

# $\int$ Skripte *Mo. 25. März*

## Kryptologie ICS.KRYPTO

Folien zur Präsenz <sup>6</sup>

«Mathematische Grundlagen der asymmetrischen Kryptographie», FS 24, V3.2

**Wichtig: Die Kapitel 1 – 4 in diesen Folien sind Repetitionen aus D-MATH und Teil Ihrer Vorbereitung (flipped classroom)!**

Tutorial zur Vorbereitung [https://hslu.zoom.us/rec/share/bzgdIR4FNEO6oJ8lF9rhQcpYdolu3A7xojKP9e\\_7mzg5kup-cjq8x5Ymk9jGKBf.G3jc40Pm76GMDbpr](https://hslu.zoom.us/rec/share/bzgdIR4FNEO6oJ8lF9rhQcpYdolu3A7xojKP9e_7mzg5kup-cjq8x5Ymk9jGKBf.G3jc40Pm76GMDbpr)

### Satz von Euler

Der **Satz von Euler**, auch als "Satz von Euler-Fermat" bekannt nach Leonhard Euler und Pierre de Fermat, stellt eine Verallgemeinerung des **kleinen Fermatschen Satzes** auf.

### Satz 164S (Satz von Euler)

Seien  $a, n \in \mathbb{N}$  und  $\text{ggT}(a, n) = 1$  Dann gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

wobei  $\varphi(n)$  die **Eulersche Phi-Funktion** bezeichnet.

Da für prime **Moduln**  $p$  gilt:  $f(p) = p - 1$ , geht für diese der Satz von Euler in den **kleinen Satz von Fermat** über.

<https://www.youtube.com/watch?v=-J3P9pzL4sY> und weitere Videos von Christian Spannagel.

<https://www.youtube.com/watch?v=xotqVLOdONc>

Und zu zyklischen Gruppen: <https://www.youtube.com/watch?v=QcFTPDvoIKU>

©Josef Schuler, dipl. math., dipl. Ing. NDS ETHZ, MSc Applied IT-Security, Feldhof 25, 6300 Zug, [j.schuler@bluewin.ch](mailto:j.schuler@bluewin.ch) resp. [josef.schuler@hslu.ch](mailto:josef.schuler@hslu.ch)

# ***Der Slogan zu dieser Präsenz***

Die asymmetrische Kryptographie ist eines der besten Beispiele, um zu zeigen, wie sinnvoll Grundlagenforschung ist.

Warum? Ganz einfach:

Die moderne asymmetrischen Kryptographie kann mit dem folgenden Slogan zusammengefasst werden:

***Jahrhundert Jahre alte Mathematik in den modernsten Anwendungen.***

Zudem ist es einfacher als in der ersten Primarklasse:

In der ersten Primarklasse haben Sie die Ganzzahldivision kennengelernt:

**$20 : 3 = 6 \text{ Rest } 2$ .**

Nun an der Hochschule wollen wir es noch einfacher machen.

Uns interessiert nämlich nur der Rest, der übrig bleibt, wenn 20 mit 3 dividiert wird:  $20 \bmod 3 \equiv 2$ .

Zitate von Josef Schuler, Autor des Skripts

# Inhaltsübersicht

- Kap. 1 – 5 = Repetition der relevanten Teile von D-MATH SW 9 – 11, «Einführung in die Zahlentheorie I – III»
  - Die mod  $N$  Arithmetik: Addition, Subtraktion, Multiplikation, Potenzieren & das Bilden des inversen Elements, wenn es möglich ist!
  - Die Euler'sche  $\phi$ -Funktion.
  - Anzahl der Primzahlen, die Funktion  $\pi(n)$  (von Carl Friederich Gauss)
  - Primzahlen: Verteilung der Primzahlen, der kl. Satz von Fermat, Primzahlerzeugung.
  - Der Satz von Euler
  - **Wichtig:** In der Präsenz wird der Inhalt der Kap. 1 – 4 nicht mehr besprochen. Da D-MATH Voraussetzung für unser Modul ist, ist es statthaft diesen Stoff vorauszusetzen. Der Inhalt von Kap. 5 ist zwar auch schon in D-MATH behandelt worden, trotzdem werden wir das Kap. 5 in der Präsenz miteinander behandeln. Die Unterlagen zu D-MATH SW 9 – 11 sind in Ilias im Sinne eines Nachschlagewerks hochgeladen.
- Kap. 6 = Einführung in die abstrakte Algebra
  - Gruppen, Untergruppen, Ordnung einer Gruppe, resp. Ordnung einer Untergruppe, Erzeugende Elemente, Ordnung eines Elementes usw.

# Verweise zur Literatur

- **Für die Repetition der Zahlentheorie, Kap. 1 – 5 (davon Kap. 1 – 4 als flipped classroom vorgängig im Selbststudium):**
  - JS Skript „Einführung in die Kryptologie“, Kap. 7.3.2, 19 & 25.
  - JS Skript, Präsenzsript in D-MATH SW 9 – 11, „Zahlentheorie I – III“.
  - In [CP-D] die Kap. 1.4.1, 1.4.2, 4.3.1, 4.3.2, 6.3, 7.3, 7.4, 7.6, wobei 7.6.2 nur informell und **nicht prüfungsrelevant** ist.
- **Für die Einführung in die abstrakte Algebra, Kap. 6:**
  - JS Skript „Einführung in die Kryptologie“, Kap. 26.
  - JS Skript „Elliptische Kurven Kryptosysteme, ECCS und weitere Aspekte zu Signaturen, speziell von RSA“, Kap. 8.1 „Anhang 1: Gruppen“.
  - In [CP-D] das Kap. 8.2.
- **Aufgaben**
  - Aufgaben in den Folien & JS Skript „Einf. in die Kryptologie“, Kap. 19, 25 & 26.
  - JS Skript „Aufgaben und Lösungen zum Modul KRYPT an der HSLU-I“, Kap. 2.2, „Aufgaben zur Präsenz 6“.

# Agenda

## Kap. 1 – 5: Für alle asym. Verfahren

- Die sechs wichtigsten Protagonisten der zugrunde gelegten Mathematik
- Grundlagen (Näherungsformel & mod N Operation)
- Addition & Subtraktion mod N
- Multiplikation, Inverses & Division mod N
- Nullteilerfreiheit
- Potenzieren, inkl. Square and Multiply (säm Algorithmus)
- n-te Wurzelziehen und Logarithmieren
- Primzahlen, Primzahldarstellung & Anzahl Primzahlen
- Die Euler'sche Phi-Funktion, die Gauss'sche Pi-Funktion
- Die Sätze von Fermat und Euler

## Kap. 6: Brauchen wir vornehmlich für Diffie-Hellman & Elliptische Kurven

- Gruppentheorie
  - Definitionen und Beispiele
  - Gruppenoperationen, Ordnung der Gruppe
  - Untergruppen und deren (möglichen) Ordnungen
  - Ordnung eines Elementes
  - Erzeugende Elemente usw.

# Lernziele

- Ich habe die mathematischen Grundlagen (siehe auch Vorkenntnisse) repetiert und gefestigt.
- Ich kenne insbesondere
  - Die Mod N Operationen wie Addition, Subtraktion, Multiplikation, Bilden des Inversen.
  - Potenzieren, Square and Multiply, usw.
- Ich kann die Anzahl Primzahlen bis zur Grösse  $n$ , resp. der Grösse  $n$  berechnen (Gauss'sche Pi-Funktion).
- Ich kann die Anzahl teilerfremde Zahlen berechnen (Euler'sche Phi-Fkt.)
- Ich kenne den Unterschied zw. dem deterministischen und dem probabilistischen Ansatz zum Finden von Primzahlen.
- Ich kenne die Sätze und Berechnungen zu den Primzahlen.
- Ich kann die Sätze von Euler und Fermat einsetzen.
- Ich kenne die Elemente der Gruppentheorie.
- Ich habe die Aufgaben im JS Skript „Aufgaben und Lösungen zum Modul KRYPT an der HSLU-I“, Kap. 2.2 „Aufgaben zur Präsenz 6“ durchgearbeitet.

# **Kap. 1**

## **DIE GRUNDLEGENDE MATHEMATIK**



# Sechs Protagonisten und deren Mathematik

Pierre Fermat, 1607 – 1665 →

Kleiner Satz von Fermat:  $a^p \equiv a \pmod{p}$ , für eine beliebige ganze Zahl  $a$  und Primzahl  $p$ .

**Folgerung:**  $a^{p-1} \equiv 1 \pmod{p}$  resp.  $a^{p-2} \equiv a^{-1} \pmod{p}$

**Bemerkung:** Fermat's last theorem, ca. 1637:

$x^n + y^n \neq z^n$ , für  $n \in \mathbb{N}$ ,  $n > 2$  und  $x, y, z \in \mathbb{N} \setminus \{0\}$

Erst 1994 gelang der Beweis!



Leonhard Euler, 1707 – 1783, hier auf dem schweizerischen 10-Franken-Schein der Banknotenserie von 1984.

Verallgemeinerung des kleinen Satzes von Fermat:

$a^{\varphi(n)} \equiv 1 \pmod{n}$ , für  $a$  und  $n$  teilerfremd sowie  $\varphi(n)$  die Euler'sche Phi-Funktion und damit  $a^{\varphi(n)+1} \equiv a \pmod{n}$ , resp.  $a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}$ .



# Sechs Protagonisten und deren Mathematik

Carl Friederich Gauss, 1777 – 1855 →

Einer der allergrössten Mathematiker der Geschichte. Als 15-jähriger kreierte er die Abschätzung der Anzahl der Primzahlen von 1 bis  $n$ ; die Pi-Funktion:  $\pi(n) \approx \frac{n}{\ln(n)}$



Niels Henrik Abel, 1802 – 1829. Z.B. bekannt für abelsche (= kommutative) Gruppen.

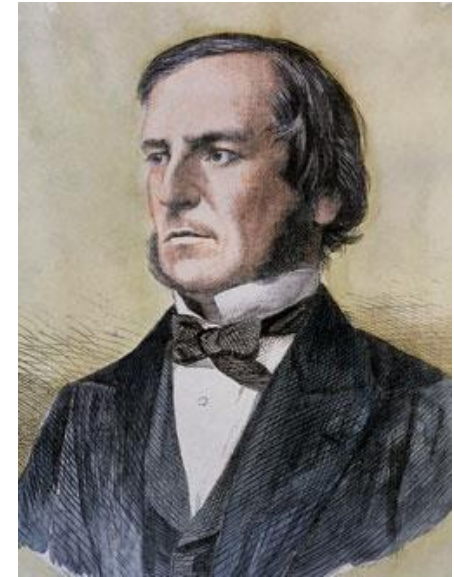
# Sechs Protagonisten und deren Mathematik



← Evariste Galois, 1811 – 1832

Galoistheorie, Gruppen, Körper

George Boole, 1815 – 1864 →  
Begründer der Boole'schen  
Algebra und damit auch der XOR-  
Operation.



## Weitere grundlegende Mathematik

- Ca. 300-stellige (und grösser) Primzahlen und die Modulo Operation spielen bei asymmetrischen Verfahren eine grosse Rolle.
- Beispiele zu mod  $N$ 
  - a)  $13 \bmod 5 = 3$ , da  $13 : 5 = 2$  Rest 3
  - b)  $27 \bmod 9 = 0$ , da  $27 : 9 = 3$  Rest 0
  - c)  $35 \bmod 12 = 11$ , da  $35 : 12 = 2$  Rest 11**Eigenschaft:**  $\bmod N \in \{0; 1; 2; \dots; N - 1\}$

# **Kap. 2**

## **GRUNDLAGEN**

# $2^{2048}$ sind wie viele Dezimalstellen?

Es gelten die Potenzregeln:  $(a^b)^c = a^{b \cdot c}$  resp.  $(a^b)^c = a^{b \cdot c} = a^{c \cdot b} = (a^c)^b$

*Eine Näherungsformel:  $2^{10} = 1024 \approx 1000 = 10^3 \Rightarrow 2^{10} \approx 10^3$*

*Anzahl Dezimalstellen von  $2^x = \log_{10} 2^x = x \cdot \log_{10} 2 \approx x \cdot 0,3$*

*Anzahl Dezimalstellen von  $2^x \approx \frac{x}{3} - 0,1 \cdot \frac{x}{3} = 0,9 \cdot \frac{x}{3}$*

## Beispiel:

$$2^{2048} = 2^{10 \cdot 204,8} = (2^{10})^{204,8} \approx (10^3)^{204,8} = 10^{3 \cdot 204,8} = 10^{614,4} \approx 10^{615}$$

*Anzahl Dezimalstellen von  $2^{2048} = 2048 \cdot \log_{10} 2 \approx 2048 \cdot 0,3 = 614,4$*

*Anzahl Dezimalstellen von  $2^{2048} \approx \frac{2048}{3} - 0,1 \cdot \frac{2048}{3} = 614,4$*

Die genaue Berechnung mit dem TR zeigt, dass die Grössenordnung stimmt:

$$2^{2048} \approx 3,3 \cdot 10^{616}$$

# Die mod N Operation

$c \equiv a \bmod N$  heisst, dass bei der Ganzzahldivision von  $c$  durch  $N$  der Rest  $a$  übrigbleibt.

## Beispiele:

1.  $22 \bmod 6 \equiv 4$ , da  $22 : 6 = 3$  Rest 4
2.  $43 \bmod 8 \equiv 3$ , da  $43 : 8 = 5$  Rest 3
3.  $51 \bmod 8 \equiv 3$ , da  $51 : 8 = 6$  Rest 3
4.  $20 \bmod 4 \equiv 0$ , da  $20 : 4 = 5$  Rest 0
5.  $25 \bmod 5 \equiv 0$ , da  $25 : 5 = 5$  Rest 0
6.  $55 \bmod 9 \equiv 1$ , da  $55 : 9 = 6$  Rest 1

## Allgemein:

1.  $c \equiv a \bmod N \rightarrow c \in \{0; 1; \dots; N-1\}$
2.  $c \equiv a \bmod N = (a + k*N) \bmod N$

## Folgerungen:

1. Aufteilung der ganzen Zahlen  $\mathbb{Z}$  in disjunkte Äquivalenzklassen:  
Beispiel, siehe nächste Folie.
2.  $-55 \bmod 9 \equiv (-55 + 7*9) \bmod 9 \equiv (-55 + 63) \bmod 9 \equiv 8 \bmod 9 = 8$

# Äquivalenzklassen mod $N$

Betrachten wir die ganzen Zahlen  $\mathbb{Z}$ , bezüglich mod 5, so wird  $\mathbb{Z}$  in die Äquivalenzklassen  $\{0, 1, 2, 3, 4\}$  aufgeteilt. Wir bezeichnen diese Menge  $\{0, 1, 2, 3, 4\} = \mathbb{Z}_5$ .

In der strengen Literatur werden die Klassen mit einem Querstrich versehen, also  $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$[0] = \overline{0} = \{\dots, -10, -5, 0, 5, 10, 15, \dots\}$ , also alle ganzzahligen Zahlen mit mod 5 = 0

$[1] = \overline{1} = \{\dots, -9, -4, 1, 6, 11, 16, \dots\}$ , also alle ganzzahligen Zahlen mit mod 5 = 1

$[2] = \overline{2} = \{\dots, -8, -3, 2, 7, 12, 17, \dots\}$ , also alle ganzzahligen Zahlen mit mod 5 = 2

$[3] = \overline{3} = \{\dots, -7, -2, 3, 8, 13, 18, \dots\}$ , also alle ganzzahligen Zahlen mit mod 5 = 3

$[4] = \overline{4} = \{\dots, -6, -1, 4, 9, 14, 19, \dots\}$ , also alle ganzzahligen Zahlen mit mod 5 = 4

D.h.  $\mathbb{Z}$  wird in die Äquivalenzklassen  $[0], [1], [2], [3], [4]$  aufgeteilt.

**Bemerkung:** Das Gleichheitszeichen  $c = a \bmod N$  ist streng genommen nicht richtig. Richtig ist das Äquivalentzeichen  $\equiv$ , also  $c \equiv a \bmod N$ , z.B.  $4 \equiv 12 \bmod 8$ . Siehe auch Lehrbuch [CP], Kap. 1.4.1.

# **Kap. 3**

## **DIE MOD N ARITHMETIK**

# Die Addition mod N

$$c \equiv (a + b) \bmod N \equiv (a \bmod N + b \bmod N) \bmod N$$

**Beispiel:** mit Modulus  $N = 5$

+	0	1	2	3	4	$a$
0	0	1	2	3	4	
1	1	2	3	4	0	
2	2	3	4	0	1	
3	3	4	0	1	2	
4	4	0	1	2	3	
$b$						$c$

$$(7 + 9) \bmod 5 \equiv 16 \bmod 5 \equiv 1$$

$$\begin{aligned}(7 + 9) \bmod 5 &\equiv (7 \bmod 5 + 9 \bmod 5) \bmod 5 \\ &\equiv (2 + 4) \bmod 5 \\ &\equiv 6 \bmod 5 = 1\end{aligned}$$



# Negative Elemente mod $N$

$$y \equiv -x \pmod{N}$$

or

$$y + x \pmod{N} \equiv 0$$

**Beispiel:** mit Modulus  $N = 5$

$x$	0	1	2	3	4
$y$	0	4	3	2	1

**Beispiel:**  $-55 \pmod{9} \equiv (-55 + 7 \cdot 9) \pmod{9} \equiv (-55 + 63) \pmod{9} \equiv 8 \pmod{9} = 8$

# Die Multiplikation mod $N$

$$c \equiv (a \cdot b) \bmod N \equiv (a \bmod N \cdot b \bmod N) \bmod N$$

**Beispiel:** mit Modulus  $N = 5$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$a$

$b$

$c$

$$(7 \cdot 9) \bmod 5 \equiv 63 \bmod 5 = 3$$

$$\begin{aligned}(7 \cdot 9) \bmod 5 &\equiv (7 \bmod 5 \cdot 9 \bmod 5) \bmod 5 \\ &\equiv (2 \cdot 4) \bmod 5 \\ &\equiv 8 \bmod 5 = 3\end{aligned}$$

# Das multiplikative Inverse mod $N$

$$y \equiv x^{-1} \bmod N$$

or

$$y \cdot x \bmod N \equiv 1$$

**Beispiel:** mit  $N = 5$

$x$	0	1	2	3	4
$y$	–	1	3	2	4

Mit dem ext. Euklid Algorithmus kann man das mult. Inverse mod  $N$  direkt berechnen. Wir werden es i.d.R. mit Durchprobieren od. einer Tabelle machen.

**Beispiel:**                      Gesucht:  $15^{-1} \bmod 26$

$x$	0	1	2	3	4	5	6	7
$x \cdot 15 \bmod 26$	–	15	4	19	8	23	12	1

**Kontrolle:**  $7 \cdot 15 \equiv 105 \equiv 104 + 1 \equiv 4 \cdot 26 + 1 \equiv 1 \bmod 26$ , also  $7 \equiv 15^{-1} \bmod 26$

und somit auch:  $15 \equiv 7^{-1} \bmod 26$

# Existenz des mult. inversen Elementes mod $N$

$$y \equiv x^{-1} \pmod{N}$$

Ex. nur wenn

$$\text{ggt}(x, N) = 1$$

d.h.  $x$  und  $N$  müssen teilerfremd d.h. relativ prim sein.

**Beispiel 1:**  $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$x$	0	1	2	3	4	5	6	7	8
$y = x^{-1} \pmod{9}$	-	1	5	-	7	2	-	4	8

**Beispiel 2:**  $\text{ggt}(15, 26) = 1$  darum ex.  $15^{-1} \pmod{26}$

**Beispiel 3:**  $\text{ggt}(14, 26) = 2 \neq 1$  darum ex.  $14^{-1} \pmod{26}$  *nicht*.

# Das Berechnen von $y \equiv x^{-1} \bmod N$ in der MEP

In der Modulendprüfung MEP werden Sie das multiplikative Inverse in Anwendungen...

- ... in einfachen Fällen mittels Durchprobieren berechnen.
- ... in aufwändigeren Fällen wird eine Tabelle mit den multiplikativen Inversen zur Verfügung stehen.

**Beispiel:**

x	1	2	3	4	5	6	7	8	9
$x^{-1} \bmod 19$	1	10	13	5	4	16	11	12	17

x	10	11	12	13	14	15	16	17	18
$x^{-1} \bmod 19$	2	7	8	3	15	14	6	9	18

Es kann aber sein, dass in Theorieaufgaben ...

- ... mit dem Satz von Euler oder Fermat das multiplikative Inverse berechnet werden muss (cf. Kap. 5).
- ... oder dass ein Inverses mod N geprüft werden muss.

**Beispiel 2, Fortsetzung:** Überprüfen Sie, dass  $15^{-1} \bmod 26 \equiv 7$  ist.

Richtig, weil  $(15 \cdot 7) \equiv 105 \equiv 104 + 1 \equiv 4 \cdot 26 + 1 \equiv 1 \bmod 26$

**Aufgabe 1a)** Ex.  $125^{-1} \bmod 192$ ? Wenn ja, ist der Wert 148?

**Aufgabe 1b)** Ist der Wert 149?

# Das Berechnen von $y \equiv x^{-1} \pmod{N}$ in der MEP

Wie berechnen Sie das multiplikative Inverse mod  $N$ , wenn die Multiplikationstabelle gegeben ist?

**Aufgabe 2:** Gegeben ist die Multiplikationstabelle von  $\langle \mathbb{Z}_{11} \setminus \{0\}, \cdot \pmod{11} \rangle$ . Bestimmen Sie alle multiplikativen Inversen mod 11.

$\cdot$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

# Bruchrechnen mod $N$

$$z \equiv \frac{x}{y} \bmod N \equiv (x \cdot y^{-1}) \bmod N$$

Resp.

$$x \equiv (z \cdot y) \bmod N$$

**Beispiel erste Berechnungsvariante:**  $\frac{5}{7} \bmod 9$

$$\frac{5}{7} \bmod 9 \equiv (5 \cdot 7^{-1}) \bmod 9 \equiv (5 \cdot 4) \bmod 9 \equiv 20 \bmod 9 = 2$$

Resp. wir suchen  $z$  so, dass  $5 \equiv (z \cdot 7) \bmod 9$

Es gilt:  $(2 \cdot 7) \bmod 9 \equiv 14 \bmod 9 \equiv 5$ , also  $z = 2$

**Beispiel zweite Berechnungsvariante:**  $\frac{5}{7} \bmod 9$

Wir suchen zunächst den Kehrwert von  $7 \bmod 9$ , d.h.  $t$  so, dass  $(t \cdot 7) \bmod 9 \equiv 1$ .

Durch trial and error finden wir  $t = 4$ , denn  $(t \cdot 7) \equiv 28 \equiv 1 \bmod 9$

Nun müssen wir noch  $(5 \cdot 4) \equiv 20 \equiv 2 \bmod 9$  rechnen.

**Bemerkung 1:** Es gibt zwar Kürzungsregeln, mein Tipp: **Nie Kürzen!**

**Bemerkung 2:**

Der TI-89 o.ä. TR können  $\frac{5}{7} \bmod 9$ , besser gesagt  $(5 \cdot 7^{-1}) \bmod 9$ , **nicht** richtig rechnen!

# Nullteilerfreiheit

Für reelle Zahlen gilt:

$$a = 0 \vee b = 0 \Leftrightarrow (a \cdot b) = 0$$

Die reellen Zahlen sind nullteilerfrei; die diskreten Zahlen sind nicht nullteilerfrei

Für diskrete Zahlen gilt hingegen:

$$a = 0 \vee b = 0 \Rightarrow (a \cdot b) \equiv 0 \bmod N \text{ aber } “\Leftarrow” \text{ gilt nicht!}$$

## Beispiele:

- 1)  $a = 5$  und  $b = 4$  und  $N = 10$ , dann ist  $(5 \cdot 4) \bmod 10 \equiv 0$ . Dabei ist weder  $5 \bmod 10 \equiv 0$  noch  $4 \bmod 10 \equiv 0$
- 2)  $a = 2$  und  $b = 3$  und  $N = 6$ , dann ist  $(2 \cdot 3) \bmod 6 \equiv 0$ .
- 3)  $a = 4$  und  $b = 6$  und  $N = 8$ , dann ist  $(4 \cdot 6) \bmod 8 \equiv 0$



# Potenzieren mod $N$

Die mod  $N$  Reduktion kann man jederzeit machen!

**Beispiel:**

$$3^8 \bmod 7 \equiv 6561 \bmod 7 = 2$$

$$3^8 \bmod 7 \equiv (3^4 \cdot 3^4) \bmod 7 \equiv (81 \cdot 81) \bmod 7$$

$$= [(81 \bmod 7) \cdot (81 \bmod 7)] \bmod 7 \equiv (4 \cdot 4) \bmod 7 \equiv 16 \bmod 7 = 2$$

**Frage:** Wie macht man das mit 300-stelligen Zahlen?

**Antwort:** Mit square and multiply (sam)

**Bemerkung:**

Im Rahmen der Elliptischen Kurven werden wir einen analogen Algorithmus „double and add“ kennenlernen.

# Schnelles Potenzieren mit square & multiply (sam)

**Ziel:** Die Berechnung von  $5^m \bmod 11$  mittels dem SAM-Algorithmus.

## Schritte:

- Exponent m binär darstellen.
- Erstes 1 „weglassen“, d.h. mit dem ersten 1 der binären Darstellung muss man nichts machen.
- Danach wird bei
  - „0“ quadriert.
  - „1“ wird zuerst quadriert dann mit dem Ausgangswert multipliziert.

**Präsenzbeispiel:** Wir wollen nun konkret  $5^{22} \bmod 11 = \underline{\hspace{2cm}}$  berechnen, also  $m = 22$ .

$(22)_{10} =$

Bit	
1	5
0	
1	
1	
0	

# ***Schnelles Potenzieren mit square & multiply (sam)***

## **Die Fakts zusammengestellt:**

- Die Potenz von dezimal in binär umgewandelt.
- Von links nach rechts
- Die erste Eins zählt nicht.
- Bei einer „1“ square und multiply
- Bei einer „0“ nur square
- Aufwand: square  $0,75t$  (\*); multiply  $1t$
- Es gibt schnellere Algorithmen → wäre eine Spezialvorlesung, ev. Teil des Moduls im MSc.

(\*) Die eigentliche Quadratur braucht sogar nur ca.  $\frac{1}{2}$  vom Aufwand einer Multiplikation. Doch die jeweilige Reduktion mod  $n$  muss bei beiden Operationen gemacht werden. Die Reduktion mod  $n$  ist aber in etwa gleich aufwändig wie die eigentliche Operation. Daraus ergibt sich dieser Aufwand von  $\frac{3}{4}$  einer Multiplikation.

**Präsenzbeispiel, Fortsetzung:** Berechnen des Aufwandes,  $t$  = Aufwand einer Mult.

•

---

## **Aufwand bei 3072 Bit RSA:**

- 3071 Quadraturen und im stat. Mittel ca. 1535 Multiplikationen, also total ca. der Aufwand  $3840t$ .

# SAM und „nur“ die Exponenten sind gefragt

**Beispiel:**  $x^{13} = x^{1101_2} = x^{(b_3, b_2, b_1, b_0)_2}$

#1  $(x^1)^2 = x^2 = x^{10_2}$  SQ, bit processed:  $b_2$

#2  $x^2 \cdot x = x^3 = x^{11_2}$  MUL, since  $b_2 = 1$

#3  $(x^3)^2 = x^6 = x^{110_2}$  SQ, bit processed:  $b_1$

#4  $x^6 \cdot 1 = x^6 = x^{110_2}$  no MUL operation since  $b_1 = 0$

#5  $(x^6)^2 = x^{12} = x^{1100_2}$  SQ, bit processed:  $b_0$

#6  $x^{12} \cdot x = x^{13} = x^{1101_2}$  MUL, since  $b_0 = 1$

- Wegen der Bitdarstellung  $(13)_{10} = (1\mathbf{1}0\mathbf{1})_2$  folgt die Reihenfolge der Exponenten:  $2 \rightarrow 3 \rightarrow 6 \rightarrow 12 \rightarrow 13$
- Aufwand: square 0,75t, multiply 1t
- **Beispiel:**  $3 \cdot \text{SQ} + 2 \cdot \text{MUL} = 4,25\text{t}$

## Aufgabe 3:

- Berechnen Sie nun konkret  $3^{13} \bmod 8$
- Bestimmen Sie die Reihenfolge der Exponenten bei  $x^{39}$ , und bestimmen Sie den Aufwand.
- Berechnen Sie nun konkret  $3^{39} \bmod 7$

# ***e-te Wurzel mod N & Logarithmus mod p***

Die Gleichung  $x^e = y$  hat die Lösung  $x = \sqrt[e]{y}$

Analog:  $x^e \equiv y \bmod N$  hat die Lösung  $x \equiv \sqrt[e]{y} \bmod N$  (\*)

Resp.

Die Gleichung  $a^x = y$  hat die Lösung  $x = \log_a y$

Analog:  $a^x \equiv y \bmod p$  hat die Lös.  $x \equiv \log_a y \bmod p$  (\*)

(\*) Die diskrete Wurzel und der diskrete Logarithmus können i.a. **nicht** mit einer Formel berechnet werden!! Es sind sogenannte Einweg- oder Oneway-Funktionen. Dabei ist die diskrete Wurzel eine Trapdoor-Funktion, d.h. mit einem Geheimnis kann diese diskrete Wurzel berechnet werden (cf. **RSA**). Zum diskreten Log. ist **keine** Trapdoor bekannt, d.h. ihn kann man **nicht** berechnen (cf. **Diffie-Hellman, resp. Elgamal**).

# ***Potenzieren mod N ist kein Problem, aber ...***

Die Berechnung von  $x^e \equiv y \mod N$

Resp. von  $a^x \equiv y \mod p$  ist kein Problem  $\rightarrow$  SAM

Die Umkehrung  $x \equiv \sqrt[e]{y} \mod N$

Resp.  $x \equiv \log_a y \mod p$  jedoch schon!

**Frage:** Warum?

**Antwort:**

Zunächst ist für beide Umkehrberechnungen festzuhalten:

- Es ist nicht gesichert, dass es einen solchen Wert gibt.
- Es ist nicht gesichert, dass wenn es einen Wert gibt, dass dieser Wert eindeutig ist.
- Für beide Umkehrberechnungsarten gilt aber, dass wenn gewisse Bedingungen erfüllt sind, die Umkehrung – also die e-te Wurzel mod N resp. der diskrete Logarithmus mod p – existiert und eindeutig ist. Aus der Existenz der Eindeutigkeit kann aber nicht gefolgert werden, dass man die Umkehrberechnung durchführen kann!!!
- Alle 4 Berechnungen – also  $x^e \equiv y \mod N$ ,  $x \equiv \sqrt[e]{y} \mod N$ ,  $a^x \equiv y \mod p$  und  $x \equiv \log_a y \mod p$  – haben ein chaotisches Verhalten.

# Ziehen der e-ten Wurzel mod N

Also Lösen der Gleichung:  $x^e \equiv y \pmod{N} \Leftrightarrow x \equiv \sqrt[e]{y} \pmod{N}$

$x$	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 \pmod{13}$	0	1	8	1	12	8	8	5	5	1	12	5	12

Somit ist  $\sqrt[3]{8} \pmod{13} = \{2; 5; 6\}$ , da  $2^3 \equiv 5^3 \equiv 6^3 \equiv 8 \pmod{13}$

Andererseits gibt es z.B. keinen Wert zu  $\sqrt[3]{9} \pmod{13}$ , da es keinen Wert  $x$  mit  $x^3 \equiv 9 \pmod{13}$  gibt.

Im folgenden Beispiel ist die Zuordnung in beide Richtungen eindeutig, aber die Werte sind chaotisch angeordnet.

$x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$x^3 \pmod{33}$	0	1	8	27	31	26	18	13	17	3	10	11	12	19	5	9	4
$\sqrt[3]{x} \pmod{33}$	0	1	29	9	16	14	30	28	2	15	10	11	12	28	20	27	25

$x$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$x^3 \pmod{33}$	29	24	28	14	21	22	23	30	16	20	15	7	2	6	25	32
$\sqrt[3]{x} \pmod{33}$	8	6	13	26	21	22	23	18	31	5	3	19	17	24	4	32

## Beispiel 1:

$\sqrt[3]{2} \pmod{33} \equiv ?$  d.h. ich muss diejenige Zahl „?“ suchen so dass  $?^3 \pmod{33} \equiv 2$  gilt.  
In der Tabelle sieht man, dass  $? = 29$  sein muss, denn  $29^3 \pmod{33} \equiv 2$ .

# Ziehen der e-ten Wurzel mod N, Fortsetzung

$x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$x^3 \bmod 33$	0	1	8	27	31	26	18	13	17	3	10	11	12	19	5	9	4
$\sqrt[3]{x} \bmod 33$	0	1	29	9	16	14	30	28	2	15	10	11	12	28	20	27	25

$x$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$x^3 \bmod 33$	29	24	28	14	21	22	23	30	16	20	15	7	2	6	25	32
$\sqrt[3]{x} \bmod 33$	8	6	13	26	21	22	23	18	31	5	3	19	17	24	4	32

## Beispiel 2:

$\sqrt[3]{26} \bmod 33 \equiv ?$  d.h. ich muss diejenige Zahl „?“ suchen so dass  $?^3 \bmod 33 \equiv 26$  gilt. In der Tabelle sieht man, dass  $? = 5$  sein muss, denn  $5^3 \bmod 33 \equiv 26$ .

**Aufgabe (ohne Musterlösung)** Verifizieren Sie nun in analoger Weise.

- $x \equiv \sqrt[3]{15} \bmod 33 \Rightarrow x = 27$
- $x \equiv \sqrt[3]{24} \bmod 33 \Rightarrow x = 18$
- Weitere eigene Werte.

## Wichtig:

Bei gewissen Bedingungen vom Modulus N und dem Exponenten e gibt es einen „Trick“ – genauer, wenn man ein Geheimnis kennt – so dass die e-te Wurzel mod N berechnet werden kann. M.a.W. in diesem Falle ist die e-te Wurzel mod N eine Einwegfunktion mit Trapdoor. Dies wird dann beim ersten asym. Verfahren, dem RSA, verwendet.



# Logarithmieren mod $p$

Also Lösen der Gleichung:  $a^x \equiv y \mod p \Leftrightarrow x \equiv \log_a y \mod p$ ,  $p$  eine Primzahl.

$x$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$8^x \mod 19$	8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12

Somit ist  $\log_8 11 \mod 19 = \{4; 10; 16\}$ , da  $8^4 \equiv 8^{10} \equiv 8^{16} \equiv 11 \mod 19$

Andererseits gibt es z.B. keinen Wert zu  $\log_8 15 \mod 19$ , da es keinen Wert  $x$  mit  $8^x \equiv 15 \mod 19$  gibt.

Im folgenden Beispiel ist die Zuordnung in beide Richtungen eindeutig, aber die Werte sind chaotisch angeordnet.

$x$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$15^x \mod 19$	15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
$\log_{15} x \mod 19$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

## Beispiel 3:

$\log_{15} 4 \mod 19 \equiv ?$  d.h. ich muss diejenige Zahl „?“ suchen so dass  $15^? \mod 19 \equiv 4$  gilt. In der Tabelle sieht man, dass  $? = 10$  sein muss, denn  $15^{10} \mod 19 \equiv 4$ .

## Beispiel 4:

$\log_{15} 7 \mod 19 \equiv ?$  d.h. ich muss diejenige Zahl „?“ suchen so dass  $15^? \mod 19 \equiv 7$  gilt. In der Tabelle sieht man, dass  $? = 12$  sein muss, denn  $15^{12} \mod 19 \equiv 7$ .

# Logarithmieren mod $p$ , Fortsetzung

**Aufgabe (ohne Musterlösung)** Verifizieren Sie nun in analoger Weise.

d)  $x \equiv \log_{15} 8 \bmod 19 \equiv 15$

e)  $x \equiv \log_{15} 13 \bmod 19 \equiv 10$

f) Weitere eigene Werte.

## Wichtig:

Beim diskreten Logarithmus mod  $p$  handelt es sich um eine Einwegfunktion ohne Trapdoor. M.a.W. es gibt für niemanden einen Trick, um diesen rechnen zu können. Wie das dann in der asymmetrischen Kryptographie verwendet wird, sehen wir dann beim Diffie-Hellman Schlüsselaustausch.

# Die chaotische Anordnung

Anbei die chaotische Anordnung der Werte bei  $627^x \bmod 941$ . Die Umkehrung, also  $\log_{627} x \bmod 941$ , wird ebenfalls sehr chaotische Werte haben.

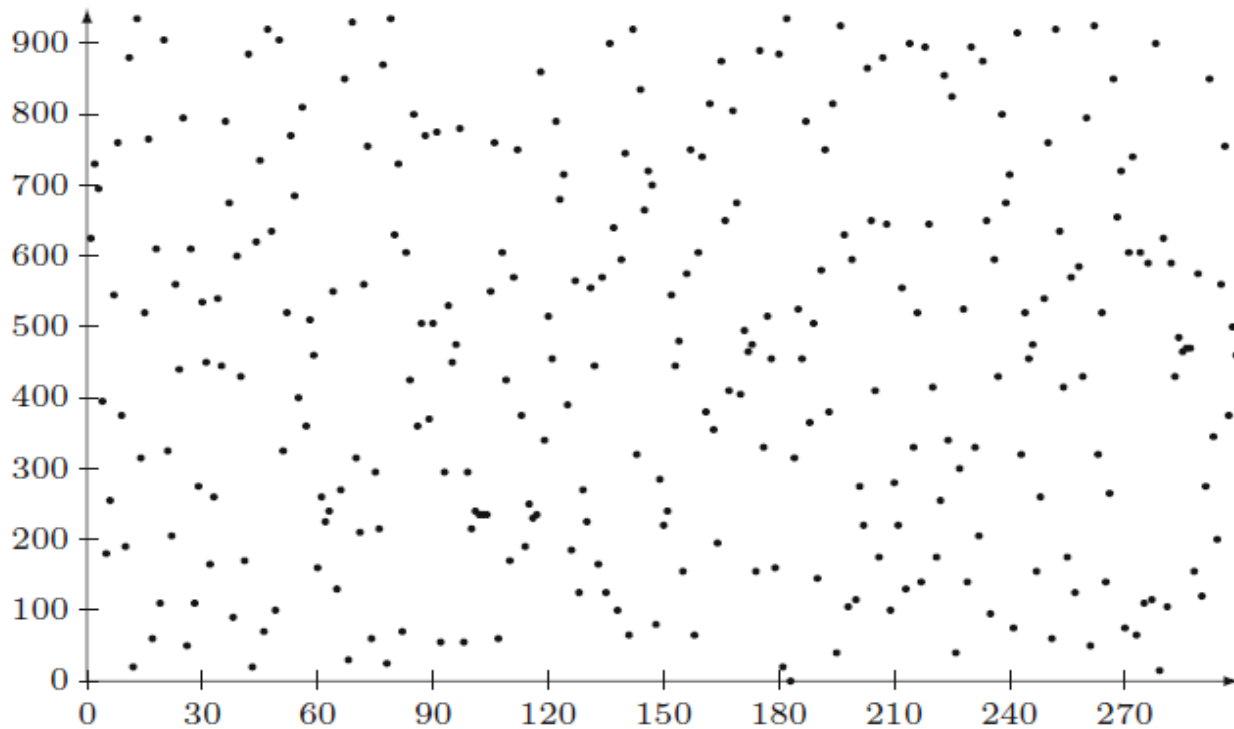


Figure 2.2: Powers  $627^i \bmod 941$  for  $i = 1, 2, 3, \dots$

Nun stelle man sich vor der Modulus  $N$  resp.  $p$  ist eine Zahl mit 2048 Bit. D.h.  $N$  resp.  $p$  haben die Größenordnung von  $> 10^{600}$ . Dabei muss man sich im Klaren sein, dass die Anzahl Atome im Weltall die Größenordnung  $10^{80}$  hat. Und wenn auf jedem Atom im Weltall ein Weltall liegen würde, so wäre die Anzahl der Atome erst in der Größenordnung von  $10^{160}$ . Diese Zahl ist direkt niedlich klein gegenüber  $10^{600}!!$

# **Kap. 4**

## **PRIMZAHLEN**

# Ein paar Zahlen

Referenz	Größenordnung
Sekunden pro Jahr	$3 \cdot 10^7$
Taktzyklen pro Jahr bei 5 GHz PC	$1,6 \cdot 10^{17}$
Sekunden seit Entstehung des Weltalls	$2 \cdot 10^{17}$
Dezimalwert von $2^{64}$ = Anz. mög. Schlüssel eines 64 Bit Schlüssels	$1,8 \cdot 10^{19}$
Dezimalwert von $2^{128}$ = Anz. mög. Schlüssel eines 128 Bit Schlüssels	$3,4 \cdot 10^{38}$
Anzahl Atome in unserer Milchstrasse	$10^{67}$
Anzahl 75-stelliger Primzahlen	$5,2 \cdot 10^{72}$
Dezimalwert von $2^{256}$ = Anz. mög. Schlüssel eines 256 Bit Schlüssels	$1,2 \cdot 10^{77}$
Anzahl Atome im Weltall	$10^{78}$
Anzahl 120-stelliger Primzahlen = Anz. Primzahlen mit 400 Bit	Ca. $10^{117}$
Anzahl der Rechenoperationen, seit der Entstehung des Weltalls, wenn jedes Atom des Weltalls ein Supercomputer mit einer Leistung von $10^{20}$ Operationen pro Sekunde wäre.	$2 \cdot 10^{115}$
Anzahl 150-stelliger Primzahlen = Anz. Primzahlen mit 500 Bit	Ca. $10^{147}$
Anzahl Atome, wenn auf jedem Atom im Weltall ein Weltall läge	Ca. $10^{156}$
Anz. 308-stelliger Primz. = Anz. Primz. mit 1024 Bit (für 2048 Bit RSA)	Ca. $10^{305}$
Anz. 616-stelliger Primz. = Anz. Primz. mit 2048 Bit (für 2048 Bit DH)	Ca. $10^{613}$

# Primzahldarstellung

Die Primzahldarstellung einer natürlichen Zahl  $n$  ist eindeutig:

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_k^{n_k} = \prod_{i=1}^k p_i^{n_i}$$

## Beispiele:

$$144 = 2^4 \cdot 3^2$$

$$21420 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17$$

# Anzahl Primzahlen bis zur natürlichen Zahl $x$

Näherungsformel zur Anzahl der Primzahlen von 1 bis  $x$ :

$$\pi(x) \approx \frac{x}{\ln(x)}$$

Anteil der Primzahlen in allen ungeraden Zahlen von 1 bis  $x$ :

$$APZ(x) = \frac{\text{Anz. PZ}}{\text{Anz. ungerade Z.}} \approx \frac{\frac{x}{\ln(x)}}{\frac{x}{2}} = \frac{2}{\ln(x)}$$

**Beispiel:**  $x = 10^{150}$

$$\pi(10^{150}) \approx \frac{10^{150}}{\ln(10^{150})} = \frac{10^{150}}{150 \cdot \ln(10)} \approx \frac{10^{150}}{345} \approx \frac{10^{150}}{3,5 \cdot 10^2} = \frac{10 \cdot 10^{149}}{3,5 \cdot 10^2} = \frac{10 \cdot 10^{147}}{3,5} \approx 2,9 \cdot 10^{147}$$

$$APZ(10^{150}) \approx \frac{2}{\ln(10^{150})} = \frac{2}{150 \cdot \ln(10)} \approx \frac{2}{345} = 0,0058 = 0,58\% = 5,8\text{‰} \approx \frac{1}{170}$$

Der Anteil der Primzahlen aller ungeraden Zahlen von 1 bis  $10^{150}$  ist ca. 0,58%. D.h. ca. jede **170-ste** ungerade Zahl ist eine Primzahl.

**Wie sieht das für n-stellige Primzahlen aus? In der nächsten Folie schätzen wir das genau ab. Braucht es die genaue Abschätzung?**

# Anzahl der n-stelligen Primzahlen

Anzahl der n-stelligen Primzahlen:

$$\pi(10^n) - \pi(10^{n-1})$$

Anteil der n-stelligen PZ. in den n-stelligen ungeraden Zahlen:

$$APZ(n) = \frac{\text{Anz. PZ}}{\text{Anz. ung. Z.}} \approx \frac{\pi(10^n) - \pi(10^{n-1})}{\frac{0,9 \cdot 10^n}{2}} = \frac{\pi(10^n) - \pi(10^{n-1})}{0,45 \cdot 10^n}$$

**Beispiel:**  $n = 150 \Rightarrow x = 10^{150}$

$$\pi(10^{150}) - \pi(10^{149}) \approx \frac{10^{150}}{\ln(10^{150})} - \frac{10^{149}}{\ln(10^{149})} \approx 2,6 \cdot 10^{147}$$

$$APZ(n) \approx \frac{\frac{10^{150}}{\ln(10^{150})} - \frac{10^{149}}{\ln(10^{149})}}{0,45 \cdot 10^{150}} = \frac{2,6}{0,45} \cdot \frac{10^{147}}{10^{150}} \approx \frac{5,8}{1000} = 0,58\% = 5,8\text{‰} \approx \frac{1}{170}$$

Der Anteil der 150-stelligen Primzahlen aller 150-stelligen ungeraden Zahlen ist ca. 0,58%. D.h. ca. jede **170-ste** 150-stellige ungerade Zahl ist eine 150-stellige Primzahl.

**Fazit:** Nein, die genaue Abschätzung braucht es nicht unbedingt!



## Aufgabe 4:

Um einen RSA mit Modulus  $N = 2048$  Bit zu generieren, müssen 2 Primzahlen je der Grösse von 1024 Bit erzeugt werden. Das Produkt  $N = pq$  ist eine Zahl der Grösse von 2048 Bit, denn beim Multiplizieren verdoppelt sich die Stellenzahl.

a) Wie gross ist eine Zahl (in Dezimalstellen) von 1024 Bit?

Im Folgenden ist  $n = \text{Anzahl der Dezimalstellen der Zahl aus a)}$ .

- b) Schätzen Sie die Anzahl Primzahlen von 1 bis  $10^n$ .
- c) Wie gross ist der Anteil an Primzahlen in den ungeraden Zahlen von 1 bis  $10^n$ ?
- d) Schätzen Sie die Anzahl Primzahlen innerhalb der  $n$ -stelligen Dezimalzahlen.
- e) Wie gross ist der Anteil an Primzahlen innerhalb der  $n$ -stelligen ungeraden Dezimalzahlen?
- f) Formulieren Sie das Resultat aus e) im Sinne «ca. jede  $y$ -ste  $n$ -stellige ungerade Zahl ist eine  $n$ -stellige Primzahl».

# ***Erzeugung von Primzahlen***

## **Die zentrale Frage:**

Eine zentrale Frage lautet nun: „Wie erzeugt man 308-stellige Primzahlen, die es für einen RSA mit Modulus  $N = 2048$  Bit braucht?“

## **Antwort:**

Bei der Wahl der Primzahlen gibt es 2 Methoden:

- Die probabilistische Methode (z.B. Miller-Rabin Test).
- Die deterministische M. (eine Primzahl wird konstruiert).

# Die probabilistische Methode

- Wir wählen eine zufällige 308-stellige ungerade Zahl, wie wir in Aufgabe 4 berechnet haben, ist Wsk. ca.  $1 : 355$  oder etwa 0,28%.
- Nun berechnet man ob der ggt dieser Zahl und dem Produkt (ca.) der ersten 50 Primzahlen 1 ist oder nicht. (Das Produkt der ersten 52 Primzahlen ist eine 100-stellige Zahl).
- Wenn  $\text{ggt} \neq 1$ , dann wählt man eine neue Zahl.
- Wenn  $\text{ggt} = 1$ , dann macht man sogenannte Primzahltests. Wenn der Test missrät, dann ist es sicher keine Primzahl, wenn erfolgreich, dann ist es bis auf eine Wsk. von x% eine Primzahl. Mit genügenden Durchläufen wird die Wsk. beliebig hoch (siehe nächste Folie). Details siehe in [CP-D], Kap. 7.6.2 «Primzahltests» → **nicht Prüfungstoff!**

Diese Methode ist nicht sehr schnell. Da man das aber nicht sehr oft macht (typischerweise einmal pro User), ist das verkraftbar.

# RSA *How to find large prim numbers?*

- There are about  $10^{616}$  primes with 2048 bits in length.
- There are only  $10^{77} - 10^{80}$  atoms in the universe.
- The chance that two people choose the same prime factors for key generation is therefore near to nil!
- To prove that a randomly chosen number is really prime you would have to factor it. Try the about first 50 small factors (3, 5, 7, 11, ...)
- Probabilistic Primality Tests (e.g. Miller–Rabin)

Result of Primality Test	not prime	is prime	random number is a
	100 %	0.1 %	composite number
	0 %	99.9 %	prime number

- That means:
  - If the test says “not prim”, then the number is 100% not prim (= composite) and 0% prim.
  - If the test says “prim”, then the number 0,1% not prim (= composite) and 99,9% prim.
  - Passing a test means: “the number is prim”.
  - After passing 1 test, the prob. a random number not to be prim = 1 : 1000
  - After passing 5 tests, the prob. a random number not to be prim =  $(1 : 1000)^5 = 10^{-15}$  = one to one billion, therefore we assume to be prime.
  - If you need a better probability, do additional tests.

# ***Die deterministische Methode***

Man produziert mittels einer Formel Primzahlen.  
Diese Methode ist sehr schnell.

Dabei ist zu beachten, dass es **keine** Formel gibt, die **alle** Primzahlen erzeugt.

Mit der obigen Formel muss man aber sicher sein, dass die gewählten Primzahlen wie eine zufällige Wahl sind.

Die Methode ist mathematisch sehr anspruchsvoll.

Auf weitere Details gehen wir an dieser Stelle nicht ein.

# **Kap. 5**

## **ZAHLENTHEORETISCHE FUNKTIONEN**

# Zahlentheorie I: Der kleine Satz von Fermat

Sei  $p$  eine Primzahl und  $a$  relativ prim zu  $p$

(d.h.  $\text{ggT}(a, p) = 1$ ), dann gilt:

$$a^{p-1} \equiv 1 \pmod{p} \quad \begin{array}{l} | \cdot a \\ | : a \end{array}$$

$$\text{resp. } a^p \equiv a \pmod{p}$$

$$\text{resp. } a^{p-2} \equiv a^{-1} \pmod{p} (*)$$

(\*) Als Alternative zur Berechnung mit ext. Euklid.

## Beispiele $a < p$ :

Für  $a = 4$  &  $p = 5$  gilt:  $4^{5-1} \equiv 256 \equiv 1 \pmod{5}$

resp.  $4^5 \equiv 1024 \equiv 4 \pmod{5}$ ,

resp.  $4^{5-2} \equiv 64 \equiv 4 \equiv 4^{-1} \pmod{5}$ , Check:  $4 \cdot 4 \equiv 1 \pmod{5}$

$$\Rightarrow 4^{-1} \pmod{5} = 4$$

$a = 4$  &  $p = 7$  gilt:  $4^{7-1} \equiv 4^6 \equiv 1 \pmod{7}$

resp.  $4^7 \equiv 4 \pmod{7}$

resp.  $4^{7-2} \equiv 2 \equiv 4^{-1} \pmod{7}$ , Check:  $2 \cdot 4 \equiv 1 \pmod{7}$

$$\text{Wert} \cdot \text{Kehrwert} \equiv 1 \pmod{p}$$

$$\Rightarrow 4 \equiv 2^{-1} \pmod{7}$$

# Zahlentheorie I: Der kleine Satz von Fermat

Sei  $p$  eine Primzahl und  $a$  relativ prim zu  $p$

(d.h.  $\text{ggT}(a, p) = 1$ ), dann gilt:  $a^{p-1} \equiv 1 \pmod{p}$

resp.  $a^{\varphi(p)+1} \equiv a \pmod{p}$  resp.  $a^{\varphi(p)-1} \equiv a^{-1} \pmod{p}$

Beispiel  $a > p$ :

und  $\text{ggT}(a, p) = 1$  d.h.  $a \neq n \cdot p$  ( $a$  ist kein Vielfaches von  $p$ )

Der Satz gilt auch für  $a > p$ :  $a = 10$  und  $p = 7$  gilt:

$$10^{7-1} \equiv 10^6 \equiv 1 \pmod{7}$$

$$\text{resp. } 10^7 \equiv 10^6 \cdot 10 \equiv 1 \cdot 10 \equiv 10 \equiv 3 \pmod{7},$$

$$\text{resp. } 10^{7-2} \equiv 5 \equiv 10^{-1} \equiv 3^{-1} \pmod{7}, \text{ Check: } 10 \cdot 5 \equiv 3 \cdot 5 \equiv 1 \pmod{7}$$

Beispiel  $a > p$  und  $\text{ggT}(a, p) \neq 1$ :

d.h. Wenn Bed. nicht erfüllt  
Satz funktioniert nicht.

$$a = 14 \text{ \& } p = 7, \text{ also } \text{ggT}(a, p) = 2 \neq 1: 14^{7-1} \equiv 14^6 \equiv 0 \not\equiv 1 \pmod{7}$$



# Zahlentheorie II: Die Euler'sche $\phi$ – Funktion

Sei  $n$  eine natürliche Zahl, dann bezeichnet  $\phi(n)$  die Anzahl der teilerfremden Zahlen, die zwischen 1 und  $n$  liegen (inkl. die 1, exkl.  $n$ ).

Erste Beispiele:

$p$  Primzahl  
 $\phi(p) = p - 1$

Alle Werte für  $\phi(n) = \varphi(n)$  für  $n = 1, \dots, 36$

$n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6

$n$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$\phi(n)$	18	8	12	10	22	8	20	12	18	12	28	8	30	16	20	16	24	12

Bemerkung: Es sind beide Bezeichnungen  $\phi(n)$  und  $\varphi(n)$  üblich!!

# Die Euler'sche $\varphi$ -Funktion, Regeln

Für  $n = p$  eine Primzahl gilt:  $\varphi(p) = p - 1$ , z.B.  $\varphi(11) = 11 - 1 = 10$

Für  $n, m$  teilerfremd gilt:  $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

z.B.  $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = 1 \cdot 2 \cdot 4 = 8$

$$\begin{aligned}\varphi(3 \cdot 10) &= \\ \varphi(3) \cdot \varphi(10) &= \\ 2 \cdot 4 &= 8\end{aligned}$$

Es sind dies die Zahlen 1; 7; 11; 13; 17; 19; 23; 29.

**!!**  $25 = 5 \cdot 5$ , aber  $\varphi(25) \neq \varphi(5) \cdot \varphi(5) = 4 \cdot 4 = 16$ , denn  $\varphi(25) = 20$

$n = p^k$  (p eine Primz.)  $\Rightarrow \varphi(p^k) = p^k - p^{k-1} = \underbrace{(p - 1)}_{\substack{\uparrow \\ \text{p-1} \\ \text{ausgeklemmt}}} p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$

z.B.  $\varphi(27) = \varphi(3^3) = 3^3 - 3^{3-1} = 27 - 9 = 18$

$\uparrow$   $\text{p-1}$   $\text{ausgeklemmt}$   $\uparrow$   $\text{p}^k$   $\text{ausge-}$   $\text{klemmt}$

resp.  $\varphi(3^3) = 3^3 \left(1 - \frac{1}{3}\right) = 27 \cdot \frac{2}{3} = 18$

Es sind dies die Zahlen 1; 2; 4; 5; 7; 8; 10; 11; 13; 14; 16; 17; 19; 20; 22; 23; 25; 26.

**!!**  $\varphi(25) = \varphi(5^2) = 5^2 - 5^{2-1} = 25 - 5 = 20$

**Aufgabe 5:** Repetieren Sie nun die affine Chiffre in Präsenz 5:  $y = e_k(x) \equiv a \cdot x + b \bmod n$

- Wie gross ist der grösstmögliche Schlüsselraum, wenn vorausgesetzt wird, dass die Parameter a und b, je weder Null noch Eins sein dürfen und  $n = 2^m$  gilt?
- Wie gross ist der Schlüsselraum für  $m = 12$ ?

# Die Euler'sche $\varphi$ - Funktion, Regeln, Fort.

$$\underline{\varphi(315)} = \varphi(3^2 \cdot 5 \cdot 7) = \varphi(3^2) \cdot \varphi(5) \cdot \varphi(7) = 3^2 \left(1 - \frac{1}{3}\right) \cdot 4 \cdot 6 = 6 \cdot 4 \cdot 6 = 144$$

$$\underline{\varphi(315)} = \varphi(3^2) \cdot \varphi(5) \cdot \varphi(7) = (3^2 - 3^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0) = 6 \cdot 4 \cdot 6 = 144$$

Oder mit der Formel mit den Primteiler von n:

*n = 315 hat 3 Teiler  
nämlich 3, 5, 7*

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \cdot \prod_{p|n} \left(\frac{p-1}{p}\right) \quad \checkmark$$

$$\underline{\varphi(315)} = 315 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) = 315 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 3 \cdot 3 \cdot 5 \cdot 7 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 144$$

Und zum Abschluss ein Beispiel mit allen 3 Formeln:

$$\varphi(40) = \varphi(2^3 \cdot 5) = \varphi(2^3) \cdot \varphi(5) = 2^3 \left(1 - \frac{1}{2}\right) \cdot 4 = 4 \cdot 4 = 16$$

$$\varphi(40) = \varphi(2^3 \cdot 5) = \varphi(2^3) \cdot \varphi(5) = (2^3 - 2^2) \cdot (5^1 - 5^0) = 4 \cdot 4 = 16$$

$$\varphi(40) = 40 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40 \cdot \frac{1}{2} \cdot \frac{4}{5} = 8 \cdot 5 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4 \cdot 4 = 16$$

# Zahlentheorie III: Der Satz von Euler

Sei  $a$  und  $n$  relativ prim, d.h.  $\text{ggt}(a, n) = 1$ , dann gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad | \cdot a \quad | \div a$$

$$\text{resp. } a^{\varphi(n)+1} \equiv a \pmod{n} \quad \text{resp. } a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}$$

**Beispiele:** Für  $a = 4$  &  $n = 9$  mit  $\varphi(9) = 6$  gilt:  $4^6 \equiv 1 \pmod{9}$

$$\text{resp. } 4^7 \equiv 4 \pmod{9},$$

$$\text{resp. } 4^5 \equiv 7 \equiv 4^{-1} \pmod{9}, \text{ Check } 7 \cdot 4 \equiv 28 \equiv 1 \pmod{9}$$

Das gilt auch für  $a > n$ :  $a = 14$  und  $n = 9$  mit  $\varphi(9) = 6$  gilt:

$$14^6 \equiv 1 \pmod{9} \quad \text{resp. } 14^7 \equiv 14 \equiv 5 \pmod{9}, \quad \text{resp. } 14^5 \equiv 14^{-1} \equiv 2 \pmod{9}$$

$$\text{Check } 14 \cdot 2 \equiv 28 \equiv 1 \pmod{9}$$

$$a = 15 \text{ \& } n = 10, \text{ ggt}(a, n) = 5 \neq 1 \text{ \& mit } \varphi(10) = 4 \text{ gilt: } 15^4 \equiv 5 \not\equiv 1 \pmod{10}$$

**Aufgabe 6:** Führen Sie die Berechnungen für  $a = 22$  und  $n = 27$  durch.

bis 16h15

# Kap. 6

## EINFÜHRUNG IN DIE ABSTRAKTE ALGEBRA

heuer Stoff  
→ brauchen wir um Diffie-Hellman  
versteht zu verstehen Pr 7/8  
und Elliptische Kurven → 9/10



# Definition: Algebraische Gruppe $\langle G, * \rangle$

Eine Gruppe ist ein algebraisches System mit einer Menge  $G$  und einer Operation  $*$ , so dass für alle Elemente  $a, b$  &  $c$  in  $G$  die folgenden Bedingungen erfüllt sind:

- Abgeschlossenheit:  $a * b$  ist auch in  $G$  *das Resultat ist wieder ein Element der Menge*
- Assoziativ Gesetz:  $a * (b * c) = (a * b) * c$
- Neutral Element:  $a * e = e * a = a$  *d.h.  $e$  bewirkt nichts*
- Inverses Element:  $a * a' = a' * a = e$  *( $a'$  ist auch Element der Menge  $G$ )*
- Kommutativ Gesetz:  $a * b = b * a$  (wenn das KG gilt, dann ist es eine sogenannte Abel'sche Gruppe)

$|G|$  = Ordnung der Gruppe = Anzahl Elemente der Gruppe.

## Beispiele:

- Addition in  $\mathbb{R}$ :  $\langle \mathbb{R}, + \rangle$   $e = 0$ ,  $a' = -a$ ,  $\text{Ord} = \infty$
- Multiplikation in  $\mathbb{R} \setminus \{0\} = \mathbb{R}^*$ :  $\langle \mathbb{R}^*, \cdot \rangle$   $e = 1$ ,  $a' = a^{-1}$ ,  $\text{Ord} = \infty$

# Weitere Beispiele

## Gruppen sind:

- $\langle \mathbb{Z}, + \rangle$ ,  $\{1, \dots, p^{-1}\}$  Ord =  $\infty$
- $\langle \mathbb{Q} \setminus \{0\} = \mathbb{Q}^*, \cdot \rangle$ , Ord =  $\infty$
- $\langle \mathbb{Z}_n, + \bmod n \rangle$ , für beliebiges  $n \in \mathbb{N}$  Ord =  $n$  da Element
- $\langle \mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*, \cdot \bmod p \rangle$ , für beliebige Primzahl  $p$  Ord =  $p-1$
- $\langle \mathbb{Z}_n^*, \cdot \bmod n \rangle$ ,  $n \in \mathbb{N}$  bel.,  $\mathbb{Z}_n^* = \{a \in \mathbb{N} < n \ \& \ \text{ggT}(a, n) = 1\}$  Ord =  $\varphi(n)$
- Im Rahmen der Elliptischen Kurven lernen wir weitere Gruppen kennen.

## Keine Gruppen sind:

- $\langle \mathbb{N}, + \rangle$ , da  $-a \notin \mathbb{N}$ , d.h. das inverse Element zu  $a$  ist keine nat. Zahl.
- $\langle \mathbb{N}, - \rangle$ , da  $a - b$  ev.  $\notin \mathbb{N}$  ist. Z.B.  $3 - 5 \notin \mathbb{N}$ , also Abgeschlossenheit NOK.
- $\langle \mathbb{Z} \setminus \{0\}, \cdot \rangle$ , da  $a^{-1} \notin \mathbb{Z} \setminus \{0\}$ , d.h. das inv. Element zu  $a$  ist keine ganze Zahl.
- $\langle \mathbb{Z}_n \setminus \{0\}, \cdot \bmod n \rangle$ ,  $n \in \mathbb{N}$  und  $n$  keine Primzahl, nicht alle Elemente haben ein Inverses – nur für  $a$  mit  $\text{ggT}(a, n) = 1$  ex.  $a^{-1} \bmod n$  – es gibt genau  $\varphi(n)$  solcher Elemente  $a$ , die ein Inverses mod  $n$  haben.
- $\langle G, \cdot \rangle$ , mit  $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$  usw. z.B.  $0^{-1}$  nicht ex., tw. weitere Gründe.

# Definition: Untergruppe(n) der Gruppe $\langle G, * \rangle$

Eine Teilmenge  $U$  einer Gruppe  $G$  mit  $*$  heisst Untergruppe von  $G$ , wenn die Operation  $*$  in  $U$  abgeschlossen ist, d.h. für alle Elemente  $a$  und  $b$  in  $U$  gilt:

Abgeschlossenheit:  $a * b$  ist wieder in  $U \rightarrow$  die anderen Eigenschaften sind dann automatisch erfüllt

## Bemerkungen:

- Eine Untergruppe ist eine Gruppe in der Gruppe.
- Sei  $U$  eine Untergruppe von  $G$ , dann teilt die Ordnung von  $U$  die Ordnung von  $G$ :  $\text{Ord } U \mid \text{Ord } G$ .
- Die Gruppe  $G$  hat immer  $\{e\}$  ( $e = \text{NE}$ ) und  $G$  als (sog. «triviale») Untergruppen.
- Als direkte Folgerung der zweiten Bemerkung: Ist die Gruppenordnung prim, dann hat  $G$  nur  $\{e\}$  und  $G$  als Untergruppen.

## Beispiele:

- $\{e\}$  und  $G$  sind (triviale) Untergruppen von  $G$ .  $\text{Ord } \{e\} = 1$
- $\langle \mathbb{Z}_7, + \bmod 7 \rangle$  hat die Ordnung 7 und hat daher nur  $\{e\}$  und  $G$  als UG
- $\{e\} = \{1\}$  ist eine UG von  $\langle \mathbb{Z}_7 \setminus \{0\}, \cdot \bmod 7 \rangle$ ,  $\text{Ord } \{1\} = 1 \leftarrow \text{UG}$
- $G = \{1; 2; 3; 4; 5; 6\}$  ist eine UG von  $\langle \mathbb{Z}_7 \setminus \{0\}, \cdot \bmod 7 \rangle$ ,  $\text{Ord } G = 6 \leftarrow 6$
- $\{1; 2; 4\}$  ist eine UG von  $\langle \mathbb{Z}_7 \setminus \{0\}, \cdot \bmod 7 \rangle$ ,  $\text{Ord } \{1; 2; 4\} = 3$
- $\{1; 6\}$  ist eine UG von  $\langle \mathbb{Z}_7 \setminus \{0\}, \cdot \bmod 7 \rangle$ ,  $\text{Ord } \{1; 6\} = 2$



# Beispiel: Die Gruppe $\langle \mathbb{Z}_7 \setminus \{0\} = \mathbb{Z}_7^*, \cdot \bmod 7 \rangle$

6

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

ord 6

$UG_1$

·	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

$UG_2$

·	1	6
1	1	6
6	6	1

$UG_3$

·	1
1	1

Geg. Multi.tab. v.  $G = \langle \mathbb{Z}_7 \setminus \{0\} = \mathbb{Z}_7^*, \cdot \bmod 7 \rangle$  u.  $UG_1 = \langle \{1, 2, 4\}, \cdot \bmod 7 \rangle$ ,  $UG_2 = \langle \{1, 6\}, \cdot \bmod 7 \rangle$  &  $UG_3 = \langle \{1\}, \cdot \bmod 7 \rangle$ . Wir besprechen nun einige Fakts der Gruppentheorie:

- Die Anzahl Elemente einer Gruppe ist die Gruppenordnung  $|G| = 6$ .
- Dito für die Untergruppen: **Lösung:**  $|UG_1| = 3$ ;  $|UG_2| = 2$ ;  $|UG_3| = 1$
- Allgemein, für  $p$  eine Primzahl:  $G = \langle \mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*, \cdot \bmod p \rangle \Rightarrow |G| = p-1$
- Allgemein, für  $n \in \mathbb{N}$ :  $G = \langle \mathbb{Z}_n^*, \cdot \bmod n \rangle \Rightarrow |G| = \varphi(n)$
- Welches Element muss immer in einer Untergruppe drin sein?
  - Lösung:** das Neutralelement
- Allgemein: Die Ord. der UG muss die Gruppenord. teilen, also: Welche Ordnungen können die UG von  $G = \langle \mathbb{Z}_7^*, \cdot \bmod 7 \rangle$  haben?
  - Lösung:** 6, 3, 2, 1
- Es gibt also 2 echte UG's ( $UG_1$  &  $UG_2$  und die zwei trivialen UG's ( $UG_3$  &  $G$ ).
- Bemerkung:** Eine UG kann mehrere UG's einer best. Ord. haben, ausg. die triv. UG's.
- Siehe Aufgabe 2:** Bestimmen der inversen Elementen mod 7 anhand der Mult.tab.

bis 1645

# Definition: Ordnung eines Gruppenelementes

Sei  $G$  eine Gruppe mit der Operation  $*$ ,  $a$  ein Element der Gruppe und  $n$  eine natürliche Zahl, dann ist  $n*a$  ein Element der Gruppe.

- Für additive Gruppen ist  $n*a = a + a + \dots + a$  ( $n$ -mal)
- Für multiplikative Gruppen ist  $n*a = a^n = a \cdot a \cdot a \cdot \dots \cdot a$  ( $n$ -mal)

*Handwritten: 16/55*

## Satz:

Sei  $G$  eine Gruppe mit der Operation  $*$  und  $n$  eine natürliche Zahl, dann ist die Teilmenge  $\{n*a\}$  eine Untergruppe der Gruppe  $G$ .

## Definition:

Sei  $G$  eine Gruppe mit der Operation  $*$  und  $m$  eine natürliche Zahl. Die kleinste natürliche Zahl  $m > 0$  für die gilt  $a^m = e$  heißt Ordnung des Elementes  $a$ , d.h.  $\text{Ord}(a) = m$  in der Gruppe  $G$ .

*Handwritten:  $\{a, a^2, a^3, \dots, a^n\}$*

## Bemerkungen:

- Analog zu vorhin: Die Ordnung eines Elements teilt die Gruppenordnung.
- Es können verschiedene Elemente  $a, b$  die gleiche (Unter-)gruppe erzeugen.
- Das NE  $e$  ist das einzige Element der Ordnung 1, es erzeugt die triviale UG  $\{e\}$ .
- Da  $m*a = e$  ist, folgt dass  $(m-1)*a = a'$  ( $a'$  ist das Inverse von  $a$  bez. der Op.  $*$ ).

## Beispiel: Immer mod 7 rechnen!!

$\{n*5\} = \{5^n\} = \{5, 4, 6, 2, 3, 1\} \rightarrow$  «5» erzeugt  $G$ , resp.  $5^6 \equiv 1 \pmod{7} \rightarrow \text{ord}(5) = 6$ .

$\rightarrow$  Weiter gilt:  $5^{6-1} \equiv 5^5 \equiv 3 \equiv 5^{-1} \pmod{7}$ . Richtig, denn  $5 \cdot 3 \equiv 15 \equiv 1 \pmod{7}$

*Handwritten:  $5^2 \equiv 25 \equiv 4 \pmod{7}$   $\rightarrow$  Anwendung Satz von Euler*

# Beispiel: Die Gruppe $\langle \mathbb{Z}_7 \setminus \{0\} = \mathbb{Z}_7^*, \cdot \bmod 7 \rangle$

Tabelle der Potenzen  $a^k \bmod 7$

aller Elemente in  $\mathbb{Z}_7^* = \mathbb{Z}_7 \setminus \{0\}$

und Visualisierung der Ordnung der Elemente

*Sowohl 2 wie 4 erzeugen die  $U_3$*

*6 erzeugt die  $U_2$*

*basen*

a \ k	1	2	3	4	5	6	ord
7							
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

*Potenzen*

*erzeugen die ganze Gruppe*

Wir besprechen nun weitere Fakts:

- Die Ordnung n eines Elements a ist die kl. Zahl, so dass  $a^n = 1$  ist  $\rightarrow$  cf. Tab.
- Die Ordnung n eines Elements a muss die Gruppenordnung teilen  $\rightarrow$  cf. Tab.
- Welche Ordnungen können die Elemente von  $G = \langle \mathbb{Z}_7^*, \cdot \bmod 7 \rangle$  haben?

• **Lösung:** 1, 2, 3, 6

- Für das inv. Element gilt:  $a^{\text{ord}(a)-1} \equiv a^{-1} \bmod 7$ , z.B. *4 hat die Ordg 3*  
 $4^{3-1} \equiv 4^2 \equiv 16 \equiv 2 \bmod 7$  und  $4^{-1} \bmod 7 = 2$ , da  $2 \cdot 4 \equiv 1 \bmod 7$

• **Aufgabe 7** Berechnen Sie die restlichen Werte.

- Allgemein: Es gibt  $\varphi(\text{Ord}(a))$  Elemente der  $\text{Ord}(a)$ .
  - D.h.  $\text{Ord}(1) = 1 \Rightarrow \varphi(1) = 1$  Elemente der Ordnung 1, nämlich das Element 1.
  - $\text{Ord}(2) = \text{Ord}(4) = 3 \Rightarrow \varphi(3) = 2$  Elemente der Ordnung 3, die El. 2 & 4.
  - $\text{Ord}(3) = \text{Ord}(5) = 6 \Rightarrow \varphi(6) = 2$  El. der Ord. 6, die primitiven El. 3 & 6.
  - $\text{Ord}(6) = 2 \Rightarrow \varphi(2) = 1$  Element der Ordnung 2, nämlich das Element 6.
- In  $\mathbb{Z}_p^*$  hat 1 immer die Ordnung 1 und  $p-1$  immer die Ordnung 2.

*bis 1745*

# Beispiel: Die Gruppe $\langle \mathbb{Z}_7 \setminus \{0\} = \mathbb{Z}_7^*, \cdot \bmod 7 \rangle$

Tabelle der Potenzen  $a^k \bmod 7$

aller Elemente in  $\mathbb{Z}_7^* = \mathbb{Z}_7 \setminus \{0\}$

und Visualisierung der Ordnung der Elemente

a \ k	1	2	3	4	5	6	ord
7							
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

Wir besprechen nun weitere Fakts, Fortsetzung:

- Die Summe aller  $\varphi(\text{Ord}(a))$  muss  $\text{Gruppenord}$  ergeben:  $1 + 2 + 2 + 1 = 6$
- Die Elemente 3 und 5 sind erzeugend (synonym: primitiv). Die Potenzen erzeugen die Gruppe.
- Die restlichen Elemente erzeugen je die Untergruppen.
- Somit kann es keine weiteren Untergruppen mehr geben.

Es gibt folg. Ordnungen der Elemente:

$1 \rightarrow \varphi(1) = 1$   
 $2 \rightarrow \varphi(2) = 1$   
 $3 \rightarrow \varphi(3) = 2$   
 $6 \rightarrow \varphi(6) = 2$

$1 + 1 + 2 + 2 = 6$   
 $= \text{Ord der Gruppe}$

# Beispiel: Gruppe $\langle \mathbb{Z}_{19} \setminus \{0\} = \mathbb{Z}_{19}^*, \cdot \bmod 19 \rangle$

Tabelle der Potenzen  $a^k \bmod 19$  aller Elemente in  $\mathbb{Z}_{19}^* = \mathbb{Z}_{19} \setminus \{0\}$  und Visualisierung der Ordnung der Elemente

a \ k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	ord
19																			
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	18
3	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1	18
4	4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1	9
5	5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1	9
6	6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1	9
7	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	3
8	8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1	6
9	9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1	9
10	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1	18
11	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	3
12	12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1	6
13	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1	18
14	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1	18
15	15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1	18
16	16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1	9
17	17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1	9
18	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	2

17 4 3 0

→  $\varphi(1) =$   
→  $\varphi(18)$

→  $\varphi(9)$

→  $\varphi(13)$   
→  $\varphi(6)$

→  $\varphi(2)$  18

# Beispiel: Gruppe $\langle \mathbb{Z}_{19} \setminus \{0\} = \mathbb{Z}_{19}^*, \cdot \bmod 19 \rangle$

- Die Anzahl Elemente einer Gruppe ist die Gruppenordnung  $|G| = 18$ .
- Allgemein: Die Ord. der UG und die Ordnung der Elemente muss die Gruppenord. teilen.
- Welche Ordnungen können die UG und die Elemente von  $G = \langle \mathbb{Z}_{19}^*, \cdot \bmod 19 \rangle$  haben?
  - **Lösung:** 1; 2; 3; 6; 9; 18.
- Für das inv. Element gilt:  $a^{\text{ord}(a)-1} \equiv a^{-1} \bmod 19$ , z.B.  $2^{18-1} \equiv 2^{17} \equiv \dots \equiv 10 \equiv 2^{-1} \bmod 19$ , denn  $2 \cdot 10 \equiv 20 \equiv 1 \bmod 19$ .
  - **Aufgabe 8** Berechnen Sie die restlichen Werte.
- Allgemein: Es gibt  $\varphi(\text{Ord}(a))$  Elemente der  $\text{Ord}(a)$ .
  - $\text{Ord}(1) = 1 \Rightarrow \varphi(1) = 1$  Elemente der Ordnung 1, nämlich das Element 1.
  - $\text{Ord}(2) = \dots = 18 \Rightarrow \varphi(18) = 6$  El. der Ord. 18, die El. 2, 3, 10, 13, 14 & 15.
  - $\text{Ord}(4) = \dots = 9 \Rightarrow \varphi(9) = 6$  El. der Ord. 9, die El. 4, 5, 6, 9, 16 & 17.
  - $\text{Ord}(7) = \text{Ord}(11) = 3 \Rightarrow \varphi(3) = 2$  El. der Ord. 3, die El. 7 & 11.
  - $\text{Ord}(8) = \text{Ord}(12) = 6 \Rightarrow \varphi(6) = 2$  El. der Ord. 6, die El. 8 & 12.
  - $\text{Ord}(18) = 2 \Rightarrow \varphi(2) = 1$  El. der Ord. 18, das El. 18.
- Die Summe aller  $\varphi(\text{Ord}(a))$  muss n ergeben:  $1 + 6 + 6 + 2 + 2 + 1 = 18$
- Die El. 2, 3, 10, 13, 14 & 15 sind erzeugend = primitiv, die Potenzen erzeugen die Grup.
- Die rest. El. erzeugen je die UG's:  $\{1\}$ ,  $\{1; 18\}$ ,  $\{1; 4; 5; 6; 7; 9; 11; 16; 17\}$ ,  $\{1; 7; 11\}$ ,  $\{1; 7; 8; 11; 12; 18\}$ . Es gilt sogar, dass  $\{1; 7; 11\}$  eine UG von  $\{1; 4; 5; 6; 7; 9; 11; 16; 17\}$  ist.

# Aufgabe 9 Die Gruppe $\langle \mathbb{Z}_{11} \setminus \{0\}, \cdot \bmod 11 \rangle$

·	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9				
8	8	5	2	10	7	4				
9	9	7	5	3	1	10				
10	10	9	8	7	6	5				

- 1) Füllen Sie die Tabelle fertig aus.
- 2) Bestimmen die Ordnung der Gruppe und die möglichen Ordnungen der Untergruppen.
- 3) Geben Sie die Anzahl der erzeugenden Elemente der Gruppe an.
- 4) Geben Sie die Anzahl der erzeugenden Elemente der Untergruppen an.
- 5) Addieren Sie die Werte aus 4) zusammen. Was stellen Sie fest?
- 6) Bestimmen Sie anhand der Tabelle das jeweilige inverse Element mod 11.

Tabelle der Potenzen  $a^k \bmod 11$  aller Elemente in  $\mathbb{Z}_{11}^* = \mathbb{Z}_{11} \setminus \{0\}$  und Visualisierung der Ordnung der Elemente

a \ k	1	2	3	4	5	6	7	8	9	10	ord
11											
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1	10
3	3	9	5	4	1	3	9	5	4	1	5
4	4	5	9	3	1	4	5	9	3	1	5
5	5	3	4	9	1	5	3	4	9	1	5
6	6	3	7	9	10	5	8	4	2	1	10
7	7	5	2	3	10	4	6	9	8	1	10
8	8	9	6	4	10	3	2	5	7	1	10
9	9	4	3	5	1	9	3	3	5	1	5
10	10	1	10	1	10	1	10	1	10	1	2

a \ k	1	2	3	4	5	6	7	8	9	10	ord
11											
1	1										1
2	2	4	8	5	10	9	7	3	6	1	10
3	3	9	5	4	1						5
4	4	5	9	3	1						5
5	5	3	4	9	1						5
6	6	3	7	9	10	5	8	4	2	1	10
7	7	5	2	3	10	4	6	9	8	1	10
8	8	9	6	4	10	3	2	5	7	1	10
9	9	4	3	5	1						5
10	10	1									2



## Aufgabe 9, Fortsetzung: $\langle \mathbb{Z}_{11} \setminus \{0\}, \cdot \bmod 11 \rangle$

- 7) Bestimmen Sie anhand der Tabellen in der vorangegangenen Folie die Ordnung von jedem Element.
- 8) Welche Untergruppen können Sie in den Tabellen feststellen.
- 9) Welche Elemente sind erzeugende Elemente der Gruppe, welche Elemente erzeugen Untergruppen?
- 10) Stimmen die Anzahlen mit denjenigen aus den Aufgabe 3) & 4) überein?
- 11) Anhand der Multiplikationstabelle haben Sie schon das jeweilige inverse Element mod 11 bestimmt.  
Verifizieren Sie das nun anhand der Formel  $a^{\text{ord}(a)-1} \equiv a^{-1} \bmod 11$ .

## Aufgabe 10

Machen Sie nun analoge Überlegungen zu  $\langle \mathbb{Z}_{17} \setminus \{0\}, \cdot \bmod 17 \rangle$ , siehe Tabelle rechts.

**Tipp:** Arbeiten Sie auch mit Farben.

Dito zu  $\langle \mathbb{Z}_{23} \setminus \{0\}, \cdot \bmod 23 \rangle$ , deren Tabelle im JS Skript, Kap. 26 enthalten ist.

a \ k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	ord
17																	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
2	2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1	
3	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	
4	4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1	
5	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1	
6	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1	
7	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1	
8	8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1	
9	9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1	
10	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1	
11	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1	
12	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1	
13	13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1	
14	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1	
15	15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1	
16	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	

# Einleitung: Zyklische Gruppen

Wir haben bisher im Kap. 6 die folg. Sachen erarbeitet:

- Definition der Begriffe
  - Gruppe
  - Untergruppe
  - Ordnung der Gruppe
  - Ordnung einer Untergruppe
  - Ordnung eines Elements
- Beispiele betrachtet
  - Div. Gruppen kurz betrachtet
  - $\langle \mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*, \cdot \bmod p \rangle$  für  $p = 7; 11; 19$  im Detail und für  $p = 17$  &  $23$  als Aufgaben
  - Ordnung der Gruppe, einer UG, eines Elementes.
- Eigenschaften betrachtet
  - Ordnung der Untergruppe muss Gruppenordnung teilen.
  - Ordnung des Elements muss Gruppenordnung teilen.
  - $\{e\}$  und  $G$  sind die trivialen Untergruppen von  $G$
  - Das Neutralelement  $e$  muss in jeder Untergruppe drin sein.
  - Anzahl erzeugende Elemente der Gruppe und der Untergruppen (\*)
  - (\*) Wichtig: Diese Eigenschaft gilt nur für zyklische Gruppen (Def. nun nachfolgend).

# Definition & erste Beispiele: Zyklische Gruppen

## Definition:

Eine Gruppe  $G$  mit der Operation  $*$  heisst **zyklisch**, wenn es ein  $x \in G$  gibt mit  $G = \{x^k \mid k \in \mathbb{Z}\}$ ; d.h. das Element erzeugt die Gruppe.

Ein solches erzeugendes Element heisst **erzeugend** oder synonym **primitiv**.

## Bemerkungen und erste Beispiele:

- M.a.W. wird eine Gruppe  $G$  von einem Element erzeugt, dann nennt man diese Gruppe **zyklisch**.
- Oder nochmals anders gesagt: Gibt es ein Element, dessen Ordnung gleich der Gruppenordnung ist, dann ist die Gruppe zyklisch.
- Wenn die Operation  $*$  = +, also die Addition ist, so kann jedes Element der Gruppe mit  $x \cdot k$  dargestellt werden; d.h.  $x$  erzeugt die Gruppe.
- Wenn die Operation  $*$  =  $\cdot$ , also die Multiplikation, so kann jedes Element der Gruppe mit  $x^k$  dargestellt werden; d.h.  $x$  erzeugt die Gruppe.
- $\langle \mathbb{Z}, + \rangle$  ist eine unendliche zyklische Gruppe. Das Element 1 erzeugt diese additive Gruppe.
- Für  $n \in \mathbb{N}$  ist  $\langle \mathbb{Z}_n, + \rangle$  eine zyklische Gruppe der Ordnung  $n$ . Z.B. das Element 1 erzeugt diese additive Gruppe.
- $\langle \mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*, \cdot \bmod p \rangle$  ist für  $p$  = Primzahl eine zyklische multiplikative Gruppe der Ordnung  $p - 1$ . Sie hat  $\varphi(p - 1)$  erzeugende Elemente.

# Beispiele zu zykl. & n. zykl. multip. Gruppen

## Bemerkung:

Der Normalfall ist, dass eine Gruppe nicht zyklisch ist. Aber die Basis für unsere Anwendungen (DH & ECC) sind zyklische Gruppen.

Multiplikationstabelle von  $\mathbb{Z}_8^* = \{1; 3; 5; 7\}$  und Tabelle der Potenzen  $a^k \bmod 8$  und Visualisierung der Ordnung der Elemente. Die Gruppe hat Ord. 4

→

·	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Weil  $\mathbb{Z}_8^* = \{1; 3; 5; 7\}$  kein Element der Ordnung 4 hat, ist sie nicht zyklisch.

*baso*

*Potenz*

a \ k	1	2	3	4	ord
8					
1	1	1	1	1	1
3	3	1	3	1	2
5	5	1	5	1	2
7	7	1	7	1	2

Multiplikationstabelle von  $\mathbb{Z}_9^* = \{1; 2; 4; 5; 7; 8\}$  und Tabelle der Potenzen  $a^k \bmod 9$  und Visualisierung der Ord. der Ele. D. Gruppe hat Ord. 6 & ist zyklisch.

→

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Weil  $\mathbb{Z}_9^* = \{1; 2; 4; 5; 7; 8\}$  zyklisch ist, gelten nun wieder die Gesetze bez. Anzahl erzeug. Elemente usw.

a \ k	1	2	3	4	5	6	ord
9							
1	1	1	1	1	1	1	1
2	2	4	8	7	5	1	6
4	4	7	1	4	7	1	3
5	5	7	8	4	2	1	6
7	7	4	1	7	4	1	3
8	8	1	8	1	8	1	2

# Beispiele zu zykl. add. Gruppen

$(\mathbb{Z}_8, +)$  Tabelle der Produkte  $a \cdot k \bmod 8$  und Visualisierung der Ordnung der Elemente. Die Gruppe hat Ord. 8 (also nicht von Primordnung) & ist zyklisch, es gelten nun wieder die Gesetze bez. Anzahl erzeug. Elemente usw.

a \ k	1	2	3	4	5	6	7	8	ord
8									
0	0	0	0	0	0	0	0	0	1
1	1	2	3	4	5	6	7	0	8
2	2	4	6	0	2	4	6	0	4
3	3	6	1	4	7	2	5	0	8
4	4	0	4	0	4	0	4	0	2
5	5	2	7	4	1	6	3	0	8
6	6	4	2	0	6	4	2	0	4
7	7	6	5	4	3	2	1	0	8

Sie hat neben den trivialen UG  $\{0\}$  und  $G$  eine UG der Ord. 2,  $\{0; 4\}$  und eine UG der Ord. 4,  $\{0; 2; 4; 6\}$ .

$(\mathbb{Z}_7, +)$  *Ordnung 7 ist eine Primzahl* Tabelle der Produkte  $a \cdot k \bmod 7$  und Visualisierung der Ordnung der Elemente. Die Gruppe hat Ord 7 & ist zyklisch, es gelten nun wieder die Gesetze bez. Anzahl erzeug. Elemente usw.

a \ k	1	2	3	4	5	6	7	ord
7								
0	0	0	0	0	0	0	0	1
1	1	2	3	4	5	6	0	7
2	2	4	6	1	3	5	0	7
3	3	6	2	5	1	4	0	7
4	4	1	5	2	6	3	0	7
5	5	3	1	6	4	2	0	7
6	6	5	4	3	2	1	0	7

Wegen der Ordnung 7 ist sie von Primordnung und daher sind alle Elemente ausser 0 erzeugend.

$(\mathbb{Z}_7, +)$  hat keine weiteren UG als die trivialen.

*d.h. alle Elemente ausser 0 erzeugen die Gruppe*

# Eigenschaften: Zyklische Gruppen

**Satz:** Sei  $G$  eine Gruppe der Ordnung  $|G| = p$  eine Primzahl, dann gilt:

- I. Die Gruppe ist zyklisch.
- II. Die Gruppe ist abelsch.
- III. Es gibt bis auf Isomorphie (\*) nur eine solche Gruppe.
- IV. Jedes Element  $a$  der Gruppe (ausser  $a = e = NE$ ) hat die Ordnung  $p$ .
- V. Jedes Element  $a$  der Gruppe (ausser  $a = e = NE$ ) erzeugt die Gruppe  $G$ .
- VI. Die Anzahl der Erzeugenden Elemente ist  $\varphi(p) = p - 1$ .

## **Bemerkungen zu:**

- I. Die Umkehrung gilt nicht: eine zyklische Gruppe muss nicht notwendigerweise von Primordnung sein, siehe z.B.  $(\mathbb{Z}_9^*, \cdot)$  mit Ord. 4 oder  $(\mathbb{Z}_8, +)$  mit Ord. 8.
- II. Die Umkehrung gilt nicht: eine abelsche Gruppe muss nicht notwendigerweise von Primordnung sein, siehe z.B.  $(\mathbb{Z}_9^*, \cdot)$  oder  $(\mathbb{Z}_8, +)$ .
- III. Die Umkehrung gilt nicht: so gibt es bis auf Isomorphie (\*) genau eine Gruppe der Ordnung 15, das ist aber keine Primordnung.
- IV. – VI. Hingegen gelten die Umkehrungen der restlichen 3 Aussagen IV – VI.

(\*) Der Begriff «Isomorphie» kennen Sie aus der Graphentheorie in D-MATH.  
Dort definierten wir diesen Begriff zur «Gleichheit» von Graphen.

# Zyklische Gruppen: Bekanntes Wissen

## Satz:

Sei  $G$  eine zyklische Gruppe der Ordnung  $|G| = n$ ,  $n$  eine natürliche Zahl, dann ist die Anzahl der erzeugenden Elemente  $\varphi(n)$ . Zu jeder Untergruppe der Ordnung  $m$  ( $m$  teilt  $n$ ) gibt es  $\varphi(m)$  Elemente, die diese Untergruppe erzeugt.

## Beispiel, Fortsetzung: Die Gruppe $\langle \mathbb{Z}_7 \setminus \{0\}, \cdot \bmod 7 \rangle$

- Die Gruppe  $\langle \mathbb{Z}_7 \setminus \{0\}, \cdot \bmod 7 \rangle$  hat die Ordnung 6 und ist zyklisch. Sie hat  $\varphi(6) = 2$  erzeugende Elemente, nämlich 3 und 5 (siehe weiter vorne). Die Elemente 3 und 5 sind also primitive Elemente von  $\langle \mathbb{Z}_7 \setminus \{0\}, \cdot \bmod 7 \rangle$ .
- Die Untergruppe  $\{1\}$  hat die Ordnung 1. Sie hat  $\varphi(1) = 1$  erzeugende Elemente, nämlich die 1).
- Die Untergruppe  $\{1; 6\}$  hat die Ordnung 2. Sie hat  $\varphi(2) = 1$  erzeugende Elemente, nämlich die 6).
- Die Untergruppe  $\{1; 2; 4\}$  hat die Ordnung 3. Sie hat  $\varphi(3) = 2$  erzeugende Elemente, nämlich die 2 und 4).
- Die Anzahl aller erzeugenden Elemente der Untergruppen muss die Anzahl der Elemente in  $G$  sein:  $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6 = \text{Ord}(G) = \text{Anzahl Elemente in } G$ .
- Die Gruppe hat keine weiteren Untergruppen.

Analoges gilt für die betrachteten Gruppen  $\langle \mathbb{Z}_p \setminus \{0\}, \cdot \bmod p \rangle$

# Zyklische (Unter-)Gruppen

## Elliptische Kurven:


Bei den Elliptischen Kurven wollen wir gerne mit zyklischen Gruppen arbeiten. Hier haben wir die Möglichkeit eine Gruppe von Primordnung (Ordnung der Gruppe ist eine Primzahl) zu haben.

## Diffie-Hellman:

Ebenso beim DH will man mit zyklischen Gruppen arbeiten. Hier gibt es nicht die Möglichkeit, mit Gruppen von Primordnung zu arbeiten. *p-1 Elemente  
p eine Primzahl, dann p-1  
keine Primzahl*

**Grund:** Die Ord. von  $\langle \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}, \cdot \bmod p \rangle$  beträgt immer  $p - 1$ . Da  $p$  eine Primzahl ist, ist  $p - 1$  eine gerade Zahl, sie kann demnach nicht prim sein.

Deshalb brauchen wir bei diesen Gruppen (grosse) Untergruppen mit Primordnung. Z.B. in  $\langle \mathbb{Z}_{47}^* = \mathbb{Z}_{47} \setminus \{0\}, \cdot \bmod 47 \rangle$  hat es eine Untergruppe der Ordnung 23.



Date	Symmetric	Factoring Modulus	Discrete Logarithm Key	Group	Elliptic Curve	Hash
2020 - 2022	128	2000	250	2000	250	SHA-256 SHA-512/256 SHA-384 SHA-512
2023 - 2026	128	3000	250	3000	250	SHA-256 SHA-512/256 SHA-384 SHA-512

Und jetzt sollten wir auch diese Zahlen verstehen!!



# Basis-Test Präsenz 6

Aussage	Richtig o. falsch?	Begründung
Die asymmetrische Kryptographie basiert auf einer ganz neuen Mathematik.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
In der asymmetrischen Kryptographie muss man i.d.R. mit der Modulo Operation rechnen.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Primzahlen spielen in der asymmetrischen Kryptographie eine grosse Rolle.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$2^{3072}$ ist in etwa eine 924-stellige Zahl.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$3^{-1} \bmod N$ kann immer berechnet werden.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$3^{-1} \bmod 331$ kann mit den meisten Rechner ganz einfach berechnet werden.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$3^{-1} \bmod 331 \equiv 221$ , weil $3 \cdot 221 \equiv 663 \equiv 662 + 1 \equiv 2 \cdot 331 + 1 \equiv 1 \bmod 331$ .	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Die Nullteilerfreiheit gilt nicht nur für reelle Zahlen sondern auch für diskrete.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
„Square and multiply“ ist ein Algorithmus, um sehr schnell multiplizieren zu können.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Grosse natürliche Zahlen können oft auf mehrere Arten als Produkt von Primzahlen dargestellt werden.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\pi(2^{3072}) \approx 3 \cdot 10^{921}$	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	

# Basis-Test Präsenz 6, Fortsetzung

Aussage	Richtig o. falsch?	Begründung
Ca. 1% aller ungeraden Zahlen von $1, \dots, 2^{3072}$ sind Primzahlen.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Der Anteil der Primzahlen von $1, \dots, 10^{921}$ ist in etwa gleich gross wie der Anteil der 921-stelligen Primzahlen in allen 921-stelligen Zahlen.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Es gibt verschiedene Methoden, um Primzahlen zu erzeugen.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Der kleine Satz von Fermat ist ein Spezialfall des Satzes von Euler.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Der Satz von Euler ist ein Spezialfall des kleinen Satzes von Fermat.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(12 \cdot 15) = \varphi(12) \cdot \varphi(15)$	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(180) = \varphi(12 \cdot 15) = \varphi(4 \cdot 9 \cdot 5)$ $= \varphi(4) \cdot \varphi(9) \cdot \varphi(5) = 2 \cdot 6 \cdot 4 = 48$	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(77) = \varphi(7 \cdot 11) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(72) = \varphi(8 \cdot 9) = \varphi(8) \cdot \varphi(9) = \varphi(2^3) \cdot \varphi(3^2) =$ $= (2^3 - 2^2) \cdot (3^2 - 3^1) = 4 \cdot 6 = 24$	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(6^3) = 6^3 - 6^2 = 216 - 36 = 180$	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(3^6) = 3^6 - 3^5 = 729 - 243 = 486$	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	

# Basis-Test Präsenz 6, Fortsetzung

Aussage	Richtig o. falsch?	Begründung
$\varphi(6^3) = \varphi(2^3 \cdot 3^3) = \varphi(2^3) \cdot \varphi(3^3) = (2^3 - 2^2) \cdot (3^3 - 3^2) = 4 \cdot 18 = 72$	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Hat eine Gruppe 29 Elemente, ist sie zyklisch.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Hat eine Gruppe 29 Elemente, dann kann sie Untergruppen der Ordnung 1, ..., 29 haben.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Hat eine Gruppe 30 Elemente, hat sie primitive Elemente.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Wenn eine Gruppe mit 30 Elemente zyklisch ist, dann hat sie $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = 1 \cdot 2 \cdot 4 = 8$ primitive Elemente.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Eine Gruppe mit 30 Elementen kann nur Untergruppen der 1 und 30 haben.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	
Die Ordnung der Elemente einer Gruppe mit 30 Elementen kann jede Zahl 1,..., 30 sein.	<input type="checkbox"/> richtig <input type="checkbox"/> falsch	

# **Kap. 7**

# **LÖSUNGEN**

**Aufgabe 1a)**  $\text{ggT}(125, 192) = \text{ggT}(5^3, 3 \cdot 2^6) = 1 \rightarrow \text{OK}, (125 \cdot 148) \bmod 192 \equiv 68 \neq 1$ ,  
also  $125^{-1} \bmod 192 \neq 148$

**Aufgabe 1b)**  $(125 \cdot 149) \bmod 192 \equiv 1$ , also  $125^{-1} \bmod 192 \equiv 149$

## Aufgabe 2

$2^{-1} \bmod 11 \equiv 6$ , denn  $2 \cdot 6 \bmod 11 \equiv 1$  usw. Es gilt:  $3^{-1} \bmod 11 \equiv 4$ ;  $4^{-1} \bmod 11 \equiv 3$ ;  $5^{-1} \bmod 11 \equiv 9$   
 $6^{-1} \bmod 11 \equiv 2$ ;  $7^{-1} \bmod 11 \equiv 8$ ;  $8^{-1} \bmod 11 \equiv 7$ ;  $9^{-1} \bmod 11 \equiv 5$ ;  $10^{-1} \bmod 11 \equiv 10$ .

## Aufgabe 3

a)  $3^{13} \bmod 8 = 3$

b)  $x^{39} = x^{100111}$  Das gibt dann die folgenden Schritte

- $x \rightarrow x^2$
- $x^2 \rightarrow x^4$
- $x^4 \rightarrow x^8$  und dann  $x^8 \rightarrow x^9$
- $x^9 \rightarrow x^{18}$  und dann  $x^{18} \rightarrow x^{19}$
- $x^{19} \rightarrow x^{38}$  und dann  $x^{38} \rightarrow x^{39}$
- $(39)_{10} = (100111)_2$ , Also:  $2 \rightarrow 4 \rightarrow 8 \rightarrow 9 \rightarrow 18 \rightarrow 19 \rightarrow 38 \rightarrow 39$
- Das ergibt einen Aufwand von  $5 \cdot \text{square} \rightarrow \frac{3}{4} \cdot t$  und  $3 \cdot \text{mult.} \rightarrow t$ ; das ergibt einen Aufwand von 6,75 t

c)  $3^{39} \bmod 7 = 6$  (Die Zwischenresultate sind hier nicht aufgeführt. In einer Prüfung müssten diese natürlich im Detail angegeben werden.)

## Aufgabe 4

a)  $2^{1024} \approx 10^{308}$

b)  $\pi(10^{308}) \approx \frac{10^{308}}{\ln(10^{308})} \approx 1,41 \cdot 10^{305}$

c)  $APZ(x = 10^{308}) \approx \frac{2}{\ln(10^{308})} \approx \frac{2,8}{1000} = 0,28\% = 2,8\text{‰}$

d)  $\pi(10^{308}) - \pi(10^{307}) = \frac{10^{308}}{\ln(10^{308})} - \frac{10^{307}}{\ln(10^{307})} \approx 1,27 \cdot 10^{305}$

#### Aufgabe 4, Fortsetzung

- e)  $APZ(n = 308) \approx \frac{\frac{10^{308}}{\ln(10^{308})} - \frac{10^{307}}{\ln(10^{307})}}{0,45 \cdot 10^{308}} \approx \frac{2,8}{1000} = 0,28\% = 2,8\text{‰}$
- f)  $\frac{2,8}{1000} = \frac{1,4}{500} \approx \frac{1}{355}$ , also ca. jede 355-igste ungerade 308-stellige ungerade Zahl ist eine 308-stellige Primz.

#### Aufgabe 5

- Wegen der Entschlüsselung  $x = d_k(y) \equiv a^{-1} \cdot (y - b) \bmod n$ , gilt für den Parameter a gilt:  $\text{ggT}(a, 2^m) = 1$ .
  - Es gibt  $\varphi(2^m) = 2^m - 2^{m-1}$  Werte, die grundsätzlich infrage kommen.
  - Da aber  $a \neq 1$  gilt, sind es „nur“  $2^m - 2^{m-1} - 1$  mögliche Werte für a.
  - Der Parameter b kann alle Werte von 2 bis  $2^m - 1$  annehmen. Es gibt daher  $2^m - 2$  Möglichkeiten.
  - Somit beträgt der Schlüsselraum:  $(2^m - 2^{m-1} - 1) \cdot (2^m - 2)$  mögliche Werte.
  - **Kontrolle für  $m = 4 \Rightarrow 2^4 = 16$ :**
    - $(2^4 - 2^3 - 1) \cdot (2^4 - 2) = 7 \cdot 14 = 98$
    - a kann die Werte  $\{3; 5; 7; 9; 11; 13; 15\}$  annehmen, d.h. für a gibt es 7 Möglichkeiten.
    - b kann alle 14 Werte von  $[2; \dots; 15]$  annehmen.
- a) Also Schlüsselraumgrösse =  $(2^m - 2^{m-1} - 1) \cdot (2^m - 2)$ , wenn vorausgesetzt wird, dass die Parameter a und b, je weder Null noch Eins sein dürfen und  $n = 2^m$  gilt.
- b) Für  $m = 12$  gibt es dann 8'380'418 mögliche Schlüssel.

#### Aufgabe 6

Für  $a = 22$  &  $n = 27$  gilt:  $\text{ggT}(22, 27) = 1$  und  $\varphi(27) = 18$

$$22^{\varphi(27)} \equiv 22^{18} \equiv 1 \bmod 27$$

Resp.  $22^{\varphi(27)+1} \equiv 22^{19} \equiv 22 \cdot 22^{18} \equiv 22 \cdot 1 \equiv 22 \bmod 27$ , resp.  $22^{\varphi(27)-1} \equiv 22^{17} \equiv 22^{-1} \equiv 16 \bmod 27$ ,  
denn  $22 \cdot 16 \equiv 352 \equiv 1 \bmod 27$

## Aufgabe 7

Für  $a = 1$ , klar, denn  $1^{-1} \bmod 7 \equiv 1$ , denn  $1 \cdot 1 \bmod 7 \equiv 1$  und  $1^{1-1} \equiv 1 \bmod 7$

Für  $a = 2$ ; aus Mult. Tabelle  $2^{-1} \bmod 7 \equiv 4$ , denn  $2 \cdot 4 \bmod 7 \equiv 1$  und  $2^{3-1} \equiv 4 \bmod 7$

Für  $a = 3$ ; aus Mult. Tabelle  $3^{-1} \bmod 7 \equiv 5$ , denn  $3 \cdot 5 \bmod 7 \equiv 1$  und  $3^{6-1} \equiv 5 \bmod 7$

Für  $a = 4$ ; aus Mult. Tabelle  $4^{-1} \bmod 7 \equiv 2$ , denn  $4 \cdot 2 \bmod 7 \equiv 1$  und  $4^{3-1} \equiv 2 \bmod 7$

Für  $a = 5$ ; aus Mult. Tabelle  $5^{-1} \bmod 7 \equiv 3$ , denn  $5 \cdot 3 \bmod 7 \equiv 1$  und  $5^{6-1} \equiv 3 \bmod 7$

Für  $a = 6$ ; aus Mult. Tabelle  $6^{-1} \bmod 7 \equiv 6$ , denn  $6 \cdot 6 \bmod 7 \equiv 1$  und  $6^{2-1} \equiv 6 \bmod 7$

## Aufgabe 8 Keine Musterlösung

## Aufgabe 9

·	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

## Aufgabe 9, Fortsetzung

- 1) Siehe Tabelle in der vorherigen Folie.
- 2) Die Gruppe hat die Ordnung 10, somit kann sie Untergruppen der Ord 1 und 10 (nämlich die trivialen Untergruppen  $\{1\}$  und  $G$  selber) sowie der Ordnung 2 und 5 haben.
- 3) Da  $\text{Ord}(G) = 10$  hat sie  $\varphi(10) = 4$  erzeugende Elemente
- 4) Die UG  $\{1\}$  hat  $\varphi(1) = 1$ . Die UG der Ord 2 hat  $\varphi(2) = 1$ . Die UG der Ord 5 hat  $\varphi(5) = 4$  erzeugende Elemente.
- 5)  $\varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4 = 10 = \text{Ordnung der Gruppe}$ .
- 6)  $2^{-1} \bmod 11 \equiv 6$ , denn  $2 \cdot 6 \bmod 11 \equiv 1$  usw. Es gilt:  $3^{-1} \bmod 11 \equiv 4$ ;  $4^{-1} \bmod 11 \equiv 3$ ;  $5^{-1} \bmod 11 \equiv 9$   
 $6^{-1} \bmod 11 \equiv 2$ ;  $7^{-1} \bmod 11 \equiv 8$ ;  $8^{-1} \bmod 11 \equiv 7$ ;  $9^{-1} \bmod 11 \equiv 5$ ;  $10^{-1} \bmod 11 \equiv 10$ .
- 7)  $\text{Ord}(2) = \text{Ord}(6) = \text{Ord}(7) = \text{Ord}(8) = 10$ ;  $\text{Ord}(3) = \text{Ord}(4) = \text{Ord}(5) = \text{Ord}(9) = 5$ ;  $\text{Ord}(10) = 2$ .
- 8)  $\{1; 3; 4; 5; 9\}$  und  $\{1; 10\}$ .
- 9)  $G$  wird von den Elementen der Ordnung 10, also von 2; 6; 7 & 8 erzeugt. Die UG  $\{1; 3; 4; 5; 9\}$  wird von den Elementen der Ordnung 5, also von 3; 4; 5; 9 erzeugt. Die UG  $\{1; 10\}$  wird vom Element der Ordnung 2, also von 10 erzeugt. Die UG  $\{1\}$  wird vom Element der Ordnung 1, also von 1 erzeugt.
- 10) Ja, denn  $\varphi(1) = 1$ ;  $\varphi(2) = 1$ ;  $\varphi(5) = 4$  &  $\varphi(10) = 4$ .
- 11) Verifikation der Formel  $a^{\text{ord}(a)-1} \equiv a^{-1} \bmod 11$   
Für  $a = 1$ , klar, denn  $1^{-1} \bmod 11 \equiv 1$ , denn  $1 \cdot 1 \bmod 11 \equiv 1$  und  $1^{1-1} \equiv 1 \bmod 11$   
Für  $a = 2$ ; aus Tabelle  $2^{-1} \bmod 11 \equiv 6$ , denn  $2 \cdot 6 \bmod 11 \equiv 1$  und  $2^{10-1} \equiv 6 \bmod 11$   
Für  $a = 3$ ; aus Tabelle  $3^{-1} \bmod 11 \equiv 4$ , denn  $3 \cdot 4 \bmod 11 \equiv 1$  und  $3^{5-1} \equiv 4 \bmod 11$   
Für  $a = 4$ ; aus Tabelle  $4^{-1} \bmod 11 \equiv 3$ , denn  $4 \cdot 3 \bmod 11 \equiv 1$  und  $4^{5-1} \equiv 3 \bmod 11$   
Für  $a = 5$ ; aus Tabelle  $5^{-1} \bmod 11 \equiv 9$ , denn  $5 \cdot 9 \bmod 11 \equiv 1$  und  $5^{5-1} \equiv 9 \bmod 11$   
Für  $a = 6$ ; aus Tabelle  $6^{-1} \bmod 11 \equiv 2$ , denn  $6 \cdot 2 \bmod 11 \equiv 1$  und  $6^{10-1} \equiv 2 \bmod 11$   
Für  $a = 7$ ; aus Tabelle  $7^{-1} \bmod 11 \equiv 8$ , denn  $7 \cdot 8 \bmod 11 \equiv 1$  und  $7^{10-1} \equiv 8 \bmod 11$   
Für  $a = 8$ ; aus Tabelle  $8^{-1} \bmod 11 \equiv 7$ , denn  $8 \cdot 7 \bmod 11 \equiv 1$  und  $8^{10-1} \equiv 7 \bmod 11$   
Für  $a = 9$ ; aus Tabelle  $9^{-1} \bmod 11 \equiv 5$ , denn  $9 \cdot 5 \bmod 11 \equiv 1$  und  $9^{5-1} \equiv 5 \bmod 11$   
Für  $a = 10$ ; aus Tabelle  $10^{-1} \bmod 11 \equiv 10$ , denn  $10 \cdot 10 \bmod 11 \equiv 1$  und  $10^{2-1} \equiv 10 \bmod 11$

## Aufgabe 10 Keine Musterlösungen



# Basis-Test Präsenz 6

Aussage	R. o. f.?	Begründung
Die asymmetrische Kryptographie basiert auf einer ganz neuen Mathematik.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Die grundlegende Mathematik beruht auf Fermat, Euler usw.
In der asymmetrischen Kryptographie muss man i.d.R. mit der Modulo Operation rechnen.	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	
Primzahlen spielen in der asymmetrischen Kryptographie eine grosse Rolle.	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	
$2^{3072}$ ist in etwa eine 924-stellige Zahl.	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	Anz. Dezimalstellen $\approx 3072 \cdot 0,3 \approx 922$ , genauer $2^{3072} \approx 5,8 \cdot 10^{924}$ , d.h. eine 924-stellige Dez.zahl. Die Abschätzung stimmt aber in der Grössenordnung.
$3^{-1} \bmod N$ kann immer berechnet werden.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	$3^{-1} \bmod N$ existiert nur, wenn $\text{ggT}(3, N) = 1$ .
$3^{-1} \bmod 331$ kann mit den meisten Rechner ganz einfach berechnet werden.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Die meisten TR können solche Kehrwerte nicht rechnen.
$3^{-1} \bmod 331 \equiv 221$ , weil $3 \cdot 221 \equiv 663 \equiv 662 + 1 \equiv 2 \cdot 331 + 1 \equiv 1 \bmod 331$ .	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	
Die Nullteilerfreiheit gilt nicht nur für reelle Zahlen sondern auch für diskrete.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Gegenbeispiel: $2 \cdot 4 \bmod 8 \equiv 0$
„Square and multiply“ ist ein Algorithmus, um sehr schnell multiplizieren zu können.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Ist ein Algorithmus, um Potenzwerte rechnen zu können.
Grosse natürliche Zahlen können oft auf mehrere Arten als Produkt von Primzahlen dargestellt werden.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Die Primzahldarstellung ist eindeutig.
$\pi(2^{3072}) \approx 3 \cdot 10^{921}$	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	$\pi(2^{3072}) \approx \frac{2^{3072}}{\ln(2^{3072})} \approx 3 \cdot 10^{921}$

# Basis-Test Präsenz 6, Fortsetzung

Aussage	Richtig o. falsch?	Begründung
Ca. 1% aller ungeraden Zahlen von $1, \dots, 2^{3072}$ sind Primzahlen.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Der Anteil ist ca. 1 Promille. D.h. ca. jede 1000-te Zahl ist eine PZ.
Der Anteil der Primzahlen von $1, \dots, 10^{921}$ ist in etwa gleich gross wie der Anteil der 921-stelligen Primzahlen in allen 921-stelligen Zahlen.	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	Siehe Folien.
Es gibt verschiedene Methoden, um Primzahlen zu erzeugen.	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	Ist aber nicht Prüfungsstoff.
Der kleine Satz von Fermat ist ein Spezialfall des Satzes von Euler.	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	
Der Satz von Euler ist ein Spezialfall des kleinen Satzes von Fermat.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	
$\varphi(12 \cdot 15) = \varphi(12) \cdot \varphi(15)$	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ gilt nur, wenn $\text{ggT}(m, n) = 1$ .
$\varphi(180) = \varphi(12 \cdot 15) = \varphi(4 \cdot 9 \cdot 5)$ $= \varphi(4) \cdot \varphi(9) \cdot \varphi(5) = 2 \cdot 6 \cdot 4 = 48$	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(77) = \varphi(7 \cdot 11) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(72) = \varphi(8 \cdot 9) = \varphi(8) \cdot \varphi(9) = \varphi(2^3) \cdot \varphi(3^2) =$ $= (2^3 - 2^2) \cdot (3^2 - 3^1) = 4 \cdot 6 = 24$	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	
$\varphi(6^3) = 6^3 - 6^2 = 216 - 36 = 180$	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	$\varphi(p^k) = p^k - p^{k-1}$ gilt nur, wenn p eine Primzahl ist.
$\varphi(3^6) = 3^6 - 3^5 = 729 - 243 = 486$	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	

# Basis-Test Präsenz 6, Fortsetzung

Aussage	Richtig o. falsch?	Begründung
$\varphi(6^3) = \varphi(2^3 \cdot 3^3) = \varphi(2^3) \cdot \varphi(3^3) = (2^3 - 2^2) \cdot (3^3 - 3^2) = 4 \cdot 18 = 72$	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	
Hat eine Gruppe 29 Elemente, ist sie zyklisch.	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	Eine Gruppe von Primordnung ist zyklisch (Umkehrung gilt nicht).
Hat eine Gruppe 29 Elemente, dann kann sie Untergruppen der Ordnung 1, ..., 29 haben.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Sie hat nur die trivialen Untergruppen; also UG der Ord 1 = {e} und der Ord 29 = Gruppe selber.
Hat eine Gruppe 30 Elemente, hat sie primitive Elemente.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Ist eine Gruppenordnung nicht prim, so kann sie zyklisch sein (also primitive Elemente haben), muss aber nicht.
Wenn eine Gruppe mit 30 Elemente zyklisch ist, dann hat sie $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = 1 \cdot 2 \cdot 4 = 8$ primitive Elemente.	<input checked="" type="checkbox"/> richtig <input type="checkbox"/> falsch	Wenn eine Gruppe der Ord n (egal, ob n prim oder nicht prim) zyklisch ist, so hat sie $\varphi(n)$ primitive Elemente.
Eine Gruppe mit 30 Elementen kann nur Untergruppen der 1 und 30 haben.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Neben den trivialen UG kann jeder andere Teiler von 30 (also 2, 3, 5, 6, 10, 15) also Ordnung einer Untergruppe vorkommen.
Die Ordnung der Elemente einer Gruppe mit 30 Elementen kann jede Zahl 1,..., 30 sein.	<input type="checkbox"/> richtig <input checked="" type="checkbox"/> falsch	Die Ordnung eines Elements muss die Gruppenordnung teilen.

# ***Danksagung***

- Einige Folien in Kap. 2 – 5 entstammen ursprünglich aus der Vorlesung „Sichere Netzwerkkommunikation“ von Prof. Dr. A. Steffen, Hochschule Rapperswil. An dieser Stelle ein recht herzliches Danke schön an meinen Kollegen Andreas Steffen.