Einführung in die Zahlentheorie 2

Prof. Dr. Josef F. Bürgler

Studiengang Informatik
Hochschule Luzern, Informatik

I.BA_DMATH

Übersicht

Übersicht

Übersicht

Restklassen

Man kann beweisen, dass Kongruenz modulo m eine so genannte Äquivalenzrelation auf $\mathbb{Z}$ ist und $\mathbb{Z}$ unter dieser Relation in n paarweise disjunkte Äquivalenzklassen (hier Restklassen) zerfällt.

$$[r] = \{x \in \mathbb{Z} \mid x \equiv r \bmod n\}$$

In jeder Restklasse gibt es genau einen der Reste $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, die bei Division durch n auftreten können.

Example

$n = 3$

$$\mathbb{Z} = \underbrace{[0]}_{\{\ldots,-6,-3,0,3,6,\ldots\}} \cup \underbrace{[1]}_{\{\ldots,-5,-2,1,4,7,\ldots\}} \cup \underbrace{[2]}_{\{\ldots,-4,-1,2,5,8,\ldots\}}$$

Übersicht

Modulare Rechenoperationen

Definition

Sei $n \geqslant 2$. Wir führen auf der Menge $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ eine Addition $\oplus_n$ und eine Multiplikation $\odot_n$ ein. Für $a, b \in \mathbb{Z}_n$ sei:

$$a \oplus_n b = a + b \ \textbf{mod} \ n = R_n(a+b)$$
$$a \odot_n b = a \cdot b \ \ \textbf{mod} \ n = R_n(a \cdot b)$$

Wir könnten auch noch weitere Operationen auf $\mathbb{Z}_n$ einführen, z.B.

$$a \ominus_n b = a - b \ \textbf{mod} \ n = R_n(a-b)$$

Example

$n = 6$ und $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$3 \oplus_6 4 = R_6(3+4) = 1$ problemlos
$3 \ominus_6 4 = R_6(3-4) = 5$ problemlos
$3 \odot_6 4 = R_6(3 \cdot 4) = 0$ problemlos aber ungewöhnlich

Rechenregeln beim modularen Rechnen

Theorem (Rechenregeln)

Sei $a \geqslant 2$ *und* $a, b, c \in \mathbb{Z}_n$. *Dann gilt*

$$a \oplus_n b = b \oplus_n a$$
$$a \oplus_n 0 = a$$
$$a \odot_n b = b \odot_n a$$
$$a \odot_n 1 = a$$
$$a \odot_n (b \oplus_n c) = (a \odot_n b) \oplus_n (a \odot_n c)$$

Example

Berechnen Sie

$$3 \odot_5 (2 \oplus_5 4) =$$
$$3 \odot_7 (2 \oplus_7 4) =$$
$$(3 \odot_5 2) \oplus_5 (3 \odot_5 4) =$$
$$(3 \odot_7 2) \oplus_7 (3 \odot_7 4) =$$

Rechenregeln beim modularen Rechnen (Fort.)

Example ($\mathbb{Z}_2$)

$\oplus_2$	0	1
0	0	1
1	1	0

$\odot_2$	0	1
0	0	0
1	0	1

Example ($\mathbb{Z}_3$)

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Example ($\mathbb{Z}_4$)

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Rechenregeln beim modularen Rechnen (Fort.)

Example ($\mathbb{Z}_5$)

Ergänzen Sie alle fehlenden Einträge:

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1				
2	2				
3	3				
4	4				

$\odot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0				
2	0				
3	0				
4	0				

Übersicht

(Effizientes) Potenzieren modulo n

Wir wollen zeigen, wie man effizient Potenzen x^m **mod** n berechnet.

Allgemein: Reelle Potenzen x^m mit Exponenten $m \in \mathbb{N}$ können durch fortlaufendes Quadrieren und Multiplizieren berechnet werden.

Vorgehen: Schreibe $m = 2 \cdot k + l$ mit $l \in \{0, 1\}$ und

$$x^m = x^{2 \cdot k + l} = x^{2 \cdot k} \cdot x^l = (x^k)^2 \cdot x^l$$

k ist etwa halb so gross wie m. Fahre mit x^k in gleicher Weise (rekursiv) fort.

Example

$$x^{10} = x^{2 \cdot 5 + 0} = (x^5)^2 \cdot x^0 = (x^{2 \cdot 2 + 1})^2 \cdot x^0 = ((x^2)^2 \cdot x^1)^2 \cdot x^0$$

9 Multiplikationen $\longrightarrow$ 3 Quadrate und 2 Multiplikationen

Effizientes Potenzieren modulo n

SMA (Square and Multiply Algorithm)

Wie berechnet man effzient die modulare Potenz 5^{21} **mod** 11?

- Exponent binär schreiben und 2 nach rechts ausklammern:

$$\begin{aligned} 21 \;=\; (10101)_2 &= 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 \\ &= 2^4 + 2^2 + 1 \;=\; (2\cdot 2+1)\cdot 2\cdot 2 + 1 \end{aligned}$$

- Exponent einsetzten und entsprechend Quadrieren, Multiplizieren sowie modular reduzieren:

$$\begin{aligned} 5^{21} \bmod 11 &= 5^{(2\cdot 2+1)\cdot 2\cdot 2+1} && \bmod 11 \\ &= (((5^2)^2\cdot 5)^2)^2\cdot 5 && \bmod 11 \\ &= (((25)^2\cdot 5)^2)^2\cdot 5 && \bmod 11 \\ &\equiv ((3^2\cdot 5)^2)^2\cdot 5 && \bmod 11 \\ &= (1^2)^2\cdot 5 && \bmod 11 \\ &= 5 \end{aligned}$$

SMA (Fort.)

Formal:

- Q bedeutet quadrieren und M multiplizieren
- Ersetze in der binären Darstellung des Exponenten jede 1 durch QM und jede 0 durch Q

  $(10101)_2 \rightarrow$ QMQQMQQM
- Streiche das erste (links) QM

  QMQQMQQM $\rightarrow$ QQMQQM
- Das Symbol QQMQQM gibt die Reihenfolge von Quadrieren und Multiplizieren an, um die Potenz zu berechnen. Nach jeder Operation sollte das Ergebnis modulo 11 reduziert werden.

Übersicht

Nullteiler

Definition

Existiert zu einem $a \in \mathbb{Z}_n$ mit $a \neq 0$ ein $b \in \mathbb{Z}_n$ mit $b \neq 0$ so dass $a \odot_n b = 0$ gilt, so heisst a ein Nullteiler von $\mathbb{Z}_n$.

Bemerkungen:

- Nullteiler gibt es in $\mathbb{Z}$ oder $\mathbb{R}$ (mit der gewöhnlichen Multiplikation) **nicht**!
- Falls es in $\mathbb{Z}_n$ Nullteiler gibt, kann in $\mathbb{Z}_n$ **nicht** jede Gleichung $a \odot_n x = b$ gelöst werden. Das ist unangenehm!

Example

In $\mathbb{Z}_4$ hat die Gleichung $2 \odot_n x = 1$ keine Lösung x (siehe Multiplikationstabelle).

Nullteiler (Fort.)

Theorem

Sei $n = p$ eine Primzahl. Dann gilt:

1. $\mathbb{Z}_p$ *ist nullteilerfrei und*
2. *für alle* $a, b \in \mathbb{Z}_p$ *besitzt die Gleichung*

$$a \odot_p x = b$$

genau eine Lösung x.

Example

$\mathbb{Z}_3$: $2 \odot_3 x = 1$ Lösung: $x = 2$
$\mathbb{Z}_4$: $2 \odot_4 x = 1$ keine Lösung

Übersicht

Inverse Elemente

In $\mathbb{Z}$ hat fast kein Element ein multiplikatives Inverses. Die Gleichung $x \cdot y = 1$ hat in $\mathbb{Z}$ nur die Lösungen $1 \cdot 1 = 1$ und $(-1) \cdot (-1) = 1$.

In $\mathbb{R}$ ist jedes Element bis auf 0 invertierbar, denn $x \cdot \frac{1}{x} = 1$.

Erstaunlicherweise haben in $\mathbb{Z}_n$ viele Elemente ein multiplikatives Inverses!

Theorem

Sei n eine natürliche Zahl und $a \in \mathbb{Z}_n$. a hat genau dann ein Inverses bezüglich der Multiplikation $\odot_n$ in $\mathbb{Z}_n$, wenn $\mathrm{ggT}(a, n) = 1$ gilt.

Die Menge aller invertierbaren Elemente in $\mathbb{Z}_n$ sei mit $\mathbb{Z}_n^*$ bezeichnet. Es gilt also:

$$\mathbb{Z}_n^* = \{\, a \in \mathbb{Z}_n \mid \mathrm{ggT}(a, n) = 1 \,\}.$$

Inverse Elemente (Fort.)

Example

In $\mathbb{Z}_3 = \{0, 1, 2\}$ gilt $\mathbb{Z}_n^* = \{1, 2\}$, denn

- $1 \odot_3 1 = 1$ also $1^{-1} = 1$ und
- $2 \odot_3 2 = 1$ also $2^{-1} = 2$.

Zur Erinnerung: Multiplikative Inverse können mit Hilfe des Euklidschen Algorithmus (leicht) bestimmt werden!

Example

Bestimmen Sie alle invertierbaren Elemente in $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ und geben Sie die jeweiligen Inversen an.

In Zukunft rechnen wir nur noch in $\mathbb{Z}_n^*$.

Das Inverse berechnen mit dem kleinen Fermat

Sei p eine Primzahl. In diesem Fall kann der **Kleine Satz von Fermat** genutzt werden, um die Inversen systematisch zu bestimmen. Sei $a \in \mathbb{Z}_p^*$. Dann gilt

$$a^{p-1} = a \cdot a^{p-2} = 1 \textbf{ mod } p$$

und somit

$$a \odot_p R_p(a^{p-2}) = 1$$

d.h. $a^{-1} = R_p(a^{p-2}) = a^{p-2}$ **mod** p ist das Inverse zu a.

Example

Bestimmen Sie mit dem obigen Verfahren alle Inversen in $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.

Übersicht

Primitive Elemente

Definition

Sei p eine Primzahl. Ein Element $z \in \mathbb{Z}_p^*$ heisst **primitives Element**, von $\mathbb{Z}_p^*$, falls jedes Element $a \in \mathbb{Z}_p^*$ eine Potenz von z ist.

Example

In $\mathbb{Z}_5^*$ ist z.B. $z = 2$ ein primitives Element, denn $2^1 = 2$, $2^2 = 4$, $2^3 = 3$ und $2^4 = 1$.
Finden Sie die primitiven Elemente in $\mathbb{Z}_{11}^*$.

Übersicht

Übersicht

Einwegfunktionen

Eine Einwegfunktion ist eine Funktion, die einfach auszuführen, aber schwer (oder besser: praktisch unmöglich) zu invertieren ist.

Definition

Eine **Einwegfunktion** ist eine Abbildung f einer Menge X in eine Menge Y, so dass $f(x)$ für jedes Element in X leicht berechnet werden kann, während es für jedes y aus Y extrem schwer ist, ein Urbild x zu finden. Ist eine Einwegfunktion bijektiv, nennen wir sie **Einwegpermutation**. Eine Einwegfunktion heisst **kollisionsfrei**, falls es praktisch unmöglich ist, zwei verschiedenen $x, x' \in X$ mit $f(x) = f(x')$ zu finden.

Ein Telefonbuch ist ein ganz alltägliches Beispiel einer Einwegfunktion. Zu einem Namen kann leicht und schnell die zugehörige Telefonnummer bestimmt werden, aber es ist sehr schwierig zu einer gegebenen Nummer den Besitzer des Anschlusses zu bestimmen.

Einwegfunktionen — Bemerkungen

1. Einwegfunktionen spielen in der theoretischen und praktischen Kryptographie eine entscheidende Rolle, aber man weiss bis heute nicht, ob es Einwegfunktionen überhaupt gibt!!

2. Einige Einwegfunktionen (nach heutigem Wissensstand. Die Zahlen p und q seien dabei stets verschiedene Primzahlen.

   1. Quadrieren modulo $n = pq$:

      $$x \mapsto x^2 \textbf{ mod } n$$

   2. Potenzieren modulo $n = pq$:

      $$x \mapsto x^e \textbf{ mod } n$$

   3. Diskrete Exponentialfunktion modulo p:

      $$k \mapsto b^k \textbf{ mod } p$$

Übersicht

Modulare Quadratwurzeln

Modulare Quadratwurzeln (und modulare Logarithmen) sind in der Kryptographie von besonderem Interesse (Einwegfunktionen).

Definition

Sei $a \in \mathbb{Z}_n^*$. Eine Lösung $x \in \mathbb{Z}_n^*$ (falls sie existiert) der Gleichung

$$x^2 \;=\; a \;\mathbf{mod}\; n \text{ bzw. } x \odot_n x = a$$

heisst **modulare Quadratwurzel modulo** n.

Bezeichnung: $x \;=\; \sqrt{a} \;\mathbf{mod}\; n$

Achtung: Das ist keine Funktion, denn für ein gegebenes a kann es keine, genau eine oder mehrere modulare Quadratwurzeln geben. Deshalb schreiben wir auch:

$$\sqrt{a} \;\mathbf{mod}\; n = \{\, x \in \mathbb{Z}_n^* \mid x^2 \;=\; a \;\; \mathbf{mod}\; n \,\}$$

Modulare Quadratwurzeln (Fort.)

Example

$n = 7$ und $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

x	1	2	3	4	5	6
$x^2 = x \odot_7 x$	1	4	2	2	4	1

a	1	2	3	4	5	6
$\sqrt{a}$ **mod** 7	1, 6	3, 4	-	2, 5	-	-

Es gibt in $\mathbb{Z}_7^*$ Elemente

- ohne (3, 5 und 6) und
- mit genau zwei (1, 2 und 4)

Quadratwurzeln. Ungewöhnlich!?

Modulare Quadratwurzeln (Fort.)

Example

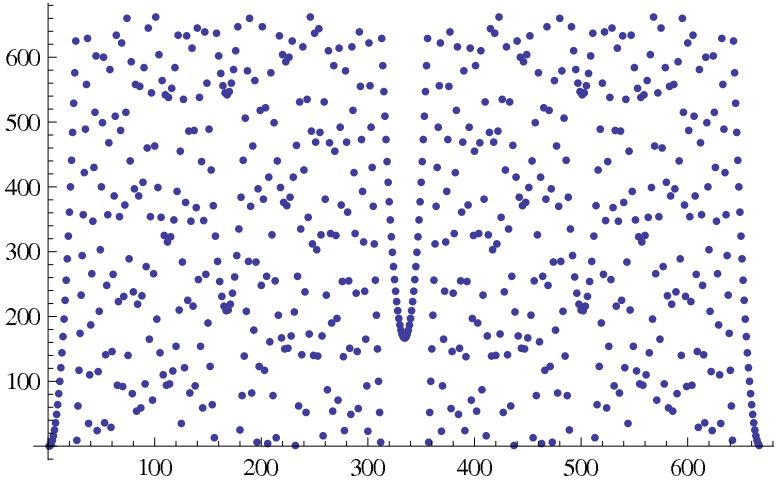
$n = 14$ und $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$

Ergänzen Sie die folgenden Tabellen:

x	1	3	5	9	11	13
$x^2 = x \odot_{14} x$						

a	1	3	5	9	11	13
$\sqrt{a} \mod 14$						

Modulare Qudrate modulo 667



Modulare Quadratwurzeln (Fort.)

Es gilt:

- Falls $n = p$ eine Primzahl ist, so hat jedes Element in $\mathbb{Z}_p^*$ keine oder genau zwei Quadratwurzeln (x und $p - x$).
- Falls $n = p \cdot q$ das Produkt von zwei verschiedenen Primzahlen $(p, q \neq 2)$ ist, so hat jedes Element in $\mathbb{Z}_n^*$ entweder keine oder genau vier Quadratwurzeln (x, $n - x$, y, $n - y$).

Modulare Quadratwurzeln (Fort.)

Auch die Bestimmung der modularen Quadratwurzeln ist schwierig (hier durch Berechnung aller Quadrate).

Ist n eine Primzahl, so gibt es schnelle Verfahren.

Ist n aber zusammengesetzt, gibt es keine schnellen Verfahren! Das modulare Quadrieren scheint hier eine Einwegfunktion zu sein.

$$\text{Einfach:} x \longrightarrow x^2 \bmod n$$

$$\text{Schwierig:} a \longrightarrow \sqrt{a} \bmod n$$

Theorem

Sei $n = p \cdot q$ das Produkt zweier verschiedener Primzahlen p und q (beide $\neq 2$). Dann ist das Berechnen von Quadratwurzeln modulo n genau so schwierig, wie das Faktorisieren von n.

Übersicht

Der diskrete Logarithmus

Sei p stets eine Primzahl und $b \in \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.

Definition

Die **diskrete Exponentialfunktion zur Basis** b **modulo** p ist definiert (und effizient berechenbar) durch

$$\exp_b(k) = b^k \textbf{ mod } p.$$

Definition

Unter dem **Problem des diskreten Logarithmus** versteht man:

Finde zu gegebenem $y \in \mathbb{Z}_p^*$ ein $k \in \mathbb{N}$ (falls es existiert), so dass die folgende Gleichung erfüllt ist:

$$y = b^k \textbf{ mod } p$$

Man schreibt auch: $k = \log_b(y) \textbf{ mod } p$

Der diskrete Logarithmus (Fort.)

Die diskrete Exponentialfunktion scheint eine Einwegfunktion zu sein.

$$\text{Einfach:} \quad k \longrightarrow b^k \bmod p$$

$$\text{Schwierig:} \quad y \longrightarrow \log_b(y) \bmod p$$

Example

Finden Sie eine Lösung k der Gleichung $7 = 3^k \bmod 17$.

$k = \log_3(7) \bmod 17 =$

Übersicht

Diffie-Hellmann Schlüsselvereinbarung

Können zwei Personen A und B ein Geheimnis (z.B. einen Schlüssel) vereinbaren, obwohl jemand ihre Kommunikation vollständig überwacht? Nein, unmöglich!? Es geht, falls es Einwegfunktionen gibt!

Diffie-Hellmann Schlüsselvereinbarung

1. Wähle zwei (allgemein bekannte) natürliche Zahlen p und s
2. A wählt eine (nur ihm bekannte) Zufallszahl $a < p$, berechnet $\alpha = s^a \bmod p$ und sendet α über einen (öffentlichen) Kanal an B
   B wählt eine (nur ihm bekannte) Zufallszahl $b < p$, berechnet $\beta = s^b \bmod p$ und sendet β über einen (öffentlichen) Kanal an A
3. A berechnet $\beta^a \bmod p = s^{b\cdot a} \bmod p$
   B berechnet $\alpha^b \bmod p = s^{b\cdot a} \bmod p$
4. Beide haben den gemeinsamen Schlüssel und ein Angreifer kann aus der Kenntnis von α und β den Schlüssel praktisch nicht rekonstruieren.

Diffie-Hellmann Schlüsselvereinbarung (Fort.)

Example

Vereinbaren Sie mittels des Verfahrens von Diffie-Hellmann mit Ihrem Banknachbarn einen Schlüssel. Nutzen Sie $p = 17$ und $s = 5$.

Zusammenfassung

Wir haben folgende Begriffe kennen gelernt, können Sie einordnen und mit Ihnen umgehen. Weiter kennen wir einige Anwendungen:

- Wir können nun im Restesystem rechnen
- Wir können Potenzen effizient berechnen
- Wir können (multiplikative) Inverse berechnen
- Wir wissen, wie man primitive Elemente findet
- Wir wissen was eine Einwegfunktion ist und kennen ein paar Beispiele (modulare Quadratwurzel, diskreter Logarithmus)
- Wir können mit Hilfe der Diffie-Hellmann mit irgend jemandem einen nur uns bekannten gemeinsamen Schlüssel vereinbaren.

Fragen ?