Damen, Läufer, Türme, Primzahlen, Modulo

Bernhard Ganter

Institut für Algebra
TU Dresden
D-01062 Dresden
bernhard.ganter@tu-dresden.de

Zahlentheorie, die Königin

Als *Königsdisziplin der Mathematik* bezeichnet man gelegentlich die **Zahlentheorie**.

Gemeint ist die Theorie der *ganzen* Zahlen.

Besonders geheimnisvoll und schwierig ist die Lehre von den Primzahlen.

In den letzten Jahrzehnten hat sich gezeigt, dass die Zahlentheorie wichtige praktische Anwendungen z.B. für die Kryptologie liefert.

Gaußsche ganze Zahlen

Wir haben die komplexen Zahlen kennen gelernt als

$$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}.$$

Von besonderen Interesse sind natürlich die komplexen Zahlen mit ganzzahligem Real- und Imaginärteil, also

$$\{a + bi \mid a, b \in \mathbb{Z}\}.$$

Zu Ehren von C.F.Gauß nennt man diese Zahlen die Gaußschen ganzen Zahlen.

Gaußsche Primzahlen

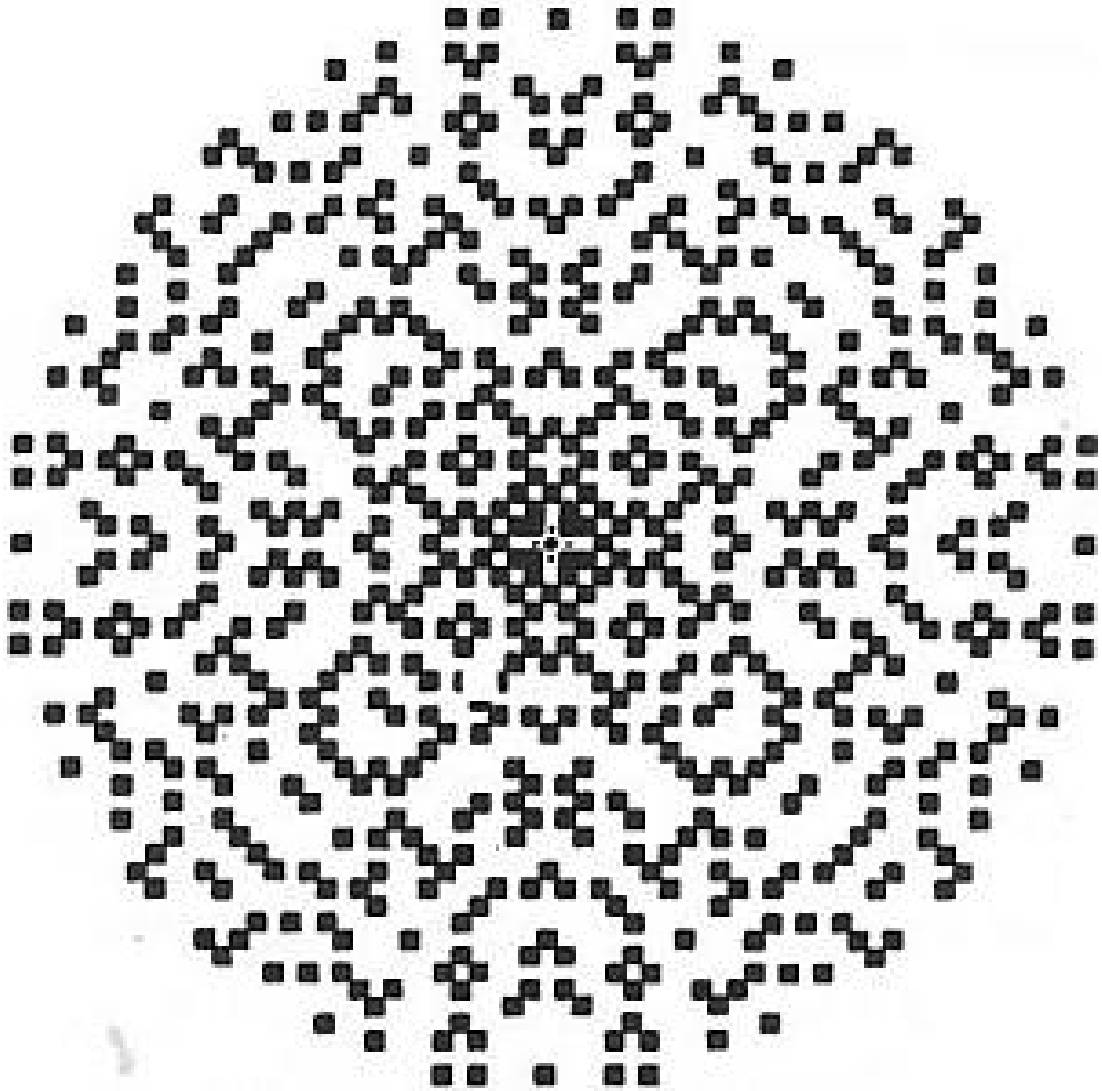
Wenn man sich die komplexen Zahlen durch die Anschauungsebene veranschaulicht, dann entsprechen die Gaußschen ganzen Zahlen gerade den Gitterpunkten des karierten Papiers.

Man kann nun eine *komplexe Zahlentheorie* anfangen.

Naheliegend ist die Frage nach *komplexen Primzahlen*.

Eine Gaußsche ganze Zahl p ist eine (Gaußsche) Primzahl, wenn sie nicht als ein Produkt anderer Gaußscher ganzer Zahlen (Teiler sind nur $1, -1, p, -p$) geschrieben werden kann.

Kleine Gaußsche Primzahlen



Eine kleine Überraschung

Man erwartet vielleicht naiv, dass der Begriff der Gaußschen Primzahl den der gewöhnlichen Primzahl verallgemeinert.

Aber Vorsicht:

$$5 = (2 + i) \cdot (2 - i) \quad = 2^2 + 1^2.$$

Die Zahl 5 ist *keine* Gaußsche Primzahl!

Reelle komplexe Primzahlen

Es stellt sich sogleich die Frage: Welche gewöhnlichen Primzahlen sind auch komplex prim?

Die Antwort ist einfach: Wenn eine gewöhnliche Primzahl p Summe zweier Quadrate ist, wenn also

$$p = a^2 + b^2,$$

dann ist sie *keine* komplexe Primzahl, denn dann gilt

$$p = (a + bi)(a - bi).$$

Umgekehrt gilt: Jede gewöhnliche Primzahl, die *nicht* Summe zweier Quadrate (reeller ganzer Zahlen) ist, ist auch eine Gaußsche Primzahl.

$p = a^2 + b^2$?

Welche (gewöhnlichen) Primzahlen sind Summe zweier Quadrate?

Rechnet man modulo 4, so bekommt man ein erstes Ergebnis:
Beim Quadrieren modulo 4 findet man

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 0, \quad 3^2 \equiv 1 \pmod 4.$$

Für ganz Zahlen a und b hat man also immer

$$a^2 + b^2 \not\equiv 3 \pmod 4.$$

Ein Teilergebnis

Wir wissen nun

- $2 = 1^2 + 1^2$.
- (Prim-) Zahlen der Form $\equiv 3 \pmod 4$ sind niemals Summe zweier Quadrate.
- $5 = 2^2 + 1^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4 + 2$, $29 = 2^2 + 5^2$,...

Das bedeutet:

- Die Zahl 2 ist keine komplexe Primzahl.
- Primzahlen der Form $\equiv 3 \pmod 4$ sind auch Gaußsche Primzahlen.
- Ob es eine ganze Zahl $\equiv 1 \pmod 4$ gibt, die eine Gaußsche Primzahl ist, bleibt unklar.

Ein Forschungsproblem

Die Frage, welche gewöhnlichen Primzahlen auch komplex Primzahlen sind, haben wir bis auf ein Problemchen lösen können. Die offene Teilfrage lautet:

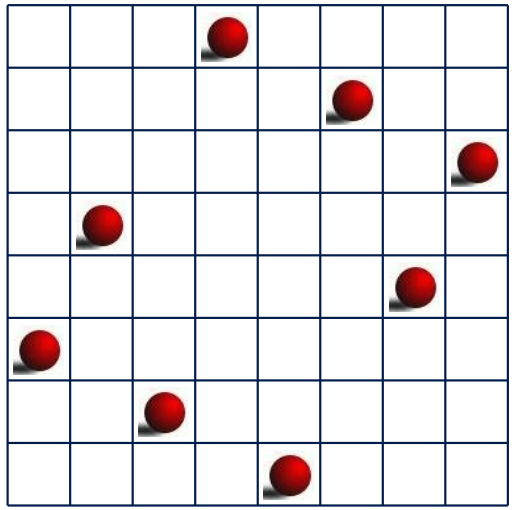
> *Welche Primzahlen* $p \equiv 1 \pmod 4$ *sind Summe zweier Quadrate?*

Das Achtköniginnenproblem

In der Zeitschrift der Berliner Schachgesellschaft erschien 1848 das Problem, auf welche Weisen es möglich sei,

> *„acht Schachfiguren, von denen jede den Rang einer Königin hat, auf dem Brett so aufzustellen, dass keine von einer anderen geschlagen werden kann.*

Das Problem machte bald als das *Achtköniginnenproblem* Furore. Die vollständige Reihe aller 92 Lösungen ist seit 1850 bekannt.



Das n-Damen-Problem

Die naheliegende Verallgemeinerung, nämlich n Damen auf einem $n \times n$-Brett entsprechend zu postieren, ist für kleine n heute eine beliebte Programmierübung.

Die Anzahl der Lösungen bis $n = 11$ ist seit 1904 bekannt. Heute kennt man die Anzahlen bis $n = 23$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
	1	0	0	2	10	4	40	92	352	724	2680	14200	73712

Eine allgemeine Formel für die Anzahl der Lösungen kennt man nicht.
Man vermutet, dass es eine Konstante c (ungefähr 2.54) gibt mit

$$L(n) \sim \frac{n!}{c^n}.$$

n Türme, n Läufer

Eine Lösung des n-Damen-Problems ist offenbar gleichzeitig eine Lösung des n-Türme–Problems und des n-Läufer-Problems, denn die Dame hat ja die Zugmöglichkeiten des Läufers und des Turms.

Eine Lösung des n-Türme-Problems ist genau dann gegeben, wenn sich in jeder Zeile und in jeder Spalte des Schachbretts genau ein Turm aufhält.

n Türme

Wir bezeichnen die Spalten des (verallgemeinerten) Schachbretts von links nach rechts mit $0, 1, \ldots, n-1$, und die Zeilen von unten nach oben ebenso.

Wir schreiben $\varphi(i)$ für die Zeile, in der sich der Turm aus Spalte i aufhält.

Eine Lösung des n-Türme-Problems ist genau dann gegeben, wenn die Abbildung

$$\varphi : \{0, 1, \ldots, n-1\} \to \{0, 1, \ldots, n-1\}$$

eine Permutation ist.

n Läufer

Damit eine Lösung des n-Türme-Problems auch eine Lösung des n-Läufer-Problems ist, muss für alle $i, j \in \{0, 1, \ldots, n-1\}$ gelten

- $\varphi(i) - \varphi(j) = i - j \quad \Longrightarrow \quad i = j$ und
- $\varphi(i) - \varphi(j) = j - i \quad \Longrightarrow \quad i = j.$

Umformuliert:

- $\varphi(i) - i = \varphi(j) - j \quad \Longrightarrow \quad i = j$ und
- $\varphi(i) + i = \varphi(j) + j \quad \Longrightarrow \quad i = j.$

Die Lösungen des n-Damen-Problems entsprechen also genau den Permutationen φ, welche diese Bedingungen erfüllen.

Hinreichende Bedingung

Wir verschärfen diese Bedingungen etwas, um sie leichter handhaben zu können. Wir finden dann vielleicht nicht alle Lösungen, aber hoffentlich noch einige.

- $\varphi(i) - i \equiv \varphi(j) - j \pmod{n} \quad \Longrightarrow \quad i = j \quad$ und
- $\varphi(i) + i \equiv \varphi(j) + j \pmod{n} \quad \Longrightarrow \quad i = j.$

Anders formuliert: Die Abbildungen

- $i \mapsto \varphi(i)$,
- $i \mapsto \varphi(i) - i \mod n \quad$ und
- $i \mapsto \varphi(i) + i \mod n$

sollen allesamt Permutationen sein.

Ein Konstruktionsversuch

Wir probieren, ob wir mit dem Ansatz

$$\varphi(i) := a \cdot i + b \mod n$$

Lösungen finden.

Hilfssatz

Die Abbildung

$$i \mapsto a \cdot i + b \mod n$$

ist genau dann bijektiv, wenn a zu n teilerfremd ist.

Für $\mathrm{ggT}(a, n) = 1$ erhalten wir also eine Lösung des n-Türme–Problems.

Lösungen für das Damenproblem

Wann liefert der Lösungsansatz auch eine Lösung des n-Damen-Problems? Die hinreichenden Bedingungen sind, dass die drei Abbildungen

- $i \mapsto \varphi(i) \quad = a \cdot i + b,$
- $i \mapsto \varphi(i) - i \quad = (a-1) \cdot i + b \quad$ und
- $i \mapsto \varphi(i) + i \quad = (a+1) \cdot i + b$

Permutationen sein müssen.

Hilfssatz

Der Ansatz

$$\varphi(i) := a \cdot i + b \mod n$$

führt auf eine Lösung des n-Damen–Problems, wenn die Zahlen $a-1$, a *und* $a+1$ *alle teilerfremd zu* n *sind.*

Das Ergebnis

Satz

Mit Hilfe des Ansatzes

$$\varphi(i) := a \cdot i + b \mod n$$

erhalten wir Lösungen des n-Damen–Problems für alle n, die weder durch zwei noch durch drei teilbar sind, also für

$$n \equiv \pm 1 \pmod 6.$$

Wir nennen die so gefundenen Lösungen **regulär**.

Die Anzahl der regulären Lösungen

Es ist nicht ganz einfach, für vorgegebenes n die Anzahl der regulären Lösungen zu bestimmen. Leicht ist es für Primzahlen:

Satz

Die Anzahl $L_r(p)$ der regulären Lösungen des p-Damen–Problems, $p \neq 2$ prim, ist

$$L_r(p) = p(p-3).$$

Beweis.

Der Ansatz $\varphi(i) := a \cdot i + b \mod p$ führt zum Erfolg für alle b und für alle a außer $0, 1, p-1$. □

Symmetrische Lösungen

Die Anzahl der regulären Lösungen ist von der Form

$$L_r(n) = 8x + 4y + 2z.$$

Dabei ist $8x$ die Anzahl der Lösungen ohne Symmetrie, $4y$ die Anzahl der Lösungen, die eine $180°$-Drehsymmetrie, aber keine $90°$-Drehsymmetrie aufweisen und $2z$ die Anzahl der Lösungen, die $90°$-drehsymmetrisch (**doppelt symmetrisch**) sind.

Es gibt doppelt symmetrische Lösungen

Wir haben für Primzahlen $p \neq 2$:

$$L_r(p) = p(p-3) = 8x + 4y + 2z.$$

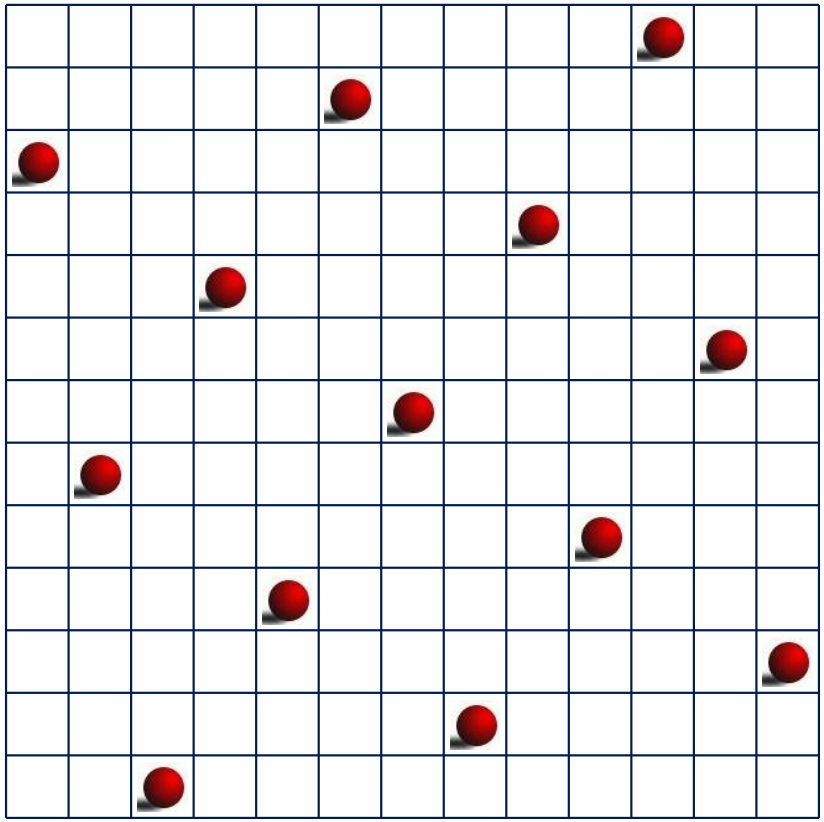
Dabei gilt

$$p(p-3) \bmod 4 = \begin{cases} 2 & \text{falls } p \equiv 1 \pmod 4, \\ 0 & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

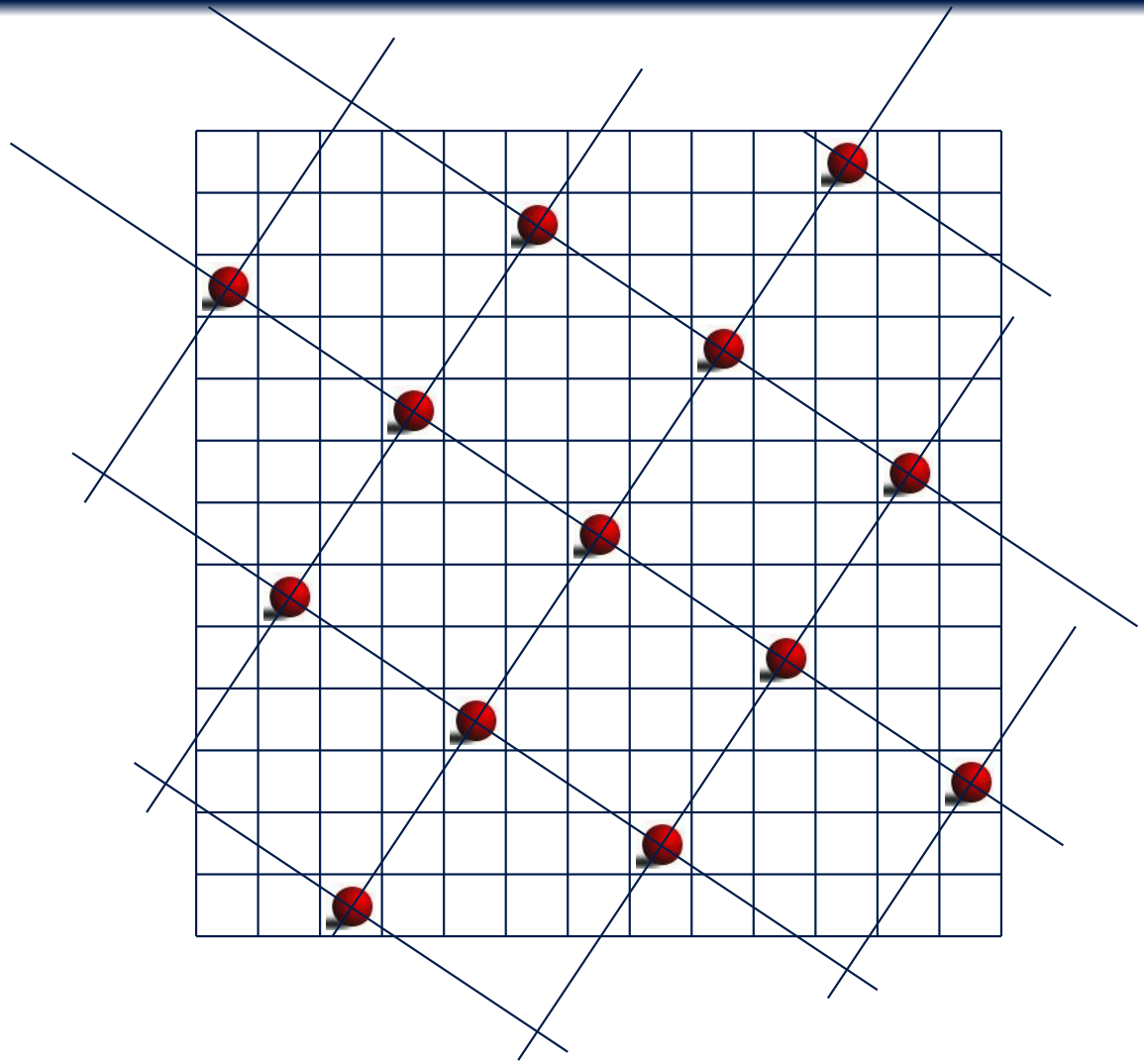
Satz

Wenn p eine Primzahl $\equiv 1 \pmod 4$ ist, dann gibt es eine doppelt symmetrische Lösung des p-Damen–Problems.

13 Damen, doppelt symmetrisch



13 Damen



13 Quadrate der Seitenlänge $\sqrt{2^2 + 3^2}$ überdecken das Spielfeld.

Überdeckung mit Quadraten

- Wenn es eine doppelt symmetrische Lösung des n-Damen–Problems gibt, dann kann das Spielfeld mit n Quadraten der Seitenlänge $\sqrt{u^2 + v^2}$ überdeckt werden.
- Jedes dieser Quadrate hat den Flächeninhalt n.
- Es ist dann $n = (\sqrt{u^2 + v^2})^2 = u^2 + v^2$. Die Zahl n ist dann also die Summe zweier Quadrate.
- Wenn $p \equiv 1 \pmod 4$ eine Primzahl ist, dann gibt es eine doppelt symmetrische Lösung des p-Damen–Problems.

Also:

Ein Lemma von Fermat

Lemma

Eine Primzahl ist genau dann die Summe zweier Quadrate ganzer Zahlen, wenn sie nicht $\equiv 3 \pmod 4$ *ist.*

Die Antwort!

Satz

Eine gewöhnliche Primzahl ist genau dann eine Gaußsche Primzahl, wenn sie $\equiv 3 \pmod 4$ *ist.*