Karlsruhe
March 28 2016

Note on a Recurrence for Approximation Sequences of p-adic Square Roots

Wolfdieter L a n g [1]

Abstract

A recurrence for the two standard approximation sequences of the p-adic square root $\sqrt{-b}$ is derived for those integers of b with Legendre symbol $\left(\frac{-b}{p}\right) = +1$.

In the context of algebraic congruences to prime-power moduli a standard theorem (see *e.g.*, Nagell [2], Theorem 50, p. 87) states that if a degree m polynomial $f(x)$ over the integers which is primitive (has *gcd* of the coefficients equal to 1) and has a simple root x_1 modulo a prime p, $f(x_1) \equiv 0\,(mod\,p)$, then the congruence $f(x) = 0\,(mod\,p^n)$ has exactly one solution modulo p^n, x_n say, which is congruent to x_1 modulo p for every $n \in \mathbb{N}$. The recursive proof adapts *Newton's* [5] method to modular analysis. In the $p-$adic setting it is also known as *Hensel*-lifting, an application of *Hensel's* lemma [1, 3]. Here we consider $f(x) = x^2 + b$ with non-vanishing integer b. This note originated in a solution of the special exercise 1.8, on p. 33, of [6] (or exercise 5 ii), p. 54, of [1]). The general case will be treated by the following proposition.

Proposition: Recurrence for p-adic $\pm\sqrt{-\mathbf{b}}$ approximation sequences

For $x_n^{(i)} = x_n^{(i)}(p,b)$, the solution of the congruence

$$x_n^{(i)\,2} + b \equiv 0\,(mod\,p^n),\ \text{for}\ n = \{2,\,3,\ldots\}, \tag{1}$$

with an odd prime p and $b \in \mathbb{Z}\setminus\{0\}$, the following recurrence holds. The notation $modp(k,p)$ (like in MAPLE [4]) is used to pick the representative of the residue class of k modulo p from the complete residue system $CRS_0(p) = \{0,\,1,\,\ldots,\,p-1\}$.

$$x_n^{(i)} = modp\left(x_{n-1}^{(i)} + z_i\,((x_{n-1}^{(i)})^2 + b),\,p^n\right)\quad \text{for}\ i = 1,\,2\ \text{and}\ n \ge 2,\ \text{with input}\ \ x_1^{(i)} = x_i, \tag{2}$$

and the two simple roots x_i of $f(x) \equiv x^2 + b\,(mod\,p)$, for b with Legendre symbol $\left(\frac{-b}{p}\right) = +1$, and

$$z_i = z_i(p,x_i) = modp\left(-(2\,x_i)^{p-2},\,p\right)\,. \tag{3}$$

Proof: The following three sequences $P_n^{(i)}$, $K_n^{(i)}$ and $L_n^{(i)}$ will be needed (they always depend on p and b):

$$x_n^{(i)} = x_i + P_n^{(i)}\,p\,, \tag{4}$$

with an odd prime p.

$$x_n^{(i)\,2} + b = K_n^{(i)}\,p^n\,. \tag{5}$$

Like in the proof of *Nagell*'s Theorem 50 [2] (or in *Hensel*-lifting) one uses also

$$x_n^{(i)} = x_{n-1}^{(i)} + L_{n-1}^{(i)}\,p^n,\ \text{for}\ n = 2,\,3,\,\ldots\,. \tag{6}$$

The aim is to find $L_{n-1}^{(i)}$, *i.e.*, a recurrence formula which produces the numbers $x_n^{(i)} = x_n^{(i)}(p,b)$ lying in $CRS_0(p^n) = \{0,\,1\ldots p^n-1\}$. This sequence $\{x_n^{(i)}\}_{n=0}^{\infty}$ with $x_0^{(i)} := 0$ and $x_1^{(i)} := x_i$ (one of the two

[1] wolfdieter.lang@partner.kit.edu, http://www.itp.kit.edu/~wl

simple zeros modulo p) is known as standard sequence representing a p-adic integer from $\mathbb{Z}_p$ (the set of the p-adic integers).

See *e.g.*, Frey [1] III, §4, for the definition of $\mathbb{Z}_p$ as an equivalence class of sequences $\{s_n\}_0^\infty$ with $s_n \in \mathbb{Z}_{(p)}$, the set of rational numbers (in lowest terms) which have no factor p at all (*e.g.*, 0), or p does not divide the denominator which is taken as a positive integer. Furthermore, $s_{n+1} - s_n = L_{p,n}$ with $L_{p,n} \in \{L \in \mathbb{Q} \mid |L|_p \leq \frac{1}{p^n}\}$, with the p-adic valuation $|L|_p := \dfrac{1}{p^{w_p(L)}}$, where $w_p(L)$ is for non-vanishing rational L the integer exponent a_p of p in the factorization $L = \varepsilon \prod p_i^{a_i}$ ($\varepsilon = +1$ or -1). If there is no factor p in the numerator or denominator of L then $w_p(L) = 0$, and one puts $w_p(0) = \infty$. An equivalence relation between such sequences is defined by $\{s_n\} \sim \{s'_n\}$ iff $s_n \equiv s'_n \mod (\mathbb{Z}_{(p)}\, p^n)$. This notation stands for $s_n - s'_n = r_{p,n}$ with $r_{p,n} \in \{y \cdot p^n \mid y \in \mathbb{Z}_{(p)}\} = \{r \in \mathbb{Q} \mid |r|_p \leq \frac{1}{p^n}\}$. (In [1] $|s|_p$ is called $\varphi_p(s)$, and our powers of p are n, not $n+1$.)

From eq. (4) with $P_1^{(i)} = 0$ and eq. (5) we have, for $n \geq 2$,

$$K_n^{(i)} = \frac{x_n^{(i)\,2} + b}{p^n} = \frac{K_1^{(i)} + 2\,x_i\,P_n^{(i)} + p\,P_n^{(i)\,2}}{p^{n-1}} \in \mathbb{N}_0\ . \tag{7}$$

For $n = 1$ this is trivial because $P_1^{(i)} = 0$. A special rôle plays $K_1^{(i)} = \dfrac{x_i^2 + b}{p}$, with the zeros x_i. Eq. (7) determines $K_n^{(i)}$, for $n \geq 2$, in terms of x_i and $P_n^{(i)}$ (and b, p).

The digits of the p-adic integer are related to

$$L_{n-1}^{(i)} = \frac{x_n^{(i)} - x_{n-1}^{(i)}}{p^{n-1}},\ \text{for integer } n \geq 2. \tag{8}$$

Namely, the coefficient of p^n in the p-adic expansion is $L_n^{(i)}$, $n \geq 1$, starting with $L_0^{(i)} := x_i$. Now eq. (6) is used in computing $K_n^{(i)}\,p^n = x_n^{(i)\,2} + b$. This yields $K_{n-1}^{(i)}\,p^{n-1} + 2\,x_{n-1}^{(i)}\,L_{n-1}^{(i)}\,p^{n-1} + L_{n-1}^{(i)\,2}\,p^n\,p^{n-2}$. After elimination of $x_{n-1}^{(i)}$ with eq. (4) one has

$$K_n^{(i)}\,p^n = p^{n-1}\left(2\,x_i\,L_{n-1}^{(i)} + K_{n-1}^{(i)}\right) + p^n\left(p^{n-2}\,L_{n-1}^{(i)\,2} + 2\,P_{n-1}^{(i)}\,L_{n-1}^{(i)}\right)\ . \tag{9}$$

Because an overall factor p^n has to appear also on the *r.h.s.* one chooses

$$L_{n-1}^{(i)} = z_i\,K_{n-1}^{(i)}\,, \tag{10}$$

where the n independent number z_i, for $i = 1, 2$ is determined by

$$2\,x_i\,z_i + 1 \equiv 0\,(mod\,p)\ . \tag{11}$$

This is a linear congruence, and because $\gcd(2\,x_i, p) = \gcd(x_i, p) = 1$, the solution is unique, and by *Fermat*'s little theorem given by (see *e.g.*, *Nagell*, Theorem 38, pp. 76-77)

$$z_i \equiv -(2\,x_i)^{p-2}\,(mod\,p)\ . \tag{12}$$

(One might bother about this special choice of $L_{n-1}^{(i)}$, but the general requirement would be $2\,x_i\,L_{n-1}^{(i)} + K_{n-1}^{(i)} = 0\,(mod\,p)$ with the unique solution $L_{n-1}^{(i)} \equiv -(2\,x_i)^{p-2}\,K_{n-1}^{(i)}\,(mod\,p)$ which has just been found.)

This now becomes a recurrence for $K_n^{(i)}$ (after dividing by p^n) for $n \geq 2$ with input $K_1^{(i)}$:

$$K_n^{(i)} = K_{n-1}^{(i)}\left[\frac{1 + 2\,x_i\,z_i}{p} + z_i^2\left(K_1^{(i)} + 2\,x_i\,P_{n-1}^{(i)} + p\,P_{n-1}^{(i)\,2}\right) + 2\,z_i\,P_{n-1}^{(i)}\right]\ . \tag{13}$$

Due to eq. (7) this could be converted to an equation involving only the $P_n^{(i)}$ and $P_{n-1}^{(i)}$ (and p, x_i, z_i, $K_1^{(i)}$). But this is not of interest here.

The proposition follows now from eq. (6) after the choice of $L_{n-1}^{(i)}$ from eqs. (10) and (11) which was valid modulo p:

$$x_n^{(i)} = x_{n-1}^{(i)} + z_i\, K_{n-1}^{(i)}\, p^{n-1}\, (mod\, p^n)\ . \tag{14}$$

Inserting $K_{n-1}^{(i)}\, p^{n-1}$ from eq. (7) (with $n \to n-1$) and replacing $K_1^{(i)}$ leads to

$$x_n^{(i)} = x_{n-1}^{(i)} + p\, z_i \left(\frac{x_i^2 + b}{p} + 2\, x_i\, \frac{\hat{x}_{n-1}^{(i)}}{p} + \frac{\hat{x}_{n-1}^{(i)\,2}}{p} \right) (mod\, p^n)\ , \tag{15}$$

where we have used $p\, P_{n-1}^{(i)} = \hat{x}_{n-1}^{(i)} = x_{n-1}^{(i)} - x_i$. The second term on the *r.h.s.* simplifies after cancellation of the x_i and $x_{n-1}^{(i)}\, x_i$ terms to $z_i\, (x_{n-1}^{(i)\,2} + b)$.

Because we look for $x_n^{(i)} \in CRS_0(p^n) = \{0, 1, \ldots p^n - 1\}$ we use the $modp(a, p^n)$ notation explained in the proposition (replacing $(mod\, p^n)$). This then produces the asserted equation of the proposition. $\square$

From *Nagel*'s [2] proof of his Theorem 50, pp. 86 - 87, one would obtain the recurrence

$$x_n^{(i)} = modp\left(x_{n-1}^{(i)} + (-2\, (x_{n-1}^{(i)})^{p-2})\, ((x_{n-1}^{(i)})^2 + b),\, p^n\right). \tag{16}$$

for $i = 1,\, 2$ and $n \geq 2$, with input $x_1^{(i)} = x_i$.

The difference to the recurrence derived here is that the z_i of eq. (3) which needs besides p only the input x_i is in this case replaced by a similar quantity which used $x_{n-1}^{(i)}$.

The data p, b, x_1, x_2, z_1, z_2 given in the *Table*, for $p = 3, 5, \ldots, 31$ refers to $f(x) = x^2 + b \equiv 0\, (mod\, p)$ with $b > 0$ and *Legendre* symbol $\left(\frac{-b}{p}\right) = +1$, and with $b < 0$ and *Legendre* symbol $\left(\frac{b}{p}\right) = +1$. Because of $(mod\, p)$ the inputs x_1 and x_2, and thus also z_1 and z_2, are the same for corresponding positive or negative b. The different sequences for $n \geq 2$ arise from the b appearance in the recurrence under $(mod\, p^n)$.

Some examples: $\mathbf{p = 5}$: $b = 1, x_1 = 2, z_1 = 1$ produce the standard sequence $\{x_n^{(1)}\}_0^\infty$ (where a leading 0 for $n = 0$ has been added) $[0, 2, 7, 57, 182, 2057, 14557, 45807, 280182, 280182, \ldots]$ which is A048898. $b = 1, x_3 = 2, z_1 = 2$ yields $[0, 3, 18, 68, 443, 1068, 1068, 32318, 110443, 1672943, \ldots]$ which is A048899. $b = 4, x_1 = 2, z_1 = 2$ yields $[0, 1, 11, 11, 261, 2136, 2136, 64636, 220886, 1392761, \ldots]$ which is A268922 and $b = 4, x_2 = 4, z_2 = 3$ yields $[0, 4, 14, 114, 364, 989, 13489, 13489, 169739, 560364, \ldots]$ which is A269590. The corresponding digit sequences $\{L_n^{(i)}\}_0^\infty$ from eq. (8) and $L_0^{(i)} = x_i$ are given in A210850, A210851, A269591, A269592, respectively. The $\{K_n^{(i)}\}_0^\infty$ of eq. (5) sequences are found under A210848, A210849, A269593 , A269594, respectively.

The seqeunces for $\mathbf{p = 3}$, $\mathbf{b = 2}$, with $x_1 = 1$, $z_1 = 1$ and $x_1 = 2$, $z_2 = 2$ are A268924, A271223, A271225, and A271222, A271224, A271226.

Of course, one may also use the recurrence for other members of the residue classes of the considered b. For example, for $p = 5$, $b = 6$ also with $x_1 = 2$ and $z_1 = 1$ one finds $[2, 12, 37, 162, 1412, 10787, 42037, 354537, 1526412, 3479537, \ldots]$, the standard sequence for the 5-adic integer $\sqrt{-6}$ (call it $+\sqrt{-6}$) . The other approximation sequence for $x_2 = 3$ and $z_2 = 4$, $-\sqrt{-6}$, is $[3, 13, 88, 463, 1713, 4838, 36088, 36088, 426713, 6286088, \ldots]$.

In *Maple* [4] one can use the package with(padic) and then the two expansion for the p-adic integers $\pm\sqrt{-b}$ are given, with $[evalp(RootOf(x^2 + b), p, N)]$, up to Order p^{N-1}.

References

[1] Gerhard Frey, Elementare Zahlentheorie, Vieweg & Sohn, Braunschweig, 1984

[2] Trygve Nagell, Introduction to Number Theory, Chelsea Publishing Company, New York, 1964.

[3] Hensel's lemma, https://en.wikipedia.org/wiki/Hensel%27s_lemma

[4] Maple http://www.maplesoft.com/

[5] Newton's method, https://en.wikipedia.org/wiki/Newton%27s_method

[6] Joseph H. Silverman and John Tate, Rational Points on Elliptic Curves, Springer, 1992

Keywords: p-adic square roots, Hensel lifting

AMS MSC number: 11D09, 11S05

OEIS A-numbers: A048898, A048899, A210848, A210849, A210850, A210851, A268922, A268924, A269590, A269591, A269592, A269593, A269594, A271222, A271223, A271224, A271225, A271226.

Table: Odd primes, radicands $-b$, zeros x_1, x_2 and numbers z_1, z_2

Prime p	b	b	x_1	x_2	z_1	z_2	Prime p	b	b	x_1	x_2	z_1	z_2
3	2	−1	1	2	1	2	23	5	−18	8	15	10	13
5	1	−4	2	3	1	4		7	−16	4	19	20	3
	4	−1	1	4	2	3		10	−13	6	17	21	2
7	3	−4	2	5	5	2		11	−12	9	14	14	9
	5	−2	3	4	1	6		14	−9	3	20	19	4
	6	−1	1	6	3	4		15	−8	10	13	8	15
11	2	−9	3	8	9	2		17	−6	11	12	1	22
	6	−5	4	7	4	7		19	−4	2	21	17	6
	7	−4	2	9	8	3		20	−3	7	16	18	5
	8	−3	5	6	1	10		21	−2	5	18	16	7
	10	−1	1	10	5	6		22	−1	1	22	11	12
13	1	−12	5	8	9	4	29	1	−28	12	17	6	23
	3	−10	6	7	1	12		4	−25	5	24	26	3
	4	−9	3	10	2	11		5	−24	13	16	10	19
	9	−4	2	11	3	10		6	−23	9	20	8	21
	10	−3	4	9	8	5		7	−22	14	15	1	28
	12	−1	1	12	6	7		9	−20	7	22	2	27
17	1	−16	4	13	2	15		13	−16	4	25	18	11
	2	−15	7	10	6	11		16	−13	10	19	13	16
	4	−13	8	9	1	16		20	−9	3	26	24	5
	8	−9	3	14	14	3		22	−7	6	23	12	17
	9	−8	5	12	5	12		23	−6	8	21	9	20
	13	−4	2	15	4	13		24	−5	11	18	25	4
	15	−2	6	11	7	10		25	−4	2	27	7	22
	16	−1	1	16	8	9		28	−1	1	28	14	15
19	2	−17	6	13	11	8	31	3	−28	11	20	7	24
	3	−16	4	15	7	12		6	−25	5	26	3	28
	8	−11	87	12	4	15		11	−20	12	19	9	22
	10	−9	3	16	3	16		12	−19	9	22	12	19
	12	−7	8	11	13	6		13	−18	7	24	11	20
	13	−6	5	14	17	2		15	−16	4	27	27	4
	14	−5	9	10	1	18		17	−14	13	18	25	6
	15	−4	2	7	14	5		21	−10	14	17	21	10
	18	−1	1	18	9	10		22	−9	3	28	5	26
								23	−8	15	16	1	30
								24	−7	10	21	17	14
								26	−5	6	25	18	13
								27	−4	2	29	23	8
								29	−2	8	23	29	2
								30	−1	1	30	15	16