PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 142, Number 7, July 2014, Pages 2337–2352
S 0002-9939(2014)12168-X
Article electronically published on April 4, 2014

LINEAR RECURRENCE SEQUENCES SATISFYING CONGRUENCE CONDITIONS

GREGORY T. MINTON

(Communicated by Ken Ono)

Abstract. It is well-known that there exist integer linear recurrence sequences $\{x_n\}$ such that $x_p \equiv x_1 \pmod{p}$ for all primes p. It is less well-known, but still classical, that there exist such sequences satisfying the stronger condition $x_{p^n} \equiv x_{p^{n-1}} \pmod{p^n}$ for all primes p and $n \geq 1$, or even $m \mid \sum_{d|m} \mu(m/d)x_d$ for all $m \geq 1$. These congruence conditions generalize Fermat's little theorem, Euler's theorem, and Gauss's congruence, respectively. In this paper we classify sequences of these three types. Our classification for the first type is in terms of linear dependencies of the characteristic zeros; for the second, it involves recurrence sequences vanishing on arithmetic progressions; and for the last type we give an explicit classification in terms of traces of powers.

1. Introduction

In a recent elementary note [16] we surveyed three proofs of the following fact: the Perrin sequence $\{P_n\}$, defined by $P_1 = 0$, $P_2 = 2$, $P_3 = 3$, and $P_n = P_{n-2}+P_{n-3}$ for $n \geq 4$ (OEIS A001608 [17]), satisfies $p \mid P_p$ for all primes p. This sequence and close relatives (e.g., OEIS A050443 and A001634) have repeatedly appeared in the literature: in problems [5–7, 21]; as sources for pseudoprimality tests [1, 13]; and even in a popular comic strip [2]!

The Perrin sequence is an example of a *trace sequence*, i.e., a sequence $\{x_n\}$ of the form $x_n = \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^n)$ for an algebraic integer θ. All such sequences satisfy the congruence

$$x_p \equiv x_1 \pmod{p} \tag{1.1}$$

for all primes p. In fact, they satisfy the stronger congruence condition

$$x_{p^n} \equiv x_{p^{n-1}} \pmod{p^n} \tag{1.2}$$

for all primes p and integers $n \geq 1$, and even the still-stronger congruence condition

$$\sum_{d|m} \mu(\tfrac{m}{d})x_d \equiv 0 \pmod{m} \tag{1.3}$$

for all positive integers m, where μ is the Möbius function.

These properties have been well-studied; Zarelua gives a discussion of their history and many more references in a survey article [23]. In particular, congruence

Received by the editors August 2, 2012.
2010 *Mathematics Subject Classification.* Primary 11B50, 11R45.
The author was supported by a Fannie and John Hertz Foundation Fellowship and a National Science Foundation Graduate Research Fellowship.

(1.3) has an illustrious pedigree, having been studied in the contexts of combinatorics [20], number theory [22], and dynamical systems [4].

Following Gillespie [10], we call a sequence satisfying congruence (1.1) a *Fermat sequence*. It is so named because Fermat's little theorem is the assertion that, for any $a \in \mathbb{Z}$, $\{a^n\}$ is a Fermat sequence. Continuing in this spirit, we call a sequence satisfying congruence (1.2) an *Euler sequence*, after Euler's theorem, and we call a sequence satisfying congruence (1.3) a *Gauss sequence*, after Gauss's congruence.

We are not aware of any linear recurrence sequences other than trace sequences which have previously been identified as being Gauss, Euler, or even Fermat. In the present paper we address this by classifying all linear recurrence sequences of these three types. More precisely, we generalize the conditions to rational sequences and then answer the following question: given a characteristic polynomial $f(t)$, what is the space of Fermat (or Euler, or Gauss) linear recurrence sequences with characteristic polynomial $f(t)$?

Our classifications are explicit to varying degrees. For Fermat sequences, we translate the problem into a Galois-theoretic question of linear relations amongst the zeros of $f(t)$. For Euler sequences, we give a description in terms of sequences vanishing on arithmetic progressions. The classification for Gauss sequences, by contrast, is completely explicit: only (linear combinations of) trace sequences are Gauss. Summarizing these results colloquially,

"There are novel Fermat sequences, and some extra Euler sequences,
but there are no new Gauss sequences."

2. Statement of results

In the study of Fermat, Euler, and Gauss sequences, it is convenient to allow nonintegrality and divisibility exceptions at finitely many primes; that makes the set of all such sequences form a $\mathbb{Q}$-vector space. This remark motivates the following.

Definition 2.1. A rational linear recurrence sequence $\{x_n\}_{n=1}^{\infty}$ is a *Fermat sequence*, *Euler sequence*, or *Gauss sequence* if congruence (1.1), (1.2), or (1.3), respectively, holds in all but finitely many completions $\mathbb{Z}_p$.

Our classification will treat separately the "separable" part of a linear recurrence sequence, as defined below.

Definition-Lemma 2.2. Given a linear recurrence sequence $\{x_n\}_{n=1}^{\infty}$, we can uniquely write $x_n = y_n + nz_n + w_n$ such that $\{y_n\}$, $\{z_n\}$, and $\{w_n\}$ are linear recurrence sequences with the following properties: the characteristic polynomial of $\{y_n\}$ is separable; 0 is not a zero of the characteristic polynomial of either $\{y_n\}$ or $\{z_n\}$; and $w_n = 0$ for all sufficiently large n. We call $x_n = y_n + nz_n + w_n$ the *separable decomposition* of $\{x_n\}$.

Proof. Follows from the expansion of $\{x_n\}$ in terms of its characteristic zeros. □

In §5 we study Fermat sequences. The following are our main results.

Proposition 2.3. *Let $\{x_n\}$ be a rational linear recurrence sequence with separable decomposition $x_n = y_n + nz_n + w_n$. Then $\{x_n\}$ is a Fermat sequence iff $\{y_n\}$ is a Fermat sequence and $z_1 + w_1 = 0$.*

Theorem 2.4. *Let $f(t) \in \mathbb{Q}[t]$ be a separable polynomial with $f(0) \neq 0$. Let $\{r_i\}_{i=1}^{s}$ be the zeros of f in its splitting field K. Let $e = \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}}\{r_i\}_{i=1}^{s}$, and let*

$\epsilon \in \{0,1\}$ equal 1 iff $\mathrm{Tr}_{K/\mathbb{Q}}(r_i) \neq 0$ for some $i \in \{1,\dots,s\}$. Then the dimension of the vector space of Fermat sequences with characteristic polynomial $f(t)$ is exactly $s - e + \epsilon$.

Remark 2.5. In addition to computing the dimension, our forthcoming argument implicitly gives an algorithm for computing the space of Fermat sequences in terms of the space of vanishing $\mathbb{Q}$-linear combinations of $\{r_i\}$.

Corollary 2.6. *Let $f(t) \in \mathbb{Q}[t]$ be a polynomial of degree d, with s distinct nonzero zeros $\{r_i\}_{i=1}^s$ in its splitting field. Let e, ϵ be as in Theorem 2.4, and let $u = \max\{0, d-s-1\}$. Then the vector space of Fermat sequences with characteristic polynomial $f(t)$ has dimension exactly $(s-e+\epsilon)+u$.*

Proof. This follows from the combination of Proposition 2.3 and Theorem 2.4. □

In certain cases we can simplify the classification, for instance, as follows.

Corollary 2.7. *Let $f(t) \in \mathbb{Q}[t]$ be an irreducible polynomial. Suppose that either (i) $\deg f(t)$ is prime or (ii) the Galois group of f acts doubly-transitively on its zeros. Then, letting θ be a zero of f, the only Fermat sequences with characteristic polynomial $f(t)$ are multiples of $\{\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^n)\}$.*

When the conditions of Corollary 2.7 do not hold, we can sometimes find many more Fermat sequences. We discuss some examples of this in §5.

In §6 we move on to Euler sequences, obtaining the following results.

Proposition 2.8. *Let $\{x_n\}$ be a rational linear recurrence sequence with separable decomposition $x_n = y_n + nz_n + w_n$. Let $z_n = z'_n + nz''_n$ be the separable decomposition of $\{z_n\}$. Then $\{x_n\}$ is an Euler sequence iff $\{y_n\}$ is an Euler sequence, $\{z'_n\}$ is a Fermat sequence, $z'_1 = 0$, and $z''_1 + w_1 = 0$.*

Definition 2.9. A *trace sequence* is a sequence $\{x_n\}$ of the form

$$x_n = \sum_{i=1}^{r} a_i \,\mathrm{Tr}_{K/\mathbb{Q}}(\theta_i^n),$$

where K is an algebraic number field, $a_1,\dots,a_r \in \mathbb{Q}$, and $\theta_1,\dots,\theta_r \in K$.

Definition 2.10. A *vanishing sequence* is a rational linear recurrence sequence $\{x_n\}$ such that, for some integer $m \geq 1$, $x_n = 0$ for all n relatively prime to m.

Theorem 2.11. *Let $\{y_n\}$ be a rational linear recurrence sequence with separable characteristic polynomial. Then $\{y_n\}$ is an Euler sequence iff it is the sum of a trace sequence and a vanishing sequence.*

As with Fermat sequences, in certain special cases the classification simplifies.

Definition 2.12 ([8, §1.1.9])**.** A linear recurrence sequence is *degenerate* if its characteristic polynomial has two distinct zeros whose quotient is a root of unity.

Corollary 2.13. *Let $\{y_n\}$ be a rational linear recurrence sequence with separable characteristic polynomial. If $\{y_n\}$ is nondegenerate, then it is an Euler sequence iff it is a trace sequence.*

Corollary 2.14. *Suppose $f(t) \in \mathbb{Q}[t]$ is a separable polynomial such that the quotient of every pair of zeros is a root of unity. Then a sequence with characteristic polynomial $f(t)$ is Euler iff it is Fermat.*

After proving these results, we end §6 with some examples.

In §7 we solve the classification problem for Gauss sequences.

Theorem 2.15. *A sequence is Gauss iff it is a trace sequence.*

As mentioned in the introduction, it was already known that trace sequences are Gauss. The novelty in our result is that there are no others. In the context of dynamical systems, the literature contains some special cases of Theorem 2.15 [18, Theorem 1], [8, Theorem 11.9]. In particular, our Theorem 2.15 supplies the missing proof for Theorem 11.9 in Everest et al. [8].

Remark 2.16. Call a Fermat, Euler, or Gauss sequence *strict* if it is integral and satisfies the corresponding congruence condition at every prime. Classifying strict sequences adds additional complication. First, to have integer sequences, the characteristic polynomial must be monic. Assuming this, in the case of Fermat or Gauss sequences, the set of strict sequences is a full-rank free abelian subgroup of the corresponding space of rational sequences. This is clear from the definition in the case of Fermat sequences, and it follows easily from Theorem 2.15 in the case of Gauss sequences. For Euler sequences the full-rank condition may or may not hold. We give an example of each type in Example 6.13.

Remark 2.17. The definitions of Fermat, Euler, and Gauss sequences generalize naturally to number fields, and our results extend almost verbatim to this setting. For instance, the following is the generalization of Theorem 2.15. Let F be a number field with ring of integers $\mathcal{O}_F$. Let μ be the Möbius function of the lattice of ideals in $\mathcal{O}_F$, and let the norm of an ideal $\mathfrak{a} \subset \mathcal{O}_F$ be $N(\mathfrak{a}) = |\mathcal{O}_F/\mathfrak{a}|$. Define a sequence $\{x_n\}$ in F to be "F-Gauss" if

$$\sum_{\mathfrak{d}|\mathfrak{a}} \mu(\mathfrak{d}, \mathfrak{a}) x_{N(\mathfrak{d})} \in \hat{\mathfrak{a}}$$

for all ideals $\mathfrak{a} \subset \mathcal{O}_F$ and almost every completion of $\mathcal{O}_F$. Then the space of F-Gauss sequences is just the space of trace sequences, i.e., $\operatorname{span}_F\{\operatorname{Tr}_{F(\theta)/F}(\theta^n)\}$.

3. Results from number theory

Throughout we will assume familiarity with basic algebraic number theory. In addition, we will require the following results concerning the behavior of primes in number fields. Theorems 3.1 and 3.2 are immediate corollaries of Theorem 3.3, but we state all three separately in order to highlight how strong a result is actually required in our various applications.

Theorem 3.1. *In any number field there exist infinitely many primes which split completely.*

Proof. This has a short and elementary proof [9, Corollary to Theorem 5]. □

Theorem 3.2. *Let K be a number field and fix $\alpha \in K$. Suppose that, at almost every prime of K, the residue of α lies in the prime subfield of the residue field. Then $\alpha \in \mathbb{Q}$.*

Proof. This is the $\mathbb{Q}(\alpha)/\mathbb{Q}$ case of the theorem that, in any nontrivial extension of number fields, there are infinitely many primes which are not completely split. The more general statement is an easy consequence of the first inequality of class field theory, which has an algebraic proof [14, p. 19]. □

Theorem 3.3. *Let K be a Galois number field. For any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, there exist infinitely many primes $\mathfrak{p}$ of K such that $Frob_{\mathfrak{p}} = \sigma$.*

Proof. This is a weakened form of the Chebotarëv density theorem [15, p. 35], the proof of which requires analytic techniques. (In exchange one obtains the density of the set of primes with a given Frobenius, but we will not need this.) □

4. Notation

In the sequel we adopt the following notation.

We will always use $f(t) \in \mathbb{Q}[t]$ to refer to a characteristic polynomial. Given $f(t)$, let $\{r_1, \ldots, r_s\}$ be its distinct nonzero zeros, let $K = \mathbb{Q}(r_1, \ldots, r_s)$ be the splitting field, let $G = \mathrm{Gal}(K/\mathbb{Q})$ be the Galois group, and let $\mathcal{O}$ be the ring of integers in K. We extend the definitions of Fermat, Euler, and Gauss sequences to K-sequences by imposing the appropriate congruences at almost every completion of $\mathcal{O}$. (This is *not* the same concept as in Remark 2.17.)

The permutation action of G on $\{r_1, \ldots, r_s\}$ induces a permutation action on the indices $\{1, \ldots, s\}$ by setting $r_{g(i)} = g(r_i)$.

Given a linear recurrence $\{x_n\}$, we always denote its separable decomposition by $x_n = y_n + nz_n + w_n$, as in Definition-Lemma 2.2. The set $\{n \in \mathbb{N} : w_n \neq 0\}$ is the *support* of $\{w_n\}$. If the characteristic polynomial of $\{x_n\}$ is $f(t)$, then we write

$$y_n = \sum_{i=1}^{s} \alpha_i r_i^n$$

for some coefficients $\alpha_i \in K$.

For convenience we shall say that a rational prime p is of *good reduction* if (1) p is unramified in K, (2) $\{z_n\}$ and $\{w_n\}$ are integral at p, (3) the coefficients α_i are all integral at p, and (4) the zeros r_i are all units at p. Given a prime $\mathfrak{p}$ of K,

$$\kappa = \mathcal{O}/\mathfrak{p} = \hat{\mathcal{O}}_{\mathfrak{p}}/\hat{\mathfrak{p}}$$

denotes the residue field. We use $\alpha \mapsto \bar{\alpha}$ to denote reduction to κ. Whenever we write $\bar{\alpha}$, we assume implicitly that α is integral at $\mathfrak{p}$.

The conditions of good reduction imply in particular that the sequences $\{x_n\}$, $\{y_n\}$, $\{z_n\}$, and $\{w_n\}$ are all integral at p and that $\bar{r}_1, \ldots, \bar{r}_s \in \kappa$ are distinct and nonzero. Almost every (a.e.) prime is of good reduction. Given a prime p of good reduction, we say that $\{x_n\}$ is Fermat (resp., Euler or Gauss) at p if the corresponding congruence condition holds modulo p (resp., powers of p).

5. Classification of Fermat sequences

Proof of Proposition 2.3. If $\{y_n\}$ is Fermat and $z_1 + w_1 = 0$, then it is clear that $\{x_n\}$ is Fermat. The converse follows from the following slight generalization in the case $c = x_1$. □

Lemma 5.1. *Let $\{x_n\}$ be a rational linear recurrence sequence with separable decomposition $x_n = y_n + nz_n + w_n$. Suppose that, for some $c \in \mathbb{Q}$, $x_p \equiv c \pmod{p}$ for a.e. prime p. Then $\{y_n\}$ is a Fermat sequence with $y_1 = c$.*

Proof. Let p be a prime of good reduction, larger than the support of $\{w_n\}$, at which $x_p \equiv c$. Then $y_p \equiv x_p \equiv c \pmod{p}$, so to finish we just need to show that

$y_1 = c$. Towards this end, suppose additionally that p is completely split in K. At any prime over p we have $\kappa = \mathbb{F}_p$, so

$$\bar{y}_p = \sum_{i=1}^{s} \bar{\alpha}_i \bar{r}_i^p = \sum_{i=1}^{s} \bar{\alpha}_i \bar{r}_i = \bar{y}_1 \in \kappa.$$

Thus $y_p \equiv y_1 \pmod{p}$, and so $y_1 \equiv c \pmod{p}$. By Theorem 3.1 this holds at infinitely many primes, so $y_1 = c$, as desired. □

Suppose $f(t)$ is separable and $f(0) \neq 0$. Let W be the K-space of all recurrence sequences with characteristic polynomial $f(t)$. There are two particularly natural identifications of W with K^s: we may map a sequence $\{y_n = \sum \alpha_i r_i^n\}$ either to $(y_1, \ldots, y_s)$ or to $(\alpha_1, \ldots, \alpha_s)$. We refer to these as the *value basis* and the *coefficient basis*, respectively. We say that a K-subspace $V \subset W$ is *rational in the value (resp., coefficient) basis* if the corresponding subspace of K^s is generated in $\mathbb{Q}^s$.

Consider the following two actions of the Galois group G on W: G acts *on values* by $\rho_{\mathrm{v}}(g)(\{y_n\}) = \{g(y_n)\}$, and G acts *by permutation* by $\rho_{\mathrm{p}}(g)(\{\sum \alpha_i r_i^n\}) = \{\sum \alpha_i r_{g(i)}^n\}$. For convenience we write y_n^g for the nth term of $\rho_{\mathrm{p}}(g)(\{y_n\})$.

Lemma 5.2. *Let $V \subset W$ be a K-subspace. If V is invariant with respect to both G actions, then V is rational in the value and coefficient bases.*

Proof. Consider first the value basis. Identify V with a subspace of K^s and take a basis for V, thought of as a $d \times s$ matrix. Row-reduce this matrix so that it has a $d \times d$ identity submatrix and then replace each row v by its average $\frac{1}{|G|} \sum_{g \in G} \rho_{\mathrm{v}}(g)(v)$. The resulting rows are still in V, by invariance under the action on values, and they are linearly independent as there is an identity submatrix. Hence we have a new basis for V which is defined over $\mathbb{Q}^s$. To handle the coefficient basis, consider the following third action of G on W: $\rho(g)(\{\sum \alpha_i r_i^n\}) = \{\sum g(\alpha_i) r_i^n\}$. Then $\rho(g) = \rho_{\mathrm{v}}(g) \circ \rho_{\mathrm{p}}(g^{-1})$, so V is also invariant with respect to the ρ action. Now rationality in the coefficient basis follows similarly. □

Proposition 5.3. *Suppose $f(t)$ is separable and $f(0) \neq 0$. Let $V \subset W$ be the space of Fermat K-sequences with characteristic polynomial $f(t)$. Then V is exactly the space of sequences $\{y_n\}$ such that $y_1^g = y_1^h$ for all $g, h \in G$.*

Proof. Let $\{y_n = \sum \alpha_i r_i^n\} \in V$ be an arbitrary Fermat K-sequence and choose $g \in G$. Choose a prime $\mathfrak{p}$ of K, lying over a prime p of good reduction at which $\{y_n\}$ is Fermat, such that $\mathrm{Frob}_{\mathfrak{p}} = g$. There exist infinitely many such primes $\mathfrak{p}$ by Theorem 3.3. Working in the residue field κ at $\mathfrak{p}$,

$$\bar{y}_p = \sum_{i=1}^{s} \bar{\alpha}_i \bar{r}_i^p = \sum_{i=1}^{s} \bar{\alpha}_i \overline{\mathrm{Frob}_{\mathfrak{p}}(r_i)} = \sum_{i=1}^{s} \bar{\alpha}_i \bar{r}_{g(i)} = \bar{y}_1^g. \tag{5.1}$$

But $\bar{y}_p = \bar{y}_1$, so $\bar{y}_1 = \bar{y}_1^g$. This holds for infinitely many primes, so in fact $y_1 = y_1^g$.

It remains to show that a sequence satisfying $y_1^g = y_1^h$ for all $g, h \in G$ is Fermat. Let p be any prime of good reduction and let $\mathfrak{p}$ be any prime of K lying over p. Letting $g = \mathrm{Frob}_{\mathfrak{p}}$, we have $\bar{y}_p = \bar{y}_1^g$ by equation (5.1). By assumption the right side is $\bar{y}_1$. This holds for all primes over p, so $y_p \equiv y_1 \pmod{p}$. □

Proof of Theorem 2.4. Let V be the space of Fermat K-sequences as in Proposition 5.3. Evidently V is invariant under ρ_{v}, and Proposition 5.3 shows that V is invariant under ρ_{p}. Applying Lemma 5.2, the following two $\mathbb{Q}$-subspaces of V have

the same dimension: (1) Fermat sequences with rational values, and (2) Fermat sequences with rational coefficients. Consider the second space. If $\{y_n\}$ is a sequence with rational coefficients, then $g(y_1) = y_1^g$. This reduces the condition of Proposition 5.3 to $g(y_1) = y_1$ for all $g \in G$, or equivalently $y_1 \in \mathbb{Q}$. Thus we are looking for the dimension of $A = \{(a_1, \ldots, a_s) \in \mathbb{Q}^s : \sum a_i r_i \in \mathbb{Q}\}$. If we require the sum to be 0, then we get a space $A' \subseteq A$ of dimension $s - e$. The codimension of A' in A is either 0 or 1, with the latter holding iff $\mathbb{Q} \subseteq \operatorname{span}_{\mathbb{Q}}\{r_i\}$. But that happens iff some r_i has nonzero trace, as desired. $\square$

Theorem 2.4 reduces the classification of Fermat sequences to the problem of classifying linear dependencies amongst the zeros of $f(t)$. This problem has been studied in the literature: for our purposes, the results of Girstmair [11, 12] and of Berry et al. [3] are particularly relevant. We now briefly survey the implications of this theory in the context of Fermat sequences.

If $f(t)$ has k irreducible factors over $\mathbb{Q}$, then it always has at least a k-dimensional space of Fermat sequences: namely, the trace sequences. One source of additional Fermat sequences is interaction between distinct irreducible factors. The polynomial $f(t) = (x^2+1)(x^2-2x+2)$ provides an example: its space of Fermat sequences has dimension 3, but there is only a 2-dimensional space of trace sequences.

If we limit our attention to irreducible characteristic polynomials, there can still be more Fermat sequences than trace sequences. Let θ, θ' be algebraic numbers such that $\mathbb{Q}(\theta)$ and $\mathbb{Q}(\theta')$ are linearly disjoint. If $\{\theta_i\}_{i=1}^s$ and $\{\theta'_j\}_{j=1}^{s'}$ are the conjugates of θ and θ', respectively, then the conjugates of $\theta + \theta'$ are $\{\theta_i + \theta'_j\}_{i \le s, j \le s'}$. The space A in the proof of Theorem 2.4 includes any set of coefficients $\{a_{ij}\}$ such that both $j \mapsto \sum_{i=1}^s a_{ij}$ and $i \mapsto \sum_{j=1}^{s'} a_{ij}$ are constant. Thus, taking $f(t)$ to be the minimal polynomial of $\theta + \theta'$, the corresponding space of Fermat sequences has dimension $\ge (s-1)(s'-1)+1$. This corresponds to the fact that both $\bar{y}_1$ and $\bar{y}_p$ are additive in the zeros $\{r_1, \ldots, r_s\}$. In such examples the Galois group is an *imprimitive* permutation group.

Even if we further limit our attention to irreducible characteristic polynomials such that the Galois group is primitive, there may still be Fermat sequences other than the trace sequences. Girstmair gives a procedure to determine exactly what spaces A can arise for an irreducible polynomial $f(t)$ with given Galois group G [11]. He also gives an application of this theory [11, Theorem 1] which, after translating into the language of Fermat sequences, yields the following.

Example 5.4. There exist Fermat sequences of recurrence length 9, with irreducible characteristic polynomial and primitive Galois group, which do not arise from trace sequences. In these cases the Galois group is necessarily isomorphic to either $(\mathbb{Z}/3)^2 \rtimes \mathbb{Z}/4$ or $S_3 \wr S_2$. There are no such examples of smaller recurrence length.

Girstmair expands upon this framework in a later article [12], where he also produces more examples: for instance, there are irreducible polynomials $f(t)$ of degree 55, with primitive Galois group, admitting a 5-dimensional space of Fermat sequences [12, p. 71].

More spectacular examples are provided by Berry et al., who answer the following question: for fixed $e = \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}}\{r_i\}_{i=1}^s$, what is the largest possible value of s [3, Theorem 1]? (Note that there is no primitivity assumption here.) For

$e \notin \{2,4,6,7,8,9,10\}$, the answer is $2^e e!$. In the exceptional dimensions, s may be larger. For instance, we have the following.

Example 5.5. There exists an irreducible, monic polynomial $f(t) \in \mathbb{Z}[t]$ of degree 1152 such that the space of Fermat sequences with characteristic polynomial $f(t)$ has dimension 1148.

Despite all of this, there are cases in which we can be assured of only getting trace sequences. We close this section with the

Proof of Corollary 2.7. By Theorem 2.4, the desired conclusion is equivalent to the following: if $\sum_{i=1}^s a_i r_i \in \mathbb{Q}$ with $a_i \in \mathbb{Q}$, then $a_1 = \cdots = a_s$. In this formulation, both cases are in the literature [11, Propositions 4(3) and 6]. We repeat here an abbreviated proof of (i). Let $M \subset \mathbb{Q}^s$ be the space of vectors $(a_1, \ldots, a_s)$ with $\sum a_i = 0$ and let $N \subset M$ be the subspace of vectors with $\sum a_i r_i \in \mathbb{Q}$. Letting G act by permutation of coordinates, N and M are G-invariant. By Cauchy's theorem, G contains an element σ of order s, i.e., a cycle of $\{r_1, \ldots, r_s\}$. The characteristic polynomial of $\sigma|_M$ is $t^{s-1} + \cdots + t + 1$, which is $\mathbb{Q}$-irreducible, so M is already $\langle\sigma\rangle$-irreducible. Thus $N = 0$ or $N = M$, and the latter is impossible. □

6. Classification of Euler sequences

In this section we prove Proposition 2.8, Theorem 2.11, and Corollaries 2.13 and 2.14. The plan for this is as follows. First, we relax the definition of Euler sequences and establish some properties of these generalized sequences. Then we use these to show that the relaxed definition actually coincides with the original definition, obtaining at the same time an equivalent Galois-theoretic formulation. This reformulation is the heart of the argument; once we have it, the main results follow easily.

Definition 6.1. A rational (resp., K-valued) linear recurrence sequence $\{x_n\}$ is *weakly Euler* if, for almost every prime p, the sequence $\{x_{p^n}\}$ converges in $\mathbb{Z}_p$ (resp., in every completion of $\mathcal{O}$ at a prime over p).

Definition-Lemma 6.2. Let D be a complete discrete valuation ring with finite residue field κ. Any element of $\kappa^\times$ has a unique lift to a root of unity in D of order prime to $|\kappa|$, its *Teichmüller lift*. The resulting map $\omega : \kappa^\times \to D^\times$ is a group homomorphism, the *Teichmüller character* of D.

Proof. This is standard; apply Hensel's lemma to the polynomials $t^{|\kappa|^e} - t$. □

Let $c_1, \ldots, c_s \in K$ be coefficients and consider the linear equation $\sum_{i=1}^s c_i \zeta_i = 0$, where each ζ_i is required to be a root of unity (in K^{ab}, say). We say that two solutions $(\zeta_1, \ldots, \zeta_s)$ and $(\zeta_1', \ldots, \zeta_s')$ are *equivalent* if there is a partition $\{1, \ldots, s\} = I_1 \sqcup \cdots \sqcup I_t$ of the indices such that, for each $k \in \{1, \ldots, t\}$, (i) $\sum_{i \in I_k} c_i \zeta_i = 0$ and (ii) there exists a root of unity ζ such that $\zeta_i' = \zeta \zeta_i$ for all $i \in I_k$.

Theorem 6.3. *Up to equivalence, any linear equation has finitely many solutions in roots of unity.*

Proof. By passing to subsets, we may assume without loss of generality that no proper subsum vanishes; by scaling, we may assume $\zeta_1 = 1$. But then a theorem of Schinzel [19, Theorem 1] bounds the order of the remaining ζ_i's. □

Corollary 6.4. *For each prime $\mathfrak{p}$ of K, let $\omega_{\mathfrak{p}} : \kappa^\times \to \hat{\mathcal{O}}_{\mathfrak{p}}^\times$ be the Teichmüller character. Let $c_i \in K$ and $r_i \in K^\times$, $i \in \{1, \dots, s\}$, be elements such that*

$$\sum_{i=1}^{s} c_i \cdot \omega_{\mathfrak{p}}(\bar{r}_i) = 0 \in \hat{\mathcal{O}}_{\mathfrak{p}} \tag{6.1}$$

for infinitely many primes $\mathfrak{p}$. Then there exists a partition $\{1, \dots, s\} = I_1 \sqcup \cdots \sqcup I_t$ of the indices such that, for all $k \in \{1, \dots, t\}$, (i) $\sum_{i \in I_k} c_i r_i = 0$ and (ii) r_i/r_j is a root of unity for all $i, j \in I_k$.

Proof. Each Teichmüller lift $\omega_{\mathfrak{p}}(\bar{r}_i)$ is a root of unity, so we may think of equation (6.1) as a linear equation with solutions in roots of unity. There are finitely many equivalence classes of solutions by Theorem 6.3, so some equivalence class occurs infinitely often. That is, we can find a partition $\{1, \dots, s\} = I_1 \sqcup \cdots \sqcup I_t$ and vectors $\{(\zeta_i : i \in I_k)\}_{k=1}^t$ of roots of unity such that, for each $k \in \{1, \dots, t\}$, (1) $\sum_{i \in I_k} c_i \zeta_i = 0$ and (2) for infinitely many primes $\mathfrak{p}$ the vector $(\omega_{\mathfrak{p}}(\bar{r}_i) : i \in I_k)$ is a multiple of $(\zeta_i : i \in I_k)$.

Fix $k \in \{1, \dots, t\}$ and let $\mathfrak{p}$ be a prime of K such that $(\omega_{\mathfrak{p}}(\bar{r}_i) : i \in I_k)$ is a multiple of $(\zeta_i : i \in I_k)$. Let $i, j \in I_k$ be arbitrary; then reducing at $\mathfrak{p}$ gives $\bar{r}_i/\bar{r}_j = \bar{\zeta}_i/\bar{\zeta}_j$. This holds at infinitely many primes, so in fact $r_i/r_j = \zeta_i/\zeta_j$. This gives (ii). It also implies that $(r_i : i \in I_k)$ is a multiple of $(\zeta_i : i \in I_k)$, which together with property (1) proves (i). □

Observation 6.5. If $\alpha \equiv \beta \pmod{p}$, then $\alpha^{p^n} \equiv \beta^{p^n} \pmod{p^{n+1}}$ for all $n \geq 0$.

Proposition 6.6. *Suppose $f(t)$ is separable and $f(0) \neq 0$. Let $\{r_i\}_{i=1}^s = R_1 \sqcup \cdots \sqcup R_t$ be the partition of the zeros of $f(t)$ with respect to the following equivalence relation: $r_i \sim r_j$ iff r_i/r_j is a root of unity. Let $\{y_n = \sum_{i=1}^s \alpha_i r_i^n\}$ be a linear recurrence sequence over K with characteristic polynomial $f(t)$. For $g \in G$ and $k \in \{1, \dots, t\}$, define the partial sum*

$$\beta_k^g = \sum_{i : r_i \in R_k} \alpha_{g^{-1}(i)} r_i.$$

If $\{y_n\}$ is weakly Euler, then $\beta_k^g = \beta_k^h$ for all $g, h \in G$ and all $k \in \{1, \dots, t\}$.

Proof. Choose an automorphism $g \in G$ and let $\mathfrak{p}$ be a prime of K, lying over a prime of good reduction at which $\{y_n\}$ is weakly Euler, with $\mathrm{Frob}_{\mathfrak{p}} = g$. There exist infinitely many such primes by Theorem 3.3. For each $i \in \{1, \dots, s\}$, let $\hat{r}_i = \omega_{\mathfrak{p}}(\bar{r}_i) \in \hat{\mathcal{O}}_{\mathfrak{p}}$, the Teichmüller lift of the residue of r_i at $\mathfrak{p}$. Then $r_i \equiv \hat{r}_i \pmod{p}$, so $r_i^{p^n} \equiv \hat{r}_i^{p^n} \pmod{p^{n+1}}$ for all $n \geq 0$ by Observation 6.5. In particular, the p-adic convergence of $\{\sum \alpha_i r_i^{p^n}\}$ implies the $\mathfrak{p}$-adic convergence of $\{\sum \alpha_i \hat{r}_i^{p^n}\}$.

Let e be the residual degree of $K/\mathbb{Q}$ at p, i.e., $e = [\kappa : \mathbb{F}_p]$. Then $\hat{r}_i^{p^e - 1} = 1$ for each i, which implies that $\{\sum \alpha_i \hat{r}_i^{p^n}\}$ is periodic. Convergent periodic sequences are constant, so in particular $\sum \alpha_i \hat{r}_i^p = \sum \alpha_i \hat{r}_i$. Now $\hat{r}_i^p$ is a $(p^e - 1)$th root of unity with residue $\bar{r}_i^p = \overline{\mathrm{Frob}_{\mathfrak{p}}(r_i)} = \bar{r}_{g(i)}$. Hence $\hat{r}_i^p = \hat{r}_{g(i)}$ by the uniqueness of Teichmüller lifts. Substituting this into the equation $\sum \alpha_i \hat{r}_i^p = \sum \alpha_i \hat{r}_i$ and reindexing, we have

$$\sum_{i=1}^{s} (\alpha_{g^{-1}(i)} - \alpha_i) \hat{r}_i = 0. \tag{6.2}$$

This holds for infinitely many primes $\mathfrak{p}$, so we can apply Corollary 6.4. That implies $\sum_{i : r_i \in R_k} (\alpha_{g^{-1}(i)} - \alpha_i) r_i = 0$ for each $k \in \{1, \dots, t\}$, as desired. □

Proposition 6.7. *With notation as in Proposition* 6.6*, suppose* $\{y_n\}$ *satisfies* $\beta_k^g = \beta_k^h$ *for all* $g, h \in G$ *and all* $k \in \{1, \dots, t\}$*. Then* $\{y_n\}$ *is an Euler sequence.*

Proof. Let p be any prime of good reduction and let $\mathfrak{p}$ be any prime of K over p. Let $k \in \{1, \dots, t\}$ be arbitrary. For any $r_i, r_j \in R_k$, $r_i/r_j \in K$ is a root of unity, and its order must be prime to p because p is unramified in K. Thus $\hat{r}_i/\hat{r}_j = \omega_{\mathfrak{p}}(\overline{r_i/r_j}) = r_i/r_j$ by the uniqueness of Teichmüller lifts. As this holds for all i, j, the vector $(\hat{r}_i : r_i \in R_k)$ is a multiple of $(r_i : r_i \in R_k)$.

Let $g, h \in G$ be arbitrary. By assumption $\beta_k^g = \beta_k^h$, i.e., $\sum_{i: r_i \in R_k} (\alpha_{g^{-1}(i)} - \alpha_{h^{-1}(i)}) r_i = 0$. Because they are related by a scalar multiple, the same relation holds with each r_i replaced with $\hat{r}_i$. Summing over k and reindexing,

$$\sum_{i=1}^{s} \alpha_i \hat{r}_{g(i)} = \sum_{i=1}^{s} \alpha_i \hat{r}_{h(i)}. \tag{6.3}$$

Choose $n \geq 1$ and let $g = (\mathrm{Frob}_{\mathfrak{p}})^n$ and $h = (\mathrm{Frob}_{\mathfrak{p}})^{n-1}$. Then, arguing as in Proposition 6.6, $\hat{r}_{g(i)} = \hat{r}_i^{p^n}$ and $\hat{r}_{h(i)} = \hat{r}_i^{p^{n-1}}$. Applying Observation 6.5, these are congruent modulo p^n to $r_i^{p^n}$ and $r_i^{p^{n-1}}$, respectively. Substituting this back into equation (6.3), we get the congruence $y_{p^n} \equiv y_{p^{n-1}} \pmod{p^n}$ in $\hat{\mathcal{O}}_{\mathfrak{p}}$. This holds for a.e. $\mathfrak{p}$, so $\{y_n\}$ is Euler. □

Corollary 6.8. *Suppose* $f(t)$ *is separable and* $f(0) \neq 0$*. A linear recurrence sequence with characteristic polynomial* $f(t)$ *is weakly Euler iff it is Euler. Moreover, the condition* $\beta_k^g = \beta_k^h$ *in Propositions* 6.6 *and* 6.7 *exactly characterizes Euler sequences.*

Proof. Proposition 6.6 is the implication (weakly Euler) $\Rightarrow$ ($\beta_k^g = \beta_k^h$), Proposition 6.7 states that ($\beta_k^g = \beta_k^h$) $\Rightarrow$ (Euler), and (Euler) $\Rightarrow$ (weakly Euler) *a fortiori.* □

We can now proceed directly to the

Proof of Proposition 2.8. The ($\Leftarrow$) implication is straightforward, so we show ($\Rightarrow$). Suppose $\{x_n\}$ is Euler. Let p be any prime of good reduction, larger than the support of $\{w_n\}$, at which $\{x_n\}$ is Euler. Then $x_{p^n} \equiv x_{p^{n-1}} \pmod{p^n}$. Taking $n \geq 2$ and looking modulo p^{n-1} instead of p^n, this implies $y_{p^n} \equiv y_{p^{n-1}} \pmod{p^{n-1}}$. Hence $\{y_n\}$ is weakly Euler, and so Euler by Corollary 6.8.

With p as above, $x_{p^2} \equiv x_p \pmod{p^2}$ and $y_{p^2} \equiv y_p \pmod{p^2}$, so we have $z_p \equiv 0 \pmod{p}$. Thus Lemma 5.1 yields that $\{z'_n\}$ is Fermat with $z'_1 = 0$. Finally, Proposition 2.3 applied to $\{x_n\}$ (which is Fermat *a fortiori*) yields $z_1 + w_1 = 0$. □

Lemma 6.9. *With notation as in Proposition* 6.6*,* $\{y_n\}$ *is a vanishing sequence iff* $\beta_k^g = 0$ *for all* $k \in \{1, \dots, t\}$ *and* $g \in G$*.*

Proof. We first prove ($\Leftarrow$). For $k \in \{1, \dots, t\}$, let $R_k = \{\theta_k, \omega_{k,1}\theta_k, \dots, \omega_{k,f_k}\theta_k\}$, where each $\omega_{k,j}$ is a root of unity. Let m be the least common multiple of the orders of all of the roots of unity $\omega_{k,j}$. Then K contains $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive mth root of unity. Let n be relatively prime to m and let σ be any extension of the automorphism $\zeta_m \mapsto \zeta_m^n$ from $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ to $K/\mathbb{Q}$. For convenience, set $\omega_{k,0} = 1$ and let $\alpha_{k,j}$ be the coefficient α_i for the index i such that $r_i = \omega_{k,j}\theta_k$. Let G act

on indices $k \in \{1, \ldots, t\}$ by $R_{g \cdot k} = g(R_k)$. Then

$$y_n = \sum_{k=1}^{t} \sum_{j=0}^{f_k} \alpha_{k,j} \omega_{k,j}^n \theta_k^n = \sum_{k=1}^{t} \frac{\theta_k^n}{\sigma(\theta_k)} \sum_{j=0}^{f_k} \alpha_{k,j} \sigma(\omega_{k,j} \theta_k) = \sum_{k=1}^{t} \frac{\theta_k^n}{\sigma(\theta_k)} \beta_{\sigma \cdot k}^{\sigma}. \tag{6.4}$$

Each β_k^g vanishes, so $y_n = 0$ as desired.

We now prove ($\Rightarrow$), keeping the same notation as above. Suppose $y_n = 0$ for all n relatively prime to $m' \geq 1$. After possibly replacing m' by a multiple, we may assume that $m \mid m'$. Let $g \in G$ be arbitrary. Then $g(\zeta_m) = \zeta_m^e$ for some e relatively prime to m. The exponent e is only defined modulo m, so in particular we may assume that e is relatively prime to m'. Now for any $n \equiv e \pmod{m'}$, we get equation (6.4) with $\sigma = g$. Writing this out, for any integer d we have

$$\sum_{k=1}^{t} (\theta_k^{m'})^d \cdot \frac{\theta_k^e}{g(\theta_k)} \beta_{g \cdot k}^g = 0.$$

Note that $\theta_k^{m'} \neq \theta_{k'}^{m'}$ for $k \neq k'$, as θ_k and $\theta_{k'}$ are in different $\sim$-equivalence classes. Taking the above equation for $d \in \{0, \ldots, t-1\}$ and using nonvanishing of the corresponding Vandermonde determinant, we see that $\beta_{g \cdot k}^g = 0$ for all k. $\square$

Remark 6.10. One can compute the dimension of the space of vanishing sequences by using Lemma 6.9 and applying Lemma 5.2 as in the proof of Theorem 2.4. By the same methods one can compute the dimension of the intersection of this space with the space of trace sequences, and (invoking Theorem 2.11) thereby compute the dimension of the space of Euler sequences.

Proof of Theorem 2.11. If $\{y_n\}$ is a trace sequence, then $\alpha_{g(i)} = \alpha_i$ for all $i \in \{1, \ldots, s\}$ and $g \in G$. Hence we certainly have $\beta_k^g = \beta_k^h$ for all $k \in \{1, \ldots, t\}$ and $g, h \in G$. If $\{y_n\}$ is a vanishing sequence, then $\beta_k^g = 0$ for all k and g by Lemma 6.9, so again $\beta_k^g = \beta_k^h$ for all k and g, h. By Corollary 6.8, in either case $\{y_n\}$ is an Euler sequence. This implies ($\Leftarrow$).

We now prove ($\Rightarrow$). Suppose $\{y_n\}$ is an Euler sequence with separable characteristic polynomial $f(t)$. Proposition 2.8 implies $w_1 = 0$, so we may assume $f(0) \neq 0$. With this, Corollary 6.8 tells us that $\beta_k^g = \beta_k^h$ for all $k \in \{1, \ldots, t\}$ and $g, h \in G$.

The sequence $\{y_n\}$ is rational valued, and so Galois-invariant. It follows that $\alpha_{g(i)} = g(\alpha_i)$ for all $i \in \{1, \ldots, s\}$ and $g \in G$. Define a sequence $\{y_n^{\mathrm{tr}}\}$ by

$$y_n^{\mathrm{tr}} = \sum_{i=1}^{s} \left(\frac{1}{|G|} \sum_{g \in G} \alpha_{g(i)} \right) r_i^n = \sum_{i=1}^{s} \left(\frac{1}{|G|} \sum_{g \in G} g(\alpha_i) \right) r_i^n.$$

Consider the coefficients of this sequence. From the middle expression it is clear that Galois-conjugate zeros have the same coefficient, and from the last expression it is clear that these coefficients are rational. Thus $\{y_n^{\mathrm{tr}}\}$ is a rational trace sequence.

Let $\{y_n^{\mathrm{van}}\}$ be the sequence $y_n^{\mathrm{van}} = y_n - y_n^{\mathrm{tr}}$. For $k \in \{1, \ldots, t\}$ and $g \in G$ let γ_k^g be the partial sum for $\{y_n^{\mathrm{van}}\}$ analogous to β_k^g for $\{y_n\}$. Then

$$\gamma_k^g = \sum_{i : r_i \in R_k} \left(\alpha_{g^{-1}(i)} - \frac{1}{|G|} \sum_{h \in G} \alpha_{hg^{-1}(i)} \right) r_i = \beta_k^g - \frac{1}{|G|} \sum_{h \in G} \beta_k^{gh^{-1}} = 0.$$

Thus $\{y_n^{\mathrm{van}}\}$ is a vanishing sequence by Lemma 6.9. This completes the proof. $\square$

Remark 6.11. This proof actually yields slightly more than was claimed: given an Euler sequence with separable characteristic polynomial $f(t)$, we may find constituent trace and vanishing sequences both having characteristic polynomial $f(t)$.

Proof of Corollary 2.13. Lemma 6.9 implies that a nondegenerate vanishing sequence is zero. Degeneracy is a property of the characteristic polynomial, so there are no nonzero vanishing sequences with the same characteristic polynomial as $\{y_n\}$. Now the corollary follows from Theorem 2.11 and Remark 6.11. □

Proof of Corollary 2.14. With such a characteristic polynomial $f(t)$, the partition in Proposition 6.6 consists of a single equivalence class. Thus, by Corollary 6.8, a sequence $\{y_n\}$ with characteristic polynomial $f(t)$ is Euler iff $\sum_{i=1}^{s} \alpha_{g^{-1}(i)} r_i = \sum_{i=1}^{s} \alpha_{h^{-1}(i)} r_i$ for all $g, h \in G$. In the notation of §5 this is the condition $y_1^g = y_1^h$, which by Proposition 5.3 is the same condition characterizing Fermat sequences. □

The corollaries just proven show that in many cases Euler sequences are the same as Gauss sequences (Corollary 2.13; cf. Theorem 2.15) and in some cases Euler sequences are the same as Fermat sequences (Corollary 2.14). It is also possible for the space of Euler sequences to lie strictly between the spaces of Gauss and Fermat sequences, as the following example demonstrates.

Example 6.12. Choose relatively prime $n, m \geq 2$, n composite, and distinct primes $p \neq q$ not dividing nm. Let $f(t)$ be the minimal polynomial of $p^{1/m}(1 - q^{1/n})$. The zeros of $f(t)$ are $\{r_{ij} := \zeta_m^i p^{1/m}(1 - \zeta_n^j q^{1/n})\}_{i \leq m, j \leq n}$. In the decomposition of Proposition 6.6, there are n equivalence classes, one for each choice of j. Following the procedure sketched in Remark 6.10, one computes that all trace sequences with characteristic polynomial $f(t)$ are also vanishing sequences, and the space of vanishing sequences has dimension $(m - \phi(m))n$. This comes from the $(m - \phi(m))$-dimensional spaces, for each j, of $\mathbb{Q}$-relations of $\{r_{ij}\}_{i \leq m}$. Using Theorems 2.4 and 2.15, the spaces of Fermat and Gauss sequences with characteristic polynomial $f(t)$ have dimension $mn - \phi(m)(\phi(n) + 1)$ and 1, respectively. Thus the space of Euler sequences lies strictly between the spaces of Fermat and Gauss sequences.

Finally, we consider the integrality issue raised in Remark 2.16. As mentioned there, for Euler sequences it may not be the case that the subgroup of strict sequences is of full rank. To determine the rank, one needs to consider additional local equations like equation (6.2) at the ramified primes — or, more precisely, at the primes dividing the orders of the roots of unity that arise as quotients of characteristic zeros. Sometimes these equations can only be satisfied by trace sequences, and sometimes they admit more solutions.

Example 6.13. Consider the sequence $\{Q_n\}$ defined by $Q_1 = 0$, $Q_2 = 1$, $Q_3 = 0$, $Q_4 = -2$, and $Q_n = -Q_{n-2} - Q_{n-4}$ for $n \geq 5$. This is a vanishing sequence, and so an Euler sequence. However, the subsequence $\{Q_{2^n}\}$ alternates between 1 and -2, so in particular it does not converge 2-adically. Thus no multiple of $\{Q_n\}$ is a strict Euler sequence. One can compute that the space of Euler sequences with characteristic polynomial $t^4 + t^2 + 1$ is 2-dimensional, but the subgroup of strict sequences only has rank 1 because of the deficiency of $\{Q_n\}$. The polynomial $t^6 - 3t^3 - 1$ provides a different sort of example. Again one can compute that the space of Euler sequences with this characteristic polynomial is 2-dimensional. To test for strictness one has to look at a local equation at $p = 3$, which turns out to be always satisfied. Hence the subgroup of strict Euler sequences is of full rank.

7. Classification of Gauss sequences

Proof of necessity in Theorem 2.15. Let p be any prime of good reduction, larger than s and larger than the support of $\{w_n\}$, at which $\{x_n\}$ is Gauss. Fix $k \in \{1, \dots, s\}$ and consider the Gauss congruence in $\mathbb{Z}_p$ for $m = p^2 k$. This simplifies to the condition

$$\sum_{d|k} \mu(\tfrac{k}{d})(x_{p^2 d} - x_{pd}) \equiv 0 \pmod{p^2}.$$

Letting k vary, we get a unimodular triangular system; hence $x_{p^2 d} - x_{pd} \equiv 0 \pmod{p^2}$ for each $d \in \{1, \dots, s\}$. Let $\mathfrak{p}$ be any prime of K above p and consider this congruence modulo $\mathfrak{p}$ instead of p^2. We see that

$$\bar{y}_{p^2 d} = \bar{x}_{p^2 d} = \bar{x}_{pd} = \bar{y}_{pd} \in \kappa.$$

Let $\sigma \in \mathrm{Gal}(\kappa/\mathbb{F}_p)$ be the Frobenius automorphism. Both $\bar{y}_{p^2 d}$ and $\bar{y}_{pd}$ lie in $\mathbb{F}_p$, so they are σ-invariant. Thus $\sigma^{-2}(\bar{y}_{p^2 d}) = \bar{y}_{p^2 d} = \bar{y}_{pd} = \sigma^{-1}(\bar{y}_{pd})$. Expanding this,

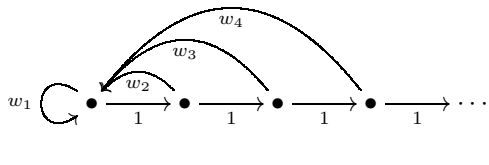
$$\sum_{i=1}^{s} (\sigma^{-2}(\bar{\alpha}_i) - \sigma^{-1}(\bar{\alpha}_i))\bar{r}_i^d = 0.$$

This holds for all $d \in \{1, \dots, s\}$, and $\{\bar{r}_i\}$ is a set of s distinct elements in the field κ, all of which are nonzero. Thus, by the nonvanishing of the Vandermonde determinant, we must have $\sigma^{-2}(\bar{\alpha}_i) - \sigma^{-1}(\bar{\alpha}_i) = 0$, i.e., $\sigma(\bar{\alpha}_i) = \bar{\alpha}_i$, for each i. This implies that $\bar{\alpha}_i \in \mathbb{F}_p$. We have this for a.e. prime $\mathfrak{p}$ of K, so $\alpha_i \in \mathbb{Q}$ by Theorem 3.2. Now Galois invariance of $\{y_n\}$ shows that $\alpha_i = \alpha_j$ when r_i and r_j are conjugate, so $\{y_n\}$ has the desired form.

It remains only to show that $z_n = w_n = 0$. Let ℓ be the recurrence length of $\{z_n\}$ and let $\ell' \geq 0$ be larger than the support of $\{w_n\}$. Let p be as above, with the additional condition that $p > \ell + \ell'$. Considering the Gauss congruence for $m = pk$ instead of $m = p^2 k$, the same argument shows that $x_{pd} \equiv x_d \pmod{p}$ for each $d \in \{1, \dots, \ell + \ell'\}$. Using the form just proven for $\{y_n\}$, it is easy to verify that $y_{pd} \equiv y_d \pmod{p}$. (Alternately, one may use Theorem 3.1 and limit to completely split primes p, whence $y_{pd} \equiv y_d \pmod{p}$ automatically holds.) Thus the congruence $x_{pd} \equiv x_d \pmod{p}$ reduces to $p \mid dz_d + w_d$. Taking $d \in \{\ell' + 1, \dots, \ell' + \ell\}$, we have $p \mid dz_d$. This is true for infinitely many p, so $z_d = 0$; but that holds for a full set of initial conditions for $\{z_n\}$, so in fact $z_n = 0$ for all $n \geq 1$. Substituting back into $p \mid dz_d + w_d$, $d \in \{1, \dots, \ell'\}$, the same argument now yields $w_d = 0$. □

Remark 7.1. One can easily check that a sequence $\{x_n\}_{n=1}^{\infty}$ is Gauss iff every subsequence $\{x_{dn}\}_{n=1}^{\infty}$, $d \geq 1$, is Euler. Using this, Theorem 2.15 can be obtained as a corollary of Proposition 2.8 and Theorem 2.11. However, the proof just given is simpler and more elementary than the proof of Theorem 2.11.

The remaining part of Theorem 2.15 is the assertion that trace sequences are Gauss. This fact was previously known, but for completeness we also give a proof here. Our proof proceeds by analyzing the zeta function of the sequence and using the following proposition. It is not new [4, Theorems 1.3 and 1.8], but we give a slightly different, more direct combinatorial argument.



Γ

$$\begin{pmatrix} w_1 & w_2 & w_3 & \cdots \\ 1 & 0 & & \\ & 1 & 0 & \\ & & 1 & \ddots \\ & & & \ddots \end{pmatrix}$$

A

FIGURE 1. A weighted, directed, infinite graph Γ and its adjacency matrix A

Proposition 7.2. *Let R be a domain of characteristic 0, let $\{x_n\}$ be an R-valued sequence, and define the associated zeta function*

$$\zeta_x(t) = \exp\left(\sum_{n\geq 1} x_n \frac{t^n}{n}\right) \in \mathrm{Frac}(R)[\![t]\!].$$

Then $\{x_n\}$ satisfies the Gauss congruence (1.3) in R, for all $m \geq 1$, iff $\zeta_x(t)$ has coefficients in R.

Proof. Given weights $\{w_n\}_{n\geq 1}$ to be specified later, consider the weighted graph Γ in Figure 1. For each $n \geq 1$, let x'_n be the total weight of the cycles in Γ of length n, with distinct cyclic shifts counted separately, and let b_n be the total weight of the cycles of period exactly n, with cyclic shifts *not* counted separately. We make the following observations:

- The number of distinct cyclic shifts of any cycle is equal to its period. Thus $x'_n = \sum_{m|n} m b_m$ for all $n \geq 1$.
- For each n, x'_n equals nw_n plus a polynomial in $\{w_i\}_{i<n}$. Thus, inductively, we may uniquely choose weights $\{w_n\}$ in $\mathrm{Frac}(R)$ such that $x'_n = x_n$ for all $n \geq 1$. We henceforth make this choice.
- For any $n \geq 1$, b_n equals w_n plus an integer-coefficient polynomial in $\{w_i\}_{i<n}$. Thus, inductively, $\{b_n\}$ is a sequence in R iff $\{w_n\}$ is.

Using the first two observations and applying Möbius inversion,

$$b_m = \frac{1}{m}\sum_{d|m} \mu(\tfrac{m}{d}) x_d$$

for all $m \geq 1$. Hence $\{x_n\}$ satisfies the Gauss congruence in R iff $\{b_m\}$ is an R-valued sequence. Using the third observation, it remains only to show that the sequence $\{w_n\}$ is R-valued iff $\zeta_x(t)$ has coefficients in R.

Let A be the (infinite) adjacency matrix of Γ as in Figure 1. Applying the identity $\det(\exp M) = \exp(\mathrm{tr}\, M)$ to $M = -\log(I - tA)$ yields

$$\det(I - tA)^{-1} = \exp\left(\sum_{n\geq 1} \mathrm{tr}(A^n)\frac{t^n}{n}\right).$$

We have $\mathrm{tr}\, A^n = x'_n = x_n$ for all $n \geq 1$, so the right side is just $\zeta_x(t)$. The left side is

$$(1 - w_1 t + w_2 t^2 - w_3 t^3 + \cdots)^{-1}.$$

This has R-coefficients iff each w_n is in R, as desired. $\square$

Proof of sufficiency in Theorem 2.15. It suffices to show that $\{x_n := \mathrm{Tr}_{\mathbb{Q}(\theta)/\theta}(\theta^n)\}$ is a Gauss sequence for any algebraic element $\theta \neq 0$. Let $f(t) \in \mathbb{Q}[t]$ be the minimal polynomial of $1/\theta$, normalized so that $f(0) = 1$. Then the ordinary generating function of $\{x_n\}$ is $F_x(t) = \sum_{n=1}^{\infty} x_n t^n = -tf'(t)/f(t)$, so the zeta function is the formal power series $\zeta_x(t) = \exp(\int \mathrm{d}t\ F_x(t)/t) = f(t)^{-1}$. This has coefficients in $\mathbb{Z}_p$ for any p such that the coefficients of $f(t)$ are p-adically integral. Applying Proposition 7.2 to these p-adic rings completes the proof. $\square$

References

[1] William Adams and Daniel Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), no. 159, 255–300, DOI 10.2307/2007637. MR658231 (84c:10007)

[2] B. Amend, *FoxTrot comic strip*, 2005, http://www.gocomics.com/foxtrot/2005/10/11.

[3] Neil Berry, Artūras Dubickas, Noam D. Elkies, Bjorn Poonen, and Chris Smyth, *The conjugate dimension of algebraic numbers*, Q. J. Math. **55** (2004), no. 3, 237–252, DOI 10.1093/qjmath/55.3.237. MR2082091 (2005h:11238)

[4] A. Dold, *Fixed point indices of iterated maps*, Invent. Math. **74** (1983), no. 3, 419–435, DOI 10.1007/BF01394243. MR724012 (85c:54077)

[5] E. Escott, *Reply to query 1484*, L'Intermédiaire des Math. **8** (1901), 63–64.

[6] ———, *Solution to problem 151*, Amer. Math. Monthly **15** (1908), no. 10, 187.

[7] Mihaly Bencze, Dan Saracino, Allen Stenger, S. Amghibech, J. Anglesio, R. Bauer, A. Siegel, D. M. Bloom, G. L. Body, D. Callan, R. J. Chapman, K. Ford, S. M. Gagola, N. Gauthier, W. V. Grounds, T. Hagedorn, R. T. Koether, N. Komanda, R. N. Krishnan, K.-W. Lau, J. H. Lindsey II, L. E. Mattics, C. A. Minh, H. N. Ozsoylev, C. Y. Yildirim, P. G. Poonacha, N. R. Sanjeev, C. Popescu, J. Robertson, H.-J. Sieffert, J. O. Shallit, N C. Singer, A. Stadler, D. C. Terr, T. V. Triff, T. Trimble, P. Trojovsky, Anchorage Math Solutions Group, GCHQ Problems Group, and NSA Problems Group, *Problems and Solutions: Solutions: A Recurrence Generating Multiples of Primes: 10655*, Amer. Math. Monthly **107** (2000), no. 3, 281–282, DOI 10.2307/2589334. MR1543639

[8] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003. MR1990179 (2004c:11015)

[9] Irving Gerst and John Brillhart, *On the prime divisors of polynomials*, Amer. Math. Monthly **78** (1971), 250–266. MR0279071 (43 #4797)

[10] Frank S. Gillespie, *A generalization of Fermat's little theorem*, Fibonacci Quart. **27** (1989), no. 2, 109–115. MR995558 (90e:11006)

[11] Kurt Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements*, Manuscripta Math. **39** (1982), no. 1, 81–97, DOI 10.1007/BF01312446. MR672402 (84d:12008)

[12] Kurt Girstmair, *Linear relations between roots of polynomials*, Acta Arith. **89** (1999), no. 1, 53–96. MR1692195 (2000e:12005)

[13] Jon Grantham, *There are infinitely many Perrin pseudoprimes*, J. Number Theory **130** (2010), no. 5, 1117–1128, DOI 10.1016/j.jnt.2009.11.008. MR2607304 (2011d:11290)

[14] H. W. Lenstra Jr. and P. Stevenhagen, *Primes of degree one and algebraic cases of Čebotarev's theorem*, Enseign. Math. (2) **37** (1991), no. 1-2, 17–30. MR1115741 (92f:11162)

[15] P. Stevenhagen and H. W. Lenstra Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37, DOI 10.1007/BF03027290. MR1395088 (97e:11144)

[16] G. Minton, *Three approaches to a sequence problem*, Math. Mag. **84** (2011), no. 1, 33–37.

[17] *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org, 2012.

[18] Yash Puri and Thomas Ward, *A dynamical property unique to the Lucas sequence*, Fibonacci Quart. **39** (2001), no. 5, 398–402. MR1866354 (2002j:37020)

[19] A. Schinzel, *Reducibility of lacunary polynomials. VIII*, Acta Arith. **50** (1988), no. 1, 91–106. MR945276 (89f:11144)

[20] C. J. Smyth, *A coloring proof of a generalisation of Fermat's little theorem*, Amer. Math. Monthly **93** (1986), no. 6, 469–471, DOI 10.2307/2323475. MR843194 (87k:11012)

[21] R. Tudoran, *A well-known sequence*, College Math. J. **31** (2000), no. 3, 223–224.

[22] A. V. Zarelua, *On matrix analogues of Fermat's little theorem* (Russian, with Russian summary), Mat. Zametki **79** (2006), no. 6, 838–853, DOI 10.1007/s11006-006-0090-y; English transl., Math. Notes **79** (2006), no. 5-6, 783–796. MR2261239 (2007g:11004)

[23] A. V. Zarelua, *On congruences for the traces of powers of some matrices* (Russian, with Russian summary), Tr. Mat. Inst. Steklova **263** (2008), no. Geometriya, Topologiya i Matematicheskaya Fizika. I, 85–105, DOI 10.1134/S008154380804007X; English transl., Proc. Steklov Inst. Math. **263** (2008), no. 1, 78–98. MR2599373 (2011a:11004)

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139

Current address: Microsoft Research New England, One Memorial Drive, Cambridge, Massachusetts 02142

E-mail address: gminton@alum.mit.edu