

Herzlich Willkommen zum Seminarvortrag Modulare Arithmetik

Gliederung

Definition einer algebraischen Struktur

Operationen in dieser algebraischen Struktur

Praktische Anwendungen dieser Operationen im Bereich der Kryptographie

Definition einer algebraischen Struktur

Wir bewegen uns während des gesamten Vortags in

$$\mathbb{Z} = \{ \dots -2; -1; 0; 1; 2 \dots \}$$

$$\text{Operationen} = \{ +, * \}$$

Definition einer algebraischen Struktur

Stellen wir die erste Frage

Feststellung: $2 * x = 10$

Frage: Was ist x ?

Gibt es ein Element a^{-1} , so dass $a^{-1} * 2 = 1$ ist?

$1 =$ Neutrales Element (e) der Multiplikation

und $1 * x =$ Antwort

NEIN!

Definition einer algebraischen Struktur

Konzept der Restklassen

Die bekannteste Restklassenmenge überhaupt:

Für die späteren Stunden des Tages gibt es zwölf Äquivalenzklassen.

$$\mathbb{Z}_{12} = \{[0]_{12}; [1]_{12}; [2]_{12}; [3]_{12}; [4]_{12}; [5]_{12}; [6]_{12}; [7]_{12}; [8]_{12}; [9]_{12}; [10]_{12}; [11]_{12}\}$$

Die Uhrzeiten 0, 12 und 24 Uhr bezeichnen die gleiche Uhrzeit, sie sind in einer Äquivalenzklasse und bilden ein Restklasse innerhalb der Restklassenmenge



Definition einer algebraischen Struktur

Rechnen mit Restklassen

$$|\mathbb{Z}_{12}| = 12$$

$$\mathbb{Z}_{12} = \{ [0]_{12}; [1]_{12}; [2]_{12}; [3]_{12}; [4]_{12}; [5]_{12}; [6]_{12}; [7]_{12}; [8]_{12}; [9]_{12}; [10]_{12}; [11]_{12} \}$$

$$[0]_{12} = \{ \dots; -24; -12; 0; 12; 24; \dots \}$$

$$[8]_{12} = \{ \dots; -16; -4; 8; 20; 32; \dots \}$$

$$[8]_{12} + [11]_{12} = [7]_{12}, \text{ denn } 8 + 11 = 19 = 12 \cdot 1 + 7 \Rightarrow 19 \in [7]_{12}$$

$$[4]_{12} * [8]_{12} = [8]_{12}, \text{ denn } 4 * 8 = 32 = 12 * 2 + 8 \Rightarrow 32 \in [8]_{12}$$

Definition einer algebraischen Struktur

$$[2]_{12} * [x]_{12} = [10]_{12}$$

Suche nach a^{-1} , dem inversen Element zu 2

$$[2]_{12} * [0]_{12} = [0]_{12}$$

$$[2]_{12} * [1]_{12} = [2]_{12}$$

$$[2]_{12} * [2]_{12} = [4]_{12}$$

$$[2]_{12} * [3]_{12} = [6]_{12}$$

$$[2]_{12} * [4]_{12} = [8]_{12}$$

$$[2]_{12} * [5]_{12} = [10]_{12}$$

$$[2]_{12} * [6]_{12} = [0]_{12}$$

$$[2]_{12} * [7]_{12} = [2]_{12}$$

$$[2]_{12} * [8]_{12} = [4]_{12}$$

$$[2]_{12} * [9]_{12} = [6]_{12}$$

$$[2]_{12} * [10]_{12} = [8]_{12}$$

$$[2]_{12} * [11]_{12} = [10]_{12}$$

Zwei Lösungen gefunden,
aber nur durch probieren

$$[2]_{12} * [x]_{12} = [7]_{12}$$

Nicht lösbar, da man die Operation „*2“ nicht
wirklich invertieren kann!

Definition einer algebraischen Struktur



$$\text{ggT}(2, 12) = 2$$

$$\text{ggT}(1, 12) = 1$$

$$\text{ggT}(7, 12) = 1$$

Definition einer algebraischen Struktur

Beispiel für eine so definierte Restklassenmenge \mathbb{Z}_p , $p=7$

$(\mathbb{Z}_7, +)$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$(\mathbb{Z}_7, *)$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Definition einer algebraischen Struktur

Nun können wir die Frage beantworten

$(\mathbb{Z}_7, *)$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$$2 * x \equiv 10 \pmod{7}$$

$$a \equiv 2 \pmod{7}$$

$$a^{-1} \equiv 4 \pmod{7}$$

$$2 * x \equiv 10 \pmod{7} \mid *4$$

$$4 * 2 * x \equiv 4 * 10 \pmod{7}$$

$$1 * x \equiv 40 \equiv 5 * 7 + 5 \pmod{7}$$

Definition einer algebraischen Struktur

Die Modulare Arithmetik arbeitet in dieser algebraischen Struktur, einem Körper

Die beschriebene Struktur erfüllt die Eigenschaften eines Körpers und geht auf den französischen Mathematiker Galois(1811-1832) zurück

Operationen in dieser algebraischen Struktur

Wir werden drei Operationen im Speziellen betrachten

Potenzieren

Radizieren

Logarithmieren

Operationen in dieser algebraischen Struktur

Potenzen am Beispiel von \mathbb{Z}_7
 (mod 7) zur besseren Lesbarkeit weggelassen

$1^1 \equiv 1$	$2^1 \equiv 2$	$3^1 \equiv 3$	$4^1 \equiv 4$	$5^1 \equiv 5$	$6^1 \equiv 6$
$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 2$	$4^2 \equiv 2$	$5^2 \equiv 4$	$6^2 \equiv 1$
$1^3 \equiv 1$	$2^3 \equiv 1$	$3^3 \equiv 6$	$4^3 \equiv 1$	$5^3 \equiv 6$	$6^3 \equiv 6$
$1^4 \equiv 1$	$2^4 \equiv 2$	$3^4 \equiv 4$	$4^4 \equiv 4$	$5^4 \equiv 2$	$6^4 \equiv 1$
$1^5 \equiv 1$	$2^5 \equiv 3$	$3^5 \equiv 5$	$4^5 \equiv 2$	$5^5 \equiv 3$	$6^5 \equiv 6$
$1^6 \equiv 1$	$2^6 \equiv 1$	$3^6 \equiv 1$	$4^6 \equiv 1$	$5^6 \equiv 1$	$6^6 \equiv 1$

Wir erreichen nicht alle Restklassen
 Erzeugende Elemente

Es scheint $a^{(7-1)} = 1$

Operationen in dieser algebraischen Struktur

Kleiner Satz von Fermat

Sei $p \in \mathbb{P}$, dann gilt

$$x^{(p-1)} \equiv 1 \pmod{p}$$

Beweis durch Induktion

1. $x^{(p-1)} \equiv 1 \pmod{p} \mid *x$

Behauptung: $x^p \equiv x \pmod{p}$

2. Verankerung: x sei 0 $0^p \equiv 0 \pmod{p}$

3. Zu zeigen: $(x+1)^p \equiv x+1$

Operationen in dieser algebraischen Struktur

Zu zeigen: $(x + 1)^p \equiv x + 1$

$$(x + 1)^p \equiv x^p + \binom{p}{1} x^{p-1} + \binom{p}{2} x^{p-2} + \dots + \binom{p}{p-1} x^1 + 1 \pmod{p}$$

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{p * (p-1) * \dots * (p-k)}{k * (k-1) * \dots * 1}$$

$$(x + 1)^p \equiv x^p + p * \left(\frac{(p-1)!}{(p-1)!*1!} x^{p-1} + \frac{(p-1)!}{(p-2)!*2!} x^{p-2} + \dots + \frac{(p-1)!}{1!*(p-1)!} x^1 \right) + 1 \pmod{p}$$

$$(x + 1)^p \equiv x^p + 1 \pmod{p} \wedge x^p \equiv x \pmod{p} \Rightarrow \underline{\underline{(x + 1)^p \equiv x + 1 \pmod{p}}}$$

q.e.d.

Operationen in dieser algebraischen Struktur

Quadratwurzeln am Beispiel von \mathbb{Z}_7

$$\sqrt{4} \equiv 2 \pmod{7} \quad \wedge \quad \sqrt{4} \equiv (7-2) \equiv 5 \pmod{7}$$

$$5^2 = 25 = 3 \cdot 7 + \underline{4}$$

$$-2 \in [5]_7$$

$$x^2 \equiv (x-p)^2 \equiv x^2 - 2xp + p^2 \equiv x^2 - p(x-p) \equiv x^2 \pmod{p}$$

$$\sqrt{1} \equiv \{1;6\}; \sqrt{2} \equiv \{3;4\}; \sqrt{3} \equiv ?; \sqrt{4} \equiv \{2;5\}; \sqrt{5} \equiv ?; \sqrt{6} \equiv ? \pmod{7}$$

Operationen in dieser algebraischen Struktur

Quadratwurzelstruktur am Beispiel von \mathbb{Z}_7

(mod 7) zur besseren Lesbarkeit weggelassen

$1^1 \equiv 1$	$2^1 \equiv 2$	$3^1 \equiv 3$	$4^1 \equiv 4$	$5^1 \equiv 5$	$6^1 \equiv 6$
$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 2$	$4^2 \equiv 2$	$5^2 \equiv 4$	$6^2 \equiv 1$
$1^3 \equiv 1$	$2^3 \equiv 1$	$3^3 \equiv 6$	$4^3 \equiv 1$	$5^3 \equiv 6$	$6^3 \equiv 6$
$1^4 \equiv 1$	$2^4 \equiv 2$	$3^4 \equiv 4$	$4^4 \equiv 4$	$5^4 \equiv 2$	$6^4 \equiv 1$
$1^5 \equiv 1$	$2^5 \equiv 4$	$3^5 \equiv 5$	$4^5 \equiv 2$	$5^5 \equiv 3$	$6^5 \equiv 6$
$1^6 \equiv 1$	$2^6 \equiv 1$	$3^6 \equiv 1$	$4^6 \equiv 1$	$5^6 \equiv 1$	$6^6 \equiv 1$

$$\sqrt{1} \equiv \{1;6\}; \sqrt{2} \equiv \{3;4\}; \sqrt{3} \equiv ?; \sqrt{4} \equiv \{2;5\}; \sqrt{5} \equiv ?; \sqrt{6} \equiv ? \pmod{7}$$

$$a^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow a \text{ hat eine Quadratwurzel?}$$

Operationen in dieser algebraischen Struktur

Quadratwurzelstruktur am Beispiel von \mathbb{Z}_7

(mod 7) zur besseren Lesbarkeit weggelassen

$1^1 \equiv 1$	$2^1 \equiv 2$	$3^1 \equiv 3$	$4^1 \equiv 4$	$5^1 \equiv 5$	$6^1 \equiv 6$
$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 2$	$4^2 \equiv 2$	$5^2 \equiv 4$	$6^2 \equiv 1$
$1^3 \equiv 1$	$2^3 \equiv 1$	$3^3 \equiv 6$	$4^3 \equiv 1$	$5^3 \equiv 6$	$6^3 \equiv 6$
$1^4 \equiv 1$	$2^4 \equiv 2$	$3^4 \equiv 4$	$4^4 \equiv 4$	$5^4 \equiv 2$	$6^4 \equiv 1$
$1^5 \equiv 1$	$2^5 \equiv 4$	$3^5 \equiv 5$	$4^5 \equiv 2$	$5^5 \equiv 3$	$6^5 \equiv 6$
$1^6 \equiv 1$	$2^6 \equiv 1$	$3^6 \equiv 1$	$4^6 \equiv 1$	$5^6 \equiv 1$	$6^6 \equiv 1$

$$\sqrt{1} \equiv \{1;6\}; \sqrt{2} \equiv \{3;4\}; \sqrt{3} \equiv ?; \sqrt{4} \equiv \{2;5\}; \sqrt{5} \equiv ?; \sqrt{6} \equiv ? \pmod{7}$$

$$a^{(p-1)/2} \equiv (p-1) \pmod{p} \Rightarrow a \text{ hat keine Quadratwurzel?$$

Operationen in dieser algebraischen Struktur

Warum ist das so?

$a^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow a$ Hat eine Quadratwurzel

$a^{(p-1)/2} \equiv (p-1) \pmod{p} \Rightarrow a$ Hat keine Quadratwurzel

Das Element 1 wird in den Potenzen jedes Elements definiert, denn: $1 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \pmod{7}$

Da der Exponent 6 gerade ist, kann die Wurzel gezogen werden

$$\sqrt{1} \equiv \{1; -1\} \wedge -1 \in [p-1]_p$$

Operationen in dieser algebraischen Struktur

Können erzeugende Elemente nie Quadratwurzeln haben?

Erzeugende Elemente
enthalten alle Vorhandenen
Wurzeln mit geraden
Exponenten

$$\sqrt{2} \equiv \{3;4\};$$

$$\sqrt{4} \equiv \{2;5\};$$

$$\sqrt{1} \equiv \{1;6\};$$

$$3^1 \equiv 3$$

$$3^2 \equiv 2$$

$$3^3 \equiv 6$$

$$3^4 \equiv 4$$

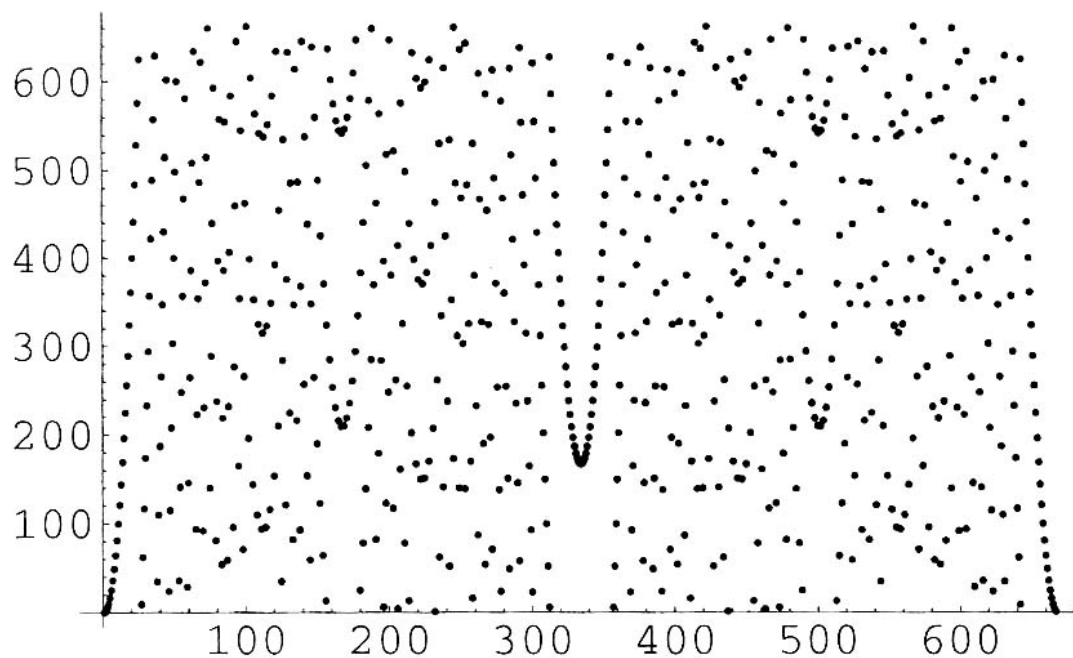
$$3^5 \equiv 5$$

$$3^6 \equiv 1$$

Erzeugende Elemente
enthalten sich selbst
und alle anderen erzeugenden
Elemente, bzw. hier auch
das letzte Element nur mit
einem ungeraden Exponenten

Operationen in dieser algebraischen Struktur

Quadrate am Beispiel von \mathbb{Z}_{667} $f(x) = x^2$



Anfangs bekannte
Parabelform

Symmetrie durch
 $x^2 \equiv (x - p)^2 \pmod{p}$

Es gibt auch mächtigere
Lösungsmengen als 2,
wenn \mathbb{Z}_n wie hier $n = p \cdot q$
 $667 = 23 \cdot 29$
 $\sqrt{506} = \{62; 315; 352; 602\}$

Operationen in dieser algebraischen Struktur

Die modulare Quadratwurzel berechnen

Innerhalb einer Restklassenmenge mit einer Primzahl als Basis gibt es effiziente Berechnungsschemata

Ist $n=p \cdot q$ entsprechend groß (200stellig), ist auch für moderne Rechensysteme

$$\sqrt{a} \equiv x \pmod{n}$$

nur noch in extrem langer Zeit (Jahren) zu berechnen.

Natürlich muss hierbei $a^2 > p$ sein

Auf der anderen Seite ist die Umkehrfunktion, das Quadrieren, extrem einfach zu berechnen. Sei bekannt $a \in \mathbb{Z}_p$

$$a^2 \equiv x \pmod{n}$$

Sei gesucht $x \in \mathbb{Z}_p$

Operationen in dieser algebraischen Struktur

Logarithmen am Beispiel von \mathbb{Z}_7

Frage: mit welchem Element muss 2 potenziert werden, damit 4 herauskommt? Oder $2^x \equiv 4 \pmod{7}$

Antwort: $\log_2 4 \equiv 2 \pmod{7}$ denn $2^2 \equiv 4 \pmod{7}$

und $\log_2 4 \equiv 5 \pmod{7}$ denn $2^5 \equiv 32 \equiv 4 * 7 + 4 \equiv 4 \pmod{7}$

Frage: $2^x \equiv 5 \pmod{7}$

Antwort: $\log_2 5 \equiv ? \pmod{7}$ also keine Lösung

Operationen in dieser algebraischen Struktur

Logarithmenstruktur am Beispiel von \mathbb{Z}_7

(mod 7) zur besseren Lesbarkeit weggelassen

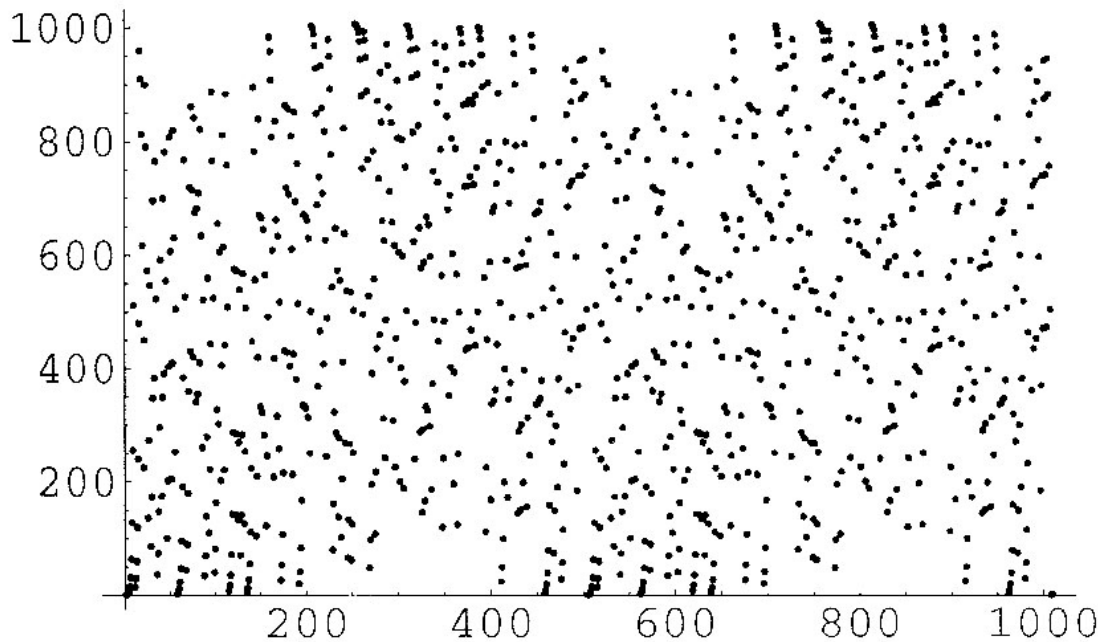
$1^1 \equiv 1$	$2^1 \equiv 2$	$3^1 \equiv 3$	$4^1 \equiv 4$	$5^1 \equiv 5$	$6^1 \equiv 6$
$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 2$	$4^2 \equiv 2$	$5^2 \equiv 4$	$6^2 \equiv 1$
$1^3 \equiv 1$	$2^3 \equiv 1$	$3^3 \equiv 6$	$4^3 \equiv 1$	$5^3 \equiv 6$	$6^3 \equiv 6$
$1^4 \equiv 1$	$2^4 \equiv 2$	$3^4 \equiv 4$	$4^4 \equiv 4$	$5^4 \equiv 2$	$6^4 \equiv 1$
$1^5 \equiv 1$	$2^5 \equiv 4$	$3^5 \equiv 5$	$4^5 \equiv 2$	$5^5 \equiv 3$	$6^5 \equiv 6$
$1^6 \equiv 1$	$2^6 \equiv 1$	$3^6 \equiv 1$	$4^6 \equiv 1$	$5^6 \equiv 1$	$6^6 \equiv 1$

Alle Elemente aus \mathbb{Z}_7 sind nicht erreichbar
z.B. $\log_2 5 \equiv ?$ und Elemente sind doppelt erreichbar

Für erzeugende Elemente ergibt sich eine eindeutige Abbildung

Operationen in dieser algebraischen Struktur

Potenzen am Beispiel von $\mathbb{Z}_{1009} f(x) = 2^x$



Anfangs bekannte
Exponentialsteigung

Graph ist hier periodisch
zu einem Teiler von
 $(p-1) = (1009-1)$
Hier $1008/2 = 504$

Operationen in dieser algebraischen Struktur

Den modularen Logarithmus berechnen

Ist p entsprechend groß (200stellige Primzahl), ist auch für moderne Rechensysteme

$$\log_b a \equiv x \pmod{p}$$

nur noch in extrem langer Zeit (Jahren) zu berechnen. Natürlich muss hierbei $b^x > p$ sein

Auf der anderen Seite ist die Umkehrfunktion, die Potenz, extrem einfach zu berechnen.

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

Sei bekannt $b, a \in \mathbb{Z}_p$

Sei gesucht $x \in \mathbb{Z}_p$

Praktische Anwendungen dieser Operationen im Bereich der Kryptographie

Authentifizierung:

Fiat-Shamir-Protokoll

(Nutzt das Berechnungsproblem der modularen Quadratwurzel)

Schlüsselaustausch:

Diffie-Hellman-Schlüsselaustausch

(Nutzt das Berechnungsproblem des modularen Logarithmus)

Praktische Anwendungen dieser Operationen im Bereich der Kryptographie

Das Dilemma der Authentifizierung



Praktische Anwendungen dieser Operationen im Bereich der Kryptographie

1. Ich weiß etwas, das mich authentifiziert
2. Diese Information gebe ich nicht heraus
3. Ich kann beweisen, dass ich die Information habe

Praktische Anwendungen dieser Operationen im Bereich der Kryptographie

Fiat-Shamir-Protokoll

1. Ich wähle ein $n=p \cdot q$ für meine Restklassenmenge und ein Element s in dieser und quadriere s
2. Die Zahl s gebe ich unter keinen Umständen preis
3. Authentifizierungsprozess

1. Ich gebe allgemein s^2 und n bekannt
2. Ich gebe zusätzlich zu s^2 und n ein frei gewähltes r^2 bekannt

Nun darfst du fragen:

entweder was ist $s \cdot r \rightarrow$ deine Prüfung $(s \cdot r)^2 \equiv s^2 \cdot r^2 \pmod{n}?$

oder was ist $r \rightarrow$ deine Prüfung $r_{neu}^2 \equiv r^2 \pmod{n}?$

3. Wüsste jemand die Fragen im Voraus, könnte er mogeln und sich als mich ausgeben. Darum wird Schritt 2 vielfach durchgeführt.

Praktische Anwendungen dieser Operationen im Bereich der Kryptographie

Wie könnte man mogeln?

- a) Wenn ich weiß, es wird nach r gefragt,
gebe ich dir irgendein von mir berechnetes r^2
und auf deine Frage, dann das gewählte r
Wichtig: Die Frage nach s^*r könnte ich nicht beantworten, da ich
 s nicht kenne
- b) Wenn ich weiß, es wird nach s^*r gefragt,
nehme ich eine Zahl a und quadriere sie, multipliziere das
inverse Element von s^2 mit a^2 und gebe dir das Ergebnis als r^2 .
Fragst du nach s^*r gebe ich dir a . Da $r^2 = (s^2)^{-1} * a^2$, ist
 $s^2 * (s^2)^{-1} * a^2 = a^2$
Wichtig: Die Frage nach r könnte ich nicht beantworten.

Praktische Anwendungen dieser Operationen im Bereich der Kryptographie

Das Problem des Schlüsselaustausches



$b = qa + r$ $\text{ggT}(a, b)$
 $2^{10} = 28$
 $2^{10} = 17$
 $536 \cdot 115$
 $x^2 = 2^x$
 \log
 $x(1-x)$
 57
 311
 2
 1
 $\sqrt{a} \pmod{m}$
 $4 = \sqrt{5}$
 $9 = \sqrt{5}$
 $\sqrt{a} \pmod{m}$
 Induktions Beweis
 $\text{mod}(a)$

Praktische Anwendungen dieser Operationen im Bereich der Kryptographie

Diffie-Hellman-Schlüsselaustausch

1. Es sei ein p für eine Restklassenmenge und ein Element s in dieser allgemein bekannt.
2. Zwei Kommunikationspartner A und B wollen einen gemeinsamen Schlüssel verwenden.

A wählt geheim eine natürliche Zahl a und berechnet
 $s^a \equiv \alpha \pmod{p}$

B wählt geheim eine natürliche Zahl b und berechnet
 $s^b \equiv \beta \pmod{p}$

3. A und B schicken sich gegenseitig α und β zu
4. A berechnet nun $\beta^a \equiv s^{ba} \equiv k \pmod{p}$
und B berechnet nun $\alpha^b \equiv s^{ab} \equiv k \pmod{p}$

Wenn jemand α und β abfängt, wie errechnet er dann a oder b ?

$$\log_s \beta \equiv ? \vee \log_s \alpha \equiv ?$$

**Danke für die
Aufmerksamkeit**