INTEGRAL GENERATORS IN A CERTAIN QUARTIC FIELD AND RELATED DIOPHANTINE EQUATIONS

Andrew Bremner

1. Given a subring of the ring of integers in an algebraic number field K, then an effective procedure is known for determining whether or not the ring is principally generated over $\mathbf{Z}$ (see Győry [6, Corollaire 3.3]). In the case that the ring does have principal generators, then it clearly has infinitely many, since $\mathbf{Z}[\alpha]=\mathbf{Z}[m+\alpha]$ for an arbitrary integer m. If, however, one defines two algebraic integers α, α' to be equivalent if $\alpha-\alpha'\equiv 0 \bmod \mathbf{Z}$, then Győry shows that the numbers of generators up to equivalence is finite, and effectively bounds the height of such a generator in terms of the degree of K over $\mathbf{Q}$ and the discriminant of K. Actually to determine all the generators in a given ring still seems in general a difficult question, since the bound on the height of the generators lies well beyond present computing power. Nagell [10] solves this problem in the three quartic fields corresponding to the fifth, eighth, and twelfth roots of unity. An equivalent formulation of the problem is to determine all those β in the number ring $\mathbf{Z}[\alpha]$ of index 1; or again, to determine all those β in $\mathbf{Z}[\alpha]$ satisfying discriminant $(\alpha)=$ discriminant (β). Nagell [11] in a later paper observes that in the field $\mathbf{Q}(\xi)$, $\xi^4-\xi+1=0$, then the discriminants of $\xi, \xi^2, \xi^3, \xi^4, \xi^6, \xi^7$ are all equal to 229, and notes that it is not known if the discriminant of ξ^m can equal 229 for $m>7$.

In this paper we solve this problem as a corollary to finding all the generators for the ring of integers $\mathbf{Z}[\xi]$ in $\mathbf{Q}(\xi)$. This in turn is achieved by solving in integers the Diophantine equation $G^2+6183=4H^3$; this latter involves a considerable amount of numerical detail about six particular quartic extensions of $\mathbf{Q}$. In particular, a standard algorithm for computing units had to be strengthened in order that calculations by computer could be effective. I wish to thank here the referee for appreciably improving the presentation of this paper.

2. We consider the quartic field $\mathbf{Q}(\xi)$, where $\xi^4-\xi+1=0$, and wish to determine those α in $\mathbf{Z}[\xi]$ with $\mathbf{Z}[\alpha]=\mathbf{Z}[\xi]$. Denote the conjugates of ξ by $\xi_1=\xi, \xi_2, \xi_3, \xi_4$ and similarly define α_i, $i=1,\dots,4$. Since $\operatorname{disc}(\alpha)=\operatorname{disc}(\xi)$ and $\operatorname{disc}(\alpha)=\prod_{1\le i<j\le 4}(\alpha_i-\alpha_j)^2$,

$$\prod_{1\le i<j\le 4}\left(\frac{\alpha_i-\alpha_j}{\xi_i-\xi_j}\right)=\pm 1. \tag{1}$$

Now if i,j,k,l is a permutation of $1,2,3,4$, then $\xi_i\xi_j+\xi_k\xi_l$ is a zero of the resolvent cubic equation associated to the quartic polynomial x^4-x+1, namely the equation $\Xi^3-4\Xi-1=0$. Simple Galois theory shows that

Received December 8, 1983. Revision received October 11, 1984.
Michigan Math. J. 32 (1985).

$$\left(\frac{\alpha_i-\alpha_j}{\xi_i-\xi_j}\right)\left(\frac{\alpha_k-\alpha_l}{\xi_k-\xi_l}\right)\in \mathbf{Q}(\xi_i\xi_j+\xi_k\xi_l);$$

indeed, since up to equivalence α may be taken as $\alpha=b\xi+c\xi^2+d\xi^3$ for integers b, c, d,

$$\left(\frac{\alpha_i-\alpha_j}{\xi_i-\xi_j}\right)\left(\frac{\alpha_k-\alpha_l}{\xi_k-\xi_l}\right)=M-N(\xi_i\xi_j+\xi_k\xi_l),$$

where

(2) $$M=b^2-cd+d^2, \qquad N=-bd+c^2.$$

Since the left-hand side of (1) is simply a norm from $\mathbf{Q}(\Xi)$, (1) may be rewritten as

(3) $$M^3-4MN^2-N^3=\pm 1.$$

Now the conjugates of Ξ are all real, so $\mathbf{Z}[\Xi]$ has two fundamental units η_1, η_2 and (3) implies

$$\pm(M-N\Xi)=\eta_1^r\eta_2^s.$$

Equating the coefficients of Ξ^2 gives a single equation in the two exponents r, s, and it is difficult in general to apply p-adic arguments. It is necessary to introduce relative extensions of $\mathbf{Q}(\Xi)$ and the arithmetic details become very technical; see for example Ljunggren [7] and Baulin [1], who solve in this manner the equations $x^3-3xy^2-y^3=1$, $x^3+x^2y-2xy^2-y^3=1$, respectively. It is preferable to use relations between the quadratic and cubic covariants of the cubic form at (3) which give an equation to which Skolem's p-adic methods may be directly applied. See for example Tzanakis [13], who solves Ljunggren's equation in this manner.

The relation between covariants (see e.g. Mordell [9, Chapter 24]) gives, from (3),

(4) $$G^2+27.229=4H^3,$$

where

(5) $$G=27M^3+288M^2N+108MN^2-101N^3,$$
$$H=12M^2+9MN+16N^2.$$

Equation (4) is solved in the next two sections, thus giving all solutions to (3); then all (b, c, d) at (2) are found in §5. In §6, the original problem is solved and all ξ^m of discriminant 229 are found.

3.1. We proceed to solve in integers the equation

(6) $$G^2+6183=4H^3.$$

Let $K=\mathbf{Q}(\psi)$ where $\psi^3=458$. Then (6) may be written

(7) $$(2H-3\psi)(4H^2+6H\psi+9\psi^2)=2G^2.$$

Arithmetic details of K are as follows (see Beach, Williams, and Zarnke [2]): the ring of integers is $\mathbf{Z}[1, \psi, \omega]$ with $\omega=(1-\psi+\psi^2)/3$; the class-number is 6; and a fundamental unit is given by

(8) $$\epsilon=90685-16644\psi+633\psi^2$$

with inverse

(8′) $$\epsilon^{-1}=13049097841+1692876702\psi+219619131\psi^2.$$

It is readily checked that we have the following prime ideal factorizations:

(9) $$(2)=\mathfrak{p}_2^3; \qquad (3)=\mathfrak{p}_3^2\mathfrak{p}_3'; \qquad (8-\psi)=\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'^2$$

with

(10) $$\mathfrak{p}_3=(3, \psi+1, \omega); \mathfrak{p}_3'=(3, \psi+1, \omega-1),$$

and

(11) $$\mathfrak{p}_2=(1402+209\psi+72\omega).$$

The highest common factor of the two factors on the left-hand side at (7) is $(2H-3\psi, 27\psi^2)$. Since clearly $(H, 229)=1$ and $2H-3\psi$ is divisible by only the first power of $\mathfrak{p}_2$, this highest common factor is precisely $\mathfrak{p}_2$ in the case $(H, 3)=1$. Then in this instance, (7) implies the existence of an integral ideal $\mathfrak{a}$ of K satisfying

(12) $$(2H-3\psi)=\mathfrak{p}_2\mathfrak{a}^2.$$

In the case that $3 \mid H$, then $9 \mid G$. Put $H=3h$, $G=9g$; then (6) implies $4h^3=3g^2+229$ so that

(13) $$h\equiv 1 \bmod 3, \qquad g\equiv 0 \bmod 3.$$

Then $\operatorname{Norm}(2h-\psi)=8h^3-458=6g^2\equiv 0 \bmod 3^3$ by (13). Now $2h-\psi=2(h-4)+(8-\psi)$; and since $\mathfrak{p}_3^2\mathfrak{p}_3'=(3)$ cannot divide $2h-\psi$, (9) and (13) force $(2h-\psi)\equiv 0 \bmod \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'^2$. Accordingly, the highest common factor of the two factors on the left-hand side at (7) is

$$\begin{aligned}(2H-3\psi, 27\psi^2)&=(3)(2h-\psi, 9\psi^2)\\ &=(3)\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'^2\\ &=(3)(8-\psi).\end{aligned}$$

So (7) implies the existence of an integral ideal $\mathfrak{a}$ of K satisfying

(14) $$(2h-\psi)=(8-\psi)\mathfrak{a}^2.$$

Now in K we have the further factorizations:

(15) $$(11)=\mathfrak{p}_{11}\mathfrak{p}_{11}',$$

with

(16) $$\mathfrak{p}_{11}^2=(365-20\psi-12\omega).$$

It is straightforward to show that $\mathfrak{p}_{11}$ is not principal as follows. Let $\mathfrak{p}_5$ be the first degree prime factor of 5 in K. Since $\psi^3 \equiv 3 \bmod 5$, $\psi \equiv 2 \bmod \mathfrak{p}_5$. Then

$$\epsilon = 90685 - 16644\psi + 633\psi^2 \equiv 4 \bmod \mathfrak{p}_5,$$
$$365 - 20\psi - 12\omega \equiv 3 \bmod \mathfrak{p}_5.$$

Consequently, no generator of $\mathfrak{p}_{11}^2$ is a square mod $\mathfrak{p}_5$, and so $\mathfrak{p}_{11}$ is not principal. Thus $\mathfrak{p}_{11}$ may be taken as the nontrivial element of order 2 in the class group of K, and in each of the equations (12) and (14) it is necessary to consider the two possibilities, either that $\mathfrak{a}$ is principal or that $\mathfrak{a} \sim \mathfrak{p}_{11}$.

3.2. Take equation (14) where we first assume a is principal. Then there exist integers a, b, c such that

$$(17) \qquad 2h - \psi = \pm(8-\psi)\epsilon^r(a + b\psi + c\omega)^2, \quad r = 0, 1.$$

We have the following multiplication table of elements in K:

$$\psi^2 = -1 + \psi + 3\omega$$
$$\psi\omega = 153 - \omega$$
$$\omega^2 = -102 + 51\psi + \omega.$$

Then at (13), using $h \equiv 1 \bmod 3$, (17) implies $-1-\psi \equiv \pm(-1-\psi)(a-b)^2 \bmod 3$. From (10), $(\psi+1) \equiv 0 \bmod \mathfrak{p}_3\mathfrak{p}_3'$, so we deduce $1 \equiv \pm(a-b)^2 \bmod \mathfrak{p}_3$, that is, $1 \equiv \pm(a-b)^2 \bmod 3$. Hence, the upper sign holds. When $r = 0$, expanding (17) and equating coefficients of $1, \psi, \omega$ gives:

$$(18) \qquad h = 4a^2 - 233b^2 - 459c^2 + ab - 153ac + 1377bc,$$
$$(18') \qquad -1 = -a^2 + 8b^2 + 459c^2 + 14ab - 306bc,$$
$$(18'') \qquad 0 = 4b^2 - 24c^2 - ab + 3ac - 3bc.$$

Modulo 3, the latter two equations give $(a-b)^2 \equiv 1$, $(a-b)b \equiv 0$, so that $b \equiv 0 \bmod 3$. Put $b = 3c + 3d$; then (18″) gives

$$ad = c^2 + 21cd + 12d^2,$$

and since from (18′) a, c, d can have no common factor, it follows (without loss of generality assuming $d > 0$) that there exist co-prime integers m, n such that

$$(19) \qquad a = m^2 + 21mn + 12n^2; \qquad c = mn; \qquad d = n^2; \qquad b = 3n(m+n).$$

Substituting (19) into (18′) results in

$$(20) \qquad m^4 - 72m^2n^2 - 108mn^3 - 432n^4 = 1.$$

From the solution $\pm(m, n) = (1, 0)$ we recover $(a, b, c) = (1, 0, 0)$, $(H, G) = (12, 27)$; and in §4.1 we show that (20) has no further solutions.

If $r = 1$ at (17), then multiplying out and equating coefficients of ψ, ω gives

$$-1 = -202129a^2 + 10377830b^2 + 34736661c^2 + 423458ab + 6642648ac - 68494122bc$$

$$0 = 10854a^2 + 217783b^2 - 6701433c^2 - 223837ab + 227037ac + 3094287bc.$$

These quadratics simplify under the transformation

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 1299 & -1229 & -20364 \\ 325 & -365 & -5269 \\ 5 & 14 & -138 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix};$$

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} -124136 & 454698 & 957259 \\ -18505 & 67782 & 142699 \\ -6375 & 23351 & 49160 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix}$$

to give

(21) $$-1 = 581A^2 + 8253B^2 + 399C^2 - 4380AB - 960AC + 3618BC,$$

(21′) $$0 = -A^2 + 3AB + 3B^2 + AC.$$

Modulo 3, $1 \equiv A^2$, $0 \equiv -A^2 + AC$; and thus $C = A + 3D$ say, with

$$0 = AB + B^2 + AD.$$

On assuming $A > 0$, then $A = m^2$, $B = mn$, $D = -mn - n^2$, $C = m^2 - 3mn - 3n^2$ for co-prime integers m, n. Substitution into (21) gives

$$-1 = 20m^4 - 276m^3n + 1476m^2n^2 - 3672mn^3 + 3591n^4.$$

Certainly $n \equiv 1 \bmod 2$; then $0 \equiv 4m^4 + 4m^3 + 4m^2 \bmod 8$, so $m \equiv 0 \bmod 2$. Then $-1 \equiv 7 \bmod 16$, a contradiction. So there are no solutions to (17) when $r = 1$.

3.3. Suppose now in (14) that $\mathfrak{a} \sim \mathfrak{p}_{11}$. Then from (16) it follows that

(22) $$(365 - 20\psi - 12\omega)(2h - \psi) = \pm(8 - \psi)\epsilon^r(a + b\psi + c\omega)^2, \quad r = 0, 1$$

for integers a, b, c. Now $\mathfrak{p}_{11}$ is of first degree, and $\psi^3 \equiv 7 \bmod 11$; so $\psi \equiv 6 \bmod \mathfrak{p}_{11}$, and then $\omega \equiv 3 \bmod \mathfrak{p}_{11}$. From (22), $a + b\psi + c\omega \equiv 0 \bmod \mathfrak{p}_{11}$, and so

(23) $$a + 6b + 3c \equiv 0 \bmod 11.$$

As before, (22) taken modulo 3 gives $1 \equiv \pm(a - b)^2 \bmod \mathfrak{p}_3$ so that only the upper sign is possible.

Suppose $r = 0$ in (22). Equating coefficients of $1, \psi, \omega$ and simplifying gives

$$-1 = 7a^2 + 416b^2 + 2163c^2 + 108ab + 246ac + 1896bc,$$

$$0 = 248a^2 + 14736b^2 + 76548c^2 + 3823ab + 8715ac + 67173bc.$$

Certainly $a + c \equiv 1 \bmod 2$, $b \equiv 0 \bmod 2$, and then $-1 \equiv -a^2 - 2ac + 3c^2 \bmod 8$ so that $a \equiv 1 \bmod 2$, $c \equiv 0 \bmod 2$. Similarly, $0 \equiv -a^2 + ab \bmod 3$, $-1 \equiv a^2 - b^2 \bmod 3$, so that $a \equiv 0 \bmod 3$. Combining these congruences with (23), put

$$a=33a'-12b'-6c', \qquad b=2b', \qquad c=2c'.$$

Then under the further transformation

$$\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = \begin{pmatrix} 10 & -1 & 1 \\ -99 & 10 & -1 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix}; \qquad \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 10 & 1 & 9 \\ 99 & 10 & 89 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix}$$

the quadratics become

$$(24) \qquad -1=-21780A^2-217B^2-C^2+4356AB-1188AC+122BC,$$

$$(24') \qquad 0=174A^2-37AB+2B^2+AC.$$

It follows that $A\equiv 0 \bmod 2$, and so assuming $A>0$, there exist co-prime integers m, n with $A=2n^2$, $B=mn$, $C=-m^2+37mn-348n^2$.

Substituting into (24) gives

$$m^4+48m^3n-4608m^2n^2+95904mn^3-618624n^4=1.$$

Put $2n=N$, $m=-M+11N$; then

$$(25) \qquad M^4-68M^3N+366M^2N^2-680MN^3+397N^4=1.$$

Now (25) has the points $\pm(M,N)=(1,0),(9,8)$ and from §4.2 no further solutions. From the former, we recover $(a,b,c)=(-51,2,2)$, $(H,G)=(228,6885)$; and from the latter, $(a,b,c)=(-5739,218,234)$, $(H,G)=(3041076,10606470939)$.

Suppose secondly that $r=1$ in (22). As before, only the upper sign is permissible. From (23), put $a=5b-3c+11d$. Then (22) becomes, after a certain amount of arithmetic,

$$\begin{aligned} 2h-\psi=&[43148b^2+1395378c^2+19826d^2-602382bc+486362bd-1440474cd] \\ &+\psi[11087b^2-12564c^2-40345d^2-35130bc-40408bd+175674cd] \\ &+\omega[-7320b^2-73908c^2+16572d^2+49698bc-9954bd+4914cd]. \end{aligned}$$

Under the transformation

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 35 & -77 & -34 \\ -109 & 498 & -251 \\ -50 & 224 & -109 \end{pmatrix} \begin{pmatrix} b \\ c \\ d \end{pmatrix};$$

$$\begin{pmatrix} b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1942 & -16009 & 36259 \\ 669 & -5515 & 12491 \\ 484 & -3990 & 9037 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix},$$

after equating coefficients of ψ, ω there results

$$(26) \qquad -1=84A^2+2717B^2+13782C^2-954AB+2148AC-12240BC,$$

$$(26') \qquad 0=-5B^2+3C^2+10BC+AB.$$

Modulo 3, $B^2 \equiv 1$, $B(A+B+C) \equiv 0$. Thus, we may put $A = -B-C+3D$ to give $0 = -2B^2+3BC+C^2+BD$. Then, assuming $B>0$, there exist co-prime integers m, n with $B = m^2$, $C = mn$, $D = 2m^2-3mn-n^2$, $A = 5m^2-10mn-3n^2$. Substituting into (26) and putting $M = 2n$, $N = m-2n$, results in

(27) $$M^4+22M^3N-12M^2N^2-32MN^3-188N^4 = 4.$$

Now $MN \not\equiv 0 \bmod 5$, and so $M^4 \equiv N^4 \equiv 1 \bmod 5$. Then (27) implies

$$2MN(M+2N)^2 \equiv 1 \bmod 5,$$

and it is easy to check that this is a congruence with no solution. Thus, (27) has no integer solutions.

3.4. Consider now equation (12) with $\mathfrak{a}$ principal. Using (11), (12) implies an equation

(28) $$2H-3\psi = \pm\epsilon^r(1402+209\psi+72\omega)(a+b\psi+c\omega)^2, \quad r = 0, 1$$

for integers a, b, c. Positivity implies the upper sign. When $r = 0$, expanding and equating coefficients of ψ, ω yields

$$-3 = 209a^2+12418b^2+64515c^2+3222ab+7344ac+56610bc,$$
$$0 = 36a^2+2139b^2+11113c^2+555ab+1265ac+9751bc.$$

It follows that $c \equiv 0 \bmod 2$. Putting

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} -31 & 101 & 19 \\ 4 & -13 & -7 \\ 0 & 0 & 2 \end{pmatrix}\begin{pmatrix} A \\ B \\ C \end{pmatrix}; \quad \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 13 & 101 & 230 \\ 4 & 31 & 141/2 \\ 0 & 0 & 1/2 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

the two quadratics become

(29) $$-3 = 9A^2+165B^2-3C^2-76AB-12AC+58BC,$$

(29′) $$0 = 12B^2-3AB+AC.$$

Modulo 3, $0 \equiv -AB+BC \equiv AC$. If $A \equiv C \equiv 0$ then (29′) would imply $B \equiv 0 \bmod 3$, which is impossible. So $B \equiv 0 \bmod 3$ and $AC \equiv 0 \bmod 9$. If we suppose $C \equiv 0 \bmod 9$, then (29′) gives $0 \equiv -3B+C \bmod 27$. Put $A = D$, $B = 3E$, $C = 9E-27F$ so that (29) and (29′) give

(30) $$-1 = 3D^2+936E^2-729F^2-112DE+108DF-1080EF,$$

(30′) $$0 = 4E^2-DF.$$

Modulo 2, $D+F \equiv 1$. If $F \equiv 0 \bmod 4$ then (30) gives $-1 \equiv 3D^2 \bmod 8$, which is impossible. So from (30′), $D = 4m^2$, $F = n^2$, $E = mn$, and substitution into (30) gives

$$-1 = 48m^4-448m^3n+1368m^2n^2-1080mn^3-729n^4,$$

whence $8\equiv 9n^4-1\equiv 8m^2n^2+8mn^3\equiv 0 \bmod 16$, a contradiction. It follows that $A\equiv 0 \bmod 9$ in (29′); whence also $A\equiv 0 \bmod 27$. Put $A=27D$, $B=3E$, $C=F$ so that (29) and (29′) give

$$(31)\qquad -1=2187D^2+495E^2-F^2-2052DE-108DF+58EF,$$

$$(31')\qquad 0=4E^2-9DE+DF.$$

Modulo 4, $1\equiv D^2+(E-F)^2$, $0\equiv D(E-F)$. Then modulo 8, $1\equiv 5D^2+(E-F)^2$ so that $D\equiv 0 \bmod 4$, $E-F\equiv 1 \bmod 2$. From (31′) we may suppose $D=4m^2$, $9E-F=n^2$, $E=mn$; and substituting into (31) with the further transformation $M=10m-n$, $N=2n$, results in

$$(32)\qquad M^4-40M^3N+108M^2N^2-92MN^3-52N^4=1.$$

From the point $\pm(M,N)=(1,0)$ we get $(a,b,c)=(-19,7,-2)$, $(H,G)=(82,1483)$. In §4.4, we show there are no further solutions to (32).

When $r=1$ in (28) we obtain, in a manner similar to the above,

$$(33)\qquad -3=275a^2-19184b^2-15657c^2+738ab-12852ac+97002bc,$$

$$(33')\qquad 0=-63a^2+78b^2+30523c^2+951ab-307ac-18971bc.$$

Transforming via

$$\begin{pmatrix}A\\B\\C\end{pmatrix}=\begin{pmatrix}24&-161&0\\5&14&-138\\46&-85&-649\end{pmatrix}\begin{pmatrix}a\\b\\c\end{pmatrix};$$

$$\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}20816&104489&-22218\\3103&15576&-3312\\1069&5366&-1141\end{pmatrix}\begin{pmatrix}A\\B\\C\end{pmatrix},$$

the equations (33) and (33′) become

$$(34)\qquad -3=-3A^2+215B^2+3C^2+34AB-60BC$$

$$(34')\qquad 0=3B^2-5BC+C^2-AC.$$

Assuming $C>0$, then (34′) implies either $(A,B,C)=(3m^2-5mn+n^2, mn, n^2)$ or $(A,B,C)=(m^2-5mn+3n^2, mn, 3n^2)$ for co-prime integers m,n. In the former instance, substitution into (34) gives $3=m(27m^3-192m^2n+48mn^2-4n^3)$ so that $m\mid 3$, and there are no solutions. In the latter instance, substitution into (34) gives $3=m(3m^3-64m^2n+48mn^2-12n^3)$, and again $m\mid 3$ with a solution precisely when $n=0$. So

$$(A,B,C)=(1,0,0),$$

$$(a,\ b,\ c)=(20816,3103,1069),$$

$$(H,\ G)=(232,7067).$$

3.5. Consider finally (12) with $\mathfrak{a} \sim \mathfrak{p}_{11}$. Then

(35)
$$(365-20\psi-12\omega)(2H-3\psi)=\pm\epsilon^r(1402+209\psi+72\omega)(a+b\psi+c\omega)^2, \quad r=0,1$$

for integers a, b, c satisfying the congruence (23). By positivity, only the upper sign can occur. Put $a=5b-3c+11d$; then (35) can be rewritten in the form

$$\begin{aligned}2H-3\psi=\epsilon^{r-1}[&(-126b^2-2508c^2+134d^2+1254bc+722bd+1902cd)\\ &+\psi(-11b^2+102c^2+51d^2+6bc+80bd-306cd)\\ &+\omega(12b^2+98c^2+30d^2-74bc+6bd+26cd)].\end{aligned} \tag{36}$$

If $r=0$, then apply the transformation

$$\begin{pmatrix}B\\C\\D\end{pmatrix}=\begin{pmatrix}-2574 & -2951 & -2228\\ -5810 & -6661 & -5029\\ 1 & 13 & -3\end{pmatrix}\begin{pmatrix}b\\c\\d\end{pmatrix};$$

$$\begin{pmatrix}b\\c\\d\end{pmatrix}=\begin{pmatrix}85360 & -37817 & -129\\ -22459 & 9950 & 34\\ -68869 & 30511 & 104\end{pmatrix}\begin{pmatrix}B\\C\\D\end{pmatrix},$$

and equate coefficients of ψ, ω:

$$-3=-1297513B^2-256374C^2-3D^2+1153526BC+3946BD-1754CD, \tag{37}$$

$$0=3B^2+661BC-293C^2-CD. \tag{37'}$$

Assuming $C>0$, then (37′) implies either

$$(B, C, D)=(mn, n^2, 3m^2+661mn-293n^2)$$

or

$$(B, C, D)=(mn, 3n^2, m^2+661mn-879n^2)$$

for co-prime integers m, n. In the former instance, substitution into (37) gives

$$3=27m^4+60m^3n-42m^2n^2+8mn^3-n^4.$$

Certainly $m+n\equiv 1 \bmod 2$, and $3\equiv 3m^4-n^4 \bmod 8$, whence $m\equiv 1$, $n\equiv 0 \bmod 2$. Then $3\equiv 11m^4+12m^3n+6m^2n^2 \bmod 16$; but with $n=2k$ we have

$$12m^3n+6m^2n^2=24m^2k(m+k)\equiv 0 \bmod 16,$$

so that $3\equiv 11m^4 \bmod 16$, a contradiction. In the latter instance substitution into (37) gives

$$-3=-3m^4-20m^3n+42m^2n^2-24mn^3+9n^4.$$

Then $m^3n\equiv 0 \bmod 3$, and clearly $m\not\equiv 0 \bmod 3$. So putting $m=M$, $n=3N$:

$$M^4+20M^3N-126M^2N^2+216MN^3-243N^4=1. \tag{38}$$

In §4.5 we show that (38) has only the solution $\pm(M,N)=(1,0)$, with corresponding $(a,b,c)=(397,-129,34)$, $(H,G)=(46,619)$.

If $r=1$ in (36), then applying the transformation

$$\begin{pmatrix} B \\ C \\ D \end{pmatrix} = \begin{pmatrix} -3 & 13 & -6 \\ -2 & 8 & -3 \\ 0 & 1 & -2 \end{pmatrix} \begin{pmatrix} b \\ c \\ d \end{pmatrix}; \qquad \begin{pmatrix} b \\ c \\ d \end{pmatrix} = \begin{pmatrix} -11 & -20 & -9 \\ 4 & -6 & -3 \\ 2 & -3 & -2 \end{pmatrix} \begin{pmatrix} B \\ C \\ D \end{pmatrix}$$

and equating coefficients of ψ, ω yields

(39) $$-3=-79B^2-257C^2-3D^2+288BC+32BD-58CD$$

(39′) $$0=-4B^2+5BC+3C^2+BD.$$

Then assuming $B>0$, (39′) implies either $(B,C,D)=(m^2,mn,4m^2-5mn-3n^2)$ or $(B,C,D)=(3m^2,mn,12m^2-5mn-n^2)$ for co-prime integers m,n. In the former case, substitution into (39) gives

$$-3=m^4+16m^3n-66m^2n^2+84mn^3-27n^4,$$

which, as before, is insolvable modulo 16. In the latter case, substitution into (39) gives

$$-3=9m^4+48m^3n-66m^2n^2+28mn^3-3n^4.$$

Clearly $m\equiv 0 \bmod 3$. Put $m=3N$, $n=-M+6N$, giving

(40) $$M^4+4M^3N-90M^2N^2+216MN^3-459N^4=1.$$

In §4.6 we show that the only solution of (40) is $\pm(M,N)=(1,0)$, with corresponding $(a,b,c)=(58,9,3)$, $(H,G)=(16,101)$.

4.1. We turn now to the solution of the quartic equations obtained in §3.

First, we present a modification of the well-known theorem of Skolem [12]. I am grateful to the referee for suggesting this form of the lemma.

LEMMA. *Let θ be an algebraic integer of degree 4 which has two real and two complex conjugates, and with minimal polynomial $f(X)$. Let $F(X,Y)$ be the binary form defined by $F(X,Y)=Y^4f(X/Y)$ for $Y\neq 0$. Let $K=\mathbf{Q}(\theta)$, and let $\mathfrak{O}_K$ denote the ring of integers of K with an integral basis given by $\{1,\theta,\phi,\Phi\}$. If $\alpha\in K$, denote by $\alpha(1),\alpha(\theta),\alpha(\phi),\alpha(\Phi)$, the rational numbers defined by $\alpha=\alpha(1)+\alpha(\theta)\theta+\alpha(\phi)\phi+\alpha(\Phi)\Phi$. Let $\{\epsilon_1,\epsilon_2\}$ be a system of fundamental units in $\mathfrak{O}_K$, let $p>2$ be a prime number, and let L,M be positive integers such that*

(41) $$\epsilon_1^L=\pm 1+pE_1, \qquad \epsilon_2^M=\pm 1+pE_2$$

for certain $E_1,E_2\in\mathfrak{O}_K$. Let R',S' be rational integers with $|R'|\leq L/2$, $|S'|\leq M/2$ such that

(42) $$\epsilon_1^{R'}\epsilon_2^{S'}(\phi)\equiv\epsilon_1^{R'}\epsilon_2^{S'}(\Phi)\equiv 0 \bmod p$$

and

(43) $$\Delta=(\epsilon_1^{R'}\epsilon_2^{S'}E_1)(\phi)\cdot(\epsilon_1^{R'}\epsilon_2^{S'}E_2)(\Phi)-(\epsilon_1^{R'}\epsilon_2^{S'}E_1)(\Phi)\cdot(\epsilon_1^{R'}\epsilon_2^{S'}E_2)(\phi)$$
$$\not\equiv 0 \bmod p.$$

Then the equation

$$F(x, y) = 1, \quad x, y \in \mathbf{Z} \tag{44}$$

has at most one solution satisfying

$$x - y\theta = \pm \epsilon_1^R \epsilon_2^S \tag{45}$$

where R; S are rational integers with $R \equiv R' \bmod L$, $S \equiv S' \bmod M$.

Proof. Certainly for a solution x, y of (44) there exist $R, S \in \mathbf{Z}$ such that (45) holds. Suppose (x_0, y_0) is a solution of (44) for which (45) holds with integers R, S satisfying $R \equiv R' \bmod L$, $S \equiv S' \bmod M$. Suppose (x, y) is a further solution of (44) with this property. Then there are rational integers R'', S'' such that $x - y\theta = \pm(x_0 - y_0\theta)\epsilon_1^{LR''}\epsilon_2^{MS''}$. Together with (41), this implies that

(46)

$$\begin{aligned} x - y\theta &= \pm(x_0 - y_0\theta)(1 \pm pE_1)^{R''}(1 \pm pE_2)^{S''} \\ &= \pm(x_0 - y_0\theta) \pm p[(x_0 - y_0\theta)E_1R'' \pm (x_0 - y_0\theta)E_2S''] + p^2(\ \ ) + p^3(\ \ ) + \cdots \end{aligned}$$

where the expressions ( ) denote polynomials in R'', S'' of which the coefficients are of type $\alpha + \beta\theta + \gamma\phi + \delta\Phi$ with $\alpha, \beta, \gamma, \delta \in \mathbf{Z}_p$. Equating coefficients of ϕ, Φ in (46), using (42) and $x_0 - y_0\theta \equiv \pm\epsilon_1^{R'}\epsilon_2^{S'} \bmod p$, and dividing by p yields

$$\begin{aligned} &\alpha_1 R'' + \alpha_2 S'' + p(\ \ ) + p^2(\ \ ) + \cdots = 0, \\ &\beta_1 R'' + \beta_2 S'' + p(\ \ ) + p^2(\ \ ) + \cdots = 0, \end{aligned} \tag{47}$$

where $(\alpha_i, \beta_i) \equiv \pm((\epsilon_1^{R'}\epsilon_2^{S'}E_i)(\phi), (\epsilon_1^{R'}\epsilon_2^{S'}E_i)(\Phi)) \bmod p$, for $i = 1, 2$, and the expressions ( ) denote polynomials in $\mathbf{Z}_p[R'', S'']$. But by (43), $\alpha_1\beta_2 - \alpha_2\beta_1 \not\equiv 0 \bmod p$. Thus, by Skolem's theorem [12], (47) can have at most one solution in R'', S'' which is obviously equal to $R'' = 0$, $S'' = 0$. Hence (x_0, y_0) is the only solution of (44) for which (45) holds with R, S satisfying $R \equiv R' \bmod L$, $S \equiv S' \bmod M$. □

In each particular instance that follows, the arithmetic details of the relevant quartic extension of the rationals are quoted, with justification postponed to §7.

Consider first equation (20). Define $K = \mathbf{Q}(\theta)$ where $\theta^4 - 72\theta^2 - 108\theta - 432 = 0$. Then K has integer base $\{1, \theta, \phi, \Phi\}$ where $\phi = \theta^2/6$, $\Phi = \theta^3/36$, with discriminant $\Delta^2(K) = -2^2 \cdot 3^3 \cdot 229^2$. A pair of independent units in K is

$$\eta_1 = 31 + 11\theta + 38\phi + 24\Phi,$$

$$\eta_2 = 483602731 + 174202120\theta + 316187252\phi - 293718704\Phi.$$

In §7.2 we show that there exists in K a pair of fundamental units ϵ_1, ϵ_2 satisfying $\epsilon_i \equiv \eta_i \bmod 3$.

Equation (20) can be written in the form $\mathrm{Norm}(m - n\theta) = 1$, so that

$$\pm(m - n\theta) = \epsilon_1^r \epsilon_2^s \tag{48}$$

for integers r, s.

Now

$$\epsilon_1^3 \equiv \eta_1^3 \equiv 1-3\theta+3\phi \bmod 9,$$
$$\epsilon_2^9 \equiv \eta_2^9 \equiv 1+3\theta+3\phi-3\Phi \bmod 9.$$

Put $r=3R+\rho$, $s=9S+\sigma$ with $0\le\rho\le 2$, $0\le\sigma\le 8$, and then (48) implies that the coefficients of ϕ,Φ in $\epsilon_1^\rho\epsilon_2^\sigma$ must both be zero modulo 3. This forces $\rho=0$, $\sigma=0,3,6$. Put $R=3P+\rho'$, $S=3Q+\sigma'$, $0\le\rho',\sigma'\le 2$; then (48) gives

$$\pm(m-n\theta)=\epsilon_1^{9P}\epsilon_2^{27Q}\cdot\epsilon_1^{3\rho'}\epsilon_2^{9\sigma'+\sigma}$$

whence the coefficients of ϕ,Φ in the latter factor must both be zero modulo 9; and this forces $\rho'=0$, $\sigma'=\sigma=0$. The lemma now applies, with $p=3$, $(L,M)=(3,9)$, $(R',S')=(0,0)$. The only solution of (48) is $r=s=0$, with corresponding $\pm(m,n)=(1,0)$.

4.2. Define $K=\mathbf{Q}(\theta)$, where $\theta^4-68\theta^3+366\theta^2-680\theta+397=0$. Then K has integer base $\{1,\theta,\phi,\Phi\}$ where $\phi=(\theta+1)^2/6$, $\Phi=(\theta+1)^3/36$, and $\Delta^2(K)=-2^2\cdot 3^3\cdot 229^2$. A pair of fundamental units is given by

$$\epsilon_1=251-776\theta+916\phi-80\Phi,$$
$$\epsilon_2=145415-218888\theta+214656\phi-18432\Phi,$$
$$(\epsilon_2^{-1}=-9+8\theta).$$

Now (22) takes the form $\text{Norm}(M-N\theta)=1$, so that

$$\pm(M-N\theta)=\epsilon_1^r\epsilon_2^s. \tag{49}$$

The p-adic method of dealing with equations such as (49) is to find a prime p such that the coefficients of ϕ,Φ in $\epsilon_1^r\epsilon_2^s$, taken modulo p, vanish as infrequently as possible. To save excessive calculation it is best to consider first those primes which split completely in K, so that the orders of ϵ_1,ϵ_2 taken modulo p divide $p-1$. See Bremner [3; 4] and Bremner and Tzanakis [5] for other numerical examples. Here the primes splitting completely in K include 199, 271, 337, 421, 457, ... It is best to work with $p=421$. Machine computation gives

$$\epsilon_1^{105}=1+421E_1 \quad\text{with } E_1\equiv 61+56\theta-134\phi+198\Phi \bmod 421,$$
$$\epsilon_2^{420}=1+421E_2 \quad\text{with } E_2\equiv 153+136\theta+168\phi-170\Phi \bmod 421,$$

and $(\rho,\sigma)=(0,0),(0,-1)$ are the only values of ρ,σ satisfying $-52\le\rho<53$, $-210\le\sigma<210$ such that the coefficients of ϕ,Φ in $\epsilon_1^\rho\epsilon_2^\sigma$ both vanish modulo 421. The lemma now applies with $p=421$, $(L,M)=(105,420)$, and $(R',S')=(0,0)$ or $(0,-1)$ (it is straightforward to check condition (43)). The only solutions to (49) are $(r,s)=(0,0)$, $(0,-1)$ with corresponding $\pm(M,N)=(1,0)$, $(9,8)$, respectively.

4.3. Define $K=\mathbf{Q}(\theta)$ where $\theta^4-40\theta^3+108\theta^2-92\theta-52=0$. Then K has integer base $\{1,\theta,\phi,\Phi\}$ where $\phi=(\theta^2+2)/2$, $\phi=(\theta^3-26\theta^2+14\theta-4)/54$, and $\Delta^2(K)=-2^4\cdot 3\cdot 229^2$. A pair of fundamental units is

$$\epsilon_1 = -807 - 11130\theta + 5635\phi + 1620\Phi,$$

$$\epsilon_2 = -120697 - 338780\theta + 409864\phi + 159264\Phi.$$

The primes that factor completely in K include $127, 163, 193 \ldots$. It is appropriate here to use $p = 163$. Computation gives

$$\epsilon_1^{81} = -1 - 163E_1 \quad \text{with } E_1 \equiv -52 + 68\theta + 49\phi + 67\Phi \bmod 163$$

$$\epsilon_2^{81} = 1 + 163E_2 \quad \text{with } E_2 \equiv 73 - 18\theta + 78\phi - 57\Phi \bmod 163$$

and $(\rho, \sigma) = (0, 0)$ are the only values of ρ, σ satisfying $-40 \leq \rho, \sigma < 41$ such that the coefficients of ϕ, Φ in $\epsilon_1^\rho \epsilon_2^\sigma$ both vanish modulo 163. Thus we can now apply the lemma with $p = 163$, $(L, M) = (81, 81)$, $(R', S') = (0, 0)$ to show that (32) has the unique solution in integers $\pm(M, N) = (1, 0)$.

4.4. Let $K = \mathbf{Q}(\theta)$ where $\theta^4 + 20\theta^3 - 126\theta^2 + 216\theta - 243 = 0$. Then K has integer base $\{1, \theta, \phi, \Phi\}$ where $\phi = (\theta^2 + 2\theta + 3)/6$, $\Phi = (\theta^3 + 2\theta^2 - 27\theta)/54$, and $\Delta^2(K) = -2^4 \cdot 3 \cdot 229^2$. A pair of fundamental units is

$$\epsilon_1 = 36 - 13800\theta + 2950\phi + 1065\Phi,$$

$$\epsilon_2 = 1552 - 305430\theta + 68814\phi + 28686\Phi.$$

Primes factoring completely in K include $163, 337, 547 \ldots$. We work here with $p = 337$. Computation gives

$$\epsilon_1^{42} = -1 - 337E_1 \quad \text{with } E_1 \equiv -132 + 85\theta + 134\phi - 32\Phi \bmod 337,$$

$$\epsilon_2^{336} = 1 + 337E_2 \quad \text{with } E_2 \equiv 128 + 20\theta + 109\phi - 147\Phi \bmod 337,$$

and $(\rho, \sigma) = (0, 0)$ are the only values of ρ, σ satisfying $-21 \leq \rho < 21$, $-168 \leq \sigma < 168$ such that the coefficients of ϕ, Φ in $\epsilon_1^\rho \epsilon_2^\sigma$ are both zero modulo 337. Applying the lemma with $p = 337$, $(L, M) = (42, 336)$, $(R', S') = (0, 0)$ shows that (38) has only the solution $\pm(M, N) = (1, 0)$.

4.5. Let $K = \mathbf{Q}(\theta)$ where $\theta^4 + 4\theta^3 - 90\theta^2 + 216\theta - 459 = 0$. Then K has integer base $\{1, \theta, \phi, \Phi\}$ where $\phi = (\theta^2 - 2\theta + 3)/6$, $\Phi = (\theta^3 + \theta^2 + 15\theta - 45)/108$, and $\Delta^2(K) = -2^2 \cdot 3 \cdot 229^2$. A pair of fundamental units is

$$\epsilon_1 = 179 - 113\theta + 27\phi + 126\Phi,$$

$$\epsilon_2 = -6087998 + 1285904\theta - 3940781\phi - 7498800\Phi.$$

Primes splitting completely in K include $163, 271, 523 \ldots$. Working with the prime 271,

$$\epsilon_1^{270} = 1 + 271E_1 \quad \text{with } E_1 \equiv 11 + 75\theta - 68\phi + 96\Phi \bmod 271,$$

$$\epsilon_2^{270} = 1 + 271E_2 \quad \text{with } E_2 \equiv -28 - 104\theta + 33\phi + 24\Phi \bmod 271,$$

and $(\rho, \sigma) = (0, 0)$ are the only values of ρ, σ satisfying $-135 \leq \rho, \sigma < 135$ such that the coefficients of ϕ, Φ in the product $\epsilon_1^\rho \epsilon_2^\sigma$ are both zero modulo 271. Applying the lemma with $p = 271$, $(L, M) = (270, 270)$, $(R', S') = (0, 0)$, (40) can have only the solution $\pm(M, N) = (1, 0)$.

Putting the foregoing together yields the following result.

THEOREM 1. *The only integer solutions of* $G^2+6183=4H^3$ *are the following:*

$$(50)\qquad \begin{aligned}(H, \pm G) = {} & (12,27),(16,101),(46,619),(82,1483),(228,6885),\\ & (232,7067),(3041076,10606470939).\end{aligned}$$

COROLLARY 2. *The only integer solutions of* $X^3-4XY^2-Y^3=1$ *are the following:*

$$(51)\qquad (X,Y)=(-2,-1),(0,-1),(1,0),(1,-4),(2,-1),(508,-273).$$

Proof. For each (H,G) listed at (50) it is simple to find the corresponding (X,Y) (if any) via the transformations at (2), (4), and (5). Only the point $(228, \pm 6885)$ has no corresponding (X,Y). □

We note here also the following result.

COROLLARY 3. *There are essentially seven distinct monic cubic polynomials in* $\mathbf{Z}[X]$ *with discriminant* 229, *namely:*

$$(52)\qquad \begin{aligned}&x^3-4x-1;\quad x^3+x^2-5x+2;\quad x^3-x^2-15x+28;\quad x^3-x^2-27x+64;\\ &x^3-76x-255;\quad x^3-x^2-77x-236;\quad x^3-1013692x+392832257.\end{aligned}$$

Proof. "Essentially" here means up to translation by an integer, or changing the sign of x.

Since there is a unique cubic field of discriminant 229, namely $\mathbf{Q}(\Xi)$, then a polynomial of the required type has an algebraic integer root in $\mathbf{Q}(\Xi)$ which is of index 1 in $\mathbf{Z}[\Xi]$; the result follows from the previous sections. Alternatively, there is the following polynomial identity. Let x^3+ax^2+bx+c have discriminant 229; then

$$(27c-9ab+2a^3)^2+6183=4(a^2-3b)^3,$$

and using (50) it is straightforward to list the possibilities for a, b, c normalizing in each case so as to achieve $|a|\leq 1$. □

5.1. In order to solve the problem of generators in the ring $\mathbf{Z}[\xi]$, it is now necessary by the remarks of §1 to investigate for each $(M,N)=(X,Y),(-X,-Y)$, where (X,Y) is one of the points listed at (51), the solvability in integers of the equations

$$(53)\qquad \begin{aligned}b^2-cd+d^2&=M,\\ -bd+c^2&=N.\end{aligned}$$

For a real parameter λ, (53) may be written in the form

$$(54)\qquad M+\lambda N=\left(b-\frac{1}{2}\lambda d\right)^2+\lambda\left(c-\frac{1}{2\lambda}d\right)^2-\frac{\lambda^3-4\lambda+1}{4\lambda}d^2.$$

Taking $\lambda=1$,

$$(55)\qquad M+N=\left(b-\frac{1}{2}d\right)^2+\left(c-\frac{1}{2}d\right)^2+\frac{1}{2}d^2,$$

and so the system (53) is insolvable if $M+N$ is negative. Thus, it remains to consider only the cases $(M,N)=(-1,4)$, $(0,1)$, $(1,0)$, $(2,-1)$, $(2,1)$, $(508,-273)$.

First, suppose $(M,N)=(508,-273)$. Taking $\lambda=508/273$ at (54) gives

$$0=\left(b-\frac{254}{273}d\right)^2+\frac{508}{273}\left(c-\frac{283}{1016}d\right)^2-\frac{1}{4\cdot 508\cdot 273^2}d^2$$

and, in particular,

$$b-\frac{254}{273}d\neq 0.$$

Thus,

$$\frac{1}{4\cdot 508\cdot 273^2}d^2>\frac{1}{273^2},$$

whence

(56) $$d^2>4\cdot 508=2032.$$

But from (55), $d^2<2(M+N)=470$, contradicting (56). Hence, (53) is unsolvable for $(M,N)=(508,-273)$.

In the remaining cases $(M,N)=(-1,4)$, $(0,1)$, $(1,0)$, $(2,-1)$, $(2,1)$, b,c,d can be determined from (53) and (55) by straightforward computation. Thus, we obtain table (57).

(57)

(M,N)	Solutions (b,c,d) of (53)
$(-1,4)$	No solutions
$(0,1)$	$\pm(0,1,0)$, $\pm(0,1,1)$
$(1,0)$	$\pm(1,0,0)$, $\pm(0,0,1)$, $\pm(1,1,1)$
$(2,-1)$	$\pm(1,0,1)$
$(2,1)$	$\pm(-1,0,1)$, $\pm(0,-1,1)$, $\pm(0,1,2)$.

6. We have thus proved the following result.

THEOREM 7. *Up to equivalence, precisely the following integers α of $\mathbf{Z}[\xi]$, $\xi^4-\xi+1=0$, satisfy $\mathbf{Z}[\alpha]=\mathbf{Z}[\xi]$:*

(58) $$\pm\alpha=\xi,\ \xi^2,\ \xi^3,\ \xi\pm\xi^3,\ \xi+\xi^2+\xi^3,\ \xi^2\pm\xi^3,\ \xi^2+2\xi^3,\ 2\xi^2+\xi^3.$$

THEOREM 8. *In $\mathbf{Z}[\xi]$, precisely the following powers of ξ generate the ring of integers:*

$$\xi^{-7},\ \xi^{-6},\ \xi^{-4},\ \xi^{-3},\ \xi^{-2},\ \xi^{-1},\ \xi,\ \xi^2,\ \xi^3,\ \xi^4,\ \xi^6,\ \xi^7.$$

Proof. It is required to find those integers n such that

(59) $$\pm\xi^n=a+p(\xi)$$

for some integer a, where $p(\xi)$ is one of the elements α listed at (58). Now

(60) $$\xi^{30}=1+4X,\quad X=-2-5\xi+15\xi^2-12\xi^3.$$

Let $n=30N+\nu$, $-15\leq\nu<15$, so that (59) implies

(61) $$\pm\xi^{\nu}\equiv a+p(\xi) \bmod 4.$$

It is easy to check that (61) has no solution in the instances $p(\xi)=\xi+\xi^3$, $2\xi^2+\xi^3$. The following table (62) gives the solutions ν for the remaining possibilities for $p(\xi)$.

(62)

$p(\xi)$	ν
ξ	1, 4
ξ^2	2
ξ^3	−1, 3, 14
$\xi-\xi^3$	−6, 7
$\xi+\xi^2+\xi^3$	−3, −4, 11
$\xi^2+\xi^3$	−2
$\xi^2-\xi^3$	6, 13
$\xi^2+2\xi^3$	−13, −7.

Consider for example $p(\xi)=\xi^2+2\xi^3$, $\nu=-7$. Then (59) and (60) give

$$\pm\xi^{-7}(1+4X)^N=a+\xi^2+2\xi^3.$$

Since $\xi^{-7}=-3+\xi^2+2\xi^3$, a congruence mod 4 implies the upper sign.

Putting $(1+4X)^N=L_0+L_1\xi+L_2\xi^2+L_3\xi^3$, where

$$L_0=1+4(-2N)+4^2(\ )$$
$$L_1=4(-5N)+4^2(\ )$$
$$L_2=4(15N)+4^2(\ )$$
$$L_3=4(-12N)+4^2(\ ),$$

and equating coefficients of ξ^2 gives $L_0-L_2-L_3=1$, whence there is the 2-adic equation

$$-5N+4(\ )+4^2(\ )+\cdots=0.$$

Skolem's theorem once again implies at most one solution, which is clearly $N=0$.

The cases $\nu=7, \pm 6, \pm 4, \pm 3, \pm 2, \pm 1$ with the corresponding $p(\xi)$, in which there actually does exist a solution to (59) (viz. with $n=\nu$), are entirely analogous, and details are omitted.

It remains to show that there are no solutions to (59) in the four cases $p(\xi)=\xi^3$, $\nu=14$; $p(\xi)=\xi^2-\xi^3$, $\nu=13$; $p(\xi)=\xi^2+2\xi^3$, $\nu=-13$; $p(\xi)=\xi+\xi^2+\xi^3$, $\nu=11$. In the first case $n\equiv 14, -16 \bmod 60$; but

$$\xi^{14}=3-4\xi+3\xi^3, \qquad \xi^{-16}=-1-8\xi-8\xi^2-5\xi^3.$$

Since $\xi^{60}\equiv 1 \bmod 8$ (from (60)), (59) gives an impossible congruence modulo 8. Similar arguments dispose of the second and third cases, using

$$\xi^{13}=-1+3\xi^2-3\xi^3, \qquad \xi^{-17}=-9-8\xi-5\xi^2+\xi^3,$$
$$\xi^{-13}=8-3\xi^2-6\xi^3, \qquad \xi^{17}=4-4\xi-3\xi^2+6\xi^3.$$

In the last case $n \equiv 11, -19 \bmod 60$. Since $\xi^{11} = 2 - 3\xi + \xi^2 + \xi^3$, the case $n \equiv 11 \bmod 60$ is impossible, by taking (59) modulo 8. Then $n \equiv -19, 41 \bmod 120$. But $\xi^{-19} = -22 + \xi + 9\xi^2 + 17\xi^3$, $\xi^{41} = -198 + 153\xi + 233\xi^2 - 351\xi^3$, so using $\xi^{120} \equiv 1 \bmod 16$, (59) gives an impossible congruence modulo 16.

7.1. We give in the following sections the arithmetic details of the quartic fields $\mathbf{Q}(\theta)$. In each instance, the module generated over $\mathbf{Z}$ by $\{1, \theta, \phi, \Phi\}$ is the ring of integers of K. To show that ϕ, Φ are indeed integers, we simply give the minimal polynomials. It is easy to verify that 2 and 3 are the only primes which may divide the index of this module in the ring of integers. So it is then straightforward to check that $(a_0 + a_1\theta + a_2\phi + a_3\Phi)/p$, with $0 \leq a_i < p$, cannot be an integer for $p = 2, 3$, unless each a_i is zero. The explicit details are omitted.

Each quartic field has two real embeddings and one pair of complex embeddings into $\mathbf{C}$, so that there are indeed two fundamental units in K. The procedure we adopt to find a pair of fundamental units is as follows. First, find a pair of independent units. In each case, this was achieved by factoring ideals of small norm and suitably combining the factors to give units; independence follows from the non-vanishing of the regulator, and is easily verified in each of the specific instances below. Now normalize the independent units ϵ_1, ϵ_2 to satisfy $\epsilon_2 > \epsilon_1 > 1$. To show that ϵ_1, ϵ_2 are actually fundamental, we invoke the following theorem of Baulin [1].

THEOREM. *If there exist two independent units ϵ_1, ϵ_2 in K such that neither relation*

$$\epsilon_1 = \tau_1^m, \tag{63}$$

$$\epsilon_1^l \epsilon_2 = \tau_2^n \tag{64}$$

holds for any units τ_1, τ_2 and integers l, m, n, then ϵ_1, ϵ_2 are fundamental units.

So it is necessary in each instance to show the impossibility of relations (63) and (64) where clearly it may be supposed $m, n > 0$. We strengthen the technique used by London and Finkelstein [8] as follows. Clearly, it may be supposed in (64) that $|l| \leq n/2$, since putting $l = kn + l'$, $|l'| \leq n/2$, gives the relation $\epsilon_1^{l'}\epsilon_2 = (\tau_2\epsilon_1^{-k})^n$. We first give congruences modulo appropriate first degree primes in the relevant field K which show that (63) and (64) can have no solution if $m < n_0$ or $n < n_0$ for a fixed integer n_0. If now (63) and (64) are to hold, then there exist units τ_1, τ_2 such that

$$\tau_1 = \epsilon_1^{1/m}, \quad m \geq n_0, \tag{65}$$

$$\tau_2 = \epsilon_1^{l/n}\epsilon_2^{1/n}, \quad n \geq n_0, \quad |l| \leq n/2. \tag{66}$$

We can thus bound τ_i and its conjugates $\tau_i', \tau_i'', \overline{\tau_i''}$. Certainly

$$\tau_1 \leq \epsilon_1^{1/n_0}, \tag{67}$$

$$\tau_2 \leq \epsilon_1^{1/2}\epsilon_2^{1/n_0}, \tag{67'}$$

and conjugating (63) and (64) gives

$$|\tau_1'| = |\epsilon_1'|^{1/m} \leq \max(1, |\epsilon_1'|^{1/n_0}), \tag{68}$$

$$|\tau_2'| \leq \max(|\epsilon_1'|^{1/2}, |\epsilon_1'|^{-1/2}) \cdot \max(1, |\epsilon_2'|^{1/n_0}). \tag{69}$$

Similarly

$$|\tau_1''| = |\overline{\tau_1''}| \leq \max(1, |\epsilon_1''|^{1/n_0}), \tag{70}$$

$$|\tau_2''| = |\overline{\tau_2''}| \leq \max(|\epsilon_1''|^{1/2}, |\epsilon_1''|^{-1/2}) \cdot \max(1, |\epsilon_2''|^{1/n_0}). \tag{71}$$

In some cases, the bounds at (67′), (69), (71) may be rather weak, and so it can also be advantageous to consider two ranges for the value of l at (66) as follows.

First, if $|l| \leq n/4$, then we clearly obtain

$$\tau_2 \leq \epsilon_1^{1/4} \epsilon_2^{1/n_0}, \tag{72}$$

$$|\tau_2'| \leq \max(|\epsilon_1'|^{1/4}, |\epsilon_1'|^{-1/4}) \cdot \max(1, |\epsilon_2'|^{1/n_0}), \tag{73}$$

$$|\tau_2''| = |\overline{\tau_2''}| \leq \max(|\epsilon_1''|^{1/4}, |\epsilon_1''|^{-1/4}) \cdot \max(1, |\epsilon_2''|^{1/n_0}). \tag{74}$$

Second, suppose $n/4 < |l| \leq n/2$. Then we may write $n = k|l| + l'$ with $|l'| \leq |l|/2$, $2 \leq k \leq 4$. So raising (64) to the kth power gives the relation $\epsilon_1^{-l'|l|/l} \epsilon_2^k = (\tau_2^k \epsilon_1^{-|l|/l})^n$, that is, a relation

$$\tau_3 = \epsilon_1^{l''/n} \epsilon_2^{k/n}, \quad |l''| \leq n/4, \ 2 \leq k \leq 4. \tag{75}$$

Then we have the bounds

$$\tau_3 \leq \epsilon_1^{1/4} \epsilon_2^{4/n_0}, \tag{76}$$

$$|\tau_3'| \leq \max(|\epsilon_1'|^{1/4}, |\epsilon_1'|^{-1/4}) \cdot \max(1, |\epsilon_2'|^{4/n_0}), \tag{77}$$

$$|\tau_3''| = |\overline{\tau_3''}| \leq \max(|\epsilon_1''|^{1/4}, |\epsilon_1''|^{-1/4}) \cdot \max(1, |\epsilon_2''|^{4/n_0}). \tag{78}$$

The region defined by the bounds at (72), (73), (74) is a subset of the region at (76), (77), (78); and the region for the unit τ_1 defined by the bounds at (67), (68), (70) is a subset of the region for τ_2 at (67′), (69), (71). Accordingly, it suffices to determine all the units τ satisfying either the inequalities (67′), (69), (71) or the inequalities (76), (77), (78), whichever is the stronger. Let now $\tau = a + b\theta + c\phi + d\Phi$ represent either τ_2 or τ_3. Then the equations

$$\begin{aligned} a + b\theta + c\phi + d\Phi &= \tau, \\ a + b\theta' + c\phi' + d\Phi' &= \tau', \\ a + b\theta'' + c\phi'' + d\Phi'' &= \tau'', \\ a + b\overline{\theta''} + c\overline{\phi''} + d\overline{\Phi''} &= \overline{\tau''}, \end{aligned} \tag{79}$$

can be solved for a, b, c, d to give

$$
\begin{aligned}
d &= (D_1\tau + D_2\tau' + D_3\tau'' + D_4\overline{\tau''})/|\Delta|, \\
c &= (D_1\alpha\tau + D_2\alpha'\tau' + D_3\alpha''\tau'' + D_4\overline{\alpha''}\,\overline{\tau''})/|\Delta|, \qquad (80)\\
b &= (D_1\beta\tau + D_2\beta'\tau' + D_3\beta''\tau'' + D_4\overline{\beta''}\,\overline{\tau''})/|\Delta|,
\end{aligned}
$$

where Δ^2 is the discriminant $\Delta^2(K)$ of the field K; α, β are certain linear and quadratic functions respectively of θ; and $(-1)^i D_i$ is the determinant of the matrix obtained by deleting the ith column from the matrix

$$
\begin{pmatrix} 1 & 1 & 1 & 1 \\ \theta & \theta' & \theta'' & \overline{\theta''} \\ \phi & \phi' & \phi'' & \overline{\phi''} \end{pmatrix}
$$

Thus, the inequalities (67′), (69), (71) and (76), (77), (78) give explicit bounds on d, c, b at (80), whence a can be bounded directly from any of the equations at (79). The finitely many possibilities for τ can now be tested by computer to find the potential units; in no case do 'new' units occur, and ϵ_1, ϵ_2 being fundamental units then follows.

7.2.

$$K = \mathbf{Q}(\theta), \qquad \theta^4 - 72\theta^2 - 108\theta - 432 = 0.$$

$$\phi = \frac{\theta^2}{6}, \qquad \Phi = \frac{\theta^3}{36}, \qquad \Delta^2(K) = -2^2 \cdot 3^3 \cdot 229^2.$$

$$\phi^4 - 24\phi^3 + 120\phi^2 + 234\phi + 144 = 0; \qquad \Phi^4 - 9\Phi^3 - 333\Phi^2 + 189\Phi - 48 = 0.$$

Multiplication table:

$$
\begin{aligned}
\theta^2 &= 6\phi, & \phi^2 &= 12 + 3\theta + 12\phi, \\
\theta\phi &= 6\Phi, & \phi\Phi &= 2\theta + 3\phi + 12\Phi, \\
\theta\Phi &= 12 + 3\theta + 12\phi, & \Phi^2 &= 24 + 6\theta + 26\phi + 3\Phi.
\end{aligned}
$$

Units:

$$\eta_1 = 31 + 11\theta + 38\phi + 24\Phi; \qquad \eta_1^{-1} = -17 + 25\theta + 4\phi - 12\Phi;$$

$$\eta_2 = 483602731 + 174202120\theta + 316187252\phi - 293718704\Phi$$

(η_2 arises from the identity

$$\eta_1^5\eta_2(4 + 5\theta + 2\phi - \Phi)(1 + \theta + 2\phi + \Phi)^2 = (2 + 3\phi - 2\Phi)^4).$$

Now (3) factors in K as $\mathfrak{p}_3^4$ so that the multiplicative group $\mathfrak{G}_3$ of residues modulo 3 has order 54. It is easily checked that η_1 has order 3 modulo 3, η_2 has order 9 modulo 3, and the residues $\eta_1^\rho\eta_2^\sigma$ mod 3, for $0 \le \rho \le 2$, $0 \le \sigma \le 8$, are all distinct. So $\mathfrak{G}_3$ is generated by the residues of η_1, η_2 mod 3, together with -1. If ϵ_1, ϵ_2 are fundamental units in K, then the subgroup of $\mathfrak{G}_3$ generated by $\epsilon_1, \epsilon_2, -1$ certainly contains η_1, η_2 mod 3 and so is precisely $\mathfrak{G}_3$. Thus there exist fundamental units congruent modulo 3 to η_1, η_2.

7.3.

$$K=\mathbf{Q}(\theta),\qquad \theta^4-68\theta^3+366\theta^2-680\theta+397=0.$$

$$\phi=\frac{(\theta+1)^2}{6},\qquad \Phi=\frac{(\theta+1)^3}{36},\qquad \Delta^2(K)=-2^2\cdot 3^3\cdot 229^2.$$

$$\phi^4-672\phi^3+2820\phi^2-4086\phi+1764=0;$$

$$\Phi^4-7047\Phi^3+14139\Phi^2-10989\Phi+2058=0.$$

Multiplication table:

$\theta^2=-1-2\theta+6\phi,$

$\theta\phi=-\phi+6\Phi,$

$\theta\Phi=3+45\theta-96\phi+71\Phi,$

$\epsilon_1=251-776\theta+916\phi-80\Phi;$

$\epsilon_2=145415-218888\theta$
$+214656\phi-18432\Phi,$

$\phi^2=3+45\theta-96\phi+72\Phi,$

$\phi\Phi=29+533\theta-1107\phi+768\Phi,$

$\phi^2=300+5676\theta-11755\phi+8109\Phi.$

$\epsilon_1^{-1}=3+56\theta-116\phi+80\Phi,$

$\epsilon_2^{-1}=-9+8\theta.$

Congruences: The appropriate first degree prime factor of p is identified by the residue class of θ.

p	13	19	31	43	61	71		79	83		89		103	139	149		173
θ	3	17	26	13	44	30	32	55	42	74	47	84	74	130	16	31	50
ϕ	7	16	13	4	2	30	4	75	73	66	28	62	62	57	73	121	1
Φ	9	10	12	38	15	13	22	68	39	78	46	18	54	63	33	99	95
ϵ_1	1	3	13	32	45	3	43	54	33	31	76	31	37	58	62	141	93
ϵ_2	7	3	12	24	53	4	23	11	33	42	81	69	50	12	144	101	50

p	229	233	239	277	313	349	373	397	419	659		1117
θ	109	125	164	205	130	239	155	0	399	204	235	323
ϕ	32	83	116	240	304	177	326	331	130	524	496	741
Φ	205	112	83	207	273	100	270	386	147	330	618	919
ϵ_1	27	143	88	131	121	329	327	225	324	299	45	750
ϵ_2	108	79	135	134	44	148	10	296	119	121	516	606

We take $n_0=53$, and for each prime value of n less than 53 indicate which congruences mod p show the impossibility of $\pm\epsilon_1^l\epsilon_2=\tau^n$, $|l|\le n/2$: $n=2$, $p=13$; $n=3$, $p=13,19$; $n=5$, $p=31,61$; $n=7, p=43,71$; $n=11$, $p=89,397$; $n=13$, $p=79,313$; $n=17$, $p=103,239$; $n=19$, $p=229,419$; $n=23$, $p=139,277$; $n=29$, $p=233,349$; $n=31$, $p=373,1117$; $n=37$, $p=149$; $n=41$, $p=83$; $n=43$, $p=173$; $n=47$, $p=659$.

Real values (all calculations were performed with quadruple precision): the exponent of 10 is given in brackets at the end of the number.

$$\theta \sim 1.1250022(0), \quad \theta' \sim 6.2298637(1), \quad \theta'' \sim 2.2881802(0)+6.5474585(-1)i,$$

$$\epsilon_1 \sim 4.6061280(1), \quad \epsilon_1' \sim 2.0423669(-6), \quad \epsilon_1'' \sim -9.0306409(0)+1.0270527(2)i,$$

$$\epsilon_2 \sim 5.5803835(4), \quad \epsilon_2' \sim 2.0433639(-3), \quad \epsilon_2'' \sim 8.1606967(-2)-4.5935980(-2)i.$$

The polynomials α, β at (80) are given by $\alpha = (-71+\theta)/6$, $\beta = (505-70\theta+\theta^2)/36$.

The bounds resulting on a, b, c, d using (76)-(78) are:

$$|a| \le 91, \qquad |b| \le 44, \qquad |c| \le 47, \qquad |d| \le 4.$$

The only units in the range are $1, \epsilon_2^{-1}$.

7.4.

$$K = \mathbf{Q}(\theta), \qquad \theta^4+22\theta^3-12\theta^2-32\theta-188=0.$$

$$\phi = \frac{\theta^2+2\theta+4}{6}, \qquad \Phi = \frac{\theta^3-3\theta^2+4}{18}, \qquad \Delta^2(K) = -2^4\cdot 3^3\cdot 229^2.$$

$$\phi^4-80\phi^3+198\phi^2-26\phi+1=0; \qquad \Phi^4+714\Phi^3-1260\Phi^2+768\Phi-21=0.$$

Multiplication table:

$$\theta^2 = -4-2\theta+6\phi, \qquad \phi^2 = 11+3\theta-5\phi-9\Phi,$$

$$\theta\phi = -4-\theta+5\phi+3\Phi, \qquad \phi\Phi = -107-29\theta+72\phi+86\Phi,$$

$$\theta\Phi = 30+9\theta-21\phi-25\Phi, \qquad \Phi^2 = 991+269\theta-667\phi-795\Phi.$$

Units:

$$\epsilon_1 = \phi; \qquad \epsilon_1^{-1} = 10-3\theta-\phi;$$

$$\epsilon_2 = 95+84\theta+208\phi+20\Phi; \qquad \epsilon^{-1} = 38575+104600\theta-25952\phi-30980\Phi.$$

Congruences:

p	7	13	17	19	23		31	43	61	71	79	131
θ	6	9	4	1	7	20	28	16	18	29	70	8
ϕ	4	2	16	17	15	5	27	20	20	44	77	14
Φ	0	6	3	17	6	10	11	37	33	8	34	18
ϵ_1	4	2	16	17	15	5	27	20	20	44	77	103
ϵ_2	3	3	11	8	13	2	6	18	22	57	77	109

We take $n_0 = 17$; and with the notation of §7.3, $n=2$, $p=13, 17$; $n=3$, $p=7, 19$; $n=5$, $p=31, 61$; $n=7$, $p=43, 71$; $n=11$, $p=23$; $n=13$, $p=79, 131$.

Real values:

$$\theta \sim 2.3901604(0), \quad \theta' \sim -2.2486894(1), \quad \theta'' \sim -9.5163306(-1)+1.6100452(0)i,$$

$$\epsilon_1 \sim 2.4155312(0), \quad \epsilon_1' \sim 7.7447771(1), \quad \epsilon_1'' \sim 6.8348944(-2)+2.5957655(-2)i,$$

$$\epsilon_2 \sim 7.9877738(2), \quad \epsilon_2' \sim 5.008078(-8), \quad \epsilon_2'' \sim 4.6611311(1)+1.5108032(2)i.$$

The polynomials α, β at (80) are given by $\alpha=(25+\theta)/3$, $\beta=(-62+20\theta+\theta^2)/18$.
The bounds resulting on a, b, c, d using (67′), (69), (71) are:

$$|a|\leq 11, \qquad |b|\leq 3, \qquad |c|\leq 6, \qquad d=0.$$

The only units in the range are $1, \epsilon_1, \epsilon_1^{-1}$.

7.5.

$$K=\mathbf{Q}(\theta), \qquad \theta^4-40\theta^3+108\theta^2-92\theta-52=0,$$

$$\phi=\frac{\theta^2+2}{6}, \qquad \Phi=\frac{\theta^3-26\theta^2+14\theta-4}{54}, \qquad \Delta^2(K)=-2^4\cdot 3\cdot 229^2.$$

$$\phi^4-232\phi^3+348\phi^2-246\phi+54=0; \qquad \Phi^4-294\Phi^3-292\Phi^2-552\Phi-120=0.$$

Multiplication table:

$$\theta^2=-2+6\phi, \qquad \phi^2=-46-13\theta+156\phi+60\Phi,$$

$$\theta\phi=-8-2\theta+26\phi+9\Phi, \qquad \phi\Phi=-58-16\theta+198\phi+78\Phi,$$

$$\theta\Phi=-8-2\theta+30\phi+14\Phi, \qquad \Phi^2=-76-22\theta+256\phi+98\Phi.$$

Units:

$$\epsilon_1=-807-11300\theta+5635\phi+1620\Phi; \qquad \epsilon_1^{-1}=-6743-197050\theta-115\phi+2595\phi;$$

$$\epsilon_2=-120697-338780\theta+409864\phi+159264\Phi;$$

$$\epsilon_2^{-1}=74367-769540\theta+60800\phi-38064\Phi.$$

Congruences:

p	5	7	13	29		31	41	53		67	331
θ	3	6	0	6	12	13	10	32	14	21	226
ϕ	1	4	9	16	5	13	17	12	33	18	238
Φ	4	5	11	15	28	16	23	16	13	3	44
ϵ_1	3	2	11	8	8	9	39	22	12	13	40
ϵ_2	4	2	6	17	26	27	3	8	47	1	12

We take $n_0=17$; and with notation as above, $n=2$, $p=5,41$; $n=3$, $p=7,13$; $n=5$, $p=31,41$; $n=7$, $p=29$; $n=11$, $p=67,331$; $n=13$, $p=53$.
Real values:

$$\theta\sim 3.7161391(1), \quad \theta'\sim -3.7596381(-1), \quad \theta''\sim 1.6072864(0)+1.0670220(0)i,$$

$$\epsilon_1\sim 1.7339328(6), \quad \epsilon_1'\sim 1.2391714(3), \quad \epsilon_1''\sim -1.8365571(-5)+1.1318855(-5)i,$$

$$\epsilon_2\sim 1.4007416(8), \quad \epsilon_2'\sim 7.4540294(-6), \quad \epsilon_2''\sim -3.0469625(-2)-5.4174817(-3)i.$$

The polynomials α, β at (80) are given by $\alpha=(-14+\theta)/9$; $\beta=(94-40\theta+\theta^2)/54$.
The bounds resulting on a, b, c, d using (76)–(78) are:

$$|a|\leq 22, \qquad |b|\leq 12, \qquad |c|\leq 24, \qquad |d|\leq 14$$

The only unit in the range is 1.

7.6.

$$K = \mathbf{Q}(\theta), \qquad \theta^4 + 4\theta^3 - 90\theta^2 + 216\theta - 459 = 0.$$

$$\phi = \frac{\theta^2 - 2\theta + 3}{6}, \qquad \Phi = \frac{\theta^3 + \theta^2 + 15\theta - 45}{108}, \qquad \Delta^2(K) = -2^2 \cdot 3 \cdot 229^2.$$

$$\phi^4 - 36\phi^3 + 138\phi^2 + 126\phi + 27 = 0; \qquad \Phi^4 + 17\Phi^3 - 52\Phi^2 - 50\Phi - 18 = 0.$$

Multiplication table:

$$\theta^2 = -3 + 2\theta + 6\phi, \qquad \phi^2 = -6 + 3\theta + 18\phi - 24\Phi,$$

$$\theta\phi = 9 - 3\theta - 3\phi + 18\Phi, \qquad \phi\Phi = 9 - 3\theta - 8\phi + 21\Phi,$$

$$\theta\Phi = 6\phi - 3\Phi, \qquad \Phi^2 = -2 + \theta + 7\phi - 9\Phi.$$

Units:

$$\epsilon_1 = 179 - 113\theta + 27\phi + 126\Phi; \qquad \epsilon_1^{-1} = 6089 - 2330\theta - 9363\phi + 17424\Phi;$$

$$\epsilon_2 = 6087998 - 1285904\theta + 3940781\phi + 7498800\Phi$$

$$\epsilon_2^{-1} = 4337 - 1661\theta - 6653\phi + 12390\Phi.$$

Congruences:

p	13	29		31	41	43	67	79	89	131
θ	7	8	18	14	14	16	27	37	12	47
ϕ	2	23	5	13	8	2	46	32	65	91
Φ	9	2	18	21	39	21	36	68	26	100
ϵ_1	4	3	26	13	37	39	25	58	27	100
ϵ_2	8	13	7	1	14	10	22	35	28	39

We take $n_0 = 17$; and for $n = 2$, $p = 13, 29$; $n = 3$, $p = 13, 43$; $n = 5$, $p = 31, 41$; $n = 7$, $p = 29$; $n = 11$, $p = 67, 89$; $n = 13$, $p = 79, 131$.

Real values:

$$\theta \sim 6.4593879(0), \quad \theta' \sim -1.2672530(1), \quad \theta'' \sim 1.1065711(0) + 2.0935268(0)i,$$

$$\epsilon_1 \sim 1.5855978(1), \quad \epsilon_1' \sim -1.6678785(-6), \quad \epsilon_1'' \sim -8.9279882(0) - 1.9425091(2)i,$$

$$\epsilon_2 \sim 4.3884124(7), \quad \epsilon_2' \sim -2.3466788(-6), \quad \epsilon_2'' \sim -5.6011315(-2) + 8.1075148(-2)i.$$

The polynomials α, β at (80) are given by $\alpha = (3 + \theta)/18$; $\beta = (-99 + 6\theta + \theta^2)/108$.

The bounds resulting on a, b, c, d using (76)–(78) are:

$$|a| \leq 32, \qquad |b| \leq 5, \qquad |c| \leq 12, \qquad |d| \leq 24.$$

The only unit in the range is 1.

7.7.

$$K = \mathbf{Q}(\theta), \qquad \theta^4 + 20\theta^3 - 126\theta^2 + 216\theta - 243 = 0.$$

$$\phi = \frac{\theta^2+2\theta+3}{6}, \qquad \Phi = \frac{\theta^3+2\theta^2-27\theta}{54}, \qquad \Delta^2(K) = -2^4\cdot 3\cdot 229^2.$$

$$\Phi^4-104\phi^3+504\phi^2-566\phi+418=0; \qquad \Phi^4+266\Phi^3+418\Phi^2+312\Phi+81=0.$$

Multiplication table:

$$\theta^2 = -3-2\theta+6\phi, \qquad \phi^2 = -7-27\theta+28\phi-24\Phi,$$

$$\theta\phi = 5\theta+9\Phi, \qquad \phi\Phi = 17+66\theta-58\phi+71\Phi,$$

$$\theta\Phi = -3-18\theta+15\phi-18\Phi, \qquad \Phi^2 = -44-177\theta+154\phi-190\Phi.$$

Units:

$$\epsilon_1 = 36-1380\theta+2950\phi+1065\Phi; \quad \epsilon^{-1} = -18209+480\theta+4475\phi+1560\Phi;$$

$$\epsilon_2 = 1552-30543\theta+68814\phi+28686\Phi; \quad \epsilon_2^{-1} = -614-2505\theta+2178\phi-2676\Phi.$$

Congruences:

p	11		13	19	23		29		41	47		59		79	103	137	149	157
θ	1	7	9	12	18	20	5	25	14	4	10	16	45	6	70	10	114	41
ϕ	1	0	4	0	3	1	16	26	31	28	44	19	58	48	68	89	44	85
Φ	2	1	12	6	19	9	19	10	4	5	12	38	29	55	78	2	47	33
ϵ_1	7	10	2	12	3	13	19	19	2	3	36	18	32	40	58	69	72	131
ϵ_2	10	5	2	2	3	5	3	11	11	42	10	37	21	18	69	92	69	34

p	191		223	373	683	739	821	941		947	
θ	30	123	16	108	181	37	297	198	832	746	767
ϕ	65	80	160	302	57	241	23	484	376	38	132
Φ	9	70	3	207	211	67	594	187	630	210	301
ϵ_1	104	79	15	11	374	410	2	593	615	457	37
ϵ_2	166	169	160	203	34	12	152	767	202	805	574

We take $n_0=53$; and for $n=2$, $p=13,41$; $n=3$, $p=13,19$; $n=5$, $p=11$; $n=7$, $p=29$; $n=11$, $p=23$; $n=13$, $p=79,157$; $n=17$, $p=103,137$; $n=19$, $p=191$; $n=23$, $p=47$; $n=29$, $p=59$; $n=31$, $p=373,683$; $n=37$, $p=149,223$; $n=41$, $p=739,821$; $n=43$, $p=947$; $n=47$, $p=941$.

Real values:

$$\theta \sim 3.5899700(0), \quad \theta' \sim -2.5326689(1), \quad \theta'' \sim 8.6835938(-1)+1.3851249(0)i,$$

$$\epsilon_1 \sim 5.9327085(3), \quad \epsilon_1' \sim 4.5321292(4), \quad \epsilon_1'' \sim 5.9499101(-5)-1.3379673(-5)i,$$

$$\epsilon_2 \sim 1.4324827(5), \quad \epsilon_2' \sim 1.0142277(-6), \quad \epsilon_2'' \sim 1.3319892(-1)-2.6201560(0)i.$$

The polynomials α, β at (80) are given by $\alpha=(18+\theta)/9$, $\beta=(-135+18\theta+\theta^2)/54$.

The bounds resulting on a, b, c, d using (76)-(78) are:

$$|a| \le 72, \qquad |b| \le 18, \qquad |c| \le 22, \qquad |d| \le 10.$$

The only unit in the range is 1.

REFERENCES

1. V. I. Baulin, *On an indeterminate equation of the third degree with least positive discriminant* (Russian), Tul'sk. Gos. Ped. Inst. Učen. Zap. Fiz.-Mat. Nauk Vyp. 7 (1960), 138–170.
2. B. D. Beach, H. C. Williams, and C. R. Zarnke, *Some computer results on units in quadratic and cubic fields*. Proceedings of the Twenty-Fifth Summer Meeting Canadian Mathematical Congress (Lakehead Univ., Thunder Bay, Ont., 1971), 609–648, Lakehead Univ., Thunder Bay, Ont., 1971.
3. A. Bremner, *Solution of a problem of Skolem,* J. Number Theory 9 (1977), 499–501.
4. ———, *A Diophantine equation arising from tight 4-designs,* Osaka J. Math. 16 (1979), 353–356.
5. A. Bremner and N. Tzanakis, *Integer points on* $y^2 = x^3 - 7x + 10$, Math. Comp. 41 (1983), 731–741.
6. K. Györy, *Sur les polynômes à coefficients entiers et de discriminant donné,* III, Publ. Math. Debrecen 23 (1976), 141–165.
7. W. Ljunggren, *Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante,* Acta Math. 75 (1942), 1–21.
8. H. London and R. Finkelstein, *On Mordell's equation* $y^2 - k = x^3$, Bowling Green State Univ. Press, Bowling Green, Ohio, 1973.
9. L. J. Mordell, *Diophantine equations,* Academic Press, London, 1969.
10. T. Nagell, *Sur les discriminants des nombres algébriques,* Ark. Mat. 7 (1967), 265–282.
11. ———, *Sur les unités dans les corps biquadratiques primitifs du premier rang,* Ark. Mat. 7 (1967), 359–394.
12. Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen,* 8 de Skand. Mat. Kongress, Stockholm, 1934, 163–188.
13. N. Tzanakis, *The Diophantine equation* $x^3 - 3xy^2 - y^3 = 1$ *and related equations,* J. Number Theory 18 (1984), 192–205.

Department of Mathematics
Arizona State University
Tempe, Arizona 85287