b_1 . \end{cases}
$$

It is these formulae, together with (49), which constitute the "simplified" solution. As noted in Part 3 however, we want a solution of (4) in terms of $\boldsymbol{L}, \cdots, \boldsymbol{W}$ (see (16)) rather than $L, \cdots, W$, in order that integer values of the parameters α, β, γ may produce integer values of D in equation (5). Taking advantage of the bi-homogeneity of (4), we therefore cause the Greek letters in (49) to absorb a factor $(3\phi)^3$, the Roman letters in (56) a factor $(3\phi)^4$, and so write down the following as our final form of the solution to equations (4):

$$
(57)\qquad \begin{cases} \boldsymbol{K} = \boldsymbol{M} + \boldsymbol{V} + 3\phi \qquad \text{(see (41))} \\ \lambda = -\boldsymbol{W}(2\boldsymbol{L}^2 - \boldsymbol{L}\boldsymbol{W} + \boldsymbol{W}^2) \\ \mu/\boldsymbol{K} = (\boldsymbol{N}+\boldsymbol{U})^2 + \boldsymbol{W}(\boldsymbol{M}-\boldsymbol{V}) \\ \nu = \boldsymbol{L}^2(\boldsymbol{N}+\boldsymbol{U}) - \boldsymbol{K}\boldsymbol{W}(\boldsymbol{M}-\boldsymbol{V}) \\ a = -\boldsymbol{L}\boldsymbol{W}(\boldsymbol{L}-\boldsymbol{W})(\boldsymbol{N}-\boldsymbol{U}) \\ \boldsymbol{K}b = -\lambda(3\phi\boldsymbol{K} - \boldsymbol{L}\boldsymbol{U}) - \mu\boldsymbol{K}\boldsymbol{N} \\ c/\boldsymbol{L} = 3\phi(-\lambda/\boldsymbol{W}) + \boldsymbol{U}(-a/\boldsymbol{L}\boldsymbol{W}) \\ \boldsymbol{N}\mu b_1 = 3\phi\lambda a - \boldsymbol{L}\mu b \\ \boldsymbol{K}\nu c_1 = \boldsymbol{W}\lambda a - \boldsymbol{K}\mu b_1 . \end{cases}
$$

Lastly, we remark that formulae (35) become valid for the above solution if $L, \cdots, W$ are replaced by $\boldsymbol{L}, \cdots, \boldsymbol{W}$. The relations so obtained will find use in Part 8.

7. The main example

The present section will exhibit a specific imaginary quadratic field with 3-rank (at least) four. How from this one example we may infer the existence of infinitely many such fields, will be seen in Part 8.
Take as solution to (7a) (ii)

$$
(58)\qquad [\alpha, \beta, \gamma] = [0, 3, -3] .
$$

By (9-a) we have $\phi = 3^3$, hence by (17)

$$
(59)\qquad \begin{bmatrix} \boldsymbol{L} & \boldsymbol{U} \\ \boldsymbol{M} & \boldsymbol{V} \\ \boldsymbol{N} & \boldsymbol{W} \end{bmatrix} = \begin{bmatrix} 1 & 729 \\ 244 & 738 \\ -242 & 720 \end{bmatrix} .
$$

It is then a matter of patience (see Note B) to verify the following values coming from (57):

$$
(60)\qquad \begin{cases}
\boldsymbol{K} = 1063 \\
\lambda = -2^5\cdot 3^2\cdot 5\cdot 11\cdot 23531 \\
\mu/\boldsymbol{K} = -\mathbf{37}\cdot 3203 \\
\nu = \mathbf{378\ 088\ 327} \\
a = -2^4\cdot 3^2\cdot 5\cdot 719\cdot 971 \\
\boldsymbol{K}b = -2\cdot 11\cdot \mathbf{2749}\cdot 2837\cdot 3413 \\
c = 3^4\cdot 6\ 801\ 023 \\
\mu b_1 = -\mathbf{79}\cdot 79018\ 39513\ 77089 \\
\boldsymbol{K}\nu c_1 = 1231\cdot 736\ 717\cdot 22\ 19170\ 41539\,.
\end{cases}
$$

We shall need the fact that the four numbers printed in bold type are primes congruent to 1 (mod 3). While three of these numbers scarcely require the use of tables, the value of ν lies beyond the range of existing tables. Its primality can be confirmed without recourse to mechanical means of computation, by applying the Gaussian method of exclusions, for example (see Note C).

The Proposition stated in the Introduction is next brought to bear on the field $\boldsymbol{Q}(\sqrt{D})$, D being given by (5). These two are placed in relation to one another by the table which follows.

i	A_i	B_i	l_i	Integer Multiples
1	$x_0z_0=x_1z_1$	$x_0^3-y_0^3+z_0^3$	ν	z_0
2	y_2z_2	$-x_2^3+y_2^3+z_2^3$	37	$y_2/\boldsymbol{K}$, y_0
3	x_1y_1	$x_1^3+y_1^3-z_1^3$	79	y_1
4	$x_0y_0=x_2y_2$	$x_0^3+y_0^3-z_0^3$	2749	$\boldsymbol{K}x_2$, y_0

Equations (2-a) have been used in forming the second column. By noting that $y_0=(\mu/\boldsymbol{K})(\boldsymbol{K}b)$ and $y_2z_2=(\mu/\boldsymbol{K})a(\boldsymbol{K}\nu c_1)$, we see from (3) and (60) that the entries in this column are integral. Those in the third column are likewise all integers. This is already clear in the case of B_1 and B_4, while from equations (2-b) we obtain

$$
(61)\qquad \begin{cases} B_2 = B_4+2y_2^3 \\ B_3 = B_1+2x_1^3 \end{cases}
$$

(where y_2 and x_1 are integers). The last column of the table lists multiples of l_i for each value of i, as can be checked using (3) and (60). A comparison with the second column yields in particular the result

$$A_i \equiv 0 \pmod{l_i}, \qquad 1 \leqslant i \leqslant 4,$$

needed for (iii) of the Proposition. We proceed to a systematic examination of the other requirements for the isomorphism (1).

Greatest common divisors

(a) $$(A_1, B_1) = 1 = (A_4, B_4).$$

These conditions take the form

$$(x_0 z_0, x_0^3 - y_0^3 + z_0^3) = 1 = (x_0 y_0, x_0^3 + y_0^3 - z_0^3),$$

so are equivalent to

$$(x_0, y_0^3 - z_0^3) = (y_0, x_0^3 - z_0^3) = (z_0, x_0^3 - y_0^3) = 1.$$

It will be enough to show that $(3, y_0^3 - z_0^3) = 1$ (which is clearly satisfied), together with

$$(x_0/3^4, \boldsymbol{U}^3(y_0^3 - z_0^3)) = (y_0, \boldsymbol{L}^3(x_0^3 - z_0^3)) = (z_0, \boldsymbol{L}^3(x_0^3 - y_0^3)) = 1.$$

By (37-a) (i),

$$\begin{cases} \boldsymbol{U} y_0 \equiv -\boldsymbol{N} z_0 \pmod{x_0/3^4} \\ \boldsymbol{L} x_0 \equiv \boldsymbol{N} z_0 \pmod{y_0} \\ \boldsymbol{L} x_0 \equiv \boldsymbol{U} y_0 \pmod{z_0}. \end{cases}$$

The conditions above therefore reduce to

$$(x_0/3^4, (\boldsymbol{N}^3 + \boldsymbol{U}^3) z_0) = (y_0, (\boldsymbol{L}^3 - \boldsymbol{N}^3) z_0) = (z_0, (\boldsymbol{L}^3 - \boldsymbol{U}^3) y_0) = 1.$$

By (3) and (60) however,

(62) $$\begin{cases} x_0 = 2^9 \cdot 3^4 \cdot 5^2 \cdot 11 \cdot 719 \cdot 971 \cdot 23531 \\ y_0 = 2 \cdot 11 \cdot 37 \cdot 2749 \cdot 2837 \cdot 3203 \cdot 3413 \\ z_0 = 3^4 \cdot 6\ 801\ 023 \cdot 378\ 088\ 327 \end{cases}$$

where the factorizations are complete ($c/3^4$ being within the limits of the table of Lehmer [7]). Hence

(63) $$(x_0/3^4, z_0) = 1 = (y_0, z_0)$$

and it requires only to be shown that

$$(x_0, \boldsymbol{N}^3 + \boldsymbol{U}^3) = (y_0, \boldsymbol{L}^3 - \boldsymbol{N}^3) = (z_0, \boldsymbol{L}^3 - \boldsymbol{U}^3) = 1.$$

From (42),

$$\boldsymbol{N}^3 + \boldsymbol{U}^3 = \boldsymbol{K}(\boldsymbol{L} + \boldsymbol{W})(\boldsymbol{N} + \boldsymbol{U}) = 7 \cdot 103 \cdot 487 \cdot 1063,$$

which is prime to x_0. And

(64-a) $$\boldsymbol{L}^3-\boldsymbol{N}^3=(\boldsymbol{L}-\boldsymbol{N})(\boldsymbol{L}^2+(\boldsymbol{L}+\boldsymbol{N})\boldsymbol{N})=3^6\cdot 19441\,,$$

prime to y_0, while

$$\begin{aligned}\boldsymbol{U}^3-\boldsymbol{L}^3&=(3^9-1)(3^9+1)\\&=(3^3-1)(3^6+3^3+1)(3^3+1)((3^3+1)^2-3^4)\end{aligned}$$

or

(64-b) $$\boldsymbol{U}^3-\boldsymbol{L}^3=2^3\cdot 7\cdot 13\cdot 19\cdot 37\cdot 757\,,$$

which is plainly prime to z_0.

(b) $$(A_3,\,B_3)=1\,.$$

This requires $(x_1,\,B_3)=1=(y_1,\,B_3)$, the first part of which is immediate from (61) (ii) together with $(A_1,\,B_1)=1$. We are left to show

$$(y_1,\,x_1^3-z_1^3)=1\,,$$

and this will follow from

$$(y_1,\,\boldsymbol{LM}(x_1-z_1)^2)=1=(y_1,\,\boldsymbol{LM}(x_1^2+x_1z_1+z_1^2))\,.$$

By (39-a) however,

$$\boldsymbol{LM}(x_1+z_1)^2\equiv\boldsymbol{N}^2x_1z_1\ (\mathrm{mod}\ y_1)\,,$$

so that these conditions can be replaced with

(65) $$\begin{cases}(y_1,\,\boldsymbol{N}^2-4\boldsymbol{LM})=(y_1,\,\boldsymbol{N}^2-\boldsymbol{LM})=1\\(x_1z_1,\,y_1)=1\,.\end{cases}$$

For (65) (i) we have

(66) $$\begin{cases}\boldsymbol{N}^2-\boldsymbol{LM}=3\phi\boldsymbol{W}=2^4\cdot 3^6\cdot 5\\\boldsymbol{N}^2-4\boldsymbol{LM}=3\phi\boldsymbol{W}-3\boldsymbol{LM}=2^2\cdot 3\cdot 4799\,,\end{cases}$$

while by (2-a) (i), equation (65) (ii) can be written as

(67) $$(x_0,\,y_1)=1=(z_0,\,y_1)\,.$$

To confirm (67), we note that the ideal $(x_0,\,y_1)$ must contain

$$(3\phi x_0-\boldsymbol{N}y_1,\,\boldsymbol{M}x_0+\boldsymbol{U}y_1)=(\boldsymbol{L}y_0,\,\boldsymbol{L}z_0)\,,$$

by (36-a) (i) and (37-a) (ii). Similarly, $(z_0,\,y_1)$ will include

$$(3\phi z_0-\boldsymbol{L}y_1,\,z_0)=(\boldsymbol{M}y_0,\,z_0)\,,$$

by (36-a) (ii). Since $\boldsymbol{L}=1=(\boldsymbol{M}, z_0)$, the latter part of (63) supplies what is needed.

(c) $$(A_2, B_2) = 1 .$$

It is to be noted that whereas x_2 and z_2 are non-integral, all three of $\boldsymbol{K}x_2$, $y_2/\boldsymbol{K}$, $\boldsymbol{K}z_2$ are integers. We have $A_2=(y_2/\boldsymbol{K})(\boldsymbol{K}z_2)$ and so must show that

$$(y_2/\boldsymbol{K}, B_2) = 1 = (\boldsymbol{K}z_2, B_2) .$$

Now $$(x_2y_2, B_4) = (A_4, B_4) = 1$$

by (a) above. The former requirement is thus a consequence of (61) (i). The latter one will follow from

$$(\boldsymbol{K}z_2, (\boldsymbol{K}x_2)^3-(\boldsymbol{K}y_2)^3) = 1 .$$

But by (53),

$$\boldsymbol{L}(3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W})(\boldsymbol{K}x_2+\boldsymbol{K}y_2)^2\equiv\boldsymbol{K}\boldsymbol{U}^2(\boldsymbol{K}x_2)(\boldsymbol{K}y_2) \qquad (\mathrm{mod}\ \boldsymbol{K}z_2) .$$

It will be sufficient to check that

$$\begin{cases} (\boldsymbol{K}z_2, \boldsymbol{L}(3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W})(\boldsymbol{K}x_2-\boldsymbol{K}y_2)^2) = 1 \\ (\boldsymbol{K}z_2, \boldsymbol{L}(3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W})((\boldsymbol{K}x_2)^2+(\boldsymbol{K}x_2)(\boldsymbol{K}y_2)+(\boldsymbol{K}y_2)^2)) = 1 \end{cases}$$

and therefore that

(68) $$\begin{cases} (\boldsymbol{K}z_2, (\boldsymbol{K}x_2)y_2) = 1 \\ (\boldsymbol{K}z_2, \boldsymbol{K}\boldsymbol{U}^2-4\boldsymbol{L}(3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W})) = 1 \\ (\boldsymbol{K}z_2, \boldsymbol{K}\boldsymbol{U}^2-\boldsymbol{L}(3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W})) = 1 . \end{cases}$$

We have

$$\begin{aligned} \boldsymbol{K}\boldsymbol{U}^2-\boldsymbol{L}(3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W}) &= (\boldsymbol{K}\boldsymbol{V}+\boldsymbol{L}\boldsymbol{N})\boldsymbol{W} \\ &= \frac{\boldsymbol{L}^3-\boldsymbol{U}^3}{\boldsymbol{M}-\boldsymbol{V}}\boldsymbol{W}, \end{aligned}$$

by (42) and (13). So by (59) and (64-b), equation (68) (iii) reduces simply to

$$(\boldsymbol{K}z_2, 2^6\cdot3^2\cdot5\cdot7\cdot37\cdot757) = 1 .$$

Again, in (68) (ii),

$$\begin{aligned} \boldsymbol{K}\boldsymbol{U}^2-4\boldsymbol{L}(3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W}) &= 4\boldsymbol{W}(\boldsymbol{L}^3-\boldsymbol{U}^3)/(\boldsymbol{M}-\boldsymbol{V})-3\boldsymbol{K}\boldsymbol{U}^2 \\ &= 3^2\cdot62\ 653\ 379 \end{aligned}$$

(the larger factor being actually prime).

To handle (68) (i), since z_2 is non-integral it is enough to see that

$$(\boldsymbol{K}z_2, (\boldsymbol{K}x_2)(y_2/\boldsymbol{K})) = 1$$

and hence by (2-a) (ii) that

$$(\boldsymbol{K}z_2, x_0) = 1 = (\boldsymbol{L}(\boldsymbol{K}z_2), y_0) .$$

From (52) we have

$$\boldsymbol{K}z_2 = \boldsymbol{W}x_0 - \boldsymbol{K}y_1 .$$

Our first condition then follows readily from (62) (i) and (67). For the second, note that by (51)

$$\boldsymbol{L}(\boldsymbol{K}z_2) = \boldsymbol{JK}y_0 - (3\phi\boldsymbol{K} - \boldsymbol{NW})z_0$$

and we need only check that

$$(y_0, (3\phi\boldsymbol{K} - \boldsymbol{NW})z_0) = 1 .$$

However,

$$3\phi\boldsymbol{K} - \boldsymbol{NW} = 3^2 \cdot 28927 ,$$

and the result follows by (62) (ii) and (63).

The discriminant

The truth of $D<0$ can be confirmed from (5) and (62) with the aid of a table of logarithms.

To see that the discriminant d of $\boldsymbol{Q}(\sqrt{D})$ satisfies $d<-4$, note that $D=C^2d$ where C is an integer. It is thus sufficient to check

$$(D, 6) = 1 .$$

This is easily achieved, since from (62)

$$\begin{cases} x_0 \equiv y_0 \equiv z_0 - 1 \equiv 0 \pmod 2 \\ x_0 \equiv z_0 \equiv y_0 + 1 \equiv 0 \pmod 3 , \end{cases}$$

giving by (5)

$$D \equiv 1 \pmod 3 \text{ and } \pmod 4 .$$

Non-cubic residues

It must next be shown that for $1 \leqslant i \leqslant 4$,

$$B_i \not\equiv \text{cube} \pmod{l_i} .$$

The techniques of the preceding section apply. Thus

$$\begin{cases} \boldsymbol{L}^3 B_1 \equiv (\boldsymbol{U}^3 - \boldsymbol{L}^3) y_0^3 \pmod{z_0} \\ \boldsymbol{L}^3 B_4 \equiv -(\boldsymbol{L}^3 - \boldsymbol{N}^3) z_0^3 \pmod{y_0} \\ (\boldsymbol{LM})^3 B_3^2 \equiv (\boldsymbol{N}^2 - 4\boldsymbol{LM})(\boldsymbol{N}^2 - \boldsymbol{LM})^2 (x_1 z_1)^3 \pmod{y_1} \end{cases}$$

while from (61) (i),

$$B_2 \equiv B_4 \pmod{y_2}.$$

(See also the last column of the table.) Taken in conjunction with (63) and (65) (ii), the following conditions will therefore furnish our requirements:

$$\begin{cases} U^3 - L^3 \not\equiv \text{cube} \pmod{\nu} \\ L^3 - N^3 \not\equiv \text{cube} \pmod{37} \text{ and } \pmod{2749} \\ (N^2 - 4LM)(N^2 - LM)^2 \not\equiv \text{cube} \pmod{79}. \end{cases}$$

These, in turn, reduce to the conditions

$$\text{(69-a)} \qquad 73 \text{ and } 757 \equiv \text{cubes} \pmod{\nu},$$

$$\text{(69-b)} \qquad \begin{cases} 11 \text{ and } 17 \equiv \text{cubes} \pmod{\nu} \\ 5 \not\equiv \text{cube} \pmod{\nu} \\ 2 \not\equiv \text{cube} \pmod{37} \\ 3 \not\equiv \text{cube} \pmod{79} \text{ and } \pmod{2749}. \end{cases}$$

Indeed, the reader may check that

$$\begin{aligned} 2^3 \cdot 5(7 \cdot 11 \cdot 13)(17 \cdot 19)37 &= 40 \cdot 1001 \cdot 323\ (111/3) \\ &= \nu + 100\ 429\ 713. \end{aligned}$$

Multiplying by 8×8 and reducing, we obtain

$$2^6 \cdot 5(11 \cdot 17)(2^3 \cdot 7 \cdot 13 \cdot 19 \cdot 37) \equiv 73 \pmod{\nu}$$

hence by (64-b),

$$2^6 \cdot 5(11 \cdot 17)(U^3 - L^3) \equiv 73 \cdot 757 \pmod{\nu}.$$

Again,

$$19441 \equiv \begin{cases} 2^4 \pmod{37} \\ 2 \cdot 3^2 \cdot 11 \pmod{2 \cdot 5^3 \cdot 11 - 1} \end{cases}$$

so from (64-a),

$$\begin{aligned} L^3 - N^3 &\equiv 2(2 \cdot 3^2)^3 \pmod{37}, \\ 5^3(L^3 - N^3) &\equiv 3^8 \pmod{2749}. \end{aligned}$$

Lastly,

$$4799 \equiv -2^2 \cdot 5 \pmod{79}$$

and (66) gives

$$(N^2 - 4LM)(N^2 - LM)^2 \equiv -3(2^4 \cdot 3^4 \cdot 5)^3 \pmod{79}.$$

To avoid repetition, we shall postpone checking (69) until the end of the next section.

Trace conditions

Concerning (iv) of the Proposition, we have by equations (2-b) and the table,

$$\begin{cases} \frac{1}{2}(B_1+B_2) = x_0^3+y_2^3 \equiv x_0^3 \pmod{l_2} \\ \frac{1}{2}(B_1+B_3) = y_1^3-z_1^3 \equiv -z_1^3 \pmod{l_3} \\ \frac{1}{2}(B_2+B_3) = x_0^3+x_1^3+y_2^3 \\ \frac{1}{2}(B_1+B_4) = x_0^3 \\ \frac{1}{2}\boldsymbol{K}^3(B_2+B_4) = -(\boldsymbol{K}x_2)^3+(\boldsymbol{K}z_2)^3 \equiv (\boldsymbol{K}z_2)^3 \pmod{l_4} \\ \frac{1}{2}(B_3+B_4) = x_0^3+x_1^3 . \end{cases}$$

Since

$$(x_0,\ l_2l_4) = (z_1,\ l_3) = (\boldsymbol{K}z_2,\ l_4) = 1 ,$$

it has only to be shown that

$$(70) \qquad \begin{cases} x_0^3+x_1^3+y_2^3 \equiv \text{non-zero cube} \pmod{l_3} \\ x_0^3+x_1^3 \equiv \text{non-zero cube} \pmod{l_4} . \end{cases}$$

From (60) we find

$$[\lambda,\ \mu,\ a,\ c] \equiv [-34,\ -1,\ 3,\ -16] \pmod{79} ,$$

giving

$$[x_0,\ x_1,\ y_2] \equiv [-23,\ -9,\ -3] \pmod{79} ,$$

so

$$2^3(x_0^3+x_1^3+y_2^3) \equiv 3^3 \pmod{79} .$$

This gives (70) (i). For (70) (ii), since $(\lambda,\ l_4)=1$, we must show

$$a^3+c^3 \equiv \text{non-zero cube} \pmod{2749} .$$

Now from (60),

$$[a,\ c] \equiv [-3^2\cdot 487,\ -3^5] \pmod{2749} .$$

Thence

$$a^3+c^3 \equiv 3^6\cdot 241 \pmod{2749} ,$$

or

$$2\cdot 7(a^3+c^3) \equiv 5(3^2\cdot 5)^3 \pmod{2749} ,$$

and the desired conclusion will follow from

$$(71) \qquad 2 \text{ and } 5 \text{ and } 7 \equiv \text{cubes} \pmod{2749} .$$

The verification of (69-b) and (71) is immediate from the product criterion of Note D, applied to the decompositions

$$\begin{cases} 4\nu = (17\cdot 2207)^2+27(11\cdot 179)^2 \\ 4\cdot 37 = 11^2+27\cdot 1^2 \\ 4\cdot 79 = 17^2+27\cdot 1^2 \\ 2749 = 7^2+27(2\cdot 5)^2 . \end{cases}$$

Conditions (69-a) meanwhile, are a consequence of the following factorizations of the reduced period equation (see Note D):

$$\tau^3-\nu(3\tau+17\cdot 2207) \equiv \begin{cases} (\tau+5)(\tau+15)(\tau-20) \pmod{73} \\ (\tau-10)(\tau-46)(\tau+56) \pmod{757} . \end{cases}$$

This completes the checking of (i)-(iv) of the Proposition. We may thus conclude that for the field $\boldsymbol{Q}(\sqrt{D})$ here considered, the ideal class group has a subgroup isomorphic with $\boldsymbol{C}(3)^4$.

8. An infinite collection

To obtain further imaginary quadratic fields with 3-rank four (at least), we take in place of (58)

$$[\alpha, \beta, \gamma] = [0, t, -t] .$$

By (9-a), $\phi=3t^2$, and so in (17)

$$\begin{bmatrix} \boldsymbol{L} & \boldsymbol{U} \\ \boldsymbol{M} & \boldsymbol{V} \\ \boldsymbol{N} & \boldsymbol{W} \end{bmatrix} = \begin{bmatrix} 1 & 9t^4 \\ 1+9t^3 & 3t(3t^3+1) \\ 1-9t^3 & 3t(3t^3-1) \end{bmatrix} . \tag{72}$$

Write $D(t)$ for the value of D produced by (5), (57), (72). Depending on context, t will denote an indeterminate, a real variable, or a positive integer. In the last case, define $d(t)$ as the discriminant of the field $\boldsymbol{Q}(\sqrt{D(t)})$. The Theorem of the Introduction will be proved by showing in turn that

(a) $d(t) \to -\infty$ as $t \to \infty$;

(b) For infinitely many positive integers t, the isomorphism (1) is valid.

The polynomial $D(t)$

Formulae (72) yield

$$\boldsymbol{L}, \boldsymbol{M}, \boldsymbol{N} \equiv 1; \quad \boldsymbol{U}, \boldsymbol{V}, \boldsymbol{W} \equiv 0 \pmod{t} .$$

In (57) therefore, we have $\boldsymbol{K} \equiv 1 \pmod{t}$ and

$$\lambda, a, c \equiv 0; \quad \mu/\boldsymbol{K}, -\boldsymbol{K}b, \nu \equiv 1 \pmod{t} . \tag{73}$$

Thus

$$(x_0, y_0, z_0) \equiv (0, -1, 0) \pmod{t}. \tag{74}$$

Again, from (72) it is easy to calculate

$$-\lambda, \nu = 3^6 t^{12} + O(t^9) \quad \text{and} \quad -a, c = 3^6 t^{12} + 3^6 t^{11} + O(t^{10}),$$

so that with the help of (37-a) (i) we obtain

$$\begin{cases} x_0, z_0 = 3^{12} t^{24} + 3^{12} t^{23} + O(t^{22}) \\ \quad y_0 = \qquad\quad 3^{12} t^{23} + O(t^{22}). \end{cases} \tag{75}$$

Combining (74) and (75) with (5) shows $D(t)$ to be a polynomial of the form

$$D(t) = 1 + \cdots - 4 \cdot 3^{72} t^{141}.$$

We see from this equation that $D(t) \to -\infty$ as $t \to \infty$. Condition (a) will follow immediately by Siegel's Theorem [14] once it is determined that three or more roots of $D(t)$ are simple. Since $D(t)$ is of odd degree however, we have only to show it has no rational root.

Such a root would be of the form

$$t = \pm 2^{-m} 3^{-n}, \quad 0 \leqslant m \leqslant 2, \ 0 \leqslant n \leqslant 72.$$

Now by (5), $D(t) > 0$ if $\lambda a \mu b < 0$. We use this fact to construct an interval about $t=0$ within which $D(t) \neq 0$. Indeed, from (35-a) (iii) and (57),

$$-\lambda a \mu b = \boldsymbol{L} \boldsymbol{W}^2 (\boldsymbol{L} - \boldsymbol{W})(\boldsymbol{N} - \boldsymbol{U})(2\boldsymbol{L}^2 - \boldsymbol{L}\boldsymbol{W} + \boldsymbol{W}^2)(\boldsymbol{L}\lambda^2 - \boldsymbol{M}\lambda\nu + \boldsymbol{N}\nu^2).$$

The last factor on the right is a quadratic from and will agree in sign with $\boldsymbol{L}$ when the discriminant is negative. We are thus reduced to the problem of marking off a neighborhood of $t=0$ within which

$$\begin{cases} \boldsymbol{M}^2 - 4\boldsymbol{L}\boldsymbol{N} = 3\phi \boldsymbol{V} - 3\boldsymbol{L}\boldsymbol{N} \\ \qquad\qquad = 3(-1 + 18t^3 + 27t^6) < 0 \\ \boldsymbol{L} - \boldsymbol{W} = 1 + 3t - 9t^4 > 0 \\ \boldsymbol{N} - \boldsymbol{U} = 1 - 9t^3 - 9t^4 > 0. \end{cases}$$

By Descartes' Rule of Signs, none of these three polynomials can have more than one real root of either sign. We find that $\phi \boldsymbol{V} - \boldsymbol{L}\boldsymbol{N}$ changes sign in the intervals $\left(-1, -\frac{1}{2}\right)$, $\left(\frac{1}{3}, \frac{1}{2}\right)$ and that $\boldsymbol{L} - \boldsymbol{W}$, $\boldsymbol{N} - \boldsymbol{U}$ change sign in $\left(-\frac{1}{3}, -\frac{1}{4}\right)$, $\left(\frac{1}{2}, 1\right)$ and $(-2, -1)$, $\left(\frac{1}{3}, \frac{1}{2}\right)$ respectively. Thus each polynomial has exactly one positive and one negative root. Moreover, the

inequalities above will hold simultaneously for $-\frac{1}{4} \leqslant t \leqslant \frac{1}{3}$.

The work can be completed by checking that $D(t) \neq 0$ for $t = \pm 1, \pm\frac{1}{2}, -\frac{1}{3}$. Except when $t=1$, it is found that $\lambda avc < 0$, while a more elaborate calculation with logarithms yields $D(1) > 0$.

Congruences

The table of Part 7 is used without modification for relating the Proposition to the field $\boldsymbol{Q}(\sqrt{D(t)})$. The arguments which before showed the second and third columns to contain integers, apply to show these entries lie now in $\boldsymbol{Z}[t]$, and they will be denoted as $A_i(t)$ and $B_i(t)$. We shall demonstrate condition (*b*) under the *Assumption:* For $1 \leqslant i \leqslant 4$, the polynomials $A_i(t)$, $B_i(t)$ are relatively prime in $\boldsymbol{Q}[t]$.

Set

$$T = l_1 l_2 l_3 l_4 R_1 R_2 R_3 R_4$$

where l_i is the same as in column 4 of the table and R_i is the *resultant* of $A_i(t)$ and $B_i(t)$ in $\boldsymbol{Z}[t]$. By assumption, R_i is a non-zero rational integer. Next, let t be an integer satisfying

$$t \equiv 3 \pmod{T}. \tag{76}$$

Then (i), (iii) and (iv) of the Proposition are fulfilled in the case of $\boldsymbol{Q}(\sqrt{D(t)})$.

In fact, (76) gives

$$A_i(t) \equiv A_i(3), \quad B_i(t) \equiv B_i(3) \pmod{T}. \tag{77}$$

Since $T \equiv 0 \pmod{l_i}$, conditions (iii) and (iv) follow easily from the results of Part 7. To obtain (i) we observe that (77) combined with Part 7 yields

$$(A_i(t), B_i(t)) \equiv 1 \pmod{T},$$

where the left member also divides T, since it divides R_i.

From condition (*a*) proved above, we shall certainly have $d(t) < -4$ if t is positive and sufficiently large, which supplies the remaining requirement (ii) of the Proposition. The fields $\boldsymbol{Q}(\sqrt{D(t)})$ formed in this way are thus imaginary quadratic fields of 3-rank at least four, and they constitute a set of infinite cardinality.

Polynomial common divisors

Our final task is therefore to justify the *Assumption* made above, and by the reductions performed in the course of Part 7, it will be enough to show that the following pairs of polynomials are coprime.

(a) For $i=1$ and 4:

$$\begin{cases} (t,\ y_0^3-z_0^3),\ (x_0/t^2,\ z_0),\ (y_0,\ z_0) \\ (x_0,\ \boldsymbol{N}^3+\boldsymbol{U}^3),\ (y_0,\ \boldsymbol{L}^3-\boldsymbol{N}^3),\ (z_0,\ \boldsymbol{L}^3-\boldsymbol{U}^3)\,. \end{cases}$$

(b) Additionally, for $i=3$:

$$(y_1,\ 3\phi\boldsymbol{W}),\ (y_1,\ \boldsymbol{N}^2-4\boldsymbol{L}\boldsymbol{M}),\ (\boldsymbol{M},\ z_0)\,.$$

(c) Additionally, for $i=2$:

$$\begin{cases} (\boldsymbol{K}z_2,\ \boldsymbol{W}(\boldsymbol{L}^3-\boldsymbol{U}^3)/(\boldsymbol{M}-\boldsymbol{V})) \\ (\boldsymbol{K}z_2,\ 4\boldsymbol{W}(\boldsymbol{L}^3-\boldsymbol{U}^3)/(\boldsymbol{M}-\boldsymbol{V})-3\boldsymbol{K}\boldsymbol{U}^2) \\ (y_0,\ 3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W})\,. \end{cases}$$

A combination of two different techniques will be employed.

(i) If two polynomials with odd leading coefficients are not coprime, they will have a common factor of positive degree after reduction modulo 2. The algebra needed for computing the reduced forms of the polynomials from formulae (57) can be minimized by representing polynomials modulo 2 as strings of binary digits, in the obvious fashion. We require also a table of irreducible polynomials (mod 2), such as the one given in [1, Appendix IV].

By (72),

$$\begin{bmatrix} \boldsymbol{L} & \boldsymbol{U} \\ \boldsymbol{M} & \boldsymbol{V} \\ \boldsymbol{N} & \boldsymbol{W} \end{bmatrix} \equiv \begin{bmatrix} 1 & t^4 \\ 1+t^3 & t(1+t^3) \\ 1+t^3 & t(1+t^3) \end{bmatrix} \pmod 2\,,$$

so from (57) we obtain (congruences being modulo 2)

$$(78)\qquad \begin{cases} \boldsymbol{K}\equiv 1+t+t^2+t^3+t^4 \\ \lambda\equiv t^2(1+t)^2(1+t+t^2)^2(1+t+t^4) \\ \mu/\boldsymbol{K}\equiv(1+t^2+t^3)(1+t+t^4) \\ \nu\equiv(1+t+t^4)(1+t^3+t^4+t^5+t^8) \\ a\equiv t(1+t)(1+t+t^2)(1+t+t^4)(1+t^3+t^4) \\ \boldsymbol{K}b\equiv(1+t)(1+t+t^2)(1+t+t^4)(1+t^3+t^4+t^7+t^9) \\ c\equiv t^3(1+t+t^4)(1+t+t^3+t^4+t^5) \\ \boldsymbol{K}\nu c_1\equiv(1+t^2+t^3)(1+t+t^4)^2(1+t+t^2+t^4+t^6+t^7+t^8)(1+t^4+t^9)\,. \end{cases}$$

All factorizations shown are complete. The value of μb_1 will not be needed and is omitted. From (37-a) (ii) however, we see

$$y_1 = -3^{12}t^{23}+O(t^{22})\,,$$

whence by (52)

$$\boldsymbol{K}z_2 = 3^{14}t^{28}+O(t^{27}).$$

Consequently, there is no loss of degree due to reduction in the last congruence of (78). The same holds for all the others, as follows immediately from (75).
(ii) Let ord denote the 3-adic exponential valuation of $\boldsymbol{Q}$, and also its unique extension to the algebraic closure $\bar{\boldsymbol{Q}}_3$ of the 3-adic completion $\boldsymbol{Q}_3$. (N.B. $\mathrm{ord}(0)=\infty$.) The 3-adic Newton polygon for

$$f(t) = \sum a_i t^i \in \boldsymbol{Z}[t]$$

is the lower convex envelope of the points $(i, \mathrm{ord}(a_i))$ (see [15, Ch. 3]). Since the side-slopes for the polygon give the values of ord at the roots, polynomials $f(t)$, $g(t)$ generating disjoint sets of slopes can have no common root in $\bar{\boldsymbol{Q}}_3$ and must be coprime. (Notationally, $(f(t), g(t))=1$. There will be no confusion, since t always stands for an indeterminate in what follows.)

From (57) and (72) we find

$$(79)\quad \begin{cases} -\lambda/\boldsymbol{W} = 2+3t+3^2t^2-3^2t^4-2\cdot 3^3t^5+3^4t^8 \quad \left(\text{Slope: } \dfrac{1}{2}\right) \\ -\lambda/\boldsymbol{W}-a/\boldsymbol{L}\boldsymbol{W} = 3(1+2t+3t^2-3t^3-2\cdot 3^2t^4-3^3t^5+3^3t^7+2\cdot 3^3t^8) \\ \qquad\qquad \left(\text{Slopes: } 0, \dfrac{3}{7}\right) \\ \mu/\boldsymbol{K} = 1-3t+3^2t^2-2\cdot 3^2t^3+3^4t^6-3^4t^7 \quad \left(\text{Slope: } \dfrac{4}{7}\right) \\ 3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W} = 3t(1+3t+3^2t^2+3\cdot 5t^3+3^3t^4+3^3t^5+3^3t^6) \\ \qquad\qquad \left(\text{Slopes: } \infty, \dfrac{1}{3}, \dfrac{2}{3}\right). \end{cases}$$

These preparations completed, we proceed to investigate conditions (a), (b), (c) above. (see also the remarks following (57).)
(a) The truth of $(t, y_0^3 - z_0^3)=1$ is apparent from (74). Also,

$$(80)\qquad (-\lambda/\boldsymbol{W}, -a/\boldsymbol{L}\boldsymbol{W}) = 1,$$

by application of the 3-adic argument to the first two members in (79). In view of (35-a) (i), this leads to $(-\lambda/\boldsymbol{W}, \nu)=1$. From (57) (iv) it is easily seen that

$$(81)\qquad (\boldsymbol{W}, \nu) = 1$$

and we obtain $(\lambda, \nu)=1$. This can be strengthened to read

$$(\lambda a, \nu) = 1,$$

by use of (35-a) (i) again. On the other hand, since

$$(\lambda/3t,\ \nu \boldsymbol{U}) = 1\,,$$

equation (35-a) (ii) gives

$$(\lambda/3t,\ c) = 1\,.$$

The desired conclusion

$$((3t)^{-2}x_0,\ z_0) = 1 \tag{82}$$

will be obtained once it is shown that

$$(a/3t,\ c) = 1\,.$$

Now $(-a/\boldsymbol{L}\boldsymbol{W},\ 3\phi)=1$, hence

$$(a/\boldsymbol{W},\ c) = 1$$

by (57) (vii) and (80). And

$$(\boldsymbol{W}/3t,\ c) = 1$$

by (81), since from (35-a) (ii)

$$c \equiv \nu \boldsymbol{U} \pmod{\lambda} \text{ and therefore } \pmod{\boldsymbol{W}}\,.$$

The result follows on multiplying the last two equations.

From (57) it can be seen that t^2 is the highest power of t dividing c, and therefore also z_0, by (73). Thus (82) yields

$$(x_0,\ (3t)^{-2}z_0) = 1$$

and by (37-a) (i) we get

$$(\boldsymbol{U}y_0,\ (3t)^{-2}z_0) = 1\,.$$

Hence by (74),

$$(y_0,\ z_0) = 1\,.$$

To show $(\lambda a,\ \boldsymbol{N}^3+\boldsymbol{U}^3)=1$, we check that

$$(\lambda,\ \boldsymbol{L}^3+\boldsymbol{W}^3) = 1 = (a,\ \boldsymbol{K}(\boldsymbol{L}+\boldsymbol{W})(\boldsymbol{N}+\boldsymbol{U}))$$

(see (42)). However, from (57), $\lambda \equiv 4\boldsymbol{L}^3 \pmod{(\boldsymbol{L}+\boldsymbol{W})}$ so $(\lambda,\ \boldsymbol{L}+\boldsymbol{W})=1$, while

$$(\boldsymbol{W},\ \boldsymbol{L}^2-\boldsymbol{L}\boldsymbol{W}+\boldsymbol{W}^2) = 1 = (2\boldsymbol{L}^2-\boldsymbol{L}\boldsymbol{W}+\boldsymbol{W}^2,\ \boldsymbol{L}^2-\boldsymbol{L}\boldsymbol{W}+\boldsymbol{W}^2)\,,$$

where the first term in the right member equals $(-\lambda/\boldsymbol{W})$. This gives the former requirement. For the latter, note

$$\begin{cases} a = 3t(1-3t^3)(1+3t-9t^4)(1-9t^3-9t^4) \\ \boldsymbol{K}(\boldsymbol{L}+\boldsymbol{W})(\boldsymbol{N}+\boldsymbol{U}) = (1+3t+9t^2+9t^3+9t^4)(1-3t+9t^4)(1-9t^3+9t^4)\,. \end{cases}$$

All five quartic factors appearing are irreducible, being irreducible (mod 2). Since they are all distinct, the result is immediate.

In order to prove

$$((\mu/\boldsymbol{K})(\boldsymbol{K}b),\ \boldsymbol{L}^3-\boldsymbol{N}^3)=1\,,$$

we note that

$$\boldsymbol{L}^3-\boldsymbol{N}^3=3\phi(\boldsymbol{L}\boldsymbol{U}-\boldsymbol{N}\boldsymbol{W})=(3t)^3(1-3^2t^3+3^3t^6)\,.$$

The Newton polygon for the second factor (which is a factor of $1+3^9t^{18}$) has a single side of slope $\frac{1}{2}$. By (79) (iii), this sextic must be prime to $\mu/\boldsymbol{K}$. And as reduction produces $1+t^3+t^6$, which is irreducible (mod 2), its coprimality with $\boldsymbol{K}b$ is a consequence of (78) (vi).

Lastly, we must show

$$(\nu c,\ \boldsymbol{L}^3-\boldsymbol{U}^3)=1\,.$$

But this follows at once from (78). For

$$1+t^{12}\equiv(1+t^3)^4 \qquad (\mathrm{mod}\ 2)$$

which gives

$$\boldsymbol{L}^3-\boldsymbol{U}^3\equiv(1+t)^4(1+t+t^2)^4 \qquad (\mathrm{mod}\ 2)\,. \tag{83}$$

(b) To verify

$$(y_1,\ 3\phi\boldsymbol{W})=1\,,$$

we need only show $(y_1,\ \boldsymbol{W})=1$. However, as

$$y_1\equiv\nu^2 \qquad (\mathrm{mod}\ \lambda)$$

by (35-a) (iv), this is a consequence of (81).

Again, seeing that $\boldsymbol{N}^2-4\boldsymbol{L}\boldsymbol{M}$ has the same degree as $\boldsymbol{N}^2$, the condition

$$(y_1,\ \boldsymbol{N}^2-4\boldsymbol{L}\boldsymbol{M})=1$$

requires only the coprimality of y_1, $\boldsymbol{N}$ (mod 2). Now

$$\boldsymbol{M}\equiv\boldsymbol{N}\equiv1+t^3 \qquad (\mathrm{mod}\ 2)\,,$$

whereas with congruences modulo the ideal $(2,\ 1+t^3)$ of $\boldsymbol{Z}[t]$, we have in (78)

$$\begin{cases} \nu\equiv(1+t(1+t^3))((1+t^3)+t^4+t^5(1+t^3))\equiv t \\ c\equiv t^3(1+t(1+t^3))((1+t)(1+t^3)+t^5)\equiv t^2 \end{cases}$$

hence $\nu c\equiv1$. By (36-a) (ii) therefore, $y_1\equiv3\phi\equiv t^2$, which gives the result sought. The last condition

$$(\boldsymbol{M}, z_0) = 1$$

is easy from (78).

(c) We have

$$\boldsymbol{M}-\boldsymbol{V} \equiv (1+t)^2(1+t+t^2) \qquad (\mathrm{mod}\ 2)\,,$$

so by (83)

$$\boldsymbol{W}\frac{\boldsymbol{L}^3-\boldsymbol{U}^3}{\boldsymbol{M}-\boldsymbol{V}} \equiv t(1+t)^3(1+t+t^2)^4 \qquad (\mathrm{mod}\ 2)\,,$$

which is seen to be prime to $\boldsymbol{K}\nu c_1$ (mod 2) in (78). For showing $\boldsymbol{K}\nu c_1$ is prime to

$$4\boldsymbol{W}\frac{\boldsymbol{L}^3-\boldsymbol{U}^3}{\boldsymbol{M}-\boldsymbol{V}}-3\boldsymbol{K}\boldsymbol{U}^2\,,$$

we note that the terms in the latter expression are both of degree 12, so it is enough to check $\boldsymbol{K}\nu c_1$, $\boldsymbol{K}\boldsymbol{U}^2$ are coprime (mod 2). This is immediate from (78).

Regarding the sole remaining requirement

$$((\mu/\boldsymbol{K})(\boldsymbol{K}b),\ 3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W}) = 1\,,$$

we obtain from (79) the fact

$$(\mu/\boldsymbol{K},\ 3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W}) = 1\,.$$

And since

$$3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W} \equiv t(1+t+t^3)(1+t^2+t^3) \qquad (\mathrm{mod}\ 2)\,,$$

it follows from (78) we have also

$$(\boldsymbol{K}b,\ 3\phi\boldsymbol{K}-\boldsymbol{N}\boldsymbol{W}) = 1\,.$$

The correctness of the *Assumption* is thereby proved, and with it the Theorem.

Notes

A. An alternative derivation

For simplicity, set $\lambda=1=a$, so equations (4) assume the inhomogeneous form

$$\begin{cases} \mu^3(b^3+b_1^3) = (1+\nu^3)(1+c^3) \\ \nu^3(c^3+c_1^3) = (1+\mu^3)(1+b^3)\,. \end{cases}$$

Solutions of the system may be denoted by ordered tuples $[\mu, \nu, b, b_1, c, c_1]$. Each such solution gives rise to another, namely $[\nu, \mu, c, c_1, b, b_1]$, the effect of the corresponding linear transformation of the variables being to interchange

the two equations. Again, when μ, b, b_1 are replaced by b, μ, $\mu b_1/b$ respectively (ν, c, c_1 being held fixed), the equations are separately preserved. By incorporating the analogous alteration of ν, c, c_1 we derive from the original solution, $\mathcal{S}$ say, the solution $\mathcal{T}$ given by $[b, c, \mu, \mu b_1/b, \nu, \nu c_1/c]$.

The particular self-transformation of the system to which this corresponds is distinguished as follows. The resolution of (4) obtained in Part 4 resulted from the solution (33) of equation (27). The latter has other solutions, however. In fact, we may use (29) to write (27) (in its inhomogeneous form) as

$$(U'/W'+\mu)(L/W-E\nu+k\nu^2)+(U/W+\nu)(L'/W'-E'\mu+k\mu^2)=0\,,$$

where $E=(M-V)/W$ and $E'=(M'-V')/W'$. Note that by (14) (ii), we have

$$L+EU+kV=0\,. \tag{84}$$

Let

$$\mu+\nu=-k^*$$

where the value of k^* remains to be chosen (cf. (30)). Elimination of μ then yields the quadratic equation

$$\begin{aligned}[kk^*+k^2+E+E']\nu^2+[k^*(kk^*+E+E'+2kU/W)+E'U/W-EU'/W']\nu \\ +[(k-k^*)L/W+k^*(kk^*+E')U/W]=0\,.\end{aligned}$$

As we know, one way of solving this equation is to choose $k^*=k$. Another way takes advantage of the fact that the coefficient of ν^2 is linear in k^* and can be made to vanish. Thus on choosing

$$k^*=-k-\frac{1}{k}(E+E')\,,$$

ν will be determined by the linear equation

$$[kk^*(-k+2U/W)+E'U/W-EU'/W']\nu+[(k-k^*)L/W-k^*(k^2+E)U/W]=0\,.$$

From (28), the coefficient of ν may be written as

$$\begin{aligned}(U'/W'-U/W)(k^2+E+E')+E'U/W-EU'/W' \\ =(k^2+E')U'/W'-(k^2+E)U/W\,,\end{aligned}$$

and using (84)-(84′) to eliminate E, E' we can bring this to the simple form $k(L'/W'^2-L/W^2)$. For present purposes however, we write it instead as

$$k(k^2+E')-(2k^2+E+E')U/W\,.$$

Again, the constant term in the equation is

$$\begin{aligned} kL/W-k^*(L+EU)/W+k(k^2+E+E')U/W \\ &= (k-k^*)(L+EU)/W+k(k^2+E')U/W \\ &= -(2k^2+E+E')V/W+k(k^2+E')U/W\,, \end{aligned}$$

by (84). The value of ν is therefore given by the ratio

$$-\frac{(2k^2+E+E')V-k(k^2+E')U}{(2k^2+E+E')U-k(k^2+E')W}.$$

This however, is precisely the value assigned to c in (the inhomogeneous form of) (33)-(34). If $\mathcal{S}$ stand for the latter solution and $\mathcal{T}^*$ for the new one, we have therefore shown that

$$\nu(\mathcal{T}^*) = c(\mathcal{S})\,.$$

Now this implies that, additionally,

$$c(\mathcal{T}^*) = \nu(\mathcal{S})\,.$$

For the equation

$$c = -\frac{V+\nu U}{U+\nu W} = F(\nu) \text{ say}$$

(which is valid for both solutions), remains correct when the roles of ν and c are interchanged. Thus

$$c(\mathcal{T}^*) = F(\nu(\mathcal{T}^*)) = F(c(\mathcal{S})) = \nu(\mathcal{S})\,.$$

Moreover, by symmetry we have

$$\mu(\mathcal{T}^*) = b(\mathcal{S}), \quad b(\mathcal{T}^*) = \mu(\mathcal{S})\,.$$

The equations (4-a) and (4-b) themselves suffice to determine now the values of $b_1(\mathcal{T}^*)$ and $c_1(\mathcal{T}^*)$, and we see that $\mathcal{T}^*$ is none other than the solution $\mathcal{T}$ described earlier.

Finally, a glance at (5) shows the value of D will be the same for $\mathcal{T}$ (hence $\mathcal{T}^*$) as for $\mathcal{S}$. The two quite different techniques for solution of (27) lead accordingly to the same results.

B. Numerical values

Less factored forms of the larger numbers in (60) are

$$\begin{cases} \boldsymbol{K}b = -2\cdot 11\cdot 2\ 66176\ 90069 \\ \mu b_1 = -62\ 42453\ 21587\ 90031 \\ \boldsymbol{K}\nu c_1 = 2\ 01256\ 26027\ 96210\ 66953\,. \end{cases}$$

The labor of checking the work can be reduced as follows. Instead of recomputing $\boldsymbol{K}b$ from (57) (vi), let the equation be written as

$$\boldsymbol{Kb}+(\mu/\boldsymbol{K})\boldsymbol{K}^2\boldsymbol{N}=-\lambda(3\phi\boldsymbol{K}-\boldsymbol{LU}).$$

If the proposed value be used for $\boldsymbol{Kb}$, the left side will read

$$2\cdot 11(11\cdot 37\cdot 3203\cdot 1063^2-2\ 66176\ 90069).$$

Multiplication by 11 and 37 ($=111/3$) are easy. For the first term in parentheses we find the value 147 30513 17749. After performing the subtraction indicated, the result can be compared with the right side of the equation by trying the factors of λ given by (60) (ii). In this way, successive divisions (resulting in smaller numbers) take the place of repeated multiplication.

Similar remarks apply with greater force to the calculations for μb_1 and $\boldsymbol{K}\nu c_1$, the terms containing the factor λa in the last two formulae of (57) being the ones to isolate.

C. Primality of $\nu=378\ 088\ 327$

The known idoneal determinant -462 (see [6, §303]) divides

$$\nu-1=2\cdot 3^2\cdot 7\cdot 11\cdot 53\cdot 5147.$$

The eight reduced forms for this determinant are ax^2+cy^2 with $a<c$, $ac=462$. Only the principal form represents quadratic residues of 3, 7, 11 so we are to show there is just one decomposition (with x, y positive)

$$\nu=x^2+462y^2.$$

Now $x\leqslant 19444$, while

$$x\equiv\pm 1 \qquad (\text{mod } 2, 3, 7, 11),$$

so that by the Chinese remainder theorem

$$\pm(x-462t)=1,\ 43,\ 155 \text{ or } 197$$

with $0\leqslant t\leqslant 42$. For the cases $x=\pm 1+462t$, we have therefore (upper and lower signs corresponding throughout)

$$y^2=3\cdot 53\cdot 5147\mp 2t-462t^2$$
$$\equiv\begin{cases} -3\mp 2t+2t^2 & (\text{mod } 8)\\ \pm t & (\text{mod } 3)\\ -2(1\pm t+t^2) & (\text{mod } 5)\\ 3\mp 2t & (\text{mod } 7)\\ -5\mp 2t & (\text{mod } 11)\\ -3\mp 2t+6t^2 & (\text{mod } 13).\end{cases}$$

From these congruences it is easy to see that $t\not\equiv 0,\ 1 \pmod 4$, and moreover

$$\pm t \not\equiv 2\ (3);\ 0,\ 4\ (5)\ ;\ 0,\ 2,\ 6\ (7);\ 0,\ 2,\ 5,\ 9,\ 10\ (11);$$
$$3,\ 4,\ 5,\ 6,\ 10,\ 12\ (13)\,.$$

If we write down the numbers $\equiv 2, 3 \pmod 4$ from 2 to 42, then deletion of those $\equiv 2 \pmod 3$ and so on, will be found to exclude all. The case $x=1+462t$ is therefore impossible. However, after deleting numbers $\equiv -2 \pmod 3$ etc., there remain 18 and 38. Taking $t=18$ gives $y^2=668\ 721$, which is not a perfect square. But from $t=38$, we obtain the representation

$$\nu = 17555^2+6462\cdot 389^2\,.$$

The same exclusion moduli 4, 3, 5, 7, 11, 13 may be used to show that $\pm x \equiv 43,\ 155,\ 197 \pmod{462}$ do not lead to further decompositions. The one above is therefore unique and ν must be a prime number.

D. Cubic residues

If p is a prime $\equiv 1 \pmod 3$, we may write

$$4p = \xi^2+27\eta^2\,.$$

Sufficient conditions for the prime $q(\neq p)$ to be a cubic residue of p are then as follows.

(i) $$\xi\eta \equiv 0 \qquad (\mathrm{mod}\ q)\,.$$

When $q=2$, 3, 5 or 7, this condition is also necessary. See [10], [11].

(ii) The congruence

$$\tau^3 \equiv p(3\tau+\xi) \qquad (\mathrm{mod}\ q)$$

has a root $\tau (\mathrm{mod}\ q)$, provided $(q, 3\eta)=1$. See [8]. (Note that (ii) is just the condition for q to split fully in the cubic abelian field of discriminant p^2. The latter field is $\boldsymbol{Q}(\tau)$ or $\boldsymbol{Q}(\tau')$, where (cf. [6, §358])

$$\tau^3 = p(3\tau+\xi), \quad \tau'^3 = p(\tau'+\eta)\,.$$

We have

$$\mathrm{discr}\,(\tau) = (27\eta p)^2\,, \quad \mathrm{discr}\,(\tau') = (\xi p)^2\,,$$

the connection between τ, τ' being

$$2+\xi/\tau+3\eta/\tau' = 0\,.)$$

E. Real quadratic fields

By the second inequality in Scholz' condition [12]

$$s \leqslant r \leqslant s+1\,,$$

the Theorem proved above ($r \geqslant 4$ infinitely often) has the immediate consequence that infinitely many real quadratic fields have 3-rank three or larger. It would clearly be preferable (in retrospect!) to have a proof that $s \geqslant 4$ infinitely often and to deduce our Theorem from the first inequality.

A means for achieving this end is given by Yamamoto in Part II of [16]. Since

$$-27B^2+4A^3 = -27(B^2-4(A/3)^3),$$

the problem of finding several trinomial cubics x^3-Ax+B having the same discriminant is exactly the one treated above (see Part 2). Assuming some four of these cubics define unramified extensions of the same (real) quadratic field K (criteria for this being given in [16]), we shall have $s(K) \geqslant 4$ provided the extensions are independent, that is, none is contained in the compositum of the others.

A test for independence is easily supplied. Let $K_1, K_2, \cdots$ be cubic fields of discriminant d, where d is the discriminant of K. Then the composite, sextic fields KK_i will be independent provided there are rational primes $l_1, l_2, \cdots$ such that for each i, (l_i) is fully split in $K_1, \cdots, K_i$ but inert in K_{i+1}. For example, with $d=3^6+4\cdot 19^6$ we have

$$x^3-370x+731 \equiv \begin{cases} x(x-8)(x+8) & \pmod{17} \\ (x+1)(x+2)(x-3) & \pmod{11} \end{cases}$$

$$x^3-694x+6523 \equiv \begin{cases} x^3+3x-5 & \pmod{17} \\ x(x-1)(x+1) & \pmod{11} \end{cases}$$

$$x^3-604x+5067 \equiv \begin{cases} x^3+8x+1 & \pmod{17} \\ x^3+x-4 & \pmod{11}. \end{cases}$$

Thus $\boldsymbol{Q}(\sqrt{d})$ has $s \geqslant 3$. The class group is in fact precisely $\boldsymbol{C}(3)^3$ (see [13]).

F. Correction to [3]

The second sentence of the proof of Lemma 4 should state that there is a natural imbedding of $\boldsymbol{Q}[s]$ in $\boldsymbol{Q}_H[s, t]$ given by

$$f(s) \to t^{\deg(f)} f(s/t)$$

(to which the map $t \to 1$ is inverse).

STATE UNIVERSITY OF NEW YORK AT BUFFALO

References

[1] A.A. Albert: Fundamental concepts of higher algebra, Univ. of Chicago Press, Chicago, 1956.

[2] R.D. Carmichael: Diophantine analysis, Dover. (§15)

[3] M. Craig: *A type of class group for imaginary quadratic fields*, Acta Arith. **22** (1973), 449–459.

[4] M. Craig: Dissertation, Univ. of Michigan, Ann Arbor, 1972.

[5] L.E. Dickson: History of the theory of numbers II, Carnegie Institution, Washington, 1920. (550 ff.)

[6] C.F. Gauss: Disquisitiones arithmeticae, Yale Univ. Press, New Haven, 1966 (Clarke translation).

[7] D.N. Lehmer: List of prime numbers from 1 to 10,006,721, Hafner, New York, 1956.

[8] E. Lehmer: *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.

[9] L.J. Mordell: Diophantine equations, Academic Press, New York, 1969. (Ch. 11)

[10] T. Nagell: *Sur les restes et les non-restes cubiques*, Arkiv för Mat. **1** (1952), 579–586.

[11] T. Nagell: *Sur quelques problèmes dans la théorie des restes quadratiques et cubiques*, ibid. **3** (1956), 211–222.

[12] A. Scholz: *Über die Beziehungen der Klassenzahlen quadratische Körper zueinander*, Crelle **166** (1932), 201–203.

[13] D. Shanks and P. Weinberger: *A quadratic field of prime discriminant requiring three generators for its class group*, Sierpinski Memorial Volume, Acta Arith. **21** (1972), 71–87.

[14] C.L. Siegel: *Über einige Anwendungen Diophantische Approximationen*, Gesammelte Abhandlungen Bd I, Springer, 209–266.

[15] E. Weiss: Algebraic number theory, McGraw-Hill, 1963.

[16] Y. Yamamoto: *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.