ERGODICITY OF p-ADIC MULTIPLICATIONS AND THE DISTRIBUTION OF FIBONACCI NUMBERS

ZAQUEU COELHO AND WILLIAM PARRY

Dedicated to the memory of V.A. Rokhlin

Abstract. We characterise ergodicity of p-adic multiplication on the units of $\boldsymbol{Z}_p$ where p is an odd prime. We do the same for the subgroup of units of $\boldsymbol{Z}_p(\sqrt{D})$ of norm ± 1, when D is not a square in $\boldsymbol{Z}_p$. These results are then applied to give a complete description of the distribution mod p^k of the Fibonacci numbers.

Introduction

The main direction of research into the distribution mod p^k of linear recurrence sequences seems to lean toward problems associated with uniform distribution (see for instance [Nie, KS, KN, Bum, Nat, Nar, Tur, Ve]). Enquiries into other distributions have not, so far, received the same attention. The purpose of this paper is to consider this more general question in the concrete setting of the Fibonacci sequence. (In this case one has uniform distribution mod p^k only when $p = 5$.) By restricting ourselves to this special case we are able to give a complete characterisation of the asymptotic distribution mod p^k, for all $k > 0$, where p is an odd prime. However, we feel confident that our methods, involving the elementary ergodic theory of p-adic multiplication, will prove to be of use to more general linear recurrence sequences and we expect to return to this question elsewhere.

For an odd prime p we consider the multiplicative group $\boldsymbol{U}$ of units of the ring $\boldsymbol{Z}_p$ of p-adic integers. For each $\lambda \in \boldsymbol{U}$, the map $T_\lambda \colon \boldsymbol{U} \to \boldsymbol{U}$ given by $T_\lambda(x) = \lambda x$ is the restriction of an automorphism of $\boldsymbol{Z}_p$ and as such preserves Haar measure. The following characterises the ergodicity of T_λ.

Theorem 1. *Let $1 \neq \lambda \in \boldsymbol{U}$ then $T_\lambda \colon \boldsymbol{U} \to \boldsymbol{U}$ is ergodic if and only if λ is a primitive root* $\bmod p$ *and $\lambda^{p-1} \not\equiv 1 \pmod{p^2}$. Moreover, all such transformations are isomorphic.*

This is an immediate consequence of the following result which gives a complete description of the ergodic decompositions of all maps T_λ, $\lambda \neq 1$.

Theorem 2. *If λ has order $m \bmod p$ $(m \mid p-1)$ and $\lambda^m = 1 + \mu p^k$ where μ is a unit then T_λ has $p^{k-1}(p-1)/m$ ergodic components. The restriction of T_λ to these components are all isomorphic to the map of $(\boldsymbol{Z}/m\boldsymbol{Z}) \times \boldsymbol{Z}_p$ defined by $(i, x) \mapsto (i + 1$* $\bmod m, x + 1)$.

Date: 27th July 1999.

1991 *Mathematics Subject Classification.* Primary 11B39, 28D05; Secondary 11N69, 11K41.

The first named author acknowledges partial support from the European Science Foundation Programme PRODYN during part of this work.

We take $\boldsymbol{Z}_p$ to be the ring of sums $x = \sum_{n=0}^{\infty} x_n p^n$ $(x_n = 0, 1, \cdots, p-1)$ whose convergence is assured with respect to the p-adic metric. This metric gives the infinite direct product topology on $\{0, 1, \cdots, p-1\}^{\boldsymbol{Z}^+}$ which is compact and zero dimensional. (An element is close to zero when it is divisible by p^N for N large.) The units (invertible elements) of $\boldsymbol{Z}_p$ consist of those $x \in \boldsymbol{Z}_p$ with $x_0 \neq 0$, i.e. $\boldsymbol{U} = \{x\colon\ p \not| \, x\}$. Since one can write $\boldsymbol{Z}_p = \cup_{n=0}^{\infty} p^n \boldsymbol{U} \cup \{0\}$, once we have the ergodic decomposition structure of $T_\lambda\colon \boldsymbol{U} \to \boldsymbol{U}$ we have it for $T_\lambda\colon \boldsymbol{Z}_p \to \boldsymbol{Z}_p$. (The structure is copied on each $p^n \boldsymbol{U}$.)

If $D \in \boldsymbol{U}$ is not a square $\boldsymbol{Z}_p(\sqrt{D}) = \boldsymbol{Z}_p + \sqrt{D}\, \boldsymbol{Z}_p$ is a ring with the obvious addition, multiplication and topology. (Again $x + \sqrt{D}\, y$ is close to zero if both x, y are divisible by a high power of p.) The units $\boldsymbol{U}(\sqrt{D})$ consist of all $x + \sqrt{D}\, y$ with one of x, y a unit of $\boldsymbol{Z}_p$. Since the expression $x + \sqrt{D}\, y$ is unique we can define the norm N by $N(x + \sqrt{D}\, y) = x^2 - D\, y^2$ and this is a homomorphism of $\boldsymbol{U}(\sqrt{D})$ into $\boldsymbol{U}$ with ‘kernel’

$$\boldsymbol{U}^0(\sqrt{D}) \ = \ \left\{ x + \sqrt{D}\, y\colon\ x^2 - D\, y^2 = \pm 1 \right\} .$$

Along with the maps $T_\lambda\colon \boldsymbol{U} \to \boldsymbol{U}$ we shall consider the maps $T_\lambda\colon \boldsymbol{U}^0(\sqrt{D}) \to \boldsymbol{U}^0(\sqrt{D})$ where $\lambda \in \boldsymbol{U}^0(\sqrt{D})$.

The cardinality of $\boldsymbol{U}(\sqrt{D})$ mod p is clearly $p^2 - 1$, whereas the order of $\boldsymbol{U}^0(\sqrt{D})$ mod p is $2(p+1)$. To see this we note that each element of $\boldsymbol{F}_p^\times$ is the mod p norm of some element of $\boldsymbol{U}(\sqrt{D})$ and it is not difficult to see there is a one-one correspondence between $\{x \in \boldsymbol{U}(\sqrt{D}) \bmod p\colon\ N(x) = k\}$ and $\{x \in \boldsymbol{U}(\sqrt{D})\colon\ N(x) = 1\}$. For this reason each of these sets has cardinality $(p^2-1)/(p-1) = p+1$, and therefore $\boldsymbol{U}^0(\sqrt{D})$ has order $2(p+1)$. Furthermore, as $\boldsymbol{U}^0(\sqrt{D})$ mod p is a subgroup of the multiplicative group of a finite field we see that $\boldsymbol{U}^0(\sqrt{D})$ is cyclic. The analogue of Theorem 1 for $\boldsymbol{U}^0(\sqrt{D})$ is

Theorem 3. *For $\lambda \in \boldsymbol{U}^0(\sqrt{D})$ the map $T_\lambda\colon x \mapsto \lambda x$ is ergodic on $\boldsymbol{U}^0(\sqrt{D})$ if and only if λ is primitive* mod$p$ *(i.e. $2(p+1)$ is the least positive integer k for which $\lambda^k = 1 \bmod p$) and $\lambda^{2(p+1)} \not\equiv 1 \pmod{p^2}$.*

There is a corresponding analogue of Theorem 2 in the sense that there are finitely many T_λ ergodic components for arbitrary $\lambda \in \boldsymbol{U}^0(\sqrt{D})$. These components can be completely described in terms of the order m of λ (which must divide $2(p+1)$) and the largest k for which $\lambda^m = 1 \bmod p^k$. Since the proof follows the same lines as Theorems 2 and 3 we shall omit a precise statement and demonstration.

In Section 3 we specialise to the case $D = 5$ in order to study the Fibonacci sequence mod p^k where $p \neq 2, 5$ is prime. (But see our remarks for the case $p = 5$.)

Defining $N(z) = 1$ or -1 according to whether z is a square or not (in $\boldsymbol{U}$ or $\boldsymbol{U}^0(\sqrt{5})$) we let f be the function $f\colon \boldsymbol{U} \to \boldsymbol{Z}_p$ $(\boldsymbol{U}^0(\sqrt{5}) \to \boldsymbol{Z}_p)$ given by

$$f(z) \ = \ \frac{1}{\sqrt{5}} \left(z - \frac{N(z)}{z} \right) .$$

The Jacobian J of this function measures the expansion or contraction of f with respect to Haar measures $(J\colon \boldsymbol{U}\,(\boldsymbol{U}^0(\sqrt{5})) \to \mathbb{R}^+)$, and we define $\boldsymbol{j}(y) = J(z)^{-1}$ when $f(z) = y$ so that $\boldsymbol{j}\colon \boldsymbol{Z}_p \to \mathbb{R}^+$. In addition we define the counting function $\boldsymbol{i}\colon \boldsymbol{Z}_p \to \{0, 1, 2, 3, 4\}$ where $\boldsymbol{i}(y) = \mathrm{Card}\, f^{-1}(y)$. With these definitions we have

Theorem 4. *The density of the distribution of the Fibonacci sequence in $\boldsymbol{Z}_p$ is, up to multiplicative constant, $\boldsymbol{k}(y) = \boldsymbol{i}(y)\boldsymbol{j}(y)$.*

The function $\boldsymbol{k}$, which is locally constant except at points y (at most 4) where $5y^2 + 4N(z) = 0$ ($f(z) = y$) is completely determined in Sections 4-7, together with the required normalisation constant $\int \boldsymbol{k}\, d\mu$ where μ is Haar measure on $\boldsymbol{Z}_p$.

The theorem will be proved under the assumption that $T_\beta \colon \boldsymbol{U} \to \boldsymbol{U}$ ($\boldsymbol{U}^0(\sqrt{5}) \to \boldsymbol{U}^0(\sqrt{5})$) is ergodic where $\beta = (1+\sqrt{5})/2$, although this restriction is not necessary since, as we shall see, $\boldsymbol{U}$ ($\boldsymbol{U}^0(\sqrt{5})$) *always* decomposes into a finite number of closed-open ergodic sets which can be completely described in terms of number theoretic properties of β.

1. Ergodicity for multiplications of the units of $\boldsymbol{Z}_p$

For each $n \in \mathbb{N}$ define the subgroup $\boldsymbol{U}_n = 1 + p^n \boldsymbol{Z}_p$ of $\boldsymbol{U}$, so that

$$\boldsymbol{U} \supseteq \boldsymbol{U}_1 \supseteq \boldsymbol{U}_2 \supseteq \cdots \quad \text{and} \quad \cap_{n=1}^{\infty} \boldsymbol{U}_n = \{1\}\,.$$

It is clear that $\boldsymbol{U}/\boldsymbol{U}_1$ is isomorphic to the multiplicative group of $\boldsymbol{Z}/p\boldsymbol{Z}$ (or equivalently the additive group of $\boldsymbol{Z}/(p-1)\boldsymbol{Z}$). Using the fact that each element of $\boldsymbol{U}_1$ has a $(p-1)$th root (see later) it follows that there is a subgroup $\boldsymbol{V}$ of $\boldsymbol{U}$ such that $\boldsymbol{U} = \boldsymbol{V} \times \boldsymbol{U}_1$ where $\boldsymbol{V}$ is isomorphic to $\boldsymbol{Z}/(p-1)\boldsymbol{Z}$ (moreover $\boldsymbol{V}$ is uniquely defined). To see this we choose x in a coset of $\boldsymbol{U}_1$ which cyclically generates $\boldsymbol{U}/\boldsymbol{U}_1$ and let $x^{p-1} = y \in \boldsymbol{U}_1$. As remarked above there exists $z \in \boldsymbol{U}_1$ such that $z^{p-1} = y$. Hence xz^{-1} generates a cyclic subgroup $\boldsymbol{V}$ of $\boldsymbol{U}$ of order $p-1$ and it is clear that $\boldsymbol{U} = \boldsymbol{V} \cdot \boldsymbol{U}_1$. (If $\boldsymbol{V}'$ is another subgroup with the same property and $v \in \boldsymbol{V}$, $v' \in \boldsymbol{V}'$ belong to the same generating coset then $v'v^{-1} \in \boldsymbol{U}_1$ which implies $v = v'$ since $\boldsymbol{U}_1$ is torsion-free.) A convenient isomorphism of $\boldsymbol{V}$ to the multiplicative group of $\boldsymbol{Z}/p\boldsymbol{Z}$ is given by $x \mapsto x_0$.

Corollary 5. *The subgroup $\boldsymbol{U}^2 \subseteq \boldsymbol{U}$ of square elements decomposes $\boldsymbol{U}$ into two cosets $\boldsymbol{U} = \boldsymbol{U}^2 \cup \gamma\boldsymbol{U}^2$ where $\gamma \notin \boldsymbol{U}^2$.*

Proof. We write $\boldsymbol{U} = \boldsymbol{V} \cdot \boldsymbol{U}_1$. Since $\boldsymbol{V}$ is cyclic of even order, the squares of $\boldsymbol{V}$ form a subgroup of index 2. The fact that $\boldsymbol{U}_1$ consists of squares completes the proof. □

Corollary 5 enables us to define the Legendre symbol $N(x) = \left(\dfrac{x}{p}\right) = 1$ or -1 according to whether x is a square or not.

Lemma 6. *The groups $\boldsymbol{U}_1$, $\boldsymbol{Z}_p$ are isomorphic via a map ϕ, say, which maps $\boldsymbol{U}_k$ onto $p^{k-1}\boldsymbol{Z}_p$.*

Proof. Define $\psi_n \colon \boldsymbol{Z}/p^{n-1}\boldsymbol{Z} \to \boldsymbol{U}_1/\boldsymbol{U}_n$ by $m \bmod p^{n-1} \mapsto (1+p)^m \bmod \boldsymbol{U}_n$. These maps form a consistent sequence of isomorphisms. (Each is a homomorphism between two groups of the same order.) It therefore suffices to note that the map sending $\boldsymbol{Z}$ to $\boldsymbol{U}_1$ given by $m \to (1+p)^m$ is uniformly continuous since $\boldsymbol{Z}$ is dense in $\boldsymbol{Z}_p$. This is a simple exercise and it follows that $\boldsymbol{U}_1$ is isomorphic to $\boldsymbol{Z}_p$. The proof that this map restricts to an isomorphism between $\boldsymbol{U}_k$ and $p^{k-1}\boldsymbol{Z}_p$ is essentially the same. □

Remark. This justifies our earlier assertion that each element of $\boldsymbol{U}_1$ has a $(p-1)$th root since $\boldsymbol{Z}_p$ is divisible by any natural number which is not a multiple of p.

As we have seen $\boldsymbol{U} = \boldsymbol{V} \cdot \boldsymbol{U}_1$ so we can write $\lambda \in \boldsymbol{U}$ as $\lambda = \lambda_V \cdot \lambda_1$ where $\lambda_V \in \boldsymbol{V}$ and $\lambda_1 \in \boldsymbol{U}_1$.

Lemma 7. *If λ has order m $\bmod p$ $(m \mid p-1)$ and $\lambda^m = 1+\mu p^n$ where $p \not| \mu$ (i.e. $\lambda^m \in \boldsymbol{U}_n \setminus \boldsymbol{U}_{n+1}$) then $\lambda_1 \in \boldsymbol{U}_n \setminus \boldsymbol{U}_{n+1}$.*

Proof. Let $\lambda_1 = 1 + \nu p^k$ where $p \not| \nu$, then

$$\begin{aligned} \lambda^m = \lambda_1^m &= (1+\nu p^k)^m \\ &= 1 + m\nu p^k + \cdots \\ &= 1 + \mu p^n , \end{aligned}$$

which is only possible if $n = k$ since none of μ, m, ν is divisible by p. □

With ϕ defined as in Lemma 6 we have the commutative diagram

$$\begin{array}{ccc} \boldsymbol{U}_1 & \xrightarrow{T_{\lambda_1}} & \boldsymbol{U}_1 \\ \phi \big\downarrow & & \big\downarrow \phi \\ \boldsymbol{Z}_p & \xrightarrow[S_{\phi(\lambda_1)}]{} & \boldsymbol{Z}_p \end{array}$$

where $S_m(x) = x + m$. Hence, $\lambda_1 \in \boldsymbol{U}_n \setminus \boldsymbol{U}_{n+1}$ if and only if $\phi(\lambda_1) \in p^{n-1}\boldsymbol{Z}_p \setminus p^n \boldsymbol{Z}_p$.

Lemma 8. *If $\alpha, \beta \in p^{n-1}\boldsymbol{Z}_p \setminus p^n\boldsymbol{Z}_p$ then S_α and S_β are isomorphic. In fact they are both isomorphic to $S_{p^{n-1}}$. The isomorphism is $x \mapsto \frac{\beta}{\alpha} \cdot x$ since $\frac{\beta}{\alpha}(x+\alpha) = \beta + \frac{\beta}{\alpha} x$.*

Proof of Theorem 2. Let $\lambda \in \boldsymbol{U}$ have order $m \bmod p$ $(m \mid p-1)$ and suppose $\lambda^m = 1 + \mu p^k$ where $p \not| \mu$. Then $\lambda = \lambda_V \cdot \lambda_1$ and the map $x \mapsto \lambda_V x$ on $\boldsymbol{V}$ is isomorphic to the translation $i \mapsto i + (p-1)/m \bmod p-1$ on $\boldsymbol{Z}/(p-1)\boldsymbol{Z}$ or, equivalently, to $(p-1)/m$ copies of the translation $i \mapsto i+1$ on $\boldsymbol{Z}/m\boldsymbol{Z}$. On the other hand $\lambda_1 \in \boldsymbol{U}_k \setminus \boldsymbol{U}_{k+1}$ by Lemma 7. Hence by Lemma 8 $T_{\lambda_1} \colon \boldsymbol{U}_1 \to \boldsymbol{U}_1$ is isomorphic to the translation $x \mapsto x + p^{k-1}$ on $\boldsymbol{Z}_p$ or, equivalently, to p^{k-1} copies of the translation $x \mapsto x+1$ on $\boldsymbol{Z}_p$. Since $T_\lambda = T_{\lambda_V} \times T_{\lambda_1}$ (on $\boldsymbol{V} \times \boldsymbol{U}_1$) we see that T_λ is isomorphic to $p^{k-1}(p-1)/m$ copies of the standard map for m. Finally we note that the standard map is ergodic. This follows from the fact that each factor is ergodic and the m-th power $x \mapsto x+m$ of $x \mapsto x+1$ is ergodic on $\boldsymbol{Z}_p$. □

2. The units of $\boldsymbol{Z}_p(\sqrt{D})$

Suppose $D \in \boldsymbol{U}$ is not a square in $\boldsymbol{Z}_p$ and define $\boldsymbol{Z}_p(\sqrt{D}) = \boldsymbol{Z}_p + \sqrt{D}\,\boldsymbol{Z}_p$ a ring with units $\boldsymbol{U}(\sqrt{D})$ consisting of $z = x + \sqrt{D}\,y$ where x or $y \in \boldsymbol{U}$ (units of $\boldsymbol{Z}_p$). Note that if $z \in \boldsymbol{U}(\sqrt{D})$ then $N(z) = x^2 - D\,y^2 \in \boldsymbol{U}$ (i.e. $N(z)$ is not divisible by p) and the inverse of z is $(x - \sqrt{D}\,y)/N(z)$.

Let $\boldsymbol{U}_1(\sqrt{D}) = 1 + p\,\boldsymbol{Z}_p(\sqrt{D}) \subseteq \boldsymbol{U}(\sqrt{D})$, i.e. the units of $\boldsymbol{Z}_p(\sqrt{D})$ which can be written as $1 + p(x + \sqrt{D}\,y)$. This is a subgroup of $\boldsymbol{U}(\sqrt{D})$ and $\boldsymbol{U}(\sqrt{D})/\boldsymbol{U}_1(\sqrt{D})$ can be identified with $\boldsymbol{F}_p(\sqrt{D})^\times$ where $\boldsymbol{F}_p(\sqrt{D})$ is the *field* consisting of elements of the form $a+\sqrt{D}\,b$ where $a,b\in \boldsymbol{F}_p$, with addition and multiplication $\bmod\, p$. (Note that $a^2-D\,b^2\neq 0 \bmod p$ unless $(a,b)=(0,0)$.) Since $\boldsymbol{F}_p(\sqrt{D})$ is a finite field, $\boldsymbol{F}_p(\sqrt{D})^\times\cong \boldsymbol{U}(\sqrt{D})/\boldsymbol{U}_1(\sqrt{D})$ is cyclic. The order of $\boldsymbol{F}_p(\sqrt{D})$ is p^2 and the order of $\boldsymbol{F}_p(\sqrt{D})^\times$ is p^2-1.

Lemma 9. *There is a unique finite cyclic subgroup $\boldsymbol{V}(\sqrt{D})$ of $\boldsymbol{U}(\sqrt{D})$ of order p^2-1 isomorphic to $\boldsymbol{F}_p(\sqrt{D})^\times$ via the map $z\mapsto z_0$ (where $z=\sum_{n=0}^\infty z_np^n$).*

Proof. Suppose $w=\sum_{i=0}^{n-1} z_ip^i$ has been constructed such that $w\in \boldsymbol{U}(\sqrt{D})$ and $w^{p^2-1}=1 \bmod p^n$. Find z_n such that

$$(w+z_np^n)^{p^2-1} \;=\; 1 \bmod p^{n+1}\,,$$

which is equivalent to

$$w^{p^2-1}+(p^2-1)z_np^n \;=\; 1 \bmod p^{n+1}\,.$$

We have $w^{p^2-1}=1+\lambda p^n$ so we require

$$1+\lambda p^n+(p^2-1)z_np^n \;=\; 1 \bmod p^{n+1}\,,$$

i.e. $\lambda+(p^2-1)z_n=0 \bmod p$, which uniquely defines z_n. □

Corollary 10. $\boldsymbol{U}(\sqrt{D})=\boldsymbol{V}(\sqrt{D})\cdot\boldsymbol{U}_1(\sqrt{D})\,.$

Proof. By the previous Lemma, for $z\in\boldsymbol{U}(\sqrt{D})$ there exists a unique $\tilde z\in\boldsymbol{V}(\sqrt{D})$ such that $\tilde z_0=z_0$. Since $z/\tilde z\in\boldsymbol{U}_1(\sqrt{D})$ then $z=\tilde z\cdot(z/\tilde z)$ is the required decomposition. □

Lemma 11. *$N\colon \boldsymbol{F}_p(\sqrt{D})^\times\to\boldsymbol{F}_p^\times$ surjectively.*

Proof. We need to show that every $k=1,\cdots,p-1$ is a value of $x^2-D\,y^2=k \bmod p$. If k is a square this is obvious (put $y=0$ and $x=\sqrt{k}$). There are $(p+1)/2$ quadratic residues including 0 which we denote by $\mathcal{R}$, and there are $(p-1)/2$ non quadratic residues which we denote by $\mathfrak{N}$. Note that $\mathfrak{N}+D \bmod p$ must intersect $\mathcal{R}$ (since otherwise we would have $\mathfrak{N}=\mathfrak{N}+D \bmod p$ which is impossible). Hence if $z\in\mathcal{R}\cap(\mathfrak{N}+D \bmod p)$ then $z=x^2=\nu+D$ where ν is not a quadratic residue (i.e. $x^2-D\,y^2=\nu$ with $y=1$), so the image of N contains a non quadratic residue, therefore the image is $\boldsymbol{F}_p^\times$. □

Define the subgroups $\boldsymbol{U}^0(\sqrt{D})=\{z\in\boldsymbol{U}(\sqrt{D})\colon\ N(z)=\pm 1\}$, $\boldsymbol{U}_1^0(\sqrt{D})=\{z\in\boldsymbol{U}_1(\sqrt{D})\colon\ N(z)=1\}$ and $\boldsymbol{V}^0(\sqrt{D})=\{z\in\boldsymbol{V}(\sqrt{D})\colon\ N(z)=\pm 1\}$ in what follows. From Lemma 11 we have

Corollary 12. *The kernel of N has $(p^2-1)/(p-1)=p+1$ elements. Hence* Card $\boldsymbol{V}^0(\sqrt{D})=2(p+1)$.

Lemma 13. $\boldsymbol{U}^0(\sqrt{D})=\boldsymbol{V}^0(\sqrt{D})\cdot\boldsymbol{U}_1^0(\sqrt{D})\,.$

Proof. Suppose $N(z)=\pm 1$ and $z=c\cdot w$, where $c\in\boldsymbol{V}(\sqrt{D})$ and $w\in\boldsymbol{U}_1(\sqrt{D})$, then $N(z)=\pm 1=N(c)N(w)$. Therefore $1=N(c^{2(p+1)})N(w^{2(p+1)})=N(w)^{2(p+1)}$. If $w=1+p(a+\sqrt{D}\,b)$ then $N(w)=(1+ap)^2-D\,b^2p^2\in\boldsymbol{U}_1\subseteq\boldsymbol{Z}_p$. Since $\boldsymbol{U}_1$ is torsion-free we get $N(w)=1$ and $N(c)=\pm 1$. □

Lemma 14. $\boldsymbol{U}_1^0(\sqrt{D}) \cong \boldsymbol{Z}_p$.

Proof. Let $1 + (a + \sqrt{D}\, b)p \in \boldsymbol{U}_1^0(\sqrt{D})$ where $a + \sqrt{D}\, b \in \boldsymbol{U}(\sqrt{D})$ then $(1 + ap)^2 - D\, b^2p^2 = 1$. Since $1+D\, b^2p^2$ is a square with a square root of the form $1+D\, b^2p^2/2+cp^3$ (with $c \in \boldsymbol{Z}_p$) we have

$$ap \;=\; D\, b^2p^2/2 + cp^3$$

i.e. $a = D\, b^2p/2+cp^2$. Since b can be chosen in p^{n-1} different ways for $1+(a+\sqrt{D}\, b)p \in \boldsymbol{U}_1^0(\sqrt{D}) \bmod p^n$, the order of $\boldsymbol{U}_1^0(\sqrt{D}) \bmod p^n$ is p^{n-1}. To complete the proof we show that if $1 + zp \in \boldsymbol{U}_1^0(\sqrt{D})$ with $z \in \boldsymbol{U}(\sqrt{D})$ then $1 + zp$ has order $p^{n-1} \bmod p^n$. In fact if $(1 + zp)^m = 1 \bmod p^n$ then

$$mzp + m(m-1)z^2p^2/2 + \cdots \;=\; 0 \bmod p^n \ ,$$

and therefore $p^{n-1} \mid m$. $\square$

Proof of Theorem 3. Let $\lambda \in \boldsymbol{U}^0(\sqrt{D})$ then $\lambda = c_0 \cdot \lambda_0$ where $c_0 \in \boldsymbol{V}^0(\sqrt{D})$ and $\lambda_0 \in \boldsymbol{U}_1^0(\sqrt{D})$. The map $z \mapsto \lambda z$ on $\boldsymbol{U}^0(\sqrt{D})$ is ergodic if and only if both maps (multiplication by λ_0 on $\boldsymbol{U}_1^0(\sqrt{D})$ and multiplication by c_0 on $\boldsymbol{V}^0(\sqrt{D})$) are ergodic (the latter means that c_0 has order $2(p+1)$).

For the multiplication by λ_0 on $\boldsymbol{U}_1^0(\sqrt{D})$ to be ergodic we need that $\lambda_0 = 1+zp$ with $z \in \boldsymbol{U}$ as we have seen, and this is equivalent to $\lambda_0^{2(p+1)} = 1 + 2(p+1)zp \bmod p^2 \neq 1 \bmod p^2$. Therefore T_λ is ergodic if and only if λ has order $2(p+1) \bmod p$ but $\lambda^{2(p+1)} \neq 1 \bmod p^2$. $\square$

3. The Fibonacci sequence

From here on we consider the special case $D = 5$. This allows us to consider the Fibonacci sequence $\{u_n\}$ ($u_{n+1} = u_n + u_{n-1}$, $u_0 = 0$, $u_1 = 1$). One easily sees that we can write

$$u_n \;=\; \frac{1}{\sqrt{5}} \left(\beta^n - \left(\frac{-1}{\beta}\right)^n \right) \ , \tag{1}$$

where $\beta = \dfrac{1+\sqrt{5}}{2}$ ($\beta^2 = \beta + 1$). Defining $T_\beta \colon \boldsymbol{U} \to \boldsymbol{U}$ when 5 is a square and $T_\beta \colon \boldsymbol{U}(\sqrt{5}) \to \boldsymbol{U}(\sqrt{5})$ when 5 is not a square, we see that $u_n = f(T_\beta^n 1) = f(\beta^n)$, where

$$f(z) \;=\; \frac{1}{\sqrt{5}} \left(z - \frac{N(z)}{z} \right) \ . \tag{2}$$

We shall assume that $T_\beta \colon \boldsymbol{U} \to \boldsymbol{U}$ is ergodic when 5 is a square and $T_\beta \colon \boldsymbol{U}^0(\sqrt{5}) \to \boldsymbol{U}^0(\sqrt{5})$ is ergodic when 5 is not a square. To unify our presentation we denote by X the space (group) on which T_β acts. Since $T = T_\beta$ is an ergodic translation of a compact abelian group we have

$$\frac{1}{N} \sum_{n=0}^{N-1} F(T^n z) \;\longrightarrow\; \int F\, dm$$

uniformly in $z \in X$, for all $F \in \mathcal{C}(X)$, where m is the normalised Haar measure on X (cf. [Wat]). From this it follows that for each closed-open set $Y \subseteq \boldsymbol{Z}_p$ we have

$$\frac{1}{N}\sum_{n=0}^{N-1} \chi_Y(u_n) \quad \longrightarrow \quad m(f^{-1}(Y)) ,$$

where χ_Y is the indicator function of Y. Hence the distribution of u_n in $\boldsymbol{Z}_p$ (or $\bmod p^k$) is given by the distribution $Y \mapsto m \circ f^{-1}(Y)$, which we proceed to examine. In fact we shall determine its density function. To do this we shall find the Jacobian (or positive Radon-Nikodym derivative) of the map f and we shall calculate the number of f-inverse images of each point in $\boldsymbol{Z}_p$.

4. The Jacobian

Let μ, m, m_0 be the normalised Haar measures on $\boldsymbol{Z}_p$, $\boldsymbol{U}$ and $\boldsymbol{U}^0(\sqrt{5})$, respectively. The Jacobian of $f\colon \boldsymbol{U} \to \boldsymbol{Z}_p$ ($f\colon \boldsymbol{U}^0(\sqrt{5}) \to \boldsymbol{Z}_p$) is defined by

$$J(z) \;=\; \lim_{n\to\infty} \frac{\mu f C_n(z)}{m C_n(z)} \quad \left(J(z) \;=\; \lim_{n\to\infty} \frac{\mu f C_n(z)}{m_0 C_n(z)} \right) ,$$

where $C_n(z) = \{z + \nu p^n \colon\ \nu \in \boldsymbol{Z}_p\}$ and $C_n^0(z) = \{z + \nu p^n \colon\ \boldsymbol{Z}_p(\sqrt{5})\} \cap \boldsymbol{U}^0(\sqrt{5})$. The measures m, m_0 are determined by their values on the sets $C_n(z), C_n^0(z)$ since $\lambda C_n(z) = C_n(\lambda z)$ (for $\lambda \in \boldsymbol{U}$) and $\lambda C_n^0(z) = C_n^0(\lambda z)$ (for $\lambda \in \boldsymbol{U}^0(\sqrt{5})$). This follows from the essential uniqueness of Haar measures.

Proposition 15. *For both cases $\boldsymbol{U}$, or $\boldsymbol{U}^0(\sqrt{5})$ if 5 is not a square, we have $J(z) = 1/p^k$ when $z^2 + N(z) = \lambda p^k$, $\lambda \in \boldsymbol{U}(\sqrt{5})$, $k \geq 0$.*

Proof. The proof for both cases is virtually the same. We shall give the proof for $f\colon \boldsymbol{U}^0(\sqrt{5}) \to \boldsymbol{Z}_p$.

If $z^2 + N(z) = \lambda p^k$, $\lambda \in \boldsymbol{U}(\sqrt{5})$, $k \geq 0$, it suffices to show that, for n sufficiently large (depending only on k), we have:

(i) Whenever $z + \nu p^n \in \boldsymbol{U}^0(\sqrt{5})$, $\nu \in \boldsymbol{Z}_p(\sqrt{5})$, there exists $\tilde{\nu} \in \boldsymbol{Z}_p$ such that $f(z + \nu p^n) = f(z) + \tilde{\nu} p^{n+k}$;

(ii) Whenever $\tilde{\nu} \in \boldsymbol{Z}_p$, there exists $\nu \in \boldsymbol{Z}_p(\sqrt{5})$ such that $f(z + \nu p^n) = f(z) + \tilde{\nu} p^{n+k}$ ($z + \nu p^n \in \boldsymbol{U}^0(\sqrt{5})$).

Note that if w is small enough (i.e. divisible by a high power of p) and $z + w \in \boldsymbol{U}^0(\sqrt{5})$ then $N(z+w) = N(z)$. Therefore, in this case,

$$\begin{aligned} f(z+w) - f(z) \;&=\; \frac{1}{\sqrt{5}}\left(z + w - \frac{N(z+w)}{z+w} - z + \frac{N(z)}{z} \right) \\ &=\; \frac{w}{\sqrt{5}\, z(z+w)}\,(z^2 + N(z) + zw) \\ &=\; \frac{w}{\sqrt{5}\, z(z+w)}\,(\lambda p^k + zw) \ . \end{aligned}$$

Hence, to prove (i) we set $w = \nu p^n$ and notice that $f(z+w) - f(z)$ is divisible by p^{n+k}.

For (ii) we need to show there exists a solution w of the form νp^n ($\nu \in \boldsymbol{Z}_p(\sqrt{5})$) to the equation

$$\frac{w}{\sqrt{5}\, z(z+w)}\,(\lambda p^k + zw) \;=\; \tilde{\nu} p^{n+k}\,. \tag{3}$$

However, if such a solution w exists, it must be divisible by p^n since $\lambda p^k + zw$ is exactly divisible by p^k for large enough n. Writing $w = \nu p^n$ in (3) gives

$$\nu p^n(\lambda p^k + z\nu p^n) \;=\; \sqrt{5}\, z(z+\nu p^n)\tilde{\nu} p^{n+k}\,,$$

and so

$$\nu^2 z p^{n-k} + \nu\,(\lambda - \sqrt{5}\, z\tilde{\nu} p^n) - \sqrt{5}\, z^2\tilde{\nu} \;=\; 0\,. \tag{4}$$

The discriminant of this quadratic equation is given by

$$\Delta \;=\; (\lambda - \sqrt{5}\, z\tilde{\nu} p^n)^2 + 4\sqrt{5}\, z^3\tilde{\nu} p^{n-k} \;=\; \lambda^2 + \xi p^{n-k}\,,$$

for some $\xi \in \boldsymbol{Z}_p(\sqrt{5})$. Since Δ has a square root of the form $\lambda + \dfrac{\xi}{2\lambda}\, p^{n-k} + c p^{n-k+1}$ for some $c \in \boldsymbol{Z}_p(\sqrt{5})$, we see that

$$\begin{aligned}\nu \;&=\; \frac{-(\lambda - \sqrt{5}\, z\tilde{\nu} p^n) + \lambda + \dfrac{\xi}{2\lambda}\, p^{n-k} + c p^{n-k+1}}{2 z p^{n-k}} \\ &=\; \frac{\xi}{4z\lambda} + \frac{\sqrt{5}\,\tilde{\nu}}{2}\, p^k + cp\end{aligned}$$

is the unique solution of (4). □

With $\boldsymbol{j}\colon \boldsymbol{Z}_p \to \mathbb{R}^+$ defined as $\boldsymbol{j}(y) = J(z)^{-1}$ when $f(z) = y$, and $\boldsymbol{j}(y) = 0$ when y is not in the range of f, we have

Proposition 16. *If y is in the range of f and $f(z) = y$ ($z \in \boldsymbol{U}$ or $\boldsymbol{U}^0(\sqrt{5})$) then $5y^2 + 4N(z)$ is necessarily a square and $\boldsymbol{j}(y) = p^k$ if $5y^2 + 4N(z) = \lambda^2 p^{2k}$ for some $\lambda \in \boldsymbol{U}$, $k \geq 0$.*

Proof. Since $f(z) = y$ we have

$$\left(z - \frac{N(z)}{z}\right)^2 \;=\; 5y^2\,.$$

Adding $4N(z)$ we obtain

$$\left(z + \frac{N(z)}{z}\right)^2 \;=\; 5y^2 + 4N(z)\,,$$

from which we derive

$$z^2 + N(z) \;=\; z\sqrt{5y^2 + 4N(z)} \;=\; z\lambda p^k\,,$$

where z, λ are units. By Proposition 15 we conclude that $\boldsymbol{j}(y) = p^k$. □

5. Inverse images when 5 is a square

We write $\boldsymbol{i}(y) = \boldsymbol{i}_+(y) + \boldsymbol{i}_-(y)$ where $\boldsymbol{i}_+(y)$ (resp. $\boldsymbol{i}_-(y)$) is the number of square (resp. non-square) solutions of

$$f(z) = \frac{1}{\sqrt{5}}\left(z - \frac{N(z)}{z}\right) = y\,.$$

Equivalently, $\boldsymbol{i}_+(y)$ is the number of squares of the form $(\sqrt{5}\,y \pm \sqrt{5y^2+4})/2$ and $\boldsymbol{i}_-(y)$ is the number of non-squares of the form $(\sqrt{5}\,y \pm \sqrt{5y^2-4})/2$. When $5y_0^2+4 \neq 0 \bmod p$ (resp. $5y_0^2 - 4 \neq 0 \bmod p$) $\boldsymbol{i}_+(y) = \boldsymbol{i}_+(y_0)$ (resp. $\boldsymbol{i}_-(y) = \boldsymbol{i}_-(y_0)$) depends only on y_0. Moreover

Proposition 17. (i) *If $5y_0^2 + 4 \neq 0 \bmod p$ is not a square then $\boldsymbol{i}_+(y) = 0$. If $5y_0^2+4 \neq 0 \bmod p$ is a square then $\boldsymbol{i}_+(y) = 2$ or 0 when -1 is a square, depending on whether $(\sqrt{5}\,y + \sqrt{5y^2+4})/2$ is a square or not. If $5y_0^2 + 4 \neq 0 \bmod p$ is a square then $\boldsymbol{i}_+(y) = 1$ when -1 is not a square.*

(ii) *If $5y_0^2 - 4 \neq 0 \bmod p$ is not a square then $\boldsymbol{i}_-(y) = 0$. If $5y_0^2 - 4 \neq 0 \bmod p$ is a square then $\boldsymbol{i}_-(y) = 0$ or 2, depending on whether or not $(\sqrt{5}\,y + \sqrt{5y^2-4})/2$ is a square.*

Proof. This merely depends on the products

$$\left(\frac{\sqrt{5}\,y + \sqrt{5y^2+4}}{2}\right)\left(\frac{\sqrt{5}\,y - \sqrt{5y^2+4}}{2}\right) = -1$$

and

$$\left(\frac{\sqrt{5}\,y + \sqrt{5y^2-4}}{2}\right)\left(\frac{\sqrt{5}\,y - \sqrt{5y^2-4}}{2}\right) = 1\,,$$

and whether these are squares or not. For $\boldsymbol{i}_+$ we look for squares, whereas for $\boldsymbol{i}_-$ we look for non-squares. □

The above proposition allows us to compute $\boldsymbol{i}_+, \boldsymbol{i}_-$ for the cases where $5y_0^2 \pm 4 \neq 0 \bmod p$. In the remaining cases the procedure is more involved.

When $5y_0^2 + 4 = 0 \bmod p$ we have $5y_0^2 + 4 = \lambda p^k$, $k \geq 1$, $\lambda \in \boldsymbol{U}$. This is not a square if k is odd. If k is even $5y^2 + 4$ is a square or not according to whether λ_0 is square or not mod p. Of course there will be $(p-1)/2$ λ_0's for which λ_0 is a square and $(p-1)/2$ λ_0's for which λ_0 is not a square. When λ_0 is a square $\boldsymbol{i}_+(y) = 2$ or 0 depending on whether $(\sqrt{5}\,y \pm \sqrt{5y^2+4})/2$ are both squares or not, and when λ_0 is not a square $\boldsymbol{i}_+(y) = 0$. Similar remarks apply to the case where $5y_0^2 - 4 = 0 \bmod p$ with appropriate modifications.

These remarks should be supplemented with

Theorem 18. (a) *Let $5y_0^2 + 4 = 0 \bmod p$ then $\boldsymbol{i}_+(y) = 2$ if -1 is a fourth power and $5y^2 + 4$ is a square. Otherwise $\boldsymbol{i}_+(y) = 0$.*

(b) *Let $5y_0^2 - 4 = 0 \bmod p$ then $\boldsymbol{i}_-(y) = 0$ if $5y^2 - 4$ is not a square or $\sqrt{5}y_0/2$ $(= \pm 1)$ is a square mod p. Otherwise $\boldsymbol{i}_-(y) = 2$.*

Proof. (a) For $\boldsymbol{i}_+(y) \neq 0$ we must have $5y^2+4$ is a square, in which case $5y^2+4 = \lambda^2 p^{2k}$ ($k \geq 1$, $\lambda \in \boldsymbol{U}$) and then

$$\frac{\sqrt{5}\,y}{2} = \pm(-1)^{1/2}\left(1 - \frac{\lambda^2 p^{2k}}{4}\right)^{1/2}.$$

For

$$\frac{\sqrt{5}\,y + \sqrt{5y^2+4}}{2} = \pm(-1)^{1/2}\left(1 - \frac{\lambda^2 p^{2k}}{4}\right)^{1/2} + \frac{\lambda p^k}{2}$$

to be a square it is necessary and sufficient that $(-1)^{1/2}$ exist and be a square, i.e. -1 should be a fourth power.

(b) For $\boldsymbol{i}_-(y) \neq 0$ we must have $5y^2-4$ is a square, in which case $5y^2-4 = \lambda^2 p^{2k}$ ($k \geq 1$, $\lambda \in \boldsymbol{U}$) and then

$$\frac{\sqrt{5}\,y}{2} = \pm\left(1 + \frac{\lambda^2 p^{2k}}{4}\right)^{1/2}.$$

Thus

$$\frac{\sqrt{5}\,y + \sqrt{5y^2-4}}{2} = \pm\left(1 - \frac{\lambda^2 p^{2k}}{4}\right)^{1/2} + \frac{\lambda p^k}{2},$$

which is a square if and only if $\sqrt{5}y_0/2$ $(= \pm 1)$ is a square mod p. When this is a square then $(\sqrt{5}\,y - \sqrt{5y^2-4})/2$ is also a square, so that $\boldsymbol{i}_-(y) = 0$. When it is not a square then $(\sqrt{5}\,y - \sqrt{5y^2-4})/2$ is not a square and $\boldsymbol{i}_-(y) = 2$. ☐

Example. Let p be 11. Then 5 is a square and -1 is not a square in $\boldsymbol{Z}_p$. Consider the following table where numbers are written mod 11 and boxed numbers are non-zero squares.

y_0	0	1	2	3	4	5	6	7	8	9	10
y_0^2	0	1	4	9	5	3	3	5	9	4	1
$5y_0^2$	0	5	9	1	3	4	4	3	1	9	5
$5y_0^2+4$	$\boxed{4}$	$\boxed{9}$	2	$\boxed{5}$	7	8	8	7	$\boxed{5}$	2	$\boxed{9}$
$5y_0^2-4$	7	$\boxed{1}$	$\boxed{5}$	8	10	0	0	10	8	$\boxed{5}$	$\boxed{1}$

(a) $\boldsymbol{i}_+(y) = 0$ if $y_0 = 2, 4, 5, 6, 7, 9$. Since -1 is not a square, exactly one of $(\sqrt{5}\,y \pm \sqrt{5y^2+4})/2$ is a square when $y_0 = 0, 1, 3, 8, 10$ and in this case $\boldsymbol{i}_+(y) = 1$.

(b) $\boldsymbol{i}_-(y) = 0$ if $y_0 = 0, 3, 4, 7, 8$; $\boldsymbol{i}_-(y) = 2$ if $y_0 = 1, 2$; and $\boldsymbol{i}_-(y) = 0$ if $y_0 = 9, 10$.

Leaving the case when $y_0 = 5$ aside, and as we shall see below $\boldsymbol{i}_-(y) = 0$ when $y_0 = 6$, we have in total

y_0	0	1	2	3	4	5	6	7	8	9	10
$\boldsymbol{i}_+(y)$	1	1	0	1	0	0	0	0	1	0	1
$\boldsymbol{i}_-(y)$	0	2	2	0	0	$*$	0	0	0	0	0
$\boldsymbol{i}(y)$	1	3	2	1	0	$*$	0	0	1	0	1

For $y_0 = 5$ or 6 we have $\boldsymbol{i}_+(y) = 0$ and to evaluate $\boldsymbol{i}_-(y)$ we have to consider all the cases when $5y^2 - 4 = \lambda^2 p^{2k}$ where $\lambda \in \boldsymbol{U}$ and $k \geq 1$, since when y does not satisfy this equation $\boldsymbol{i}_-(y) = 0$. When $y_0 = 5$ and y satisfy such an equation, $\boldsymbol{i}_-(y)$ is the number of non-squares of the form $(\sqrt{5}\,5 \pm \lambda p^k)/2 = 10 \bmod p$, i.e. $\boldsymbol{i}_-(y) = 2$. If $y_0 = 6$ then since $(\sqrt{5}\,6 \pm \lambda p^k)/2 = 12 \bmod p = 1 \bmod p$ is always a square we have $\boldsymbol{i}_-(y) = 0$.

6. Inverse images when 5 is not a square

In many ways this is simpler than the last case and we can even give a formula for $\boldsymbol{i}(y)$. Again let $\boldsymbol{i}(y) = \boldsymbol{i}_+(y) + \boldsymbol{i}_-(y)$, where $\boldsymbol{i}_+(y)$ is the number of inverse images, under f, which are square and $\boldsymbol{i}_-(y)$ is the number of inverse images which are not square. Since $N\big((\sqrt{5}\,y \pm \sqrt{5y^2+4})/2\big) = 1$ (when $5y^2 + 4$ is a square) we have $\boldsymbol{i}_+(y) = N(5y^2+4)+1$ (i.e. 2 when $5y^2+4$ is a square and 0 otherwise). Similarly, since $N\big((\sqrt{5}\,y \pm \sqrt{5y^2-4})/2\big) = -1$, $\boldsymbol{i}_-(y) = N(5y^2-4)+1$. Again it is clear that $\boldsymbol{i}_+(y)$ and $\boldsymbol{i}_-(y)$ depend only on y_0 when, respectively, $5y_0^2+4 \neq 0 \bmod p$, $5y_0^2-4 \neq 0 \bmod p$. We should therefore examine the alternatives.

If $5y^2+4 = 0 \bmod p$ then $5y^2+4 = \lambda^2 p^{2k}$ ($\lambda \in \boldsymbol{U}$, $k \geq 1$) if it is to be square, in which case $\boldsymbol{i}_+(y) = 2$ and $\boldsymbol{i}_+(y) = 0$ otherwise. Similarly, when $5y^2 - 4 = 0 \bmod p$ $\boldsymbol{i}_-(y) = 2$ or $\boldsymbol{i}_-(y) = 0$ according to whether $5y^2+4 = \lambda^2 p^{2k}$ ($\lambda \in \boldsymbol{U}$, $k \geq 1$) or not. To summarise

Theorem 19. *When 5 is not a square $\boldsymbol{i}_+(y)$, $\boldsymbol{i}_-(y)$ depend only on y_0 when, respectively, $5y_0^2+4 \neq 0 \bmod p$, $5y_0^2-4 \neq 0 \bmod p$. When $5y^2+4 = 0 \bmod p$, $\boldsymbol{i}_+(y) = 2$ or $\boldsymbol{i}_+(y) = 0$ according to whether $5y^2+4$ has the form λ^2p^{2k} ($\lambda \in \boldsymbol{U}$, $k \geq 1$) or not. When $5y^2-4 = 0 \bmod p$, $\boldsymbol{i}_-(y) = 2$ or $\boldsymbol{i}_-(y) = 0$ according to whether $5y^2-4$ has the form λ^2p^{2k} ($\lambda \in \boldsymbol{U}$, $k \geq 1$) or not. In any case,*

$$\boldsymbol{i}(y) \;=\; N(5y^2+4) + N(5y^2-4) + 2\,.$$

Note. Each of $(\sqrt{5}\,y \pm \sqrt{5y^2+4})/2$ is a square with product -1. This is no contradiction since -1 is *always* a square in $\boldsymbol{U}^0(\sqrt{5})$ by virtue of $\boldsymbol{V}^0(\sqrt{5})$ having order $2(p+1)$ which is divisible by 4.

Example. Let p be 13. Then 5 is not a square in $\boldsymbol{Z}_p$ and $5y_0^2 \pm 4$ is never 0 mod p. Consider the following table where numbers are written mod 13 and boxed numbers are non-zero squares.

y_0	0	1	2	3	4	5	6	7	8	9	10	11	12
y_0^2	0	1	4	9	3	12	10	10	12	3	9	4	1
$5y_0^2$	0	5	7	6	2	8	11	11	8	2	6	7	5
$5y_0^2+4$	$\boxed{4}$	$\boxed{9}$	11	$\boxed{10}$	6	$\boxed{12}$	2	2	$\boxed{12}$	6	$\boxed{10}$	11	$\boxed{9}$
$5y_0^2-4$	$\boxed{9}$	$\boxed{1}$	$\boxed{3}$	2	11	$\boxed{4}$	7	7	$\boxed{4}$	11	2	$\boxed{3}$	$\boxed{1}$

We deduce immediately that the values of $\boldsymbol{i}(y)$ are given by the next table.

y_0	0	1	2	3	4	5	6	7	8	9	10	11	12
$\boldsymbol{i}(y)$	4	4	2	2	0	4	0	0	4	0	2	2	4

7. The normalising constant

Since we now have algorithms for computing $\boldsymbol{i}_-$, $\boldsymbol{i}_+$, $\boldsymbol{j}$, it remains to evaluate $\int \boldsymbol{k}\, d\mu$ the normalising constant, in order to specify the density function for the p-adic distribution of the Fibonacci sequence.

However, this is easily done when 5 is not a square in $\boldsymbol{Z}_p$ using the above. In fact, if $\{a_0\} = \{y\colon\ y = a_0 \bmod p\}$ and $5a_0^2 - 4 = 0 \bmod p$ then

$$\int_{\{a_0\}} \boldsymbol{i}_-(y)\boldsymbol{j}(y)\, d\mu(y) \;=\; 2\sum_{k=1}^{\infty} \frac{p-1}{2}\cdot\frac{p^k}{p^{2k}} \;=\; 1 \;=\; \left(\frac{5a_0^2-4}{p}\right) + 1\,.$$

In the above we make the convention that $\left(\frac{0}{p}\right) = 0$. Thus

$$\int \boldsymbol{k}_-\, d\mu \;=\; \sum_{y_0=0}^{p-1} \left[\left(\frac{5y_0^2-4}{p}\right)+1\right].$$

In the same way we have

$$\int \boldsymbol{k}_+\, d\mu \;=\; \sum_{y_0=0}^{p-1} \left[\left(\frac{5y_0^2+4}{p}\right)+1\right],$$

and consequently

$$\int \boldsymbol{k}\, d\mu \;=\; \sum_{y_0=0}^{p-1} \left[\left(\frac{5y_0^2+4}{p}\right) + \left(\frac{5y_0^2-4}{p}\right)+2\right].$$

When 5 is a square in $\boldsymbol{Z}_p$ a similar expression holds, however the functions $\boldsymbol{i}_+$, $\boldsymbol{i}_-$ do not only depend on the Legendre symbol of $5y_0^2 \pm 4$ (as we showed in Section 5). For computing $\boldsymbol{i}_+(y)$, when $5y_0^2+4 \neq 0 \bmod p$ is a square, we define $s_0^{\pm}(y_0) = (y_0\sqrt{5} \pm \sqrt{5y_0^2+4})/2 \bmod p$ and if -1 is a square in $\boldsymbol{Z}_p$ then either both of $s_0^{\pm}(y_0)$ are squares or both are non-squares. If -1 is not a square then necessarily there is exactly one square among $s_0^{\pm}(y_0)$. Putting these together in terms of Legendre symbols give

$$\boldsymbol{i}_+(y) \;=\; \frac{1}{4}\left\{\left[1-\left(\frac{-1}{p}\right)\right] + \left[1+\left(\frac{-1}{p}\right)\right]\left[1+\left(\frac{s_0^+(y_0)}{p}\right)\right]\right\}\left[\left(\frac{5y_0^2+4}{p}\right)+1\right].$$

For $\boldsymbol{i}_-(y)$ when $5y_0^2-4 \neq 0 \bmod p$ is a square we define $t_0^{\pm}(y_0) = (y_0\sqrt{5} \pm \sqrt{5y_0^2-4})/2 \bmod p$ and then either both of $t_0^{\pm}(y_0)$ are squares or both are non-squares. Hence in terms of Legendre symbols we obtain the simpler expression

$$\boldsymbol{i}_-(y) \;=\; \frac{1}{2}\left[1-\left(\frac{t_0^+(y_0)}{p}\right)\right]\left[\left(\frac{5y_0^2-4}{p}\right)+1\right].$$

Now if $\{a_0\} = \{y\colon\ y = a_0 \bmod p\}$ and $5a_0^2 - 4 = 0 \bmod p$ then using part (b) of Theorem 18 defining

$$c_0 \;=\; \left[1-\left(\frac{t_0^+(a_0)}{p}\right)\right],$$

we note that c_0 is either 0 or 2 according to whether $t_0^+(a_0)$ is a square or not, and then

$$\begin{aligned}\int_{\{a_0\}} \boldsymbol{i}_-(y)\boldsymbol{j}(y)\,d\mu(y) &= c_0 \sum_{k=1}^{\infty} \frac{p-1}{2}\cdot\frac{p^k}{p^{2k}} = \frac{c_0}{2} \\ &= \frac{1}{2}\left[1-\left(\frac{t_0^+(y_0)}{p}\right)\right]\left[\left(\frac{5y_0^2-4}{p}\right)+1\right].\end{aligned}$$

Again in the above we make the convention that $\left(\dfrac{0}{p}\right)=0$. Thus we obtain

$$\int \boldsymbol{k}_-\,d\mu = \frac{1}{2}\sum_{y_0=0}^{p-1}\left[1-\left(\frac{t_0^+(y_0)}{p}\right)\right]\left[\left(\frac{5y_0^2-4}{p}\right)+1\right].$$

In the case when $\{a_0\}=\{y\colon\ y=a_0 \bmod p\}$ and $5a_0^2+4=0 \bmod p$ we use part (a) of Theorem 18 and defining

$$c_0 = \left[1+\left(\frac{s_0^+(a_0)}{p}\right)\right],$$

we note that c_0 is either 0 or 2 depending on whether -1 is a fourth power or not. A similar computation as above shows that

$$\int_{\{a_0\}} \boldsymbol{i}_+(y)\boldsymbol{j}(y)\,d\mu(y) = \frac{1}{2}\left[1+\left(\frac{s_0^+(a_0)}{p}\right)\right].$$

Therefore if I denotes the set $\{a_0\in \boldsymbol{F}_p\colon\ 5a_0^2+4\neq 0 \bmod p\}$, collecting all the terms we finally obtain

$$\begin{aligned}\int \boldsymbol{k}\,d\mu &= \frac{1}{2}\sum_{y_0=0}^{p-1}\left[1-\left(\frac{t_0^+(y_0)}{p}\right)\right]\left[\left(\frac{5y_0^2-4}{p}\right)+1\right]+\frac{1}{2}\sum_{y_0\notin I}\left[1+\left(\frac{s_0^+(y_0)}{p}\right)\right] \\ &+\frac{1}{4}\sum_{y_0\in I}\left\{\left[1-\left(\frac{-1}{p}\right)\right]+\left[1+\left(\frac{-1}{p}\right)\right]\left[1+\left(\frac{s_0^+(y_0)}{p}\right)\right]\right\}\left[\left(\frac{5y_0^2+4}{p}\right)+1\right].\end{aligned}$$

8. The case $p=5$

Here we should note that $\boldsymbol{Z}_5(\sqrt{5})=\boldsymbol{Z}_5+\sqrt{5}\,\boldsymbol{Z}_5$ has for units the numbers of the form $a+b\sqrt{5}$ where $a\in\boldsymbol{U}$ and $b\in\boldsymbol{Z}_5$, for then $(a+b\sqrt{5})^{-1}=(a-b\sqrt{5})/(a^2-5b^2)$, the denominator being a unit of $\boldsymbol{Z}_5$. The units mod 5 total $20=p(p-1)$ unlike the cases we have dealt so far. Moreover, it is not true that each of the elements of $\boldsymbol{U}(\sqrt{5})$ mod 5 can be extended to an element of $\boldsymbol{U}(\sqrt{5})$ of order 20. (However, an element of $\boldsymbol{U}(\sqrt{5})$ mod 5 of order 4 can always be extended to an element of $\boldsymbol{U}(\sqrt{5})$ of order 4.) An important consequence is that the subgroup $\boldsymbol{U}_1(\sqrt{5})=1+5\,\boldsymbol{Z}_5(\sqrt{5})\subseteq \boldsymbol{U}(\sqrt{5})$ does not have a direct complement. Nevertheless the essentials of Section 2 still apply. In particular one can verify that $\beta=(1+\sqrt{5})/2$ satisfies $\beta^{20}\not\equiv 1 \bmod 25$ and β has order 20 mod 5. The argument we have used remains valid and multiplication by β on $\boldsymbol{U}^0(\sqrt{5})=\{x+\sqrt{5}\,y\in\boldsymbol{U}(\sqrt{5})\colon\ x^2-5y^2=\pm 1\}$ is ergodic. Furthermore, the quadratic forms $5y^2\pm 1$ can never vanish and are always squares since ± 1 are quadratic residues mod 5. Applying the considerations of Section 6 we see that $\boldsymbol{i}(y)=4$ and $\boldsymbol{j}(y)=1$ for all $y\in\boldsymbol{Z}_5$, which means that the density function is constant. Hence the

Fibonacci sequence is uniformly distributed mod 5^k for all $k \geq 1$. This result (in a more general setting) was proved in [Nie], together with the fact that $p = 5$ is the only prime for which the sequence is uniformly distributed mod p. To see this suppose the Fibonacci sequence is uniformly distributed mod p, then $5y^2 \pm 1$ can never vanish, so that $\left(\frac{5}{p}\right) = -1$ and $\left(\frac{-1}{p}\right) = 1$. However, $5y^2 \pm 1$ are both squares when $y = 0$ and therefore $\boldsymbol{i}(0) = 4$. With our hypothesis it follows that $\boldsymbol{i}(y) = 4$ for all $y \in \boldsymbol{Z}_p$ and therefore $5y^2 \pm 4$ are always squares. Since the range of each form consists of $(p+1)/2$ elements (when $p \neq 5$) this is clearly impossible. We conclude that $p = 5$.

9. When multiplication by β in $\boldsymbol{U}$ or $\boldsymbol{U}^0(\sqrt{5})$ is not ergodic

The asymptotic distribution of the Fibonacci sequence in the case when T_β acting on $\boldsymbol{U}$ or $\boldsymbol{U}^0(\sqrt{5})$ is not ergodic can be described by a procedure similar to the one used in the ergodic case. Since the situation in some cases is not completely analogous, we clarify on some of the differences.

Suppose 5 is a square in $\boldsymbol{Z}_p$. Let $\beta_0 = \beta \bmod p$ and denote by $\langle \beta_0 \rangle$ the group generated by β_0 in $\boldsymbol{F}_p^\times$. Suppose $\langle \beta_0 \rangle$ has index $k > 1$ in $\boldsymbol{F}_p^\times$ and assume $\beta^{p-1} \not\equiv 1 \bmod p^2$. The ergodic decomposition of T_β acting on $\boldsymbol{U}$ described in Section 1 shows that the ergodic component of T_β containing 1 is the subgroup of $\boldsymbol{U}$ given by $\boldsymbol{W} = \{z \in \boldsymbol{U} \colon\ z_0 \in \langle \beta_0 \rangle\}$.

There are now two cases to consider depending on whether the order of β_0 in $\boldsymbol{F}_p^\times$ is even or odd. If it is even then $\langle \beta_0^2 \rangle$ has index 2 in $\langle \beta_0 \rangle$ and hence T_{β^2} is ergodic on the subgroup of squares of $\boldsymbol{W}$. Hence the situation is completely analogous to our previous discussion since one can define a norm N on $\boldsymbol{W}$ by $N(z) = z_0^{(p-1)/2k} = \pm 1$ and study the Jacobian of f as in (2) with respect to Haar measure on $\boldsymbol{W}$ (which is the restriction of Haar measure on $\boldsymbol{U}$). This shows that the asymptotic distribution of u_n can be obtained by computing the density function $\boldsymbol{k} = (\boldsymbol{i}_+ + \boldsymbol{i}_-)\boldsymbol{j}$, where $\boldsymbol{j}$ is given by Proposition 16 (with appropriate modifications) and $\boldsymbol{i}_+$ counts the number of inverse images under f which are in $\boldsymbol{W}$ and are squares and $\boldsymbol{i}_-$ counts the corresponding number of non-squares.

If the order of β_0 in $\boldsymbol{F}_p^\times$ is odd then $\langle \beta_0^2 \rangle = \langle \beta_0 \rangle$ and both T_β and T_{β^2} are ergodic on $\boldsymbol{W}$. In this case we introduce the functions $f_\pm \colon \boldsymbol{U} \to \boldsymbol{Z}_p$ given by

$$f_+(z) = \frac{1}{\sqrt{5}}\left(z - \frac{1}{z}\right) \quad \text{and} \quad f_-(z) = \frac{1}{\sqrt{5}}\left(z + \frac{1}{z}\right),$$

and given an open and closed subset Y of $\boldsymbol{Z}_p$ we compute the limit of

$$\frac{1}{2N}\sum_{\ell=0}^{2N-1} \chi_Y(u_\ell) = \frac{1}{2N}\sum_{n=0}^{N-1}\big(\chi_Y(u_{2n}) + \chi_Y(u_{2n+1})\big) \tag{5}$$

$$= \frac{1}{2}\Big(\frac{1}{N}\sum_{n=0}^{N-1}\chi_Y(f_+(T_{\beta^2}^n 1)) + \frac{1}{N}\sum_{n=0}^{N-1}\chi_Y((f_-\circ T_\beta)(T_{\beta^2}^n 1))\Big). \tag{6}$$

If m denotes Haar measure on $\boldsymbol{W}$ then we obtain

$$\lim_{N\to\infty} \frac{1}{2N} \sum_{\ell=0}^{2N-1} \chi_Y(u_\ell) \;=\; \frac{1}{2}\left(m(f_+^{-1}(Y)) + m(f_-^{-1}(Y))\right).$$

Since the Jacobians $j_\pm$ of $f_\pm$ satisfy the conclusions of Proposition 16 (again with appropriate changes) we see that the density function of the asymptotic distribution of u_n is (up to normalisation) given by $\boldsymbol{k} = \boldsymbol{i}_+\boldsymbol{j}_+ + \boldsymbol{i}_-\boldsymbol{j}_-$ where $\boldsymbol{i}_\pm$ counts the number of inverse images under f which are in $\boldsymbol{W}$.

When 5 is not a square in $\boldsymbol{Z}_p$ and $\beta^{2(p+1)} \not\equiv 1 \bmod p^2$ we argue in a similar way. Hence when the ergodicity of T_β fails purely by β not being primitive mod p the above can be applied to compute the density of the asymptotic distribution of u_n. When ergodicity fails because of either $\beta^{p-1} \equiv 1 \bmod p^2$ or $\beta^{2(p+1)} \equiv 1 \bmod p^2$ then one should use the general expression (6) and study the ergodic component $\boldsymbol{W}'$ of T_{β^2} containing 1. Therefore if m denotes Haar measure on $\boldsymbol{W}'$ the Jacobians $\boldsymbol{j}_\pm$ of $f_\pm$ still satisfy Proposition 16 and the density function of the asymptotic distribution of u_n is again (up to normalisation) given by $\boldsymbol{k} = \boldsymbol{i}_+\boldsymbol{j}_+ + \boldsymbol{i}_-\boldsymbol{j}_-$ where $\boldsymbol{i}_+$ counts the number of inverse images under f_+ which are in $\boldsymbol{W}'$ and $\boldsymbol{i}_-$ counts the number of inverse images under f_- which are in the coset $\beta\cdot\boldsymbol{W}'$. (Note that this could have been the procedure adopted in Section 3 without the need to introduce the norm N. However, we chose to introduce it to unify our presentation.)

Example. Let p be 19. Then 5 is a square, -1 is not a square in $\boldsymbol{Z}_p$, β_0 has order 9, β is a square in $\boldsymbol{U}$ which is not a fourth power and $\beta^{18} \not\equiv 1 \bmod 19^2$. Hence $\boldsymbol{W}$ is the subgroup of squares in $\boldsymbol{U}$. Consider the following table where numbers are written mod 19 and boxed numbers are non-zero squares.

y_0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
y_0^2	0	1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1
$5y_0^2+4$	$\boxed{4}$	$\boxed{9}$	$\boxed{5}$	$\boxed{11}$	8	15	13	2	$\boxed{1}$	10	10	$\boxed{1}$	2	13	15	8	$\boxed{11}$	$\boxed{5}$	$\boxed{9}$
$5y_0^2-4$	15	$\boxed{1}$	$\boxed{16}$	3	0	$\boxed{7}$	$\boxed{5}$	13	12	2	2	12	13	$\boxed{5}$	$\boxed{7}$	0	3	$\boxed{16}$	$\boxed{1}$

Let $\boldsymbol{i}_\pm(y)$ be the number of inverse images under $f_\pm$ which are in $\boldsymbol{W}$ (i.e. those which are squares). Then

(a) $\boldsymbol{i}_+(y) = 0$ if $y_0 = 4, 5, 6, 7, 9, 10, 12, 13, 14, 15$. Since -1 is not a square, exactly one of $(\sqrt{5}\,y \pm \sqrt{5y^2+4})/2$ is a square when $y_0 = 0, 1, 2, 3, 8, 11, 16, 17, 18$ and in this case $\boldsymbol{i}_+(y) = 1$.

(b) $\boldsymbol{i}_-(y) = 0$ if $y_0 = 0, 3, 7, 8, 9, 10, 11, 12, 16$; $\boldsymbol{i}_-(y) = 2$ if $y_0 = 1, 2, 5, 13$; and $\boldsymbol{i}_-(y) = 0$ if $y_0 = 6, 14, 17, 18$.

Leaving the case when $y_0 = 15$ aside, and as we shall see below $\boldsymbol{i}_-(y) = 0$ when $y_0 = 4$, we have in total

y_0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\boldsymbol{i}_+(y)$	1	1	1	1	0	0	0	0	1	0	0	1	0	0	0	0	1	1	1
$\boldsymbol{i}_-(y)$	0	2	2	0	0	2	0	0	0	0	0	0	0	2	0	$*$	0	0	0
$\boldsymbol{i}(y)$	1	3	3	1	0	2	0	0	1	0	0	1	0	2	0	$*$	1	1	1

For $y_0 = 4$ or 15 we have $\boldsymbol{i}_+(y) = 0$ and to evaluate $\boldsymbol{i}_-(y)$ we have to consider all the cases when $5y^2 - 4 = \lambda^2 p^{2k}$ where $\lambda \in \boldsymbol{U}$ and $k \geq 1$, since when y does not satisfy this equation $\boldsymbol{i}_-(y) = 0$. When $y_0 = 15$ and y satisfy such an equation, $\boldsymbol{i}_-(y)$ is the number of squares of the form $(\sqrt{5}\,15 \pm \lambda p^k)/2 = 1 \bmod p$, i.e. $\boldsymbol{i}_-(y) = 2$. If $y_0 = 4$ then since $(\sqrt{5}\,15 \pm \lambda p^k)/2 = 18 \bmod p$ is always a non-square we have $\boldsymbol{i}_-(y) = 0$.

10. Final Remark

The above results for the Fibonacci sequence extends directly to the sequence u_n given by the linear recurrence sequence $u_n = Au_{n-1} + u_{n-2}$ with $u_0 = 0$ and $u_1 = 1$, where A is an integer such that p does not divide $A(A^2+4)$. This is because, in this case the sequence also satisfies Binet's formula:

$$u_n = \frac{1}{\sqrt{D}}\left(\beta^n - \left(\frac{-1}{\beta}\right)^n\right),$$

where $D = A^2 + 4$ is the discriminant of $P(x) = x^2 - Ax - 1$ and $\beta = (A + \sqrt{D})/2$ is the dominant root of P. The conditions on p imply that β is a unit in $\boldsymbol{Z}_p$ if D is a square and β is a unit in $\boldsymbol{Z}_p(\sqrt{D})$ if D is not a square. Hence, essentially everything we stated works in this case replacing 5 by D in our presentation.

Appendix A. The graph of the density function

The combination of Proposition 16 and Theorems 18 and 19 show that the asymptotic distribution of the Fibonacci sequence on $\boldsymbol{Z}_p$ is absolutely continuous with respect to Haar measure of $\boldsymbol{Z}_p$ and the density function is locally constant. Using the map $\pi\colon \boldsymbol{Z}_p \to [0,1]$ given by

$$\pi\Big(\sum_{n\geq 0} x_n p^n\Big) = \sum_{n\geq 0} x_n p^{-n-1},$$

we notice that π is a continuous and surjective map which fails to be injective only on a countable number of points. The map π carries the Haar measure on $\boldsymbol{Z}_p$ to the Lebesgue measure on $[0,1]$. Hence we can express the density of the Fibonacci numbers by a graph of a locally constant function defined on $[0,1]$. For the examples given in the paper (i.e. for $p = 11, 13, 19$) we have the graphs depicted in Figures 1, 2 and 3. (Notice we decided to portray them not normalised.) The points for which the density is locally unbounded are called the singularities of the distribution and we recall from the paper that these correspond exactly to the points $y \in \boldsymbol{Z}_p$ such that $\boldsymbol{i}_+(y) \neq 0$ and $5y^2 + 4 = 0$, or $\boldsymbol{i}_-(y) \neq 0$ and $5y^2 - 4 = 0$. Hence there are in general at most 4 singularities.

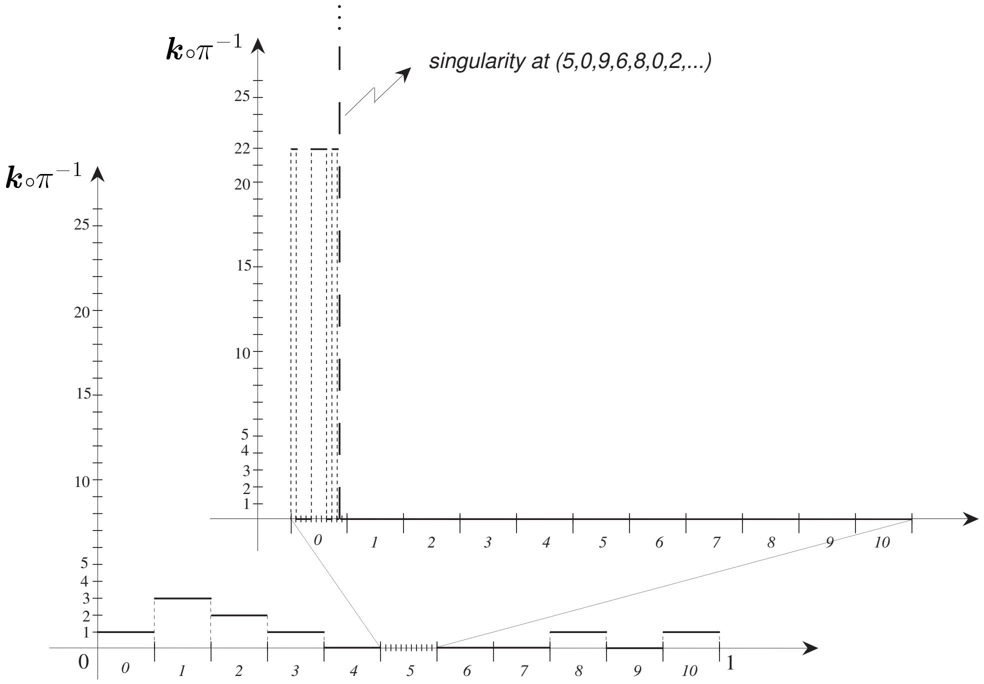

FIGURE 1. The graph of $\boldsymbol{k}\circ\pi^{-1}$ for $p = 11$.

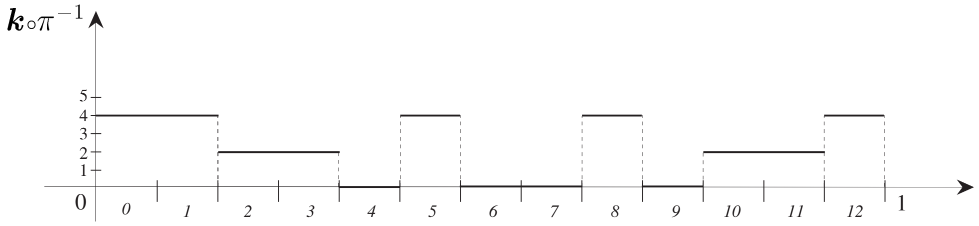

FIGURE 2. The graph of $\boldsymbol{k}\circ\pi^{-1}$ for $p = 13$.

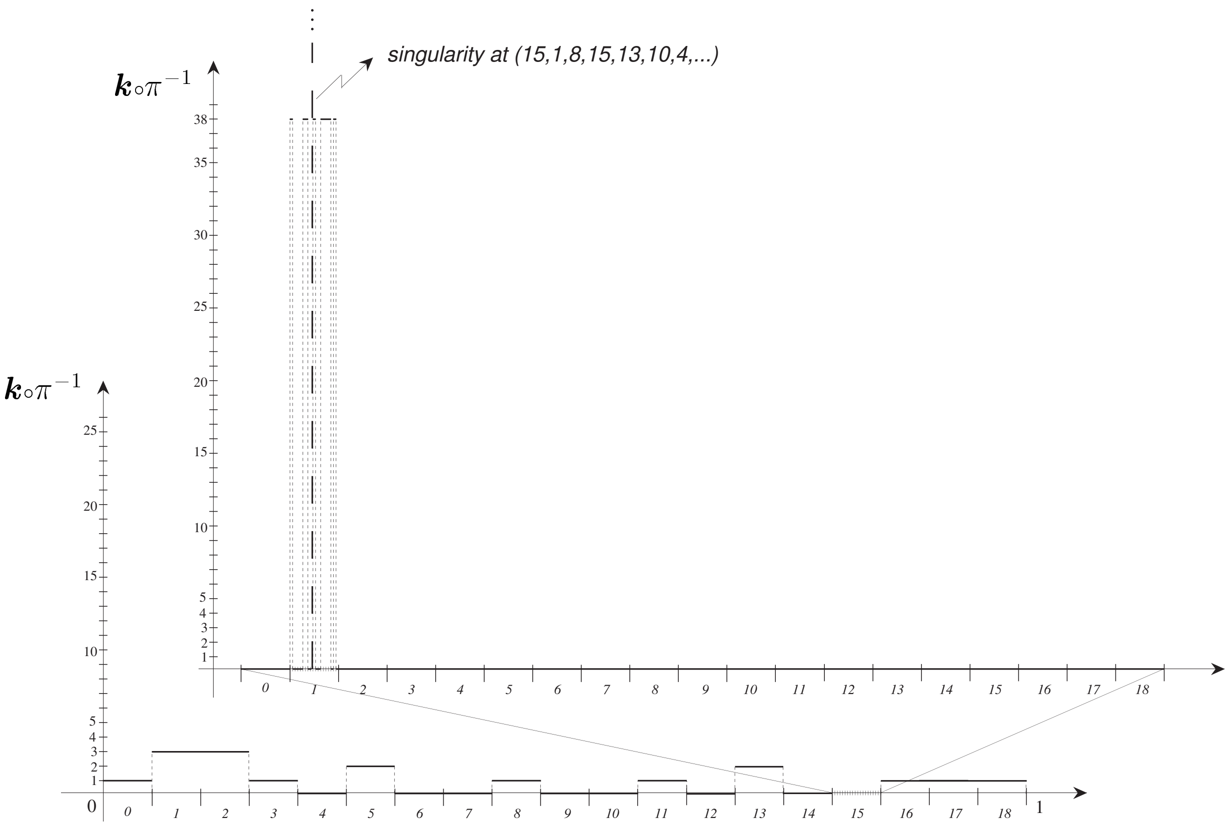

FIGURE 3. The graph of $\boldsymbol{k}\circ\pi^{-1}$ for $p = 19$.

APPENDIX B. ERGODICITY CHART

As an illustration of checking the ergodicity conditions for T_β acting on U or $U^0(\sqrt{5})$, where $\beta = (1+\sqrt{5})/2$, we show the next chart containing this information for the first 180 odd primes. In all of these cases the condition of β primitive mod p is checked by means of computing the index of the group generated by $\beta_0 = \beta \bmod p$ in $\boldsymbol{V}$ or $\boldsymbol{V}^0(\sqrt{5})$, according to whether 5 is a square in $\boldsymbol{Z}_p$ or $\boldsymbol{Z}_p(\sqrt{5})$ respectively.

Remark. The second condition for ergodicity of T_β, i.e. $\beta^{p-1} \not\equiv 1 \bmod p^2$ (if 5 is a square in Z_p) and $\beta^{2(p+1)} \not\equiv 1 \bmod p^2$ (if 5 is not square in Z_p) is satisfied for all the primes in the chart.

Table 1: Ergodicity Chart of T_β for the First 180 odd primes

p	$\sqrt{5} \in \boldsymbol{Z}_p$	$\lvert\boldsymbol{V}/\langle\beta_0\rangle\rvert$	$\lvert\boldsymbol{V}^0(\sqrt{5})/\langle\beta_0\rangle\rvert$	T_β Ergodic															
3	$\times$	-	1	$\checkmark$	5	$\times$	-	1	$\checkmark$	7	$\times$	-	1	$\checkmark$	11	$\checkmark$	1	-	$\checkmark$
13	$\times$	-	1	$\checkmark$	17	$\times$	-	1	$\checkmark$	19	$\checkmark$	2	-	$\times$	23	$\times$	-	1	$\checkmark$
29	$\checkmark$	2	-	$\times$	31	$\checkmark$	2	-	$\times$	37	$\times$	-	1	$\checkmark$	41	$\checkmark$	1	-	$\checkmark$
43	$\times$	-	1	$\checkmark$	47	$\times$	-	3	$\times$	53	$\times$	-	1	$\checkmark$	59	$\checkmark$	1	-	$\checkmark$
61	$\checkmark$	1	-	$\checkmark$	67	$\times$	-	1	$\checkmark$	71	$\checkmark$	2	-	$\times$	73	$\times$	-	1	$\checkmark$
79	$\checkmark$	2	-	$\times$	83	$\times$	-	1	$\checkmark$	89	$\checkmark$	2	-	$\times$	97	$\times$	-	1	$\checkmark$
101	$\checkmark$	4	-	$\times$	103	$\times$	-	1	$\checkmark$	107	$\times$	-	3	$\times$	109	$\checkmark$	1	-	$\checkmark$
113	$\times$	-	3	$\times$	127	$\times$	-	1	$\checkmark$	131	$\checkmark$	1	-	$\checkmark$	137	$\times$	-	1	$\checkmark$

p	$\sqrt{5} \in \boldsymbol{Z}_p$	$\|\boldsymbol{V}/\langle\beta_0\rangle\|$	$\|\boldsymbol{V}^0(\sqrt{5})/\langle\beta_0\rangle\|$	T_β Ergodic															
139	✓	6	-	×	149	✓	1	-	✓	151	✓	3	-	×	157	×	-	1	✓
163	×	-	1	✓	167	×	-	1	✓	173	×	-	1	✓	179	✓	2	-	×
181	✓	4	-	×	191	✓	1	-	✓	193	×	-	1	✓	197	×	-	1	✓
199	✓	18	-	×	211	✓	5	-	×	223	×	-	1	✓	227	×	-	1	✓
229	✓	2	-	×	233	×	-	9	×	239	✓	2	-	×	241	✓	1	-	✓
251	✓	1	-	✓	257	×	-	1	✓	263	×	-	3	×	269	✓	1	-	✓
271	✓	1	-	✓	277	×	-	1	✓	281	✓	5	-	×	283	×	-	1	✓
293	×	-	1	✓	307	×	-	7	×	311	✓	1	-	✓	313	×	-	1	✓
317	×	-	1	✓	331	✓	3	-	×	337	×	-	1	✓	347	×	-	3	×
349	✓	2	-	×	353	×	-	3	×	359	✓	2	-	×	367	×	-	1	✓
373	×	-	1	✓	379	✓	2	-	×	383	×	-	1	✓	389	✓	1	-	✓
397	×	-	1	✓	401	✓	2	-	×	409	✓	1	-	✓	419	✓	2	-	×
421	✓	5	-	×	431	✓	1	-	✓	433	×	-	1	✓	439	✓	2	-	×
443	×	-	1	✓	449	✓	1	-	✓	457	×	-	1	✓	461	✓	10	-	×
463	×	-	1	✓	467	×	-	1	✓	479	✓	2	-	×	487	×	-	1	✓
491	✓	1	-	✓	499	✓	2	-	×	503	×	-	1	✓	509	✓	4	-	×
521	✓	40	-	×	523	×	-	1	✓	541	✓	6	-	×	547	×	-	1	✓
557	×	-	9	×	563	×	-	3	×	569	✓	1	-	✓	571	✓	1	-	✓
577	×	-	1	✓	587	×	-	1	✓	593	×	-	1	✓	599	✓	2	-	×
601	✓	1	-	✓	607	×	-	1	✓	613	×	-	1	✓	617	×	-	1	✓
619	✓	6	-	×	631	✓	1	-	✓	641	✓	1	-	✓	643	×	-	1	✓
647	×	-	1	✓	653	×	-	1	✓	659	✓	2	-	×	661	✓	3	-	×
673	×	-	1	✓	677	×	-	3	×	683	×	-	1	✓	691	✓	5	-	×
701	✓	1	-	✓	709	✓	12	-	×	719	✓	2	-	×	727	×	-	1	✓
733	×	-	1	✓	739	✓	2	-	×	743	×	-	3	×	751	✓	1	-	✓
757	×	-	1	✓	761	✓	2	-	×	769	✓	4	-	×	773	×	-	1	✓
787	×	-	1	✓	797	×	-	7	×	809	✓	4	-	×	811	✓	3	-	×
821	✓	1	-	✓	823	×	-	1	✓	827	×	-	1	✓	829	✓	3	-	×
839	✓	2	-	×	853	×	-	1	✓	857	×	-	1	✓	859	✓	22	-	×
863	×	-	1	✓	877	×	-	1	✓	881	✓	5	-	×	883	×	-	1	✓
887	×	-	1	✓	907	×	-	1	✓	911	✓	13	-	×	919	✓	1	-	✓
929	✓	1	-	✓	937	×	-	1	✓	941	✓	4	-	×	947	×	-	1	✓
953	×	-	9	×	967	×	-	11	×	971	✓	1	-	✓	977	×	-	3	×
983	×	-	1	✓	991	✓	1	-	✓	997	×	-	1	✓	1009	✓	1	-	✓
1013	×	-	1	✓	1019	✓	2	-	×	1021	✓	2	-	×	1031	✓	1	-	✓
1033	×	-	1	✓	1039	✓	1	-	✓	1049	✓	4	-	×	1051	✓	1	-	✓
1061	✓	2	-	×	1063	×	-	1	✓	1069	✓	3	-	×	1087	×	-	17	×

References

[Bum] R.T. Bumby, A distribution property for linear recurrence of the second order, *Proc. Amer. Math. Soc.* **50** (1975) 101–106.

[Jac] E.T. Jacobson, Distribution of the Fibonacci numbers mod 2^k, *Fibonacci Quart.* (1992) .

[KN] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences of integers in residue classes*, New York, Wiley-Interscience, 1974.

[KS] L. Kuipers and J. Shiue, A distribution property of the sequence of Fibonacci numbers, *Fibonacci Quart.* **10.5** (1972) 375–376, 392.

[Nar] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lect. Notes in Math. 1087. Springer Verlag, Berlin-New York, 1984.

[Nat] M. Nathanson, Linear recurrences and uniform distribution, *Proc. Amer. Math. Soc.* **48**, (1975) 289–291.

[Nie] H. Niederreiter, Distribution of Fibonacci numbers mod 5^k, *Fibonacci Quart.* **10**, no. 4, (1972) 373–374.

[Ser] J-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics **7**, Springer-Verlag, 1973.

[Tur] G. Turnwald, Uniform distribution of second-order linear recurring sequences, *Proc. Amer. Math. Soc.* **96**, no. 2, (1986) 189–198.

[Wal] D.D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960) 525–532.

[Wat] P. Walters, *An introduction to ergodic theory*, Graduate Texts in Maths **79**, Springer Verlag, New York, 1982.

[War] M. Ward, The arithmetical theory of linear recurring sequences, *Trans. Amer. Math. Soc.* **35** (1933) 600–628.

[Ve] W.Y. Velez, Uniform distribution of two-term recurrence sequences, *Trans. Amer. Math. Soc.* **301** (1987) 37–45.

Department of Mathematics, Statistics and Operational Research, Nottingham Trent University, Burton Street, Nottingham NG1 4BU, UK

E-mail address: zc@maths.ntu.ac.uk

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK