Endliche Körper in der Zahlentheorie

Christian Bernert, 28. September 2020

Eine Aufgabe mit Fibonaccizahlen

Wir beginnen mit einer Fragestellung, die uns fast durch den gesamten Brief begleiten wird. Diese Frage handelt von der Fibonaccifolge $(F_n)_{n=0}^{\infty}$, die definiert ist durch die Anfangswerte $F_0 = 0, F_1 = 1$ und die Rekursion

$$F_{n+2} = F_{n+1} + F_n, \quad n \geq 0.$$

Die ersten Fibonaccizahlen sind also $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$. Man kann sich nun zu dieser Folge verschiedene Fragen stellen. Etwa: Wie schnell wächst F_n mit $n \to \infty$? Ein Zahlentheoretiker wird vielleicht eher fragen:

Frage 1: Gibt es eine Fibonaccizahl, deren Dezimaldarstellung auf 999999999 endet?

Allgemeiner kann man sich fragen, welche Reste die Fibonaccifolge bei Division durch eine bestimmte natürliche Zahl n (Reste modulo n) annimmt.

Übung 1: Sei $n \in \mathbb{N}$. Zeige, dass die Fibonaccifolge periodisch modulo n ist, d.h. es gibt ein $\ell > 0$ mit $F_{k+\ell} \equiv F_k \mod n$ für alle k. (Tipp: Schubfachprinzip)

Übung 2: Nutze Übung 1, um Frage 1 zu beantworten. (Tipp: Setze die Fibonaccifolge „nach links“ fort.)

Das kleinste ℓ mit der Eigenschaft aus Übung 1 nennen wir $\kappa(n)$, die minimale Periodenlänge. Modulo $n = 2$ ist die Fibonaccifolge beispielsweise

$$0, 1, 1, 0, 1, 1, 0, 1, 1, \ldots,$$

also ist $\kappa(2) = 3$. Unsere Fragestellung ist nun:

Frage 2: Kann man etwas Interessantes über die Zahl $\kappa(n)$ sagen? Wie groß ist sie? Gibt es eine einfache Formel?

Diese Frage ist im Allgemeinen sehr schwierig. Wir schränken uns hier auf den Fall ein, in dem $n = p$ eine Primzahl ist. Hier ist eine Liste der ersten Werte von $\kappa(p)$:

p	$\kappa(p)$	p	$\kappa(p)$	p	$\kappa(p)$	p	$\kappa(p)$
2	3	7	16	17	36	29	14
3	8	11	10	19	18	31	30
5	20	13	28	23	48	37	76

Auffallend ist hier, dass bei den Primzahlen $p \in \{3, 7, 13, 17, 23, 37\}$ stets $\kappa(p) = 2(p+1)$ ist, während für $p \in \{11, 19, 31\}$ immer $\kappa(p) = p - 1$ ist. Bei $p = 29$ ist immerhin $p - 1$ auch eine Periode (ein Vielfaches von $\kappa(p)$), wenn auch nicht die kleinste .

Wir wollen dieses Phänomen nun genauer untersuchen und versuchen zu verstehen. Dazu stellt sich überraschenderweise eine Formel als sehr nützlich heraus, die auf den ersten Blick eher für die Beantwortung der oben gestellten Frage nach der Größe von F_n geeignet erscheint, nämlich die explizite Form der Fibonaccizahlen.

Da diese einerseits möglicherweise nicht allen bekannt ist und wir andererseits eine Variante der Herleitung gleich noch brauchen werden, überlegen wir uns an dieser Stelle, wie man darauf kommt.

Man beginnt mit einem Ansatz der Form $a_n = \lambda^n$ für ein gewisses $\lambda \neq 0$. Soll eine solche Folge die Rekursion $a_{n+2} = a_{n+1} + a_n$ der Fibonaccifolge erfüllen, müsste $\lambda^{n+2} = \lambda^{n+1} + \lambda^n$ gelten, also $\lambda^2 = \lambda + 1$.
Sind nun umgekehrt λ_1 und λ_2 die beiden (verschiedenen!) Nullstellen der quadratischen Gleichung $x^2 = x + 1$, so erfüllt offensichtlich jede Folge der Form $\alpha \cdot \lambda_1^n + \beta \cdot \lambda_2^n$ die Rekursionsgleichung.

Nun können wir ein lineares Gleichungssystem lösen, um die Werte α und β zu bestimmen, für die unsere Anfangswerte $F_0 = 0$ und $F_1 = 1$ angenommen werden und erhalten die berühmte **Formel von de Moivre und Binet:**

$$F_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2}.$$

Bisher haben wir absichtlich die Werte von λ_1 und λ_2 nicht explizit bestimmt. Natürlich kann man sie leicht berechnen und erhält $\lambda_1 = \frac{1+\sqrt{5}}{2}$ und $\lambda_2 = \frac{1-\sqrt{5}}{2}$ und somit $\lambda_1 - \lambda_2 = \sqrt{5}$, also

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

Da $|\lambda_2| < 1$ ist, sieht man nun leicht, dass F_n für große n sehr nahe an $\frac{\lambda_1^n}{\sqrt{5}}$ ist. Dies ist allerdings wie bereits erwähnt nicht die Frage, für die wir uns im Moment interessieren.

Für zahlentheoretische Anwendungen erscheint die Formel schon allein deshalb nicht geeignet, weil aus ihr aufgrund des Auftretens von $\sqrt{5}$ und Nennern nicht einmal vollkommen ersichtlich ist, dass es sich bei F_n um eine ganze Zahl handelt.

An dieser Stelle ist es nützlich, sich einige Dinge über Restklassen in Erinnerung zu rufen. Über allem, was jetzt folgt, steht das Motto, dass man mit Restklassen modulo p „genauso wie mit richtigen Zahlen“ rechnen kann.

* * *

Wir erinnern uns, dass eine Restklasse modulo p die Menge aller ganzen Zahlen ist, die den gleichen Rest modulo p haben. Die Menge aller Restklassen modulo p wird oft mit $\mathbb{Z}/p\mathbb{Z}$ bezeichnet, wir nennen sie jetzt $\mathbb{F}_p$. Diese Benennung wird gleich erklärt werden.
Wir führen nun eine bequeme Notation ein und identifizieren eine ganze Zahl mit ihrer Restklasse in $\mathbb{F}_p$. So können wir $0 \in \mathbb{F}_p, 1 \in \mathbb{F}_p$ und $p \in \mathbb{F}_p$ schreiben und auch $p = 0$ als Elemente von $\mathbb{F}_p$, aber $0 \neq 1$. ($a = b \in \mathbb{F}_p$ bedeutet also immer $a \equiv b \mod p$).

Die Menge $\mathbb{F}_p$ ist aber nicht nur eine Menge, sondern wir können mit ihren Elementen auch rechnen: Bekanntlich können wir zwei Restklassen addieren, subtrahieren und auch multiplizieren (aus $a \equiv a' \mod p$ und $b \equiv b' \mod p$ folgt etwa $ab \equiv a'b' \mod p$).[1]

Ganz entscheidend ist nun aber auch, dass wir zu einer Restklasse $a \neq 0 \in \mathbb{F}_p$ ein *multiplikatives Inverses* haben, eine Restklasse $\overline{a}$ (oder auch a^{-1}) mit $a \cdot \overline{a} = 1 \in \mathbb{F}_p$. Wir schreiben nun etwas provokativ für dieses Inverse auch $\overline{a} = \frac{1}{a}$ und müssen uns nur erinnern, dass wir nicht durch Null (d.h. die Null-Restklasse!) teilen dürfen.

Damit haben wir alle für uns wichtigen Eigenschaften der Menge $\mathbb{F}_p$ gesammelt, die $\mathbb{F}_p$ zu einem *Körper* machen. Dies bedeutet, dass wir addieren, subtrahieren, multiplizieren und

[1] Soweit würde das auch mit den Restklassen modulo einer beliebigen natürlichen Zahl n funktionieren, man sagt dann auch, dass diese einen *Ring* bilden.

dividieren (außer durch 0) dürfen, wobei die üblichen Gesetze (Kommutativ-, Assoziativ- und Distributivgesetz) erfüllt sind. Außerdem haben wir spezielle Elemente 0 und 1 mit $x + 0 = x$ und $x \cdot 1 = x$ für alle $x \in \mathbb{F}_p$.

Damit erklärt sich auch unsere Notation $\mathbb{F}_p$ als den *Körper mit p Elementen*, wobei $\mathbb{F}$ für *field* (englisch für *Körper*) steht.
Beispiele für andere (unendliche) Körper sind die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$. Nicht-Beispiele sind die ganzen Zahlen $\mathbb{Z}$ und die Restklassen $\mathbb{Z}/n\mathbb{Z}$, wenn n keine Primzahl ist.

Wir benötigen nun nur noch eine fundamentale Tatsache über $\mathbb{F}_p$, nämlich den kleinen Satz von Fermat, der in unserer Notation einfach $x^{p-1} = 1$ für alle $x \in \mathbb{F}_p$ mit $x \neq 0$ besagt.

* * *

Damit kommen wir wieder zu den Fibonaccizahlen. Wir wählen eine Primzahl p und möchten die Fibonaccifolge modulo p untersuchen. Wichtig ist hierbei, dass die Restklasse von F_{n+2} nur von den Restklassen von F_{n+1} und F_n abhängt. So können wir eine Fibonaccifolge F_n in $\mathbb{F}_p$ definieren mit $F_0 = 0 \in \mathbb{F}_p$ und $F_1 = 1 \in \mathbb{F}_p$ sowie $F_{n+2} = F_{n+1} + F_n$.[2]

Die entscheidende Beobachtung ist nun, dass die Herleitung der expliziten Formel oben sich fast wörtlich übertragen lässt: Angenommen, es gibt eine Zahl (=Restklasse) $\lambda \in \mathbb{F}_p$ mit $\lambda^2 = \lambda + 1$. Dann erfüllt die Folge λ^n die Rekursionsgleichung. Können wir also zwei verschiedene Lösungen $\lambda_1, \lambda_2 \in \mathbb{F}_p$ der quadratischen Gleichung $x^2 = x + 1$ finden, so ist die Folge $\frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} \in \mathbb{F}_p$ eine Folge, die die gleiche Rekursionsgleichung wie F_n erfüllt und außerdem die gleichen Anfangswerte 0 und 1 annimmt. Da die Folge durch diese beiden Bedingungen eindeutig bestimmt ist, folgt nun wiederum

$$F_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} \in \mathbb{F}_p.$$

Wohlgemerkt sind λ_1 und λ_2 nun Elemente von $\mathbb{F}_p$, also sicherlich nicht identisch mit $\frac{1 \pm \sqrt{5}}{2}$. Es ist außerdem überhaupt nicht klar, ob es diese Zahlen λ_1 und λ_2 (Nullstellen der quadratischen Gleichung über $\mathbb{F}_p$) gibt.

Wenn es sie allerdings gibt, folgt nun sofort aus dem kleinen Satz von Fermat

$$F_{n+p-1} = \frac{\lambda_1^{n+p-1} - \lambda_2^{n+p-1}}{\lambda_1 - \lambda_2} = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} = F_n \in \mathbb{F}_n$$

und somit $F_{n+p-1} \equiv F_n \mod p$, also $\kappa(p) \mid p - 1$ (d.h. $p - 1$ ist eine Periodenlänge, wenn auch nicht notwendig die kleinste).

Wir haben also einen Teil unserer Beobachtungen über $\kappa(p)$ erklärt, unter der einzigen Annahme, dass die quadratische Gleichung $x^2 - x - 1 = 0$ zwei verschiedene Lösungen in $\mathbb{F}_p$ hat. Dies ist aber offensichtlich nicht immer der Fall, für $p = 2$ ist etwa stets $x^2 - x - 1 = 1 \neq 0 \in \mathbb{F}_2$.

[2] Genau genommen sollten wir nicht die gleiche Notation für die Zahlen $F_n \in \mathbb{Z}$ und die „Zahlen“ (=Restklassen) $F_n \in \mathbb{F}_p$ verwenden, aber wir erlauben uns hier ein wenig Bequemlichkeit.

Ist nun $p > 2$, so können wir eine quadratische Ergänzung versuchen: Die Gleichung ist äquivalent zu

$$x^2 - x - 1 = 0 \Leftrightarrow 4x^2 - 4x - 4 = 0 \Leftrightarrow 4x^2 - 4x + 1 = 5 \Leftrightarrow (2x-1)^2 = 5.$$

Diese Gleichung kann also nur dann lösbar sein, wenn 5 ein quadratischer Rest modulo p ist.[3] Ist umgekehrt $a \in \mathbb{F}_p$ eine „Wurzel“ von 5, also eine Restklasse mit $a^2 = 5 \in \mathbb{F}_p$, so erhalten wir die beiden Lösungen $x = \frac{1+a}{2}$ und $x = \frac{1-a}{2}$. Diese sind verschieden, sobald $a \neq 0$ ist, also $p \neq 5$.[4]

Unsere Formel wird jetzt übrigens zu

$$F_n = \frac{\left(\frac{1+a}{2}\right)^n - \left(\frac{1-a}{2}\right)^n}{a} \in \mathbb{F}_p.$$

Wenn man sich daran erinnert, dass a „so etwas wie $\sqrt{5}$“ ist, erkennt man eine erstaunliche Ähnlichkeit mit der Formel von de Moivre und Binet.

Wir fassen unsere Ergebnisse zusammen: Ist 5 ein quadratischer Rest modulo p und $p \neq 2$ und $p \neq 5$, so gilt $\kappa(p) \mid p - 1$.

* * *

Für welche Primzahlen p tritt dieser Fall nun ein? Bei uns waren dies $p \in \{11, 19, 29, 31\}$, also die Primzahlen $p \equiv \pm 1 \mod 5$. Tatsächlich folgt aus dem *quadratischen Reziprozitätsgesetz*, dass 5 genau dann ein quadratischer Rest modulo p ist, wenn p ein quadratischer Rest modulo 5 ist. Für diesen tief liegenden und für die Zahlentheorie fundamentalen Satz ist in diesem Brief leider kein Platz.

Übung 3: Denke einen Moment über die obige Aussage nach und vergewissere dich, dass sie extrem überraschend und überhaupt nicht offensichtlich ist!

Da die quadratischen Reste modulo 5 genau 1 und 4 sind, haben wir also gezeigt, dass für $p \equiv 1, 4 \mod 5$ stets $\kappa(p) \mid p - 1$ gilt.

Damit bleiben allerdings noch die Primzahlen $p \equiv 2, 3 \mod 5$, bei denen unsere Vermutung war, dass $\kappa(p)$ etwas mit $2(p+1)$ zu tun hat.
Allein die Form dieser Vermutung sagt uns, dass es wohl keine leichte Variation dieses Arguments gibt, die auch für diese Werte von p funktioniert.

* * *

Technisch gesehen liegt unser Problem darin, dass es in dem nun betrachteten Fall im Körper $\mathbb{F}_p$ kein Element a mit $a^2 = 5$ gibt. Anders gesagt: Es gibt keine Wurzel aus 5.
Wenn ihr die Konstruktion der komplexen aus den reellen Zahlen kennt, ahnt ihr nun, worin die Lösung des Problems besteht: In den reellen Zahlen gibt es keine Wurzel aus -1. Wir lösen dieses Problem, indem wir künstlich ein Element i mit $i^2 = -1$ hinzufügen. Damit wir weiterhin „rechnen“ können (=einen Körper erhalten!), müssen wir natürlich auch alle Zahlen der Form $a+bi$ mit $a, b \in \mathbb{R}$ hinzunehmen. Dann ist Addition, Subtraktion

[3] Eine Zahl a heißt quadratischer Rest modulo p, wenn es ein x gibt mit $x^2 \equiv a \mod p$.

[4] Damit haben wir auch schon eine Erklärung dafür, warum die Primzahlen $p = 2$ und $p = 5$ nicht so recht in unser Muster passen.

und Multiplikation (letzteres unter Benutzung von $i^2 = -1$) offensichtlich möglich und auch die Division bereitet wegen

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} \cdot i$$

für $(a,b) \neq (0,0)$ kein Problem.

Wir versuchen nun, diese Konstruktion auf unseren Körper $\mathbb{F}_p$ und die Wurzel aus 5 zu übertragen. Wenn man nun etwas Angst hat, mit Zahlen zu rechnen, die es *gar nicht gibt*, kann man auch zunächst den Fall der rationalen Zahlen $\mathbb{Q}$ betrachten. Auch hier gibt es keine $\sqrt{5}$. Wir wissen aber, was $\sqrt{5}$ ist, nämlich eine reelle Zahl. Wir können also die Menge

$$\mathbb{Q}(\sqrt{5}) := \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$$

einfach als Teilmenge der reellen Zahlen auffassen. Hier wissen wir natürlich auch, wie man rechnen kann, es ist nämlich

$$(a + b\sqrt{5}) \pm (c + d\sqrt{5}) = (a \pm c) + (b \pm d)\sqrt{5} \in \mathbb{Q}(\sqrt{5})$$

sowie

$$(a + b\sqrt{5}) \cdot (c + d\sqrt{5}) = (ac + 5bd) + (bc + ad)\sqrt{5} \in \mathbb{Q}(\sqrt{5})$$

und schließlich (mit einem kleinen Trick!)

$$\frac{1}{a+b\sqrt{5}} = \frac{a-b\sqrt{5}}{(a+b\sqrt{5})(a-b\sqrt{5})} = \frac{a-b\sqrt{5}}{a^2-5b^2} = \frac{a}{a^2-5b^2} - \frac{b}{a^2-5b^2} \cdot \sqrt{5} \in \mathbb{Q}(\sqrt{5}),$$

falls $(a,b) \neq (0,0)$ (denn nur dann ist $a^2 - 5b^2 = 0$, da $\sqrt{5}$ irrational ist!).

Nachdem wir uns davon überzeugt haben, dass es hier mit rechten Dingen zugeht, versuchen wir es nun mit $\mathbb{F}_p$ und fügen ein neues Element w mit $w^2 = 5$ hinzu. Damit wir weiterhin „rechnen“ können, benötigen wir allerdings noch mehr Zahlen, unsere Grundmenge wird also zu

$$\mathbb{F}_{p^2} := \{a + bw : a, b \in \mathbb{F}_p\}.$$

Dabei hat die rechte Seite offensichtlich p^2 verschiedene Elemente und die Notation links deutet schon darauf hin, dass es sich bei $\mathbb{F}_{p^2}$ um einen Körper mit p^2 Elementen handelt.

Wir müssen nun erklären, wie man „Zahlen“ aus $\mathbb{F}_{p^2}$ addieren, subtrahieren und multiplizieren kann. Dies geht aber wortwörtlich so wie oben für $\mathbb{Q}(\sqrt{5})$ erklärt:

$$(a + bw) \pm (c + dw) = (a \pm c) + (b \pm d)w \in \mathbb{F}_{p^2},$$

$$(a + bw) \cdot (c + dw) = (ac + 5bd) + (bc + ad)w \in \mathbb{F}_{p^2}$$

sowie

$$\frac{1}{a+bw} = \frac{a-bw}{(a+bw)(a-bw)} = \frac{a-bw}{a^2-5b^2} = \frac{a}{a^2-5b^2} - \frac{b}{a^2-5b^2} \cdot w \in \mathbb{F}_{p^2}$$

für $(a,b) \neq (0,0)$ (denn nur dann ist $a^2 - 5b^2 = 0$, da 5 kein quadratischer Rest ist!).

Mit diesen Rechenoperationen wird $\mathbb{F}_{p^2}$ also tatsächlich zu einem Körper mit p^2 Elementen. Wir bemerken noch, dass dieser auf natürliche Weise den Körper $\mathbb{F}_p$ enthält.

Wie sieht es nun mit den Fibonaccizahlen aus? Wie zuvor können wir $F_0 = 0 \in \mathbb{F}_{p^2}$ und $F_1 = 1 \in \mathbb{F}_{p^2}$ sowie $F_{n+2} = F_{n+1} + F_n \in \mathbb{F}_{p^2}$ definieren. Da diese Zahlen selbst alle in $\mathbb{F}_p$ sind („sie enthalten keine $\sqrt{5}$“), folgt aus $F_{n+\ell} = F_n \in \mathbb{F}_{p^2}$ sofort $F_{n+\ell} = F_n \in \mathbb{F}_p$ und somit $F_{n+\ell} \equiv F_n \mod p$. Wir können also wieder die Fibonaccifolge in $\mathbb{F}_{p^2}$ untersuchen, um die Periodenlänge zu bestimmen.

Wie zuvor folgt auch: Gibt es zwei verschiedene Lösungen $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2}$ der quadratischen Gleichung $x^2 = x + 1$, so ist die Folge $\frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2}$ eine Folge, die die Rekursionsgleichung der Fibonaccifolge erfüllt und außerdem die gleichen Startwerte 0 und 1 besitzt. Da die Folge damit eindeutig bestimmt ist, folgt sofort

$$F_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} \in \mathbb{F}_{p^2}.$$

Bis jetzt haben wir noch nicht ausgenutzt, dass wir jetzt in $\mathbb{F}_{p^2}$ „leben“. Dies tun wir jetzt: Wie zuvor ist die Gleichung $x^2 = x + 1$ für $p > 2$ nämlich äquivalent zu $(2x - 1)^2 = 5$. Wir können also sofort zwei verschiedene Lösungen $x = \frac{1 \pm w}{2} \in \mathbb{F}_{p^2}$ hinschreiben!

Um nun daraus etwas über die Periodenlänge zu schließen, benötigen wir eine dem kleinen Satz von Fermat analoge Aussage über $\mathbb{F}_{p^2}$. Um die richtige Idee zu finden, erinnern wir uns kurz an den Beweis des kleinen Fermat.[5]

Wir nehmen uns also ein $a \in \mathbb{F}_p$ mit $a \neq 0$. Sei $x_1, x_2, \ldots, x_{p-1}$ eine Liste aller Elemente von $\mathbb{F}_p$ außer der Null. Dann besteht die Liste $ax_1, ax_2, \ldots, ax_{p-1}$ aus $p-1$ verschiedenen Elementen von $\mathbb{F}_p$ (denn wir könnten auch wieder durch a teilen!), die allesamt ungleich Null sind. Die beiden Listen stimmen also bis auf die Reihenfolge überein, insbesondere folgt

$$x_1 x_2 \ldots x_{p-1} = (ax_1)(ax_2) \ldots (ax_{p-1}) \in \mathbb{F}_p.$$

Teilen wir nun beide Seiten durch $x_1 x_2 \ldots x_{p-1} \neq 0$, so folgt sofort $a^{p-1} = 1$.

Dies beweist den kleinen Satz von Fermat und wir sehen auch sofort, wie sich das Ergebnis auf $\mathbb{F}_{p^2}$ übertragen lässt: Ist $a \in \mathbb{F}_{p^2}$ mit $a \neq 0$, so können wir die Liste $x_1, x_2, \ldots, x_{p^2-1}$ aller Elemente von $\mathbb{F}_{p^2}$ außer der Null betrachten. Wie zuvor folgt dann, dass die Liste $ax_1, ax_2, \ldots, ax_{p^2-1}$ die gleichen Elemente in anderer Reihenfolge enthält und somit

$$x_1 x_2 \ldots x_{p^2-1} = (ax_1) \ldots (ax_{p^2-1}) \in \mathbb{F}_{p^2}$$

gelten muss. Nach Division beider Seiten durch $x_1 x_2 \ldots x_{p^2-1} \neq 0$ folgt jetzt $a^{p^2-1} = 1$.

Wenden wir dieses Ergebnis mit $a = \lambda_1$ und $a = \lambda_2$ an, so folgt jetzt

$$F_{n+p^2-1} = \frac{\lambda_1^{n+p^2-1} - \lambda_2^{n+p^2-1}}{\lambda_1 - \lambda_2} = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} = F_n \in \mathbb{F}_{p^2}$$

und somit $\kappa(p) \mid p^2 - 1$. Dies ist schon interessant und nicht-trivial, aber noch nicht so stark wie erwartet bzw. erhofft.

[5] Dies ist einer der Sätze, bei dem es sich unbedingt lohnt, sich den Beweis zu merken, da man dieselbe Idee sehr häufig anwenden kann!

Um das Ergebnis zu verbessern, müssen wir benutzen, dass λ_1, λ_2 keine beliebigen Elemente von $\mathbb{F}_{p^2}$ sind, sondern eine spezielle Eigenschaft haben. Ziel ist es, eine kürzere „Liste“ von Elementen $x_1, x_2, \dots$ zu finden, die bei Multiplikation mit λ_1 bzw. λ_2 auf sich selbst übergeht.[6]

Um eine solche Liste zu finden, benötigen wir einen Trick. Zu jedem Element $\zeta = a + bw \in \mathbb{F}_{p^2}$ definieren wir die **Norm**

$$N(\zeta) = (a + bw)(a - bw) = a^2 - 5b^2 \in \mathbb{F}_p.$$

Aus der Faktorisierung sieht man nun leicht $N(\zeta_1\zeta_2) = N(\zeta_1)N(\zeta_2)$, die Norm ist *multiplikativ*. Weiter sieht man sofort, dass es genau ein Element mit Norm 0 gibt, nämlich die 0.

Übung 4: Zeige, dass jedes $c \in \mathbb{F}_p$ eine Norm ist. (Tipp: Wir suchen a, b mit $a^2 = 5b^2 + c$. Wie viele Werte nehmen die beiden Seiten an, wenn a und b alle Restklassen durchlaufen?)

Übung 5: Folgere aus Übung 4 und der Multiplikativität der Norm, dass jede Norm $c \neq 0$ gleich oft angenommen wird, es gibt also genau $\frac{p^2-1}{p-1} = p + 1$ Elemente mit Norm c.

Es ist

$$N(\lambda_1) = N(\lambda_2) = \lambda_1 \cdot \lambda_2 = \frac{1 + w}{2} \cdot \frac{1 - w}{2} = \frac{1 - w^2}{4} = -1.$$

Mithilfe von Übung 5 können wir nun mehr über $\kappa(p)$ herausfinden: Dazu betrachten wir die Liste $x_1, x_2, \dots, x_{2(p+1)}$ aller Elemente mit Norm 1 oder -1. Die Elemente $\lambda_1 x_1, \lambda_1 x_2, \dots, \lambda_1 x_{2(p+1)}$ sind nun allesamt verschieden und haben wiederum Norm 1 oder -1 (Multiplikativität der Norm!), stimmen also mit den vorigen Elementen bis auf die Reihenfolge überein. Es folgt

$$x_1 x_2 \dots x_{2(p+1)} = (\lambda_1 x_1)(\lambda_1 x_2) \dots (\lambda_1 x_{2(p+1)}) \in \mathbb{F}_{p^2}$$

und somit nach Kürzen des Produkts $\lambda_1^{2(p+1)} = 1$ und analog $\lambda_2^{2(p+1)} = 1$. Wie zuvor folgt jetzt sofort

$$F_{n+2(p+1)} = \frac{\lambda_1^{n+2(p+1)} - \lambda_2^{n+2(p+1)}}{\lambda_1 - \lambda_2} = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} = F_n \in \mathbb{F}_{p^2}$$

und somit $\kappa(p) \mid 2(p + 1)$ wie vermutet. Wir fassen zusammen:

Für $p \equiv 1, 4 \mod 5$ gilt $\kappa(p) \mid p - 1$.
Für $p \equiv 2, 3 \mod 5$ gilt $\kappa(p) \mid 2(p + 1)$.

Wir haben also gesehen, dass sich diese erstaunlich unterschiedlichen Ergebnisse mit den Eigenschaften der endlichen Körper $\mathbb{F}_p$ bzw. $\mathbb{F}_{p^2}$ erklären lassen.[7]
Daher wollen wir den restlichen Teil dieses Briefs nutzen, um noch ein wenig auf die allgemeinen Eigenschaften endlicher Körper einzugehen.

[6] Mathematiker würden auch sagen: Eine Untergruppe der multiplikativen Gruppe von $\mathbb{F}_p$, die λ_1 bzw. λ_2 enthält.

[7] Über die exakten Werte von $\kappa(p)$ ist bis auf die hier bewiesenen Eigenschaften wenig bekannt. Noch schwieriger wird es für $\kappa(p^2)$. Dazu findet man im Internet eine interessante Arbeit von Jörg Jahnel und Andreas-Stephan Elsenhans: https://www.uni-math.gwdg.de/jahnel/Preprints/Fibams4.pdf

Zur Theorie der endlichen Körper

In diesem Abschnitt geht es um die folgenden Fragen: Wie viele endliche Körper gibt es? Und was kann man allgemein über sie aussagen?

Schon die erste Frage ist natürlich schlecht gestellt: Wir kennen bereits unendlich viele endliche Körper, denn für jede Primzahl p gibt es den endlichen Körper $\mathbb{F}_p$. Wir haben außerdem für jede Primzahl, für die 5 kein quadratischer Rest ist, den Körper $\mathbb{F}_{p^2}$ durch künstliches Hinzufügen einer Quadratwurzel aus 5 konstruiert.

Natürlich ist an der 5 nichts besonders Spezielles und man kann für jede Primzahl $p > 2$ den Körper $\mathbb{F}_{p^2}$ erzeugen, indem man statt 5 einen quadratischen Nicht-Rest r wählt und dann ein w mit $w^2 = r$ hinzufügt. Übrigens ist es egal, aus welchem quadratischen Rest man die Wurzel hinzufügt, denn der Quotient zweier Nicht-Reste ist immer ein quadratischer Rest!

Auch einen Körper $\mathbb{F}_4$ mit 4 Elementen kann man konstruieren, obwohl es modulo 2 keinen quadratischen Nicht-Rest gibt. Stattdessen fügt man ein α mit $\alpha^2 + \alpha + 1 = 0$ hinzu und erhält dann $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$.

Mit einer ähnlichen Methode kann man auch Körper $\mathbb{F}_{p^n}$ für jede Primzahl p und jede natürliche Zahl $n \geq 1$ konstruieren. Statt der quadratischen Gleichung, die in $\mathbb{F}_p$ keine Lösung besitzt, benötigen wir nun ein modulo p irreduzibles Polynom P und fügen ein Element w mit $P(w) = 0$ hinzu. Dann kann man ähnlich wie zuvor zeigen, dass

$$\mathbb{F}_{p^n} := \{a_0 + a_1 w + \cdots + a_{n-1} w^{n-1} : a_0, \ldots, a_{n-1} \in \mathbb{F}_p\}$$

ein Körper mit p^n Elementen ist. Allerdings ist es nicht einmal vollkommen offensichtlich, dass es solch ein irreduzibles Polynom stets gibt, daher ersparen wir uns hier die Details. In jedem konkreten Fall (etwa $w = \sqrt[3]{2}$, falls 2 kein kubischer Rest ist,...) kann man die gewünschten Eigenschaften normalerweise mehr oder weniger leicht direkt überprüfen.

* * *

Wir wollen nun umgekehrt möglichst viel über einen beliebigen endlichen Körper K mit q Elementen herausfinden, wobei q zunächst eine beliebige natürliche Zahl ist. Für jede natürliche Zahl $n \in \mathbb{N}$ gibt es eine Zahl $n = 1 + 1 + \cdots + 1 \in K$. Da K nur endlich viele Elemente hat, gibt es eine kleinste natürliche Zahl n mit $n = 0 \in K$. Diese Zahl n heißt die Charakteristik von K.
Die bereits konstruierten Körper $\mathbb{F}_p$ und $\mathbb{F}_{p^2}$ haben jeweils die Charakteristik p. Allgemein kann man leicht zeigen, dass die Charakteristik stets eine Primzahl ist. Denn wäre $n = a \cdot b$ mit $a, b < n$, so wäre

$$0 = n = 1 + 1 + \cdots + 1 = (1 + 1 + \cdots + 1) \cdot (1 + 1 + \cdots + 1) = a \cdot b$$

und somit $a = 0$ oder $b = 0$, im Widerspruch zur Minimalität der Charakteristik n.

Sei nun K ein Körper mit q Elementen und Charakteristik p. Wir zeigen jetzt, dass q eine Potenz von p ist. Dazu bemerken wir zunächst, dass K den Körper $\mathbb{F}_p$ enthält, entsprechend den Zahlen $0, 1, 1 + 1, 1 + 1 + 1, \cdots \in K$. Jetzt wählen wir maximal viele *linear unabhängige* Elemente $x_1, \ldots, x_m \in K$. Dies bedeutet, dass

$$a_1 x_1 + \cdots + a_m x_m = 0 \in K$$

mit $a_1, \dots, a_m \in \mathbb{F}_p$ nur für $a_1 = a_2 = \cdots = a_m = 0$ möglich ist. Wir behaupten jetzt, dass

$$K = \{a_1 x_1 + \cdots + a_m x_m : a_1, \dots, a_m \in \mathbb{F}_p\}$$

ist, wobei die Elemente rechts paarweise verschieden sind. Daraus würde sofort $q = p^m$ folgen. Zum Beweis der Behauptung: Wären zwei Elemente gleich, also etwa

$$a_1 x_1 + \cdots + a_m x_m = b_1 x_1 + \cdots + b_m x_m,$$

so würde

$$(a_1 - b_1)x_1 + \cdots + (a_m - b_m)x_m = 0$$

und somit $a_1 - b_1 = \cdots = a_m - b_m = 0$, also $a_1 = b_1, \dots a_m = b_m$ folgen. Also sind die Elemente auf der rechten Seite paarweise verschieden. Wir müssen nun noch zeigen, dass jedes Element aus K von dieser Form ist. Dafür benutzen wir die Maximalität von m. Ist nämlich $x \in K$ ein beliebiges weiteres Element, so ist die Menge $\{x, x_1, \dots, x_m\}$ nach Annahme nicht linear unabhängig, es gibt also $a, a_1, \dots, a_m \in \mathbb{F}_p$, die nicht alle Null sind, mit

$$ax + a_1 x_1 + \cdots + a_m x_m = 0.$$

Wir wissen sogar, dass $a \neq 0$ ist, denn sonst wären schon $x_1, \dots, x_m$ nicht linear unabhängig. Dann können wir aber auch durch a teilen und erhalten nach Umstellen

$$x = b_1 x_1 + \cdots + b_m x_m$$

mit $b_i = -\frac{a_i}{a} \in \mathbb{F}_p$. Damit ist gezeigt, dass auch x von der gesuchten Form ist und die Behauptung $q = p^m$ folgt.[8]

Fassen wir zusammen: Jeder endliche Körper hat eine Charakteristik p, die eine Primzahl ist und die Anzahl an Elementen ist eine Potenz p^m dieser Primzahl. Umgekehrt gibt es für jede Primzahl p und jede natürliche Zahl m einen Körper $\mathbb{F}_{p^m}$ mit p^m Elementen. Man kann sogar zeigen, dass dieser im Wesentlichen eindeutig ist, sodass es erlaubt ist, von *dem* Körper mit p^m Elementen zu sprechen.

Wir beenden dieses Skript mit einem wichtigen Hinweis.

!!!Warnung!!! Für $m > 1$ hat der Körper $\mathbb{F}_{p^m}$ nichts mit den Restklassen $\mathbb{Z}/p^m\mathbb{Z}$ zu tun. In $\mathbb{F}_{p^m}$ ist $p = 0$, in $\mathbb{Z}/p^m\mathbb{Z}$ natürlich nicht. Umgekehrt gibt es Restklassen p und p^{m-1}, deren Produkt die Null-Restklasse ist, die aber beide nicht Null sind, was in einem Körper natürlich nicht sein kann.

Darin liegt aber oftmals auch die Stärke von $\mathbb{F}_{p^m}$, da es hier Objekte gibt, von denen man eigentlich denken würde, dass sie „in der Natur“ nicht vorkommen, etwa das Element $\alpha \in \mathbb{F}_4$ mit $2\alpha = 2 = 0$, aber $\alpha(\alpha + 1) = 1$.

[8] Wer schon etwas lineare Algebra kennt: Wir haben hier K als Vektorraum über dem Körper $\mathbb{F}_p$ betrachtet und gezeigt, dass $x_1, \dots, x_m$ eine Basis dieses Vektorraums ist.