DS

Tutorial

Norina Grosch, Sebastian Reichmann

19. November 2019

Organisatorisches

Feedback, Kritik, Wünsche per Unimail an:

- norina.marie.grosch [at] uni-weimar.de
- sebastian.reichmann [at] uni-weimar.de

Bitte an beide Mails, dann bekommt ihr schneller eine Antwort.
Die Folien findet ihr :
`www.uni-weimar.de/~qari3759/tutorium`

Am Besten bis Freitag Abend, damit wir es noch einarbeiten können ;)

Das Tutoriat ist nicht für das Lösen der Übungsaufgaben bestimmt!

Ablauf

1. Anmerkungen zu Belegabgaben
2. Stoffwiederholung

Section 1

Anmerkungen zu Belegabgaben

Abgaben

- $7^{(7^7)} \neq (7^7)^7$
- Beweise
  - Was wird bewiesen?
  - Beispiele sind kein Beweis
- Aufgabenstellungen lesen: ist $X \subseteq \mathbb{N}$?

Section 2

Stoffwiederholung

Erweiterter Euklidischer Algorithmus

- ggT berechnen
- multiplikatives Inverse finden
  - $ggT(a, b) = s \cdot a + t \cdot b = 1$
  - $1 \equiv t \cdot b \ (mod\ a)$

Erweiterter Euklidischer Algorithmus

- ggT berechnen
- multiplikatives Inverse finden
  - $ggT(a, b) = s \cdot a + t \cdot b = 1$
  - $1 \equiv t \cdot b \ (mod\ a)$
    $\rightarrow$ t ist das multiplikative Inverse zu b modulo a

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$a = x \cdot b + r$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$a = x \cdot b + r$$

$$110 = 3 \cdot 29 + 23$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$a = x \cdot b + r$$
$$110 = 3 \cdot 29 + 23$$
$$29 = 1 \cdot 23 + 6$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$a = x \cdot b + r$$
$$110 = 3 \cdot 29 + 23$$
$$29 = 1 \cdot 23 + 6$$
$$23 = 3 \cdot 6 + 5$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$
\begin{aligned}
a &= x \cdot b + r \\
110 &= 3 \cdot 29 + 23 \\
29 &= 1 \cdot 23 + 6 \\
23 &= 3 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1 \rightarrow (ggtT = 1)
\end{aligned}
$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$
\begin{aligned}
a &= x \cdot b + r \\
110 &= 3 \cdot 29 + 23 \\
29 &= 1 \cdot 23 + 6 \\
23 &= 3 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1 \rightarrow (ggtT = 1) \\
5 &= 5 \cdot 1 + 0
\end{aligned}
$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$
\begin{aligned}
a &= x \cdot b + r \\
110 &= 3 \cdot 29 + 23 \\
29 &= 1 \cdot 23 + 6 \\
23 &= 3 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1 \rightarrow (ggtT = 1) \\
5 &= 5 \cdot 1 + 0
\end{aligned}
$$

Zurück rechnen:

$$1 = 6 - 1 \cdot 5$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$
\begin{aligned}
a &= x \cdot b + r \\
110 &= 3 \cdot 29 + 23 \\
29 &= 1 \cdot 23 + 6 \\
23 &= 3 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1 \rightarrow (ggtT = 1) \\
5 &= 5 \cdot 1 + 0
\end{aligned}
$$

Zurück rechnen:

$$
\begin{aligned}
1 &= 6 - 1 \cdot 5 \\
1 &= 6 - 1 \cdot (23 - 3 \cdot 6) = -1 \cdot 23 + 4 \cdot 6
\end{aligned}
$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$
\begin{aligned}
a &= x \cdot b + r \\
110 &= 3 \cdot 29 + 23 \\
29 &= 1 \cdot 23 + 6 \\
23 &= 3 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1 \rightarrow (ggtT = 1) \\
5 &= 5 \cdot 1 + 0
\end{aligned}
$$

Zurück rechnen:

$$
\begin{aligned}
1 &= 6 - 1 \cdot 5 \\
1 &= 6 - 1 \cdot (23 - 3 \cdot 6) = -1 \cdot 23 + 4 \cdot 6 \\
1 &= -1 \cdot 23 + 4 \cdot (29 - 1 \cdot 23) = 4 \cdot 29 - 5 \cdot 23
\end{aligned}
$$

Multiplikatives Inverses berechnen

Für a = 110 und b = 29: $ggT(29, 110) = 1$ und $1 \equiv t \cdot 29 \ (mod\ 110)$

$$
\begin{aligned}
a &= x \cdot b + r \\
110 &= 3 \cdot 29 + 23 \\
29 &= 1 \cdot 23 + 6 \\
23 &= 3 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1 \rightarrow (ggtT = 1) \\
5 &= 5 \cdot 1 + 0
\end{aligned}
$$

Zurück rechnen:

$$
\begin{aligned}
1 &= 6 - 1 \cdot 5 \\
1 &= 6 - 1 \cdot (23 - 3 \cdot 6) = -1 \cdot 23 + 4 \cdot 6 \\
1 &= -1 \cdot 23 + 4 \cdot (29 - 1 \cdot 23) = 4 \cdot 29 - 5 \cdot 23 \\
1 &= 4 \cdot 29 - 5 \cdot (110 - 3 \cdot 29) = -5 \cdot 110 + 19 \cdot 29 \rightarrow t = 19
\end{aligned}
$$

Erweiterter Euklidischer Algorithmus

Nochmal exakt das gleiche, nur anders aufgeschrieben (tabellarische Form aus der Vorlesung)

$a = 110, b = 29$

a	b	$a = z \cdot b + r$	z	r	$(d, x, y) = (d_o, y_o, x_o - z \cdot y_o)$
110	29	$110 = 3 \cdot 29 + 23$	3	23	
29	23	$29 = 1 \cdot 23 + 6$	1	6	
23	6	$23 = 3 \cdot 6 + 5$	3	5	
6	5	$6 = 1 \cdot 5 + 1$	1	1	
5	1	$5 = 5 \cdot 1 + 0$	5	0	

d_o, x_o, y_o sind die entsprechenden Werte aus der Zeile darunter, z stammt aus der gleichen Zeile!

Erweiterter Euklidischer Algorithmus

Nochmal exakt das gleiche, nur anders aufgeschrieben (tabellarische Form aus der Vorlesung)

$a = 110, b = 29$

a	b	$a = z \cdot b + r$	z	r	$(d, x, y) = (d_o, y_o, x_o - z \cdot y_o)$
110	29	$110 = 3 \cdot 29 + 23$	3	23	
29	23	$29 = 1 \cdot 23 + 6$	1	6	
23	6	$23 = 3 \cdot 6 + 5$	3	5	
6	5	$6 = 1 \cdot 5 + 1$	1	1	
5	1	$5 = 5 \cdot 1 + 0$	5	0	$(1, 0, 1)$

Von unten nach oben zurück rechnen, mit (1, 0, 1) anfangen (so $ggT(a, b) = 1$)

Erweiterter Euklidischer Algorithmus

Nochmal exakt das gleiche, nur anders aufgeschrieben (tabellarische Form aus der Vorlesung)

$a = 110, b = 29$

a	b	$a = z \cdot b + r$	z	r	$(d, x, y) = (d_o, y_o, x_o - z \cdot y_o)$
110	29	$110 = 3 \cdot 29 + 23$	3	23	$(1, -5, 4 - (3 \cdot -5)) = (1, -5, 19)$
29	23	$29 = 1 \cdot 23 + 6$	1	6	$(1, 4, -1 - (1 \cdot 4)) = (1, 4, -5)$
23	6	$23 = 3 \cdot 6 + 5$	3	5	$(1, -1, 1 - (3 \cdot -1)) = (1, -1, 4)$
6	5	$6 = 1 \cdot 5 + 1$	1	1	$(1, 1, 0 - (1 \cdot 1)) = (1, 1, -1)$
5	1	$5 = 5 \cdot 1 + 0$	5	0	$(1, 0, 1)$

Das multiplikative Inverse von 29 modulo 110 ist also 19
Probe: $29 \cdot 19 \mod 110 = 551 \mod 110 = 1$

Multiplikatives Inverses Aufgabe

Gegeben: $a = 91$, $b = 8$ und $ggT(91, 8) = 1$
Gesucht: $1 \equiv t \cdot 8 \ (mod\ 91)$

Hinweis: $t \in \mathbb{N}$, wenn $t < 0$ dann $t = t + a$

Multiplikatives Inverses Aufgabe

Gegeben: $a = 91$, $b = 8$ und $ggT(91, 8) = 1$
Gesucht: $1 \equiv t \cdot 8 \ (mod\ 91)$

Hinweis: $t \in \mathbb{N}$, wenn $t < 0$ dann $t = t + a$

Lösung: $1 \equiv 57 \cdot 8 \ (mod\ 91)$

Erweiterter Euklidischer Algorithmus

Lösung in tabellarischer Form:

$a = 91, b = 8$

a	b	$a = z \cdot b + r$	z	r	$(d, x, y) = (d_o, y_o, x_o - z \cdot y_o)$
91	8	$91 = 11 \cdot 8 + 3$	11	3	$(1, 3, -1 - (11 \cdot 3)) = (1, 3, -34)$
8	3	$8 = 2 \cdot 3 + 2$	2	2	$(1, -1, 1 - (2 \cdot -1)) = (1, -1, 3)$
3	2	$3 = 1 \cdot 2 + 1$	1	1	$(1, 1, 0 - (1 \cdot 1)) = (1, 1, -1)$
2	1	$2 = 2 \cdot 1 + 0$	2	0	$(1, 0, 1)$

Das multiplikative Inverse von 8 modulo 91 ist also $-34 \mod 91 = 57$
Probe: $8 \cdot 57 \mod 91 = 456 \mod 91 = 1$

Gruppeneigenschaften

- Gruppoid:
  - Nichtleere Menge G
  - Verknüpfung $\circ : G \times G \rightarrow G$ (Abgeschlossenheit)

Gruppeneigenschaften

- Gruppoid
- Halbgruppe:
  - Assoziativität $a \circ (b \circ c) = (a \circ b) \circ c$

Gruppeneigenschaften

- Gruppoid
- Halbgruppe
- Monoid
  - Neutrales Element $a \circ e = e \circ a = a$

Gruppeneigenschaften

- Gruppoid
- Halbgruppe
- Monoid
- Gruppe
  - Inverses Element $a \circ a^{-1} = e$

Chinesischer Restsatz

$$x \equiv a_i \ mod \ m_i$$
$$m = m_1 * \ldots * m_i$$
$$M_i = \frac{m}{m_i}$$
$$y_i = M_i^{-1} mod \ m_i$$
$$x = (a_1 * y_1 * M_1 + \ldots + a_i * y_i * M_i) \ mod \ m$$

Chinesischer Restsatz

$x \equiv a_i \ mod \ m_i$
$m = m_1 * \ldots * m_i$
$M_i = \frac{m}{m_i}$
$y_i = M_i^{-1} mod \ m_i$
$x = (a_1 * y_1 * M_1 + \ldots + a_i * y_i * M_i) \ mod \ m$

gegeben:
$x \equiv 4 \ mod \ 5$
$x \equiv 3 \ mod \ 7$
$x \equiv 2 \ mod \ 11$

Chinesischer Restsatz

$x \equiv a_i \ mod \ m_i$
$m = m_1 * \ldots * m_i$
$M_i = \frac{m}{m_i}$
$y_i = M_i^{-1} mod \ m_i$
$x = (a_1 * y_1 * M_1 + \ldots + a_i * y_i * M_i) \ mod \ m$

gegeben:
$x \equiv 4 \ mod \ 5$
$x \equiv 3 \ mod \ 7$
$x \equiv 2 \ mod \ 11$

$m = 5 \cdot 7 \cdot 11 = 385$

Chinesischer Restsatz

$x \equiv a_i \ mod \ m_i$
$m = m_1 * \ldots * m_i$
$M_i = \frac{m}{m_i}$
$y_i = M_i^{-1} mod \ m_i$
$x = (a_1 * y_1 * M_1 + \ldots + a_i * y_i * M_i) \ mod \ m$

gegeben:
$x \equiv 4 \ mod \ 5$
$x \equiv 3 \ mod \ 7$
$x \equiv 2 \ mod \ 11$

$m = 5 \cdot 7 \cdot 11 = 385$
$M_1 = \frac{385}{5} = 77, \ M_2 = \frac{385}{7} = 55, \ M_3 = \frac{385}{11} = 35$

Chinesischer Restsatz

gegeben:

$x \equiv 4 \ mod \ 5$

$x \equiv 3 \ mod \ 7$

$x \equiv 2 \ mod \ 11$

$m = 5 \cdot 7 \cdot 11 = 385$

$M_1 = \frac{385}{5} = 77, \ M_2 = \frac{385}{7} = 55, \ M_3 = \frac{385}{11} = 35$

Chinesischer Restsatz

gegeben:

$x \equiv 4 \ mod \ 5$

$x \equiv 3 \ mod \ 7$

$x \equiv 2 \ mod \ 11$

$m = 5 \cdot 7 \cdot 11 = 385$

$M_1 = \frac{385}{5} = 77, \ M_2 = \frac{385}{7} = 55, \ M_3 = \frac{385}{11} = 35$

$y_i = M_i^{-1} \ mod \ m_i$

$y_1 : 77^{-1} \ mod \ 5 = 2^{-1} \ mod \ 5 \equiv 3$

$y_2 : 55^{-1} \ mod \ 7 = 6^{-1} \ mod \ 7 \equiv 6$

$y_3 : 35^{-1} \ mod \ 11 = 2^{-1} \ mod \ 11 \equiv 6$

Chinesischer Restsatz

gegeben:

$x \equiv 4 \ mod \ 5$

$x \equiv 3 \ mod \ 7$

$x \equiv 2 \ mod \ 11$

$m = 5 \cdot 7 \cdot 11 = 385$

$M_1 = \frac{385}{5} = 77, \ M_2 = \frac{385}{7} = 55, \ M_3 = \frac{385}{11} = 35$

$y_i = M_i^{-1} \ mod \ m_i$

$y_1 : 77^{-1} \ mod \ 5 = 2^{-1} \ mod \ 5 \equiv 3$

$y_2 : 55^{-1} \ mod \ 7 = 6^{-1} \ mod \ 7 \equiv 6$

$y_3 : 35^{-1} \ mod \ 11 = 2^{-1} \ mod \ 11 \equiv 6$

$x = (a_1 * y_1 * M_1 + \ldots + a_i * y_i * M_i) \ mod \ m$

$x = (4 \cdot 3 \cdot 77 + 3 \cdot 6 \cdot 55 + 2 \cdot 6 \cdot 35) \ mod \ 385 = 24$

Chinesischer Restsatz - Aufgabe

$x \equiv a_i \ mod \ m_i$
$m = m_1 * \ldots * m_i$
$M_i = \frac{m}{m_i}$
$y_i = M_i^{-1} mod \ m_i$
$x = (a_1 * y_1 * M_1 + \ldots + a_i * y_i * M_i) \ mod \ m$

gegeben:
$x \equiv 2 \ mod \ 7$
$x \equiv 5 \ mod \ 9$

Chinesischer Restsatz - Aufgabe

$x \equiv a_i \ mod \ m_i$
$m = m_1 * \ldots * m_i$
$M_i = \frac{m}{m_i}$
$y_i = M_i^{-1} mod \ m_i$
$x = (a_1 * y_1 * M_1 + \ldots + a_i * y_i * M_i) \ mod \ m$

gegeben:
$x \equiv 2 \ mod \ 7$
$x \equiv 5 \ mod \ 9$

$m = 63$
$M_1 = 9, M_2 = 7$
$y_1 = 4, y_2 = 4$
$x = (2 \cdot 4 \cdot 9 + 5 \cdot 4 \cdot 7) \ mod \ 63 = 23$

Fragen?

https://pbs.twimg.com/profile_images/472920133414158336/8MqCNSsC.jpeg