Computer Algebra

Sebastian Iwanowski
FH Wedel

3. Modulare Arithmetik

Referenzen zum Nacharbeiten:

Köpf 4 (außer 4.3, 4.6)
von zur Gathen, Gerhard 4.1, 4.2
Seminararbeit 4 (Hendrik Annuth)

Computer Algebra 3

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 Restklassemenge

aus: Seminarvortrag Annuth

Computer Algebra 3

Restklassen

Rechnen mit Restklassen

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

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

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

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

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

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

aus: Seminarvortrag Annuth

Computer Algebra 3

Restklassen

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

Suche nach $[\text{„}10/2\text{“}]_{12}$

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

Zwei Lösungen gefunden,
aber nur durch probieren

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

Modulare Division ist nicht effizient lösbar.
Außerdem kann man die Operation „*2“
in $\mathbb{Z}_{12}$ nicht für jedes Ergebnis invertieren!

nach: Seminarvortrag Annuth

Computer Algebra 3

Restklassen

Beispiel für eine Restklassenmenge $\mathbb{Z}_p$
mit vollständig und eindeutig definierter Division:

$(\mathbb{Z}_7, +)$	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

In $\mathbb{Z}_7$ kann man die Operation „*“
für jeden Operanden und jedes Ergebnis invertieren:
Geht es auch effizient, d.h. besser als durch Probieren?

nach: Seminarvortrag Annuth

Computer Algebra 3

Restklassen

Division über Bestimmung des Inversen:

$(\mathbb{Z}_7, *)$	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

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

$$a \equiv 2 \pmod 7$$

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

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

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

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

aus: Seminarvortrag Annuth

Computer Algebra 3

Restklassen

Division über Bestimmung des Inversen:

- Inversenbestimmung über erweiterten Euklidischen Algorithmus

  Berechnet a^{-1} mod n, wenn ggt(a,n) = 1
  ⇒ funktioniert für alle $a \in \mathbb{Z}_n$, wenn n eine Primzahl ist

  Laufzeit: $O(\#n^2)$

Fazit:

- Modulare Multiplikation immer effizient
- Modulare Division auch effizient für Primzahlmoduli
- Modulare Division für zusammengesetzte Moduli n = p • q:
  ggt(a,n) = 1: effizient
  ggt(a,n) > 1: kein effizienter Algorithmus bekannt!

Computer Algebra 3

Weitere Operationen in Restklassen

Wir werden drei Operationen im Speziellen betrachten

Potenzieren

Radizieren

Logarithmieren

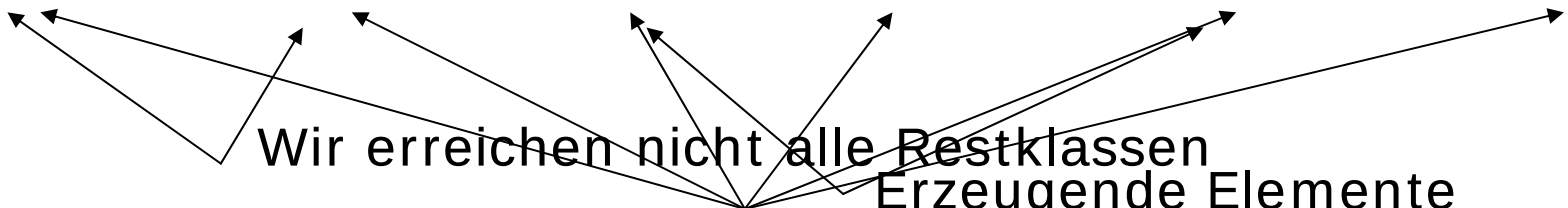
aus: Seminarvortrag Annuth

Weitere Operationen in Restklassen: Potenzen

Potenzen am Beispiel von $\mathbb{Z}_7$

(mod 7) zur besseren Lesbarkeit weggelassen

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



Wir erreichen nicht alle Restklassen

Erzeugende Elemente

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

aus: Seminarvortrag Annuth

Weitere Operationen in Restklassen: Potenzen

Kleiner Satz von Fermat

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

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

Beweis durch Induktion über x

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

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

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

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

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen: Potenzen

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

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

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

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

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

q.e.d.

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen: Quadratwurzeln

Quadratwurzeln am Beispiel von $\mathbb{Z}_7$

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

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

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

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

$$\sqrt{1} \equiv \{1;6\}; \sqrt{2} \equiv \{3;4\}; \sqrt{3} \equiv ?; \sqrt{4} \equiv \{2;5\}; \sqrt{5} \equiv ?; \sqrt{6} \equiv ? (\text{mod } 7)$$

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen: Quadratwurzeln

Quadratwurzelstruktur am Beispiel von $\mathbb{Z}_7$

(mod 7) zur besseren Lesbarkeit weggelassen

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

$$\sqrt{1} \equiv \{1;6\}; \sqrt{2} \equiv \{3;4\}; \sqrt{3} \equiv ?; \sqrt{4} \equiv \{2;5\}; \sqrt{5} \equiv ?; \sqrt{6} \equiv ? (\text{mod } 7)$$

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

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen: Quadratwurzeln

Quadratwurzelstruktur am Beispiel von $\mathbb{Z}_7$

(mod 7) zur besseren Lesbarkeit weggelassen

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

$$\sqrt{1} \equiv \{1;6\}; \sqrt{2} \equiv \{3;4\}; \sqrt{3} \equiv ?; \sqrt{4} \equiv \{2;5\}; \sqrt{5} \equiv ?; \sqrt{6} \equiv ? (\text{mod } 7)$$

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

aus: Seminarvortrag Annuth

Weitere Operationen in Restklassen: Quadratwurzeln

Warum ist das so?

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

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

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

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

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

aus: Seminarvortrag Annuth

Weitere Operationen in Restklassen: Quadratwurzeln

Können erzeugende Elemente nie Quadratwurzeln haben?

Erzeugende Elemente enthalten alle Vorhandenen Wurzeln mit geraden Exponenten

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

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

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

$3^1 \equiv 3$

$3^2 \equiv 2$

$3^3 \equiv 6$

$3^4 \equiv 4$

$3^5 \equiv 5$

$3^6 \equiv 1$

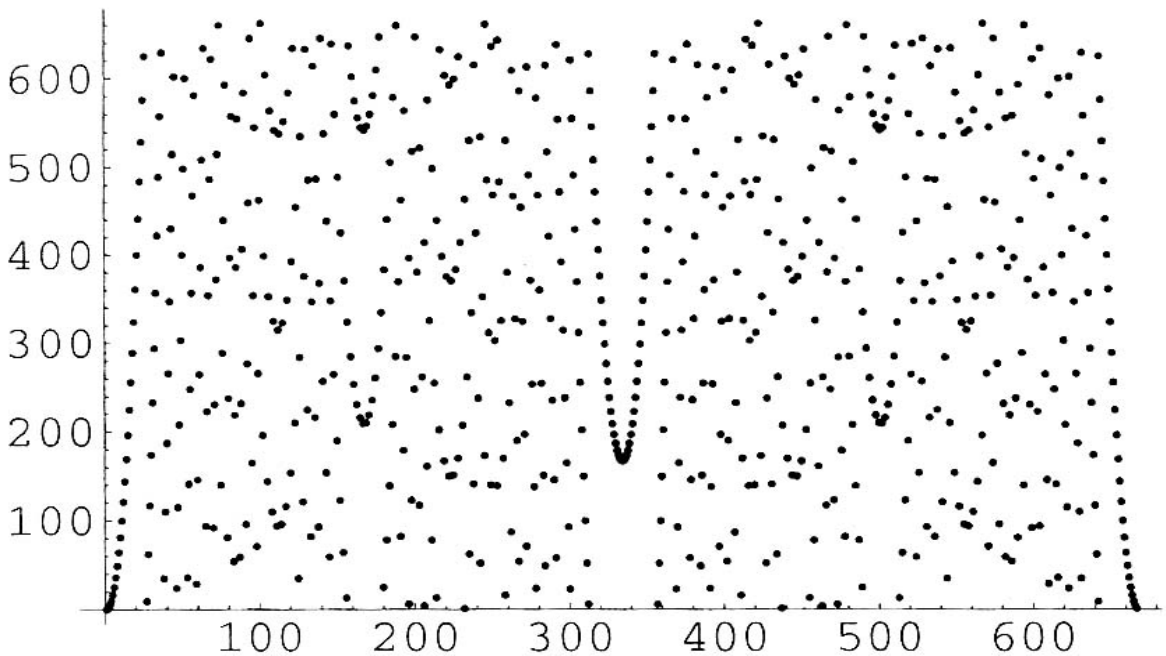
Erzeugende Elemente enthalten sich selbst und alle anderen erzeugenden Elemente, bzw. hier auch das letzte Element nur mit einem ungeraden Exponenten

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen: Quadratwurzeln

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*q

667=23*29

$$\sqrt{506} = \{62;315;352;602\}$$

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen: Quadratwurzeln

Die modulare Quadratwurzel berechnen

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

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

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

Ist n=p*q entsprechend groß (200stellig), ist $\sqrt{a} \equiv x \pmod{n}$
auch für moderne Rechensysteme nur in extrem langer Zeit (Jahren) zu berechnen.
Hierbei sollte $x^2 > n$ sein.

Auf der anderen Seite ist die Umkehrfunktion, das Quadrieren,
extrem einfach zu berechnen: $a^2 \equiv x \pmod{n}$

nach: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen

Logarithmen am Beispiel von $\mathbb{Z}_7$

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

Antwort: $\log_2 4 \equiv 2 (\mathrm{mod}\ 7)$ denn $2^2 \equiv 4 (\mathrm{mod}\ 7)$

und $\log_2 4 \equiv 5 (\mathrm{mod}\ 7)$ denn $2^5 \equiv 32 \equiv 4 * 7 + 4 \equiv 4 (\mathrm{mod}\ 7)$

Frage: $2^x \equiv 5 (\mathrm{mod}\ 7)$

Antwort: $\log_2 5 \equiv ? (\mathrm{mod}\ 7)$ also keine Lösung

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen

Logarithmenstruktur am Beispiel von $\mathbb{Z}_7$

(mod 7) zur besseren Lesbarkeit weggelassen

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

Für erzeugende Elemente ergibt sich eine eindeutige Abbildung.

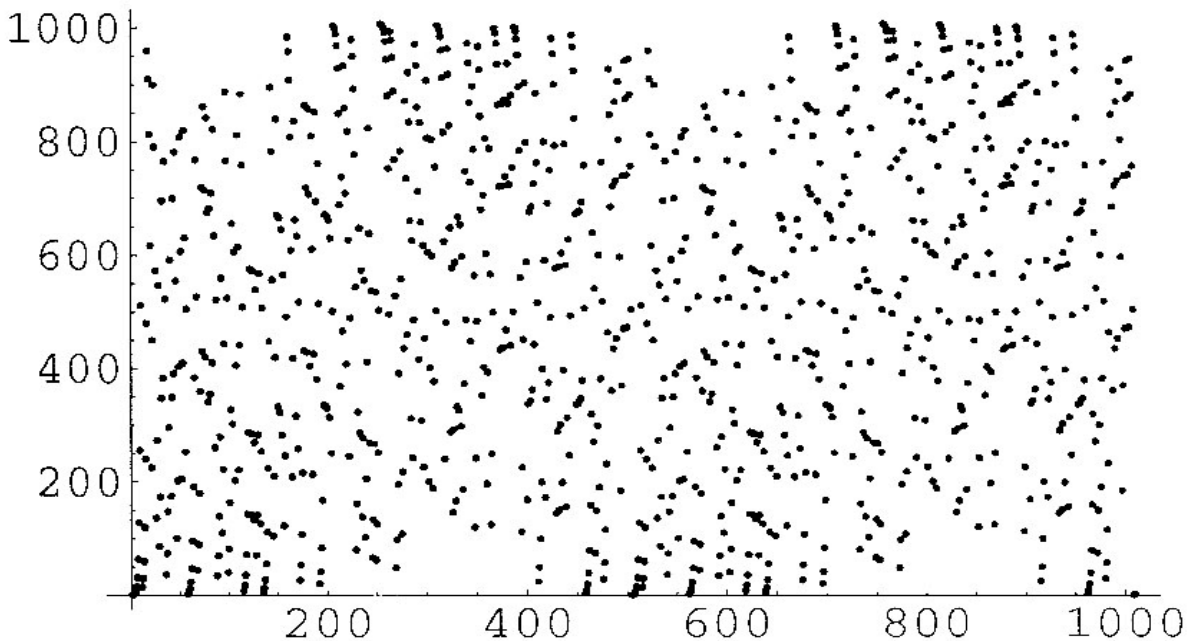
Nicht alle Elemente aus $\mathbb{Z}_7$ sind nicht erreichbar, z.B. $\log_2 5 \equiv ?$
Einige Elemente sind doppelt erreichbar.

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen

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

aus: Seminarvortrag Annuth

Computer Algebra 3

Weitere Operationen in Restklassen

Den modularen Logarithmus berechnen

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

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

Ist p entsprechend groß (200stellige Primzahl), ist $\log_b a \equiv x \pmod{p}$
auch für moderne Rechensysteme nur in extrem langer Zeit (Jahren) zu berechnen.
Hierbei sollte $b^x > p$ sein.

Auf der anderen Seite ist die Umkehrfunktion, die Potenz,
extrem einfach zu berechnen: $b^a \equiv x \pmod{p}$

nach: Seminarvortrag Annuth

Computer Algebra 3

Zusammenfassung: Operationen der modularen Arithmetik

- Finden von multiplikativen Inversen b/a mod n (modulare Division):

  Umkehroperation der Multiplikation. Diese ist für jedes n effizient lösbar.
  Algorithmen zur Division:
  - für Primzahlmoduli n: $O(\#n^2)$ mit Hilfe des erweiterten Euklidischen Algorithmus
  - für zusammengesetzte Moduli n, ggt(a,n) = 1: wie oben
  - für zusammengesetzte Moduli n, ggt(a,n) > 1: kein effizienter Algorithmus bekannt

- Finden von Quadratwurzeln mod n

  Umkehroperation des Quadrierens. Dieses ist für jedes n effizient lösbar.
  Algorithmen zum Wurzelziehen:
  - für Primzahlmoduli: es gibt polynomielle Verfahren (nicht trivial)
  - für zusammengesetzte Moduli n: kein effizienter Algorithmus bekannt

- Finden von Logarithmen mod n

  Umkehroperation des Potenzierens. Dieses ist für jedes n effizient lösbar
  Algorithmen zum Logarithmieren:
  - Für kein Modulus n ist ein effizienter Algorithmus bekannt.