Ich selbst habe den Beweis des Satzes 3.15 geskipped

Gelesen bis vor Kapitel 8, Seite 99.

nächstes Video: https://www.fau.tv/clip/id/3608 (ab 01:01 h)

https://www.fau.tv/clip/id/3542 skipped (WeihnachtsVL, nicht klausurrelevant laut ihr)

(I): ∀b: ℕ. |{p prime | ∃a: ℕ. p ≡ a mod b ∧ gcd(a, b) = 1}| = ∞ (II): ∀a: ℕ. ∀b: ℕ. gcd(a, b) = 1 ⇒ |{p prime | p ≡ a mod b}| = ∞

Übungsaufzeichnung für Übung 3 angeguckt

ggT mit PFZ: https://www.video.uni-erlangen.de/clip/id/3373, 1:20

https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity#For_three_or_more_integers

Klausur: - ggT mittels euklidischem Algo können und was sonst noch mit eukl. Algo zsmhängt genaues Schema in Klausur reproduzieren mit a = q * b + r b = q' * r + r' - schriftliche Multiplikation - schriftliche Division - Proben nicht vergessen! - Skript erlaubt?

in Klausur: TR erlaubt? Zumindest laut Aufzeichnung 2013. Nutze meinen Casio fx-991DE PLUS mit ":R"-Taste! Klausur: RECHENAUFGABEN

`ggT(a*c, b*c) = c` wenn b, c teilerfremd?

Für a, b in N: a/ggT(a,b) und b/ggT(a,b) teilerfremd, d.h. ggT(a/ggT(a,b), b/ggT(a,b)) = 1.

Umwandlung mod-Gleichung <-> Teilbarkeitsgleichung

- $a \mid b - c \Leftrightarrow b \equiv c$ (mod a)

Algorithmen

Erweiterter Euklidischer Algorithmus für `ggT(a, b)`

$$
\begin{array}{llclclll}
\textit{Schritt 1} & a & = & q_1 \cdot & \underline{b} & + & \underline{r_1} & \text{mit} \quad 0 \leqslant r_1 < b \\
\textit{Schritt 2} & b & = & q_2 \cdot & \underline{r_1} & + & \underline{r_2} & \text{mit} \quad 0 \leqslant r_2 < r_1 \\
\textit{Schritt 3} & r_1 & = & q_3 \cdot & \underline{r_2} & + & \underline{r_3} & \text{mit} \quad 0 \leqslant r_3 < r_2 \\
 & r_{n-1} & = & q_{n+1} \cdot & \underline{\underline{r_n}} & + & 0 &
\end{array}
$$

Erweitert: durch Rückeinsetzen r_n mittels Linearkombination a und b ausdrücken.

Lösungen von `ax + by = c` mit (x, y) in $\mathbb{Z}^2$

Sei die Gleichung `ax + by = c` mit a, b, c in $\mathbb{Z}$ gegeben. Gesucht sind `x`, `y`, falls sie existieren.

1. Berechne `ggT(a, b)` mit (erw.) Euklidischen Algorithmus

2. Falls *nicht* `ggT(a, b) ∤ c` (über ℤ), dann unlösbar. Terminiere.

3. Falls `ggT(a, b) ≠ 1`: wende Algorithmus rekursiv auf durch `ggT(a, b)` dividierte Gleichung an (sonst Satz 4.18 in Schritt 5 nicht anwendbar)

   ⇒ `a/ggT(a, b) x + b/ggT(a, b) y = c/ggT(a,b)`

   möglich, da `ggT(a,b) | a,b,c` nach Annahme und da `ggT(a,b)` kein Nullteiler in ℤ ist.

   Lösungsmenge bleibt gleich durch diese Division!

4. Berechne **Partikularlösung**, angenommen `ggT(a, b) = 1 = a x' + b y'`

   Sei `ggT(a, b) | c` via q (d.h. `q · ggT(a, b) = c`). Dann:

   - `ax' + by' = ggT(a, b)`
     - `a(qx') + b(qy') = q · ggT(a, b) = c`

   => `q (x', y')` Partikularlösung

5. Berechne **alle Lösungen**

   - es gilt: `im(ax + by ∈ ℤ[x,y]) = ggT(a,b)ℤ`, äquivalent: `aℤ + bℤ = ggT(a,b)ℤ`
   - oder allg.: `im(a₁x₁ + … + a_nx_n ∈ ℤ[x₁, …, x_n]) = ggT(a₁, …, a_n)ℤ`, äquivalent: `a₁ℤ + … + aₙℤ = ggT(a₁, …, a_n)ℤ`

   `L = {(x0 - t·b, y0 + t·a), t ∈ ℤ}` (Satz 4.18)

   Je nach Anwendungsaufgabe, stelle `x0 - t·b ≥ 0` und `y0 + t·a ≥ 0` auf; löse nach `t`, um alle (endlich) viele Lösungen zu erschließen.

Lineare dipohantische Gleichung hat entweder 0 oder unendlich viele Lösungen.

Beispiel 1

Werbegeschenkaufgabe von S. 44: 19x + 13y = 1000, wie viele Lösungen (x,y) mit x, y >= 0 gibt es? 4 Lösungen.

Abwandlung von mir: 31x + 23y = 1000, wie viele Lösungen (x,y) mit x, y >= 0 gibt es? 13 Lösungen.

Beispiel 2

Finde alle Lösungen von `6x + 4y = 14`.

1. `ggT(6, 4) = 2 = 1 * 6 - 1 * 4`

2. `ggT(6, 4) = 2 | 14`, okay!

3. Normalisierung: `3x + 2y = 7`, rekursiv:

   1. Berechne

```
3 = 1·2 + 1
2 = 2·2 + 0

⇒ 1 = (1)·(3) + (-1)·(2)
```

    2. `ggT(3, 2) = 1 | 7`, okay!

4. Partikularlösung: `7 · (1, -1) = (7, -7)`
5. Alle Lösungen: `L = {(7 + 2·t, -7 - 3·t) | t in ℤ} = {…, (5, -4), ___(7, -7)___, (9, -10), (11, -13), …}` (dieselben Lösungen von ursprünglicher Gleichung)

Beispiel 3 (mit negativen Koeffizienten!)

Finde alle Lösungen von `-51x + 5y = 13`.

1. Sofort klar: `ggT(-51, 5) = ggT(51, 5) = 1` Berechne trotzdem:

```
-51 = -11 · 5 + 4
  5 =   1 · 4 + 1
  4 =   4 · 1 + 0

⇒ 1 = (-1)·(-51) + (-10)·(5)
```

2. `ggT(-51, 5) = 1 | 13`, d.h. unendlich viele Lösungen existieren!
3. -/-
4. Partikularlösung `13 · (-1, -10) = (-13, -130)`.
5. Alle Lösungen: `L = {(-13 + 5·t, -130 - (-51)·t), t ∈ ℤ}`

kgV

- manuell:

$$kgV(\underset{10\cdot 12}{\underset{||}{120}}, \underset{5\cdot 63}{\underset{||}{315}}) = 5\cdot kgV(2\cdot 12, 63) = 5\cdot kgV(2\cdot 3\cdot 4, 3\cdot 21)$$

$$= 3\cdot 5\cdot kgV(\underset{\text{teilerfremd}}{2\underset{\uparrow}{\cdot}4, 3\underset{\uparrow}{\cdot}7})$$

$$= 3\cdot 5\cdot 2\cdot 4\cdot 3\cdot 7 = 2^3\cdot 3^2\cdot 5\cdot 7 = 2520$$

- geschickter: nutze $ggT(a,b) · kgV(a,b) = a· b$

- für $ggT(a,b) = 1 ⇒ kgV(a,b) = a · b$

Additives Inverse in ℤ/mℤ

- Problem: gesucht ist Inverses von `[a] ∈ ℤ/mℤ`
- Lösung: `[-a]`

Multiplikatives Inverse in ℤ/mℤ

- Problem: gesucht ist Inverses von `[a] ∈ ℤ/mℤ`

- Lösung: löse lineare diophantische Gleichung `ax + my = 1` via Algorithmus oben, nehme eine Partikularlösung für `y`.

  Beachte: Inverses existiert <=> `ggT(a, m) = 1`.

  Ggf. normalisiere erhaltenes `y` auf kanonischen Repräsentanten in ${0, ..., m - 1}$.

Beispiele:

- $[6]*{13}^{-1} = [11]*{13}$ (in Notation der VL: $(\bar{6})^{-1} = \bar{11}$)
- $[15]*{89}^{-1} = [6]*{89}$

Nullteiler

`zero divisor := Σ(a:R) Σ(b:R) a ≠ 0 ∧ b ≠ 0 ∧ ab = 0` (def. from lecture; usually `0` *is* considered a zero divisor...)

e.g. in ℤ/6ℤ: `(2, 3)` is zero divisor

Bestimme Rest von $a^b ÷ m$

> Wenn a und m teilerfremd, wende Satz von Euler an:
>
> $$[a^b]_m = [a]_m^b = [a]*m^{[b]*{\varphi(m)}}$$

Beispiel: $$[3^{387}]*{35} = [3]*{35}^{[387]*{24}} = [3]*{35}^{[3]*{24}} = [27]*{35}$$

da $\varphi(35) = \varphi(5 · 7) = 4 · 6 = 24$.

> Wenn a und m *nicht* teilerfremd, betrachte $\langle [a]_m, · \rangle$ und identifziere Periodenlänge s, sodass
>
> $$[a^b]_m = [a]_m^b = [a]_m^{b'}$$ wobei b' positiver Repräsentant von $[b]_s$ ist.

Beispiel: $$[2^{18}]*{10} = [2]*{10}^{2} = [4]*{10}$$ da $\langle [2]*{10} \rangle = {[1]*{10}, [2]*{10}, [4]*{10}, [8]*{10}, [16]*{10} = [6]*{10}, [12]*{10} = [2]*{10}}$, d.h. $[2]*{10}^5 = [2]*{10}$. Damit ist $s = 4$. Und ein positiver Repräsentant von 18 in $ℤ/sℤ$ ist eben 2.

Gleichungen über Z

Wenn a Faktor von LHS und RHS, dann `LHS = RHS ⇔ LHS/a = RHS/a`.

Verschiedenes

finite commutative monoids with (∀abc. ab = ac => b=c) are groups

Alle ungeraden Quadratzahlen $\equiv 1$ mod 8

Sei $q \in \mathbb{Z}$ und q^2 ungerade. Dann ist q ungerade.

$\bar{q^2} = \bar{q}^2 \in \{\bar{1}^2, \bar{3}^2, \bar{5}^2, \bar{7}^2\} = \{\bar{1}\} \Rightarrow q^2 \equiv 1$ (mod 8)

Alternativ: $q^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1 \equiv 1$, da $8 | 4n(n+1)$, denn $2 | n(n+1)$.

Satz von Euler, Kleiner Fermat'sche Satz

> **Satz (von Euler):** Seien a, m teilerfremd, dann $a^{\varphi(m)} \equiv 1$ (mod m).

(Folgt aus: a, m teilerfremd $\Rightarrow \bar{a} \in \mathbb{Z}_m^* \Rightarrow \bar{1} = \bar{a}^{\mathrm{ord}(\mathbb{Z}_m^\ast)} = \bar{a}^{\varphi(m)}$; group element raised to group order always 1)

> **Satz (kleiner Fermat):** Für $a \in \mathbb{N}$, p prim gilt: $a^p \equiv a$ (mod p)

Wenn $p | a$, trivial $0 \equiv 0$. Sonst $\mathrm{ggT}(a, p) = 1$ und $a^p \equiv a^{p-1}a \equiv 1a \equiv a$.

> **Lemma:** $\varphi(p^n) = p^{n-1} (p-1)$

> **Lemma:** (aus Internet!) $\mathrm{ggT}(a,b) = 1 \quad\Longrightarrow\quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
>
> *Beweis (siehe auch hier):* Nach CRT haben wir $\mathbb{Z}/(ab\mathbb{Z}) \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. D.h. Anzahl invertierbarer Elemente von LHS ist dieselbe wie von RHS. Ein Element (x, y) von RHS ist invertierbar gdw. x in $\mathbb{Z}/a\mathbb{Z}$ invertierbar und y in $\mathbb{Z}/bZ$ invertierbar ist. Es gibt also $\varphi(a) \cdot \varphi(b)$ viele invertierbare Elemente der RHS.

Chinesischer Restsatz

- Problem: Gleichungen $x \equiv a_i$ (mod m_i), z. B.
  - $x \equiv 3$ (mod 5)
  - $x \equiv 1$ (mod 7)
  - $x \equiv 2$ (mod 11)

  mit m_i paarweise teilerfremd. Gibt es Lösung für $x \in \mathbb{Z}$?
- Ja, es gibt eine Lösung x (eindeutig in $\mathbb{Z}/m\mathbb{Z}$, mit $m := \prod m_i$)

  Konstruiere *eine* Lösung $x := a_1 q_1 q_1' + a_2 q_2 q_2' + a_3 q_3 q_3'$ mit
  - $q_1 := 7 \cdot 11 = 77$

    In $\mathbb{Z}/5\mathbb{Z}$: $\bar{q_1} = \bar{2},\quad\bar{2}^{-1} = \bar{3} \Rightarrow$ wähle $q_1' := 3$. (I. Allg. ist $q_1' \in 3 + 5\mathbb{Z}$ möglich.)

- $q_2 = 5 \cdot 11 = 55$

  In $\mathbb{Z}/7\mathbb{Z}$: $\bar{q_2} = 6,\quad\bar{q_2}^{-1} = \bar{6} \Rightarrow$ wähle $q_2' := 6$

- $q_3 = 5 \cdot 7 = 35$

  In $\mathbb{Z}/11\mathbb{Z}$: $\bar{q_3} = 2,\quad\bar{q_3}^{-1} = \bar{6} \Rightarrow$ wähle $q_3' := 6$

Dann $x = 3 \cdot 77 \cdot 3 + 1 \cdot 55 \cdot 6 + 2 \cdot 35 \cdot 6 = 1443$.

Beachte: hier muss etwa 77 stehen, anderer Repräsentant bzgl. $\mathbb{Z}/5\mathbb{Z}$ *nicht* möglich. Für q_i' is jedoch Repräsentenwahl in $\mathbb{Z}/m_i\mathbb{Z}$ frei.

Mit $m := m_1 m_2 m_3 = 385$ ist

- Lösungsmenge $x + m\mathbb{Z} = 1443 + 385\mathbb{Z}$
- kanonischer Repräsentant $x;\%;m = 1443;\%;385 = 288$.

Andere Formulierung:

> **Satz (CRT):** Wenn $m_1, ..., m_k$ paarweise teilerfremd, dann $$\mathbb{Z}/m \cong \mathbb{Z}/m_1 \times \cdots \mathbb{Z}/m_k$$ als Ringe.

Erweiterter CRT mit erlaubten Koeffizienten vor x: siehe https://www.dave4math.com/mathematics/chinese-remainder-theorem/

Konvertierung Dezimalsystem $\rightarrow$ b-System

Immer durch b teilen, Reste ergeben b-Darstellung:

```
                      _____
8924 = 743 · 12 + |  8 |  ^   least significant digit
 743 =  61 · 12 + | 11 |  |
  61 =   5 · 12 + |  1 |  |
   5 =   0 · 12 + |  5 |  |
                   -----

Ergebnis: 51B8
```

Nicht mit Euklidischem Algorithmus verwechseln!

Probe mit TR! Auf Casio fx-991DE Plus: `Mode -> Pfeil runter -> 3 (Base-N) -> 8924 eingeben -> Dec/Hex/Bin/Oct-Taste drücken`

Schriftliches Addieren/Subtrahieren zur Basis b

Beispiele:

- $455_6 + 1_6$
- $210_3 - 1_3$
- $2302_4 - 233_4 = 2003_4$ (tricky mit Borrow und Carry!!)

Dezimalbruchentwicklung

Anzahl Stellen und Periodizität in Dezimalentwicklung *nur* abhängig von Nenner; unterscheide 3 Fälle: Nenner bestehend aus ${2,5}$, teilerfremd mit ${2,5}$ oder gemischt.

> **Sätze 7.1—7.5:** Vollständig gekürzter echte Bruch $\frac{m}{n}$ hat
>
> - *endliche* Dezimalentwicklung $0.q_1...q_s$ ⇔ $n = 2^a · 5^b$
>
>   Entwicklung hat Stellen $s := \max(a,b)$.
>
> - *reinperiodische* Dezimalentwicklung $0.\overline{q_1...q_s}$ ⇔ $\mathrm{ggT}(n, 10) = 1$
>
>   Periodenlänge $s := \min_{s \in ℕ} n \mid (10^s - 1)$
>
> - *gemischtperiodische* Dezimalentwicklung $0.p_1...p_t\overline{q_1...q_s}$ ⇔ $n = n_1 · n_2$ mit $n_1 \mid 10^t$ (t minimal), $\mathrm{ggT}(n_2, 10) = 1$
>
> t Vorziffern; Periodenlänge s ist die von $\frac{1}{n_2}$

Beispiele:

- Wie sieht Dezimalentwicklung von $\frac{3}{125}$ aus?

  Endliche Dezimalbruchentwicklung:

  $$\frac{3}{125} = \frac{3}{5^3} = \frac{3·2^3}{5^3 · 2^3} = \frac{24}{10^3} = 0.024$$

- Wie sieht Dezimalentwicklung von $\frac{1}{15}$ aus?

  $15 = 5 · 3 =: n_1 · n_2 ⇒ t = 1$ Vorziffern und Periodenlänge $1 = \min_{s \in ℕ} 3 \mid (10^s - 1)$.

  $15 = 0.0\overline{6}$.

- Wie sieht Dezimalentwicklung von $\frac{1}{28}$ aus?

  $28 = 2^2 · 7 =: n_1 · n_2 ⇒ t = 2$ Vorziffern und Periodenlänge $6 = \min_{s \in ℕ} 7 \mid (10^s - 1)$.

  $28 = 0.03\overline{571428}$.

Konstruktion periodischer Zahlen

z. B. Periode $z = 173$, Periodenlänge $s = 4$

$$\frac{a}{b} \cdot 10^s = z + \frac{a}{b} \quad\Leftrightarrow\quad \frac{a}{b} = \frac{z}{10^s - 1} = \frac{173}{9999} = 0.\overline{0173}$$

Kettenbruchdarstellung rationaler Zahlen

$$\frac{203}{95} = 2 + \frac{13}{95} = 2 + \frac{1}{\frac{95}{13}} = 2 + \frac{1}{7 + \frac{4}{13}} = 2 + \frac{1}{7 + \frac{1}{\frac{13}{4}}} = 2 + \frac{1}{7 + \frac{1}{3 + \frac{1}{4}}}$$

Daher: $\frac{203}{95} = [2;7,3,4]$.

Auch mit eukl. Algorithmus möglich:

```
          ___
203 = | 2 | · 95 + 13
 95 = | 7 | · 13 +  4
 13 = | 3 | ·  4 +  1
  4 = | 4 | ·  1 +  0
        -----
```

Teilbarkeit

Teilbarkeit bzgl. Zahl mit nur Primfaktoren ${2, 5}$

⇒ Endstellenregeln

> **Satz (Endstellenregeln; Formulierung von mir):** Sei $t \mid 10^s$, dann gilt
>
> $$z_n...z_0 ≡ z_{s-1}...z_0 \text{ (mod } t\text{)}

Beweis: $z_n...z_0 = \sum_{i=0}^n z_i 10^i ≡ \sum_{i=0}^{s-1} z_i 10^i = z_{s-1}...z_0$ (mod t).

Beispiele:

- 2, 5, 10 Teiler von 10 ⇒ Teilbarkeit auf letzte Stelle reduzierbar
- 4, 25, 50, 100 Teiler von 100 ⇒ Teilbarkeit auf letzte zwei Stellen reduzierbar

  $$4 \mid 87954236 ⇔ 4 \mid 36 ⇔ \text{wahr}$$

- 8, 125, 200, ... Teiler von 1000 ⇒ Teilbarkeit auf letzte drei Stellen reduzierbar

Quersummenregeln

> **Satz (Quersummenregeln; Formulierung von mir):**
>
> Sei $t \mid 9$, dann gilt:
>
> $$z_n...z_0 ≡ z_n + ... + z_0 \text{ (mod } t\text{)}$$
>
> Sei $t \mid 99$, dann gilt:
>
> $$z_n...z_0 ≡ z_nz_{n-1} + ... + z_1z_0 \text{ (mod } t\text{)}$$
>
> Sei $t \mid 999$, dann gilt:
>
> $$z_n...z_0 ≡ z_nz_{n-1}z_{n-2} + ... + z_2z_1z_0 \text{ (mod } t\text{)}$$

Das sind Quersummen 1-, 2-, 3- und i. Allg. s-ter Ordnung. (Um Notation für die Gruppierungen oben zu sparen, setzen wir oBdA. $s \mid (n + 1)$ voraus, ansonsten linkspadde mit Nullen.)

Beispiele:

- $11 \mid 21748 ⇔ 11 \mid (01 + 17 + 48) ⇔ 11 \mid 66 ⇔ \text{wahr}$
- $111 \mid 21748 ⇔ 111 \mid (021 + 748) = 769 ⇔ \text{falsch}$

Beweis: (für $t \mid 999$): $$ \begin{aligned} z_n...z_0 = \sum_{i=0}^n z_i 10^i = &(z_n · 10^2 + z_{n-1} 10^1 + z_{n-2}) · 10^{(3·k)}\

- &...\
- &(z_5 · 10^2 + z_4 · 10^1 + z_3) · 10^{(3·1)}\
- &(z_2 · 10^2 + z_1 10^1 + z_0) · 10^{(3·0)}\ \equiv &z_nz_{n-1}z_{n-2} + ... + z_5z_4z_3 + z_2z_1z_0 \end{aligned} $$

> **Satz:** Für $s ≥ 1$ und $t \mid (10^s + 1)$ gilt: $$z_n ... z_0 ≡ \text{alt. Quersumme }s\text{-ter Ordnung}\quad\text{(mod } t\text{)}$$

Beispiele:

- $11 \mid 6391 ⇔ 11 \mid (-6 + 3 - 9 + 1) = -11 ⇔ \text{wahr}$
- $101 \mid 100102 ⇔ 101 \mid (100 + 102) = 202 ⇔ \text{wahr}$
- $7 \mid 1001$, d.h. 7 teilt Zahl gdw. 7 teilt die alt. Quersumme 3-ter Ordnung

Teilbarkeit bzgl. 7 und 11

Siehe Skript.