Vorkurs Mathematik 2007

Vorlesung 7

Tilman Bauer

Universität Münster

25. September 2007

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

EI. Zahlentheorie I: Der kleine Satz von Fermat

Wiederholung: Kongruenzen

In Vorlesung 4 haben wir Modulo-Arithmetik behandelt.

Definition

Sei $n \in \mathbb{N}_{\geq 1}$. Auf $\mathbb{Z}$ ist eine Äquivalenzrelation "Kongruenz modulo n" definiert durch

$$x \equiv y \pmod{n} \iff n \mid (x - y).$$

- Es gibt genau n Äquivalenzklassen, nämlich

$$\begin{aligned} [0] &= \{\dots, -2n, -n, 0, n, \dots\} \\ [1] &= \{\dots, -2n+1, -n+1, 1, n+1, \dots\} \\ &\vdots \qquad\qquad\qquad \vdots \\ [n-1] &= \{-n-1, -1, n-1, 2n-1, \dots\}. \end{aligned}$$

- $\mathbb{Z}/n$ ist die Menge der Äquivalenzklassen.

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

El. Zahlentheorie I: Der kleine Satz von Fermat

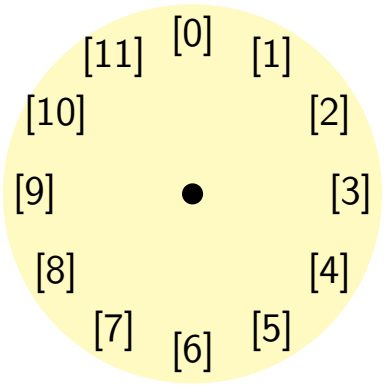
Wiederholung: Kongruenzen

Auf $\mathbb{Z}/n$ können wir Arithmetik treiben:

Definition

- Addition: $[x] + [y] = [x + y]$
- Multiplikation: $[x][y] = [xy]$.

Wir erinnern uns an die Uhr (als Beispiel für $\mathbb{Z}/12$):



$$[2] + [6] = [8]$$
$$[9] + [4] = [1] \quad (= [13])$$
$$[11] + [11] = [10] \quad (= [22])$$

El. Zahlentheorie I: Der kleine Satz von Fermat

Wiederholung: Kongruenzen

Schließlich hatten wir einen Satz über Inverse:

Satz

In $\mathbb{Z}/n$ gibt es genau zu den Äquivalenzklassen $[m]$ ein Inverses (Kehrwert), für die m und n teilerfremd sind.

Korollar

Ist p eine Primzahl, so ist in $\mathbb{Z}/p$ jedes von $[0]$ verschiedene Element invertierbar.

- In $\mathbb{Z}/p$ können wir also rechnen wie in $\mathbb{Q}$ oder $\mathbb{R}$: addieren, subtrahieren, multiplizieren und dividieren (letzteres aber nicht durch 0).

Beweis des Korollars.

Eine Zahl m ist genau dann nicht teilerfremd zu p, wenn sie ein Vielfaches von p ist.
Das ist genau dann der Fall, wenn $m \equiv 0 \pmod{p}$, also wenn $[m] = [0]$. □

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

El. Zahlentheorie I: Der kleine Satz von Fermat

Aussage des Satzes

Satz (kleiner Satz von Fermat)

Sei p eine Primzahl. Dann gilt für jede Zahl $a \in \mathbb{Z}$:

$$a^p \equiv a \pmod{p}$$

- Beispiel: $p = 5$, $a = 2$:

$$2^5 = 32 \equiv 2 \pmod{5}$$

- Beispiel: $p = 7$, $a = 4$:

$$4^7 = 16384 = 2340 \cdot 7 + 4 \equiv 4 \pmod{7}$$

- Für $a \not\equiv 0 \pmod{p}$ können wir beide Seiten durch a teilen und erhalten $a^{p-1} \equiv 1 \pmod{p}$.

Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

El. Zahlentheorie I: Der kleine Satz von Fermat

Beweis des Satzes

Wir beweisen zunächst einen Hilfssatz:

Proposition

Sei p eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gilt in $\mathbb{Z}/p$:

$$\{[1], [2], \ldots, [p-1]\} = \{[a], [2a], \ldots, [(p-1)a]\}$$

- Die Mengen sind gleich, aber die Reihenfolge ist verschieden!

Beweis.

Die Abbildung $f : \mathbb{Z}/p \to \mathbb{Z}/p$ mit $f([x]) = [ax]$ ist bijektiv, denn $g([y]) = \frac{[y]}{[a]}$ ist eine Umkehrabbildung.
$f([0]) = [0]$, also $f(\{[1], \ldots, [p-1]\}) = \{[1], \ldots, [p-1]\}$.
Andererseits $f(\{[1], \ldots, [p-1]\}) = \{[a], \ldots, [(p-1)a]\}$. □

Vorkurs Mathematik 2007

Tilman Bauer

Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

El. Zahlentheorie I: Der kleine Satz von Fermat

Beweis des Satzes

Satz
Sei p eine Primzahl. Dann gilt $a^p \equiv a \pmod{p}$.

Wir berechnen das Produkt der Elemente auf beiden Seiten von

$$\{[1],[2],\ldots,[p-1]\} = \{[a],[2a],\ldots,[(p-1)a]\} :$$

$$\prod_{i=1}^{p-1}[i] = \prod_{i=1}^{p-1}[ia] = [a]^{p-1}\prod_{i=1}^{p-1}[i].$$

Da $[i] \neq [0]$, können wir die Gleichung durch $\prod_{i=1}^{p-1}[i]$ teilen und erhalten $[1] = [a]^{p-1}$.

El. Zahlentheorie I: Der kleine Satz von Fermat

Beweis des Satzes

Satz
Sei p eine Primzahl. Dann gilt $a^p \equiv a \pmod{p}$.

- Wir wissen jetzt also $a^{p-1} \equiv 1 \pmod{p}$, falls $p \nmid a$.
- Multiplizieren wir beide Seiten mit a, erhalten wir $a^p \equiv a \pmod{p}$ für $p \nmid a$.
- Gilt $p \mid a$, so stimmt die Gleichung auch:

$$[a]^p = [0]^p = [0] = [a].$$

□

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

El. Zahlentheorie I: Der kleine Satz von Fermat

Eine wichtige Anwendung: Primalitätstest

Satz

Sei p eine Primzahl. Dann gilt $a^p \equiv a \pmod{p}$.

Tatsächlich ist die Aussage falsch, wenn p keine Primzahl ist.

Beispiel

Sei $p = 6$ und $a = 2$. Dann ist $2^6 = 64 \equiv 4 \not\equiv 2 \pmod{p}$.

- Man kann (leicht) zeigen: Ist p keine Primzahl, so stimmt der Satz für mindestens die Hälfte aller a zwischen 1 und $p-1$ nicht.
- Es ist im Allgemeinen schwierig, zu bestimmen, ob eine (große) Zahl p prim ist oder nicht.
- Wenn wir ein zufälliges a wählen und p nicht prim ist, haben wir also mindestens eine 50%-Chance, dass die Kongruenz nicht gilt.

El. Zahlentheorie I: Der kleine Satz von Fermat

Eine wichtige Anwendung: Primalitätstest

- Umgekehrt: Sei p vorgegeben und a zufällig gewählt.
- Gilt $a^p \not\equiv a \pmod{p}$, so wissen wir, dass p nicht prim ist.
- Gilt $a^p \equiv a \pmod{p}$, so ist p wahrscheinlich prim.
- Wie wahrscheinlich genau? Das ist gar nicht so leicht. Aber je größer p ist, desto genauer wird der Test.[1][2]
- Wir können die Genauigkeit erhöhen, indem wir mehrere a testen.
- Es gibt Verfeinerungen dieses Tests, die noch treffsicherer und/oder schneller zu berechnen sind.

[1] Erdős, P. und Pomerance, C., "On the number of false witnesses for a composite number", *Math. Comp.* **46** (1986), 259–279

[2] Kim, S.H. und Pomerance, C., "The probability that a random probable prime is composite", *Math. Comp.* **53** (1989), 721–741

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

RSA-Verschlüsselung

Eine Anwendung des kleinen Satzes von Fermat

- Alice und Bob möchten sich geheime Nachrichten schicken.
- Das heißt: die Nachrichten sind verschlüsselt, jeder kann sie mitlesen, aber nur Bob kann Alices Nachrichten entschlüsseln.
- Idee: Bob veröffentlicht einen Verschlüsselungsschlüssel v, mit dem Alice ihre Nachrichten an ihn verschlüsselt.
- Bob hat dazu passend einen geheimen Entschlüsselungsschlüssel e, mit dem er die mit v verschlüsselten Nachrichten lesen kann.
- Auch wenn man v und die verschlüsselte Nachricht kennt, kann man die Originalnachricht nicht rekonstruieren.
- Hier brauchen wir etwas Mathematik!

RSA-Verschlüsselung

Eine Anwendung des kleinen Satzes von Fermat

- Das RSA-Verfahren (Rivest, Shamir, Adleman, 1977) löst dieses Problem.
- Zunächst wählt Bob zwei große Primzahlen p und q und berechnet ihr Produkt $n = pq$.
- Dann sucht Bob eine Zahl $v > 1$, die zu $(p-1)(q-1)$ teilerfremd ist.
- Also hat $[v]$ ein Inverses $[e]$ in $\mathbb{Z}/(p-1)(q-1)$:

$$[v] \cdot [e] = [1] \in \mathbb{Z}/(p-1)(q-1)$$

- Bob veröffentlicht n und v und behält e für sich.

Vorkurs Mathematik 2007

Tilman Bauer

Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

RSA-Verschlüsselung

Eine Anwendung des kleinen Satzes von Fermat

$$n = pq, \quad ve \equiv 1 \pmod{(p-1)(q-1)}$$

- Nun möchte Alice eine Nachricht an Bob schicken, z.B. eine Zahl $X < n$.
- Alice verschlüsselt ihre Nachricht nun durch $[C] = [X^v] \in \mathbb{Z}/n$ und schickt sie Bob.
- Bob berechnet $[C^e] = [(X^v)^e] = [X^{ve}]$.
- Da $ve = N(p-1)(q-1) + 1$ für ein $N \in \mathbb{Z}$ gilt, ist

$$X^{ve} = X \cdot X^{(p-1)(q-1)N}$$

- Mit Fermat gilt $X^{p-1} \equiv 1 \pmod{p}$ und $(X^{p-1})^{q-1} \equiv 1 \pmod{q}$.

RSA-Verschlüsselung

Eine Anwendung des kleinen Satzes von Fermat

$$n = pq, \quad ve \equiv 1 \pmod{(p-1)(q-1)}$$

- Mit Fermat gilt $X^{p-1} \equiv 1 \pmod{p}$ und $(X^{p-1})^{q-1} \equiv 1 \pmod{q}$.
- Daraus folgt

$$X^{(p-1)(q-1)N} \equiv 1 \pmod{p}$$
$$X^{(p-1)(q-1)N} \equiv 1 \pmod{q}$$

- Also teilen sowohl p als auch q $X^{(p-1)(q-1)N} - 1$.
- Da p, q teilerfremd sind, gilt $pq \mid (X^{(p-1)(q-1)N} - 1)$.
- Also ist $X^{ve} \equiv X \pmod{n}$.

Vorkurs Mathematik 2007

Tilman Bauer

Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

RSA-Verschlüsselung

Eine Anwendung des kleinen Satzes von Fermat

Wieso kann Charlie, der die Unterhaltung C belauscht und auch n und v kennt, die Nachricht nicht rekonstruieren?

- Angenommen, Charlie könnte n faktorisieren und damit p und q herausfinden.
- Dann könnte er selbst ein Inverses $[e]$ von $[v] \in \mathbb{Z}/(p-1)(q-1)$ berechnen. Der Code wäre gebrochen.
- Die Sicherheit dieses Codes basiert auf zwei unbewiesenen Annahmen:
  1. Es gibt keine schnelle Methode, v-te Wurzeln in $\mathbb{Z}/n$ zu berechnen.
  2. Es gibt auch keine schnelle Methode, die Primfaktoren einer Zahl zu bestimmen.
- Sollte sich eine dieser Annahmen als falsch herausstellen, werden alle Verschlüsselungstechniken, die wir heute gebrauchen, unsicher!

El. Zahlentheorie II: Perfekte Zahlen

Definition von perfekten Zahlen

Definition

Eine natürliche Zahl $n \geq 1$ heißt perfekt, falls sie die Summe aller ihrer *echten* Teiler ist.

- Ein Teiler von n heißt echter Teiler, falls er ein Teiler von n ist, aber nicht gleich n.
- Die echten Teiler von 6 sind also 1, 2, 3. Da $1+2+3=6$, ist 6 perfekt.
- Die nächste perfekte Zahl ist $28 = 1+2+4+7+14$.
- Die nächste ist $496 = 1+2+4+8+16+31+62+124+248$.
- Können wir die perfekten Zahlen alle charakterisieren?
- Interessant: $6 = 2^1(2^2-1)$, $28 = 2^2(2^3-1)$, $496 = 2^4(2^5-1)$

Vorkurs Mathematik 2007

Tilman Bauer

Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

Wir kehren zu dieser Frage zurück. Zunächst:

Definition

Eine Funktion $f : \mathbb{N} \to \mathbb{R}$ heißt multiplikativ, falls $f(mn) = f(m)f(n)$ für teilerfremde m, n gilt.

Beispiel

- Die Funktion $f(n) = 1$ ist multiplikativ (haha).
- Die Funktion $\sigma(n) =$ Summe der Teiler von n ist multiplikativ.

- Denn sind m, n teilerfremd, so ist

$$\sum_{t|mn} t = \sum_{\substack{t_1|m \\ t_2|n}} t_1 t_2 = \left(\sum_{t_1|m} t_1\right)\left(\sum_{t_2|n} t_2\right)$$

$$\sigma(n) = \sum_{k|n} k$$

Lemma

Ist $n = p_1^{\mu_1} p_2^{\mu_2} \dots p_k^{\mu_k}$ die Zerlegung von n in Primfaktoren, so gilt $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\mu_i+1}-1}{p_i-1}$

Beweis.

Da σ multiplikativ ist und die $p_i^{\mu_i}$ paarweise teilerfremd sind, müssen wir nur zeigen: $\sigma(p^\mu) = \frac{p^{\mu+1}-1}{p-1}$.
Die Teiler von p^μ sind $1, p, p^2, \dots, p^\mu$.

$$\left(\sum_{i=0}^{\mu} p^i\right)(p-1) = \sum_{i=1}^{\mu+1} p^i - \sum_{i=0}^{\mu} p^i = p^{\mu+1} - 1.$$

□

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

Vorkurs Mathematik 2007
Tilman Bauer
Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II
Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler
Aufgaben

El. Zahlentheorie II: Perfekte Zahlen

Der Satz von Euklid-Euler

Satz (Euklid-Euler)

1. *Sei $m \in \mathbb{N}$ so gewählt, dass $2^m - 1$ eine Primzahl ist. Dann ist $n = 2^{m-1}(2^m - 1)$ perfekt.*
2. *Ist n eine gerade perfekte Zahl, so ist sie von dieser Form: $n = 2^{m-1}(2^m - 1)$, wobei $2^m - 1$ prim ist.*

- Es ist unbekannt, ob es ungerade perfekte Zahlen gibt!

Beweis von 1. (Euklid).

- Ist $2^m - 1$ prim, so sind 2^{m-1} und $2^m - 1$ teilerfremd.
- Also gilt $\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1)$.
- Nach dem Lemma ist das $\frac{2^m-1}{2-1}(1 + 2^m - 1) = (2^m - 1)2^m = 2n$.

□

El. Zahlentheorie II: Perfekte Zahlen

Der Satz von Euklid-Euler

Satz (Euklid-Euler)

2. *Ist n eine gerade perfekte Zahl, so ist sie von dieser Form: $n = 2^{m-1}(2^m - 1)$, wobei $2^m - 1$ prim ist.*

Beweis von 2. (Euler).

- Sei n gerade und perfekt. Schreibe $n = 2^{m-1}u$ mit u ungerade und $m > 1$.
- Also gilt
$$2n \underset{\text{n perfekt}}{=} \sigma(n) \underset{\sigma \text{ mult.}}{=} \sigma(2^{m-1})\sigma(u) \underset{\text{Lemma}}{=} (2^m - 1)\sigma(u).$$
- Umgeformt: $\sigma(u) = \frac{2^m u}{2^m-1} = u + \frac{u}{2^m-1}$.
- Da u und $\frac{u}{2^m-1}$ ganzzahlige Teiler von u sind, hat u also nur diese beiden Teiler.
- Also ist u prim. Da $1 \mid u$, muss $\frac{u}{2^m-1} = 1$ sein, also $u = 2^m - 1$.

□

Vorkurs Mathematik 2007

Tilman Bauer

Elementare Zahlentheorie I: Der kleine Satz von Fermat
Wiederholung: Kongruenzen
Der kleine Satz
Beweis
Anwendung 1
Anwendung II

Elementare Zahlentheorie II: Perfekte Zahlen
Perfekte Zahlen
Multiplikative Funktionen
Der Satz von Euklid-Euler

Aufgaben

Aufgaben

Bitte bis Donnerstag, den 27. 9., bearbeiten!

1. Berechnen Sie $[7]^{123} \in \mathbb{Z}/15$. Denken Sie zunächst darüber nach, wie man das mit wenig Arbeit machen kann, und ohne mit großen Zahlen zu rechnen.
2. Zeigen Sie, dass für jede Primzahl p gilt:

$$(p-1)! \equiv -1 \pmod{p}$$

   Tipp: Benutzen Sie, dass jeder Faktor von $(p-1)!$ in $\mathbb{Z}/p$ invertierbar ist.
3. Zeigen Sie, dass folgende Funktion multiplikativ ist:

$$\mu(n) = \begin{cases} (-1)^r, & \text{falls } n \text{ ein Produkt von } r \text{ verschiedenen Primzahlen ist} \\ 0, & \text{sonst} \end{cases}$$