Das Legendre-Symbol im täglichen Leben (eines Zauberers)

Zaubertrick: Ein Zuschauer erhält ein Blatt mit 16 linear geordneten Feldern:  Der Zuschauer wählt Zahlen $a, b \in \{1, \dots, 7\}$ aus ($a=b$ erlaubt mit Ausnahme von $a=b=7$, weil 7 eine besondere Zahl ist). Diese beiden Zahlen trägt der Zuschauer in die ersten beiden Felder ein, ohne daß der Zauberer sie sieht. Das Blatt wird gefaltet und kommt in einen Umschlag. Der Zauberer darf den Umschlag anschauen und anfassen, aber nicht öffnen. Dann trifft er eine Vorhersage, die er in einen anderen Umschlag verschließt.

Nun wird der erste Umschlag geöffnet und der Zuschauer füllt die restlichen 14 Felder aus, nach folgender Regel: In das jeweils nächste Feld kommt die Summe $a+b$ der beiden vorigen Einträge, wenn $a+b \leq 7$, und $a+b-7$, wenn $a+b > 7$.

Wenn die Felder ausgefüllt sind, addiert der Zuschauer alle Einträge und erhält S. Jetzt öffnet der Zauberer den Vorhersageumschlag und zeigt, was er geschrieben hat: S.

Beispiel: $a=1, b=3$

1	3	4	7	4	4	1	5	6	4	3	7	3	3	6	2

$S = 63$

Maximal blöde Erklärung: In allen 49 Fällen ist $S = 63$.

Diese Erklärung können wir nicht akzeptieren.

Warum $a, b \in \{1, \dots, 7\}$, warum 16 Felder?

Wenn wir im Beispiel einfach mit Feld 17 und 18 weitermachen, folgt:

1	3

$\Rightarrow$ das ist periodisch $\Rightarrow$ man erhält dasselbe S, wenn man mit 3, 4 anfängt oder mit 4, 7 oder ... (16 Möglichkeiten).

Analog mit $(a,b) = (6,7)$ und mit $(a,b) = (2,2)$, jeweils 16 weitere Paare.

Das vereinfacht die Verifikation, aber es ist noch keine Erklärung, jedenfalls keine mathematische.

Was wird hier eigentlich gemacht?

Naheliegende Vermutung: Das hat was mit den Fibonaccizahlen zu tun, $u_0=0, u_1=1, u_{n+1}=u_{n-1}+u_n$ für $n\geq 2$. Aber die u_n werden nicht in $\mathbb{Z}$ betrachtet, sondern in $\mathbb{Z}/7\mathbb{Z}$, wobei $\{1,-7\}$ als Repräsentanten gewählt werden. (Wenn man $0,-6$ nimmt, ist $S=\{0\}$.) Die Summe S wird aber in $\mathbb{Z}$ gebildet. Damit stellt sich die Frage, ob man 7 durch eine andere (Prim-) Zahl ersetzen kann und 16 durch eine andere Zahl.

Wir betrachten erst die Folge der Fibonaccizahlen, dann dieselbe Folge modulo p und ob sie periodisch ist. Und dann stellen wir fest, daß wir besonders qualifiziert sind, das eigentliche Problem zu lösen.

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

Dann gilt: (a) $P^n=\begin{pmatrix}u_{n-1}&u_n\\u_n&u_{n+1}\end{pmatrix}$ und $Q^n=(-1)^n=\begin{pmatrix}u_{n+1}&-u_n\\-u_n&u_{n-1}\end{pmatrix}$ für $n\in\mathbb{N}_0$.

(b) $u_n=(r^n-s^n)/\sqrt{5}$ für $r=\frac{1+\sqrt{5}}{2}$, $s=\frac{1-\sqrt{5}}{2}$ (Lösungen von x^2-x-1)

(das kann man als lineare Algebra Aufgabe verstehen)

(c) $u_n=\left(\binom{n}{1}+5\binom{n}{3}+5^2\binom{n}{5}+\dots\right)/2^{n-1}$ für $n\geq 1$ (hier ist wie üblich $\binom{n}{m}=0$ für $n<m$)

ungeraden

Jetzt rechnen wir modulo $\mathbb{Z}$ einer Primzahl p.

$\mathbb{Z}/p\mathbb{Z}$ ist ein Körper und $\underbrace{GL_2(\mathbb{Z}/p\mathbb{Z})}_{\text{endliche Gruppe}}\ni P, Q$

(d) Sei $P^n=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ oder $=-\begin{pmatrix}1&0\\0&1\end{pmatrix}$ für ein $n\in\mathbb{N}$. Dann ist $n=2\ell$ gerade.

(e) Falls $P^n=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ und ℓ gerade, dann ist schon $P^\ell=\pm Id\,(=\begin{pmatrix}1&0\\0&1\end{pmatrix})$

Falls $-\!\!1-$ und ℓ ungerade $\Rightarrow P^\ell=\begin{pmatrix}r&-2r\\-2r&-r\end{pmatrix}$, $r\in\mathbb{Z}/p\mathbb{Z}$, $5r^2\equiv 1 \bmod p$

(f) Falls $P^n=-\begin{pmatrix}1&0\\0&1\end{pmatrix}$ und ℓ ungerade $\Rightarrow$ $P^\ell=\begin{pmatrix}r&0\\0&r\end{pmatrix}$, $r\in\mathbb{Z}/p\mathbb{Z}$, $r^2\equiv -1 \bmod p$

$-\!\!\!\!-$ und ℓ gerade $\Rightarrow P^\ell=\begin{pmatrix}r&-2r\\-2r&r\end{pmatrix}$, $r\in\mathbb{Z}/p\mathbb{Z}$, $5r^2\equiv -1 \bmod p$

(g) $n=2\ell$ und $P^n=\begin{pmatrix}c&0\\0&c\end{pmatrix}$

für $c\in\mathbb{Z}/p\mathbb{Z}$ geht nur für $c=\pm 1$

Sind wir wirklich auf dem richtigen Weg?
Setze: $=ye(p)$ die Ordnung des Gruppenelements $P \in GL_2(\mathbb{Z}/p\mathbb{Z})$.
Beispiel: $ye(7) = 16$.
Für ye gilt: ye ist eine gerade Zahl
die Folge $(u_n \bmod p)$ ist ye-periodisch und ye ist minimal mit dieser Eigenschaft
Aber wir wissen noch nicht, welche $p \neq 7$ wir wählen können und warum die Summe S konstant ist.

In (e) und (f) kommen jedenfalls interessante Bedingungen vor:
$5r^2 \equiv 1 \bmod p$ und $-1 \equiv r^2 \bmod p$ oder $-1 \equiv 5r^2 \bmod p$. Da r^2 ein Quadrat ist, wenn es existiert, ist die Frage eigentlich, welchen Wert $\left(\frac{-1}{p}\right)$ und $\left(\frac{5}{p}\right)$ annehmen.
Für welche ungeraden Primzahlen p ist $\left(\frac{5}{p}\right) = -1$ und $\left(\frac{-1}{p}\right) = -1$?
Beispiele?

(h) Sei p eine ungerade Primzahl mit $\left(\frac{5}{p}\right) = -1$. Dann ist $P^{p+1} \equiv -Id \bmod p$ und $ye \mid 2(p+1)$.
Hinweis zum Beweis: Verwenden Sie (d) für $u_n \cdot 2^{n-1} =$ Summe $-$, einmal für $n = p$, um $u_p \equiv -1 \bmod p$ zu zeigen, und dann für $n = p+1$, um $u_{p+1} \equiv 0$ zu erhalten.
(i) $P^{ye/2} \equiv -Id \Leftrightarrow ye \equiv 0 \bmod 4$ und dieser Fall tritt ein wenn $\left(\frac{5}{p}\right) = -1$.

$ye = 2(p+1)$ ist also die maximal mögliche Periode (also der für den Zaubertrick interessanteste Fall), ye kann aber auch ein echter Teiler sein, z.B.
$p = 47$: $ye = 32$ oder $p = 967$: $ye = 176$.

Im Zaubertrick haben wir das ungewöhnliche Repräsentantensystem $1, \ldots, 7$ für $\mathbb{Z}/7\mathbb{Z}$ verwendet. Wie oft kommt 7 (also $0 \bmod 7$) in der Folge vor?
Im Beispiel immer 2mal.

(ii) Sei $\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right) = -1$. Dann kommen modulo p genau zwei Nullen in den ersten p Elementen der Fibonacci-Folge vor.

Hinweis zum Beweis: Betrachten Sie das Ideal $k_0 \cdot \mathbb{Z}$ aller k mit P^k ein Vielfacher der Identität. Schreiben Sie $\frac{\mu}{2} = \alpha \cdot k_0$ und unterscheiden Sie die Fälle $\alpha = 1$, $\alpha = 2$, $\alpha > 2$.

<u>Satz:</u> Sei $\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right) = -1$ und $\mu = 2(p+1)$. Dann ist die im Zaubertrick vorkommende Summe S, unabhängig von der Wahl von a und b, immer

$$S = p^2 + 2p.$$

(Rechnet man mit Repräsentanten $0, \dots, p-1$ ist die Summe genau

$$p^2 = p\left(\frac{\mu}{2} - 1\right).$$

(p = 7 erfüllt die Voraussetzungen, p = 3 auch.)

(Hinweis zum Beweis: Betrachten Sie die Abbildung $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto P\begin{pmatrix} x \\ y \end{pmatrix}$ und die Bahnen $\begin{pmatrix} x \\ y \end{pmatrix}, P\begin{pmatrix} x \\ y \end{pmatrix}, P^2\begin{pmatrix} x \\ y \end{pmatrix}, \sim$