Zahlentheorie

Zusammenfassung

Aless Lasaruk

29. Dezember 2005

Zusammenfassung

Dieses Dokument enthält Fragen und Antworten zum Fach Zahlentheorie. Die Fragen sind durch systematisches Durchgehen des Skriptes der Vorlesung entstanden, decken aber den Stoff nicht vollständig. Man beachte auch, dass die Antworten nicht exakt formuliert sind. Das Ziel der Formulierung ist das Minimieren der schriftlichen Antwort und Maximieren der mündlichen.

Inhaltsverzeichnis

1 Grundlagen

1.1 Natürliche Zahlen

- **Was besagt das *Reduktionsprinzip*?**

  Zu jede zwei Mengen A, B und Abbildungen $\sigma : B \to A$ und $\varphi : A \times B \to A$ gibt es genau eine eindeutige Abbildung $f : B \times \mathbb{N}_0 \to A$ mit $f(b, 0) = \sigma(b)$ und $f(b, n + 1) = \varphi(b, f(b, n))$.

- **Was besagt das *Minimalitätsprinzip*?**
  Jede nichtleere Teilmente von natürlichen Zahlen besitzt ein kleinstes Element. Man beweist es durch die Untersuchung aller Unterschranken.
- **Was besagt die Induktion mit Rückgriff auf alle Vorgänger?**
  Falls für eine Aussage über natürlichen Zahlen aus der Annahme, dass die Aussage für alle $k < n$ gilt, folgt, dass die Aussage auch für n gilt, so gilt die Aussage für alle natürliche Zahlen.
- **Wie beweist man Induktion mit Rückgriff auf alle Vorgänger?**
  Mit Hilfe des Minimalitätsprinzips. Man bildet die Menge aller Elemente für die die Aussage nicht gilt. Diese besitzt ein kleinstes Element und es gilt für alle Elemente darunter die Aussage. Das liefert einen Widerspruch.

1.2 Ganze Zahlen

- **Wie bildet man ganze Zahlen?**
  Man stellt eine ganze Zahl als eine Äquivalenzklasse von Paaren natürlicher Zahlen mit der Semantik $(a, b) \in \mathbb{N}^2$ entspricht $a - b$.
- **Welche Eigenschaften erfüllt $\mathbb{Z}$?**
  $(\mathbb{Z}, 0, 1, +, -, \cdot, \leq)$ Kommutativer total geordneter nullteilerfreier Ring mit 1.

1.3 Rationale Zahlen

- **Wie bildet man die rationalen Zahlen?**
  Äquivalenzklassen von Paaren $(a, b) \in \mathbb{Z} \times \mathbb{N}$ mit semantik a/b.
- **Welche Eigenschaften erfüllt $\mathbb{Q}$?**
  $(\mathbb{Q}, 0, 1, +, -, \cdot, ^{-1}, \leq)$ bildet einen geordneten Körper.
- **Wie kann man $x^2 \geq 0$ herleiten?**
  Monotonie der Ordnung.

2 Teilbarkeit, GGT und Kongruenzen

2.1 Bildung von GGT

- **Wie ist der *größte gemeinsame Teiler* GGT definiert?**
  Ein positiver Teiler alle Elemente $d \mid a$ mit $a \in A$ einer Menge und für jeden weiteren positiven Teiler d' gilt $d' \mid d$.
- **Warum ist GGT eindeutig?**
  Angenommen es gibt ein weiteres $d' = \text{GGT}(A)$. Dann $d \mid d'$ und $d' \mid d$, woraus $d = d'$ folgt.
- **Warum existiert ein GGT einer Menge A?**
  Man bildet die Menge aller Linearkombinationen der Elemente. Der Schnitt mit $\mathbb{N}$ ist nicht leer und besitzt ein kleinstes Element nach dem Minimalprinzip. Das ist der GGT $= d$, weil es alle Elemente von A teilt und jeder andere positive Teiler von A einen Widerspruch zur Minimalität von d liefert.
- **Wie berechnet man GGT algorithmisch?**
  Euklidischer Algorithmus. Man subtrahiert solange Zahlen voneinander in A, bis eine übrig bleibt.
- **Wieso ist der euklidische Algorithmus korrekt?**
  Weil die Invarianten: nichtleer und Linearkombinationen erhalten bleiben.
- **Wieso Terminiert euklidische Algorithmus?**
  Die Summe der Elemente sinkt nach jedem Durchlauf strikt. Es gibt also nur endlich viele Durchläufe.

- **Was sagt Division mit Rest aus?**
  Es gibt eine eindeutige Darstellung von für zwei Zahlen x und y mit $x = qy + r$ mit $0 \leq r < |y|$.
- **Wie zeigt man die Existenz der Restdarstellung?**
  Induktion nach x für ein festes y.
- **Wann heißt eine Menge von Zahlen *paarweise teilerfremd*?**
  Wenn $\text{GGT}(A) = 1$. Paarweise teilerfremd, wenn für je zwei unterschiedliche Zahlen $a, b \in A$ gilt $\text{GGT}(a, b) = 1$.
- **Welche Beziehung gilt zwischen Teilerfremd und paarweise Teilerfremd?**
  Aus paarweise Teilerfremd folgt Teilerfremd. Einfacher Widerspruchsbeweis.
- **Was ist ein Ideal von $\mathbb{Z}$?**
  Nichtleere Menge mit $a, b \in I \rightarrow a + b \in I$ und $a \in I$, $r \in \mathbb{Z} \rightarrow ra \in I$. Abgeschlossen unter Addition und robust gegenüber der Multiplikation von Elementen mit $\mathbb{Z}$.
- **Warum ist jedes Ideal ein Hauptideal in $\mathbb{Z}$?**
  Euklidischer Algorithmus.
- **Was ist der *erweiterte euklidische Algorithmus*?**
  Man merkt sich die Kofaktoren.

2.2 Lineare diophantische Gleichungen

- **Was ist eine lineare diophantische Gleichung?**
  $\sum_{i=1}^{n} a_i x_i = d$ über $\mathbb{Z}$.
- **Wann ist eine LDG lösbar?**
  Genau dann, wenn $\text{GGT}(a_1, ..., a_n) \mid d$.
- **Wie kann man eine Lösung einer LDG angeben?**
  Man bestimmt mit erweiterten Euklid $g = \text{GGT}(a_1, ..., a_n)$ als Linearkombination von $a_1, ..., a_n$ und multipliziert die Koeffizienten mit dem Kofaktor d/g.
- **Wie sieht die Lösungsmenge einer LDG aus?**
  Wenn L_0 der Lösungsraum der entsprechenden homogenen LDG, und x_0 eine spezielle Lösung, dann gilt $L = x_0 + L_0$.
- **Wie kann man L_0 darstellen?**
  $L_0 = \{(b_1, ..., b_{n-1}, -(\sum_{i=1}^{n-1} a_i b_i)/a_n \mid b_1, ..., b_n \in \mathbb{Z}, \text{ falls teilbar}\}$
- **Wie sieht der homogene Lösungsraum im Speziallfall $n = 2$ aus?**
  Für die Gleichung $a_1 x_1 + a_2 x_2 = b$ gilt $L_0 = \{(ea_2', -ea_1') \mid e \in \mathbb{Z}\}$ mit $a_1' = a_1/d$ und $a_2' = a_2/d$ und $d = \text{GGT}(a_1, a_2)$.

2.3 KGV und die Verbandsstrukture von $\mathbb{N}_0$

- **Wie ist das kleinste gemeinsame Vielfache definiert?**
  Für $k = \text{KGV}(a, b)$ gilt $a \mid k$ und $b \mid k$ und für jedes andere k' mit $a \mid k'$ und $b \mid k'$ gilt $k \mid k'$.
- **Wie kann man KGV mit Hilfe von GGT festlegen?**
  $\text{KGV}(a, b) = \frac{|a||b|}{\text{GGT}(a,b)}$.
- **Wie beweist man, dass obige Festlegung wohldefiniert ist?**
  Man beschränke sich auf positive Zahlen. Seien $d = \text{GGT}(a, b)$ und $a = a'd$ und $b = b'd$. Dann ist $\frac{ab}{\text{GGT}(a,b)} = a'db'$. Somit gilt $a \mid a'db' = ab'$ und aber $b \mid a'db' = a'b$. Sei k' mit $a \mid k'$ und $b \mid k'$. Dann gilt $k' = aa'' = a'a''d$. und $k' = bb'' = b'b''d$ wegen $d \mid a \mid k'$ und $d \mid b \mid k'$ und somit $a'a'' = b'b''$. Es gilt $d = ra + sb = ra'd + sb'd$. Somit gilt $a'' = ra'a'' + sa''b' = rb'b'' + sb'a'' = b'(rb'' + sa'')$. Also ist a'' ein Vielfaches von b'. Somit gilt $k|k' = a'a''d = a'b'd(rb'' + sa'')$.

- **Kann man analog** KGV **für eine Menge von Elementen festlegen?**
  Nein. Man muss iterativ rechnen.
- **Welche Struktur hat** $(\mathbb{N}_0, \text{KGV}, \text{GGT})$**?**
  Ein distributiver Verband.
- **Kennen Sie weitere Verbände mit ähnlichen Eigenschaften?**
  Teilverbände $T(n) = \{b \in \mathbb{N} \mid b \mid n\}$.

2.4 Kongruenzen

- **Wodurch ist eine *Kongruenzrelation* definiert?**
  $x \cong_n y$ gdw. $n \mid (x - y)$.
- **Wie setzt sich die Kongruenzeigenschaft auf Polynomausdrücke fort?**
  Für ein Polynomausdruck $f(x_1, ...x_n)$ gilt für $z_i \cong_n z_i'$ stets $f(z_1, ..., z_n) = f(z_1', ..., z_n')$.
- **Wie kann man Kongruenzklassen kanonisch repräsentieren?**
  Es gibt genau ein $0 \leq i < n \in I$ mit $x \cong_n i$.
- **Welche wichtigste Eigenschaft der Kombination von Kongruenzen mit unteschiedlichen Moduli kennen Sie?**
  Aus $x \cong_{m_i} y$ folgt $x \cong_{\text{KGV}(m_1,...,m_n)} y$.

2.5 Chinesische Restklassensatz

- **Auf welcher Beobachtung basiert der *Chinesische Restsatz*?**
  Für teilerfremde m, n gibt es ein $1 \leq x \leq mn$ mit $x \cong_m 1$ und $x \cong_n 0$.
- **Wie kann man obige Beobachtung zeigen?**
  Man bestimmt $1 = sn + rm$. Falls $s \geq 0$ setzt man $x = sn$ und sonst $x = (s + m)n$. Dann gilt $x = sn = 1 - rm \cong_m 1$ bzw. $x = sn + mn = 1 - rm + mn \cong_m 1$.
- **Wie kann man obige Behauptung für eine Menge von Kongruenzen erweitern?**
  Für eine Menge von teilerfremden Zahlen m_i existiert ein x_i mit $x_i \cong_{m_i} 1$ und $x_i \cong_{m_j} = 0$. Man setzt $m_i' = \prod_{j=1, j\neq i}^{n} m_j$.
- **Was sagt der Chinesische Restklassensatz aus?**
  Für paarweise teilerfremde Moduli m_i und Reste r_i existiert ein $x \in \mathbb{Z}$, sodass $x \cong_{m_i} r_i$ für $1 \leq i \leq n$. Also Lösung des Kongruenzensystems.
- **In wieweit ist die Lösung des Chinesischen Restklassensatzes eindeutig?**
  Bis auf Kongruenz modulo $m = \prod m_i = \text{KGV}\{m_1, ..., m_n\}$.
- **Wie konstruiert man die Lösung?**
  Man bestimmt x_i mit $x_i \cong_{m_i} 1$ und $x_i \cong_{m_j} 0$ und setze $x = \sum_{i=0}^{n} r_i x_i$.
- **Wie zeigt man die Eindeutigkeit der Lösung des Restklassensatzes?**
  Aus $x \cong_{m_i} r_i \cong_{m_i} y$ folgt $x \cong_{m_i} y$ und somit gilt $x \cong_m y$ mit $m = \text{KGV}(m_1, ..., m_n)$.
- **Funktioniert der Restklassensatz, wenn man die paarweise Teilbarkeit fallen läßt?**
  Nein.
- **Wie kann man den Restklassensatz für zwei Kongruenzen verallgemeinern?**
  Für $x \cong_{m_1} r_1$ und $x \cong_{m_2} r_2$ gibt es genau dann eine Lösung, wenn $r_1 \cong_d r_2$ mit $d = \text{GGT}(m_1, m_2)$.
- **Wie kann man obige Aussage beweisen?**
  Eine Richtung ist trivial, denn aus $r_1 \cong_d x \cong_d r_2$ folgt $r_1 \cong_d r_2$. Die andere Richtung ergibt sich aus $x = r_1 + \frac{r_2 - r_1}{d} r m_1$.
- **Wie kann man den Restklassensatz für mehrere Kongruenzen verallgemeinern?**
  Das Kongruenzensystem $x \cong_{m_i} r_i$ hat genau dann eine Lösung, falls für alle $1 \leq i < j \leq n$ gilt $r_i \cong_{\text{GGT}(m_i, m_j)} r_j$.

- **Wie beweist man den obigen Satz?**
  Induktion mit Reduktion auf zwei Kongruenzen.
- **Wie kann man dann alle Lösungen des Systems erhalten?**
  Spezielle Lösung plus $m = \text{KGV}(m_1, ..., m_n)$ faches aller ganzen Zahlen.

3 Primzahlen

3.1 Definition und Existenz

- **Wieso gibt es Primzahlen?**
  Man kann zeigen, dass für jede Zahl a in $T_{\mathbb{N}}(a)$ mindestens eine Primzahl existiert. Das ist nämlich die kleinstse in $T_{\mathbb{N}}(a) \setminus \{1\}$.
- **Kennen sie ein einfaches Verfahren zum Auffinden von Primzahlen unter einer festen Schranke?**
  Sieb des Erathostenes. Durchsuchen aller Zahlen und Streichen aller Vielfachen.
- **Wieso gibt es unendlich viele Primzahlen?**
  Nach Satz von Euklid gibt es zwischen p_n und dem Produkt aller Primzahlen bis p_n plus 1 eine Primzahl.
- **Wie beweist man obige Behauptung?**
  Sei $q = p_1...p_n$. Jedes p_i teilt q aber nicht $q + 1$, da sonst $p_i \mid 1 = (q + 1) - q$. Dann existiert eine Primzahl in $T_{\mathbb{N}}(q + 1)$ und die stimmt nicht mit p_i überein.
- **Was ist ein Primzahlenzwilling?**
  $(p, p + 2)$ mit $p, p + 2$ Primzahlen.
- **Gibt es unendlich viele Primzahlenzwillinge?**
  Offene Frage.
- **Wie verhält sich GGT und Primzahlen?**
  $\text{GGT}(p, a) \in \{1, p\}$ für $a \neq 0$.
- **Wie beweist man obige Behauptung?**
  $\text{GGT}(p, a) \in T_{\mathbb{N}}(p)$.
- **Wie kann man Primzahlen durch Teilbarkeit beschreiben?**
  $p \mid ab \rightarrow p \mid a \vee p \mid b$.
- **Wie beweist man obige Behauptung?**
  Für $p \mid ab$ und $p \nmid b$ gilt $\text{GGT}(p, b) = 1 = rp + sb$. Multiplikation mit a ergibt dann $a = arp + asb$. Rest ist klar.
- **Wie kann man obige Aussage verallgemeinern?**
  $p \mid a_1...a_n \rightarrow p \mid a_1 \vee ... \vee p \mid a_n$.
- **Wie kann man die n-te Primzahl abschätzen?**
  Durch $2^{2^{n-1}}$. Beweis durch Induktion und geometrische Reihe.
- **Wie kann man die Anzahl der Primzahlen kleiner x abschätzen?**
  Die Anzahl der Primzahlen ist größer als $\log_2(\log_2(x)) + 1$.
- **Was besagt der Satz von *Hadamard*?**
  Die Anzahl von Primzahlen kleiner x ist asymptotisch gleich mit $\frac{x}{\ln(x)}$.
- **Kommen die Primzahlen in regelmässigen Abständen?**
  Nein. Es gibt beliebig große Lücken.
- **Wie kann man die Aussage von oben beweisen?**
  Das Intervall ist $[a, a+k-1]$ für $a = (k+1)!+2$. In der Menge $(k+1)!+2, (k+1)!+3, ...$ hat jede Zahl einen Teiler, denn $(k + 1)! + j$ wird durch j geteilt.
- **Was kann man über Existenz von Primzahlen in Progressionen aussagen?**
  Es gibt sogar unendlich viele Primzahlen in $a\mathbb{N}_0 + b$ (*Satz von Dirichlet*).

- **Wie kann man beweisen, dass in $4\mathbb{N}_0 + 3$ unendlich viele Primzahlen liegen?**
  Man nimmt sich die ersten n Primzahlen in $4\mathbb{N}_0 + 3$ und bildet das Produkt q. Dann kann man zeigen, dass für $m = 4q - 1 \in 4\mathbb{N}_0 + 3$ eine Primzahl mit $p \cong_4 3$ existiert und $p \neq p_1, ..., p_n$.
- **Wie kann man große Primzahlen bestimmen?**
  Für n Primzahl $2^n \pm 1$ (*Mersennesche Primzahl*), $2^{2^n} + 1$ (*Fermatsche Zahl*).
- **Sind alle Mersenneschen Zahlen und Fermatschen Zahlen Primzahlen?**
  Nein. M_{11} und F_5 sind bereits keine. Aber gute Testkandidaten.

3.2 Primfaktorzerlegung und Anwendungen

- **Was besagt der Satz über die Primfaktorzerlegung?**
  Die ist eindeutig bis auf die Reihenfolge der Faktoren.
- **Wie bekommt man die PFZ eindeutig?**
  Exponenten und $p_1 < p_2 < ... < p_n$.
- **Welche Eigenschaft der natürlichen Zahlen man mit Hilfe der Primfaktorzerlegung zeigen?**
  Natürliche Zahlen mit GGT und KGV bilden einen distributiven Verband.
- **Wie viele Primteiler einer Zahl gibt es?**
  $|P(a)| \leq \log_2(a)$
- **Wie kann man obige Aussage beweisen?**
  Wegen $|p_i|$ gilt für $a = p_1...p_n$ auch $a \geq 2^n$. Daraus folgt $n \leq log_2(a)$.

4 Faktorringe und prime Restklassengruppen

4.1 Grundlangen

- **Welche Struktur bildet $\mathbb{Z}/n$?**
  $(\mathbb{Z}/n, 0, 1, +, \cdot, -)$ bildet einen kommutativen Ring mit 1.
- **Was ist ein *Integritätsbereich*?**
  Ein nullteilerfreier Ring mit 1.
- **Was ist ein *Nullteiler*?**
  Nullteiler ist ein Element $a \neq 0$, sodass ein $b \neq 0$ existiert mit $ab = 0$.
- **Welche Eigenschaften haben Nullteiler?**
  Sie sind nicht invertierbar.
- **Wann ist ein Element ein Nullteiler in $\mathbb{Z}/n$?**
  Genau dann, wenn $\text{GGT}(a, n) \neq 1$ und $n \nmid a$.
- **Wann ist ein Element invertierbar in $\mathbb{Z}/n$?**
  Genau dann, wenn $\text{GGT}(a, n) = 1$.
- **Wie kann man Elemente in $\mathbb{Z}/n$ differenzieren nach Invertierbarkeit und Nullteiler-Eigenschaft?**
  Entweder Nullteiler oder Invertierbar.
- **Welcher Zusammenhang gilt zwischen n prim und Ringeigehscnaften von $\mathbb{Z}/n$?**
  Genau dann Integritätsbereich und auch Körper, wenn p prim ist.
- **Wie ist U_n definiert?**
  $U_n = \{[a] \in \mathbb{Z}/n \mid a \text{ invertierbar}\}$
- **Welche Eigenschaften hat U_n?**
  1 ist immer enthalten. Produkte und inverse sind enthalten. Also bildet U_n eine multiplikative kommutative Untergruppe. Nennt sich *prime Restklassengruppe* modulo n.

- **Wie ist die *eulersche Funktion* definiert?**
  $\varphi(n) = |U_n|$.
- **Wie kann man die φ-Funktion ausrechnen?**
  $\varphi(p) = p - 1$ und $\varphi(p^k) = p^k - p^{k-1}$ für eine Primzahl p und $k \in \mathbb{Z}$.
- **Wieso gilt die zweite der obigen Formeln?**
  Man nimmt sich alle Elemente von U_{p^k}. Unter diesen sind genau die nicht invertierbar, die $ggT(x, p^k) \neq 1$ liefert. Das sind aber gerade solche, die p als Faktor enthalten. Das sind alle zwischen 1 und pj für $1 \leq j \leq p^{k-1}$.
- **Welche Homomorphieeigenschaften besitzt die φ-Funktion?**
  Falls GGT$(m, n) = 1$, so folgt $\varphi(mn) = \varphi(m)\varphi(n)$.
- **Wie beweist man obige Aussage?**
  Man definiert eine Bijektion von U_{nm} auf $U_n \times U_m$ durch $f((a, b)) = f(ab)$.
- **Welche Eigenschaften erfüllt die Abbildung $f((a, b)) = f(ab)$ zwischen $\mathbb{Z}/nm$ und $\mathbb{Z}/n \times \mathbb{Z}/m$?**
  Für Teilerfremde n, m ist die Abbildung $f((a, b)) = f(ab)$ ist ein Ringisomorphismus. Und Eingeschränkt auf die Gruppen U_{nm} ein Gruppenisomorphismus.
- **Wie ist "algebraische Version des chinesischen Restklassensatzes" zu verstehen?**
  Für jeden Wert $r_1, ..., r_n$ für teilerfremde $m_1, ..., m_n$ kann man durch die Umkehrabbildung aus $\mathbb{Z}/m_1 \times ... \times \mathbb{Z}/m_n$ einen Wert $x \in \mathbb{Z}_{m_1,...,m_n}$ bilden mit $f(x) = (r_1, ..., r_n)$.
- **Was besagt der *Satz von Euler*?**
  Für $1 = \text{GGT}(a, m)$ gilt $a^{\varphi(m)} \cong_m 1$.
- **Wie beweist man den Satz von Euler?**
  Man definiert eine Abbildung $l_a([b]) = [ab]$. Diese ist bijektiv und besitzt somit eine Umkehrabbildung l_c. Für jedes Element der Gruppe $U_n = \{[i_1], ..., [i_k]\}$ bildet man $[a]^k[i_1]...[i_k] = ([a][i_1])...([a][i_k]) = l_a([i1])l_a([i_k]) = [i_1]...[i_k]$. Durch Kürzen bekommt man $[a]^k = [1]$ $(k = \varphi(m))$.
- **Was besagt der Satz von Fermat?**
  $a^p \cong_p a$ für eine Primzahl p.
- **Wie beweist man den Satz von Fermat?**
  Korollar aus dem Satz von Euler.
- **Wie kann man $\varphi(n)$ ausrechnen?**
  Man faktorisiert die Zahl n in Primzahlenpotenzen. Dann reicht es nach dem Korrolar zum Beweis des Satzes von Euler die Kardinalitäten der Faktoren zu berechnen und miteinander zu multiplizieren.
- **Was besagt der *Satz von Wilson*?**
  p ist Primzahl gdw. $(p - 1)! \cong_p -1$.
- **Wie beweist man den Satz von Wilson?**
  Eine Richtung ist trivial durch Kontraposition, denn für $p = ab$ und $(p-1)! \cong_a -1$ folgt $(p - 1)! \cong_p 0$ und aus $a \mid p$ folgt $(p - 1) \cong_a -1$. Widerspruch. Für die andere Richtung betrachte die Nullstellen des Polynoms $p(x) = x^{p-1} - 1$ hat nach Fermat in $\mathbb{Z}/p$ alle Zahlen $1, ..., p - 1$ als Nullstellen. Man bekommt dann $p(x) = \prod_{i=1}^{p-1}(x - i)$.

4.2 Primzahlentests

- **Wie kann man einfach testen, ob eine Zahl eine Primzahl ist?**
  Alle Teilerdurchprobieren zwischen 1 und $\sqrt{n}$. ("Schwierige" Richtung ergibt sich durch Abschätzung $a^2 \leq ab = p$)
- **Wie kann man die Komplexität des obigen Tests bewerten?**
  Exponentiell in der Bitlänge von von n. Genauer gesagt $2^{k/2} - 1$.

- **Wie funktioniert der *Basis-2-Test*?**
  Wenn n eine Primzahl ist, so folgt $2^n \cong_n 2$.
- **Ist dieser Test auch hinreichend?**
  Nein.
- **Was sind *Pseudoprimzahl*en?**
  Zahlen, die den Basis-2-Test bestehen, aber keine Primzahlen sind.
- **Wie viele Pseudoprimzahlen gibt es?**
  Unendlich viele.
- **Kennen Sie eine effiziente Technik zum Berechnen von a^k modulo n?**
  Repeared Squaring: $a^k = a^{\sum_{i=0}^{d} k_i 2^i} = \prod a^{k_i 2^i}$. Wegen $k_i \in \{0, 1\}$ entstehen Produkte von Zahlen, die quadrate voneinander sind.
- **Wie hoch ist die Komplexität des Verfahrens?**
  Logarithmisch.
- **Was kann man über den Ausdruck $2^p - 1$ aussagen?**
  Primzahl oder Pseudoprimzahl.
- **Wie funktioniert *beliebiger Basis Test*?**
  Teste für ein $a \in \mathbb{N}$, ob $a^n \cong_n a$.
- **Wie heißten Zahlen, die den beliebigen Basis Test bestehen aber keine Primzahlen sind?**
  Carmichael Zahlen.
- **Wie funktioniert der *Test von Wilson*?**
  Man prüft ob $(n-1)! \cong_n -1$. Exponentielle Laufzeit.
- **Ist der Test von Wilson auch hinreichend?**
  Ja.
- **Wie Funktioniert der *Quadrat-Test*?**
  Man prüft, ob für ein $a \in \mathbb{Z}$ gilt $a^2 \cong_n 1 \rightarrow a \cong_n \pm 1$.
- **Wiso ist der Quadrat-Test für Primzahlen korrekt?**
  Für eine Primzahl ist $\mathbb{Z}/n$ ein Körper und $f(x) = x^2 - 1 = (x-1)(x+1)$. Dann folgt aus $f(a) = 0$, dass $a \cong_n \pm 1$.
- **Kennen sie einen weiteren notwendigen und hinreichenden Test außer Wilson?**
  Für jeden Primteiler q von $(n-1)$ gibt es ein a_q mit $a_q^{n-1} \cong_n 1$ und $a_q^{(n-1)/q} \ncong_n 1$.

4.3 Primitivwurzeln

- **Was ist *Gruppenordnung*?**
  Anzahl der Elemente in einer Gruppe.
- **Was ist die *Ordnung eines Gruppenelements*?**
  Das kleinste g mit $g^n = 1$.
- **Was kann man über $\mathrm{ord}(g)$ aussagen?**
  $\mathrm{ord}(g) \mid |G|$, $g^n = 1$ gdw. $\mathrm{ord}(g) \mid n$, $\mathrm{ord}(g^k) = \frac{\mathrm{ord}(g)}{\mathrm{GGT}(k, \mathrm{ord}(g))}$, $\mathrm{GGT}(k, \mathrm{ord}(g)) = 1 \rightarrow \mathrm{ord}(g^k) = \mathrm{ord}(g)$.
- **Was ist ein *erzeugendes Element*?**
  Ein Element mit $G = \{g^i \mid 1 \leq i \leq \mathrm{ord}(g)\}$.
- **Wann heißt eine Gruppe *zyklisch*?**
  Wenn sie ein erzeugendes Element besitzt.
- **Was ist eine *Primitivwurzel*?**
  a heißt eine Primitivwurzel modulo n, wenn $[a]$ erzeugt U_n.

- **Welche äquivalenten Eigenschaften erfüllen Primitivwurzeln?**
  $\text{ord}([a]) = \varphi(n)$, $a^{\varphi(n)} \cong_n 1$ und $a^k \ncong_n 1$ für alle $a < \varphi(n)$.
- **Was kann man über die Existenz von Primitivwurzeln aussagen?**
  U_n hat eine Primitivwurzel gdw. U_n ist eine zyklische Gruppe.
- **Wann existieren Primitivwurzeln?**
  Genau dann, wenn $n \in \{1, 2, 4, p^k, 2p^k \mid p \text{ ungerade Primzahl }\}$ nach Satz vom Gauss.
- **Wie bestimmt man die Anzahl von Primitivwurzeln?**
  $\varphi(\varphi(n))$. Jede Primitivwurzel a hat die Ordnung $\varphi(n)$ und unter den Potenzen a^i sind alle Primitivwurzeln mit $\text{GGT}(\varphi(n), i) = 1$.

5 Polynomielle Kongruenzen

5.1 Lösungsverfahren

- **Wie löst man *polynomielle Kongruenzen*?**
  Man faktorisiert den Modulus. Und löst die Kongrunezen in den Faktorgruppen. Dann kann man mit Hilfe des chinesischen Restklassensatzes wieder eine Lösung bestimmen.
- **Welche Beziehungen gelten für Lösungen?**
  Wenn c eine Lösung von $f(x) \cong_n 0$, so ist c eine Lösung von $f(x) \cong_{p_i^{e_i}} 0$ und umgekehrt, falls c_i Lösungen von $f(x) \cong_{p_i^{e_i}} 0$ sind dann gibt es ein $c \cong_{p_i^{e_i}} c_i$, sodass c eine Lösung von $f(x) \cong_n 0$ ist.
- **Wie löst man denn $f(x) \cong_{p^e} 0$ naiv?**
  Naiv durch probieren aller $0 \leq c \leq p^e - 1$.
- **Welche Laufzeit hat das?**
  Exponentiell.
- **Wie kann man das Verfahren verbessern?**
  Man prüft alle $0 \leq c < p$, ob $f(c) \cong_{p^e} 0$ und bekommt $y_1, ..., y_k$ positive Ergebnisse. Dann prüft man für den nächsten Schritt $e + 1$ alle $y_i + p^e l$ für $0 \leq l < p - 1$.
- **Hat sich die Laufzeit dadurch verbessert?**
  Nein. Die ist immer noch exponentiell.
- **Wie heißt c in $x^k \cong_n c$?**
  Falls lösbar, der k-te Potenzrest modulo n.
- **Wie löst man $x^k \cong_n c$?**
  O.B.D.A. ist $n = p^e$. Falls U_n eine Primitivwurzel besitzt, so besitzt $x^k \cong_n c$ eine Lösung für $d = \text{GGT}(k, \varphi(n))$ gdw. $x^k = [c]$ hat eine Lösung in U_n gdw. $[c]^{\varphi(n)/d} = 1$ in U_n gdw. $d \mid ind_d([c]_n)$.

5.2 Weitere Anwendungen

- **Ist es möglich nichtlineare diophantische Gleichungen algorithmisch zu lösen?**
  Algorithmisch nicht. 10 Hilbertsches Problem.
- **Was sind pythagoräische Tripel?**
  Tripel mit $x^2 + y^2 = z^2$.
- **Wie viele gibt es davon?**
  Unendlich viele der Form $(2k + 1, 2k^2 + 2k, 2k^2 + 2k + 1)$.
- **Was ist *diskreter Logarithmus?***
  Es gibt genau eine Zahl i mit $a = b^i$ in U_n für eine Primitivwurzel b.
- **Kennen Sie einen kürzeren Beweis des Satzes von Wilson mit Primitivwurzeln?**
  Man sucht sich eine Primitivwurzel b modulo p. Dann in U_p gilt $(p-1)! = b^1 ... b^{p-1} = b^{(p-1)p/2} = (b^{(p-1)/2})^p$. Nach Fermat gilt $b^{p-1} \cong_p 1$. Es gilt aber $b^{(p-1)/2} \neq 1$ in U_p, da b eine Primitivwurzel. D.h. $b^{(p-1)/2} = -1$ und somit gilt die Beh.

- **Was ist die Idee bei RSA?**
  Man wählt große Primzahlen p und q und betrachtet $m = pq$ und $\varphi(pq) = (p-1)(q-1)$. Man wählt ein $1 < e < \varphi(m)$ mit $\mathrm{GGT}(e, \varphi(m)) = 1$ und berechnet $1 = de + f\varphi(m)$. Öffentlicher Schlüssel ist dann (m, e). Für jeden Block schickt man die Zahl $\gamma = \beta^e$ modulo m. Der Empfänger berechnet

$$\gamma^d \cong_m = (\beta^e)^d = \beta^{ed} \cong_m \beta^{2d}(\beta\varphi(m))^f = \beta^{ed+f\varphi(m)} \cong_m \beta.$$

Index