

## Inhaltsverzeichnis Vorlesung Zahlentheorie

1. Elementare Zahlentheorie, sehr summarisch  
Teilbarkeit, euklidischer Algorithmus, eindeutige Primfaktorzerlegung, einige einfache Konsequenzen: Irrationalitätsbeweise, Quintenzirkel und wohltemperierte Stimmung.
2. Die Struktur der Restklassenringe  
Chinesischer Restsatz, Zerlegung der Einheitengruppen, Eulersche Phi-Funktion, kleiner Fermatscher Satz, Struktur der primen Restklassengruppe  $\text{mod } p^n$ , Primitivwurzeln. Anwendungen auf die Elementarmathematik: Teilbarkeitsregeln, Periodizität von Dezimalbruchentwicklungen.
3. Quadratische Reste  
Das Legendresymbol und seine Rolle als Gruppenhomomorphismus, das Eulersche Kriterium, quadratisches Reziprozitätsgesetz, Gaußsche Summen. Primzahlen in Restklassen.
4. Zahlentheorie im Gaußschen Zahlkörper  
Eindeutige Primfaktorzerlegung, Zerlegung und Verzweigung rationaler Primzahlen, Summen von zwei bzw. vier Quadraten ganzrationaler Zahlen
5. Ein elementarer Zugang zur Primzahlverteilung  
Unendlichkeit der Primzahlmenge, Sieb des Eratosthenes, Satz von Tschebyscheff
6. Die Riemannsche Zetafunktion  
Konvergenz, Eulerprodukt, einige andere Dirichletreihen mit zahlentheoretisch interessanten Koeffizienten, Fortsetzung auf die Halbebene  $\text{Re } s > 0$  und Verhalten in  $s = 1$
7. Exkurs: Einige Diophantische Probleme  
Pythagoräische Zahlentripel, das Fermat-Problem, der Fermatsche Satz für den Exponenten 4, die  $abc$ -Vermutung und ihr Analogon für Polynome
8. Die Thetafunktion  
Die Rolle der Thetafunktion als erzeugende Funktion und als Modulform. Poisson'sche Summenformel, Funktionalgleichung und Fortsetzbarkeit der Zetafunktion
9. Die Nullstellen der Zetafunktion  
Was man über die Gammafunktion wissen sollte. Nichtverschwinden der Zetafunktion auf der Geraden  $\text{Re } s > 0$ , Riemannsche Vermutung

10. Der Primzahlsatz  
Die von-Mangoldt-Funktion und ein Beweis des Primzahlsatzes
11. Ganze algebraische Zahlen  
Algebraische und transzendente Zahlen. Beispiele. Zahlkörper. Ganze algebraische Zahlen. Irreduzible Polynome und das Eisensteinsche Kriterium. Der Ring der ganzen algebraischen Zahlen eines Zahlkörpers. Quadratische und Kreisteilungskörper
12. Ideale in den Ringen ganzer Zahlen von Zahlkörpern.  
Summen und Produkte. Teilerfremdheit. Chinesischer Restsatz. Restklassenringe und Restklassenkörper
13. Ganzalgebraische Zahlen und Gitter  
Algebraische Konjugationen, Wirkung auf Elemente und Ideale. Spur und Norm. Diskriminante. Einbettung von  $K$  und  $\mathcal{O}_K$  in den  $\mathbf{R}^n$ . Der Ring der ganzen Zahlen als Gitter, Ideale als Untergitter. Warum es in  $\mathcal{O}_K$  meistens keine eindeutige Primfaktorzerlegung gibt. Euklidische Ringe quadratischer Zahlen
14. Kettenbrüche  
Der Kettenbruchalgorithmus. Endliche, unendliche und periodische Kettenbrüche. Konvergenz. Approximationseigenschaften.
15. Pellische Gleichung und reell-quadratische Grundeinheiten  
Gute Approximationen von  $\sqrt{d}$  als Lösungen der Pellischen Gleichung. Dirichletscher Einheitensatz; der Spezialfall reell-quadratischer Zahlkörper.
16. Eindeutige Primidealzerlegung, Klassenzahl  
Die multiplikative Gruppe der gebrochenen Ideale. Idealklassen und die Klassenzahl. Die neue Rolle der Primideale als erzeugende Elemente.
17. Zerlegung von Primzahlen in den Ringen  $\mathcal{O}_K$   
Zerlegung, Verzweigung und Restklassenerweiterung: allgemein und im Spezialfall der quadratischen Zahlkörper. Charakterisierung des Verzweigungsverhaltens in quadratischen Zahlkörpern durch das Legendresymbol. Warum das quadratische Reziprozitätsgesetz so wichtig ist.
18. Gitter und Klassenzahlen  
Der Minkowskische Gitterpunktsatz. Kleinste Elementnormen in Idealen. Kleinste Idealnomen in Idealklassen. Bestimmung der Klassenzahl in einigen handlichen Fällen. Warum einige imaginärquadratische Zahlringe eindeutige Primfaktorzerlegung besitzen, aber keinesfalls euklidisch sind.
19. Binäre quadratische Formen: Reduktion und Klassenzahl  
Komposition und Äquivalenz binärer quadratischer Formen. Klassenzahl und Fundamentalbereich der elliptischen Modulgruppe.

## Literaturempfehlungen

- J. Brüder: Einführung in die analytische Zahlentheorie (Springer)  
K. Ireland, M. Rosen: A Classical Introduction to Modern Number Theory (Springer)  
St. Müller–Stach, J. Piontkowski: Elementare und algebraische Zahlentheorie (Vieweg)  
A. Schmidt: Einführung in die algebraische Zahlentheorie (Springer)  
J. Steuding: Diophantine Analysis (Chapman & Hall)  
J. Wolfart: Einführung in die Zahlentheorie und Algebra (Vieweg)

## Übungsaufgaben zur Zahlentheorie

1. Man zeige: Wenn  $2^n - 1$  eine Primzahl ist, dann auch  $n$ . Gilt die Umkehrung?
2. Man zeige: Wenn  $2^n + 1$  eine Primzahl ist, dann ist  $n$  eine Zweierpotenz.
3. Man beweise die Teilbarkeit  $m!n! \mid (n+m)!$  für alle natürlichen  $m, n > 0$ .
4. Sei  $n > 0$  eine natürliche Zahl. Beweisen Sie, dass eine natürliche Zahl  $m$  existiert mit
$$(\sqrt{2} - 1)^n = \sqrt{m+1} - \sqrt{m}.$$
5. Finden Sie alle natürlichen Zahlen  $n$  mit der Eigenschaft  $\varphi(n) = n/3$ .
6.  $p^s$  sei eine ungerade Primpotenz. Zeigen Sie, dass die prime Restklassengruppe  $(\mathbf{Z}/p^s\mathbf{Z})^*$  genau  $\varphi(\varphi(p^s))$  erzeugende Elemente besitzt.
7. Man beweise:  $\frac{1}{97}$  hat eine Dezimalbruchentwicklung mit Periodenlänge 96.
8. Zeigen Sie: Jede Primzahl  $p$  außer 2 und 5 teilt unendlich viele der Zahlen 11, 111, 1111, 11111, ...
9. Unter welchen Bedingungen an die ungerade Primzahl  $p$  ist jeder quadratische Nichtrest  $\pmod{p}$  gleichzeitig eine Primitivwurzel?
10. Fortsetzung: Zeigen Sie, dass für Fermat–Primzahlen  $p = 2^{2^n} + 1$ ,  $n > 0$ , die Zahl 3 eine Primitivwurzel ist.
11. Sei  $p > 2$  eine Primzahl. Man beweise, dass die Kongruenz  $x^4 \equiv -1 \pmod{p}$  genau dann lösbar ist, wenn  $p \equiv 1 \pmod{8}$ .
12. Beweisen Sie den Wilson’schen Satz  $(p-1)! \equiv -1 \pmod{p}$ .
13. Betrachten Sie Kongruenzen modulo möglicher Primteiler von Fermat–Zahlen  $F_n := 2^{2^n} + 1$  und leiten Sie daraus her: Je zwei verschiedene Fermat–Zahlen sind teilerfremd. (Folgerung: Es gibt unendlich viele Primzahlen.)

14. Man beweise  $2 \cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{2}$  mit Hilfe einer Gaußschen Summe.
15. Zerlegen Sie die Zahlen 35, 36,  $2 + 3i$ ,  $7 + i$  in Primfaktoren des Rings  $\mathbf{Z}[i]$  der Gaußschen ganzen Zahlen.
16. Wieviele (modulo Reihenfolge) verschiedene Darstellungen der Zahlen 85, 89, 93, 97, 101 als Summe von zwei Quadraten natürlicher Zahlen gibt es?
17.  $f(t) = at^2 + bt + c$  sei ein quadratisches Polynom in  $\mathbf{F}_p[t]$ ,  $p$  prim. Entwickeln Sie ein Verfahren, die Exponentialsumme  $\sum_{t \bmod p} \zeta_p^{f(t)}$  zu berechnen.
18.  $p$  sei eine Primzahl. Wieviele Punkte liegen auf dem Einheitskreis  $x^2 + y^2 = 1$  des  $\mathbf{F}_p^2$ ?
19.  $\pi(x)$  bezeichne die Anzahl der Primzahlen  $\leq x$ . Versuchen Sie, aus dem Sieb des Eratosthenes und aus dem Kenntnis der Primzahlen  $\leq x$  eine Näherungsformel für  $\pi(x^2)$  zu erfinden. Testen Sie Ihre Formel an  $x = 10$ .
20. Beweisen Sie die Klassifikation der pythagoräischen Zahlentripel mit Hilfe der Primfaktorzerlegung in  $\mathbf{Z}[i]$ . Welche  $c$  können in den (teilerfremden) pythagoräischen Tripeln nur auftreten?
21. Wenn man über alle Primzahlen summiert, konvergiert dann die Reihe  $\sum \frac{1}{p}$ ? Wenn nein, wie schnell wächst die Funktion  $P(x) := \sum_{p \leq x} \frac{1}{p}$  so ungefähr?
22.  $\zeta$  bezeichne die Riemannsche Zetafunktion. Mit Hilfe ihres Eulerprodukts zeige man, dass für alle  $s$  mit Realteil  $> 1$

$$\zeta^{-1}(s) = \sum_{n \geq 1} \frac{\mu(n)}{n^s} \quad \text{für gewisse } \mu(n) \in \{0, 1, -1\},$$

und ermitteln Sie interessante Eigenschaften der Funktion  $\mu$ .

23. Die (inzwischen bewiesene) *Catalansche Vermutung* besagt: Außer  $y^m = 8$  und  $x^n = 9$  gibt es keine Lösung der diophantischen Gleichung  $x^n - y^m = 1$ ,  $n, m > 1$ . Man zeige: Wenn die *abc*-Vermutung stimmt, hat diese Gleichung (für feste  $n, m$ ) nur endlich viele Lösungen.
24. Fortsetzung von Aufgabe 20: Für welche  $c \in \mathbf{N}$  gibt es mehr als ein pythagoräisches Zahlentripel mit  $a^2 + b^2 = c^2$ ? Finden Sie das kleinste solche  $c$ !
25. Für  $k, n \in \mathbf{N}$ , beide  $> 0$ , sei  $d_k(n) := \sum_{d|n} d^k$  die  $k$ -te *Teilersumme* von  $n$ . Zeigen Sie, dass  $d_k$  *multiplikativ* ist, d.h.  $d_k(mn) = d_k(m)d_k(n)$  für alle teilerfremden  $m, n$  erfüllt, und konstruieren Sie mit Hilfe der Zetafunktion eine Dirichletreihe der Form  $\sum_{n>0} d_k(n)n^{-s}$ . Konvergenz wo?

26. Wenn  $\alpha$  alle ganzen Gaußschen Zahlen  $\neq 0$  durchläuft, für welche  $s \in \mathbf{C}$  konvergiert dann die Reihe  $\sum |\alpha|^{-2s}$ ? Gibt es eine Eulersche Produktentwicklung?
27. Gibt es im Polynomring  $\mathbf{C}[z]$  Lösungen der Gleichung  $a^2 + b^2 = c^2$ ? Welche?
28. Verifizieren Sie die Funktionalgleichung  $\Gamma(z+1) = z\Gamma(z)$ .
29. Beweisen Sie, dass die Zetafunktion  $\zeta(\sigma + it)$  für jedes feste  $\sigma > 1$  ein Betragsmaximum in  $t = 0$ , also auf der reellen Achse annimmt.
30. Bestimmen Sie den Körpergrad von  $\mathbf{Q}(\sqrt{-2}, \sqrt{3})$ .
31. Man zeige: für  $d = 2, 3, 5, 6, 7$ ,  $K := \mathbf{Q}(\sqrt{d})$ , hat  $\mathcal{O}_K$  eine unendliche Einheitsgruppe. Dagegen ist die Einheitengruppe für  $d < 0$  stets endlich (und besteht aus welchen Einheiten?).
32.  $p$  sei eine Primzahl und  $j \not\equiv 0 \pmod{p}$ . Man beweise, dass  $(1 - \zeta_p^j)/(1 - \zeta_p)$  eine Einheit im Ring  $\mathbf{Z}[\zeta_p]$  ist.
33. Fortsetzung: Man zeige, dass  $p$  im Ring  $\mathbf{Z}[\zeta_p]$  bis auf eine Einheit von der Form  $(1 - \zeta_p)^{p-1}$  ist.
34.  $p$  sei eine Primzahl. Bestimmen Sie die Diskriminante von  $\mathbf{Z}[\zeta_p]$ . Sie dürfen verwenden, dass die verschiedenen Einbettungen des Kreisteilungskörpers eindeutig bestimmt sind durch die Vorschrift  $\zeta_p \mapsto \zeta_p^k$ ,  $k \not\equiv 0 \pmod{p}$ .
35. Zeigen Sie, dass  $3$  und  $1 + \sqrt{-26}$  im Ring  $\mathbf{Z}(\sqrt{-26})$  ein Primideal der Norm  $3$  erzeugen.
36. Übertragen Sie das, was wir für die ganzen Gaußschen Zahlen gemacht haben, auf den Ring  $\mathbf{Z}[\sqrt{3}]$ : Welche ganzrationalen Zahlen  $p$  bleiben träge, welche sind Produkte zweier inäquivalenter Primzahlen  $\pi, \pi'$ , und welche sind „verzweigt“, d.h. äquivalent zu einem  $\pi^2$ ? Fortsetzung: Welche ganzrationale Primzahlen lassen sich als  $\pm(n^2 - 3m^2)$  schreiben mit  $n, m \in \mathbf{N}$ ?
37. Gott wählt zwei Zahlen  $a$  und  $b$  aus  $\{2, 3, \dots, 100\}$ , wobei  $a = b$  möglich ist, und gibt Mr. S. die Summe  $a + b$  und Mr. P. das Produkt  $ab$ . Nun ergibt sich folgender Dialog: Mr. S. sagt zu Mr. P.: „Ich kenne die Zahlen nicht, aber ich weiß, dass Du sie auch nicht weißt.“ Mr. P. antwortet: „Dann kenne ich die Zahlen.“ Darauf Mr. S.: „Dann kenne ich sie auch!“. Welche Zahlen hat Gott gewählt?
38. Versuchen Sie, die Zahl  $e$  in einen Kettenbruch zu entwickeln (Computerunterstützung?). Formulieren Sie eine Vermutung!
39. Bestimmen Sie die Kettenbruchentwicklung von  $\sqrt{19}$ .
40. Bestimmen Sie eine Grundeinheit von  $\mathbf{Q}(\sqrt{19})$ .

41. Ermitteln Sie möglichst große Einheitengruppen für die Kreisteilungskörper  $\mathbf{Q}(\zeta_5)$ ,  $\mathbf{Q}(\zeta_8)$  und  $\mathbf{Q}(\zeta_{12})$ .
42. Überzeugen Sie sich davon, dass für alle natürlichen  $n$  zwischen 0 und 39 der Ausdruck  $n^2 + n + 41$  eine Primzahl ist. Was hat das mit der Zahlentheorie in  $\mathbf{Q}(\sqrt{-163})$  zu tun?
43. Begründen Sie, dass es in  $\mathbf{Q}(\sqrt{-13})$  keine eindeutige Primfaktorzerlegung gibt.