Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 38 (1983)
Heft: 4

Artikel: Rechnen in endlichen Körpern (Beispiele elementarer Zahlentheorie)
Autor: Zeitler, Herbert
DOI: https://doi.org/10.5169/seals-37190

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 07.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

REFERENCES

1 C. Brezinski: Génération de suites totalement monotones et oscillantes. C.R. Acad. Sci. Paris *280*A, 729–731 (1975).
2 C. Brezinski: Padé-type approximation and general orthogonal polynomials. ISNM, Vol. 50, Birkhäuser-Verlag, Basel 1980.
3 W. Gautschi: A note on the successive remainders of the exponential series. El. Math. *37*, 46–49 (1982).
4 D.V. Widder: The Laplace transform. Princeton University Press, Princeton, N.J., 1946.

© 1983 Birkhäuser Verlag, Basel 0013-6018/83/040086-04$1.50 + 0.20/0

Rechnen in endlichen Körpern
(Beispiele elementarer Zahlentheorie)

Einleitung

Wir gehen von einem Restklassenkörper **K** ungerader Ordnung aus. Dann gilt also $|\mathbf{K}| = p$ mit p Primzahl und $p \neq 2$.
Bekanntlich lässt sich jede Primzahl $p \neq 2$ entweder in der Form $p = 4a + 1$ oder aber in der Form $p = 4a - 1$ mit $a \in \mathbf{N}$ darstellen. Im ersten Fall ist -1 Quadrat in **K**, im zweiten dagegen nicht. Mit $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$ schreiben wir $-1 \in \mathbf{K}^{*2}$ bzw. $-1 \notin \mathbf{K}^2$ [1], [3].

Das Problem

Wie viele Lösungen (x^2, y^2) *mit* $x, y \in \mathbf{K}^*$ *besitzt die Gleichung*

$$x^2 - y^2 = 1. \tag{1}$$

Die Lösung des Problems

Die Gleichung (1) besitzt genau $a - 1$ *Lösungen der genannten Art.*

Mit den bei der Behandlung diophantischer Gleichungen in **N** üblichen Verfahren [2] schreiben wir $x^2 - y^2 = (x - y)(x + y) = 1$ und setzen $x - y = v$ und $x + y = w$. Es gilt $v, w \in \mathbf{K}^*$. Weiter erhalten wir

$$w = \frac{1}{v}, \qquad x = \frac{1 + v^2}{2v}, \qquad y = \frac{1 - v^2}{2v}.$$

a) Sei v ein beliebiges Element aus $\mathbf{K}^*$. Dann folgt mit $x = (1 + v^2)/(2v)$ und $y = (1 - v^2)/(2v)$ durch Einsetzen und Ausrechnen sofort $x^2 - y^2 = 1$.
b) Seien nun umgekehrt $x, y \in \mathbf{K}^*$ mit $x^2 - y^2 = 1$ gegeben. Dann existiert mindestens ein $v \in \mathbf{K}^*$ so, dass $x = (1 + v^2)/(2v)$, $y = (1 - v^2)/(2v)$.

Beweis: Es gibt jedenfalls mindestens ein $v \in \mathbf{K}^*$ so, dass $x^2 = (v+y)^2$. Daraus folgt sofort $x^2 - y^2 = v^2 + 2vy$ und mit $x^2 - y^2 = 1$ weiter $y = (1-v^2)/(2v)$. Einsetzen dieses Ergebnisses liefert schliesslich

$$x^2 = \left(v + \frac{1-v^2}{2v}\right)^2 = \left(\frac{1+v^2}{2v}\right)^2, \qquad \text{also} \quad x = \pm \frac{1+v^2}{2v}.$$

c) Wir wissen $v \neq 0$. Wegen $x \neq 0$ und $y \neq 0$ sind vermutlich weitere Werte von v unbrauchbar. Welche?
Aus $y = 0$ folgt $v^2 = 1$, also $v = \pm 1$.
Aus $x = 0$ folgt $v^2 = -1$, also $v = \pm\sqrt{-1}$. Im Falle $p = 4a - 1$ tritt dies wegen $-1 \notin \mathbf{K}^2$ nicht ein, wohl aber im Falle $p = 4a + 1$.
Deshalb gilt
für $p = 4a - 1$: Restliche Werte $v \in \mathbf{K} \setminus \{0, \pm 1\}$, ihre Anzahl $n_1 = p - 3 = 4a - 4$,
für $p = 4a + 1$: Restliche Werte $v \in \mathbf{K} \setminus \{0, \pm 1, \pm\sqrt{-1}\}$, ihre Anzahl $n_2 = p - 5 = 4a - 4$.
d) Der Übergang von v nach $-v$ liefert äquivalente Lösungen (x^2, y^2). Gibt es noch weitere äquivalente Lösungen? Zur Beantwortung dieser Frage müssen wir feststellen, für welche $r \in \mathbf{K}^*$ mit $r \neq v$ gilt:

$$\frac{1+r^2}{2r} = \pm \frac{1+v^2}{2v} \quad \text{und} \quad \frac{1-r^2}{2r} = \pm \frac{1-v^2}{2v}.$$

(Die Äquivalenzen

$$\frac{1+r^2}{2r} = \pm \frac{1-v^2}{2v} \quad \text{und} \quad \frac{1-r^2}{2r} = \pm \frac{1+v^2}{2v}$$

können nicht auftreten.)

Sei etwa $(1+r^2)/(2r) = (1+v^2)/(2v)$. Dann folgt $rv(r-v) = (r-v)$ und mit $r \neq v$ weiter $r = 1/v$. Auf diese Weise fortfahrend, ergeben sich neben $r = -v$ nur noch zwei brauchbare Werte, nämlich $r = 1/v$ und $r = -1/v$.
Von den in Abschnitt c angegebenen Werten für v kann also jeweils nur der vierte Teil verwendet werden.
Für die Gesamtzahl der Lösungen (x^2, y^2) unserer Gleichung (1) ergibt sich also in jedem Fall

$$\frac{1}{4} n_1 = \frac{1}{4} n_2 = a - 1.$$

Erste Erweiterung

$$x^2 - y^2 = a^2 \quad \text{mit} \quad a \in \mathbf{K}^*. \tag{2}$$

Auch diese Gleichung besitzt genau $a-1$ Lösungen (x^2, y^2) mit $x, y \in \mathbf{K}^*$.

Der Beweis ergibt sich durch Division mit a^2. Denn dann erhält man

$$\left(\frac{x}{a}\right)^2 - \left(\frac{y}{a}\right)^2 = 1,$$

also eine Gleichung der Form (1).

Zweite Erweiterung

$$x^2 - y^2 = a \quad \text{mit} \quad a \notin \mathbf{K}^2. \tag{3}$$

Diese Gleichung besitzt im Falle $p = 4a - 1$, also $-1 \notin \mathbf{K}^2$ genau $a-1$, im Falle $p = 4a + 1$, also $-1 \in \mathbf{K}^{*2}$ genau a Lösungen (x^2, y^2) mit $x, y \in \mathbf{K}^*$.

Für den ersten Fall ergibt sich der Beweis durch Multiplikation mit -1. Dann erhält man $-x^2 + y^2 = -a$. Weil nach [2] aus $-1 \notin \mathbf{K}^2$ und $a \notin \mathbf{K}^2$ folgt $-a \in \mathbf{K}^{*2}$, handelt es sich um eine Gleichung der Form (2).
Im zweiten Fall muss der Beweis zu (1) wiederholt werden. Dabei ändert sich das Ergebnis c. Die Anzahl brauchbarer Werte für v beträgt nämlich dann genau $4a$.

Zahlenbeispiele

$p = 4a - 1$

$a = 5$, $p = 19$, $\mathbf{K}^{*2} = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$
$x^2 - y^2 = a^2 \in \mathbf{K}^{*2}$

a^2	Lösungen			
1	(5,4),	(6,5),	(7,6),	(17,16)
4	(11,7),	(9,5),	(5,1),	(1,16)
5	(16,11),	(11,6),	(9,4),	(6,1)
6	(17,11),	(11,5),	(7,1),	(4,17)
7	(16,9),	(11,4),	(5,17),	(4,16)
9	(16,7),	(1,11),	(6,16),	(7,17)
11	(17,6),	(16,5),	(1,9),	(9,17)
16	(17,1),	(1,4),	(4,7),	(6,9)
17	(4,6),	(5,7),	(7,9),	(9,11)

$x^2-y^2=a\notin \mathbf{K}^2$

a	Lösungen			
2	(11,9),	(9,7),	(7,5),	(6,4)
3	(9,6),	(7,4),	(4,1),	(1,17)
8	(17,9),	(9,1),	(5,16),	(6,17)
10	(17,7),	(16,6),	(11,1),	(7,16)
12	(17,5),	(16,4),	(4,11),	(9,16)
13	(17,4),	(1,7),	(5,11),	(11,17)
14	(1,6),	(4,9),	(6,11),	(11,16)
15	(16,1),	(1,5),	(5,9),	(7,11)
18	(4,5),	(5,6),	(6,7),	(16,17)

$p=4a+1$

$a=4,\ p=17,\ \mathbf{K}^{*2}=\{1,2,4,8,9,13,15,16\}$

$x^2-y^2=a^2\in \mathbf{K}^{*2}$

a^2	Lösungen		
1	(16,15),	(9,8),	(2,1)
2	(15,13),	(4,2),	(1,16)
4	(13,9),	(8,4),	(2,15)
8	(16,8),	(9,1),	(4,13)
9	(13,4),	(1,9),	(8,16)
13	(15,2),	(4,8),	(9,13)
15	(16,1),	(2,4),	(13,15)
16	(1,2),	(8,9),	(15,16)

$x^2-y^2=a\notin \mathbf{K}^2$

a	Lösungen			
3	(16,13),	(4,1),	(1,15),	(2,16)
5	(13,8),	(9,4),	(1,13),	(4,16)
6	(15,9),	(8,2),	(2,13),	(4,15)
7	(16,9),	(15,8),	(9,2),	(8,1)
10	(1,8),	(2,9),	(8,15),	(9,16)
11	(15,4),	(13,2),	(2,8),	(9,15)
12	(16,4),	(13,1),	(4,9),	(8,13)
14	(16,2),	(15,1),	(1,4),	(13,16)

Ausblick

Wir gehen jetzt vom Restklassenkörper ungerader Ordnung p über zum Galois-Feld $GF(q)$ ungerader Ordnung $q=p^e$ mit $e\in \mathbf{N}$.
Anzahl der Lösungen (x^2,y^2) von (1) und (2) mit $x,y\in GF(q)^*$

$$\text{für}\quad -1\notin \mathbf{K}^2:\ \frac{1}{4}(p^e-e-2),\qquad\qquad \text{für}\quad -1\in \mathbf{K}^{*2}:\ \frac{1}{4}(p^e-e-4).$$

Anzahl der Lösungen (x^2, y^2) von (3) mit $x, y \in GF(q)^*$

$$\text{für} \quad -1 \notin \mathbf{K}^2 : \frac{1}{4}(p^e - e - 2), \qquad \text{für} \quad -1 \in \mathbf{K}^{*2} : \frac{1}{4}(p^e - e).$$

Die Überprüfung dieser Ergebnisse, die Auffindung der Lösungsanzahlen für die Gleichung $x^2 - y^2 = 0$ sowie die Untersuchung für Galois-Felder gerader Ordnung überlassen wir dem Leser.

Herbert Zeitler, Math. Institut der Universität Bayreuth, Bayreuth

LITERATURVERZEICHNIS

1 L.E. Dickson: Linear Groups. Leipzig 1901.
2 G.H. Hardy und E.M. Wright: Einführung in die Zahlentheorie. München 1958.
3 K. Radbruch: Algebraische Strukturen und elementare Zahlentheorie (Mathematik SII). Freiburg 1975.

© 1983 Birkhäuser Verlag, Basel 0013-6018/83/040089-05$1.50 + 0.20/0

Linear operators satisfying the chain rule

In computational calculus the derivative is treated as a formal operator satisfying certain functional relationships. This leads to the question of which properties of the derivative characterize that operator on the elementary functions, i.e., the rational, logarithmic, exponential, trigonometric and inverse trigonometric functions. In this note we will show that, provided we rule out trivial cases, any operator, which acts on a suitable collection of functions containing the elementary functions and which is both linear and satisfies the chain rule formula must agree with the derivative on the elementary functions.

We begin by describing the functions on which our operators act. If f and g are two real-valued functions with domains contained in R, the real numbers, and $c \in R$, let $f+g$, fg, cf, $f \circ g$, f/g denote the usual pointwise operations of addition, multiplication, scalar multiplication, composition, and division, each defined on its natural domain (the largest set on which the resulting formula makes sense). Let F denote any set of real-valued functions with non-empty domains contained in R satisfying the following properties.

1. F is closed under addition, multiplication and scalar multiplication.
2. If f and g are in F, then $f \circ g$ and f/g are also in F whenever their natural domains are non-empty.
3. $i(x) \equiv x$ and $u(x) \equiv 1$ are in F. Observe that any such F is an algebra of real-valued functions which contains the rational functions. In what follows we shall use the facts that for all $f \in F, f \circ i \in F$; and if we set $t(x) = x + r$, with $r \in R, f \circ t \in F$.