THE LINEAR CUBIC p-ADIC RECURRENCE AND ITS VALUE FUNCTION

BY

HAROLD C. KURTZ

1. Introduction and summary of results

Let

$$\Omega_{n+3} = P\Omega_{n+2} - Q\Omega_{n+1} + R\Omega_n \tag{1.1}$$

be a linear cubic p-adic recurrence with coefficients in the rational p-adic field R_p. The roots α, β, and γ of the characteristic polynomial

$$f(Z) = Z^3 - PZ^2 + QZ - R = (Z - \alpha)(Z - \beta)(Z - \gamma)$$

are p-adic algebraic numbers generating the root field $R_p(\alpha, \beta, \gamma) = \mathfrak{R}_p$ and will be assumed distinct and nonzero.

Let $(W_n) : W_0, W_1, \cdots, W_n, \cdots$ be a solution of (1.1) with given initial values W_0, W_1, and W_2 in R_p not all zero, and let $w_n = \phi(W_n)$ be the p-adic value of W_n. We investigate the following "valuation problem": Given a sequence (W_n) satisfying (1.1) with specified initial values as above, to determine $\phi(W_n)$. This problem is trivial if one of the ratios of the roots of $f(Z)$ is a root of unity in $\mathfrak{R}_p$; $f(z)$ is then termed degenerate. Hence we assume nondegeneracy, i.e., $(\alpha/\beta)^n$, $(\beta/\gamma)^n$, and $(\alpha/\gamma)^n \neq 1$ for all positive integers n.

We show that we may restrict ourselves to recurrences whose coefficients and initial values are p-adic integers where at least one coefficient and one initial value are p-adic units. Except when $p = 2$ or 3, we need only consider these cases:

I P, Q, and R all p-adic units,
II P and Q units, R a non-unit,
III P a unit, Q and R non-units.

In Case III, the determination of $\phi(W_n)$ is trivial; for $n \geqq$ some n_0, $\phi(W_n)$ equals a constant. In II, the Hensel Lemma enables us to analyze the valuation of the cubic recurrence in terms of the valuation of the quadratic recurrence (results (3.2)–(3.5)), explicit formulas for the latter being given in Ward's paper [2]. Case I has been studied by Ward [1] when coefficients and initial values are rational integers; the results are extended to recurrences where these are p-adic integers in Section 4.

It appears likely that for a given integer t, the valuation problem for the t^{th} order nondegenerate recurrence

$$\Omega_{n+t} = A\Omega_{n+(t-1)} + \cdots + M\Omega_n$$

Received August 24, 1962.

may also be reduced to cases where all coefficients are p-adic integers and at least one is a p-adic unit. However, the complexity of reduction when $t = 3$, when contrasted with the simplicity of case $t = 2$ [2], indicates that a general reduction procedure for all t would be quite complicated, for as the order of the recurrence increases, the number of cases which must be considered also increases. Including $p = 2$ and 3, the quadratic recurrence reduces to two cases, the cubic to six.

2. Reduction of problem to Cases I, II, and III

For any given positive integer k, let j be a fixed integer in $[0, k)$. Let $(W_n^{(k)})$ be any one of the k subsequences of (W_n)

$$W_n^{(k)} = W_{kn+j} \qquad (n = 0, 1, 2, \cdots),$$

and let $f_k(Z) = (Z - \alpha^k)(Z - \beta^k)(Z - \gamma^k) = Z^3 - P_k Z^2 + Q_k Z - R_k$. Then each $(W_n^{(k)})$ is a solution of

$$\Omega_{n+3} = P_k \Omega_{n+2} - Q_k \Omega_{n+1} + R_k \Omega_n, \tag{2.1}$$

and $f_k(z)$ is nondegenerate. If $\phi(W_n^{(k)})$ can be found for each j, $\phi(W_n)$ is known.

Let $p_k = \phi(P_k)$, $q_k = \phi(Q_k)$, $r_k = \phi(R_k)$, and $d_k = \min\{p_k, [q_k/2], [r_k/3]\}$. Then $(U_n^{(k)}) = (W_n^{(k)} \cdot p^{-nd_k})$ is a solution of

$$\Omega_{n+3} = P_k' \Omega_{n+2} - Q_k' \Omega_{n+1} + R_k' \Omega_n, \tag{2.2}$$

where $p_k' = \phi(P_k') = p_k - d_k$, $q_k' = q_k - 2d_k$, $r_k' = r_k - 3d_k$. Hence P_k', Q_k', and R_k' are p-adic integers, and $\phi(W_n^{(k)})$ is known if $\phi(U_n^{(k)})$ is. By elementary algebra,

$$P_2 = P^2 - 2Q, \qquad Q_2 = Q^2 - 2RP, \qquad R_2 = R^2,$$

$$P_3 = P^3 - 3PQ + 3R, \qquad Q_3 = Q^3 + 3R^2 - 3PQR, \qquad R_3 = R^3.$$

When $k = 1$, P_1', Q_1', and R_1' are p-adic integers. Hence we are justified in assuming to begin with that *the coefficients P, Q, and R of* (1.1) *are p-adic integers*. Assuming this, let $f = \min\{\phi(W_0), \phi(W_1), \phi(W_2)\}$; then $(W_n') = (W_n \cdot p^{-f})$ is a solution of (1.1) with $\phi(W_n') = \phi(W_n) - f$. Hence W_0', W_1', and W_2' are p-adic integers, and at least one is a p-adic unit. We therefore assume to begin with that *the initial values of (W_n) are integers, and at least one is a p-adic unit.* Henceforth, in transitions to subsequences $(W_n^{(k)})$, it will be assumed that the preceding transformation is made on the terms of $(W_n^{(k)})$.

With the two preceding assumptions, let $d = \min\{p_1, [q_1/2], [r_1/3]\}$, and $U_n = W_n \cdot p^{-nd}$; then (U_n) satisfies (2.2) with $k = 1$. If $d = p_1$, then $p_1' = 0$ and P_1' is a unit; if $d = [q_1/2]$, then $q_1' = 0$ or 1; if $d = [r_1/3]$, $r_1' = 0$, 1, or 2. Since it is sufficient to determine $\phi(U_n)$, we see on examining the three possible values of d that we may assume one of the following holds:

(1) $\phi(P) = 0,\ \ \phi(Q)$ and $\phi(R) \geqq 0$;
(2a) $\phi(Q) = 0,\ \ \phi(P) \geqq 1,\ \ \phi(R) \geqq 0$;
(2b) $\phi(Q) = 1,\ \ \phi(P) \geqq 1,\ \ \phi(R) \geqq 1$;
(3a) $\phi(R) = 0,\ \ \phi(P)$ and $\phi(Q) \geqq 1$;
(3b) $\phi(R) = 1,\ \ \phi(P) \geqq 1,\ \ \phi(Q) \geqq 2$;
(3c) $\phi(R) = 2,\ \ \phi(P) \geqq 1,\ \ \phi(Q) \geqq 2$.

We now show we may assume that *at least one of P, Q, R is a p-adic unit*; of the above, (2b), (3b), and (3c) must be dealt with.

(2b) If $\phi(R) = 1$, consider $(W_n^{(3)})$. Then prime $p \neq 3$ implies $\phi(P_3) = p_3 = 1$, $q_3 = 2$, $r_3 = 3$; hence $d_3 = 1$ and $\phi(R_3') = 0$. If $p = 3$, we similarly have R_3' a p-adic unit. When $\phi(R) \geqq 2$, consider $(W_n^{(2)})$. Then $p \neq 2$ implies $\phi(P_2') = 0$, and $p = 2$ implies $\phi(Q_2') = 0$.

Hence in (2b), $\phi(W_n)$ is known if we can find the valuation of sequences $(U_n^{(k)}) = (W_n^{(k)} \cdot p^{-nd_k})$ in which at least one coefficient is a p-adic unit. Cases (3b) and (3c) may be similarly dealt with by considering subsequences $(W_n^{(3)})$.

Finally we show we may further restrict ourselves to the following six subcases:

Ia P, Q and R all p-adic units,
Ib $p = 2$, Q and R units, P a double unit,
Ic $p = 3$, R a unit, P and Q triple units,
IIa P and Q units, R a non-unit,
IIb $p = 2$, P a double unit, Q a unit, R a non-unit,
III P a unit, Q and R non-units.

Since at least one coefficient may already be assumed a unit, it remains to reduce the following four cases to the preceding six:

(1) $\phi(Q) = 0,\ \ \phi(P)$ and $\phi(R) > 0$;
(2) $\phi(R) = 0,\ \ \phi(P)$ and $\phi(Q) > 0$;
(3) $\phi(P) > 0,\ \ \phi(Q) = \phi(R) = 0$;
(4) $\phi(Q) > 0,\ \ \phi(P) = \phi(R) = 0$.

(1) Consider $(W_n^{(2)})$. If $p \neq 2$, $\phi(P_2) = \phi(Q_2) = 0$, $\phi(R_2) > 0$; this is Case IIa. If $p = 2$, $P_2 = 2 \times$ unit, $\phi(Q_2) = 0$, $\phi(R_2) > 0$; Case IIb.

(2) Consider $(W_n^{(3)})$. If $p \neq 3$, reduce to Ia; if $p = 3$, to Ic.

(3) Consider $(W_n^{(2)})$. If $p \neq 2$, reduce to Ia; if $p = 2$, to Ib.

(4) If $p \neq 2$, consider $(W_n^{(2)})$ and reduce to Ia. If $p = 2$, consider $(W_n^{(3)})$; here $\phi(Q_3) = \phi(R_3) = 0$. If $\phi(P_3) > 0$, then we have (3) with $p = 2$, and this has been reduced to Ib; if P_3 is a unit, then we have Ia.

3. Cases II and III

We investigate Case IIa in detail employing the Hensel Lemma, subsequently applying the same methods to IIb; the triviality of III will then be shown.

Case IIa. $\phi(P) = \phi(Q) = 0, \phi(R) > 0$. Then

$$f(Z) = Z^3 - PZ^2 + QZ - R \equiv Z(Z^2 - PZ + Q) \ (p).$$

By the Hensel Lemma,

$$f(Z) = (Z - \alpha)(Z^2 - P^*Z + Q^*) = (Z - \alpha)g(Z) \quad \text{in } R_p,$$

where $Z - \alpha \equiv Z \ (p)$ and $Z^2 - P^*Z + Q^* \equiv Z^2 - PZ + Q \ (p)$. In $R_p(\beta)$,

$$f(Z) = (Z - \alpha)g(Z) = (Z - \alpha)(Z - \beta)(Z - \gamma),$$

with $\phi(\beta) = \phi(\gamma) = 0$. Then

$$\begin{aligned} W_n &= A\alpha^n + B\beta^n + C\gamma^n \\ &= ((\gamma - \beta)/\delta)[A^*\alpha^n + B^*\beta^n + C^*\gamma^n] = ((\gamma - \beta)/\delta)W_n^*. \end{aligned}$$

Here $\delta = (\alpha - \beta)(\beta - \gamma)(\alpha - \gamma)$ is the square root of the discriminant of $f(z)$, and

$$\begin{aligned} A^* &= -[W_2 - W_1P^* + W_0Q^*], \\ B^* &= [W_2 - W_1(\alpha + \gamma) + W_0\alpha\gamma](\gamma - \alpha)/(\gamma - \beta), \\ C^* &= [W_2 - W_1(\alpha + \beta) + W_0\alpha\beta](\alpha - \beta)/(\gamma - \beta). \end{aligned}$$

From [2], $(B^*\beta^n + C^*\gamma^n) = (V_n^*)$ satisfies

$$\Omega_{n+2} = P^*\Omega_{n+1} - Q^*\Omega_n \tag{3.1}$$

with characteristic polynomial $g(z)$ having unit coefficients, and

$$V_n^* = \frac{(V_1^* - V_0^*\gamma)\beta^n - (V_1^* - V_0^*\beta)\gamma^n}{\beta - \gamma}.$$

Then

$$V_0^* = [W_2 - \alpha^2W_0 + (\alpha W_0 - W_1)P^*]$$

and

$$V_1^* = [W_2\alpha - W_1(\alpha^2 + Q^*) + W_0\alpha P^*]$$

are p-adic integers, and so (V_n^*) is a quadratic *integral* recurrent sequence. Letting $f = \min\{\phi(V_0^*), \phi(V_1^*)\}$, define

$$W_n' = p^{-f}\cdot W_n^* = p^{-f}(A^*\alpha^n + V_n^*) = (A'\alpha^n + V_n');$$

then $\phi(W_n) = \phi((\gamma - \beta)/\delta) + f + \phi(W_n')$. The problem is to determine the valuation of $(W_n') = (A'\alpha^n + V_n')$ where (V_n') satisfies the quadratic integral recurrence (3.1) with at least one of V_0' or V_1' a unit.

We refer to [2] to determine $\phi(V_n')$. If $\phi(V_n') = 0$ for all n, then for $n \geqq$ some n_0

$$w_n' = \phi(W_n') = 0, \tag{3.2}$$

since $\phi(\alpha) > 0$ implies $\phi(A'\alpha^n) > 0$ for $n \geqq n_0$.

Otherwise let V'_h be the first term of (V'_n) with positive value, and let ν denote the following p-adic integer, expressed as a p-adic logarithm:

$$\nu = \log [V'_{h+1} - V'_h \gamma / V'_{h+1} - V'_h \beta] / \log (\gamma/\beta)^r.$$

Here $r = 1$ if $\phi(\beta - \gamma) > 0$. If $\phi(\beta - \gamma) = 0$, sequence (V'_n) is termed ordinary, and r is the least positive n for which $\phi((\beta^n - \gamma^n)/(\beta - \gamma))$, denoted by l_n, is $\geqq 1$. [2] now yields the following:

If (V'_n) is ordinary and $\phi(V'_h) < l_r$, then by [2, Theorem 9.3]

$$\begin{aligned} \phi(V'_n) &= 0 && \text{if} \quad n - h \not\equiv 0 \ (r), \\ \phi(V'_n) &= \phi(V'_h) && \text{if} \quad n - h \equiv 0 \ (r). \end{aligned}$$

Here, there is an n_0 such that $n \geqq n_0$ implies

$$\begin{aligned} \phi(W'_n) &= 0 && \text{if} \quad n - h \not\equiv 0 \ (r), \\ \phi(W'_n) &= \phi(V'_h) && \text{if} \quad n - h \equiv 0 \ (r). \end{aligned} \tag{3.3}$$

Since l_r will usually be 1, the above situation is rare. When the above is not the case, then we have from [2, Theorems 10.1 and 11.2]

$$\begin{aligned} \phi(V'_n) &= 0 && \text{if} \quad n - h \not\equiv 0 \ (r), \\ \phi(V'_n) &= \phi(\nu - (n - h)/r) + l_r && \text{if} \quad n - h \equiv 0 \ (r). \end{aligned} \tag{3.4}$$

For those n for which $\phi(A'\alpha^n) \neq \phi(V'_n)$, we then have

$$\phi(W'_n) = \min \{\phi(A'\alpha^n), \phi(V'_n)\}.$$

Since $\phi(V'_n) = 0$ if $n - h \not\equiv 0 \ (r)$, there is an n_0 such that

$$\phi(W'_n) = 0 \quad \text{if} \quad n \geqq n_0 \quad \text{and} \quad n - h \not\equiv 0 \ (r). \tag{3.5}$$

Criteria for (V'_n) to have terms of positive valuation are given by [2, Theorems 8.1, 9.2, and 11.1], the last giving necessary and sufficient conditions for the value function $\phi(V'_n)$ to be unbounded.

Note that in general we cannot say more about $\phi(W'_n)$ by separately examining $\phi(V'_n)$ and comparing with $\phi(A'\alpha^n)$, because for given α, there exist integral sequences (V'_n) satisfying (3.1) with initial values so chosen that

$$\phi(V'_n) = \phi(A'\alpha^n) \quad \text{if} \quad n - h \equiv 0 \ (r).$$

The proof is a consequence of [2, Theorem 12.1] in conjunction with the canonical representation for p-adic integer μ:

$$\mu = \textstyle\sum_{k=0}^{\infty} a_k p^k \qquad (0 \leqq a_k < p),$$

with $A_n = \sum_{k=0}^{n} a_k p^k$ the $(n + 1)^{\text{st}}$ convergent.

Case IIb. $p = 2, \phi(Q) = 0, \phi(P) = 1, \phi(R) > 0$. Then

$$f(Z) \equiv Z(Z^2 + Q) \ (2),$$

and by the Hensel Lemma,

$$f(Z) = (Z - \alpha)(Z^2 - P^*Z + Q^*)$$

in R_2 with $\phi(\alpha) = \phi(R) > 0$ and $\phi(P^*) > 0$. Assume $\phi(P^*) = 1$. Then, as in IIa, $2^{-f} \cdot W_n = ((\gamma - \beta)/\delta) W'_n$ with $W'_n = A'\alpha^n + V'_n$, (V'_n) satisfying (3.1) with at least one initial value a unit. P^* a double unit implies $\phi(\beta - \gamma) > 0$, and so $r = 1$ in (3.4).

If $\phi(V'_n) = 0$ for all n, then $\phi(W'_n) = 0$ for all $n \geqq$ some n_0. Otherwise let V'_h be the first non-unit of (V'_n). Then

$$\phi(V'_n) = \phi(\nu - (n - h)), \tag{3.6}$$

and the valuation of (V'_n) is unbounded, as is

$$\phi(W'_n) = \min\{\phi(A'\alpha^n), \phi(V'_n)\} \quad \text{if} \quad \phi(A'\alpha^n) \neq \phi(V'_n).$$

If P^* had not initially been a double unit, then note that

$$W'_{2n+j} = A'\alpha^{2n+j} + V'_{2n+j} \qquad (j = 0, 1),$$

where $(V'_{2n+j}) = (V''_n)$ satisfies a quadratic recurrence whose coefficients P'' and Q'' are a double unit and a unit respectively [2]. Therefore P^* may be assumed a double unit to begin with.

Case III. $\phi(P) = 0$, $\phi(Q)$ and $\phi(R) > 0$. Then one root of $f(Z)$, say α, must have valuation 0, while β and γ have positive valuations. Consider the expression $W_n = (1/\delta)W'_n = (1/\delta)(A'\alpha^n + B'\beta^n + C'\gamma^n)$. Then for $n \geqq$ some n_0

$$\min\{\phi(B') + n\phi(\beta), \phi(C') + n\phi(\gamma)\} > \phi(A'\alpha^n) = \phi(A'),$$

and so $\phi(W_n) = \phi(A'/\delta)$ for $n \geqq n_0$.

4. Case I

Cases Ia, Ib, Ic will be dealt with by generalizing the results of [1] for rational integral sequences (W'_n) to p-adic integral sequences (W_n). We use the canonical power series representation for p-adic integers together with the fact that proofs in [1] depend upon the behavior of (W'_n) modulo successively higher powers of p in the residue class sequences of (W'_n) modulo p^k. Let $({}_kW'_n)$ be a rational sequence whose corresponding coefficients and initial values have the same $(k+1)^{\text{st}}$ convergents as those of (W_n). Then the residue class sequences of (W_n) and $({}_kW'_n)$ modulo p^i $(i \leqq k+1)$ are identical. If $\max_{n \leqq n_0}\{\phi(W_n)\} = k$, then $\phi(W_n) = \phi({}_kW'_n)$ for $n \leqq n_0$; if $\phi(W_n) \leqq k$ for all n, then $\phi(W_n) = \phi({}_kW'_n)$ for all n. From such arguments and [1], it follows that for (W_n) of Case I with at least one initial value a unit, $\min\{\phi(W_n), \phi(W_{n+1}), \phi(W_{n+2})\} = 0$ for all n, that is, (W_n) is not a null sequence.

Define $\Delta(W)$, restricted period ρ_k, rank of apparition, and ideal cube with respect to a p-adic integral (W_n) in the manner of [1]. Here $\alpha^n \equiv a \ (p^k)$ means $\alpha^n - a = \alpha_0 p^k$ with α_0 a p-adic algebraic integer. We say the fundamental prime p of R_p is *an ideal cube of order* $l \geqq 1$ *with respect to a given p-adic* (W_n) *if* $\rho_1 = 1$ and $l = \min \{\phi(\alpha - \beta), \phi(\beta - \gamma), \phi(\alpha - \gamma)\}$. Then by the type of argument used in the preceding paragraph, the following theorems and lemmas of [1], as well as the accompanying discussions, are proved valid for p-adic integral (W_n): Theorems 5.1–5.3, 6.1, 7.1, 7.2; Lemmas 3.3, 5.1, 5.2. The following corrections of errors in [1] should be noted: the hypothesis of Lemma 3.3 should be "prime not dividing $R\delta^2\Delta(W)$"; Theorem 5.3 should conclude, "if and only if p does not divide $\Delta(W)$ and $H^2 \equiv K^2 - 4HM \pmod p$."

References

1. MORGAN WARD, *The laws of apparition and repetition of primes in a cubic recurrence*, Trans. Amer. Math. Soc., vol. 79 (1955), pp. 72–90.
2. ———, *The linear p-adic recurrence of order two*, Illinois J. Math., vol. 6 (1962), pp. 40–52.

CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA