Recurrent sequences modulo prime powers

R.G.E. Pinch

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, 16 Mill Lane, Cambridge CB2 1SB

1 Introduction

In this paper we study the possible periods of linear recurrent sequences modulo p^n for prime p. The maximum possible period depends on the degree and ramification index of the p-adic field generated by the roots of the auxiliary polynomial of the recurrence: in most cases, this is sufficient to determine the maximum period completely. In any case, the maximum period modulo p^n is determined by the period modulo p^2 if p is odd, or modulo 2^3.

2 Some results on binomial coefficients

We collect together in this section some results about binomial coefficients.

Lemma 1. *Fix a prime p. For positive integer n let $\nu(n)$ be the exponent of the exact power of p dividing n and $S(n)$ be the sum of the digits of n expressed to base p.*

1. $\nu(n!) = \dfrac{n - S(n)}{p-1}$.
2. $\nu\left(\binom{n}{r}\right) = \dfrac{S(n-r) + S(r) - S(n)}{p-1}$.
3. *If p^b divides n then* $\nu\left(\binom{n}{p^b}\right) = \nu(n) - b$.
4. *If $a > \nu(r)$ then* $\nu\left(\binom{p^a}{r}\right) = a - \nu(r)$.

Proof. Part (1) is well-known and easy; (2) follows directly from (1). We can express the right-hand side of (2) as the total of the "carry" digits in the subtraction of r from n in base p.

From (2) we can deduce that if $\nu(n) = a$, so that there are exactly a zeroes ending the base p expansion of n, then the subtraction of p^b from n results in just $a - b$ carries to the left. Hence we obtain (3).

We deduce (4) from (3) when a is a power of p. Otherwise, let $\nu(r) = b$ and let p^c be a non-zero digit other than the last in the base p expansion of r, so that $c > b$. We have

$$\binom{p^a}{r} \bigg/ \binom{p^a}{r - p^c} = \frac{(p^a - r + p^c)!(r - p^c)!}{(p^a - r)!(r)!},$$

but $S(p^a - r + p^c) = S(p^a - r) + 1$ and $S(r) = S(r - p^c) + 1$ so

$$\nu((p^a - r + p^c)!) - \nu((p^a - r)!) = \frac{p^c}{p - 1}$$

and

$$\nu((r)!) - \nu((r - p^a c)!) = \frac{p^c}{p - 1}.$$

Hence

$$\nu\left(\binom{p^a}{r}\right) = \nu\left(\binom{p^a}{r - p^c}\right)$$

and the result follows by induction on r. ∎

Parts (1) and (2), with the observation about 'carry' digits, are due to Kummer [1] pp 115–117 (507–509). Similar results have been obtained by Singmaster [2] and Goetgheluck [3]. Early results in this direction are recorded by Dickson [4] volume I, chapter 9.

Lemma 2. *The binomial coefficients* $\binom{n}{l}$ *for* $1 \le l \le k$ *are all divisible by* p^r*, for fixed* $r \ge 1$*, if and only if* n *is divisible by* p^{r+t-1}*, where* p^t *is the smallest power of* p *which is greater than* k*.*

Proof. Suppose that p^{r+t-1} divides n. For $l \le k$ we have

$$\binom{n}{l} = \frac{n}{l}\binom{n-1}{l-1}.$$

The power of p in $\frac{n}{l}$ is at least p^r since $1 \le l < p^t$ and so l is not divisible by p^t. Since $\binom{n-1}{l-1}$ is an integer, the power of p dividing $\binom{n}{l}$ is at least p^r, as required.

Conversely, suppose that p^{r+t-1} does not divide n, so that $a = \nu(n) < r + t - 1$. Consider $\binom{n}{p^{t-1}}$. By Lemma 2, this is divisible exactly by $p^{a-(t-1)}$ and $a - (t-1) < r$. Since $p^{t-1} \le k$ by definition of t we see that p^r does not divide all the $\binom{n}{l}$ with $l \le k$. ∎

We can deduce as a corollary that the binomial coefficients $\binom{n}{l}$ are all divisible by p^r for $1 \le l < n$, if and only if n is a power of p and $r = 1$. This contains Theorem 3 of Fine [5].

3 Recurrent sequences over a general field

Fix a field K. We call a sequence $\boldsymbol{x} = (x_n)_{n\ge 0}$ of elements of K a *recurrent sequence* if it is defined by some linear recurrence relation of the form

$$x_{n+d} = a_{d-1}x_{n+d-1} + \dots + a_0 x_n \tag{3.1}$$

with $d \ge 1$, $a_i \in K$ and prescribed initial values $x_0, \dots, x_{d-1}$. The *degree* of the relation is d, and the *auxiliary polynomial* is

$$f(t) = t^d - \left(a_{d-1}t^{d-1} + \dots + a_1 t + a_0\right).$$

We suppose that $a_0 \ne 0$. The set of sequences satisfying 3.1 forms a vector space $S(f)$ over K of dimension d. We let T be the *shift operator* $(x_0, x_1, \dots) \mapsto (x_1, x_2, \dots)$ acting on $S(f)$. Clearly $f(T) = 0$. Let $\boldsymbol{s}$ denote the *impulse response sequence* with $s_0 = \dots = s_{d-2} = 0$, $s_{d-1} = 1$. Then $\boldsymbol{s}$, $T\boldsymbol{s}$, ..., $T^{d-1}\boldsymbol{s}$ forms an obvious basis for $S(f)$ and with respect to this basis, T has matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a_{d-2} \\ 0 & 0 & 0 & \cdots & 1 & a_{d-1} \end{pmatrix}$$

which is a companion matrix for f. We see that T has f as both characteristic and minimal polynomial. Since $a_0 \ne 0$, T is invertible.

We describe the sequence as *unramified* if the auxiliary polynomial f has no repeated roots and *irreducible* if the auxiliary polynomial is irreducible.

If the sequence x_n is unramified then, as is well-known, the general term may be expressed as

$$x_n = A_1\alpha_1^n + \dots + A_d\alpha_d^n$$

where the α_i are the d distinct roots of $f(t)$ in some suitable algebraic extension $\bar{K}$ of K. Over $\mathbf{Q}$ we might take the α_i to be algebraic numbers lying in the complex field $\mathbf{C}$: over $\mathbf{Z}/p$, with p prime, we might take the α_i to lie in some finite extension $\mathrm{GF}\,(p^r)$ of the finite field $\mathrm{GF}\,(p)$.

Suppose now that the sequence x_n is ramified, and the auxiliary polynomials factorises over K as

$$f(t) = \prod g_j(t)^{e_j}$$

into irreducible factors g_j; if the characteristic p of the field K is not zero, suppose further that all the e_j are less than p. It is again well-known that in this case the general term of the sequence may be expressed as

$$x_n = \sum A_j(n)\alpha_{ij}^n$$

where the α_{ij} are the roots of the g_j and the A_j are polynomials of degree at most $e_j - 1$. We see that this does not apply if $e_j \geq p > 0$ since the polynomials n and n^p take the same values in K.

We may obtain a general formula in positive characteristic by defining a *B-polynomial* $B(n)$ of degree d over a field K to be a linear combination

$$B(n) = \sum_{r=0}^{d} b_i \binom{n}{r}$$

of binomial coefficients with coefficients $b_i \in K$.

Lemma 3. *The general term of a linear recurrent sequence defined over K is*

$$x_n = \sum B_j(n)\alpha_{ij}^n$$

where the B_j are B-polynomials defined over K with the degree of B_j less than e_j.

Proof. Let T denote the shift operator. The action of T on a sequence of binomial coefficients is given by $T\left(\binom{n}{r}\right) = \left(\binom{n}{r-1}\right)$ so $(T - \alpha_{ij})^{e_j}$ annihilates $B_j(n)\alpha_{ij}^n$. Hence all such sequences lie in the solution space $S(f)$, and we need only show that they are linearly independent. But applying successive powers of $T - \alpha_{ij}$ extracts the coefficients of the binomials one at a time, and so any zero linear combination must be identically zero. ■

The only eigenvector with eigenvalue α_{ij} is the sequence $\left(\alpha_{ij}^n\right)$. Hence the shift operator T will have a Jordan normal form with one Jordan block

$$J_{ij} = \begin{pmatrix} \alpha_{ij} & 1 & 0 & \cdots & 0 & 0 \\ 0 & \alpha_{ij} & 1 & \cdots & 0 & 0 \\ 0 & 0 & \alpha_{ij} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_{ij} & 1 \\ 0 & 0 & 0 & \cdots & 0 & \alpha_{ij} \end{pmatrix}$$

of size e_j corresponding to the eigenvalue α_{ij}. (We again observe here that the minimal and characteristic polynomials of T are equal to f.) Applying successive powers of T to the impulse response sequence, we again obtain the B-polynomial expansion of the Lemma.

We define the *minimal polynomial* of the sequence $\boldsymbol{x}$ to be the polynomial g of least degree over K such that $g(T)\boldsymbol{x} = \mathbf{o}$. The minimal polynomial of the impulse sequence is f and the minimal polynomial of any sequence in $S(f)$ is a factor of f.

Proposition 4. *The minimal polynomial of $\boldsymbol{u} = (u_n)$ is f divided by the highest common factor of $f(x)$ and $U(x)$ where $U(x) = \sum_{i=0}^{d-1} u_{d-1-i}x^i$.*

Proof. We see that $\boldsymbol{u} = U(T)\boldsymbol{s}$ where $\boldsymbol{s}$ is the impulse sequence. Let $h(x) = \gcd(f(x), U(x))$ and let $g(x)$ be the minimal polynomial of $\boldsymbol{u}$. From the remarks above, g divides f. We need to show that $f/h = g$.

We have $g(T)\boldsymbol{u} = \mathbf{o}$ and so $g(T)U(T)\boldsymbol{s} = \mathbf{o}$. Hence $f(x)$ divides $g(x)U(x)$ and so f/g divides U. So f/g divides both f and U and hence f/g divides h, so that f/h divides g.

We have $(f/h)(T)\boldsymbol{u} = (f/h)(T)U(T)\boldsymbol{s} = (U/h)(T)f(T)\boldsymbol{s} = \mathbf{o}$. Hence g divides f/h. The result follows. ■

We can use this result to construct a sequence in $S(f)$ having any given factor of f as its minimal polynomial.

We refer to Lidl and Nierreiter [6], Selmer [7] and van der Poorten [8] for further discussion of recurrent sequences and recurrence relations.

4 Recurrent sequences over a finite field

Suppose that the field K is a finite field $\mathrm{GF}\left(p^f\right)$ and that the auxiliary roots α_i lie in some finite extension $\mathrm{GF}\left(p^r\right)$ of $\mathrm{GF}\left(p^f\right)$ (so that $f \mid r$). There are only finitely many d-tuples over K, and so a sequence in $S(f)$ must repeat from some point onward. The recurrence relation is invertible since $a_0 \neq 0$, and so every sequence in $S(f)$ is purely periodic.

Proposition 5. *The maximum period of a recurrent sequence over K is equal to the order of the operator T, and this maximum is attained by the impulse response sequence.*

Proof. Suppose that $T^M = I$. Then for any sequence (x_n) we have $x_n = T^M x_n = x_{n+M}$ and so the sequence is periodic with period at most M.

Now consider the impulse response sequence $\boldsymbol{s}$. Suppose that this sequence is periodic with period N, so that $s_n = s_{n+N}$ for all n, that is, $\boldsymbol{s} = T^N\boldsymbol{s}$. Now $\boldsymbol{s}, T\boldsymbol{s}, \ldots, T^{d-1}\boldsymbol{s}$ form a generating set for the set of recurrent sequences with the same auxiliary polynomial, and since $T^r\boldsymbol{s} = T^{N+r}\boldsymbol{s}$

for every r, $0 \le r \le d-1$, we see that every linear combination of the $T^r \boldsymbol{s}$, and so every recurrent sequence with the same auxiliary polynomial, is fixed by T^N. Hence the operator T has order N. ■

In particular, the order of T will be the least common multiple of the multiplicative orders of the Jordan blocks in a Jordan matrix for T.

Proposition 6. *The order of a Jordan block over* $\mathrm{GF}\left(p^f\right)$ *is equal to the multiplicative order of the corresponding root, multiplied by the smallest power of* p *which is greater than or equal to the size of the block.*

Proof. Let J be a Jordan block of size e with root α. If $e = 1$ the block is just the 1 by 1 matrix (α) and clearly has the same order as α.

If $e > 1$ then the (i,i) entry of J^M is α^M and the (i,j) entry, for $i < j$, is $\binom{M}{j-i}$. If J^M is the identity, then we must have M a multiple of the order of α and all the binomial coefficients $\binom{M}{j-i} \equiv 0 \bmod p$. The range of values $j-i$ is from 1 to $e-1$ and by Lemma 2, $\binom{M}{l}$ is divisible by p for all $l \le e-1$ iff M is divisible by p^t where p^t is the least power of p which is greater than $e-1$. The result follows. ■

We immediately deduce the following result.

Theorem 7. *The maximum period of a recurrent sequence with auxiliary polynomial* f *over a finite field of characteristic* p *is given by the least common multiple of the multiplicative orders of the roots of* f *times the least power of* p *greater than or equal to all the multiplicities of the roots of* f.

We can now describe the possible periods of the sequences in $S(f)$. Let μ denote the Möbius function.

Proposition 8.

1. *The sequences with period dividing* R *form a subspace of* $S(f)$ *of dimension equal to the degree of* $\gcd(f(x), x^R - 1)$.

2. *The number of sequences with exact period* R *is*

$$\sum_{d|R} \mu(R/d) q^{\deg \gcd(f(x), x^d - 1)}$$

Proof. A sequence $\boldsymbol{u}$ has period dividing R if and only if $x^R - 1$ annihilates $\boldsymbol{u}$, that is, iff the minimal polynomial g of $\boldsymbol{u}$ divides $x^R - 1$. But we also have g divides f and so the minimal polynomial of $\boldsymbol{u}$ must divide $h = \gcd(f(x), x^R - 1)$. The dimension of the space of sequences annihilated by f is just the dimension of $S(h)$, that is, equal to the degree of h.

The second part follows by applying Möbius inversion. ■

This result includes Theorem 4 of Zierler [9].

We observe as a corollary that if f is irreducible, then every sequence (other than the zero sequence) has the same period as the impulse sequence.

5 Recurrent sequences to prime power modulus

We are interested in recurrent sequences defined over the integers and then reduced modulo some given power of p, say p^n. We refer to Reeds and Sloane [10] for further background and related material in this case.

We regard the sequence as being defined over the p-adic field $\mathbf{Q}_p$. Let α be a root of the auxiliary polynomial $f(t)$ lying in some finite extension K of $\mathbf{Q}_p$.

If the auxiliary root α is not a p-adic unit, then α^{ne} will be divisible by p^n and so any recurrent sequence taken modulo p^n will be ultimately periodic with a non-periodic initial part of length at most ne. We therefore concentrate on the case when α is a p-adic unit.

As before, we have to compute the order of a Jordan block corresponding to α. This order will be the least common multiple of the order of α modulo p^n and of the power of p required to annihilate the off-diagonal elements. Since the group of units modulo p^n is abelian, the maximum order of the elements is equal to the exponent.

Let K have residue field degree f and ramification index e over $\mathbf{Q}_p$; let $\mathcal{O}$ be the ring of integers of K with maximal ideal $\mathcal{M}$ generated by a uniformising element π. Then $\mathcal{O}/\mathcal{M} = \mathrm{GF}\left(p^f\right)$ and $(p) = \mathcal{M}^e$. Put $q = p^f$. We normalise the order valuation so that $\nu(p) = 1$: this implies that $\nu(\pi) = \dfrac{1}{e}$. This is equivalent to normalising the absolute value so that $|p| = p^{-1}$, $|\pi| = p^{-\frac{1}{e}}$.

Unfortunately, it is not always possible to predict the exponent of the group of units of $\mathcal{O}/(p^n)$ simply from knowledge of the parameters e and f as the following example shows. Let $K = \mathbf{Q}_3(\pi)$ where $(\pi)^6 = (3)$, be a 3-adic field with $e = 6$ and $f = 1$. We ask for the maximal power of 3 in the order of an element modulo 3^2. Now

$$(1 + \pi x)^3 = 1 + 3\pi x + 3\pi^2 x^2 + \pi^3 x^3 \equiv 1 + \pi^3 x^3 \not\equiv 1 \bmod 3$$

and so for any x prime to π the element $1+\pi x$ does not have order 3 modulo 3. Further,

$$\begin{aligned}(1+x\pi)^9 &= 1+3^2\pi x+4.3^2\pi^2x^2+28.3\pi^3x^3+\\ &\qquad 14.3^2\pi^4x^4+14.3^2\pi^5x^5+28.3\pi^6x^6+\\ &\qquad 4.3^2\pi^7x^7+3^2\pi^8x^8+\pi^9x^9\\ &\equiv 1 \bmod 3\end{aligned}$$

and so for any x prime to π the element $1+\pi x$ has order 9 modulo 3. Now consider the order of $1+\pi x$ modulo 3^2. This order must be at least 9. But

$$(1+\pi x)^9 \equiv 1+28.3\pi^3x^3+\pi^9x^9 \bmod 9$$

and so $1+\pi x$ has order 9 modulo 3^2 iff $\pi^6/3 \equiv -1 \bmod 3$ and order 27 otherwise. We find that both of these cases can occur: for example, $\pi^6/3 \equiv -1 \bmod 3$ if π is $\sqrt[6]{-3}$ but not if π is $\sqrt[6]{3}$. Hence we see that in this case the maximal power of 3 which can occur as an order of an element modulo 3^2 cannot be deduced simply from knowledge of the parameters of e and f of the field K.

We define the ramification index e to be *special* if $e=p^t(p-1)$ for some integer $t\geq 0$, and otherwise *ordinary* — these terms are not standard. If e is ordinary, define t and δ by

$$p^{t-1}(p-1)<e<p^t(p-1)$$

and

$$\delta=\begin{cases}0, & \text{if } p^t<e<p^t(p-1);\\ 1, & \text{if } p^t(p-1)<e\leq p^t.\end{cases}$$

Equivalently, we have $\delta=\left[p^t/e\right]$.

Proposition 9. *Suppose that the ramification index of K is ordinary. The exponent of $\mathcal{O}/(p^n)^*$, for $n>1$, is precisely $p^{n+t-\delta}(q-1)$.*

Proof. An element z of maximal order modulo p^n is clearly congruent modulo π to a generator g of the cyclic group $\mathcal{O}/\mathcal{M}^*$ of order $q-1$. Hence it is sufficient to compute the p-power part of the order modulo p^n.

Consider $y=g/z=1+\pi x$. We consider x as being at our disposal, and compute the largest power of p, say p^r, required to ensure that $y^{p^r}\equiv 1 \bmod p^n$. We may assume that x is prime to π otherwise z would not reduce to an element of maximal order modulo π.

Consider the term in x^r in the binomial expansion of $(1+\pi x)^{p^a}-1$. By Lemma 1(4), the power of p in $\binom{p^a}{r}$ is $a-\nu(r)$, so if $r=sp^c$ with s

prime to p, we have

$$\nu\left(\binom{p^a}{sp^c}(\pi x)^{sp^c}\right) = a - c + sp^c\nu(\pi x) >$$
$$\nu\left(\binom{p^a}{p^c}(\pi x)^{p^c}\right) = a - c + p^c\nu(\pi x)$$

and therefore the minimum order occurs at a term in x^r with r a power of p.

The difference between the orders of terms with successive powers of p as index is

$$\nu\left(\binom{p^a}{p^{c+1}}(\pi x)^{p^{c+1}}\right) - \nu\left(\binom{p^a}{p^c}(\pi x)^{p^c}\right) = p^c(p-1)\nu(\pi) - 1$$

and this is never zero, since e is ordinary. Hence the term where this difference changes sign is the unique term of minimal p-adic order, and this term is that in x^{p^t} where t is the parameter defined above. Since the term of minimal order s is unique, the p-adic order of the whole sum is equal to this minimal order $s = r - t + p^t/e$. Hence we see that the power of p in $(1+\pi x)^{p^r} - 1$ is precisely $r - t + \delta$, and the result follows. ∎

If the ramification index is special, the proof of the Proposition breaks down because there are two terms of equal p-adic value in the sum and there may be cancellation between them. (This is the case in the 3-adic example given above.) We can however obtain a result in the case $f > 1$. If e is special, define t by $e = p^t(p-1)$ and ϕ to be 0 if $p > 2$ and 1 if $p = 2$.

Proposition 10. *Suppose that the ramification index of K is special and that $f > 1$. The exponent of $\mathcal{O}/(p^n)^*$ is precisely $p^{n+t-\phi}(q-1)$.*

Proof. We proceed as in the proof of the previous Proposition, except that now the minimal p-adic order among the terms, which is $s = r - t + p^t/e$, is attained by the two terms in p^t and p^{t+1}, and by no others. The sum of these terms is

$$\pi^{p^t}x^{p^t}p^{r-t}\left(\left[p^{t-r}\binom{p^r}{p^t}\right] - \left[p^{t+1-r}\binom{p^r}{p^{t+1}}\right]\left[p^{-1}\pi^{p^t(p-1)}\right]x^{p^t(p-1)}\right)$$

and each of the terms in square brackets is a p-adic unit. But there are at least two distinct values of $x^{p^t(p-1)}$ modulo π, since $f > 1$, $q \neq p$ and so x^{p-1} is not always $\equiv 1 \bmod \pi$. Hence there is a value of x for which the term in parentheses is not divisible by π, and so the p-adic order of $(1+\pi x)^{p^r} - 1$ is still s. The proof now proceeds as before. ∎

In every case we can obtain a result for n sufficiently large. Let $R = 3$ if $p = 2$ and $R = 2$ otherwise, and let p^L be the exact power of p in the exponent of the multiplicative group $\mathcal{O}/(p^R)^*$. These parameters will in general depend on K. The results above may be summarised as saying that $L = t - \delta$ if the ramification index is not special, and $L = t - \phi$ if the ramification index is special and $f > 1$. We show that the behaviour of the exponent depends only on the exponent of the multiplicative group modulo p^R.

Proposition 11.

1. *The exponent of $\mathcal{O}/(p^n)^*$ for $n \geq R$ is $p^{n-R+L}(q-1)$.*
2. *An element g of $\mathcal{O}$ of maximal order modulo p^R is also an element of maximal order modulo p^n for any $n \geq R$.*

Proof. Consider an element g of maximal p-power order modulo p^n. We prove the result by induction on n. For $n = R$ the result is true by definition of R and L. Now suppose that $n > R$, and that g is an element of maximal order p^{n-R+L} modulo p^n. Then we have

$$g^{p^{n-R+L-1}} \not\equiv 1 \bmod p^n$$

but we do have

$$g^{p^{n-R+L-1}} \equiv 1 \bmod p^{n-1}.$$

Hence

$$g^{p^{n-R+L-1}} = 1 + p^{n-1}x$$

with x not divisible by p. So

$$g^{p^{n-R+L}} = (1 + p^{n-1}x)^p = 1 + p^n x + \mathrm{O}(p^{n+1}) \not\equiv 1 \bmod p^{n+1},$$

since p^{n-1} and $2n - 1$ are both $\geq n + 1$ if $n \geq R$. Further, for any h we have

$$h^{p^{n-R+L}} = 1 + p^n y$$

and so

$$h^{p^{n-R+L+1}} \equiv 1 \bmod p^{n+1}$$

from which we conclude that g is also an element of exact order $p^{n+1-R+L}$ modulo p^{n+1} and that this is the maximal order. The results follow by induction. ■

We can deduce as a corollary the well-known results that $\mathbf{Z}/(p^n)$ has a primitive root for all n and odd p, and that 5 is an element of maximal order 2^{n-2} in $\mathbf{Z}/(2^n)$, $n \geq 3$: see, for example, Baker [11] chapter 3.6.

The parameter $L-R$ which enters into the previous Proposition can be now computed directly by consideration of the p-adic logarithm function.

Define the p-adic logarithm and exponential by the usual formulae

$$\begin{aligned} \log(1-x) &= \sum_{r\geq 1} \frac{x^r}{r} \\ \exp(x) &= \sum_{r\geq 0} \frac{x^r}{r!}. \end{aligned}$$

We see that the series for log converges for $\nu(x) > 0$ and the series for exp converges for $\nu(x) > E = \dfrac{1}{p-1}$. Let $D = \{x \mid \nu(x) > E\}$ be the domain of convergence of exp. The following result is standard.

Proposition 12.

1. *Where defined, we have* $\log(xy) = \log(x) + \log(y)$ *and* $\exp(x+y) = \exp(x)\exp(y)$.
2. *The maps* log *and* exp *are mutually inverse isometries between* $1+D$ *and* D.
3. *In particular, if* $x \in D$ *then* $|\log(1-x)| = |x|$.

Proof. For the first two parts see, for example, Cassels [12] chapter 12.2 or Schikhoff [13] section 44. The last part of course follows from (2) but we can deduce it from Lemma 1.

We claim that if $x \in D$ then the minimum of the orders $n(r) = \nu\left(\dfrac{x^r}{r}\right)$ for $r \geq 1$ is attained just at $r=1$. Since $\nu(x) > 0$, we have

$$n(ap^b) = \nu\left(\frac{x^{ap^b}}{ap^b}\right) = ap^b\nu(x) - b > n(p^b) = \nu\left(\frac{x^{p^b}}{p^b}\right) = p^b\nu(x) - b$$

if a is prime to p and $a > 1$; hence the minimum is attained at a power of p. But $n(p^{b+1}) - n(p^b) = p^b(p-1)\nu(x) - 1 \geq p^b - 1 > 0$ if $b > 0$. Hence the minimum is unique and attained at $r = 1$. The ultrametric triangle inequality gives result (3). ∎

Proposition 13. *The parameter $L-R$ is the greatest integer less than or equal to the minimum value of $\nu(\log(1-\pi x))$ as x runs over $\mathbf{Z}_p$.*

Proof. Write

$$(1-\pi x)^{p^r} = 1 + \pi^{f(x,r)} X(x,r)$$

where X is prime to π. By Proposition 12, we have

$$\nu\left(\log(1+\pi^{f(x,r)}X(x,r))\right) = \frac{f(x,r)}{e}$$

when $f(x,r)/e > 1/(p-1)$ so that $1-\pi^{f(x,r)}X(x,r)$ is in the domain D where log is an isometry. Now

$$\log\left((1-\pi x)^{p^r}\right) = p^r \log(1-\pi x)$$

and, taking p-adic orders, for r sufficiently large we have

$$r + \nu\left(\log(1-\pi x)\right) = \frac{f(x,r)}{e}.$$

Now the p-power in the order of $(1-\pi x)$ modulo p^n will be the minimum value of r for which $(1-\pi x)^{p^r} \equiv 1 \bmod p^n$, that is, for which $f(x,r)/e \geq n$. Call this minimum $g(x,n)$: we have

$$g(x,n) = \lceil n - \nu\left(\log(1-\pi x)\right)\rceil .$$

Further, the maximal p-power order modulo p^n, say $P(n)$, will be the largest such value of $g(x,n)$ as x ranges over $\mathbf{Z}_p$. But we know that $P(n) = n-(L-R)$ for n sufficiently large, and so we have

$$n-(L-R) = \max_{x\in\mathbf{Z}_p} \lceil n - \nu\left(\log(1-\pi x)\right)\rceil$$

and hence

$$L-R = \min_{x\in\mathbf{Z}_p} \left[\nu\left(\log(1-\pi x)\right)\right] . \blacksquare$$

Proposition 14. *The order modulo p^n of a Jordan block of size e for the auxiliary root α is the least common multiple of the order of α modulo p^n and p^{n+s-1}, where p^s is the least power of p with $p^s \geq e$.*

Proof. Let J be a Jordan block of size e with root α. If $e=1$ the block is just the 1 by 1 matrix (α) and clearly has the same order as α.

If $e>1$ then the (i,i) entry of J^M is α^M and the (i,j) entry, for $i<j$, is $\binom{M}{j-i}$. If J^M is the identity, then we must have M a multiple of the order of α and all the binomial coefficients $\binom{M}{j-i} \equiv 0 \bmod p^n$. The range of values $j-i$ is from 1 to $e-1$ and by Lemma 2, $\binom{M}{l}$ is divisible by p^n for all $l \leq e-1$ iff M is divisible by p^{n+s-1} where p^s is the least power of p which is greater than $e-1$. The result follows. $\blacksquare$

The maximum period of a recurrent sequence modulo a prime power is obtained by combining Propositions 14 and 11. In particular, Proposition 11 shows that the maximum period is determined by the auxiliary polynomial modulo p^2 if p is odd, and modulo 2^3 if $p=2$.

Bibliography

1. Kummer, E.E. (1852). Über die Erganzungssätze zu den allgemeinen Reciprociätsgesetzen. *J. reine angew. Math.*, **44**, 93–146. (Collected Works, I, 485–538)

2. Singmaster, D. (1974). Notes on binomial coefficients *Jour. London Math. Soc. (2)*, **8**, 545–560.

3. Goetgheluck, P. (1987). Computing binomial coefficients. *Amer. Math. Monthly*, **94**, 360–365.

4. Dickson, L.E. (1971). *History of the theory of numbers.* Chelsea, New York. (First published: Carnegie Institute, Washington, 1919–23)

5. Fine, N.J. (1947). Binomial coefficients modulo a prime. *Amer. Math. Monthly*, **54**, 589–592.

6. Lidl, R. and Niederreiter, H. (1984). *Finite fields.* Encyclopaedia of mathematics and its applications **20**. Cambridge University Press, Cambridge. (First published: Addison-Wesley, Reading, Mass. 1983)

7. Selmer, E.S. (1966). *Linear recurrence relations over finite fields.* Bergen University Department of Mathematics, Bergen.

8. van der Poorten, A. (1989). Some facts that should be better known, especially about rational functions. In *Number theory and its applications*, ed. Mollin, R.A., Kluwer Academic.

9. Zierler, N. (1959). Linear recurring sequences. *J. Soc. Indust. App. Math.*, **7**, 31–48.

10. Reeds, J.A. and Sloane, N.J.A. (1985). Shift-register synthesis (modulo m) *SIAM J. Comput.*, **14**, 505–513.

11. Baker, A. (1984). *A concise introduction to the theory of numbers.* Cambridge University Press, Cambridge.

12. Cassels, J.W.S. (1986). *Local fields.* Cambridge University Press, Cambridge.

13. Schikhoff, W.H. (1984). *Ultrametric calculus.* Cambridge University Press, Cambridge.