EUCLID'S ALGORITHM IN REAL QUADRATIC FIELDS

H. CHATLAND AND H. DAVENPORT

1. Let m be a positive square-free integer. Euclid's Algorithm is said to hold in the field $k(\sqrt{m})$ if, given any non-integral element α in the field, an integer ξ can be found so that

$$|(\xi - \alpha)(\xi' - \alpha')| < 1,$$

where accents denote conjugates. The validity or invalidity of the Euclidean Algorithm in real quadratic fields has been investigated by many writers,[1] and it was established some years ago that the Algorithm can only be valid in a finite number of fields. A new approach to the question was made in a recent paper by H. Davenport [1]. Theorem 2 of [1] asserts that if $f(x, y)$ is an indefinite quadratic form with integral coefficients whose discriminant d is not a perfect square, then rational numbers p, q exist such that

$$|f(x + p, y + q)| > 2^{-7}d^{\frac{1}{2}}$$

for all integers x, y. On taking $f(x, y)$ to be the form which represents the norm of the general integer of $k(\sqrt{m})$, it follows that Euclid's Algorithm cannot hold if $d > 2^{14}$. Here d is m or $4m$ according as $m \equiv 1 \pmod 4$ or not. Thus the enumeration of all the fields with an Euclidean Algorithm was brought within the bounds of possibility.

The fields with $d < 2^{14}$ were investigated by H. Chatland [2]. Those not already settled by earlier investigations were treated by the method of Erdös and Ko [3], and in all but six cases it was shown that Euclid's Algorithm does not hold. These six cases are:

$$m = 193, 241, 313, 337, 457, 601. \tag{1}$$

We shall now prove that Euclid's Algorithm does not hold in any of these fields, and so (in virtue of the existing results) we shall have established that *Euclid's Algorithm holds in* $k(\sqrt{m})$ *if*

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, 97$$

and in no other case.

Another proof that the algorithm does not hold in the six cases (1) has been given independently by K. Inkeri [4], using a method based on that of Erdös and Ko [3].

Received April 28, 1949.

[1]For an account of the literature, see [2].

2. We investigate the six cases (1) by a modification of Davenport's method. In order to make this intelligible, we must first summarize the necessary definitions and results of [1] with such modifications as are appropriate.

Let $f(x, y)$ be the norm-form for $k(\sqrt{m})$, which is in fact

$$f(x, y) = x^2 + xy - \tfrac{1}{4}(m-1)y^2$$

since $m \equiv 1 \pmod 4$. Let $\theta = \frac{1}{2}(1+\sqrt{m})$. Let $\theta_0 = \frac{1}{2}(u+\sqrt{m})$, $\theta'_0 = \frac{1}{2}(u-\sqrt{m})$, where u is an odd integer so chosen that

$$-0.618\ldots < \theta'_0 < 0.382\ldots.$$

The numbers in the last inequality are $(1-\sqrt{5})/2$ and $(3-\sqrt{5})/2$. Plainly $\theta_0 > 2$.

Let $f_0(x, y) = (x+\theta_0 y)(x+\theta'_0 y)$. From $f_0(x, y)$ we can derive (Lemma 2)[2] a chain of equivalent forms

$$f_n(x, y) = a_n(x+\theta_n y)(x+\theta'_n y),$$

which all satisfy $\theta_n > 2$ and

$$-0.618\ldots \leq \theta'_n \leq 0.382\ldots.$$

By comparison of discriminants we have

$$a_n(\theta_n - \theta'_n) = \pm\sqrt{m}. \tag{2}$$

These forms are connected by recurrence relations:

$$\theta_n = t_n + \frac{\mu_{n+1}}{\theta_{n+1}}, \quad \theta'_n = t_n + \frac{\mu_{n+1}}{\theta'_{n+1}}.$$

Here t_n is the integer nearest to θ_n, and μ_n is plus or minus one with sign opposite to that of θ'_n. The numbers a_n, θ_n, θ'_n, t_n, μ_n exist for all integers n (positive, negative and zero) and are periodic (Lemma 9) with a certain period N.

To prove that Euclid's Algorithm does not hold, it suffices to construct an element β_0 of $k(\sqrt{m})$ such that

$$|(x+\theta_0 y+\beta_0)(x+\theta'_0 y+\beta'_0)| \geqslant 1 \tag{3}$$

for all integers x, y. The construction of β_0 is based on a choice of a set of integers v_n, also periodic with period N. In [1] the choice was made by taking $v_n = [\frac{1}{2}\theta_n]$, but this would not lead to the desired result in the six cases now under consideration. The choices of v_n will be made separately in each case in § **4.** In terms of the v_n, we define β_n for all n by

$$\beta_n = v_n + \frac{\mu_{n+1}}{\theta_{n+1}} v_{n+1} + \frac{\mu_{n+1}\mu_{n+2}}{\theta_{n+1}\theta_{n+2}} v_{n+2} + \ldots.$$

Since $\theta_n > 2$ and the v_n are periodic, this series is absolutely convergent. It is

[2]The lemmas referred to are to be found in [1].

https://doi.org/10.4153/CJM-1950-026-7 Published online by Cambridge University Press

proved (Lemma 10) that β_n is an element of $k(\sqrt{m})$ and that its conjugate β'_n is given by

$$\beta'_n = v_{n-1} \left| \theta'_n \right| - v_{n-2} \left| \theta'_n \theta'_{n-1} \right| + v_{n-3} \left| \theta'_n \theta'_{n-1} \theta'_{n-2} \right| - \dots .$$

We prove the following general theorem, and later apply it to each of our six cases.

THEOREM. *Suppose the integers v_n can be chosen in such a way that for all n*

$$1 < \beta_n < \theta_n, \quad 0 < \beta'_n < 1, \quad \theta'_n < \beta'_n < 1, \quad \beta'_n - \theta'_n < 1, \tag{4}$$

$$\beta_n \beta'_n \left| a_n \right| > 1, \tag{5}$$

$$(\beta_n - 1)(1 - \beta'_n) \left| a_n \right| > 1, \tag{6}$$

$$(\theta_n - \beta_n)(\beta'_n - \theta'_n) \left| a_n \right| > 1, \tag{7}$$

$$(1 + \theta_n - \beta_n)(1 + \theta'_n - \beta'_n) \left| a_n \right| > 1. \tag{8}$$

Then Euclid's Algorithm does not hold in the field.

3. Proof of the theorem. We suppose there exist integers x_0, y_0 which contradict (3), so that

$$\left| (x_0 + \theta_0 y_0 + \beta_0)(x_0 + \theta'_0 y_0 + \beta'_0) \right| < 1. \tag{9}$$

Let

$$L_n(x, y) = x + \theta_n y + \beta_n, \quad L'_n(x, y) = x + \theta'_n y + \beta'_n.$$

The recurrence relations satisfied by θ_n and β_n give

$$L_n(x, y) = x + \left(t_n + \frac{\mu_{n+1}}{\theta_{n+1}} \right) y + v_n + \frac{\mu_{n+1}}{\theta_{n+1}} \beta_{n+1}$$

$$= \frac{\mu_{n+1}}{\theta_{n+1}} L_{n+1}(y, \mu_{n+1}(x + t_n y + v_n)).$$

A similar relation holds with accented symbols. Hence, if we start from x_0, y_0 and define integers x_n, y_n for $n > 0$ and $n < 0$ by the recurrence relations

$$x_{n+1} = y_n, \quad y_{n+1} = \mu_{n+1}(x_n + t_n y_n + v_n),$$

we then have

$$\left| L_n(x_n, y_n) \right| = \frac{1}{\theta_{n+1}} \left| L_{n+1}(x_{n+1}, y_{n+1}) \right| \tag{10}$$

for all n. It is also easily verified, from the recurrence relations and (2), that

$$\left| a_n L_n(x_n, y_n)\, L'(x_n, y_n) \right|$$

is independent of n, so that, by (9),

https://doi.org/10.4153/CJM-1950-026-7 Published online by Cambridge University Press

$$(11) \qquad |a_n L_n(x_n, y_n)\, L'_n(x_n, y_n)| < 1$$

for all n.

Suppose first that $L_0(x_0, y_0) \neq 0$. Then, by (10), $|L_n(x_n, y_n)|$ increases steadily from 0 to $+\infty$ as n increases from $-\infty$ to $+\infty$. There will be exactly one value of n for which

$$(12) \qquad |L_{n-1}(x_{n-1}, y_{n-1})| \leq m^{-\frac{1}{4}} < |L_n(x_n, y_n)|.$$

Then, by (10),

$$(13) \qquad |L_n(x_n, y_n)| = \theta_n |L_{n-1}(x_{n-1}, y_{n-1})| \leq m^{-\frac{1}{4}}\theta_n.$$

Also, by (11) and (2),

$$(14) \qquad |L'_n(x_n, y_n)| < |a_n L_n(x_n, y_n)|^{-1} < m^{\frac{1}{4}} |a_n|^{-1} = m^{-\frac{1}{4}}(\theta_n - \theta'_n).$$

Suppose next that $L_0(x_0, y_0) = 0$. Then $L'_0(x_0, y_0) = 0$, and moreover, by the above recurrence relations, $L_n(x_n, y_n)$ and $L'_n(x_n, y_n)$ are 0 for all n. In this case, the inequalities (11), (13), (14) are satisfied trivially for any n. Only these will be used in the rest of the proof. We now drop the suffix n on x and y, and rewrite the inequalities as

$$(15) \qquad |a_n(x + \theta_n y + \beta_n)(x + \theta'_n y + \beta'_n)| < 1,$$

$$(16) \qquad |x + \theta_n y + \beta_n| \leq m^{-\frac{1}{4}}\theta_n,$$

$$(17) \qquad |x + \theta'_n y + \beta'_n| < m^{-\frac{1}{4}}(\theta_n - \theta'_n).$$

If $y \geq 1$ or $y \leq -2$, we combine (16) and (17) by subtraction, and obtain

$$|(\theta_n - \theta'_n)y + (\beta_n - \beta'_n)| < m^{-\frac{1}{4}}(2\theta_n - \theta'_n).$$

Now, by (4), $0 < \beta_n - \beta'_n < \theta_n - \theta'_n$. Hence, if $y \geq 1$ or $y \leq -2$, we obtain

$$\theta_n - \theta'_n < m^{-\frac{1}{4}}(2\theta_n - \theta'_n).$$

But if $m^{\frac{1}{4}} > 3$, this is impossible, since it implies $3(\theta_n - \theta'_n) < 2\theta_n - \theta'_n$, or $\theta_n < 2\theta'_n$, whereas $\theta_n > 2$ and $\theta'_n < \frac{1}{2}$.

If $y = 0$, (15) becomes

$$|a_n(x + \beta_n)(x + \beta'_n)| < 1.$$

Now β'_n lies between 0 and 1, and β_n lies between v_n and $v_n + \mu_{n+1}$, since $\beta_n = v_n + \mu_{n+1}\beta_{n+1}/\theta_{n+1}$. Hence, if the last inequality holds for an integer x, it must hold when x is replaced by some one of the four values

$$0, \; -1, \; -v_n, \; -v_n - \mu_{n+1}.$$

The first two values give us inequalities which contradict (5) and (6). The last two give

$$|a_n(v_n - \beta_n)(v_n - \beta'_n)| < 1 \text{ or } |a_n(v_n + \mu_{n+1} - \beta_n)(v_n + \mu_{n+1} - \beta'_n)| < 1.$$

On using the recurrence relations satisfied by β_n and β'_n, and the relation

$$|a_n| = |\theta_{n+1}\theta'_{n+1}a_{n+1}|,$$

which follows from (2), we obtain

$$|a_{n+1}\beta_{n+1}\beta'_{n+1}| < 1 \text{ or } |a_{n+1}(\theta_{n+1} - \beta_{n+1})(\theta'_{n+1} - \beta'_{n+1}| < 1,$$

which contradicts (5) and (7).

If $y = -1$, the inequality (15) becomes

$$|a_n(x - \theta_n + \beta_n)(x - \theta'_n + \beta'_n)| < 1.$$

Since $0 < \beta'_n - \theta'_n < 1$ by (4), the values of x which are relevant to the second factor are $x = 0$ and $x = -1$. These give contradictions to (7) and (8). As regards the first factor, we have

$$\theta_n - \beta_n = t_n - v_n - \frac{\mu_{n+1}}{\theta_{n+1}}(\beta_{n+1} - 1).$$

Hence the values of x which are relevant are $t_n - v_n$ and $t_n - v_n - \mu_{n+1}$. These give the inequalities

$$|a_n(t_n - v_n - \theta_n + \beta_n)(t_n - v_n - \theta'_n + \beta'_n)| < 1$$

or

$$|a_n(t_n - v_n - \mu_{n+1} - \theta_n + \beta_n)(t_n - v_n - \mu_{n+1} - \theta'_n + \beta'_n)| < 1.$$

On using the recurrence relations as before, these become

$$|a_{n+1}(\beta_{n+1} - 1)(\beta'_{n+1} - 1)| < 1$$

or

$$|a_{n+1}(1 + \theta_{n+1} - \beta_{n+1})(1 + \theta'_{n+1} - \beta'_{n+1})| < 1,$$

which contradict (6) and (8). This proves that the inequalities (15), (16), (17) cannot be satisfied by any pair x, y of integers, and so completes the proof of the Theorem.

4. To show that Euclid's Algorithm is not valid in any of the cases (1) it is sufficient to give integers v_n, for a complete period in each case, such that the hypotheses of the theorem are satisfied. Such values for v_n, together with the resulting values (rounded off) of β_n and β'_n, are given in the following tables. We use P_n, Q_n, R_n, S_n to denote the products of the left of (5), (6), (7), (8). It will be seen that these are all greater than 1, and that the conditions (4) are satisfied throughout.

https://doi.org/10.4153/CJM-1950-026-7 Published online by Cambridge University Press

$m = 337$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\|a_n\|$	P_n	Q_n	R_n	S_n
0	18.679	.321	9	8.233	.512	1	4.22	3.53	2.00	9.26
1	3.113	.054	2	2.387	.454	6	6.51	4.54	1.75	6.20
2	8.839	−.339	4	3.421	.525	2	3.59	2.30	9.36	1.75
3	6.226	.107	3	3.602	.372	3	4.02	4.90	2.09	7.99
4	4.420	−.170	2	2.660	.446	4	4.75	3.68	4.33	4.24
5	2.383	−.240	1	1.574	.373	7	4.11	2.52	3.47	4.91
6	2.613	−.446	2	1.499	.280	6	2.52	2.16	4.86	3.47
7	2.585	.290	2	1.295	.499	8	5.17	1.18	2.16	14.49
8	2.409	.369	1	1.697	.554	9	8.46	2.80	1.18	12.55
9	2.446	−.613	1	1.706	.274	6	2.80	3.08	3.94	1.18
10	2.240	−.383	1	1.582	.278	7	3.08	2.94	3.04	3.94
11	4.170	−.420	2	2.427	.303	4	2.94	3.98	5.04	3.04
12	5.893	−.226	3	2.515	.384	3	2.90	2.80	6.18	5.12
13	9.339	.161	4	4.529	.420	2	3.81	4.09	2.50	8.60
14	2.946	−.113	2	1.559	.405	6	3.79	2.00	4.31	6.90

$m = 457$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\|a_n\|$	P_n	Q_n	R_n	S_n
0	21.189	−.189	10	10.711	.104	1	1.11	8.71	3.06	8.12
1	5.297	−.047	3	3.765	.467	4	7.03	5.89	3.15	4.92
2	3.365	−.198	2	2.573	.502	6	7.75	4.70	3.32	3.22
3	2.741	−.313	2	1.572	.468	7	5.15	2.13	6.39	3.32
4	3.865	.302	2	1.654	.462	6	4.59	2.11	2.13	16.17
5	7.396	.270	2	2.559	.416	3	3.19	2.73	2.11	14.97
6	2.524	−.149	2	1.410	.235	8	2.66	2.51	3.42	10.42
7	2.099	.318	1	1.239	.560	12	8.33	1.26	2.51	16.90
8	10.094	−.594	2	2.409	.261	2	1.26	2.08	13.15	2.51
9	10.594	−.094	5	4.338	.164	2	1.42	5.58	3.23	10.76
10	2.465	.090	1	1.632	.436	9	6.40	3.21	2.59	10.79
11	2.149	−.524	1	1.358	.295	8	3.21	2.02	5.18	2.59
12	6.730	−.396	3	2.411	.279	3	2.02	3.05	8.75	5.18
13	3.698	.135	3	2.179	.368	6	4.81	4.47	2.12	11.60
14	3.313	.259	2	2.719	.681	7	12.96	3.84	1.76	6.45
15	3.198	−.365	2	2.298	.481	6	6.63	4.04	4.57	1.76
16	5.047	−.297	1	1.505	.451	4	2.72	1.11	10.60	4.57

$m = 241$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\lvert a_n \rvert$	P_n	Q_n	R_n	S_n
0	15.262	−.262	7	7.396	.396	1	2.93	3.86	5.18	3.03
1	3.816	−.066	2	1.510	.433	4	2.61	1.16	4.60	6.64
2	5.421	.246	2	2.658	.386	3	3.07	3.06	1.16	9.71
3	2.377	−.210	1	1.564	.340	6	3.19	2.23	2.68	4.90
4	2.652	−.452	2	1.495	.299	5	2.23	1.74	4.35	2.68
5	2.877	.290	2	1.453	.493	6	4.29	1.38	1.74	11.59
6	8.131	.369	4	4.451	.556	2	4.95	3.06	1.38	7.61
7	7.631	−.131	4	3.442	.451	2	3.11	2.68	4.88	4.33
8	2.710	.123	2	1.513	.436	6	3.96	1.74	2.25	9.05
9	3.452	.348	1	1.680	.543	5	4.56	1.55	1.74	11.15
10	2.210	−.377	1	1.502	.172	6	1.55	2.50	2.33	4.62
11	4.754	−.421	3	2.389	.348	3	2.50	2.72	5.46	2.33
12	4.066	.184	2	2.485	.489	4	4.86	3.03	1.93	7.18

$m = 601$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\lvert a_n \rvert$	P_n	Q_n	R_n	S_n
0	24.758	.242	12	12.802	.373	1	4.78	7.40	1.57	11.26
1	4.126	.040	3	3.309	.470	6	9.32	7.35	2.10	6.22
2	7.919	−.253	3	2.448	.639	3	4.69	1.57	14.64	2.10
3	12.379	.121	6	6.838	.286	2	3.91	8.34	1.83	10.92
4	2.640	−.084	3	2.213	.481	9	9.58	5.67	2.17	5.58
5	2.776	.324	3	2.184	.817	10	17.84	2.17	2.91	8.08
6	4.460	.374	3	3.639	.816	6	17.82	2.91	2.18	6.09
7	2.176	−.276	1	1.391	.602	10	8.38	1.55	6.89	2.18
8	5.689	−.439	3	2.222	.175	4	1.55	4.03	8.52	6.89
9	3.220	.155	2	2.504	.439	8	8.79	6.75	1.62	9.84
10	4.552	−.352	3	2.293	.549	5	6.29	2.92	10.17	1.62
11	2.230	.187	1	1.576	.458	12	8.66	3.74	2.13	14.47
12	4.352	−.552	2	2.505	.299	5	3.74	5.28	7.85	2.13
13	2.845	−.220	2	1.437	.374	8	4.30	2.19	6.68	7.83
14	6.439	.311	3	3.626	.505	4	7.33	5.20	2.19	12.29
15	2.276	−.176	1	1.425	.439	10	6.25	2.39	5.23	7.14
16	3.626	−.460	2	1.540	.258	6	2.39	2.41	8.98	5.23
17	2.676	.224	2	1.230	.391	10	4.80	1.40	2.41	2.04
18	3.084	.360	2	2.376	.580	9	12.40	5.20	1.40	12.00
19	11.879	−.379	5	4.470	.538	2	4.81	3.21	13.59	1.40
20	8.253	.081	4	4.375	.360	3	4.73	6.47	3.25	10.54
21	3.960	−.126	2	1.483	.460	6	4.09	1.57	8.71	8.64

$m = 193$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\|a_n\|$	P_n	Q_n	R_n	S_n
0	13.446	−.446	6	6.703	.271	1	1.82	4.16	4.84	2.19
1	2.241	−.074	1	1.575	.426	6	4.03	1.98	2.00	4.99
2	4.149	−.482	2	2.385	.277	3	1.98	3.01	4.01	2.00
3	6.723	−.223	3	2.592	.384	2	1.99	1.96	5.02	4.03
4	3.612	.138	2	1.475	.362	4	2.14	1.21	1.91	9.74
5	2.574	.259	2	1.351	.424	6	3.44	1.21	1.21	11.14
6	2.350	.365	1	1.524	.575	7	6.13	1.56	1.21	10.09
7	2.862	−.612	2	1.501	.260	4	1.56	1.48	4.74	1.21
8	7.223	.277	3	3.607	.482	2	3.48	2.70	1.48	7.34
9	4.482	−.149	2	2.722	.375	3	3.06	3.23	2.76	3.95
10	2.074	−.241	1	1.498	.392	6	3.52	1.82	2.19	3.47

$m = 313$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\|a_n\|$	P_n	Q_n	R_n	S_n
0	17.346	−.346	8	8.525	.520	1	4.44	3.61	7.64	1.31
1	2.891	−.058	2	1.517	.431	6	3.92	1.76	4.03	7.28
2	9.173	.327	4	4.431	.513	2	4.55	3.34	1.76	9.35
3	5.782	−.115	3	2.494	.402	3	3.01	2.68	5.10	6.21
4	4.586	.164	3	2.319	.425	4	3.94	3.04	2.37	9.65
5	2.418	.207	1	1.646	.532	8	7.01	2.42	2.01	9.56
6	2.391	−.558	1	1.545	.261	6	2.42	2.42	4.16	2.01
7	2.558	−.391	2	1.393	.289	6	2.42	1.68	4.75	4.16
8	2.261	.295	1	1.373	.505	9	6.23	1.66	1.68	13.43
9	3.836	−.586	2	1.431	.291	4	1.66	1.22	8.44	1.68
10	6.115	.218	3	3.483	.373	3	3.89	4.67	1.22	9.21
11	8.673	−.173	5	4.185	.454	2	3.80	3.48	5.63	4.09
12	3.058	.109	2	2.491	.496	6	7.41	4.51	1.31	5.76

References

[1] H. Davenport, *Indefinite binary quadratic forms, and Euclid's Algorithm in real quadratic fields*, Proc. London Math. Soc. (in course of publication).

[2] H. Chatland, *On the Euclidean Algorithm in quadratic number fields*, Bull. Amer. Math. Soc., vol. 55 (1949), 948-953.

[3] P. Erdös and Chao Ko, *Note on the Euclidean Algorithm*, J. London Math. Soc., vol. 13 (1938), 3-8.

[4] K. Inkeri, *Über den Euklidischen Algorithmus in quadratischen Zahlkörpern*, Annales Academiae Scientiarum Fennicae, vol. 41 (1947), 5-34.

The Ohio State University
and
University College, London