Journal of Integer Sequences, Vol. 8 (2005),
Article 05.1.2

Newton, Fermat, and Exactly Realizable Sequences

Bau-Sen Du
Institute of Mathematics
Academia Sinica
Taipei 115
TAIWAN
mabsdu@sinica.edu.tw

Sen-Shan Huang and Ming-Chia Li
Department of Mathematics
National Changhua University of Education
Changhua 500
TAIWAN
shunag@math.ncue.edu.tw
mcli@math.ncue.edu.tw

Abstract

In this note, we study intimate relations among the Newton, Fermat and exactly realizable sequences, which are derived from Newton's identities, Fermat's congruence identities, and numbers of periodic points for dynamical systems, respectively.

1 Introduction

Consider a set S of all sequences with complex numbers, let I be the subset of S consisting of sequences containing only integers, and let I_+ be the subset of I containing only sequences with nonnegative integers. We shall define two operators

$$N : S \to S \text{ and } F : S \to S,$$

called Newton and Fermat operators, and we call each element of $N(S)$ a Newton sequence and each element of $F(S)$ a Fermat sequence; this terminology is motivated by Newton identities and by Fermat's Little Theorem, details of which are given below. The key questions investigated in this note are as follows: What is $N(I_+)$? What are $N(I)$ and $F(I)$? What are the relations between various Newton and Fermat sequences?

In Theorem 2, we observe that $N(I) = F(I)$; this was earlier obtained by us in [4] but here another proof is provided due to D. Zagier.

Further, we investigate sequences attached to some maps and their period-n points. Let M denote a set of some maps which will be specialized later. We shall construct a natural operator $E : M \to I_+$ and call each element of $E(M)$ an exactly realizable sequence.

In Theorem 3, we show that $E(M) = F(I_+) \subset N(I)$ and for any $\{a_n\} \in E(M)$, we construct a formula for $\{c_n\} \in I$ such that $N(\{c_n\}) = \{a_n\}$. In Theorem 4, we show that $N(I_+) \subset E(M)$ and $N(I)$ is equal to the set of term-by-term differences of two elements in $E(M)$. We also investigate when a Newton sequence is an exactly realizable sequence in a special case.

2 Newton's Identities

In this note, we work entirely with sequences in $\mathbb{C}$, but one could work with more general fields. In particular, Newton's identities below are valid in any field.

Newton's identities were first stated by Newton in the 17th century. Since then there have appeared many proofs, including recent articles [8] and [9]. For reader's convenience, we give a simple proof using formal power series based on [1, p. 212]; also refer to [3].

Theorem 1 (Newton's identities). *Let $x^k - \sum_{j=0}^{k-1} c_{k-j}x^j$ be a polynomial in $\mathbb{C}[x]$ with zeros λ_j for $1 \le j \le k$ and let $a_n = \sum_{j=1}^{k} \lambda_j^n$ for $n \ge 1$ and $c_n = 0$ for $n > k$. Then $a_n = \sum_{j=1}^{n-1} a_{n-j}c_j + nc_n$ for all $n \ge 1$.*

Proof. By writing $x^k - \sum_{j=0}^{k-1} c_{k-j}x^j = \prod_{j=1}^{k}(x - \lambda_j)$ and replacing x by $1/x$, we obtain $1 - \sum_{j=1}^{k} c_j x^j = \prod_{j=1}^{k}(1 - \lambda_j x)$. Then the formal power series

$$\begin{aligned}
\sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty}\left(\sum_{j=1}^{k}\lambda_j^n\right)x^n &= \sum_{j=1}^{k}\left(\sum_{n=1}^{\infty}(\lambda_j x)^n\right) = \sum_{j=1}^{k}\frac{\lambda_j x}{1-\lambda_j x} \\
&= -x\frac{\frac{d}{dx}\left(\prod_{j=1}^{k}(1-\lambda_j x)\right)}{\prod_{j=1}^{k}(1-\lambda_j x)} = -x\frac{\frac{d}{dx}\left(1-\sum_{j=1}^{k} c_j x^j\right)}{1-\sum_{j=1}^{k} c_j x^j} \\
&= \frac{\sum_{j=1}^{k} j c_j x^j}{1-\sum_{j=1}^{k} c_j x^j}
\end{aligned}$$

and hence $\sum_{n=1}^{\infty} a_n x^n = (\sum_{n=1}^{\infty} a_n x^n)(\sum_{j=1}^{k} c_j x^j) + \sum_{j=1}^{k} j c_j x^j$. By comparing coefficients and the assumption $c_j = 0$ for $j > k$, we have $a_n = \sum_{j=1}^{n-1} a_{n-j}c_j + nc_n$ for all $n \ge 1$. $\square$

Based on Newton's identities, it is natural to give the following definition: for a sequence $\{c_n\}$ in $\mathbb{C}$, the *Newton sequence* generated by $\{c_n\}$ is defined to be $\{a_n\}$ by $a_n = \sum_{j=1}^{n-1} a_{n-j}c_j + nc_n$ inductively for $n \geq 1$. In this case, we define the *Newton operator* N by $N(\{c_n\}) = \{a_n\}$.

Fermat's little theorem states that given an integer a, we have that $p|a^p - a$ for all primes p. In order to state its generalization, we use the following terminology: for a sequence $\{b_n\}$ in $\mathbb{C}$, the *Fermat sequence* generated by $\{b_n\}$ is defined to be $\{a_n\}$ by $a_n = \sum_{m|n} mb_m$ for $n \geq 1$; in this case, we define the *Fermat operator* F by $F(\{b_n\}) = \{a_n\}$. If $\{a^n\}$ is an integral Fermat sequence generated by $\{b_n\}$ and if p is any prime, then $pb_p = a^p - a$ and hence $b_p \in \mathbb{Z}$; this observation inspires the name *Fermat Sequence*. By the Möbius inversion formula (refer to [10]), we have that if $\{a_n\}$ is the Fermat sequence generated by $\{b_n\}$, then $nb_n = \sum_{m|n} \mu(m)a_{n/m}$ and if, in addition, $\{b_n\}$ is an integral sequence, then $n|\sum_{m|n} \mu(m)a_{n/m}$, where μ is the Möbius function, i.e., $\mu(1) = 1$, $\mu(m) = (-1)^k$ if m is a product of k distinct prime numbers, and $\mu(m) = 0$ otherwise. (In [4], we called $\{a_n\}$ a *generalized Fermat sequence* if a_n is an integer and $n|\sum_{m|n} \mu(m)a_{n/m}$ for every $n \geq 1$; now it is the Fermat sequence generated by an integral sequence.)

Fermat sequences of the form $\{a^n\}$ are related to both free Lie algebras and the number of irreducible polynomials over a given finite field. Indeed, let X be a finite set of cardinality a and let L_X be a free Lie algebra on X over some field $\mathbb{F}$. For any given $n \in \mathbb{N}$ let L_X^n be its nth homogeneous part and let $\ell_a(n)$ be the rank of L_X^n. Then

$$a^n = \sum_{m|n} m\ell_a(m) \text{ for all } n \in \mathbb{N}$$

which shows that $\{a^n\}$ is the Fermat sequence generated by $\{\ell_a(n)\}$ (See [12] and [7, Section 4 of Chapter 4]). Further, let $\mathbb{F}_q$ be a finite field with q elements and let $N_q(n)$ be the number of monic irreducible polynomials in $\mathbb{F}_q[X]$ of degree n. Then

$$q^n = \sum_{m|n} mN_q(m).$$

Hence $\{q^n\}$ is the Fermat sequence generated by $\{N_q(n)\}$.

In [4], we show that a sequence is a Newton sequence generated by integers if and only if it is a Fermat sequence generated by integers, by using symbolic dynamics. Here we give another proof using formal power series pointed out by Zagier [13] to us; also refer to [2].

Theorem 2. *Let $\{a_n\}, \{b_n\}$ and $\{c_n\}$ be sequences in $\mathbb{C}$. Then*

1. *$\{a_n\}$ is the Newton sequence generated by $\{c_n\}$ if and only if*

$$\exp\left(-\sum_{n=1}^{\infty} a_n \frac{x^n}{n}\right) = 1 - \sum_{n=1}^{\infty} c_n x^n \quad \textit{as formal power series;}$$

2. *$\{a_n\}$ is the Fermat sequence generated by $\{b_n\}$ if and only if*

$$\exp\left(-\sum_{n=1}^{\infty} a_n \frac{x^n}{n}\right) = \prod_{n=1}^{\infty} (1 - x^n)^{b_n} \quad \textit{as formal power series;}$$

3. *$\{a_n\}$ is the Newton sequence generated by an integral sequence if and only if $\{a_n\}$ is the Fermat sequence generated by an integral sequence. That is, $N(I) = F(I)$, where I is the set of all integral sequences.*

Proof. For convenience, we define formal power series $A(x) = \sum_{n=1}^{\infty} a_n x^n$, $C(x) = \sum_{n=1}^{\infty} c_n x^n$, $F(x) = \exp\left(-\sum_{n=1}^{\infty} a_n x^n/n\right)$, and $H(x) = \prod_{m=1}^{\infty}(1-x^m)^{b_m}$.

We prove item 1 as follows. By comparing coefficients and using the trivial fact $A(x) = -x\frac{d}{dx}\log F(x)$, we have that $a_n = \sum_{j=1}^{n-1} a_{n-j}c_j + nc_n$ for all $n \geq 1 \Leftrightarrow A(x) = C(x)A(x) + xC'(x) \Leftrightarrow A(x) = x\frac{C'(x)}{1-C(x)} = -x\frac{d}{dx}\log(1-C(x)) \Leftrightarrow F(x) = 1 - C(x)$. (Observe that $1 = F(0) = 1 - C(0)$).

We prove item 2 as follows. By rearranging terms of x^n and using the fact that $H(x) = \exp\left(-\sum_{m=1}^{\infty} b_m \sum_{r=1}^{\infty} x^{rm}/r\right)$, we have that $a_n = \sum_{m|n} mb_m$ for all $n \geq 1 \Leftrightarrow F(x) = \exp\left(-\sum_{m=1}^{\infty} b_m \sum_{r=1}^{\infty} x^{rm}/r\right) = H(x)$.

¿From the proof of items 1 and 2, $\{b_n\}$ and $\{c_n\}$ are both uniquely determined by $\{a_n\}$ such that $\{a_n\}$ is the Newton sequence generated by $\{c_n\}$ and also the Fermat sequence generated by $\{b_n\}$. Then $1 - \sum_{n=1}^{\infty} c_n x^n = F(x) = \prod_{n=1}^{\infty}(1-x^n)^{b_n}$. Therefore, item 3 follows since $c_n \in \mathbb{Z}$ for all $n \geq 1 \Leftrightarrow F(x) \in 1 + x\mathbb{Z}[x] \Leftrightarrow b_n \in \mathbb{Z}$ for all $n \geq 1$. □

3 Connections with Dynamical Systems

In the following, we make a connection between the above number theoretical result with dynamical systems. Let f be a map from a set S into itself. For $n \geq 1$, let f^n denote the composition of f with itself n times. A point $x \in S$ is called a *period-n point* for f if $f^n(x) = x$ and $f^j(x) \neq x$ for $1 \leq j \leq n-1$. Let $\mathrm{Per}_n(f)$ denote the set of all period-n points for f and let $\#\mathrm{Per}_n(f)$ denote the cardinal number of $\mathrm{Per}_n(f)$ if $\mathrm{Per}_n(f)$ is finite. Let a be any period-n point for f. Then $a, f(a), \ldots, f^{n-1}(a)$ are distinct period-n points and hence $n|\#\mathrm{Per}_n(f)$. Since $\#\mathrm{Per}_1(f^n) = \sum_{m|n} \#\mathrm{Per}_m(f)$, the sequence $\{\#\mathrm{Per}_1(f^n)\}$ is the Fermat sequence generated by the sequence $\{\#\mathrm{Per}_n(f)/n\}$.

Following [5], we say that a nonnegative integral sequence $\{a_n\}$ is *exactly realizable* if there is a map f from a set into itself such that $\#\mathrm{Per}_1(f^n) = a_n$ for all $n \geq 1$; in this case, we write $E(f) = \{a_n\}$. Let M be the set of maps f for which $\mathrm{Per}_n(f)$ is nonempty and finite, and let I_+ be the set of all nonnegative integral sequences. Then E is an operator from M to I_+. Exact realizability can be characterized as follows.

Theorem 3. *Let $\{a_n\}$ be a sequence in $\mathbb{C}$. Then the following three items are equivalent:*

1. *$\{a_n\}$ is exactly realizable;*

2. *there exists a nonnegative integral sequence $\{b_n\}$ such that $\{a_n\}$ is the Fermat sequence generated by $\{b_n\}$, that is, $F(\{b_n\}) = \{a_n\}$;*

3. *there exists a nonnegative integral sequence $\{d_n\}$ such that $\{a_n\}$ is the Newton sequence generated by an integral sequence $\{c_n\}$ with for all $n \geq 1$,*

$$c_n = \sum_{k_1+2k_2+\cdots+nk_n=n} (-1)^{k_1+k_2+\cdots+k_n+1} \binom{d_1}{k_1}\binom{d_2}{k_2}\cdots\binom{d_n}{k_n}$$

where $\binom{p}{q}$ *denotes a binomial coefficient; that is,* $N(\{c_n\}) = \{a_n\}$*.*

Moreover, if the above items hold then $b_n = d_n$ *for all* $n \geq 1$*.*

Proof. ($1 \Rightarrow 2$) Let f be a function such that $\#\mathrm{Per}_1(f^n) = a_n$ for all $n \geq 1$ and let $b_n = \#\mathrm{Per}_n(f)/n$ for all $n \geq 1$. Then $\{b_n\}$ is nonnegative and integral, and $a_n = \sum_{m|n} mb_m$ for all $n \geq 1$.

($1 \Leftarrow 2$) By permutation, we can define $f : \mathbb{N} \to \mathbb{N}$ by that the first b_1 integers are period-1 points, the next $2b_2$ integers are period-2 points, the next $3b_3$ are period-3 points, and so on. Then $mb_m = \#\mathrm{Per}_m(f)$ for all $m \geq 1$ and hence $a_n = \sum_{m|n} mb_m = \#\mathrm{Per}_1(f^n)$ for all $n \geq 1$. Therefore, $\{a_n\}$ is exactly realizable.

($2 \Leftrightarrow 3$) By using item 3 of Theorem 2 and letting $d_n = b_n$ for all $n \geq 1$, it remains to verify the expressions of c_n's. From items 1 and 2 of Theorem 2, we have $1 - \sum_{n=1}^{\infty} c_n x^n = \prod_{n=1}^{\infty}(1 - x^n)^{d_n}$. Equating the coefficients of x^n on both sides, we obtain the desired result.

The last statement of the theorem is a by-product from the proof of ($2 \Leftrightarrow 3$). □

Let $\{a_n\}$ be the Newton sequence generated by $\{c_n\}$. For exact realizability of $\{a_n\}$, it is not necessary that all of c_n's are nonnegative. For example, the exactly realizable sequence $\{2, 2, 2, \cdots\}$, which is derived from a map with only two period-1 points and no other periodic points, is the Newton sequence generated by $\{c_n\}$ with $c_1 = 2$, $c_2 = -1$ and $c_n = 0$ for $n \geq 3$. Nevertheless, the nonnegativeness of all c_n's is sufficient for exact realizability of $\{a_n\}$ as follows.

Theorem 4. *The following properties hold.*

1. *Every Newton sequence generated by a nonnegative integral sequence is exactly realizable, that is,* $N(I_+) \subset E(M)$*.*

2. *Every Newton sequence generated by an integral sequence is a term-by-term difference of two exactly realizable sequences, and vice versa.*

Before proceeding with the proof, we recall some basic definitions in symbolic dynamics; refer to [6, 11]. A graph G consists of a countable (resp. finite) set S of states together with a finite set E of edges. Each edge $e \in E$ has initial state $i(e)$ and terminal state $t(e)$. Let $A = [A_{IJ}]$ be a countable (resp. finite) matrix with nonnegative integer entries. The graph of A is the graph G_A with state set S and with A_{IJ} distinct edges from edge set E with initial state I and terminal state J. The *edge shift space* Σ_A is the space of sequences of edges from E specified by

$$\Sigma_A = \{e_0e_1e_2 \cdots | e_j \in E \text{ and } t(e_j) = i(e_{j+1}) \text{ for all integers } j \geq 0\}.$$

The *shift map* $\sigma_A : \Sigma_A \to \Sigma_A$ induced by A is defined to be

$$\sigma_A(e_0e_1e_2e_3\cdots) = e_1e_2e_3\cdots.$$

Now we prove Theorem 4.

Proof. First we prove item 1. Let $\{a_n\}$ be the Newton sequence generated by a nonnegative integral sequence $\{c_n\}$. Define a countable matrix $A = [A_{IJ}]$ with countable states $S = \mathbb{N}$ by A_{IJ} to be c_J if $I = 1$ and $J \geq 1$, one if $I = J + 1$ and $J \geq 1$, and zero otherwise. Let σ_A be the shift map induced by A. Then $a_n = \text{trace}(A^n) = \#\text{Per}_1(\sigma_A^n)$ for all $n \geq 1$. Therefore $\{a_n\}$ is exactly realizable.

Next we prove the forward part of item 2. Let $\{a_n\}$ be the Newton sequence generated by an integral sequence $\{c_n\}$. Setting $b_n = \frac{1}{n}\sum_{m|n}\mu(m)a_{n/m}$ for all $n \geq 1$, Theorem 2 implies that $\{a_n\}$ is a Fermat sequence generated by $\{b_n\}$ and each b_n is an integer. Let $b_n^+ = \max(b_n, 0)$ and $b_n^- = \max(-b_n, 0)$ for $n \geq 1$. Then $b_n^+ \geq 0$, $b_n^- \geq 0$ and $b_n = b_n^+ - b_n^-$ for all $n \geq 1$. Setting $a_n^+ = \sum_{m|n} mb_m^+$ and $a_n^- = \sum_{m|n} mb_m^-$, it follows from Theorem 3 that $\{a_n^+\}$ and $\{a_n^-\}$ are both exactly realizable sequences. Moreover, $a_n = \sum_{m|n} mb_m = \sum_{m|n} m(b_m^+ - b_m^-) = a_n^+ - a_n^-$ for all $n \geq 1$.

Finally we prove the backward part of item 2. By Theorem 3, we have that every exactly realizable sequence is the Fermat sequence generated by a nonnegative integral sequence. It is obvious that the term-by-term difference of two Fermat sequences is a Fermat sequence. These facts, together with item 3 of Theorem 2, imply the desired result. □

4 Formal Power Series

Combining the theorems above, we have the following result on formal power series.

Corollary 5. *Let $\{b_n\}$ and $\{c_n\}$ be two sequences in $\mathbb{C}$ such that $1 - \sum_{n=1}^{\infty} c_n x^n = \prod_{n=1}^{\infty}(1 - x^n)^{b_n}$ as formal power series. If $\{c_n\}$ is a nonnegative integral sequence then so is $\{b_n\}$.*

Proof. Let $\{a_n\}$ be the Newton sequence generated by $\{c_n\}$. By items 1 and 2 of Theorem 2, the sequence $\{a_n\}$ is the Fermat sequence generated by $\{b_n\}$. By item 1 of Theorem 4, the sequence $\{a_n\}$ is exactly realizable such that $a_n = \#\text{Per}_1(f^n)$ for some map f. Therefore, we have that $b_n = \sum_{m|n}\mu(m)a_{n/m} = \#\text{Per}_n(f)/n \geq 0$ for all $n \geq 1$. □

Finally, we give a criterion of exact realizability for the Newton sequence generated by $\{c_n\}$ with $c_n = 0$ for all $n \geq 3$.

Corollary 6. *Let $\{a_n\}$ be the Newton sequence generated by a sequence $\{c_n\}$ with $c_n = 0$ for all $n \geq 3$. Then $\{a_n\}$ is exactly realizable if and only if c_1 and c_2 are both integers with $c_1 \geq 0$ and $c_2 \geq -c_1^2/4$.*

Proof. First we prove the "if" part. If c_1 is even, we define a matrix $A = \begin{bmatrix} c_1/2 & c_1^2/4 + c_2 \\ 1 & c_1/2 \end{bmatrix}$. Then A is a nonnegative integral matrix and $a_n = \text{trace}(A^n) = \#\text{Per}_1(\sigma_A^n)$, where σ_A is the shift map induced by A (see the proof of Theorem 4 with two states). Therefore, $\{a_n\}$ is exactly realizable. Similarly, if c_1 is odd, then $c_2 \geq -c_1^2/4 + 1/4$ because c_2 is an integer, and hence $\{a_n\}$ is exactly realizable with respect to σ_A, where $A = \begin{bmatrix} (c_1+1)/2 & (c_1^2-1)/4 + c_2 \\ 1 & (c_1-1)/2 \end{bmatrix}$.

Next we prove the "only if" part. Since $\{a_n\}$ is exactly realizable, $c_1 = a_1 \geq 0$ is an integer, $c_2 = (a_2 - a_1)/2 - c_1(c_1 - 1)/2$ is an integer, and $a_n = \text{trace}(A^n) \geq 0$ for all $n \geq 1$, where $A = \begin{bmatrix} c_1/2 & c_1^2/4 + c_2 \\ 1 & c_1/2 \end{bmatrix}$. Suppose, on the contrary, that $c_2 = -c_1^2/4 - \alpha$ for some $\alpha > 0$. Let $B = \begin{bmatrix} c_1/2 & -\sqrt{\alpha} \\ \sqrt{\alpha} & c_1/2 \end{bmatrix}$. Then B has the same characteristic polynomial as A and hence $a_n = \mathrm{trace}(A^n) = \mathrm{trace}(B^n)$ for all $n \geq 1$. Let $r = \sqrt{c_1^2/4 + \alpha}$ and pick $0 < \theta \leq \pi/2$ so that $r \cos\theta = c_1/2$ and $r \sin\theta = \sqrt{\alpha}$. Then $B^n = \begin{bmatrix} r^n \cos n\theta & -r^n \sin n\theta \\ r^n \sin n\theta & r^n \cos n\theta \end{bmatrix}$ and $a_n = 2r^n \cos n\theta$ for all $n \geq 1$. This contradicts that $a_n \geq 0$ for all $n \geq 1$. Therefore, $c_2 \geq -c_1^2/4$. $\square$

Acknowledgments: We would like to thank Professor D. Zagier for his invaluable suggestions which lead to the formulation of Theorem 2 and are also grateful to the referee for helpful suggestions which have improved the presentation of this note.

References

[1] E. Berlekamp, *Algebraic Coding Theory*, MacGraw Hill Book Co., New York, 1968.

[2] L. Carlitz, Note on a paper of Dieudonne, *Proc. Amer. Math. Soc.* **9** (1958), 32–33.

[3] B.-S. Du, The linearizations of cyclic permutations have rational zeta functions, *Bull. Austral. Math. Soc.* **62** (2000), 287–295.

[4] B.-S. Du, S.-S. Huang, and M.-C. Li, Genralized Fermat, double Fermat and Newton sequences, *J. Number Theory* **98** (2003), 172–183.

[5] G. Everest, A. J. van der Poorten, Y. Puri, and T. Ward, Integer sequences and periodic points, *J. Integer Seq.* **5** (2002), Article 02.2.3, 10 pp.

[6] B. P. Kitchens, *Symbolic Dynamics: One-sided, Two-sided and Countable State Markov Shifts*, Springer-Verlag, Berlin, 1998.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[8] D. G. Mead, Newton's identities, *Amer. Math. Monthly* **99** (1992), 749–751.

[9] J. Mináč, Newton's identities once again, *Amer. Math. Monthly* **110** (2003), 232–234.

[10] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, fifth ed., Wiley, New York, 1991.

[11] C. Robinson, *Dynamical Systems: Stability, Symbolic Dynamics, and Chaos*, 2nd ed., Studies in Advanced Mathematics, CRC Press, Boca Raton, FL, 1999.

[12] J.-P. Serre, *Lie Algebra and Lie Groups*, Lectures given at Harvard University, 1964, W.A.Benjamin, Inc., New York-Amsterdam, 1965.

[13] D. Zagier, private communication by email, 2003.

2000 *Mathematics Subject Classification*: Primary 11B83; Secondary 11B50, 37B10 .
Keywords: Newton sequence, Fermat sequence, exactly realizable sequence, symbolic dynamics.

Received June 1 2004; revised version received October 20 2004. Published in *Journal of Integer Sequences*, January 12 2005.
