Infos und Aufgaben zur Elementaren Zahlentheorie

Jürgen Wolfart, Winter 2018/19

Vorlesungsprogramm mit Quellenangabe ([W] verweist auf mein Buch *Einführung in die Zahlentheorie und Algebra*, 2. Aufl. 2011, Vieweg + Teubner):

§1 Der Euklidische Algorithmus ([W] 1.2, 3.4.1, 3.4.6 und 3.4.8)

§2 Primfaktorzerlegung ([W] 1.3, 3.4.2, 3.4.3 und 3.4.7)

§3 Primzahlverteilung ([W] 1.4)

§4 Kongruenzen und Reste ([W] 1.5, 2.3.2, 3.4.5)

§5 Multiplikative zahlentheoretische Funktionen ([W] 4.1)

§6 Die Struktur der primen Restklassengruppe ([W] 4.2)

§7 Quadratische Reste ([W] 4.3)

§8 Gaußsche Summen ([W] 7.4.1)

§9 Das quadratische Reziprozitätsgesetz ([W] 7.5.1, 7.5.2, 4.4)

§10 Das Jacobisymbol ([W] 4.5)

§11 Verzweigung von Primzahlen in $\mathbb{Z}[i]$ ([W] 4.6.1 bis 4.6.3)

§12 Pythagoräische Zahlentripel, das Fermatproblem und die *abc*–Vermutung ([W] 3.5 und Ireland/Rosen, Ch. 17.4)

§13 Das RSA–Schema ([W] 5.1)

§14 Primzahltests ([W] 5.2, 5.3)

§15 Primfaktorzerlegung ([W] 5.4)

§16 Elliptische Kurven ([W] 5.5)

§17 Gitter und Untergitter ([W] 8.1, 8.2.1, 8.2.2)

§18 Der Minkowskische Gitterpunktsatz ([W] 8.3)

§19 Anwendungen des Gitterpunktsatzes ([W] 8.4)

§20 Das Kreis– und Kugelproblem ([W] 8.5)

§21 Der Satz von Minkowski–Hlawka ([W] 8.6)

§22 Packungsdichte ([W] 8.7)

§23 Packungsdichte und Codierungstheorie ([W] 8.8)

§24 Goley–Code und Leech–Gitter ([W] 8.9)

Saalübung für die Tutorien am 17. und 18.10. :

Sei K ein Körper. Wieviele Divisionen mit Rest braucht man höchstens, um den ggT von zwei Polynomen $\in K[x]$ des Grads n zu berechnen?

Hausaufgaben

1. Bestimmen Sie den ggT d von 196611 und 243 sowie *alle* ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ von

$$196611\,x \,+\, 243\,y \;=\; d \quad .$$

2. d sei der ggT von m und $n \in \mathbb{N}$. Zeigen Sie, dass $x^d - 1$ im Polynomring $K[x]$ über einem beliebigen Körper K der ggT der beiden Polynome $x^m - 1$ und $x^n - 1$ ist.

3. Bestimmen Sie den ggT von 17 und $15 + 8i$ im Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen (der ggT ist nur eindeutig bis auf Multiplikation mit Einheiten, hier also bis auf die vier Potenzen von i).

4. Entwickeln Sie die rationale Funktion $f \in \mathbb{R}(x)$,

$$f(x) \;:=\; \frac{x}{1 - x - x^2} \quad ,$$

in eine Potenzreihe (= Taylorreihe) um den Nullpunkt. Kommt Ihnen die Folge der Koeffizienten bekannt vor? Formulieren Sie eine Vermutung und beweisen Sie sie!

5. $\mathbb{P}$ bezeichne die Menge aller Primzahlen. Zeigen Sie, dass die Reihe $\sum_{p \in \mathbb{P}} \frac{1}{p}$ divergiert.

6. p sei eine Primzahl, $\nu_p(x)$ die Multiplizität von p in der Primfaktorzerlegung von $x \in \mathbb{Z}$, und $[x]$ die *Gaußklammer* von $x \in \mathbb{Z}$, also die größte ganze Zahl $\leq x$. Beweisen Sie

$$\nu_p(n!) \;=\; \sum_{m \geq 1} \left[\frac{n}{p^m} \right] \quad .$$

Mit wievielen Nullen endet (im Dezimalsystem geschrieben) die Zahl $1000!$?

7. Welche $(n-1)!\,, n \in \mathbb{N}$, sind nicht teilbar durch n ? Für welche $n \in \mathbb{N}$ ist n^2 kein Teiler von $(n-1)!$? (Aufgabe **6** dürfen Sie verwenden, auch wenn Sie sie nicht bearbeitet haben.)

8. Warum ist $2^n < \binom{2n}{n}$ für alle $n \in \mathbb{N}$, $n > 1$?

9. φ bezeichne die Eulersche Phi–Funktion. Für welche $n \in \mathbb{N}$ gilt $\varphi(n) = n/3$?

10. Entscheiden Sie, ob die folgenden Kongruenzen eine Lösung in $\mathbb{Z}$ besitzen, und wenn ja, welche:

$$31\,x \equiv 1 \bmod 257 \quad , \quad 16\,y \equiv 17 \bmod 257$$
$$117\,u \equiv 16 \bmod 169 \quad , \quad 117\,v \equiv 39 \bmod 169$$

11. μ sei die Möbiusfunktion, ζ die Riemannsche Zetafunktion. Beweisen Sie

$$\zeta(s)^{-1} \;=\; \sum_{n\in\mathbb{N}} \frac{\mu(n)}{n^s} \qquad \text{für alle} \quad s \in \mathbb{C} \quad \text{mit} \quad \operatorname{Re} s > 1 \quad .$$

12. (Variation einer Aufgabe aus einem alten chinesischen Rechenbuch) Neun Piraten haben einen Schatz aus (gleichgroßen) Goldstücken erbeutet und versuchen, diesen Schatz in neun gleiche Teile zu teilen. Dabei bleiben 5 Münzen übrig, und beim Streit um diesen Rest wird ein Pirat erstochen. Bei einem erneuten Verteilungsversuch unter den verbliebenen 8 Piraten bleiben 4 Goldstücke übrig, und beim Gerangel um sie geht ein weiterer Pirat über Bord und ertrinkt. Nun lässt sich der Goldschatz in 7 gleiche Teile teilen. Wieviele Goldmünzen sind es mindestens gewesen?

13. $n \in \mathbb{N}$ sei im *Sechsersystem* geschrieben, d.h. in der Form

$$(a_m a_{m-1} \ldots a_1 a_0)_6 := a_m 6^m + a_{m-1} 6^{m-1} + \ldots + a_1 6 + a_0 \quad \text{mit Ziffern} \quad a_j \in \{0,1,2,3,4,5\} \; .$$

Beweisen Sie die folgenden *Quersummenregeln* :

$$5 \mid n \;\Leftrightarrow\; 5 \mid \sum_0^m a_j \quad , \qquad 7 \mid n \;\Leftrightarrow\; 7 \mid \sum_0^m (-1)^j a_j$$

14. Angenommen, die prime Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ sei zyklisch. Zeigen Sie, dass sie dann genau $\varphi(\varphi(n))$ erzeugende Elemente (= Primitivwurzeln $\bmod n$) besitzt.

15. Beweisen Sie, dass die Kongruenz $x^2 \equiv 1 \bmod 385$ genau acht Lösungen in $\mathbb{Z}/385\mathbb{Z}$ besitzt, und ermitteln Sie diese Lösungen.

16. p sei eine Primzahl, $k \in \mathbb{N}$. Zeigen Sie:

$$1^k + 2^k + \ldots + (p-1)^k \;\equiv\; 0 \bmod p \quad , \quad \text{wenn} \qquad (p-1) \not\mid k \; ,$$
$$1^k + 2^k + \ldots + (p-1)^k \;\equiv\; -1 \bmod p \; , \quad \text{wenn} \qquad (p-1) \mid k \; .$$

17. (Fortsetzung von Aufg. **16**) p sei eine Primzahl > 3. Zeigen Sie, dass die Summe aller quadratischen Reste, ebenso wie die Summe aller quadratischen Nichtreste $\equiv 0 \bmod p$ ist.

18. $p = 2q + 1$ und q seien Primzahlen, dabei $q \equiv 3 \bmod 4$. Zeigen Sie (2. Ergänzungsgesetz!), dass $2^q \equiv 1 \bmod p$; schließen Sie daraus, dass $M_{11} = 2^{11} - 1$ und $M_{23} = 2^{23} - 1$ keine Mersenne–Primzahlen sind.

19. σ_0 bezeichne die Teilerfunktion, σ_1 die Teilersummenfunktion und ζ die Riemannsche Zetafunktion. Zeigen Sie, dass in der jeweiligen Konvergenzhalbebene $\operatorname{Re} s > 1$ bzw. $\operatorname{Re} s > 2$

$$\zeta^2(s) \;=\; \sum_{\mathbb{N}} \frac{\sigma_0(n)}{n^s} \quad \text{und} \qquad \zeta(s)\,\zeta(s-1) \;=\; \sum_{\mathbb{N}} \frac{\sigma_1(n)}{n^s} \quad .$$

20. Verwenden Sie die Existenz einer Primitivwurzel, um einen neuen Beweis des Satzes von Wilson $(p-1)! \equiv -1 \bmod p$ zu geben.

21. $p := F_n = 2^{2^n} + 1$, $n > 0$, sei eine Fermatprimzahl. Zeigen Sie: 3 ist eine Primitivwurzel $\bmod p$.

22. Die Primzahl p sei ein Teiler der Fermatzahl $F_n = 2^{2^n} + 1$ (jetzt nicht mehr als *prim* vorausgesetzt). Berechnen Sie $\operatorname{ord}\,[2]_p$ und zeigen Sie, dass $p = k \cdot 2^{n+1} + 1$ ist für ein $k \in \mathbb{N}$.

23. Charakterisieren Sie (durch Kongruenzbedingungen) die Menge aller Primzahlen p, für die 7 ein quadratischer Rest ist.

24. Beweisen Sie, dass $1/97$ eine Dezimalbruchentwicklung der Periodenlänge 96 besitzt.

Musterlösung zu Aufgabe 24 (Torsten Klein):

Zu zeigen ist, dass $\frac{1}{97}$ eine Dezimalbruchentwicklung der Periodenlänge 96 besitzt. Da 10 und 97 teilerfremd sind, gilt: Die Länge der Periode entspricht der (multiplikativen) Ordnung von 10 in $(\mathbb{Z}/97\mathbb{Z})^*$. Dies kann sich leicht anhand der Durchführung der schriftlichen Division klar machen.Es gilt: $\operatorname{ord}[10]_{97}$ teilt $|(\mathbb{Z}/97\mathbb{Z})^*| = 96 = 3 \cdot 2^5$

$$\Rightarrow \operatorname{ord}[10]_{97} = 3^l \cdot 2^k \text{ mit } l \in \{0,1\} \text{ und } k \in \{0,1,2,3,4,5\}$$

Angenommen, $\operatorname{ord}[10]_{97}$ sei echt kleiner als 96, dann wrde sie entweder $48 = \frac{96}{2}$ oder $32 = \frac{96}{3}$ teilen. Daraus folgt dann $10^{32} \equiv 1 \mod 97$ oder $10^{48} \equiv 1 \mod 97$ Dies kann man durch Nachrechnen zum Widerspruch führen:

$$10^{16} \equiv (10^2)^8 \equiv 100^8 \equiv 3^8 \equiv 9^4 \equiv 81^2 \equiv (-16)^2 \equiv 256 \equiv 62 \mod 97$$

$$10^{32} \equiv (10^{16})^2 \equiv 62^2 \equiv (-35)^2 \equiv 30^2 + 2 \cdot 5 \cdot 30 + 5^2 \equiv 1225 \equiv 61 \mod 97$$

$$10^{48} \equiv 10^{32} \cdot 10^{16} \equiv 61 \cdot 62 \equiv (-36) \cdot (-35) \equiv 35^2 + 35 \equiv 1260 \equiv 96 \mod 97$$

Da nun sowohl 10^{32} als auch 10^{48} nicht kongruent 1 sind, folgt $\mathrm{ord}[10]_{97} = 96$ und damit die Aussage. Alternativ kann man auch $\left(\frac{10}{97}\right) = \left(\frac{5}{97}\right)\left(\frac{2}{97}\right)$ berechnen. Nach dem 2. Ergänzungssatz gilt $97 \equiv 1 \mod 8$, also $\left(\frac{2}{97}\right) = 1$. Und der quadratische Reziprozitätssatz ergibt hier:

$$\left(\frac{5}{97}\right)\left(\frac{97}{5}\right) = (-1)^{\frac{5-1}{2}\frac{97-1}{2}} = (-1)^{96} = 1$$

Somit gilt dann:

$$\left(\frac{5}{97}\right) = \left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = -1$$

Wobei der letzte Schritt leicht mit dem Eulerkriterium zu prüfen ist oder man sieht, dass 1 und 4 die beiden einzigen quadratischen Restklassen modulo 5 repräsentieren. Da nun $\left(\frac{5}{97}\right) = -1$ gilt, folgt, dass $\left(\frac{10}{97}\right) = -1$ und somit muss $\mathrm{ord}[10]_{97} = 3^l \cdot 2^5$ gelten. Denn falls der Anteil an Zweierpotenzen nicht maximal ist muss es sich bei der Zahl um einen quadratischen Rest handeln, somit muss man nur noch 32 als mögliche Ordnung ausschließen.

25. Gegeben ein teilerfremdes pythagoräisches Zahlentripel $(x, y, z) \in \mathbb{Z}^3$ mit $x^2+y^2 = z^2$. Zeigen Sie, dass z nur Primfaktoren $\equiv 1 \mod 4$ besitzt.

26. Unter welchen Bedingungen an n hat die diophantische Gleichung $x^2 + y^2 = n$ mehr als eine Lösung? ($x > y > 0$ und teilerfremd vorausgesetzt, um triviale Antworten auszuschließen). Tipps: Denken Sie an die Primfaktorzerlegung in $\mathbb{Z}[i]$; das kleinste Beispiel ist $n = 65$.

27. K sei ein Körper der *Charakteristik* $\neq 2$ (heißt: $1+1 =: 2 \neq 0$; 2 ist also invertierbar). Wie findet man im Polynomring $K[x]$ alle pythagoräischen Tripel f, g, h (alle vom Grad > 0), d.h. mit $f^2(x)+g^2(x) = h^2(x)$? Und was passiert, wenn K die Charakteristik 2 hat, also z.B. für $K = \mathbb{F}_2$?

28. Beweisen Sie – unter der Annahme, dass die *abc*–Vermutung stimmt –, dass die *Catalan'sche Gleichung* $x^2 - y^3 = 1$ nur endlich viele Lösungen in $\mathbb{Z}$ besitzt. (Die Catalan'sche Gleichung besitzt in der Tat $(x, y) = (\pm 3, 2)$ als einzige nichttriviale Lösung (also mit $xy \neq 0$), auf ganz anderem Wege 2003 von Mihailescu bewiesen.)

29. Zeigen Sie: Es gibt keine Polynome $f, g \in \mathbb{C}[z]$ vom Grad > 0 mit $f^2 - g^3 = 1$.

30. Carmichael–Zahlen sind quadratfrei und haben mindestens 3 Primfaktoren. Warum?

31. Finden Sie die Umkehrabbildung von $(\mathbb{Z}/221\mathbb{Z})^* \to (\mathbb{Z}/221\mathbb{Z})^* : a \mapsto a^{35}$.

32. Sei $p \equiv 3 \bmod 4$ Primzahl, bekanntlich träge in $\mathbb{Z}[i]$. Zeigen Sie, dass der Restklassenring $\mathbb{Z}[i]/p\mathbb{Z}[i]$ ein Körper mit p^2 Elementen ist.

33. (Fortsetzung der Aufgabe **21**) Beweisen Sie, dass F_4 eine Primzahl ist.

34. Untersuchen Sie, ob die Mersenne–Zahlen M_{13}, M_{17}, M_{19} prim sind.

35. Beweisen Sie, dass die multiplikative Gruppe jedes endlichen Körpers $\mathbb{F}_q$ zyklisch ist.

36. Erläutern Sie, warum es nicht so schlau ist, zur Iteration in Pollard's Rho–Verfahren eine lineare Funktion $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : x \mapsto ax + b$ zu wählen.

37. Sei $p \equiv 3 \bmod 4$ eine Primzahl. Beweisen Sie, dass auf der (projektiven) elliptischen Kurve $y^2t = x^3 - xt^2$ über $\mathbb{F}_p$ genau $p + 1$ Punkte liegen. Tipp: Überlegen Sie sich, dass für $u \neq 0$ eine der Gleichungen $y^2 = \pm u$ keine Lösung, die andere aber zwei Lösungen hat.

38. Machen Sie sich ein Bild von der Punktmenge $\mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$ und zeigen Sie, dass $\mathbb{Z}[\sqrt{-2}]$ ein Ring mit euklidischem Algorithmus ist.

39. Fortsetzung von **38**: Welche Einheiten hat $\mathbb{Z}[\sqrt{-2}]$? Welche rationalen Primzahlen $p \in \mathbb{P}$ sind in $\mathbb{Z}[\sqrt{-2}]$ träge, verzweigt, zerlegt?

Musterlösung zu Aufgabe 39 (Torsten Klein):

Zu bestimmen ist, welche Primzahlen p in $\mathbb{Z}[\sqrt{-2}]$ träge, zerlegt oder verzweigt sind.

Dazu werden wir analog zu den Gaußschen Zahlen vorgehen. Zunächst werde ich zeigen, dass falls eine Primzahl p in $\mathbb{Z}[\sqrt{-2}]$ zerlegbar ist, die Zerlegung die Gestalt $p = \pm q \cdot \bar{q}$ hat, wobei q und daher auch $\bar{q}$ Primelemente in $\mathbb{Z}[\sqrt{-2}]$ sind.

Beweis: Da ± 1 die einzigen Zahlen mit Norm 1 sind, sind sie auch die einzigen Einheiten in $\mathbb{Z}[\sqrt{-2}]$. Sei p eine zerlegbare Primzahl und $p = \pm a \cdot b$ mit $a, b \in \mathbb{Z}[\sqrt{-2}]$, wobei a, b keine Einheiten sind. Also $a = c + d\sqrt{-2}$ und $b = e + f\sqrt{-2}$. Damit folgt

$$p = ab = (c + d\sqrt{-2})(e + f\sqrt{-2}) = (ce - 2df) + (cf + de)\sqrt{-2}$$

Da p eine ganze Zahl ist, muss $cf + de = 0$ gelten. Daraus folgt, dass $b = k \cdot \bar{a}$ mit $k \in \mathbb{Z}$, dies kann man leicht sehen, wenn man a, b als Elemente von $\mathbb{C}$ auffasst. Falls $k \neq \pm 1$, wäre dies ein Widerspruch dazu, dass p eine Primzahl ist.

Ich werde nun zeigen, dass eine Primzahl p genau dann in $\mathbb{Z}[\sqrt{-2}]$ zerlegt ist, falls $p \equiv 1$

mod 8 oder $p \equiv 3 \mod 8$ gilt. Zunächst ist die 2 verzweigt: Es gilt

$$2 = -\sqrt{-2}\sqrt{-2}$$

Wenn eine Primzahl $p > 2$ in $\mathbb{Z}[\sqrt{-2}]$ zerlegbar ist, dann gilt $p = q \cdot \bar{q} = a^2 + 2b^2$ Somit gilt für zerlegbare ungerade Primzahlen:

$$p \equiv 1 \text{ oder } 3 \mod 8 \,,$$

da 0,1,4 die einzigen Quadrate modulo 8 sind und a ungerade sein muss, damit p ungerade wird. Damit sind alle Primzahlen $p \equiv 5$ oder $7 \mod 8$ träge. Daher bleibt noch zu zeigen, dass Primzahlen $p \equiv 1$ oder $3 \mod 8$ tatsächlich zerlegt sind. Nun gilt für Primzahlen $p \equiv 1 \mod 8$ nach dem 1. Ergänzungssatz $(\frac{-1}{p}) = 1$, da $p \equiv 1 \mod 8 \Rightarrow p \equiv 1 \mod 4$ gilt, und nach dem 2. Ergänzungssatz $(\frac{2}{p}) = 1$. Da das Legendresymbol multiplikativ ist, folgt somit $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = 1$ Ähnlich geht man bei den Primzahlen $p \equiv 3 \mod 8$ vor: Es gilt nach dem 1. Ergänzungssatz $(\frac{-1}{p}) = -1$, da $p \equiv 3 \mod 8 \Rightarrow p \equiv 3 \mod 4$ gilt, und nach dem 2. Ergänzungssatz $(\frac{2}{p}) = -1$. Daraus folgt wieder $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = 1$. Also ist in beiden Fällen -2 ein quadratischer Rest modulo p, also gibt es eine ganze Zahl $x < p$ mit

$$x^2 \equiv -2 \mod p \Leftrightarrow x^2 + 2 \equiv 0 \Rightarrow x^2 + 2 = N(x + \sqrt{-2}) = p \cdot n, \text{für ein } n < p$$

Setzen wir jetzt $y = x + \sqrt{-2}$, dann sieht man, dass $N(y) < N(p) = p^2$ in $\mathbb{Z}[\sqrt{-2}]$ gilt. Daher folgt aus der eindeutigen Primfaktorzerlegung von y, dass es eine Zerlegung von $y = q \cdot \nu$ gibt mit $p \cdot n = y \cdot \bar{y}$, $n < p$, $p = q \cdot \bar{q}$, $n = \nu\bar{\nu}$. Also sind alle $p \equiv 1$ oder $3 \mod 8$ zerlegbar in $\mathbb{Z}[\sqrt{-2}]$.

Also ist die 2 verzweigt, Primzahlen der Form $p \equiv 1$ oder $3 \mod 8$ zerlegbar und Primzahlen der Form $p \equiv 5$ oder $7 \mod 8$ träge in $\mathbb{Z}[\sqrt{-2}]$. Damit sind auch alle Primzahlen abgedeckt.

40. Sei $n = pq$, $p \neq q$ zwei Primzahlen, $s, t \in \mathbb{Z}$ mit $st \equiv 1 \bmod (p-1)(q-1)$ (anstelle von $(p-1)(q-1)$ kann man auch das kgV der beiden Faktoren nehmen). Zeigen Sie: Für jedes $a \in \mathbb{Z}/n\mathbb{Z}$ ist $a^{st} \equiv a \bmod n$. (Diese Konsequenz des Euler'schen Satzes im RSA–Schema gilt also ohne eine Teilerfremdheitsbedingung!)

41. p sei eine Primzahl. Zeigen Sie, dass das Gitter $\mathbb{Z}^2$ genau $p+1$ Untergitter vom Index p besitzt.

42. $\Lambda := (2\mathbb{Z})^4 \subset \mathbb{R}^4$ ist ein Gitter, dessen Punkte (in der üblichen euklidischen Metrik) den Minimalabstand 2 voneinander haben. Suchen (und finden) Sie ein Obergitter $\Gamma \supset \Lambda$ im $\mathbb{R}^4$ mit Index $(\Gamma : \Lambda) = 2$, dessen Punkte immer noch den Minimalabstand 2 voneinander haben.

43. Zeigen Sie dass alle Fermatzahlen (vgl. Aufg. **22**) paarweise teilerfremd sind ($\Rightarrow$ Beweis von Polya, dass die Primzahlmenge unendlich ist!).

44. Eine Aufgabe über Gaußsche Summen: Beweisen Sie

$$2\cos\frac{2\pi}{5} \;=\; \frac{\sqrt{5}-1}{2} \quad .$$

Zusatzaufgabe für L3–Studierende: Leiten Sie daraus ab, wie man ein regelmäßiges Fünfeck mit Zirkel und Lineal konstruiert!

45. $\Lambda \subset \mathbb{R}^2$ sei ein Gitter mit Determinante $d(\Lambda) = 1$. Zeigen Sie, dass Λ einen Gitterpunkt $(x,y) \neq (0,0)$ mit $y \geq 0$, $x^2+y^2 \leq \frac{4}{\pi}$ besitzt.

46. Seien $a, b \in \mathbb{R}$ mit $a^2+b^2 = 1$ und $\frac{1}{2} > \varepsilon > 0$. Zeigen Sie, dass es $x, y \in \mathbb{Z}$ gibt, nicht beide $= 0$, mit $|ax+by| \leq \varepsilon$, $|x|, |y| \leq \frac{1}{\varepsilon}$.

47. p, $p+2$, $p+6$, $p+8$, $p+14$ seien Primzahlen. Beweisen Sie: $p = 5$.

48. Fortsetzung von **37**: Wieviele Punkte hat die (projektive) elliptische Kurve $y^2t = x^3 - xt^2$ über $\mathbb{F}_p$, wenn $p = 5, 13$ oder 17 gewählt wird?

49. $\dfrac{\pi}{2\sqrt{3}}$ ist die Gitterpackungsdichte von Ellipsen im $\mathbb{R}^2$. Warum?

50. Berechnen Sie das Volumen vierdimensionaler Einheitskugeln. Seien $\mathbf{e}_j$ die Standard–Einheitsvektoren des $\mathbb{R}^4$, dann ist

$$L \;:=\; \mathbb{Z}2\mathbf{e}_1 + \mathbb{Z}2\mathbf{e}_2 + \mathbb{Z}2\mathbf{e}_3 + \mathbb{Z}(\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3+\mathbf{e}_4)$$

das Gitter für die dichteste Kugelgitterpackung im $\mathbb{R}^4$ (erinnern Sie sich an Aufgabe **42**?). Dichte dieser Kugelgitterpackung?

51. Schwer: p sei eine Primzahl > 3 und $n < m < p$ natürliche Zahlen. Zeigen Sie

$$\left|\sum_{a=n}^{m}\left(\frac{a}{p}\right)\right| \;<\; \sqrt{p}\,\log p\,.$$

Anleitung: Nutzen Sie die Transformationsformel $g_a = (\frac{a}{p})g$ für Gaußsche Summen (schon wieder!) und vertauschen Sie die Summationsreihenfolge. Sie sollten auf einen Ausdruck vom Typ $\sum_t \frac{\zeta^{kt}-1}{\zeta^t-1}$ stoßen; Zähler nach oben durch 2 abschätzen, Nenner nach unten durch $4|t|/p$ für $|t| < p/2$. Denken Sie an die Beträge Gaußscher Summen und an

$\sum_{t=1}^{p-1} \frac{1}{t} < \log p$.

52. Fortsetzung: Zeigen Sie, dass es weniger als $\sqrt{p}\log p$ aufeinander folgende quadratische Reste/Nichtreste mod p gibt. Insbesondere: Es gibt ein $a \in \mathbb{N}$, $1 < a < \sqrt{p}\log p$, mit $(\frac{a}{p}) = -1$. (Sie dürfen das Resultat von **51** auch verwenden, wenn Sie **51** nicht selbst bearbeitet haben.)

Musterlösung zu Aufgabe 51:

Um die Behauptung $\left|\sum_{a=n}^{m} \left(\frac{a}{p}\right)\right| < \sqrt{p}\,\log p$ zu zeigen, genügt es,

$$\left|\sum_{a=n}^{m} g_a\right| < p\,\log p$$

nachzuweisen, denn wir wissen ja, dass $g_a = (\frac{a}{p})g$ und $|g| = \sqrt{p}$ ist. Nach Definition der Gaußschen Summen und durch Umordnung der Summationszeichen ist

$$\sum_{a=n}^{m} g_a = \sum_{a=n}^{m} \sum_{t \bmod p} \left(\frac{t}{p}\right) \zeta_p^{at} = \sum_{t \bmod p} \left(\frac{t}{p}\right) \sum_{a=n}^{m} \zeta_p^{at} = \sum_{t \bmod p} \left(\frac{t}{p}\right) \frac{\zeta_p^{(m+1)t} - 1}{\zeta_p^{nt} - 1}\,.$$

(man beachte $n > 0$.) Die Abschätzung der Summe kann man (sehr grob) durch Abschätzung der Beträge der einzelnen Glieder vornehmen: Klar ist $|\zeta_p^{(m+1)t} - 1| < 2$ (Satz des Pythagoras und Thales am Einheitskreis mit dem reellen Intervall $[-1, 1]$ als Hypotenuse). Etwas mühsamer ist die untere Abschätzung $|\zeta_p^{nt} - 1| > 4|nt|/p$ für $0 < |nt| < p/2$ (was man o.B.d.A. voraussetzen kann). Diese positiven Repräsentanten der $|nt| \bmod p$ durchlaufen höchstens zweimal die $0 < k < p/2$, mit $\sum \frac{1}{k} < \log p - \log 2$ ergibt sich also die Abschätzung

$$\left|\sum_{t \bmod p} \left(\frac{t}{p}\right) \frac{\zeta_p^{(m+1)t} - 1}{\zeta_p^{nt} - 1}\right| < p \log p\,.$$