Fibonacci goes magic

Autor(en): **Behrende, Ehrhard**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **69 (2014)**

PDF erstellt am: **17.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-515867

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Elem. Math. 69 (2014) 169 – 177
0013-6018/14/040169-9
DOI 10.4171/EM/260

© Swiss Mathematical Society, 2014

Elemente der Mathematik

Fibonacci goes magic

Ehrhard Behrends

Ehrhard Behrends ist Professor für Mathematik an der Freien Universität Berlin. Seine Spezialgebiete sind Funktionalanalysis und Wahrscheinlichkeitstheorie. Seit Jahren ist er auch in der Popularisierung der Mathematik aktiv. Er hat die Internetseite www.mathematik.de aufgebaut, zur Zeit entwickelt er im Auftrag der EMS die populäre Internetseite www.mathematics-in-europe.eu.

1 The phenomenon

Let p be a prime number. We write $\mathbb{Z}_p$ for the set $\{0, 1, \ldots, p-1\}$ of residues modulo p, and we consider the usual addition and multiplication modulo p on $\mathbb{Z}_p$. It will be important in the sequel that $\mathbb{Z}_p$, provided with these operations, is a field, i.e., one calculates as in the usual number system. (E.g., for $x \neq 0$, the number $1/x$ is defined as that element $y \in \mathbb{Z}_p$ for which $x \cdot y = 1$. In the case $p = 7$, for example, one has $1/5 = 3$. And $-x$ means that y such that $x + y = 0$. E.g., $-1 = p - 1$ for $x \in \mathbb{Z}_p$.) Now let numbers $a, b \in \mathbb{Z}_p$ be given. They generate a sequence $x_0, x_1, \ldots$ in $\mathbb{Z}_p$ by $x_0 := a$, $x_1 := b$, $x_n := x_{n-1} + x_{n-2} \bmod p$ for $p \geq 2$. Note that this is the usual Fibonacci sequence modulo p in the case $(a, b) = (0, 1)$.

Die Fibonacci-Folge hat auch unter Nichtmathematikern einen hohen Bekanntheitsgrad. Viele wissen, dass sie durch die Vorschrift $u_0 = 0, u_1 = 1, u_n = u_{n-1} + u_{n-2}$ für $n \geq 2$ definiert ist und dass sie etwas mit dem goldenen Schnitt zu tun hat. Über diese Folge werden immer wieder neue Forschungsergebnisse gefunden, und das *Fibonacci Quarterly* widmet sich speziell diesem Thema. Im vorliegenden Artikel geht es um ein überraschendes Phänomen, das dann auftritt, wenn man verallgemeinerte Fibonacci-Folgen modulo einer Primzahl p betrachtet. Als Beispiel betrachten wir die Primzahl $p = 7$. Für beliebige $a, b \in \{0, 1, \ldots, 6\}$ (die nicht beide Null sein sollen) definieren wir $x_0 = a, x_1 = b$ sowie $x_n = x_{n-1} + x_{n-2}$ mod 7. Dann ist die "gewöhnliche" Summe (also nicht die Summe modulo p) über die ersten 16 Folgenglieder immer gleich 49, unabhängig von a, b. Diese Tatsache ist auch schon für einen Vorhersage-Zaubertrick verwendet worden. Der Autor erklärt, wie das Ergebnis mit Konzepten der elementaren Zahlentheorie, insbesondere mit quadratischen Resten, zusammenhängt.

Sometimes it happens that, for a particular $\gamma \in \mathbb{N}$ (depending on p) the sum of the first γ elements of $(x_n)_{n=0,1,\ldots}$ is the same for all choices of a, b with $(a,b) \neq (0,0)$ (here we mean the "ordinary" sum, *not* the sum modulo p).

As a special case we note that one can work with $\gamma = 16$ if $p = 7$, there the sum is always 49. This was used as a magical trick, one finds it, e.g., in Chapter 10 (page 153 ff.) of the book "Magical Mathematics" written by Diaconis and Graham[1] (see [1]). The reader is invited to check this fact with some initial values a, b.

In the present paper we will see that a similar phenomenon occurs when 7 is replaced by certain other primes p. For example, when working with $p = 43$ one can choose $\gamma = 88$: one can predict that the sum $x_0 + \cdots + x_{87}$ equals 1849 for arbitrary $(a,b) \in \mathbb{Z}_{43} \times \mathbb{Z}_{43} \setminus (0,0)$.

Admittedly, this might be not extremely interesting for magicians since lengthy calculations are not particularly attractive. It seems, however, to be worthwile to study the interplay between ordinary summation and summation modulo p and to see the connection of this kind of problem with (mainly known) facts from elementary number theory, in particular the theory of quadratic residues.

Our main results can be found in Section 3, they are prepared in Section 2. And finally, Section 4 contains a short summary.

2 Basic definitions

Some parts of the material presented here are folklore. For generalisations see, e.g., [3] or Chapter 2(IV) in [2].

The Fibonacci sequence

By $(u_n)_{n\geq 0}$ we denote the usual Fibonacci sequence: $u_0 := 0$, $u_1 := 1$ and $u_n := u_{n-1} + u_{n-2}$ for $n \geq 2$; sometimes it will be convenient to put $u_{-1} := 1$. The following representations are well known:

Proposition 2.1. *Denote by P and Q the matrices*

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad Q = P^{-1} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}.$$

(i) $P^n = \begin{pmatrix} u_{n-1} & u_n \\ u_n & u_{n+1} \end{pmatrix}$, $Q^n = (-1)^n \begin{pmatrix} u_{n+1} & -u_n \\ -u_n & u_{n-1} \end{pmatrix}$ *for $n \geq 0$.*

(ii) *Let r, s be the roots of $x^2 - x - 1$:*

$$r = \frac{1+\sqrt{5}}{2}, \quad s = \frac{1-\sqrt{5}}{2}.$$

Then $u_n = (r^n - s^n)/\sqrt{5}$.

(iii) $u_n = \left(\binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \cdots\right)/2^{n-1}$; *note that this is a finite sum for every n since $\binom{n}{m} = 0$ for $n < m$.*

[1] The authors prescribe a slightly modified summation modulo 7: subtract 7 from the sum if it exceeds 7. As a consequence the x_n with $x_n = 0$ and $n \geq 1$ will have to be replaced by 7, and the predicted sum will be 63.

Proof. (i) and (ii) can easily be proved by induction using the definition of the u_n and the fact that $r^2 = r + 1$ as well as $s^2 = s + 1$.

(iii) From (ii) we conclude that

$$u_n = \frac{r^n - s^n}{\sqrt{5}} = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}.$$

We continue by using the binomial formula for $(x + y)^n$, and we observe that only the terms containing binomial coefficients $\binom{n}{j}$ with *odd* j survive. It only remains to simplify the resulting terms. □

Matrix calculations modulo p

We now fix an odd prime p, and we consider the powers of P and Q modulo p.

! If not otherwise stated we will calculate from now on modulo p !

The following proposition will be crucial for our investigations:

Proposition 2.2. *Suppose that $c \in \mathbb{Z}_p$ and that for some n the matrix P^n is c times the identity matrix* Id.

(i) *If $c = 1$ or $c = -1$ $(= p - 1)$ then n is an even number. We write $n = 2l$.*

(ii) *Suppose that $c = 1$. If l is even then P^l is the matrix* Id *or the matrix* $-$ Id. *If l is odd, then P^l is of the form $\begin{pmatrix} r & -2r \\ -2r & -r \end{pmatrix}$, where $r \in \mathbb{Z}_p$ is such that $5r^2 = 1 \bmod p$.*

(iii) *Suppose that $c = -1$. If l is odd then P^l is of the form $r \cdot$ Id, where $r^2 = -1$, and if l is even one has $P^l = \begin{pmatrix} r & -2r \\ -2r & -r \end{pmatrix}$ for an $r \in \mathbb{Z}_p$ such that $5p^2 = -1$.*

(iv) *If $n = 2l$ is even, then $c = 1$ or $c = -1$.*

Proof. (i) Suppose that n were of the form $2l + 1$. From $P^{2l+1} = c \cdot$ Id it would follow that $P^l = c \cdot Q^{l+1}$ so that, by Proposition 2.1 (ii),

$$\begin{pmatrix} u_{l-1} & u_l \\ u_l & u_{l+1} \end{pmatrix} = c(-1)^{l+1} \begin{pmatrix} u_{l+2} & -u_{l+1} \\ -u_{l+1} & u_l \end{pmatrix}.$$

It would follow that $u_l = c(-1)^{l+2}u_{l+1}$ and $u_{l+1} = c(-1)^{l+1}u_l$ so that $u_l = (-1)^{2l+1}c^2u_l = -u_l$, and this would imply that $u_l = u_{l+1} = 0$. (Here it is essential that $p > 2$ so that $2 \neq 0$ in $\mathbb{Z}_p$.) But this cannot happen since otherwise one would have $u_k = 0$ for $k \geq l$ in contrast to the fact that $P^n = c \cdot$ Id.

(ii) We conclude from $P^{2l} =$ Id that $P^l = Q^l$ so that $u_l = (-1)^{l+1}u_l$ and $u_{l+1} = (-1)^l u_{l-1}$. If l is even this implies that $u_l = 0$ so that P^l is diagonal. Since the square of this diagonal matrix is Id it is either Id or $-$ Id.

Now suppose that l is odd. We then know that $u_{l+1} = -u_{l-1}$ so that $u_l = (u_{l+1} - u_{l-1}) = -2u_{l-1}$. Thus, with $r := u_{l-1}$, the matrix P^l has in fact the form $\begin{pmatrix} r & -2r \\ -2r & -r \end{pmatrix}$. That $5r^2 = 1$ holds follows from $P^2 = \mathrm{Id}$.

(iii) These assertions can be proved similarly.

(iv) The assumption implies that $P^l = cQ^l$ so that $u_l = c(-1)^{l+1}u_l$ and $u_{l-1} = c(-1)^l u_{l+1}$ hold. If $u_l \neq 0$ it follows that $c = (-1)^{l+1}$, and in the case $u_l = 0$ we know that $u_{l+1} = u_{l-1}$ with $u_{l-1} \neq 0$. Therefore we can conclude from $u_{l-1} = c(-1)^l u_{l+1}$ that $c = (-1)^l$. □

The period

Let $\gamma = \gamma(p)$ be the smallest integer m such that P^m is the identity matrix modulo p. This number is just the order of P considered as an element in the finite group of invertible matrices with entries in $\mathbb{Z}_p$. From Proposition 2.1(i) it follows that $(u_n \bmod p)$ is γ-periodic and that γ is the smallest positive number m such that $u_{n+m} = u_n \bmod p$ for all n. By Proposition 2.2(1) γ is an even number.

Quadratic residues

Quadratic residues modulo p are studied since centuries. A number b is called a *quadratic residue modulo* p if there exists a such that $a^2 = b \bmod p$. For example, 9 is a quadratic residue modulo 11 since $8^2 = 9 \bmod 11$. On the other hand, 5 is not a quadratic residue modulo 7 since the only squares in $\mathbb{Z}_7$ are $1 = 1^2 = 6^2$, $4 = 2^2 = 5^2$ and $2 = 3^2 = 4^2$. If b is a quadratic residue modulo p one writes $(b \mid p) = 1$, and if this is not the case this is expressed by writing $(b \mid p) = -1$. (In many books one uses $\left(\frac{b}{p}\right)$ instead of $(b \mid p)$, but for typographical reasons we prefer our notation.)

We will take the following facts as building blocks for our further investigations. All of them are proved in a course on elementary number theory or follow easily from results shown there.

- $(a \mid p) = a^{(p-1)/2} \bmod p$.
- The prime numbers p such that $(5 \mid p) = -1$ are precisely the primes p with $p = 3 \bmod 10$ or $p = 7 \bmod 10$.
- A prime p satisfies $(-1 \mid p) = -1$ iff $p = 3 \bmod 4$, and $(-1 \mid p) = 1$ holds iff $p = 1 \bmod 4$.
- $(5 \mid p) = -1$ and $(-1 \mid p) = -1$ (i.e., $p = 3, 7 \bmod 10$ and $p = 3 \bmod 4$) are true at the same time iff $p = 3 \bmod 20$ or $p = 7 \bmod 20$. Similar characterizations are possible for all cases $(5 \mid m) = \pm 1$ and $(-1 \mid p) = \pm 1$.
- If p is a prime, then for every $a \in \{1, \ldots, p-1\}$ one has $a^{p-1} = 1$ (the "little" Fermat theorem).

The period in the cases $(5 \mid p) = \pm 1$

Proposition 2.3.

(i) *Suppose that* $(5 \mid p) = -1$. *Then* $P^{p+1} = -\mathrm{Id} \bmod p$ *so that* γ *divides* $2(p+1)$.

(ii) *If* $(5 \mid p) = 1$ *one has* $P^{p-1} = \mathrm{Id}$ *so that* $\gamma \mid p - 1$.

Proof. (i) If we multiply the representation 2.1(iv) with 2^{n-1} we arrive at

$$2^{n-1}u_n = \binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \cdots,$$

and this equation contains only integers. We will consider it modulo p for the particular values $n = p$ and $n = p + 1$.

Suppose that $n = p$. The left-hand side reduces to u_p mod p. Here we have used the fact that $2 \neq 0 \bmod p$ so that by Fermats little theorem $2^{p-1} = 1$. Also it is important that $x \mapsto x \bmod p$ is multiplicative. As far as the right-hand side is concerned we observe that all $\binom{p}{k}$ with $k < p$ contain a factor p: since p is a prime it will not be cancelled when simplifying $\binom{n}{k} = p(p-1)\cdots(p-k+1)/k!$. Thus all summands with the exception of the last one are zero modulo p. This last one is $5^{(p-1)/2}\binom{p}{p}$. The first factor modulo p is -1 (since we assumed that $(5 \mid p) = -1$) and the second is one. So we conclude that $u_p = -1 \bmod p$.

Let us now consider $n = p + 1$. Evaluated modulo p the left-hand side equals $2u_{p+1}$ mod p. The right-hand side has the same number of summands as before. Now the first summand is $p+1 = 1 \bmod p$ whereas the last one is $(-1)(p+1) = -1 \bmod p$. The remaining summands vanish modulo p since each of them contains a factor p that is not cancelled when calculating $\binom{p+1}{k}$ for $k \leq p - 1$. We thus have proved that $2u_{p+1} = 0$, and consequently u_{p+1} vanishes.

It follows from Proposition 2.1(i) that $P^{p+1} = -\mathrm{Id}$.

(ii) As in the preceding part of the proof we can show that $u_p = u_{p+1} = 1$: this time we use the fact that $5^{(p-1)/2} = 1$. It follows that $u_{p-1} = 0$ and $u_{p-2} = 1$ so that $P^{p-1} = \mathrm{Id}$. □

Note. If $(5 \mid p) = -1$ (resp. $(5 \mid p) = 1$) it is often true that $\gamma = 2(p+1)$ (resp. $\gamma = p-1$). If this is the case we will say that *p has maximal period.*

However, there are also examples where γ is smaller. The first p with $(5 \mid p) = 1$ (resp. $(5 \mid p) = -1$) is $p = 47$ where $\gamma = 32$ (resp. $p = 29$ where $\gamma = 14$).

There are also cases where γ is *much* smaller than possible. E.g., for $p = 967$, the proposition predicts that γ divides $2(p + 1) = 1936$, and one has $\gamma = 176$.

Primes where $P^{\gamma/2} = -\mathrm{Id}$

It will be clear rather soon that primes p where $P^{\gamma/2} = -\mathrm{Id}$ play an important role. We will call them *good primes.*

Proposition 2.4.

(i) *p is a good prime iff* $\gamma \bmod 4 = 0$.

(ii) *Primes such that* $(5 \mid p) = -1$ *are good primes.*

(iii) *There are no good primes with* $(5 \mid p) = 1$ *and* $(-1 \mid p) = -1$.

(iv) *Let p be such that* $(5 \mid p) = (-1 \mid p) = 1$. *If the period of p is maximal then p is a good prime.*

Proof. (i) This follows immediately from Proposition 2.2(i) and (ii).

(ii) γ is even, we write $\gamma = 2l$. By Proposition 2.2(ii) P^l is one of the matrices Id, $-$ Id or $\begin{pmatrix} r & -2r \\ -2r & -r \end{pmatrix}$ with $5r^2 = 1 \bmod p$. By the definition of γ it is not possible that $P^l = \mathrm{Id}$, and $(5 \mid p) = -1$ implies that there are no $r \in \mathbb{Z}_p$ with $5r^2 = 1$. Thus $P^l = -\mathrm{Id}$.

(iii) Suppose that, with $l := \gamma/2$, we would have $P^l = -\mathrm{Id}$. By Proposition 2.2(i) l would be even. Let R be the matrix $P^{l/2}$.

By Proposition 2.2(iii) there are two possibilities. R could be a diagonal matrix $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ with $r^2 = -1$. This is not possible since $(-1 \mid p) = -1$. Or $R = \begin{pmatrix} r & -2r \\ -2r & -r \end{pmatrix}$ with $5r^2 = -1$. But by our assumption we can write $5 = d^2$ so that $(dr)^2 = -1$ in contradiction to $(-1 \mid p) = -1$.

(iv) The p such that $(5 \mid p) = (-1 \mid p) = 1$ are precisely the primes with $p \bmod 20 \in \{1, 9\}$. Thus $p - 1 \bmod 4 = 0$ when the period is maximal. (There are, however, good p with $(5 \mid p) = (-1 \mid p) = 1$ where the period is not maximal. 89 is the smallest p with this property, the period is 44.) □

The zeros in $(u_n \bmod p)_{n=0,1,\ldots}$

As a last preparation of our main results we investigate how often the $u_n \bmod p$ vanish in a period. Let ν be the cardinality of the set $\{k \mid 0 \le k \le \gamma - 1,\ u_k = 0\}$. (Recall that all calculations are modulo p.)

Proposition 2.5.

(i) $\nu \in \{1, 2, 4\}$.

(ii) *If* $(5 \mid p) = -1$, *then* $\nu \in \{2, 4\}$. *More precisely: if* $(-1 \mid p) = -1$ *holds, then* $\nu = 2$, *and in the case* $(-1 \mid p) = 1$ *one has* $\nu = 4$.

Proof. (i) $u_l = 0$ means that P^l is diagonal. Let k be the smallest positive number such that P^k is diagonal. By Proposition 2.2(iv) P^{2k} is either Id or $-$ Id. This proves the claim: if $P^k = \mathrm{Id}$ then $k = \gamma$ and $\nu = 1$; if $k < \gamma$ and $P^{2k} = \mathrm{Id}$ then $\nu = 2$; and if $k < \gamma$ and $P^{2k} = -\mathrm{Id}$ then $\nu = 4$.

(ii) Since p is good we already know that $u_{\gamma/2} = 0$ so that $\nu \in \{2, 4\}$. Suppose that $(-1 \mid p) = -1$. If $\nu = 4$ would hold we would know that $R := P^{\gamma/4} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ is diagonal with $R^2 = -\mathrm{Id}$. This is not possible since this would imply that $r^2 = -1$, a contradiction. This proves that $\nu = 2$ in this case.

It remains to consider the case $(-1 \mid p) = 1$. Again, with $R = P^{\gamma/4}$, we know that $R^2 = -\mathrm{Id}$. By Proposition 2.2(iii) R is of the form $r \cdot \mathrm{Id}$ (which would imply $\nu = 4$) or of the form $\begin{pmatrix} r & -2r \\ -2r & -r \end{pmatrix}$ with $5r^2 = -1$. The second variant is not possible since we can write -1 as d^2 so that $5r^2 = -1$ would yield $5 = (d/r)^2$, a contradiction to $(5 \mid p) = -1$. □

3 The main results

Let us return to the problem of the first section: we choose $(a, b) \neq (0, 0)$, we define $x_0 := a, x_1 := b$ and $x_n := x_{n-1} + x_{n-2} \bmod p$, and we are interested in $x_0 + \cdots + x_{\gamma-1}$, where here we mean the "ordinary" sum, *not* the sum modulo p.

Proposition 3.1. *Suppose that p is a good prime. Then, regardless of a, b, the following is true:*

- *If no zero occurs in $x_0, \ldots, x_{\gamma-1}$, then $x_0 + \cdots + x_{\gamma-1}$ equals $\gamma \cdot p/2$.*
- *If there are zeros in $x_0, \ldots, x_{\gamma-1}$, then*

$$x_0 + \cdots + x_{\gamma-1} = p(\gamma/2 - \nu/2).$$

Proof. We know that $P^{\gamma/2} = -\mathrm{Id}$ and it is easy to see that $(x_n, x_{n+1})^\perp = P^n(a, b)^\perp$. (For a row vector (c, d) we denote by $(c, d)^\perp$ the associated column vector.) This implies that $x_{\gamma/2+t} = -x_t$ for every t.

Thus, if we write $x_0 + \cdots + x_{\gamma-1}$ as $(x_0 + x_{\gamma/2}) + (x_1 + x_{\gamma/2+1}) + \cdots$ we generate $\gamma/2$ summands of type $r + (-r)$. Each of these summands equals p if $r \neq 0$ and 0 in the case $r = 0$: note that $-r = p - r$ in $\mathbb{Z}_p$ if $r \neq 0$.

This proves the first part of the proposition. It remains to check the number of zeros in $x_0, \ldots, x_{\gamma-1}$.

Suppose that there is a zero, at position k, say. For the calculation of the (ordinary) sum of the $x_0, \ldots, x_{\gamma-1}$ we may start at x_k: $x_k, x_{k+1}, \ldots, x_{\gamma-1}, x_0, \ldots, x_{k-1}$ (note that the sequence is γ-periodic). But this is precisely the sequence "$u_0, \ldots, u_{\gamma-1} \bmod p$, multiplied with x_{k+1}". In particular there are precisely ν zeros in the shifted sequence and this is therefore also true for the original sequence. They will occur pairwise at certain positions k and $k + \gamma/2$. There are $\nu/2$ such pairs and each one contributes with the value 0 to the sum. $\gamma/2 - \nu/2$ pairs of type $r, p - r$ with $r \neq 0$ remain, and this proves the proposition. □

Sometimes it is not necessary to consider both cases in the preceding proposition. Let p be a good prime. We will call it *very good* if for each choice of $(a, b) \neq (0, 0)$ the associated sequence contains ν zeros.

Proposition 3.2.

(i) *Let p be a prime with maximal period such that $(5 \mid p) = (-1 \mid p) = -1$. Then p is a very good prime.*

(ii) *There are no other very good primes.*

Proof. (i) It will be convenient to associate with P a discrete dynamical system. We define a map Φ_p on $\Delta_p := \mathbb{Z}_p \times \mathbb{Z}_p$ by

$$(a, b)^\perp \mapsto P(a, b)^\perp = (b, a + b)^\perp.$$

By the *orbit* of an $(a, b)^\perp$ we mean the sequence $(\Phi_p^n(a, b)^\perp)_{n=0,1,\ldots}$, and the *period* of $(a, b)^\perp$ is the smallest positive m with $\Phi_p^m(a, b)^\perp = (a, b)^\perp$.

The period of $(0,1)^\perp$ is γ, and the orbit of this point visits precisely $\nu = 2$ elements in $\{0\} \times \mathbb{Z}_p$ in a full period (cf. Proposition 2.5). Let us consider any orbit starting at some $(a,b)^\perp$ that passes through an element of $\{0\} \times \mathbb{Z}_p$. It will be the shift of a multiple of the orbit through $(0,1)$ and therefore its length is also γ and it will also touch two points in $\{0\} \times \{1, \ldots, p-1\}$ on its way. Thus there are $(p-1)/2$ possible orbits that do not omit this set. Different orbits are disjoint, and we may conclude: the union of the orbits that touch $\{0\} \times \{1, \ldots, p-1\}$ visit $(p-1)/2$ (= the number of orbits) times $2(p+1)$ (= the length of each orbit) points in $\Delta' := \Delta \setminus \{(0,0)\}$. This number equals $p^2 - 1$, and this is just the cardinality of Δ'. It follows that there are no orbits that omit $\{0\} \times \mathbb{Z}_p$, and this proves (i).

The preceding argument shows that p will be very good iff γ times $(p-1)/\nu$ equals p^2-1. By propositions 2.3 and 2.5 this happens only when the conditions of (i) are met. □

4 Résumé: Which primes can be used for a magic trick?

How our results can be translated to give rise to a magic trick will be described now; p will always denote an odd prime.

Very good primes

These are the primes with $(5 \mid p) = (-1 \mid p) = -1$ (or, equivalently, the p that satisfy $p \bmod 20 \in \{3,7\}$) with maximal period $2(p+1)$. The first examples are

$$3, 7, 23, 43, 67, 83, 103, 127, 163, 167, 223, 227, 283, \ldots$$

They can be directly used for a magical prediction trick: the (ordinary) sum over the first $2(p+1)$ elements of the sequence (x_n) is $p(\gamma/2 - \nu/2) = p^2$, regardless how $(a,b) \neq (0,0)$ have been chosen.

Good primes

Good primes can be found in the following three families:

- The primes with $(5 \mid p) = (-1 \mid p) = -1$ (or, equivalently, the p that satisfy $p \bmod 20 \in \{3,7\}$) where the period is smaller than $2(p+1)$. For these p we have $\nu = 2$. Here are the first examples (with the period in brackets):

$$47(32), 107(72), 263(176), 307(88), 347(232), 563(376), \ldots$$

- The primes with $(5 \mid p) = -1$ and $(-1 \mid p) = 1$ (or, equivalently, the p that satisfy $p \bmod 20 \in \{13,17\}$). Here we have $\nu = 4$. The first examples are the following (in brackets one finds the period):

$$13(28), 17(36), 37(76), 53(108), 73(148), 97(196), 113(76), \ldots$$

- The primes with $(5 \mid p) = 1$ and $(-1 \mid p) = -1$ (or, equivalently, the p that satisfy $p \bmod 20 \in \{1,9\}$) such that $\gamma \bmod 4 = 0$. There are cases where $\nu = 2$ and others

where $\nu = 4$. We do not know a general result. Here are examples together with the associated γ and ν in brackets.

$$41(40;2), 61(60;4), 89(44;4), 109(108;4), 149(148;4), \ldots$$

The transformation to a magical prediction trick is in these cases slightly more complicated: there have to be prepared two envelopes with the "prediction", one containing the number $p(\gamma/2 - \nu/2)$, the other the number $p\gamma/2$.

One starts by inviting someone in the audience to choose $a, b \in \mathbb{Z}_p$ with $(a, b) \neq (0, 0)$ and to calculate the first γ elements of the associated sequence (x_n). It is crucial to check during these calculations whether one of these numbers is zero. Depending on whether the answer is "yes" resp. "no" the prediction of the (ordinary) sum $x_0 + \cdots + x_{\gamma-1}$ will be $p(\gamma/2 - \nu/2)$ resp. $p\gamma/2$. (It will be really necessary to prepare both envelopes since both "yes" and "no" can occur.)

It is natural to ask what one can predict in the case of p that are not good, i.e., for the p that satisfy either $p \bmod 20 \in \{11, 19\}$ or $p \bmod 20 \in \{1, 9\}$ where in addition $\gamma \bmod 4 = 2$. In all these cases there seem to be more than two – even many – candidates for $x_0 + \cdots + x_{\gamma-1}$. E.g, for $p = 29$ the period is 14, and the possible sums are 116, 145, 174, 203, 232, 261. At present there seems to be no possibility to provide precise predictions.

References

[1] P. DIACONIS AND R. GRAHAM. *Magical Mathematics*. Princeton University Press. (2012), 244 pages.

[2] P. RIBENBOIM. *The Little Book of Bigger Primes*. Springer Verlag. (2004), 366 pages.

[3] D.D. WALL. *Fibonacci Series modulo n*. American Mathematical Monthly **67** (1960), pp. 525–532.

Ehrhard Behrends
Mathematisches Institut
Freie Universität Berlin
Arnimallee 6
D-14 195 Berlin, Germany
e-mail: behrends@math.fu-berlin.de