Transactions of Illinois Academy of Sciences
(1982), Volume 75, 1 and 2, pp. 113-119

Computer generated continued fractions

by

P. J. C. Lamont

Continued fraction representations of p-adic numbers are defined. The algorithm for solving Pell's equation $x^2 - N y^2 = 1$, for N not a perfect square, in rational integers using the continued fraction development of $\sqrt{N}$ is given in a form suitable for computer application. Analogous algorithms for solving certain equations $x^2 + N = 0$, in p-adic integers with the usual representation and with the continued fraction representation are developed for odd prime p. Certain of the p-adic continued fractions are periodic.

1. Pell's equation. Assume N is not a perfect square. For $\alpha_0 = \sqrt{N}$, let $q_0 = \lfloor \alpha_0 \rfloor$ the integral part of α_0. Then $\alpha_0 = q_0 + \frac{1}{\alpha_1}$ and this process may be repeated to obtain

$$\sqrt{N} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cdots + \cfrac{1}{q_n + \cfrac{1}{\alpha_{n+1}}}}}$$

For some n, $\alpha_{n+1} = q_0 + \sqrt{N}$ and the continued fraction is periodic [1],2].

We write

$$\sqrt{N} = q_0 \overline{q_1 \cdots q_n 2q_0}.$$

The convergents A_n/B_n to $\sqrt{N}$ are given by $A_0 = q_0$, $B_0 = 1$, $A_1 = q_0 q_1 + 1$, $B_1 = q_1$, and the recurrence relations

$$A_m = q_m A_{m-1} + A_{m-2},$$

and

$$B_m = q_m B_{m-1} + B_{m-2}.$$

Since $A_n^2 - N B_n^2 = (-1)^{n-1}$, $x = A_n$ and $y = B_n$ give a solution to $x^2 - N y^2 = \pm 1$. The values $x = A_{2n+1}$ and $y = B_{2n+1}$ always give a solution of $x^2 - N y^2 = 1$.

Calculation of results with $51 \leq N \leq 99$ yielded data for the table in Figure 1. For a similar table with $2 \leq N \leq 50$ see [2].

$x^2 - Ny^2$

N	Continued fraction for $\sqrt{N}$	x	y	$x^2 - Ny^2$
51	7; 7,14	50	7	1
52	7; 4,1,2,1,4,14	649	90	1
53	7; 3,1,1,3,14	182	25	-1
54	7; 2,1,6,1,2,14	485	66	1
55	7; 2,2,2,14	89	12	1
56	7; 2,14	15	2	1
57	7; 1,1,4,1,1,14	151	20	1
58	7; 1,1,1,1,1,1,14	99	13	-1
59	7; 1,2,7,2,1,14	530	69	1
60	7; 1,2,1,14	31	4	1
61	7; 1,4,3,1,2,2,1,3,4,1,14	29718	3805	-1
62	7; 1,6,1,14	63	8	1
63	7; 1,14	8	1	1
65	8; 16	8	1	-1
66	8; 8,16	65	8	1
67	8; 5,2,1,1,7,1,1,2,5,16	48842	5967	1
68	8; 4,16	33	4	1
69	8; 3,3,1,4,1,3,3,16	7775	936	1
70	8; 2,1,2,1,2,16	251	30	1
71	8; 2,2,1,7,1,2,2,16	3480	413	1
72	8; 2,16	17	2	1
73	8; 1,1,5,5,1,1,16	1068	125	-1
74	8; 1,1,2,1,16	43	5	-1
75	8; 1,1,2,16	26	3	1
76	8; 1,2,1,1,5,4,5,1,1,2,1,16	57799	6630	1
77	8; 1,3,2,3,1,16	351	40	1
78	8; 1,4,1,16	53	6	1
79	8; 1,7,1,16	80	9	1
80	8; 1,16	9	1	1
82	9; 18	9	1	-1
83	9; 9,18	82	9	1
84	9; 6,18	55	6	1
85	9; 4,1,1,4,18	378	41	-1
86	9; 3,1,1,1,8,1,1,1,3,18	10405	1122	1
87	9; 3,18	28	3	1
88	9; 2,1,1,1,2,18	197	21	1
89	9; 2,3,1,2,18	500	53	-1
90	9; 2,18	19	2	1
91	9; 1,1,5,1,5,1,1,18	1574	165	1
92	9; 1,1,2,4,2,1,1,18	1151	120	1
93	9; 1,1,1,4,6,4,1,1,1,18	12151	1260	1
94	9; 1,2,3,7,1,5,1,8,1,5,1,1,3,2,1,18	2143295	221064	1
95	9; 1,2,1,18	39	4	1
96	9; 1,3,1,18	49	5	1
97	9; 1,5,1,1,1,1,1,1,5,1,18	5604	569	-1
98	9; 1,8,1,18	99	10	1
99	9; 1,18	10	1	1

Figure 1.

3

2. The solution of $x^2 + N \equiv 0$ in p-adic integers. Assume that N is not divisible by odd prime p and that $-N$ is a quadratic residue modulo p. The equation $x^2 + N \equiv 0 \pmod{p}$ is solved to yield q_0. Let $A_{-1} = A_0 = q_0$, $A_{m+1} = A_m + q_{m+1} 5^{m+1}$, $A = (A_m^2 + N)/p^{m+1}$, and $B = 2A_{m-1}$. Then q_{m+1} is found as the solution of $A + B x \equiv 0 \pmod{p}$. Then $\alpha = \Sigma q_m 5^m$ is the solution of $x^2 + N = 0$ in p-adic integers with the usual representation. 5-adic integer developments of $\sqrt{-N}$ for suitable N with $1 \leq N \leq 49$ are given in figure 2.

N	q_m
1	2,1,2,2,3,4,2,3,0,3,2
4	1,2,0,2,3,0,4,2,3,3,4
6	2,2,1,1,2,3,2,4,3,1,0,0,1
9	1,4,1,4,4,3,3,0,2,4,2
11	2,3,2,1,4,4,1,1,3,2,0,3
14	1,1,4,0,1,2,3,2,0,4,0,1
16	2,4,0,4,1,1,3,0,2,2,4
19	1,3,2,0,4,4,4,2,0,2,2
21	2,0,1,1,2,4,4,2,0,3,0,0,4
24	1,0,3,2,0,3,4,0,2,1,4
26	2,1,3,4,2,4,1,2,3,1,3
29	1,2,2,0,2,0,0,4,4,1,1,0,2
31	2,2,2,1,1,1,2,3,4,3,0,0,2
34	1,4,3,3,0,2,2,0,2,0,1,1
36	2,3,3,3,4,2,2,1,4,3,0,0,3
39	1,1,1,1,3,0,3,0,1,4,4
41	2,4,2,3,0,2,4,0,4,0,0,0,0,1
44	1,3,4,1,1,0,1,2,3,4,3
46	2,0,2,2,1,0,0,1,3,2,4
49	1,0,4,4,1,2,4,4,4,2,1,2

Figure 2

3. Geometry and convergence.

Theorem 3.1. Let a sequence of integers $q_0, q_1, q_2, \ldots$ and an irrational number α be given. Let $T = \pm 1$, where $r \geq 1$. Let $\alpha_0 = \alpha$ and define, for $n \geq 0$, q_{n+1} by

$$\alpha_n = q_n + \frac{T}{\alpha_{n+1}}.$$

Let $U_{-2} = (\frac{1}{T}, 0)$, $U_{-1} = (0, 1)$ and, for $n \geq 0$,

$$U_n = q_n U_{n-1} + T U_{n-2}.$$

Then, for $n \geq 0$,

$$\alpha_n U_{n-1} + T U_{n-2}$$

is on line $y = \alpha x$.

Proof: $U_0 = q_0 (0, 1) + T (\frac{1}{T}, 0) = (1, q_0)$.

$U_1 = q_1 (1, q_0) + T(0, 1) = (q_1, q_0 q_1 + T)$.

Now $\alpha_0 U_{-1} + T U_{-2} = \alpha_0 (0, 1) + T (\frac{1}{T}, 0) = (1, \alpha_0)$ is on $y = \alpha x$.

Assume that $\alpha_k U_{k-1} + T U_{k-2}$ is on $y = \alpha x$. Consider

$$\begin{aligned} y &= \alpha_{k+1} U_k + T U_{k-1} \\ &= T U_{k-1} + \alpha_{k+1}(q_k U_{k-1} + T U_{k-2}) \\ &= \alpha_{k+1} T U_{k-2} + (\alpha_{k+1} q_k + 1) U_{k-1} \\ &= \alpha_{k+1} T U_{k-2} + \alpha_{k-1}(\alpha_k + \frac{T}{\alpha_{k+1}}) U_{k-1} \\ &= \alpha_{k+1}(T U_{k-2} + \alpha_k U_{k-1}). \end{aligned}$$

The result follows by induction.

We write $U_n = (b_n, a_n)$.

Lemma 3.1. $a_n b_{n-1} - a_{n-1} b_n = (-1)^{n-1} T^n$.

Proof: $a_1 b_0 - a_0 b_1 = (\alpha_0 q_1 + T) - q_0 q_1 = T$.

$a_n b_{n-1} - a_{n-1} b_n = -T(a_{n-1} b_{n-2} - a_{n-2} b_{n-1})$.

5

Theorem 3.2. The values a_m/b_m converge to α in the p adic topology.

Proof: By theorem 3.1,

$$\alpha = \frac{\alpha_{k+1} a_k + T a_{k-1}}{\alpha_{k+1} b_k + T b_{k-1}}.$$

Hence $\alpha - \frac{a_n}{b_n} = \frac{T(a_{n-1}b_n - a_n b_{n-1})}{b_n b_{n+1}} = \frac{(-1)^n T^n}{b_n b_{n+1}}$,

by lemma 3.1. Hence, for $|T|$ a power of p, the result follows.

4. p-adic continued fractions. We consider continued fraction developments of p-adic solutions of $x^2 + N = 0$ of the form

$$q_0 + \frac{p}{q_1 - \frac{p}{q_2 - \cdots \frac{p}{q_n - \alpha_{n+1}}}} \qquad (4.1)$$

where $1 \le q_m \le p-1$. The quotients a_m/b_m converge to $\alpha = \sqrt{-N}$. The q_j are chosen so that

$$a_m^2 + N b_m^2 \equiv 0 \pmod{p^{m+1}}.$$

Let q_0 satisfy $q_0^2 + N \equiv 0 \pmod p$. Define $c = (q_0^2 + N)/p$ and $d = 2 q_0$. Then q_1 is the solution of $cx + d \equiv 0 \pmod p$. With $a_0 = q_0$, $b_0 = 1$, $a_1 = q_0 q_1 + p$, and $b_1 = q_1$, define, for $m \ge 2$,

$$a = (a_{m-1}^2 + N b_{m-1}^2)/p^m,$$

and

$$b = 2(a_{m-1} a_{m-2} + N b_{m-1} b_{m-2})/p^{m-1}.$$

Then q_m is the solution of $a x \equiv b \pmod p$.

For $m \ge 2$,

$$a_m = q_m a_{m-1} - p a_{m-2},$$

and

$$b_m = q_m b_{m-1} - p b_{m-2},$$

and we repeat the process.

In cases in which p divides a or c, we must replace p by a higher power of p in the continued fraction development. For p = 5, we find, for example, that $\sqrt{-1} = 2; \overline{1, 3, 1}$ where 1, 3, 1 repeats. For expansions of the form

$$q_0 - \frac{25}{q_1} - \frac{25}{q_2} - \cdots - \frac{25}{q_n} - \frac{25}{q_{n+1}}, \tag{4.2}$$

$\sqrt{-21} = 2; \dot{4}$ and $\sqrt{-49} = 1; \overline{1,2}$.

5. Purely periodic continued fractions. Consider developments of the form

$$q_0 - \frac{p}{q_1} - \frac{p}{q_2} - \cdots - \frac{p}{q_n} - \frac{p}{q_{n+1}} \tag{5.1}$$

with $1 \leq q_i < p-1$ for p-adic solutions of

$$a x^2 + b x + c = 0 \tag{5.2}$$

with a, b, and c rational integers.

Theorem 5.1. If α, satisfying (5.2), has a purely periodic development of the form (5.1), then α and p/β satisfy

$$b_n x^2 - (p b_{n-1} + a_n) x + p a_{n-1} = 0 \tag{5.3}$$

where β is the continued fraction with the reverse period.

Proof: The result follows from theorem 3.1 since

$$\alpha = \frac{a_n \alpha - p a_{n-1}}{b_n \alpha - p b_{n-1}}$$

and

$$\beta = \frac{a_n \beta - p b_n}{a_{n-1} \beta - p b_{n-1}}.$$

It follows that $\alpha\beta = p$. Also, if $\alpha = (P + \sqrt{D})/Q$, where P, D, and Q are integers, then Q divides $P^2 - D$.

For example, for 5-adic numbers $2 + \sqrt{-1} = \overline{4}$, $(3 + \sqrt{-11})/2 = \overline{3}$, $(2 + \sqrt{-16})/2 = \overline{2}$, and $(1 + \sqrt{-19})/2 = \overline{1}$ are all the purely periodic continued fractions of period 1 of the form (5.1). For short period length it is easy to find the equation (5.3) satisfied by α. Thus, to solve $3x^2 + 2x + 5 = 0$ in 5-adics of the form (5.1) we have convergents 1/1, -6/-1, -13/-23, -9/-64, 29/-141, 132/-103, and 251/396 corresponding to a period of length eight with $\alpha = \overline{1,4,1,3,3,4,3,3}$.

References

1. H. Davenport, The Higher Arithmetic, London (1952), 79-114.

2. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford (1954), 129-153.

QIS Department

Western Illinois University

Macomb, Illinois 61455