Rend. Sem. Mat. Univ. Politec. Torino
Vol. 68, 4 (2010), 305 – 318

T. Boggio and A. Mori

POWER MULTIPLES IN BINARY RECURRENCE SEQUENCES: AN APPROACH BY CONGRUENCES

Abstract. We introduce an elementary congruence-based procedure to look for q-th power multiples in arbitrary binary recurrence sequences ($q \geq 3$). The procedure allows one to prove that no such multiples exist in many instances.

1. Introduction and result

Let $u, v, A, B \in \mathbb{Z}$. The ($\mathbb{Z}$-valued) binary recurrence sequence with initial values u, v and coefficients A, B is the sequence $\{G_n\}_{n\geq 0}$ defined recursively as

$$G_0 = u, \quad G_1 = v, \quad G_{n+2} = AG_{n+1} + BG_n \text{ for all } n \geq 0. \tag{1}$$

The discriminant of the sequence (1) is the integer $\Delta = A^2 + 4B \neq 0$. An equivalent description is

$$\begin{pmatrix} G_{n+2} \\ G_{n+1} \end{pmatrix} \begin{pmatrix} A & B \\ 1 & 0 \end{pmatrix} \begin{pmatrix} G_{n+1} \\ G_n \end{pmatrix}, \tag{2}$$

i.e. $\begin{pmatrix} G_{n+1} \\ G_n \end{pmatrix} = \begin{pmatrix} A & B \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} G_1 \\ G_0 \end{pmatrix}$, for all $n \geq 0$. Let K be the smallest extension of $\mathbb{Q}$ containing the eigenvalues $\{\lambda_1, \lambda_2\}$ of the matrix $\begin{pmatrix} A & B \\ 1 & 0 \end{pmatrix}$ and denote by $\mathcal{O}_K$ its ring of integers. Either $K = \mathbb{Q}$ or K is quadratic, $K = \mathbb{Q}(\sqrt{\Delta})$, and in the latter case write $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$. The sequence (1) is called non-degenerate if λ_1/λ_2 is not a root of 1. Also, if $\lambda_1 \neq \lambda_2$ the sequence is a generalized power sum with constant coefficients, namely

$$G_n = g_1\lambda_1^n + g_2\lambda_2^n, \qquad \text{where } g_1 = \frac{G_1 - \lambda_2 G_0}{\lambda_1 - \lambda_2}, \;\; g_2 = \frac{\lambda_1 G_0 - G_1}{\lambda_1 - \lambda_2}.$$

A sequence with values in $\mathbb{Z}$ can be “followed” looking for integers with special interesting arithmetic properties (Ribenboim [6] likens this to picking wild flowers during a walk in the countryside). In this note we deal with the equation

$$G_n = kx^q \tag{3}$$

where $0 \neq k \in \mathbb{Z}$ is a fixed constant and $q \geq 3$. As usual, we may and shall assume that q is a prime number.

By relating it to Baker’s theory of linear forms in logarithms, Pethö [5] and Shorey and Stewart [7] proved independently that (3) has, under some mild conditions on the sequence, only finitely many solutions (n, G_n, x, q). Pethö’s precise version of the result is the following.

THEOREM 1. *Let $\{G_n\}$ be a binary recurrence sequence with coprime non-zero coefficients A and B such that $(G_0, G_1) \neq (0,0)$, $A^2 \neq -jB$ for $j \in \{1,2,3,4\}$ and $G_1^2 - AG_0G_1 - BG_0^2 \neq 0$. Let $\mathcal{P}$ be a finite set of primes and let $\mathcal{S}$ be the set of integers divisible only by primes in $\mathcal{P}$. Then, there exists an effective constant $C = C(A, B, G_0, G_1, \mathcal{P})$ such that if $G_n = kx^q$ with $k \in \mathcal{S}$ and $|x| > 1$ then* $\max(n, |G_n|, |x|, q) < C$.

REMARK 1. When the sequence $\{G_n\}$ is non-degenerate and k is any fixed integer, the finiteness of the number of solutions of $G_n = k$ (i.e. the x-trivial solutions of (3)) follows from the Skolem–Mahler–Lech theorem, [4, §2.1], which is independent of Baker's theory.

Although theorem 1 reduces in principle the problem of finding all the solutions of (3) to a finite amount of computations, from a practical point of view the possibility of using brute force is illusory since the constant C is huge. Following the steps of the proof of theorem 1 in the arguably simplest case of the Fibonacci sequence $\{F_n\}$ (obtained for $u = 0$, $v = 1$, $A = B = 1$) the first author [1] found that for a solution of (3) with $k = 1$ the bounds are $q \leq 192^{1203}$, and $|x| \leq e^{5^{80(4q!+1)(4q!+5)}/4q!}$. Even for a single sequence $\{G_n\}$, the problem of finding a complete solution of (3) may be far from trivial. For instance, it had been known for a while that the only squares and cubes in the Fibonacci sequence are $\{F_0 = 0, F_1 = 1, F_2 = 1, F_{12} = 144\}$ and $\{F_0 = 0, F_1 = 1, F_2 = 1, F_6 = 8\}$ respectively, but to prove that those are the only powers, Bugeaud, Mignotte and Siksek [3] had to combine the classical approach with modular methods similar to those used by Wiles to prove Fermat's last theorem.

Let us fix the exponent q. We present an elementary procedure, introduced in [1], to approximate the solutions of (3) in the following sense. The procedure outputs a large integer $N = N_q$ and a relatively small set $\mathcal{I} \subset \mathbb{Z}/N\mathbb{Z}$ such that if G_n solves (3) then $\overline{n} = n \bmod N \in \mathcal{I}$. The actual computations show that the procedure "converges" rather quickly and in many cases yields $\mathcal{I} = \emptyset$ showing the absence of solutions for the corresponding equation.

The procedure is explained in section 2 followed by some heuristics in section 3. We do not address the question of estimating the expected computational complexity of the procedure which does not seem to be straightforward.

A final section gives a few examples of actual computations. We test all non-trivial sequences $\{G_n\}$ with parameters $A = B = 1$, and non-negative initial values G_0 and G_1 with $\min\{G_0, G_1\} \geq 2$ and $\max\{G_0, G_1\} \leq 9$ up to shift-equivalence (see definition 1). There are two tables. Table 1 shows the result of running the procedure in search of q-powers, for $q \in \{3,5,7,11,13,17\}$. Table 2 lists the values of k for which (3) with $q = 3$ or $q = 5$ has no solutions for $2 \leq k \leq 30$ and q-power free. In particular, the following result remains proved.

THEOREM 2. *Let $\{G_n\}$ be a binary recurrence sequence with $A = B = 1$. The equation $G_n = kx^q$ has no solutions in all cases labelled $\varnothing$ in Table 1 and for all values (q, k) listed in Table 2 below.*

More extensive tables of data are included in the preliminary version [2] posted on the arXiv.

An analysis of table 1 in the text (and of tables 1–6 in [2]) shows that in many cases, up to replacing N by a large divisor, the set $\mathcal{J}$ consists of just one element, so that up to shift-equivalence we may assume that $\mathcal{J} = \{\overline{0}\}$. The following question arises naturally. Suppose that there is a (large) integer N such that a solution of $G_n = kx^q$ can occur only for $n \equiv 0 \bmod N$. Can we obtain further information on the set of solutions from arithmetic properties of the triple (k,q,N)? In particular, can we deduce the finiteness of the number of solutions independently of Baker's theory?

2. The procedure

We shall assume that $AB \neq 0$. The binary recurrence sequence (1) extends uniquely to a function $\mathbb{Z} \to \mathbb{Z}[1/B]$ in such a way that the recurrence relation $G_{n+2} = AG_{n+1} + BG_n$ remains valid for all $n \in \mathbb{Z}$. Namely, set inductively

$$G_{-n} = -\frac{A}{B}G_{-n+1} + \frac{1}{B}G_{-n+2} \qquad \text{for all } n > 0.$$

DEFINITION 1. *Two extended binary recurrence sequences $\{G_n\}_{n\in\mathbb{Z}}$, $\{G'_n\}_{n\in\mathbb{Z}}$ are called shift-equivalent if there exists $k \in \mathbb{Z}$ such that $G'_n = G_{n+k}$ for all $n \in \mathbb{Z}$.*

PROPOSITION 1. (i) *Two sequences not of the form $\{g\mu^n\}$ are shift-equivalent if and only if they share four equal consecutive terms.*

(ii) *The sequences $\{g\mu^n\}$ and $\{G_n\}$ are shift-equivalent if and only if $G_n = g'\mu^n$ with $g' = g\mu^k$ for some $k \in \mathbb{Z}$.*

Proof. The sequences $\{G_n\}_{n\in\mathbb{Z}}$ and $\{G'_n\}_{n\in\mathbb{Z}}$ with same parameters A and B are shift-equivalent if and only if they have a common segment of length 2, $G'_r = G_s$ and $G'_{r+1} = G_{s+1}$ for some r, $s \in \mathbb{Z}$. When $G_k^2 \neq AG_kG_{k-1} + BG_{k-1}^2$ for some (or, equivalently, all) $k \in \mathbb{Z}$ the parameters A and B can be recovered from the consecutive terms $G_{k-1}, \cdots, G_{k+2}$ by solving the linear equations

$$\begin{cases} G_{k+2} &= AG_{k+1} + BG_k \\ G_{k+1} &= AG_k + BG_{k-1} \end{cases}$$

This proves part 1 once we observe that the sequences of the form $\{g\mu^n\}$ are precisely those for which $G_k^2 = AG_kG_{k-1} + BG_{k-1}^2$. Part 2 is immediate. □

The previous fact remains true for R-valued sequences, where R is any domain of characteristic prime to B.

DEFINITION 2. *Let ℓ be a prime number, $(\ell, B) = 1$. The reduction modulo ℓ of the $\mathbb{Z}$-valued binary recurrence sequence* (1) *is the sequence $\{\overline{G}_n\}$ where $\overline{G}_n \in \mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$ is the class of G_n.*

The reduced sequence $\{\overline{G}_n\}$ is an $\mathbb{F}_\ell$-valued binary recurrence sequence with parameters $\overline{A}$ and $\overline{B} \neq 0$ and initial values $\overline{u}$, $\overline{v}$. Its extension $\{\overline{G}_n\}_{n\in\mathbb{Z}}$ is the reduction modulo ℓ of the extension $\{G_n\}$. The following very simple fact is the basis of the procedure.

PROPOSITION 2. *Let $\{\overline{G}_n\}$ be an extended $\mathbb{F}_\ell$-valued binary recurrence sequence. Then $\{\overline{G}_n\}$ is periodic.*

Proof. Since there are only a finite number of pairs $(a,b) \in \mathbb{F}_\ell \times \mathbb{F}_\ell$, there must be integers $r \neq s$ such that $\overline{G}_r = \overline{G}_s$ and $\overline{G}_{r+1} = \overline{G}_{s+1}$. If $0 \neq k = s-r$, an obvious induction shows that the sequences $\{\overline{G}_n\}$ and $\{\overline{G}_{n+k}\}$ coincide. □

DEFINITION 3. *For a prime number ℓ, let π_ℓ be the minimal period of the extended $\mathbb{F}_\ell$-valued reduced sequence $\{\overline{G}_n\}$, i.e.*

$$\pi_\ell = \min\left\{k \in \mathbb{Z}^{>0} \text{ such that } \overline{G}_{n+k} = \overline{G}_n \text{ for all } n \in \mathbb{Z}\right\}.$$

PROPOSITION 3. *Let ℓ be a prime number. The period π_ℓ is a divisor of*

(i) $\ell(\ell-1)$, *if $\Delta = 0$ or if Δ is not a square in $\mathbb{Z}$ with $\ell \mid \Delta$;*

(ii) $\ell-1$, *if Δ is a non-zero square or if $\left(\frac{\Delta}{\ell}\right) = 1$;*

(iii) ℓ^2-1, *if Δ is not a square and $\left(\frac{\Delta}{\ell}\right) = -1$.*

Proof. From the description (2), the period π_ℓ is the order of the cyclic quotient group $\langle\overline{M}\rangle/\langle\overline{M}\rangle \cap S_{\overline{u},\overline{v}}$ where $\overline{M} \in \mathrm{GL}_2(\mathbb{F}_\ell)$ is the reduction modulo ℓ of $M = \left(\begin{smallmatrix} A & B \\ 1 & 0 \end{smallmatrix}\right)$ and $S_{\overline{u},\overline{v}}$ is the stabilizer of the vector $\left(\begin{smallmatrix} \overline{u} \\ \overline{v} \end{smallmatrix}\right)$ under the tautological action of $\mathrm{GL}_2(\mathbb{F}_\ell)$ on $(\mathbb{F}_\ell)^2$. Thus $\pi_\ell \mid \mathrm{ord}(\overline{M})$.

If $\Delta = 0$ then $K = \mathbb{Q}$, $\lambda_1 = \lambda_2 = \lambda \in \mathbb{Z}$ and $M \sim \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$, whose order modulo ℓ is $\ell(\ell-1)$.

If $\Delta \neq 0$ the eigenvalues are different, so $M \sim \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ with $\lambda_1, \lambda_2 \in \mathbb{Q}$ if Δ is a square or $\lambda_2 = \lambda_1^\tau$ otherwise. Hence $\mathrm{ord}(\overline{M})$ is the least common divisors of the orders of $\overline{\lambda}_1$ and $\overline{\lambda}_2$ as elements of $(\mathcal{O}_K/\ell\mathcal{O}_K)^\times$. Thus the other cases follow recalling that

$$(\mathcal{O}_K/\ell\mathcal{O}_K)^\times \simeq \begin{cases} \mathbb{F}_\ell^\times & \text{if } K = \mathbb{Q}, \\ \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times & \text{if } K \text{ quadratic and } \ell \text{ split}, \\ \mathbb{F}_{\ell^2}^\times & \text{if } K \text{ quadratic and } \ell \text{ inert}, \\ (\mathbb{F}_\ell[X]/(X^2))^\times & \text{if } K \text{ quadratic and } \ell \text{ ramified}. \end{cases}$$

□

The procedure goes as follows.

Step 1: Input the defining data (u, v, A, B), the equation data (k, q) and fix a cutoff value $C_{\text{off}} > 0$.

Step 2: Consider the primes $\ell_1 < \cdots < \ell_r \le C_{\text{off}}$ satisfying the following three conditions:

(i) ℓ_i does not divide Bk for all $i = 1, \ldots, r$;

(ii) $\ell_i \equiv 1 \bmod q$ for all $i = 1, \ldots, r$;

(iii) if we set $n_1 = \pi_{\ell_1}$ and define n_{i+1} for $i = 1, \ldots r-1$ inductively as $n_{i+1} = \operatorname{lcm}(n_i, \pi_{\ell_{i+1}})$, then $n_{i+1}/n_i < q$ for all $i = 1, 2, \ldots r-1$.

Step 3: Construct inductively sets $\mathcal{I}_i \subset \mathbb{Z}/n_i\mathbb{Z}$ as follows:

(i) $\mathcal{I}_1 = \{\overline{n} \in \mathbb{Z}/n_1\mathbb{Z}$ such that $\overline{G}_n/\overline{k} \in (\mathbb{F}_{\ell_1})^q\}$;

(ii) for $i = 1, 2, \ldots r-1$, given $\mathcal{I}_i$ first set

$$\mathcal{I}_{i+1}^{\sharp} = \{\overline{n} \in \mathbb{Z}/n_{i+1}\mathbb{Z} \text{ such that } n \bmod n_i \in \mathcal{I}_i\}$$

and then let

$$\mathcal{I}_{i+1} = \mathcal{I}_{i+1}^{\sharp} - \{\overline{n} \text{ such that } \overline{G}_n/\overline{k} \notin (\mathbb{F}_{\ell_{i+1}})^q\}.$$

Step 4: If $\mathcal{I}_{r'} = \emptyset$ for some $r' \le r$ the procedure stops, else let $N = n_r$ and output $\mathcal{I} = \mathcal{I}_r \subset \mathbb{Z}/N\mathbb{Z}$.

The reason for the conditions on the primes ℓ_i is the following. The subgroup $(\mathbb{F}_\ell^\times)^q$ of q-powers in the multiplicative group $\mathbb{F}_\ell^\times$ is proper if and only if $q \mid \ell - 1$, and in this case consists of $(\ell-1)/q$ elements. Thus, the number of q-powers in $\mathbb{F}_\ell$ is $(q+\ell-1)/q$ and on average we can expect that at each step

$$|\mathcal{I}_{i+1}| \cong \frac{q + \ell_{i+1} - 1}{q\ell_{i+1}} \left|\mathcal{I}_{i+1}^{\sharp}\right|.$$

Since $|\mathcal{I}_{i+1}^{\sharp}| = (n_{i+1}/n_i)|\mathcal{I}_i|$, by forcing $n_{i+1}/n_i \le q-1$ and observing that

$$\lim_{i\to\infty} \frac{q+\ell_i-1}{q\ell_i}(q-1) < 1,$$

we can expect that eventually $|\mathcal{I}_{i+1}| < |\mathcal{I}_i|$ on average, so that the procedure should eventually produce an empty set of indices when the equation (3) has no solutions.

REMARK 2. The necessity of imposing condition 3 in Step 2 makes the procedure unsuited for the case $q = 2$.

3. Heuristic density estimates

The support of $n \in \mathbb{Z}$ is the set $\mathrm{Supp}(n) = \{p \text{ prime such that } p \mid n\}$. Fix an integer $m \geq 2$ and let $\mathcal{P}_m = \{\ell \text{ prime such that } \max(\mathrm{Supp}(\pi_\ell)) \leq m\}$ and

$$\mathcal{P}'_m = \{\ell \text{ prime such that } \max(\mathrm{Supp}(\mathrm{ord}_\ell(\overline{M}))) \leq m\}.$$

Also, let $\mathcal{P}_{m,q} = \{\ell \in \mathcal{P}_m \text{ such that } \ell \equiv 1 \bmod q\}$ and

$$\mathcal{P}'_{m,q} = \{\ell \in \mathcal{P}'_m \text{ such that } \ell \equiv 1 \bmod q\}.$$

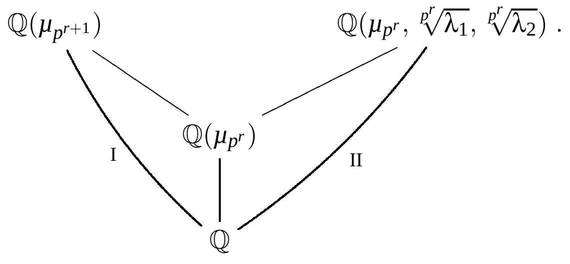
The sets $\mathcal{P}'_m$ and $\mathcal{P}'_{m,q}$ depend on the coefficients A and B, while the sets $\mathcal{P}_m$ and $\mathcal{P}_{m,q}$ depend also on the vector $\vec{v} = \binom{u}{v} \in \mathbb{Z}^2$ of initial values. Since $\pi_\ell \mid \mathrm{ord}_\ell(\overline{M})$, we have that $\mathcal{P}'_m \subseteq \mathcal{P}_m$ and $\mathcal{P}'_{m,q} \subseteq \mathcal{P}_{m,q}$. The primes $\ell_1, \ell_2, \ldots$ of Step 2 are in $\mathcal{P}_{q-1,q}$. We shall show that in the case of a non-degenerate binary recurrence sequence with non-zero initial vector $\vec{v}$, a variation of the classical Artin heuristics, under the usual independence hypotheses, yields that the expected density of the sets $\mathcal{P}_m$, and hence $\mathcal{P}_{m,q}$, is zero.

Let assume first that $K = \mathbb{Q}$ and, for the sake of uniformity of the argument, also that $\min\{|\lambda_1|, |\lambda_2|\} \geq 2$. Let Σ_0 be the finite set of primes containing 2 and the primes dividing $\lambda_1\lambda_2$. Consider a prime $\ell \notin \Sigma_0$ and write $\ell - 1 = ab$ where $\max\{\mathrm{Supp}(a)\} \leq m$ and $\min\{\mathrm{Supp}(b)\} > m$. Then $(\overline{\lambda}_1, \overline{\lambda}_2) \in \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$ and

$$\begin{aligned} \max(\mathrm{Supp}(\mathrm{ord}_\ell(\overline{M}))) \leq m \quad &\Longleftrightarrow \quad \overline{\lambda}_1 \text{ and } \overline{\lambda}_2 \text{ are } b\text{-powers in } \mathbb{F}_\ell^\times \\ &\Longleftrightarrow \quad \begin{array}{c} \overline{\lambda}_1 \text{ and } \overline{\lambda}_2 \text{ are } p^r\text{-powers in } \mathbb{F}_\ell^\times \text{ for} \\ \text{all primes } p > m \text{ such that } p^r \mid\mid \ell - 1. \end{array} \end{aligned}$$

Since the primes $\ell \equiv 1 \bmod p^r$ are precisely those that split completely in the cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\mu_{p^r})$, we can rephrase the last condition in terms of the extensions in the diagram

(4)



Namely, $\overline{\lambda}_1$ and $\overline{\lambda}_2$ are in $(\mathbb{F}_\ell^\times)^{p^r}$ and $p^r \mid\mid \ell - 1$ if and only if $\ell \in \Sigma'_{p,r}$, where $\Sigma'_{p,r} = \{\text{primes } \ell \text{ that split completely in II and do not split completely in I}\}$. By construction, $\Sigma'_{p,r} \cap \Sigma'_{p,r'}$ if $r \neq r'$, and if we let $\Sigma'_p = \cup_{r \geq 1} \Sigma'_{p,r}$ then

$$\mathcal{P}'_m = \bigcap_{p > m} \Sigma'_p. \tag{5}$$

The following proposition is a straightforward application of Kummer's theory to the situation of diagram (4).

PROPOSITION 4. *Suppose $p \notin \Sigma_0$. Then:*

(i) $[\mathbb{Q}(\mu_{p^r}, \sqrt[p^r]{\lambda_i}) : \mathbb{Q}(\mu_{p^r})] = p^r$ *for* $i = 1, 2$*;*

(ii) $\mathbb{Q}(\mu_{p^r}, \sqrt[p^r]{\lambda_1}) \cap \mathbb{Q}(\mu_{p^r}, \sqrt[p^r]{\lambda_2}) = \mathbb{Q}(\mu_{p^r})$*;*

(iii) $\mathrm{Gal}(\mathbb{Q}(\mu_{p^r}, \sqrt[p^r]{\lambda_1}, \sqrt[p^r]{\lambda_2})/\mathbb{Q}(\mu_{p^r})) \simeq (\mathbb{Z}/p^r\mathbb{Z})^2$*;*

(iv) $\mathbb{Q}(\mu_{p^{r+1}}) \cap \mathbb{Q}(\mu_{p^r}, \sqrt[p^r]{\lambda_1}, \sqrt[p^r]{\lambda_2}) = \mathbb{Q}(\mu_{p^r})$.

In particular, for $p \notin \Sigma_0$ point 4 says that $\Sigma'_{p,r} \neq \emptyset$ and by Čebotarev's theorem the expected density of $\Sigma'_{p,r}$ is

$$\begin{aligned}\delta(\Sigma'_{p,r}) &= \left(1 - \frac{1}{[\mathbb{Q}(\mu_{p^{r+1}}) : \mathbb{Q}(\mu_{p^r})]}\right) \frac{1}{[\mathbb{Q}(\mu_{p^r}, \sqrt[p^r]{\lambda_1}, \sqrt[p^r]{\lambda_2}) : \mathbb{Q}]} \\ &= \frac{p-1}{p} \frac{1}{p^{3r-1}(p-1)} = \frac{1}{p^{3r}}\end{aligned}$$

so that $\delta(\Sigma'_p) = \sum_{r\geq 1} p^{-3r} = 1/(p^3-1)$. Applying the independence assumption to (5) yields the expected value

$$\delta(\mathcal{P}'_m) = \prod_{\substack{p>m \\ p\in\Sigma_0}} \delta(\Sigma'_p) \prod_{\substack{p>m \\ p\notin\Sigma_0}} \frac{1}{p^3-1} = 0.$$

Let $\ell \in \mathcal{P}_m - \mathcal{P}'_m$, $\ell \notin \Sigma_0$. Then $M^{\pi_\ell} \not\equiv I \bmod \ell$ and yet

$$M^{\pi_\ell}\vec{v} \equiv \vec{v} \bmod \ell. \tag{6}$$

In order for this to be possible, the matrix $M^{\pi_\ell} \bmod \ell$ must admit 1 as an eigenvalue. Thus a prime $\ell \notin \Sigma_0$ is in $\mathcal{P}_m - \mathcal{P}'_m$ if and only if the following two conditions are satisfied.

C1. Exactly one of the eigenvalues λ_1, λ_2 is a b-power in $\mathbb{F}_\ell^\times$. Equivalently, exactly one of the eigenvalues λ_1, λ_2 is a p^r-power in $\mathbb{F}_\ell^\times$ for all $p^r \mid\mid \ell - 1$ with $p > m$.

C2. If λ is the eigenvalue of condition C1, then $\vec{v} \bmod \ell \in E_\lambda$ where $E_\lambda \subset (\mathbb{Z}/\ell\mathbb{Z})^2$ is the λ-eigenspace of $M \bmod \ell$.

Denote $\mathcal{P}_m^\flat$ the set of primes satisfying condition C1 only. As above $\mathcal{P}_m^\flat = \bigcap_{p>m} \Sigma_p$ where $\Sigma_p = \bigcup_{r\geq 1} \Sigma_{p,r}$ is a disjoint union with

$$\Sigma_{p,r} = \left\{ \begin{array}{c} \ell \text{ that split completely in one extension } \mathbb{Q} \subset \mathbb{Q}(\mu_{p^r}, \sqrt[p^r]{\lambda_j}), \\ j = 1, 2, \text{ but not in both or in I of diagram 4} \end{array} \right\}.$$

Given $T > 0$, let $\binom{0}{0} \notin \mathcal{V}_T \subset \mathbb{Z}^2$ be a finite set such that the restriction of the product of quotient maps

$$\mathcal{V}_T \longrightarrow \prod_{\substack{\ell \leq T \\ \ell \in \mathcal{P}_m^\flat}} (\mathbb{Z}/\ell\mathbb{Z})^2$$

is a bijection and $\mathcal{V}_T \subseteq \mathcal{V}_{T'}$ for $T \leq T'$. Then, denoting (as usual) $\pi(T)$ the number of primes less than T and making explicit the dependence of $\mathcal{P}_m$ on the initial vector,

$$\delta_T := \frac{1}{|\mathcal{V}_T|} \sum_{\vec{v} \in \mathcal{V}_T} \frac{|\{\ell \in \mathcal{P}(\vec{v})_m \text{ such that } \ell \leq T\}|}{\pi(T)} = \frac{1}{\pi(T)} \sum_{\substack{\ell \leq T \\ \ell \in \mathcal{P}_m^\flat}} \frac{1}{\ell}$$

because $|E_\lambda| = \ell$. Thus, $\delta = \lim_{T\to\infty} \delta_T$ is the average density of the sets $\mathcal{P}(\vec{v})_m$ for $\vec{v} \in \bigcup_T \mathcal{V}_T$. On the other hand, $\delta_T < \pi(T)^{-1} \sum_{n=1}^T 1/n$ and the well-known asymptotics $\pi(T) \sim T \log(T)^{-1}$ and $\sum_{n=1}^T 1/n \sim \log(T)$ yield $\delta = 0$. Since the set $\mathcal{V}_T$ can be constructed so to contain any given $0 \neq \vec{v} \in \mathbb{Z}^2$, we get an estimated density

$$\delta(\mathcal{P}(\vec{v})_m) = 0, \text{ for all } \vec{v} \neq 0, \qquad \text{if } K = \mathbb{Q}.$$

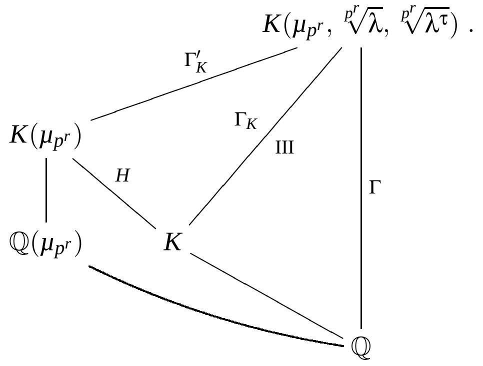
Let us assume now that K is quadratic and let $\lambda = \lambda_1$. Note that non-degeneracy is equivalent to the subgroup $\langle \lambda, \lambda^\tau \rangle < K^\times$ being free of rank 2. This time let Σ_0 be the finite set of primes containing 2, the primes dividing $\mathrm{N}_{K/\mathbb{Q}}(\lambda)$, the primes such that $K \subset \mathbb{Q}(\mu_{\ell^\infty})$ and the primes that are ramified in K. Let $\ell \notin \Sigma_0$. If ℓ is split in K, then $\overline{\lambda} \in (\mathcal{O}_K/\ell\mathcal{O}_K)^\times \simeq \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$. The situation is very similar to the case $K = \mathbb{Q}$ and we omit the details.

If ℓ is inert in K, then $\overline{\lambda} \in (\mathcal{O}_K/\ell\mathcal{O}_K)^\times \simeq \mathbb{F}_{\ell^2}^\times$. Let us write $\ell^2 - 1 = ab$ where $\max\{\mathrm{Supp}(a)\} \leq m$ and $\min\{\mathrm{Supp}(b)\} > m$. Then

$$\begin{aligned} \max(\mathrm{Supp}(\mathrm{ord}_\ell(\overline{M}))) \leq m \quad &\iff \quad \overline{\lambda} \text{ is a } b\text{-power in } \mathbb{F}_{\ell^2}^\times \\ &\iff \quad \begin{array}{c} \overline{\lambda} \text{ is a } p^r\text{-powers in } \mathbb{F}_{\ell^2}^\times \text{ for all} \\ \text{primes } p > m \text{ such that } p^r \mid\mid \ell^2 - 1. \end{array} \end{aligned}$$

Let $\Sigma'_{p,r}$ be the set of primes satisfying the latter condition at p. Consider the diagram of Galois extensions

(7)



Then

$$\Sigma'_{p,r} = \{\text{primes } \ell \text{ that split completely in III and such that } \ell \not\equiv \pm 1 \bmod p^{r+1}\}.$$

Again, $\Sigma'_{p,r} \cap \Sigma'_{p,r'} = \emptyset$ if $r \neq r'$ and if we let $\Sigma'_p = \cup_{r\geq 1}\Sigma'_{p,r}$, then

$$\widetilde{\mathcal{P}}'_m = \{\ell \in \mathcal{P}'_m \text{ such that } \ell \text{ is inert in } K\} = \bigcap_{p>m} \Sigma'_p. \tag{8}$$

The analogue of proposition 4 is the following

PROPOSITION 5. *Suppose $p \notin \Sigma_0$ and λ/λ^τ not a root of 1. Then:*

(i) $[K(\mu_{p^r}, \sqrt[p^r]{\lambda}) : K(\mu_{p^r})] = [K(\mu_{p^r}, \sqrt[p^r]{\lambda^\tau}) : K(\mu_{p^r})] = p^r$;

(ii) $K(\mu_{p^r}, \sqrt[p^r]{\lambda}) \cap K(\mu_{p^r}, \sqrt[p^r]{\lambda^\tau}) = K(\mu_{p^r})$;

(iii) $\mathrm{Gal}(K(\mu_{p^r}, \sqrt[p^r]{\lambda}, \sqrt[p^r]{\lambda^\tau})/K(\mu_{p^r})) \simeq (\mathbb{Z}/p^r\mathbb{Z})^2$;

(iv) $\mathbb{Q}(\mu_{p^{r+1}}) \cap K(\mu_{p^r}, \sqrt[p^r]{\lambda}, \sqrt[p^r]{\lambda^\tau}) = \mathbb{Q}(\mu_{p^r})$.

To estimate the density of the primes in $\Sigma'_{p,r}$, observe that an inert prime ℓ splits completely in the extension (III) of diagram (7) if and only if a Frobenius element $\sigma \in \mathrm{Frob}_{K(\mu_{p^r}, \sqrt[p^r]{\lambda}, \sqrt[p^r]{\lambda^\tau})/K}(\ell) \subset \Gamma$ satisfies the following conditions:

$$\sigma^2 = \mathrm{id} \qquad \text{and} \qquad \sigma_{|K} = \tau.$$

These conditions define a conjugacy class $C \subset \Gamma$ and by Čebotarev's theorem we need to estimate its size. The exact sequences of Galois groups

$$1 \longrightarrow \Gamma_K \longrightarrow \Gamma \longrightarrow \langle\tau\rangle \longrightarrow 1$$

and

$$1 \longrightarrow \Gamma'_K \longrightarrow \Gamma_K \longrightarrow H \longrightarrow 1$$

split, so that $\Gamma \simeq \Gamma_K \ltimes \langle\tau\rangle \simeq (\Gamma'_K \ltimes H) \ltimes \langle\tau\rangle$. The extension $\mathbb{Q} \subset K(\mu_{p^r})$ is abelian with Galois group isomorphic to $G = H \times \langle\tau\rangle$ so that we get $\Gamma \simeq \Gamma'_K \ltimes G$. Since H is cyclic (of even order $p^{r-1}(p-1)$) there are 2 elements of order 2 in G restricting to τ and finally

$$|C| \leq 2|\Gamma'_K| = 2p^{2r}.$$

Combining this estimate with Dirichlet's theorem of primes in arithmetic progression under the independence assumptions we get

$$\delta(\Sigma'_{p,r}) \leq \left(\frac{p-1}{p}\right) \frac{2p^{2r}}{2p^{3r-1}(p-1)} = \frac{1}{p^r}.$$

Thus, $\delta(\Sigma'_p) \leq \sum_{r\geq 1} p^{-r} = 1/(p-1)$ and finally, from (8) and recalling that the inert primes have density $1/2$,

$$\delta(\widetilde{\mathcal{P}}'_m) = \frac{1}{2} \prod_{\substack{p>m \\ p\in\Sigma_0}} \delta(\Sigma'_p) \prod_{\substack{p>m \\ p\notin\Sigma_0}} \frac{1}{p-1} = 0.$$

The analysis of the set $\mathcal{P}_m - \mathcal{P}'_m$ follows the same lines of the $K = \mathbb{Q}$ situation in the case of a split prime ℓ and we, again, omit the details. When ℓ is inert the basically trivial observation that λ is a b-power if and only if $\overline{\lambda}$ is a b-power implies at once that

$$\pi_\ell = \mathrm{ord}_\ell(\overline{M}) \qquad \text{if } \ell \text{ is inert.}$$

In other words, the set $\mathcal{P}_m - \mathcal{P}'_m$ consists only of split primes or primes in Σ_0 and the heuristic estimate

$$\delta(\mathcal{P}(\vec{v})_m) = 0, \text{ for all } \vec{v} \neq 0, \qquad \text{if } K \text{ is quadratic,}$$

follows.

4. Tables

We implemented the procedure using the Maple 12 package and let it run on a MacBook, with a cutoff value $C_{\mathrm{off}} = 10000$.

For reasons of space the tables in this section report only some of these computations: we consider all sequences up to shift-equivalence with parameters $A = B = 1$ and non-negative initial values G_0 and G_1 such that $\min\{G_0, G_1\} \geq 2$ and $\max\{G_0, G_1\} \leq 9$. For more extensive tables the reader may consult the preliminary version [2].

Table 1 gives the results of applying the procedure in search of pure powers for prime exponents q with $3 \leq q \leq 17$. The tables contain 3 types of entries:

(i) $\varnothing$ indicates that the procedure outputs the empty set, i.e. that the corresponding sequence does not contain q-th powers;

(ii) $\{a\}_m$ indicates that the procedure shows that the only q-th powers in the corresponding sequence $\{G_n\}$ can occur only for $n \equiv a \bmod (N_q/m)$;

(iii) m indicates that the procedure final output was a set of m different possible classes modulo N_q for indices n with G_n a q-th power, not coming from the same class modulo a large divisor of N_q.

Table 2 lists the q-power free values $2 \leq k \leq 30$ for which the procedure shows that the equation (3) has no solutions.

TABLE 1
q-powers in sequences with $A = 1$ and $B = 1$

$N_3 = 186624$, $N_5 = 15552000$, $N_7 = 127008000$,
$N_{11} = 3841992000$, $N_{13} = 43286443200$
$N_{17} = 68235175008000$

G_0	G_1	$q = 3$	$q = 5$	$q = 7$	$q = 11$	$q = 13$	$q = 17$
2	5	62	4	4	$\{-2\}_2$	4	4
2	6	24	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
2	7	$\{-3\}_2$	$\varnothing$	$\{-9\}_2$	$\varnothing$	$\varnothing$	$\varnothing$
2	8	$\{1\}_2$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
2	9	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
3	7	30	4	$\{-2\}_2$	4	4	12
3	8	$\{1\}_2$	$\varnothing$	$\{7\}_2$	$\varnothing$	$\varnothing$	$\varnothing$
3	9	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
4	9	4	$\{-2\}_2$	$\{-2\}_4$	8	4	6
6	4	$\{-2\}_2$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
6	5	20	$\{-1\}_2$	$\{-1\}_2$	48	$\{-1\}_2$	12
7	3	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
7	4	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
7	5	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
8	2	68	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
8	3	52	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
8	4	40	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
8	5	52	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
8	6	68	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
8	7	32	$\{-1\}_2$	$\{-1\}_2$	8	4	48
9	2	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
9	3	16	4	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
9	4	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
9	5	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
9	6	16	4	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
9	7	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
9	8	44	16	$\{-1\}_2$	18	4	4

TABLE 2
Values of q-power free constants $2 \leq k \leq 30$ for which the equation $G_n = kx^q$ has no solutions with $A = 1$, $B = 1$, and $q = 3, 5$

G_0	G_1	$q = 3$ $q = 5$
1	3	5, 6, 9, 10, 12–15, 17, 19, 20–23, 26, 30 5, 6, 8–10, 12–15, 16, 17, 19–23, 25–28, 30
1	4	6, 10, 13, 15, 17, 18, 20, 22, 25, 26, 28, 29 6, 8, 10, 11, 13, 15–18, 20–22, 25–30
1	5	9, 12–15, 18–20, 22, 23, 26, 29, 30 2, 8, 9, 12–16, 18–23, 25, 26, 29, 30
1	6	2, 3, 10–12, 15, 17, 18, 23, 25, 26, 30 2, 3, 8, 10, 12, 14–19, 21, 23, 25–30
1	7	3, 4, 9, 10, 12–14, 17, 18, 21, 22, 25, 26, 28–30 2–4, 9, 10, 12–14, 17–22, 25, 26, 28–30
1	8	2, 3, 5, 10–12, 15, 18, 21, 25, 28–30 2–5, 10–12, 14–16, 18, 20–23, 25, 27, 28–30
1	9	4, 5, 11, 13, 14, 17, 18, 20, 21, 23, 25, 26 2, 4–6, 11–14, 16–18, 20, 21, 23, 25–28, 30
2	5	6, 10, 13, 15, 17, 18, 20, 22, 25, 26, 28, 29 6, 8, 10, 11, 13, 15–18, 20–22, 25–30
2	6	3, 5, 9, 10–13, 15, 17, 18, 20, 21, 23, 25, 26, 28–30 3, 5, 7, 9–13, 15–21, 23, 25–27, 28–30
2	7	4, 6, 10, 12, 13–15, 18, 20, 22, 23, 26, 28, 29 6, 10, 12–15, 17, 18, 20–23, 26–29
2	8	5, 7, 9, 11, 12, 17, 19, 20, 23, 25, 26, 29, 30 3, 5, 7, 9, 11–13, 15–17, 19–23, 25–27, 29, 30
2	9	4, 6, 10, 14, 15, 18, 21–23, 25, 26, 28, 30 3, 4, 6, 8, 10, 13–16, 18, 19, 21–23, 25–28, 30
3	7	9, 12–15, 18–20, 22, 23, 26, 29, 30 2, 8, 9, 12–16, 18, 19–23, 25, 26, 29, 30
3	8	4, 6, 10, 12–15, 18, 20, 22, 23, 26, 28, 29 6, 10, 12–15, 17, 18, 20–23, 26–29
3	9	4, 5, 7, 10, 11, 13–15, 17–20, 23, 25, 26, 29, 30 2, 4, 5, 7, 8, 10, 11, 13–20, 22, 23, 25–30
4	9	2, 3, 10–12, 15, 17, 18, 23, 25, 26, 30 2, 3, 8, 10, 12, 14–19, 21, 23, 25–30

continued on the next page

Table 2: Impossible values of k in sequences with $A = 1$, $B = 1$
(continued from the previous page)

G_0	G_1	$q = 3$ $q = 5$
6	4	5, 7, 9, 11, 12, 17, 19, 20, 23, 25, 26, 29, 30 3, 5, 7, 9, 11–13, 15–17, 19–23, 25–27, 29, 30
6	5	3, 4, 9, 10, 12–14, 17, 18, 21, 22, 25, 26, 28–30 2, 4, 3, 9, 10, 12–14, 17–22, 25, 26, 28–30
7	3	2, 6, 9, 12, 14, 17, 18, 20–22, 25, 28–30 2, 5, 6, 8, 9, 12, 14, 16–19, 20–22, 25, 27–30
7	4	2, 6, 9, 12, 14, 17, 18, 20–22, 25, 28–30 2, 5, 6, 8, 9, 12, 14, 16–22, 25, 27–30
7	5	4, 6, 10, 14, 15, 18, 21–23, 25, 26, 28, 30 3, 4, 6, 8, 10, 13–16, 18, 19, 21–23, 25–28, 30
8	2	3, 5, 13, 15, 17–19, 21, 23, 25, 26, 28–30 3–5, 7, 9, 11, 13, 15–19, 21, 23, 25–30
8	3	2, 4, 6, 7, 9, 12, 15, 17, 19–23, 26, 28, 30 4, 6, 7, 9, 10, 12, 15–17, 19, 20–22, 23, 26–30
8	4	3, 5–7, 10, 11, 13, 15, 17–23, 25, 26, 29, 30 2, 3, 5–7, 9–11, 13–15, 17–23, 25–27, 29, 30
8	5	2, 4, 6, 7, 9, 12, 15, 17, 19–23, 26, 28, 30 4, 6, 7, 9, 10, 12, 15–17, 19–23, 26–30
8	6	3, 5, 13, 15, 17–19, 21, 23, 25, 26, 28–30 3–5, 7, 9, 11, 13, 15–19, 21, 23, 25–30
8	7	4, 5, 11, 13, 14, 17, 18, 20, 21, 23, 25, 26 2, 4–6, 11–14, 16–18, 20, 21, 23, 25–28, 30
9	1	2, 5–7, 12, 13, 15, 18–20, 23, 26, 28–30 2–7, 12–16, 18–20, 22, 23, 26–30
9	2	4–6, 10, 12, 14, 15, 17, 20, 25, 26, 28–30 3–6, 8, 10, 12, 14, 15, 17–22, 25–30
9	3	2, 4, 5, 7, 10, 11, 13, 14, 17–20, 22, 23, 25, 26, 28–30 2, 4, 5, 7, 8, 10, 11, 13, 14, 16–20, 22, 23, 25, 26, 28–30
9	4	3, 6, 7, 10–12, 15, 18, 20, 22, 25, 26, 29 2, 3, 6, 7, 8, 10–12, 15, 16, 18, 20–23, 25–29
9	5	3, 6, 7, 10–12, 15, 18, 20, 22, 25, 26, 29 2, 3, 6–8, 10–12, 15, 16, 18, 20–23, 25–29
9	6	2, 4, 5, 7, 10, 11, 13, 14, 17–20, 22, 23, 25, 26, 28–30 2, 4, 5, 7, 8, 10, 11, 13, 14, 16–20, 22, 23, 25, 26, 28–30
9	7	4–6, 10, 12, 14, 15, 17, 20, 25, 26, 28–30 3–6, 8, 10, 12, 14, 15, 17–22, 25–30
9	8	2, 5–7, 12, 13, 15, 18–20, 23, 26, 28–30 2–7, 12–16, 18–22, 23, 26–30

References

[1] BOGGIO T. Multipli di potenze in una relazione ricorsiva binaria. Tesi di Laurea Magistrale, Università di Torino, 2008.

[2] BOGGIO T. AND MORI A. Power multiples in binary recurrence sequences: an approach by congruences. arXiv:1009.5092v1 [math.NT].

[3] BUGEAUD Y., MIGNOTTE M. AND SIKSEK S. Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers. *Annals of Math. 163* (2006), 969–1018.

[4] EVEREST G., VAN DER POORTEN A., SHPARLINSKI I. AND WARD T. *Recurrence Sequences*, vol. 104 of *Math. Surveys and Monographs*. American Math. Society, 2002.

[5] PETHŐ A. Perfect powers in second order linear recurrences. *J. Number Theory 15* (1982), 5–13.

[6] RIBENBOIM P. FFF: Fibonacci: di Fiore in Fiore. *Boll. Unione Mat. Ital. (8) 5-A* (2002), 329–353.

[7] SHOREY T. N. AND STEWART C. L. On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences. *Math. Scand. 52* (1983), 24–36.

AMS Subject Classification: 11B39, 11B50

Teresa BOGGIO, Andrea MORI
Dipartimento di Matematica, Università degli Studi di Torino
Via Carlo Alberto 10, 10123 Torino, ITALIA
e-mail: teresa.boggio@gmail.com, andrea.mori@unito.it

Lavoro pervenuto in redazione il 02.06.2010 e, in forma definitiva, il 29.09.2010