ON THE EUCLIDEAN ALGORITHM IN QUADRATIC NUMBER FIELDS

H. CHATLAND

1. **Introduction.** Let m be a square-free rational integer. The field $R(m^{1/2})$ is said to be Euclidean or that the Euclidean algorithm exists in $R(m^{1/2})$ if for integers α, $\beta \neq 0 \subset R(m^{1/2})$ there exists an integer $\gamma \subset R(m^{1/2})$ such that

$$|N(\alpha - \beta\gamma)| < |N(\beta)|.$$

The problem of determining in what fields $R(m^{1/2})$ the algorithm exists has been worked out except for m equal to a prime of the form $24n+1$ and greater than 97. In this paper it is shown that the Euclidean algorithm does not exist for $m=24n+1>97$ except possibly for $m=193$, 241, 313, 337, 457, and 601. The problem is not settled in these six cases.

2. **Previous results.** In order that a field be Euclidean the class number must be 1. However, this condition is not sufficient for, as Dedekind pointed out [1][1], the field $R(-19^{1/2})$ has class number 1 but is not Euclidean. L. E. Dickson [2] showed that for m negative the Euclidean algorithm exists only if $m=-1$, -2, -3, -7, and -11. For m positive, the algorithm has been shown to exist for the following values of m:

(1) 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, 97.

Except for the last two values in (1) the proofs have been obtained by O. Perron [3], A. Oppenheim [4], R. Remak [5], N. Hofreiter [6], and A. Berg [7]. It was pointed out by I. Schur [4, p. 351] that the algorithm does not exist for $m=47$. A. Oppenheim [4] proved that for $m=23$ and $m=53$ the algorithm does not exist. N. Hofreiter [8] proved non-existence for $m\equiv 14 \pmod{24}$ and [6] for $m=77$ and $m\equiv 21 \pmod{24}$, $m>21$. E. Berg [7] and J. F. Keston [9] proved non-existence for $m\not\equiv 1 \pmod 4$ except for the values listed in (1). Also, apart from (1) H. Behrbohm and L. Rédei [10] showed that the algorithm can exist only in the following three cases.

I. $m = p \equiv 13 \pmod{24}$,

Presented to the Society, June 19, 1948; received by the editors May 11, 1948, and in revised form, July 23, 1948.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

II. $m = p \equiv 1 \pmod 8$,

III. $m = pq$ with $p \equiv q \equiv 3 \pmod 8$ or $p \equiv q \equiv 7 \pmod 8$

where p and q are primes.

For sufficiently large m, P. Erdös and Ch. Ko [11] proved that the algorithm cannot exist in cases I and II. H. Heilbronn [12] proved a similar result for case III. L. Schuster [13] showed that except for $m=33$ and 57 in case III the algorithm exists at most for $m\equiv 1 \pmod{24}$. A. Brauer [14] proved that the algorithm cannot exist in case I for $p>109$. There remained then in case I only the values $m=61$ and $m=109$. L. Rédei [15] proved the non-existence of the algorithm for these two values. By an entirely different method L. K. Hua and W. T. Sheh [17] proved that the algorithm does not exist for $m=61$. L. Rédei [18] obtained the result in case III that if the algorithm exists then $m=3q$. This result coupled with that of Schuster [13] completes case III in which the algorithm exists only for $m=21$, 33, 57. There remain those values of $m=p\equiv 1 \pmod 8$. For $p=73$, 97, L. Rédei [15] proved the existence of the algorithm and for p of the form $24n+17$ and greater than 41 the non-existence of the algorithm. The case $p=24n+17$ and $p>41$ was also treated by L. Hua and S. Min [16] who left in doubt however $p=89$, 113, and 137.

3. **Present results.** Recently H. Danveport [19] proved that the Euclidean algorithm does not exist for quadratic fields whose discriminants exceed $(128)^2$. In their paper, mentioned above, Erdös and Ko prove the following theorem:

THEOREM. *For a prime p of the form $4n+1$, the Euclidean algorithm cannot exist in $R(p^{1/2})$, if p can be written in the form*

$$p = q_1 m_1 + q_2 m_2, \tag{2}$$

where m_1, m_2, q_1, q_2 are all positive and quadratic non-residues $\pmod p$, *and where the q_i are odd primes which divide $q_i m_i$ to an odd power for $i=1, 2$.*

In this paper a representation of the form (2) is given for each prime of the form $24n+1$ greater than 97 and less than $(128)^2$ except for $p=193$, 241, 313, 337, 457, and 601. In the case of these last six it can be shown that no such representation exists. Hence for them no conclusion can be drawn, concerning the existence of the algorithm, by this method.

Representations of primes $p=24n+1$ in the form $p=q_1m_1+q_2m_2$

$409=14\times 19+11\times 13$	$3169=7\times 86+17\times 151$
$433=7\times 29+10\times 23$	$3217=5\times 87+13\times 214$
$577=14\times 13+5\times 79$	$3313=13\times 45+11\times 248$
$673=17\times 15+19\times 22$	$3361=11\times 68+13\times 201$
$769=23\times 21+13\times 22$	$3433=7\times 10+19\times 177$
$937=5\times 7+41\times 22$	$3457=5\times 42+17\times 191$
$1009=11\times 52+19\times 23$	$3529=13\times 57+17\times 164$
$1033=11\times 13+89\times 10$	$3673=5\times 13+11\times 328$
$1129=17\times 19+31\times 26$	$3697=5\times 92+13\times 249$
$1153=17\times 14+61\times 15$	$3769=17\times 14+11\times 321$
$1201=17\times 26+23\times 33$	$3793=19\times 60+7\times 379$
$1249=19\times 44+7\times 59$	$3889=11\times 38+13\times 267$
$1297=5\times 154+17\times 31$	$4057=29\times 20+19\times 183$
$1321=17\times 39+47\times 14$	$4129=7\times 29+13\times 302$
$1489=17\times 39+59\times 14$	$4153=13\times 102+11\times 257$
$1609=19\times 14+17\times 79$	$4177=11\times 45+7\times 526$
$1657=7\times 45+61\times 22$	$4201=11\times 38+13\times 291$
$1753=7\times 165+13\times 46$	$4273=5\times 58+7\times 569$
$1777=5\times 21+19\times 88$	$4297=5\times 19+11\times 382$
$1801=19\times 78+11\times 29$	$4441=13\times 70+11\times 321$
$1873=23\times 60+17\times 29$	$4513=19\times 15+7\times 604$
$1993=7\times 5+89\times 22$	$4561=17\times 110+13\times 207$
$2017=5\times 26+17\times 111$	$4657=5\times 46+19\times 233$
$2089=7\times 190+11\times 69$	$4729=11\times 93+17\times 218$
$2113=5\times 277+7\times 104$	$4801=23\times 21+17\times 254$
$2137=13\times 129+5\times 92$	$4969=7\times 152+11\times 355$
$2161=23\times 70+19\times 29$	$4993=5\times 57+11\times 428$
$2281=7\times 51+13\times 148$	$5113=5\times 93+7\times 664$
$2377=5\times 62+13\times 159$	$5209=11\times 306+19\times 97$
$2473=5\times 31+19\times 122$	$5233=5\times 17+11\times 468$
$2521=11\times 53+17\times 114$	$5281=7\times 38+17\times 295$
$2593=5\times 275+29\times 42$	$5449=7\times 95+13\times 368$
$2617=7\times 122+41\times 43$	$5521=7\times 89+31\times 158$
$2689=13\times 46+17\times 123$	$5569=19\times 68+13\times 329$
$2713=11\times 153+5\times 206$	$5641=7\times 172+29\times 153$
$2833=7\times 15+11\times 248$	$5689=17\times 132+13\times 265$
$2857=5\times 138+11\times 197$	$5737=37\times 20+19\times 263$
$2953=5\times 42+13\times 211$	$5857=5\times 78+7\times 781$
$3001=7\times 65+19\times 134$	$5881=31\times 13+11\times 498$
$3049=11\times 94+13\times 155$	$5953=5\times 7+11\times 538$
$3121=7\times 220+17\times 93$	$6073=5\times 29+19\times 312$

$6121=7\times 87+13\times 424$
$6217=17\times 15+11\times 542$
$6257=5\times 56+43\times 139$
$6337=5\times 61+13\times 464$
$6361=17\times 21+19\times 316$
$6481=13\times 342+11\times 185$
$6529=11\times 141+19\times 262$
$6553=11\times 280+23\times 151$
$6577=5\times 69+19\times 328$
$6673=5\times 308+29\times 177$
$6793=7\times 235+11\times 468$
$6841=29\times 67+31\times 158$
$6961=7\times 104+23\times 271$
$7057=13\times 80+11\times 547$
$7129=7\times 374+13\times 347$
$7177=5\times 38+17\times 411$
$7297=7\times 15+29\times 248$
$7321=7\times 312+11\times 467$
$7369=13\times 201+29\times 164$
$7393=23\times 29+19\times 354$
$7417=5\times 17+13\times 564$
$7489=37\times 70+23\times 213$
$7537=5\times 51+11\times 662$
$7561=13\times 73+29\times 228$
$7681=13\times 102+31\times 205$
$7753=5\times 416+31\times 183$
$7873=13\times 10+29\times 267$
$7993=5\times 88+7\times 1079$
$8017=19\times 90+17\times 371$
$8089=17\times 295+29\times 106$
$8161=7\times 29+23\times 346$
$8209=13\times 14+23\times 349$
$8233=17\times 165+23\times 236$
$8329=31\times 219+11\times 140$
$8353=5\times 17+13\times 636$
$8377=13\times 135+11\times 602$
$8521=13\times 31+11\times 738$
$8641=7\times 136+11\times 699$
$8689=29\times 195+37\times 82$
$8713=5\times 404+23\times 291$
$8737=37\times 30+29\times 263$
$8761=19\times 71+17\times 436$
$8929=13\times 114+11\times 677$
$9001=13\times 42+19\times 445$
$9049=11\times 53+17\times 498$
$9241=17\times 286+29\times 151$
$9337=5\times 203+19\times 438$
$9433=13\times 80+11\times 763$
$9601=13\times 174+41\times 179$
$9649=41\times 212+11\times 87$
$9697=11\times 30+17\times 551$
$9721=11\times 774+17\times 71$
$9769=17\times 390+43\times 73$
$9817=5\times 42+13\times 739$
$10009=11\times 105+19\times 466$
$10177=5\times 7+11\times 922$
$10273=5\times 238+31\times 293$
$10321=7\times 41+29\times 346$
$10369=13\times 207+11\times 698$
$10513=5\times 28+11\times 943$
$10657=29\times 353+7\times 60$
$10729=41\times 53+23\times 372$
$10753=5\times 351+11\times 818$
$10993=5\times 156+7\times 1459$
$11113=5\times 611+17\times 474$
$11161=7\times 66+13\times 823$
$11257=17\times 190+23\times 349$
$11329=11\times 140+13\times 753$
$11353=7\times 19+17\times 660$
$11497=7\times 60+11\times 1007$
$11593=11\times 40+19\times 587$
$11617=13\times 245+17\times 496$
$11689=7\times 264+13\times 757$
$11833=7\times 20+11\times 1063$
$11953=5\times 22+13\times 911$
$12049=19\times 156+23\times 395$
$12073=7\times 15+11\times 1088$
$12097=11\times 120+13\times 829$
$12241=13\times 126+23\times 461$
$12289=19\times 165+23\times 398$
$12409=13\times 63+19\times 610$
$12433=13\times 160+17\times 609$
$12457=19\times 330+23\times 269$
$12553=11\times 230+13\times 771$

$12577 = 5\times 126 + 13\times 919$	$14593 = 11\times 1123 + 5\times 448$
$12601 = 29\times 132 + 31\times 283$	$14713 = 11\times 399 + 29\times 356$
$12721 = 17\times 52 + 19\times 623$	$14737 = 11\times 80 + 31\times 447$
$12841 = 23\times 86 + 17\times 639$	$14929 = 11\times 42 + 17\times 851$
$12889 = 11\times 195 + 17\times 632$	$15073 = 5\times 366 + 41\times 323$
$13009 = 7\times 23 + 11\times 1168$	$15121 = 11\times 129 + 31\times 442$
$13033 = 5\times 102 + 7\times 1789$	$15193 = 17\times 250 + 31\times 353$
$13177 = 7\times 80 + 11\times 1147$	$15217 = 7\times 117 + 23\times 626$
$13249 = 7\times 13 + 17\times 774$	$15241 = 11\times 78 + 19\times 757$
$13297 = 5\times 153 + 13\times 964$	$15289 = 17\times 469 + 31\times 236$
$13417 = 11\times 40 + 19\times 683$	$15313 = 5\times 281 + 19\times 732$
$13441 = 29\times 110 + 17\times 603$	$15361 = 7\times 305 + 17\times 778$
$13513 = 5\times 126 + 13\times 991$	$15601 = 17\times 56 + 19\times 771$
$13537 = 5\times 63 + 11\times 1202$	$15649 = 11\times 492 + 29\times 353$
$13633 = 5\times 569 + 31\times 348$	$15817 = 5\times 577 + 53\times 244$
$13681 = 11\times 69 + 13\times 994$	$15889 = 7\times 374 + 23\times 577$
$13729 = 17\times 328 + 31\times 263$	$15913 = 11\times 70 + 19\times 797$
$13873 = 11\times 78 + 19\times 685$	$15937 = 7\times 165 + 19\times 778$
$13921 = 11\times 118 + 13\times 971$	$16033 = 7\times 15 + 11\times 1448$
$14281 = 13\times 124 + 41\times 309$	$16057 = 7\times 60 + 19\times 823$
$14401 = 11\times 145 + 19\times 674$	$16249 = 11\times 680 + 37\times 237$
$14449 = 11\times 62 + 13\times 1059$	$16273 = 5\times 322 + 31\times 473$

Bibliography

1. P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, ed. by R. Dirichlet, 4th ed., Braunschweig, 1894, p. 451.

2. L. E. Dickson, *Algebren und ihre Zahlentheorie*, Zürich and Leipzig, 1927, pp. 150–151.

3. O. Perron, *Quadratische Zahlkörper mit Euklidischen Algorithmus*, Math. Ann. vol. 107 (1932) pp. 489–495.

4. A. Oppenheim, *Quadratic fields with and without Euclid's algorithm*, Math. Ann. vol. 109 (1934) pp. 349–352.

5. R. Remak, *Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern*, Jber. Deutschen Math. Verein. vol. 44 (1934) pp. 238–250.

6. N. Hofreiter, *Quadratische Körper mit und ohne Euklidischen Algorithmus*, Monatshefte für Mathematik und Physik vol. 42 (1935) pp. 397–400.

7. E. Berg, *Über die Existenz eines Euklidischen Algorithmus in quadratischen Zahlkörpern*, Kungl. Fysiografiska Sällakapets i Lund Förhandlingar vol. 5 (1935) No. 5.

8. N. Hofreiter, *Quadratische Zahlkörper ohne Euklidischen Algorithmus*, Math. Ann. vol. 110 (1935) pp. 195–196.

9. J. F. Keston, *Existence of a Euclidean algorithm in quadratic fields*, Thesis, Yale University, 1935; cf. Bull. Amer. Math. Soc. vol. 41 (1935) p. 186.

10. H. Behrbohm and L. Rédei, *Dern Euklidische Algorithmus in quadratischen Körpern*, J. Reine Angew. Math. vol. 174 (1935) pp. 192–205.

11. P. Erdös and Ch. Ko, *Note on the Euclidean algorithm*, J. London Math. Soc. vol. 13 (1938) pp. 3–8.

12. H. Heilbronn, *On Euclid's algorithm in real quadratic fields*, Proc. Cambridge Philos. Soc. vol. 34 (1938) pp. 521–526.

13. L. Schuster, *Reelquadratische Zahlkörper ohne Euklidischen Algorithmus*, Monatshefte für Mathematik und Physik vol. 47 (1938) pp. 117–127.

14. A. Brauer, *On the non-existence of the Euclidean algorithm in certain quadratic number fields*, Amer. J. Math. vol. 62 (1940) pp. 697–716.

15. L. Rédei, *Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern*, Math. Ann. vol. 118 (1942) pp. 588–608.

16. L. K. Hua and S. H. Min, *On the distribution of quadratic non-residues and the Euclidean algorithm in real quadratic fields*. II, Trans. Amer. Math. Soc. vol. 56 (1944) pp. 547–569.

17. L. K. Hua and W. T. Sheh, *On the lack of an Euclidean algorithm in* $R(61^{1/2})$, Amer. J. Math. vol. 67 (1945) pp. 209–211.

18. L. Réidei, *Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern*, Matematiskai és Fizikai Lapok vol. 47 (1940) pp. 78–90.

19. H. Davenport, *Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields*, To appear in Proc. London Math. Soc.

OHIO STATE UNIVERSITY