Pacific Journal of Mathematics

FUNDAMENTAL UNITS AND CYCLES IN THE PERIOD OF REAL QUADRATIC NUMBER FIELDS. II

Leon Bernstein

Vol. 63, No. 1 March 1976

PACIFIC JOURNAL OF MATHEMATICS
Vol. 63, No. 1, 1976

FUNDAMENTAL UNITS AND CYCLES IN THE PERIOD OF REAL QUADRATIC NUMBER FIELDS

LEON BERNSTEIN

PART II

1. Fundamental unit in $Q(\sqrt{M})$ from the expansion of $\sqrt{M}$. In the first part of this paper we succeeded to state explicitly the periodic expansion of $\sqrt{M}$, M a squarefree natural number, for infinitely many classes $\sqrt{M}$, each containing infinite many numbers. There are 14 types of these infinitely many classes, and they will all be enumerated here for the calculation of the fundamental unit $e_f, |e_f|>1$, of the quadratic field $Q(\sqrt{M})$. There are many ways to calculate e_f. Many an elaborate mathematician like G. Degert [4] and H. Yokoi [7] have done so by finding the smallest solution of Pell's equation $x^2 - My^2 = 1$, or $x^2 - My^2 = \pm 4$, if the latter is solvable which necessitates $M \equiv 1 (\mathrm{mod}\, 4)$. Now to solve Pell's equation, poses another problem. If the expansion of $\sqrt{M}$ as a periodic continued fraction is known, the problem is solved. For numerical values of M, this causes arithmetic difficulties only. If M is just a symbol standing for any natural number, the challenge of stating the periodic expansion of $\sqrt{M}$ explicitly as a function of $\sqrt{M}$, has yet not been taken by mathematicians, except in a few cases enumerated by O. Perron [5]. These few cases have recently been enriched by a brilliant paper by Yamamoto [6], and by the author in [3]. Of course, $M = D^2 + d$, $1 \leqq d \leqq 2D$, and the author conjectures that if we know a functional relationship $D = D(d)$, the periodic expansion can be stated explicitly, as was indeed demonstrated by the author in the first part of this paper for certain arithmetic functions $D(d)$. But if the expansion of $\sqrt{M}$ as a periodic continued fraction is stated explicitly, the fundamental unit e_f of $Q(\sqrt{M})$ can be also stated explicitly by methods which are generally known, and will be briefly reviewed here. We shall also restate the notations and formulas of the first part of this paper of which we shall frequently make use here.

$$(15.1)\quad \begin{cases} \text{(i)}\ \sqrt{M} = w = x = \dfrac{w + P_0}{Q_0} = b_0 + \dfrac{1}{x_1};\ P_0 = 0;\ Q_0 = 1\,; \\ \qquad b_0 = [w]\,; \\ \text{(ii)}\ x_k = \dfrac{w + P_k}{Q_k} = b_k + \dfrac{1}{x_{k+1}};\ P_k = b_{k-1}Q_{k-1} - P_{k-1}\,; \end{cases}$$

$$\left\{\begin{aligned} &Q_{k-1}Q_k = M - P_k^2;\ b_k = [x_k];\ k = 1, 2, \cdots ,\\ \text{(iii)}\quad &(w + P_{k-1})(w + P_k) = Q_{k-1}[Q_k + b_{k-1}(w + P_k)] ;\\ &x_{k-1}x_k = \frac{Q_{k-}b_{k-1}(w + P_k)}{Q_k};\ k = 1, 2, \cdots . \end{aligned}\right.$$

It is especially formula (15.1), (iii) we shall use most frequently here. We shall also use the notation we have introduced in previous papers [1] for the $n-1$-dimensional Jacobi-Perron algorithm and which should be retained for the Euclidean algorithm when $n = 2$, viz.,

$$\text{(15.2)}\quad \begin{cases} \text{(i)} & A_i^{(v)} = \delta_{iv},\ (i,\ v = 0,\ 1;\ \delta_{iv} \text{ is Kronecker's symbol}) .\\ \text{(ii)} & A_i^{(v+2)} = A_i^{(v)} + b_v A_i^{(v+1)},\ (i = 0,\ 1;\ v = 0, 1, \cdots) .\\ \text{(iii)} & A_1^{(v+1)2} - MA_0^{(v+1)2} = (-1)^v Q_v,\ (v = 0, 1, \cdots) . \end{cases}$$

If m is the length of the primitive period of the expansion of $\sqrt{M}$ as a periodic continued fraction, we obtain from (15.2), (iii), since $Q_{tm} = 1,\ (t = 1, 2, \cdots)$

(15.3) All solution vectors of Pell's equation $x^2 - My^2 = (-1)^{mt}$, are given by $(A_1^{(mt+1)}, A_0^{)mt+1)})$; $e_f = A_1^{(m+1)} + A_0^{(m+1)}w$ is a unit in $Q(w)$, $w = \sqrt{M}$.

From

$$w = \frac{A_1^{(m)} + x_m A_1^{(m+1)}}{A_0^{(m)} + x_m A_0^{(m+1)}} = \frac{A_1^{(m)} + (w + b_0)A_1^{(m+1)}}{A_0^{(m)} + (w + b_0)A_0^{(m+1)}}$$

we obtain $A_1^{(m+1)} = A_0^{(m)} + b_0 A_0^{((m+1)}$; hence

$$\text{(15.4)}\qquad e_f = A_0^{(m)} + (w + b_0)A_0^{(m+1)} = A_0^{(m)} + x_m A_0^{(m+1)} .$$

(15.5) If $Q_{v_0} = 4$, then the smallest solution vector of Pell's equation $x^2 - My^2 = (-1)^v 4$ is given by $(A_1^{(v_0+1)}, A_0^{(v_0+1)})$; if $M \equiv 1 (\mathrm{mod}\ 4)$, $e_f' = \frac{1}{2}(A_1^{(v_0+1)} + wA_0^{(v_0+1)})$ is a unit in $Q(w)$, $w = \sqrt{M}$.

As above, we obtain

$$\frac{1}{2}e_f' = A_0^{(v_0)} + x_{v_0} A_0^{(v_0+1)} .$$

In [2] the author proved (for the Jacobi-Perron, hence for the Euclidean algorithm)

$$\text{(15.6)}\qquad \prod_{i=1}^{v} x_i = A_0^{(v)} + x_v A_0^{(v+1)} .$$

Since $(A_1^{(m+1)}, A_0^{(m+1)}))$, $(A_1^{(v_0+1)}, A_0^{(v_0+1)})$ are the smallest solution vectors of the corresponding Pellian equations.

THEOREM 15. *If $M \not\equiv 1 \pmod 4$, or if no Q_v in the expansion of $\sqrt{M}$ as a periodic continued fraction equals 4, the fundamental unit of the field $Q(w)$, $w^2 = M$, is given by*

$$e_f = \prod_{i=1}^{m} x_i \,, \tag{15.7}$$

where m is the length of the primitive period of the expansion of w. If $M \equiv 1 \pmod 4)$ and $Q_{v_0} = 4$, the fundamental unit of the field $Q(w)$, $w^2 = M$, is given by

$$e_f = \prod_{i=1}^{v_0} x_i \,. \tag{15.8}$$

As H. Zassenhaus [8] has pointed out, this is the most effective method to calculate e_f.

16. Fundamental unit of $Q(w)$, $w^2 = [(2a+1)^k + a]^2 + 2a + 1$; $a, k \geqq 1$. From Theorem 1, Part I, we recall that the length of the primitive period of the expansion of w equals $6k$. Since, as can be easily verified by the reader, $w^2 \equiv 1 \pmod 4$, the fundamental unit of $Q(w)$, according to (15.7), is given by

$$\frac{1}{2} e_f = \prod_{i=1}^{6k} x_i \,. \tag{16.1}$$

Taking into account formulas (0.9), (0.11), (0.13) and (15.1) and the structures of the x_i from §1, we obtain

$$e_f = x_1^2 \Big(\prod_{s=1}^{k-1} x_{3s-1} x_{3s} x_{3s+1} \Big)^2 Q_{3k} (x_{3k-1} x_{3k})^2 \,. \tag{16.2}$$

From (1.8), (i), (ii) we obtain, with formulas (15.1), (iii),

$$x_{3s-1} x_{3s} = \frac{(w + P_{3s-1})(w + P_{3s})}{Q_{3s-1} Q_{3s}} = \frac{Q_{3s} + b_{3s-1}(w + P_{3s})}{Q_{3s}} \,;$$

but $b_{3s-1} = 1$; $Q_{3s} = 2A^{k-s}$; $P_{3s} = A^k - 2A^{k-s} + (a+1)$; hence

$$x_{3s-1} x_{3s} = \frac{w + A^k + (a+1)}{2A^{k-s}} \,. \qquad (A = 2a+1) \tag{16.3}$$

Since $P_{3s+1} = A^k - (a+1)$; $Q_{3s+1} = A^{s+1}$, we obtain from (16.3)

$$x_{3s-1} x_{3s} x_{3s+1} = \frac{w + A^k + (a+1)}{2A^{k-s}} \cdot \frac{w + A^k - (a+1)}{A^{s+1}}$$

$$= \frac{w^2 + 2A^k w + A^{2k} - (a+1)^2}{2A^{k+1}}$$

$$= \frac{A^{2k} + 2aA^k + (a+1)^2 + 2A^k w + A^{2k} - (a+1)^2}{2A^{k+1}}$$

$$= \frac{2A^{2k} + 2aA^k + 2A^k w}{2A^{k+1}},$$

(16.4) $$x_{3s-1}x_{3s}x_{3s+1} = \frac{w + A^k + a}{A}.$$

We further obtain $x_{3k-1}x_{3k} = (Q_{3k} + b_{3k-1}(w + P_{3k}))/Q_{3k}$, and since $Q_{3k} = 2$, $b_{3k-1} = 1$, $P_{3k} = A^k - 2 + a + 1$,

(16.5) $$x_{3k-1}x_{3k} = \frac{w + A^k + a + 1}{2}.$$

We further have, from (1.3)

(16.6) $$x_1 = \frac{w + A^k + a}{A}.$$

Substituting the values of the x_i from (16.3)-(16.6) in (16.2), we obtain

(16.7) $$e_f = \left(\frac{w + A^k + a}{A}\right)^2 \cdot \left(\frac{w + A^k + a}{A}\right)^{2(k-1)} \cdot 2 \cdot \left(\frac{w + A^k + a + 1}{2}\right)^2,$$
$$e_f = \left(\frac{w + A^k + a}{A}\right)^2 \cdot \frac{(w + A^k + a + 1)^2}{2}.$$

Since the conjugate e'_f of e_f equals

$$\left(\frac{-w + A^k + a}{A}\right)^{2k} \cdot \frac{(-w + A^k + a + 1)^2}{2},$$

we verify that the norm of e_f is 1 by

$$N(e_f) = \left[\frac{(A^k + a)^2 - w^2}{A^2}\right]^{2k} \cdot \frac{[(A^k + a + 1)^2 - w^2]^2}{4}$$

$$= \left[\frac{(A^k + a)^2 - \{(A^k + a)^2 + A\}}{A^2}\right]^{2k} \cdot \frac{[(A^k + a + 1)^2 - \{(A^k + a)^2 + A\}]^2}{4}$$

$$= \frac{1}{4A^{2k}} \cdot [(A^k + a)^2 + 2(A^k + a) + 1 - (A^k + a)^2 - A]^2$$

$$= \frac{1}{4A^{2k}} \cdot 4A^{2k} = 1.$$

17. Fundamental unit of $Q(w)$, $w = \sqrt{(A^k - a)^2 + A}$; $A = 2a + 1$, $a, k \geqq 1$. From Theorem 2 we recall that the length of the primitive period of the expansion of w equals $6k - 2$. Since, $w^2 \equiv 1 (\mathrm{mod}\, 4)$, for $a = 2u$, $Q_v = 4$ is possible. But the reader will verify easily from formulas (2.1) to (2.4), that Q is either odd or of the form $2t$, $t = 2s + 1$. Thus the fundamental unit of $Q(w)$, according to (15.7) is given by the formula

$$e_f = \prod_{i=1}^{6k-2} x_i \, . \tag{17.1}$$

Though the cycle in the expansion of w is $(x_{3s-2}, x_{3s-1}, x_{3s})$, we shall arrange it in the form $(x_{3s-1}, x_{3s}, x_{3s+1})$, $s = 1, 2, \cdots, k-1$, leaving x_1 outside the cycles, but including x_{3k-2}. This is done in order to have $b_{3s} = 1$ not at the end of the cycle while making use of formula (15.1), (iii). We then obtain from (17.1)

$$e_f = x_1^2 \left(\prod_{s=1}^{k-1} x_{3s-1} x_{3s} x_{3s+1} \right)^2 x_{3k-1} x_{3k} \, . \tag{17.2}$$

From (2.3) we obtain, with formula (15.1), (iii),

$$x_{3s} x_{3s+1} = \frac{Q_{3s+1} + b_{3s}(w + P_{3s+1})}{Q_{3s+1}} = \frac{w + A^k + (a+1)}{A^{s+1}} \, . \tag{17.3}$$

We further obtain in virtue of (17.3)

$$\tag{17.4} \left\{ \begin{aligned} & x_{3s-1} x_{3s} x_{3s+1} \\ & \quad = \frac{w + A^k + (a+1)}{A^{s+1}} \cdot \frac{w + A^k - (a+1)}{2A^{k-s}} = \frac{(w + A^k)^2 - (a+1)^2}{2A^{k+1}} \\ & \quad = \frac{A^{2k} - 2aA^k + (a+1)^2 + 2A^k w + A^{2k} - (a+1)^2}{2A^{k+1}} \\ & \quad = \frac{2A^k w + 2A^{2k} - 2aA^k}{2A^{k+1}} \, , \\ & x_{3s-1} x_{3s} x_{3s+1} = \frac{w + A^k - a}{A} \, . \end{aligned} \right.$$

We further have from (2.3) and since $Q_{3k-1} = 2$, $P_{3k-1} = P_{3k} = A^k - (a+1)$

$$x_1 = \frac{w + A^k - a}{A} ; \; x_{3k-1} x_{3k} = \frac{[w + A^k - (a+1)]^2}{2} \, . \tag{17.5}$$

From (17.2), (17.4), (17.5) we now obtain

$$\underline{\underline{e_f = \left(\frac{w + A^k - a}{A} \right)^{2k} \frac{[w + A^k - (a+1)]^2}{2}}} \, . \tag{17.6}$$

We also have, as before,

$$N(e_f) = 1 \, . \tag{17.7}$$

18. Fundamental unit of $Q(w)$, $w^2 = (A^k + a + 1)^2 - A$; $A = 2a + 1$; $a, k \geqq 1$. From Theorem 3 we recall that the length of the primitive period of the expansion of w as a continued fraction equals $4k + 2$. The reader will verify easily from § 3, that in this expansion Q_v cannot equal 4 for any v. Hence, according to (15.7), the fundamental unit of $Q(w)$ is given by

$$e_f = \prod_{i=1}^{4k+2} x_i \, . \tag{18.1}$$

From (3.3), we obtain

$$P_{2s-1} = A^k + a,\ Q_{2s-1} = 2A^{k-s+1};\ P_{2s} = A^k - a,\ Q_{2s} = A^s ;$$
$$s = 1, \cdots, k-1;\ Q_{2k+1} = 2 \, .$$

Thus

$$e_f = \left(\prod_{s=1}^{k} x_{2s-1}x_{2s}\right)^2 2x_{2k+1}^2 \, . \tag{18.2}$$

Now

$$\begin{cases} x_{2s-1}x_{2s} = \dfrac{w + A^k + a}{2A^{k-s+1}} \cdot \dfrac{w + A^k - a}{2A^s} = \dfrac{(w + A^k)^2 - a^2}{2A^{k+1}} \\ \qquad = \dfrac{A^{2k} + 2(a+1)A^k + a^2 + 2A^k w + A^{2k} - a^2}{2A^{k+1}} \, , \\ x_{2s-1}x_{2s} = \dfrac{w + A^k + (a+1)}{A} (s = 1, \cdots, k) \, . \end{cases} \tag{18.3}$$

Also

$$x_{2k+1} = \frac{A^k + a}{2} \, . \tag{18.4}$$

From (18.2), (18.3), (18.4) we now obtain

$$\underline{\underline{e_f = \left[\frac{w + A^k + (a+1)}{A}\right]^{2k} \frac{(w + A^k + a)^2}{2}}};\ N(e_f) = 1 \, . \tag{18.5}$$

19. Fundamental unit of $Q(w)$, $w^2 = [A^k - (a + 1)]^2 - A$; $A = 2a + 1$, $a, k \geqq 2$. From Theorem 4 we recall that the length of the primitive period of the expansion of w as a periodic continued fraction equals $4(2k - 1)$. The reader will verify easily from § 4 that in the expansion of no Q_v can equal 4 for any v. Hence, according to (15.7), the fundamental unit of $Q(w)$ is given by

$$e_f = \prod_{i=1}^{8k-4} x_i \, . \tag{19.1}$$

This case is more complicated than the previous one. The cycle is of length four and starts from the third member of the primitive period. We thus obtain for e_f, with $Q_{4k-2} = 2$

$$e_f = (x_1x_2)^2\Big(\prod_{s=1}^{k-2} x_{4s-1}x_{4s}x_{4s+1}x_{4s+2}\Big)^2 2(x_{4k-5}x_{4k-4}x_{4k-3}x_{4k-2})^2 . \tag{19.2}$$

From (4.3) we obtain, since $b_1 = 1$

$$\begin{cases} x_1x_2 = \dfrac{w+P_1}{Q_1}\cdot\dfrac{w+P_2}{Q_2} = \dfrac{Q_2+b_1(w+P_2)}{Q_2} \\ \qquad = \dfrac{A+w+A^k-(A+a+1)}{A}, \\ x_1x_2 = \dfrac{w+A^k-(a+1)}{A}. \end{cases} \tag{19.3}$$

From (4.3), we obtain, since $b_{4s-1} = 1$, $b_{4s+1} = 1$,

$$\begin{cases} x_{4s-1}x_{4s} = \dfrac{Q_{4s}+b_{4s-1}(w+P_{4s})}{Q_{4s}} = \dfrac{2A^{k-s}+w+A^k-2A^{k-s}-a}{2A^{k-s}} \\ \qquad = \dfrac{w+A^k-a}{2A^{k-s}}; \\ x_{4s+1}x_{4s+2} = \dfrac{Q_{4s+2}+b_{4s+1}(w+P_{4s+2})}{Q_{4s+2}} = \dfrac{A^{s+1}+w+A^k-A^{s+1}+a}{A^{s+1}} \\ \qquad = \dfrac{w+A^k+a}{A^{s+1}} \end{cases}$$

hence

$$\begin{cases} x_{4s-1}x_{4s}x_{4s+1}x_{4s+2} = \dfrac{(w+A^k-a)(w+A^k+a)}{2A^{k+1}} \\ \qquad = \dfrac{w^2+2A^kw+A^{2k}-a^2}{2A^{k+1}} \\ \qquad = \dfrac{A^{2k}-2(a+1)A^k+a^2+2A^kw+A^{2k}-a^2}{2A^{k+1}} \\ x_{4s-1}x_{4s}x_{4s+1}x_{4s+2} = \dfrac{w+A^k-(a+1)}{A}. \end{cases} \tag{19.4}$$

We further obtain from (4.3), for $s = k-1$ (these formulas indeed hold for $s = 1, 2, \cdots, k-1$)

$$\begin{cases} x_{4k-5}\cdot x_{4k-4} = \dfrac{Q_{4k-4}+b_{4k-5}(w+P_{4k-4})}{Q_{4k-4}} = \dfrac{2A+w+A^k-2A-a}{2A} \\ \qquad = \dfrac{w+A^k-a}{2A} \end{cases}$$

$$\begin{cases} x_{4k-3}x_{4k-2} = \dfrac{Q_{4k-2} + b_{4k-3}(w + P_{4k-2})}{Q_{4k-2}} = \dfrac{2 + 2(w + A^k - a - 2)}{2} \\ \quad = w + A^k - (a + 1) . \end{cases}$$

Thus

$$(19.5) \qquad x_{4k-5}x_{4k-4}x_{4k-3}x_{4k-2} = \frac{w + A^k - a}{2} \cdot \frac{w + A^k - (a+1)}{A} .$$

Substituting the values of (19.3), (19.4), (19.5) into (19.2), we obtain

$$(19.6) \quad \begin{cases} e_f = \left(\dfrac{w + A^k - (a+1)}{A}\right)^2 \left(\dfrac{w + A^k - (a+1)}{A}\right)^{2(k-2)} \\ \cdot 2\left(\dfrac{w + A^k - (a+1)}{A}\right)^2 \cdot \left(\dfrac{w + A^k - a}{2}\right)^2 , \\ e_f = \left[\dfrac{w + A^k - (a+1)}{A}\right]^{2k} \dfrac{(w + A^k - a)^2}{2} . \quad N(e_f) = 1 . \end{cases}$$

20. **Fundamental units of** $Q(w)$, $w^2 = [A^k + (A - 1)]^2 + 4A$; $A = 2^d b$, b **odd**; $d \geqq 1$, **(not both** $d, b = 1$); $k \geqq 2$. From the expansion of w in §5, the reader will verify easily that no Q_v equals 4. Thus e_f has the form $e_f = a + bw$, a and b natural numbers. In this chapter, we shall approach the calculation of e_f by a different approach, since the direct calculation of $\prod_{i=1}^{m} x_i$ (in the length of the primitive period) seems to raise insurmountable difficulties here. We shall prove the important formula

$$(20.1) \qquad e_f = \left(\frac{w + A^k + A - 1}{2A}\right)^k \cdot \frac{w + A^k + A + 1}{2} .$$

To justify statement (20.1), we have to prove three facts:

$$(20.2) \quad \begin{cases} (\text{i}) & e_f \text{ is an algebraic integer of the form } a + bw,\ a, b \in N; \\ (\text{ii}) & N(e_f) = \pm 1; \\ (\text{iii}) & e_f \text{ is minimal.} \end{cases}$$

To prove (20.2), (i), we shall show that

$$(w + A^k + A - 1)^k(w + A^k + A - 1) \equiv 0 (\text{mod } 2^{k+1}A^k) .$$

We obtain

$$\begin{aligned} &(a + A^k + A - 1)(w + A^k + A + 1) \\ &\quad = w^2 + 2(A^k + A)w + (A^k + A)^2 - 1 \\ &\quad = A^{2k} + 2(A - 1)A^k + A^2 + 2A + A^{2k} + 2A^{k+1} + A^2 + 2(A^k + A)w \\ &\quad = 2[A^{2k} + 2A^{k+1} + A^2 + A - A^k + (A^k + A)w] \\ (20.3) &\quad = 2[A^{2k} + A^{k+1} + A^{k+1} + A^2 + A + A^k + (A^k + A)w - 2A^k] \end{aligned}$$

$$= 2[A^k(A^k + A) + A(A^k + A) + (A^k + A) + (A^k + A)w - 2A^k]$$
$$= 2[(A^k + A)(w + A^k + A + 1) - 2A^k] ,$$
$$(w + A^k + A - 1)(w + A^k + A + 1)$$
$$= 2(A^k + A)(w + A^k + A + 1) - 4A^k .$$

From (20.3) we obtain, multiplying both sides by $w + A^k + A - 1$, and using formula (20.3) on the right side, we obtain

$$(w + A^k + A - 1)^2(w + A^k + A + 1)$$
$$= 2(A^k + A)[2(A^k + A)(w + A^k + A + 1] - 4A^k]$$
$$- 4A^k(w + A^k + A - 1) ;$$

Now, since $A^k \equiv O(2^k)$, $4A^{2k} \equiv O(2^{k+1}A^k)$, hence

(20.4)
$$(w + A^k + A - 1)^2(w + A^k + A + 1)$$
$$\equiv 4(2A^{k+1} + A^2)(w + A^k + A + 1) - 8A^{k+1}$$
$$- 4A^k(w + A^k + A - 1)(\mathrm{mod}\ 2^{k+1}A^k) .$$

For $k = 2$, we obtain

$$(w + A^k + A - 1)^2(w + A^2 + A + 1)$$
$$\equiv (8A^3 + 4A^2)(w + A^k + A + 1) - 8A^3 - 4A^2(w + A^2 + A - 1)$$
$$\equiv 4A^2(w + A^2 + A + 1) - 4A^2(w + A^2 + A - 1)$$
$$\equiv 8A^2 \equiv O(8A^2) .$$

Thus (20.2), (i) is correct for $k = 2$.

The reader will have no difficulty to obtain from (20.4), multiplying both sides by $w + A^k + A - 1$

(20.5)
$$(w + A^k + A - 1)^3(w + A^k + A + 1)$$
$$\equiv 8(3A^{k+2} + A^3)(w + A^k + A + 1)$$
$$- 8^k(4A^2 - A + 1) - 8A^k(2A - 1)w(\mathrm{mod}\ 2^{k+1}A^k) .$$

For $k = 3$, we obtain from (20.5), as can be easily verified

$$(w + A^3 + A - 1)^3(w + A^3 + A + 1) \equiv 16A^3w \equiv O(2^4A^3) .$$

Thus (20.2), (i) is correct for $k = 3$. It is then easily proved by induction that (20.2), (i) correct for any $k \geqq 2$.

To prove (ii), we obtain for the conjugate of e_f

(20.6)
$$e_f' = \left(\frac{-w + A^k + A - 1}{2A}\right)^k\left(\frac{-w + A^k + A + 1}{2}\right) .$$

From (20.6), (20.1) we obtain

$$(20.7)\quad \begin{aligned} e_f \cdot e'_f &= \left[\frac{(A^k+A-1)^2-w^2}{4A^2}\right]^k \left[\frac{(A^k+A+1)^2-w^2}{4}\right] \\ &= \left[\frac{A^{2k}+2(A-1)A^k+(A-1)^2-A^{2k}-2(A-1)A^k-(A+1)^2}{4A^2}\right]^k \\ &\cdot \left[\frac{A^{2k}+2(A+1)A^k+(A+1)^2-2(A-1)A^k-(A+1)^2}{4}\right] \\ &= \left(\frac{-4A}{4A^2}\right)^k \left(\frac{4A^k}{4}\right) = (-1)^k \\ N(e_f) &= (-1)^k \,. \end{aligned}$$

To prove (iii), namely that e_f given by (20.1) is really minimal, we first observe that, since the highest powers of A in both $(w + A^k + A - 1)/2A$ and in $(w + A^k + A - 1)/2$ are respectively A^{k-1} and A^k, the highest power of A in e_f equals $(A^{k-1})^k \cdot A^k = A^{k2}$. We return now to formula (15.4), viz., $e_f = A_0^{(m)} + x_m A_0^{(m+1)}$, where m is the length of the primitive period in the expansion of w. Since, by Theorem 5, $m = 5k - 6$, we obtain from formula (15.4)

$$(20.8)\quad e_f = A_0^{(5k-6)} + b_0 A_0^{(5k-5)} + A_0^{(5k-5)} w = A_0^{(5k-4)} + A_0^{(5k-5)}(w - b_0)\,.$$

We, therefore, have to calculate the power of $A_0^{(5k-5)}$. By Theorem 5, different expansions are obtained for odd and for even values of k. We shall carry out the calculation for odd k. From the values of the $b_v - s$ in the expansion of w in § 5, we obtain, by formulas (5.2),

$$(20.9)\quad \begin{aligned} A_0^{(5s-1)} &= A_0^{(5s-3)} + b_{5s-3} A_0^{(5s-2)} = A_0^{(5s-3)} + 2A_0^{(5s-2)}\,; \\ A_0^{(5s)} &= A_0^{(5s-2)} + b_{5s-2} A_0^{(5s-1)} = A_0^{(5s-2)} + \left(\frac{1}{2}A^s - 1\right)(A_0^{(5s-3)} + 2A_0^{(5s-2)})\,, \\ A_0^{(5s)} &= \left(\frac{1}{2}A^s - 1\right)A_0^{(5s-3)} + (A^s - 1)A_0^{(5s-2)}\,. \\ A_0^{(5s+1)} &= A_0^{(5s-1)} + b_{5s-1} A_0^{(5s)} = A_0^{(5s-3)} + 2A_0^{(5s-2)} \\ &\quad + \left(\frac{1}{2}A^s - 1\right)A_0^{(5s-3)} + (A^s - 1)A_0^{(5s-2)}\,, \\ A_0^{(5s+1)} &= \frac{1}{2}A^s A_0^{(5s-3)} + (A^s + 1)A_0^{(5s-2)}\,. \\ A_0^{(5s+2)} &= A_0^{(5s)} + b_{(5s)} A_0^{(5s+1)} = \left(\frac{1}{2}A^s - 1\right)A_0^{(5s-3)} \\ &\quad + (A^s - 1)A_0^{(5s-2)} + \frac{1}{2}A^s A_0^{(5-s3)} + (A^s + 1)A_0^{(5s-2)}\,, \\ A_0^{(5s+2)} &= (A^s - 1)A_0^{(5s-3)} + 2A^s A_0^{(5s-2)}\,. \end{aligned}$$

$$A_0^{(5s+3)} = A_0^{(5s+1)} + b_{5s+1}A_0^{(5s+2)} = A_0^{(5s+1)} + \left(\frac{1}{2}A^{k-s-1} - 1\right)A_0^{(5s+2)}$$

$$= \frac{1}{2}A^s A_0^{(5s-3)} + (A^s + 1)A_0^{(5s-2)} + \left(\frac{1}{2}A^{k-s-1} - 1\right)(A^s - 1)A_0^{(5s-3)}$$

$$+ \left(\frac{1}{2}A^{k-s-1} - 1\right)\cdot 2A^s A_0^{(5s-2)} ,$$

$$(20.10) \quad A_0^{(5s+3)} = \frac{1}{2}(A^{k-1} - A^s - A^{k-s-1} + 2)A_0^{(5s-3)} + (A^{k-1} + 1)A_0^{(5s-2)} .$$

We shall use the symbolic writing $u \overset{A}{=} v$ to express that u and v contain the same highest power of A. Since $A_0^{(5s-2)} > A_0^{(5s-3)}$, we obtain from (20.10)

$$(20.11) \qquad A_0^{(5s+3)} \overset{A}{=} A^{k-1}A_0^{(5s-2)} .$$

Now $A_0^{(0)} = 1$, $A_0^{(1)} = 0$, $A_0^{(2)} = 1$, $A_0^{(3)} = A_0^{(1)} + b_1A_0^{(2)}$, and from (5.17), (i), since $b_1 \overset{A}{=} A^{k-1}$,

$$(20.12) \qquad A_0^{(3)} \overset{A}{=} A^{k-1} .$$

From (20.11), (20.12) we thus obtain the important relation

$$A_0^{(5s+3)} \overset{A}{=} A^{(k-1)(s+1)} .$$

But, according to Theorem 5, max $s = (1/2)(k - 3)$, hence

$$(20.13) \qquad \begin{aligned} A_0^{(5/2(k-3)+3)} &\overset{A}{=} A^{(k-1)[1/2(k-3)+1]} , \\ A_0^{1/2(5k-9)} &\overset{A}{=} A^{1/2(k-1)^2} . \end{aligned}$$

From (5.17), (iii), $b_{1/2(5k-11)} \overset{A}{=} b_{1/2(5k-7)} \overset{A}{=} A^0$; $b_{1/2(5k-9)} \overset{A}{=} A^{1/2(k-3)}$. Hence, from (20.13),

$$(20.14) \qquad \begin{aligned} &A_0^{1/2(5k-7)} \overset{A}{=} A_0^{1/2(5k-9)};\ A_0^{1/2(5k-5)} \overset{A}{=} A^{1/2(k-3)}A_0^{(5k-9)} , \\ &A_0^{1/2(5k-5)} \overset{A}{=} A^{1/2[(k-1)^2+(k-3)]} . \end{aligned}$$

We are now at the midterm of the primitive period. If we still remember that the last term of the primitive period is $2b_0 \overset{A}{=} A^k$, we obtain $b_0A_0^{(5k-5)} \overset{A}{=} A^k\cdot(A^{1/2[(k-1)^2+(k-3)]})^2 = A^{k^2-2}$, which proves (iii). The power $k^2 - 2$ instead of k^2 is the summation error. Thus it is proved that e_f, given by (20.1) is, indeed the fundamental unit of $Q(w)$, w^2 in the chapter title.

21. Fundamental units of various types of quadratic fields.

In this section we state the fundamental units of quadratic fields that have a structure similar to that of the previous chapter. They were treated in §6, 7, 8. We state the corresponding fundamental unit e_f by an expression $g(w, A, k)$, similar to that in (20.1); the proof that $g(w, A, k)$ is an algebraic integer of the form $a + bw$, $a, b \in N$, and that $g(w, A, k)$ is minimal is completely analogous to the proof of the corresponding statements for e_f in (20.1), and will therefore not be repeated here; only the norm of $g(w, A, k)$ will be found.

(i) Let $w^2 = [A^k - (A-1)]^2 + 4A$, $A = 2^d b$, $d, b \geqq 1$; b odd; d, b not both 1; $k \geqq 2$. The fundamental unit of $Q(w)$ is given by

$$(21.1) \quad \underline{\underline{e_f = \left[\frac{w + A^k - (A-1)}{2A}\right]^k \cdot \frac{w + A^k - (A+1)}{2}}};$$

$$N(e_f) = (-1)^{k+1}.$$

We obtain from (21.1)

$$e'_f = \left[\frac{-w + A^k - (A-1)}{2A}\right]^k \cdot \left(\frac{-w + A^k - (A+1)}{2}\right).$$

Hence

$$e_f \cdot e'_f = \left[\frac{[A^k - (A-1)]^2 - w^2}{4A^2}\right]^k \cdot \left[\frac{[A^k - (A+1)]^2 - w^2}{4}\right]$$

$$= \left[\frac{A^{2k} - 2(A-1)A^k + (A-1)^2 - A^{2k} + 2(A-1)A^k - (A+1)^2}{4A^2}\right]^2$$

$$(21.2) \qquad \cdot \left[\frac{A^{2k} - 2(A+1)A^k + (A+1)^2 - A^{2k} + 2(A-1)A^k - (A+1)^2}{4}\right]$$

$$= \left(-\frac{1}{A}\right)^k \cdot (-A^k),$$

$$N(e'_f) = (-1)^{k+1} = N(e_f).$$

(ii) Let $w^2 = [A^k + (A+1)]^2 - 4A$; $A = 2^d b$; $d, b \geqq 1$, b odd; d, b not both $= 1$; $k \geqq 2$. The fundamental unit of $Q(w)$ is given by

$$(21.3) \quad \underline{\underline{e_f = \left(\frac{w + A^k + A + 1}{2A}\right)^k \cdot \left(\frac{w + A^k + A - 1}{2}\right)}}; \; N(e_f) = -1.$$

(iii) Let $w^2 = [A^k - (A+1)]^2 - 4A$; $A = 2^d b$, $d, b \geqq 1$, b odd; d, b not both $= 1$; $k \geqq 2$.

The fundamental unit of $Q(w)$ is given by

$$(21.4) \quad \underline{\underline{e_f = \left(\frac{w + A^k - (A+1)}{2A}\right)^k \cdot \left(\frac{w + A^k - (A-1)}{2}\right)}}; \; N(e_f) = 1.$$

(iv) Let $w^2 = [2^{(d+2)k} + (2^d - 1)]^2 + 2^{d+2}$, $d \geqq 1$.
The fundamental unit of $Q(w)$ is given by

$$(21.5)\quad \begin{aligned} e_f &= \left(\frac{w + 2^{(d+2)k} + (2^d - 1)}{2^{d+2}}\right)^k \cdot \left(\frac{w + 2^{(d+2)k} + (2^d + 1)}{2}\right); \\ N(e_f) &= (-1)^k . \end{aligned}$$

(v) Let $w^2 = [2^{(d+2)k} + (2^d + 1)]^2 - 2^{d+2}$, $d \geqq 1$.
The fundamental unit of $Q(w)$ is given by

$$(21.6)\quad \begin{aligned} e_f &= \left[\frac{w + 2^{(d+2)k} + (2^d + 1)}{2^{d+2}}\right]^k \cdot \left(\frac{w + 2^{(d+2)k} + (2^d - 1)}{2}\right); \\ N(e_f) &= -1 . \end{aligned}$$

The units in (iv) and (v) are calculated from the expansions considered in §§9 and 10.

22. **Fundamental units from $\prod_{i=1}^m x_i$.** In §21 we stated a unit e_f of $Q(w)$ explicitly and then proved that it is fundamental. The explicit statement of e_f was not just a guess—we were guided by the pattern e_f achieved by the formula $\prod x_i$, as was done in §16. Concluding this paper, we shall return to the calculation of e_f from $\prod_{i=1}^m x_i$, using an expansion with the maximal length of a cycle in the period hitherto known, namely the length 12. This was achieved in Chapter 14. We recapitulate the results obtained there as follows.

$$(22.1)\quad \begin{aligned} w^2 &= [A^k - (A + 1)]^2 - 4A = A^{2k} - 2(A + 1)A^k + (A - 1)^2 ; \\ A &= 2^d b + 1;\ d,\ b \geqq 1,\ b \text{ odd} . \end{aligned}$$

$$(22.2)\quad x_1 = \frac{w + A^k + (A + 2)}{2A^k - 3(2A + 1)},\ b_1 = 1;\ x_2 = \frac{w + A^k - (5A + 1)}{4A} .$$

$$(22.3)\quad \begin{cases} b_{12s+3} = 1,\ x_{12s+4} = \dfrac{w + A^k - A^{k-3s-1} - (A - 1)}{A^{k-3s-1}} ; \\ b_{12s+5} = 1,\ x_{12s+6} = \dfrac{w + A^k - 4A^{3s+2} + (A - 1)}{4A^{3s+2}} ; \\ b_{12s+7} = 2,\ x_{12s+8} = \dfrac{w + A^k - 2A^{k-3s-2} - (A - 1)}{4A^{k-3s-2}} ; \\ b_{12s+9} = 1,\ x_{12s+10} = \dfrac{w + A^k - A^{3(s+1)} + (A - 1)}{A^{3(s+1)}} ; \\ b_{12s+11} = 1,\ x_{12s+12} = \dfrac{w + A^k - 4A^{k-3(s+1)} - (A - 1)}{4A^{k-3(s+1)}} ; \\ b_{12s+13} = 2,\ x_{12s+14} = \dfrac{w + A^k - 2A^{3(s+1)+1} + (A - 1)}{4A^{3(s+1)+1}} . \\ s = 0, 1, \cdots, s_0 - 1;\ s_0 = \dfrac{1}{6}(k - 4);\ k \equiv 4 (\mathrm{mod}\ 6) . \end{cases}$$

By Theorem 14, the length of the primitive period of the expansion of w equals $m = 4k - 2$, and has the form:

$$w = [b_0, \overline{b_1, b_2, \cdots, b_{12s+3}, \cdots, b_{12s+14}, b_{12s_0+3}, \cdots, b_{12s_0+7}, 2, b_{12s_0+7}, \cdots,} \\ \overline{b_{12s_0+3}, \cdots, b_2, b_1, 2b_0}] .$$

Since, as can be easily verified, no Q_v equals 4, we obtain for the calculation of the fundamental unit e_f of $Q(w)$

$$(22.4) \quad \begin{aligned} e_f &= (x_1x_2)^2(x_{12s_0+3}x_{12s_0+4}x_{12s_0+5}x_{12s_0+6})^2 \cdot \\ &\quad x_{12s_0+7}x_{12s_0+8}Q_{12s_0+8}\left[\prod_{s=0}^{s_0-1}(x_{12s+3}x_{12s+4}\cdots x_{12s+14})\right]^2 . \end{aligned}$$

We first prove

$$(22.5) \quad [w + A^k - (A-1)][w + A^k + (A-1)] = 2A^k[w + A^k - (A+1)] .$$

We obtain from (22.1)

$$\begin{aligned} [w + A^k - (A-1)][w + A^k + (A-1)]^2 &= (w + A^k)^2 - (A-1)^2 \\ &= w^2 + 2A^kw + A^{2k} - (A-1)^2 \\ &= A^{2k} - 2(A+1)A^k + (A-1)^2 + 2A^kw + A^{2k} - (A-1)^2 \\ &= 2A^{2k} - 2(A+1)A^k + 2A^kw = 2A^k[w + A^k - (A+1)]. \end{aligned}$$

We shall use repeatedly the formula $x_tx_{t+1} = (Q_{t+1} + b_t(w + P_{t+1}))/Q_{t+1}$ and obtain from (22.2), (22.3)

$$(22.6) \quad \begin{aligned} x_1x_2 &= \frac{4A + w + A^k - (5A+1)}{4A} = \frac{w + A^k - (A+1)}{4A} , \\ x_1x_2 &= \frac{w + A^k - (A+1)}{4A} . \end{aligned}$$

$$(22.7) \begin{cases} x_{12s+3}\cdot x_{12s+4} = \dfrac{w + A^k - (A-1)}{A^{k-3s-1}}; \; x_{12s+5}\cdot x_{12s+6} = \dfrac{w + A^k + (A-1)}{4A^{33+2}} ; \\ x_{12s+7}\cdot x_{12s+8} = \dfrac{w + A^k - (A-1)}{2A^{k-3s-2}}; \; x_{12s+9}\cdot x_{12s+10} = \dfrac{w + A^k + (A-1)}{A^{3(s+1)}} ; \\ x_{12s+11}\cdot x_{12s+12} = \dfrac{w + A^k - (A-1)}{4A^{k-3(s+1)}}; \; x_{12s+13}\cdot x_{12s+14} = \dfrac{w + A^k + (A-1)}{2A^{3(s+1)+1}} : \end{cases}$$

From (22.7) we thus obtain

$$\prod_{i=0}^{11} x_{12s+3+i} = \left(\frac{[w + A^k - (A-1)][w + A^k + (A-1)]}{4A^{k+1}}\right)^3 ,$$

hence, by formula (22.5)

$$(22.8) \quad x_{12s+3}x_{12s+4}\cdots x_{12s+14} = \left(\frac{w + A^k - (A+1)}{2A}\right)^3 .$$

we further obtain from (22.3), since these formulas also hold for $s = s_0$

$$x_{12s_0+3}x_{12s_0+4}x_{12s_0+5}x_{12s_0+6} = \frac{w + A^k - (A+1)}{2A}, \tag{22.9}$$

and further

$$x_{12s_0+7}x_{12s_0+8} = \frac{w + A^k - (A-1)}{2A^{k-3s_0-2}}, \quad Q_{12s_0+8} = 4A^{k-3s_0-2}. \tag{22.10}$$

(22.4) now takes the form, in virtue of (22.6), (22.8), (22.9), (22.10)

$$\begin{cases} e_f = \left(\dfrac{w + A^k - (A+1)}{4A}\right)^2\left(\dfrac{w + A^k - (A+1)^2}{2A}\right) \\ \quad \cdot 2[w + A^k - (A-1)]\cdot\left[\dfrac{w + A^k - (A+1)}{2A}\right]^{6s_0}, \\ e_f = \left(\dfrac{w + A^k - (A+1)}{2A}\right)^{6s_0+4}\cdot\left(\dfrac{w + A^k - (A-1)}{2}\right), \\ \quad \text{and, since } 6s_0 + 4 = k, \\ e_f = \left[\dfrac{w + A^k - (A+1)}{2A}\right]^k\cdot\left(\dfrac{w + A^k - (A-1)}{2}\right). \quad N(e_f) = 1. \end{cases} \tag{22.11}$$

We have investigated the case k even. By Theorem 14, when $k \equiv 1 (\bmod 6)$ is odd, the length of the primitive period is again $4k - 2$, and the reader will have now no difficulty that e_f has the same structure in this case as for even k. The pattern of e_f remains the same as previously. It is also easily verified that e_f has the following structure for the fields $Q(w)$.

(i) Let $w^2 = [A^k + (A-1)]^2 + 4A$; $A = 2^d b + 1$; $d, b \geqq 1$, b odd. Then the fundamental unit of $Q(w)$ is given by

$$e_f = \left(\frac{w + A^k + A - 1}{2A}\right)^k\cdot\left(\frac{w + A^k + A + 1}{2}\right); \quad N(e_f) = (-1)^k. \tag{22.12}$$

(ii) Let $w^2 = [A^k - (A-1)]^2 + 4A$, $A = 2^d b + 1$; $d, b \geqq 1$, b odd. Then the fundamental unit of $Q(w)$ is given by

$$e_f = \left(\frac{w + A^k - (A-1)}{2A}\right)^k\cdot\left(\frac{w + A^k - (A+1)}{2}\right); \quad N(e_f) = (-1)^{k+1}. \tag{22.13}$$

(iii) Let $w^2 = [A^k + (A+1)]^2 - 4A$, $A = 2^d b + 1$; $d, b \geqq 1$, b odd. Then the fundamental unit of $Q(w)$ is given by

$$e_f = \left(\frac{w + A^k + A + 1}{2A}\right)^k\cdot\left(\frac{w + A^k + A - 1}{2}\right); \quad N(e_f) = -1. \tag{22.14}$$

REFERENCES

1. L. Bernstein, *The Jacobi-Perron Algorithm, Its Theory and Application*, Lecture Notes in Mathematics, **207**, Springer-Verlag, 1-160.

2. ———, *Einheitenberedinung in Kubischen Körpern mittels des Jacobi-Perronschen Algorithmus aus der Rechenanlage*, J. f. d. reine angew. Math. Band, **244** (1970), 201-220.

3. ———, *Periodicity and Units in Quadratic Number Fields*, submitted.

4. G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper*, Hamburger Math. Abh., Bd. XXII, (1958), 92-97.

5. O. Perron, *Die Lehre von den Kettenbrüchen, Zweite verbesserte Auflage*, Chelsea Publ. Co., New York, I-XII + 1-524.

6. Y. Yamamoto, *Real quadratic number fields with large fundamental units*, Osaka J. Math., **8** No. 2, (1971), 261-271.

7. H. Yokoi, *Units and class numbers of real Quadratic fields*, Nagoya Math. J. **37** (1970), 61-65.

8. H. Zassenhaus, *On the units of orders*, J. Algebera, **20** (1972), 368-395.

Received March 22, 1972, and in revised form December 9, 1975.

ILLINOIS INSTITUTE OF TECHNOLOGY

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 63, No. 1 March, 1976