Lehrstückunterricht

Primzahlen:

Von der Steinzeit in die Moderne

Philipp Spindler (KS Alpenquai Luzern)

TMU Wettingen 2017

Lehrkunstdidaktik

J. Wiechmann, S. Wildhirt,
„Zwölf Unterrichtsmethoden“
eine der zwölf gängigsten und wichtigsten Unterrichtsmethoden

H. Meyer, R. Demuth, „Unterricht weiterentwickeln und beurteilen“
eine von neun Allgemeindidaktiken

Lehrkunstdidaktik-Reihe im hep-Verlag

Martin Wagenschein (1896-1988)

Vater der Lehrkunstdidaktik
Methodentrias genetisch – sokratisch - exemplarisch

Wolfgang Klafki

Theorie der **kategorialen Bildung** (1959)
an einem Wagenschein-Exempel entwickelt

Christoph Berg / Theodor Schulze

Erprobung von Unterrichtsexempeln Wagenscheins

Hinzufügung von Eigenkompositionen im Sinne von Wagenschein / Klafki (1995)

Lehrstücke

Einheiten von 10 – 25 Lektionen

Exemplarisch:
Gewonnene Einsichten sowie Verfahren können auf analoge Probleme / Phänomene übertragen werden.

Genetisch:
Kein Zwang treibt an, nur das Problem.

Dramat(urg)isch:
Lernende ringen mit dem Lerngegenstand, Gegenstand ringt mit den Lernenden.

Lehrstücke in Mathematik

Euklids Primzahlenbeweis
Beweisen mit Euklid (Sechsstern)
Dreiecksquadrate (Pythagoras)
Platonische Körper
Kreiszahl Pi
Wurzel 2 (Reelle Zahlen)
Vom Würfel zur Kugel
Ähnlichkeit und Strahlensätze
Landvermessen mit Dufour (Trigonometrie)
Logarithmen mit Bürgi
Kegelschnitte
Tartaglia und die kubische Gleichung
Achilles und die Schildkröte
Pascals Wahrscheinlichkeitsrechnung

Schweizer Gymnasien mit Lehrkunst

Trogen
Bern Neufeld
Basel St. Leonhard
Luzern Alpenquai

Optimierung des Lehrstücks "Das Nichtabbrechen der Primzahlfolge"

Gerwig 2013 Basel 12 Lektionen	**Renyi** Sokratischer Dialog **Opałka** 1965/1-∞ ■■	**Sieb des Eratosthenes** ■■■■	**Primzahlbeweis** $2 \cdot 3 \cdot 5 \cdot \ldots \cdot n + 1$ ■■	**Verschrift-lichung des Beweises** ■	**Euklids Beweis** ■	**Geschichte der Primzahlen, RSA** ■■
Brüngger 2005 Bern-Neufeld 12 Lektionen	**Zahlenstrahl** ▮	**Sieb des Eratosthenes,** Primfaktorzerlegung ■■■■▮	**Primzahlbeweis** $2 \cdot 3 \cdot 5 \cdot \ldots \cdot n + 1$ ■■■	**Verschrift-lichung des Beweises** ■	**Euklids Beweis** ■	**Knobel-aufgaben** ■■
Werner 1995 Marburg 10 Lektionen	**Vorbereitung** Teilbarkeit, Primfaktorzerlegung, kgV, ggT ■■■■	**Schülerideen** ■■	**Sieb des Eratosthenes,** Teilermengen ■	**Primzahlbeweis** $2 \cdot 3 \cdot 5 \cdot \ldots \cdot n + 1$ ■■	**Verschrift-lichung des Beweises** ■	
Wagenschein 1949 Golderen 5 Lektionen	**Einleitung** ? ▮	**Schülerideen** $2n \pm 1$ $6n \pm 1$ ■■	**Primzahlbeweis** $2 \cdot 3 \cdot 5 \cdot \ldots \cdot n + 1$ ■	**Verschrift-lichung des Beweises** ■	**Euklids Beweis** ■	
Euklid 300 v. Chr.			**Primzahlbeweis** $2 \cdot 3 \cdot 5 \cdot \ldots \cdot n + 1$			

1 ■ ≙ 1 Lektion

Ouvertüre:
Ein Knochen mit seltsamen Kerben

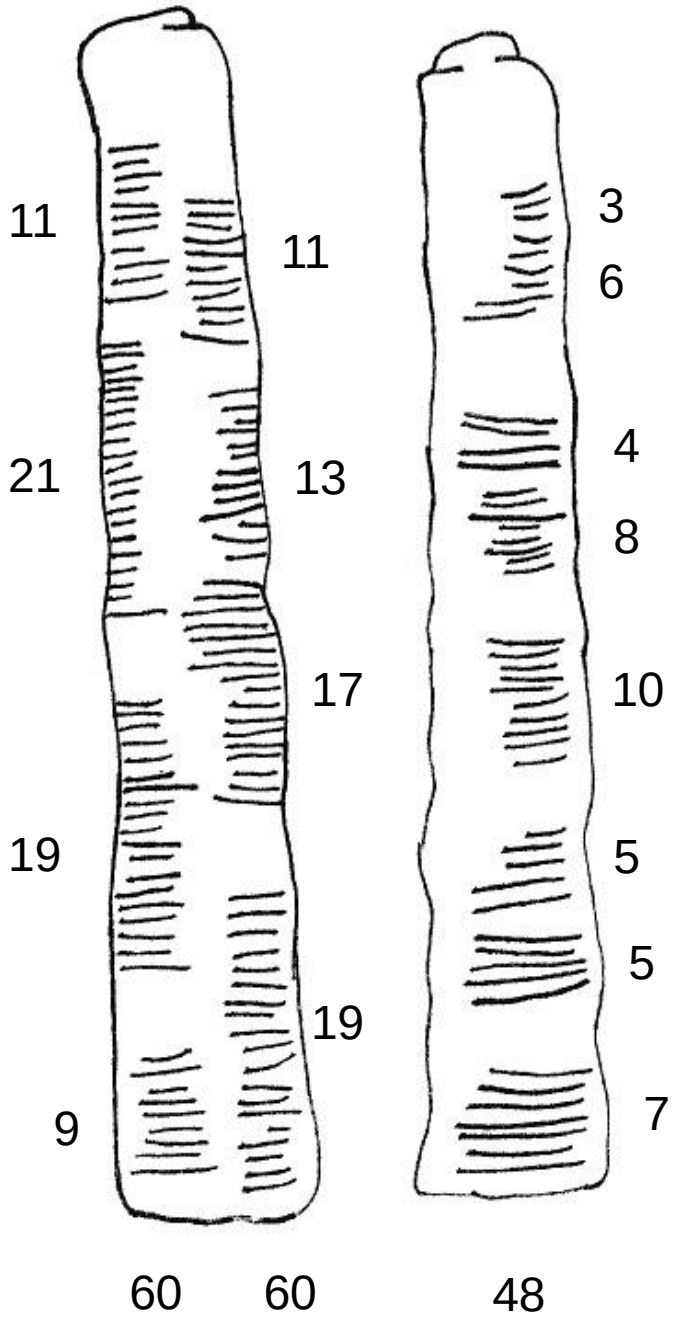
Ishango-Knochen

gefunden um 1950 in Belgisch-Kongo

20000-25000 Jahre alt, C14 schwierig

Pavian (?)

Quarz am Ende: Gravurwerkzeug in einer Kultur ohne Schrift?


11
21
19
9
11
13
17
19
3
6
4
8
10
5
5
7
60
60
48

1. Akt:
Ein Sieb, das Primzahlen herausfischt

Kurze Diskussion

Begegnung mit Primzahlen?

- ggT, kgV
- Bruchrechnen
- Bausteine der natürlichen Zahlen

Wie viele Kerben sind nötig, wenn alle Primzahlen bis 100 auf dem Knochen vermerkt werden?

1	31	61	91	121	151	181
2	32	62	92	122	152	182
3	33	63	93	123	153	183
4	34	64	94	124	154	184
5	35	65	95	125	155	185
6	36	66	96	126	156	186
7	37	67	97	127	157	187
8	38	68	98	128	158	188
9	39	69	99	129	159	189
10	40	70	100	130	160	190
11	41	71	101	131	161	191
12	42	72	102	132	162	192
13	43	73	103	133	163	193
14	44	74	104	134	164	194
15	45	75	105	135	165	195
16	46	76	106	136	166	196
17	47	77	107	137	167	197
18	48	78	108	138	168	198
19	49	79	109	139	169	199
20	50	80	110	140	170	200
21	51	81	111	141	171	201
22	52	82	112	142	172	202
23	53	83	113	143	173	203
24	54	84	114	144	174	204
25	55	85	115	145	175	205
26	56	86	116	146	176	206
27	57	87	117	147	177	207
28	58	88	118	148	178	208
29	59	89	119	149	179	209
30	60	90	120	150	180	210

1	31	61	91	121	151	181
2	32	62	92	122	152	182
3	33	63	93	123	153	183
4	34	64	94	124	154	184
5	35	65	95	125	155	185
6	36	66	96	126	156	186
7	37	67	97	127	157	187
8	38	68	98	128	158	188
9	39	69	99	129	159	189
10	40	70	100	130	160	190
11	41	71	101	131	161	191
12	42	72	102	132	162	192
13	43	73	103	133	163	193
14	44	74	104	134	164	194
15	45	75	105	135	165	195
16	46	76	106	136	166	196
17	47	77	107	137	167	197
18	48	78	108	138	168	198
19	49	79	109	139	169	199
20	50	80	110	140	170	200
21	51	81	111	141	171	201
22	52	82	112	142	172	202
23	53	83	113	143	173	203
24	54	84	114	144	174	204
25	55	85	115	145	175	205
26	56	86	116	146	176	206
27	57	87	117	147	177	207
28	58	88	118	148	178	208
29	59	89	119	149	179	209
30	60	90	120	150	180	210

Suche nach allen Primzahlen von 1 bis 1680

Erkenntnisse:

- alle geraden Zahlen streichen
- alle 5er-Zahlen streichen
- alle 3er-Zahlen streichen
- alle Vielfachen von Primzahlen streichen, aufsteigend
- Primzahlen sind die Zahlen, die nicht gestrichen werden
- Abbruchbedingung: Erreichen von $\sqrt{a}$, a : höchste Zahl in Liste


1-210
211-420
421-630
631-840
841-1050
1051-1260
46 Z
35 Z
33 Z
32 Z
30 Z
29 Z

Sieb des Eratosthenes

Eratosthenes von Kyrene

(ca. 276-194 v.Chr.)

Leiter der Bibliothek von Alexandria

Bestimmte den Erdumfang

Sterben die Primzahlen aus?

2. Akt:
Eine Tüte voller Primzahlen

Herr Prim

Hat alle Primzahlen in einer Tüte und will sie der Klasse verkaufen.

Steigt die Klasse darauf ein?

Welche Strategie?

Zeigen, dass Herr Prim alle Primzahlen hat?

Zeigen, dass Herr Prim noch Primzahlen fehlen?

Gedankenspiel:

Angenommen, Herr Prim hat die Primzahlen

$$p_1, p_2, \ldots, p_k$$

in seiner Tüte. Kann man ihm nachweisen, dass er nicht alle Primzahlen besitzt?

Gibt es eine Zahl, die nicht durch diese Primzahlen teilbar ist?

Vorschlag Nick:

Primzahlen in Tüte addieren

Test:

$$2+3=5$$
$$2+3+5=10$$

Vorschlag Maline:

Primzahlen in Tüte multiplizieren plus 1

Vorschlag Kristina:

Primzahlen in Tüte multiplizieren minus 1

Test:

$2 \cdot 3 + 1 = 7$ prim

$2 \cdot 3 - 1 = 5$ prim

$2 \cdot 3 \cdot 5 + 1 = 31$ prim

$2 \cdot 3 \cdot 5 - 1 = 29$ prim

$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ prim

$2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209$ nicht prim! $209 = 11 \cdot 19$

209 ist keine Primzahl, aber 11 und 19 sind Primzahlen, die Herr Prim nicht in der Tüte hat!

Zweifel an Kristinas Vorschlag bleiben bestehen.
Kontrolle des Vorschlags von Maline:

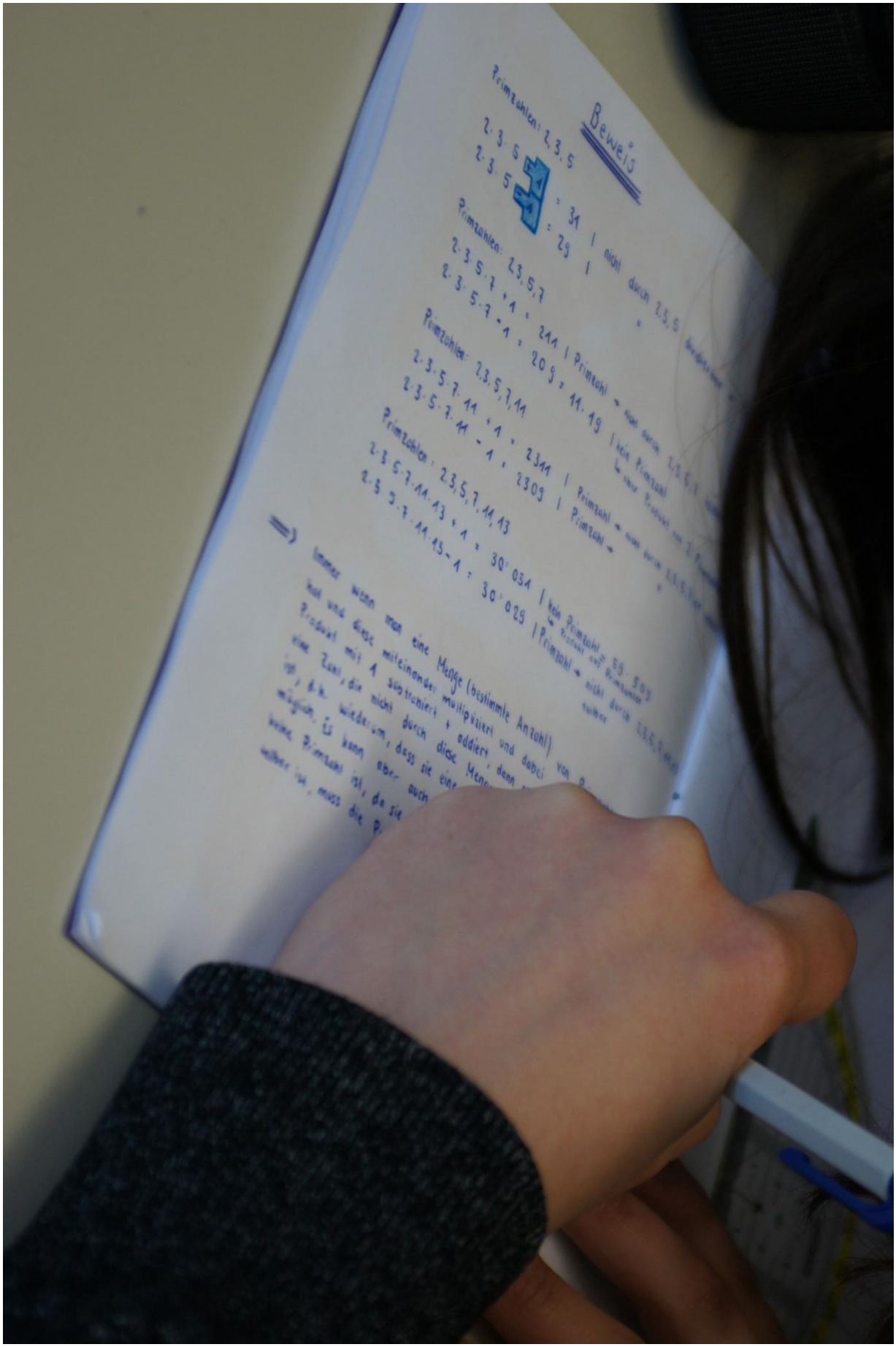
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ prim

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 - 1 = 2309$ prim

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ neue Primzahlen!

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 - 1 = 30029$ prim

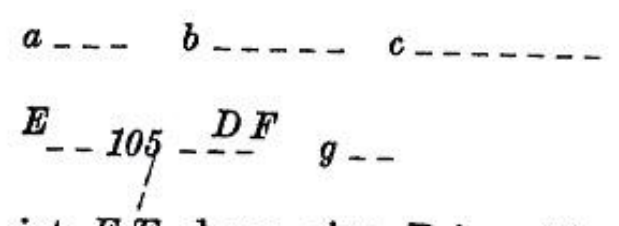
Das Produkt der Primzahlen in der Tüte von Herrn Prim plus oder minus 1 liefert
entweder eine neue Primzahl oder
ist das Produkt von Primzahlen, die noch nicht in der Tüte sind.
In beiden Fällen werden neue Primzahlen gefunden!


Beweis
Primzahlen: 2,3,5
2·3·5 + 1 = 31 | nicht durch 2,3,5
2·3·5 − 1 = 29 |
Primzahlen: 2,3,5,7
2·3·5·7 + 1 = 211 | Primzahl
2·3·5·7 − 1 = 209 = 11·19 | kein Primzahl
Primzahlen: 2,3,5,7,11
2·3·5·7·11 + 1 = 2311 | Primzahl
2·3·5·7·11 − 1 = 2309 | Primzahl
Primzahlen: 2,3,5,7,11,13
2·3·5·7·11·13 + 1 = 30 031 | kein Primzahl = 59·509
2·3·5·7·11·13 − 1 = 30 029 | Primzahl

§ 20 (L. 18).

Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen.

Die vorgelegten Primzahlen seien a, b, c. Ich behaupte, daß es mehr Primzahlen gibt als a, b, c.



Man bilde die kleinste von a, b, c gemessene Zahl (VII, 36); sie sei DE, und man füge zu DE die Einheit DF hinzu. Entweder ist EF dann eine Primzahl, oder nicht. Zunächst sei es eine Primzahl. Dann hat man mehr Primzahlen als a, b, c gefunden, nämlich a, b, c, EF.

Zweitens sei EF keine Primzahl. Dann muß es von irgendeiner Primzahl gemessen werden (VII, 31); es werde von der Primzahl g gemessen. Ich behaupte, daß g mit keiner der Zahlen a, b, c zusammenfällt. Wenn möglich tue es dies nämlich. a, b, c messen nun DE; auch g müßte dann DE messen. Es mißt aber auch EF. g müßte also auch den Rest, die Einheit DF messen, während es eine Zahl ist; dies wäre Unsinn. Also fällt g mit keiner der Zahlen a, b, c zusammen; und es ist Primzahl nach Voraussetzung. Man hat also mehr Primzahlen als die vorgelegte Anzahl a, b, c gefunden, nämlich a, b, c, g — q. e. d.

Euklid, „Die Elemente“, Buch IX, Propostion 20

3. Akt:
Rätsel über Rätsel

(1) Wie viele Primzahlzwillinge gibt es?

(2) Wie viele Primzahldrillinge gibt es?

(3) Gibt es Primzahllücken mit beliebiger Länge?

(4) Ist $x^2 + x + 41$ mit $x \in \mathbb{N}$ immer eine Primzahl? (Euler)

(5) Ist eine gerade natürliche Zahl grösser als 4 immer als Summe zweier Primzahlen darstellbar? (Goldbach)

4. Akt:
Wie Uhren rechnen

Vortrag von Frank Nelson Cole, 1903:

$$2^{67}-1=147573952589676412927$$

$$=193707721\cdot 761838257287$$

Zerlege:

$$50357=37\cdot 1361$$
$$159251=163\cdot 977$$
$$532891=727\cdot 733$$

Berechne: $a^b \bmod b$

a\b	3	4	5	6	7	8	9	10	11	12	13
2	2	0	2	4	2	0	8	4	2	4	2
3		1	3	3	3	1	0	9	3	9	3
4			4	4	4	0	1	6	4	4	4
5				1	5	1	8	5	5	1	5
6					6	0	0	6	6	0	6
7						1	1	9	7	1	7
8							8	4	8	4	8
9								1	9	9	9
10									10	4	10
11										1	11
12											12

Kleiner Satz von Fermat:

$a^p \equiv a \bmod p$ falls p Primzahl und a kein

$a^{p-1} \equiv 1 \bmod p$ Vielfaches von p

Verallgemeinerung von Euler:

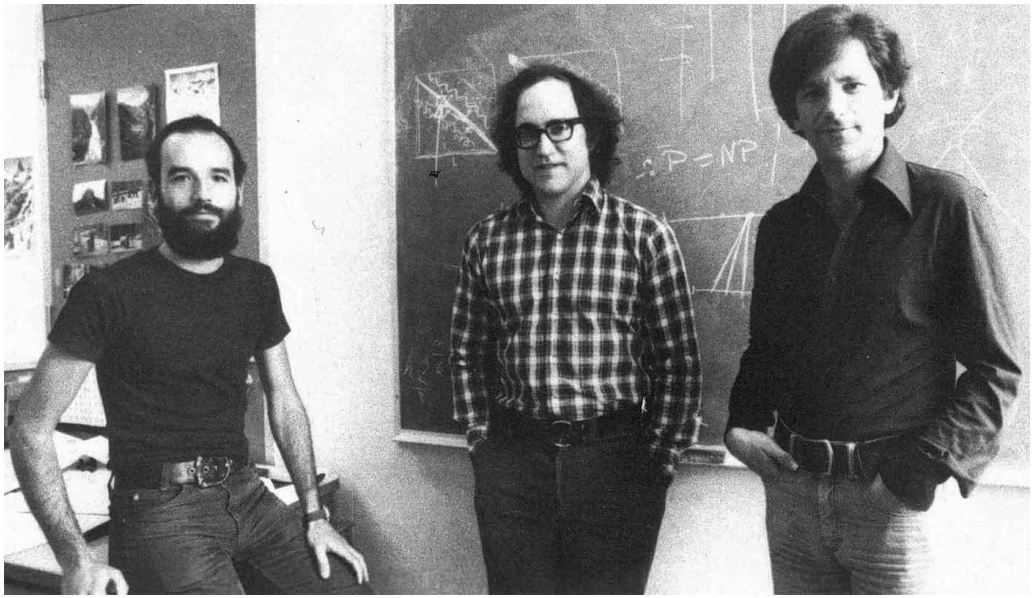
p,q verschiedene Primzahlen und $n = p \cdot q$. Dann gilt:

$a^{(p-1)(q-1)+1} \equiv a \bmod n$ Version 1

$a^{m(p-1)(q-1)+1} \equiv a \bmod n \qquad m \in N$ Version 2

5. Akt:
Verschlüsseln und entschlüsseln

Ronald Rivest
Adi Shamir
Leonard Adleman
1977



Anna gibt bei einer Internetgesellschaft eine Bestellung auf. Der Computer der Gesellschaft bildet:

$$N = p \cdot q$$

p,q: Primzahlen, geheim

N: wird veröffentlicht

Anna erhält Verschlüsselungszahl E

E: für alle Kunden gleich, öffentlich

Botschaft von Anna sei K.

Verschlüsselung:

$$K \rightarrow K^E \bmod N = \tilde{K}$$

Beispiel:

$$p = 5, q = 7 \rightarrow N = 5 \cdot 7 = 35$$

$$E = 11$$

$$K = 9$$

$$K^E = 9^{11} \equiv 4 \bmod 35$$

$$\tilde{K} = 4$$

Entschlüsselung:

$$a^{m(p-1)(q-1)+1} \equiv a \bmod N$$

$$K^{m(p-1)(q-1)+1} \equiv K \bmod N$$

$$K^{E\cdot\frac{m(p-1)(q-1)+1}{E}} \equiv K \bmod N$$

$$\tilde{K}^{\frac{m(p-1)(q-1)+1}{E}} \equiv K \bmod N$$

Bestimme m so, dass der Exponent natürlichzahlig.

Beispiel: $p = 5, q = 7, N = 35, E = 11, K = 9, \tilde{K} = 4$

$\frac{m \cdot 4 \cdot 6 + 1}{11}$ natürlichzahlig für $m = 5$

$$\tilde{K}^{\frac{m(p-1)(q-1)+1}{E}} = 4^{\frac{5\cdot 4\cdot 6+1}{11}} = 4^{11} \equiv 9 \bmod 35 \quad \rightarrow K = 9$$

Schülerzitat

Ich hätte mir niemals vorstellen können, dass man mit den Primzahlen so viel anfangen kann. Ich finde das Prinzip unglaublich gut, wenn man den Unterricht fast ausschliesslich auf unseren Erkenntnissen und Ideen aufbaut. Wenn sie uns zum Beispiel gesagt hätten, dass wir jeweils die Vielfachen einer Zahl aus einer Liste heraustreichen können und so nach und nach die Primzahlen herauskristallisieren können, hätten wir das vermutlich nicht so spannend gefunden, doch wenn man plötzlich selbst auf die Erkenntnis kommt, dass man viel effizienter ist, wenn man die Vielfachen streicht, fühlt man sich sofort clever und ist motiviert.

Literatur zu Primzahlen / Quellen

Marcus du Sautoy, Die Musik der Primzahlen

Literatur zu Lehrkunstdidaktik

Christoph Berg et al., Die Werkdimension im Bildungsprozess
Susanne Wildhirt, Lehrstückunterricht gestalten
Martin Wagenschein, Naturphänomene verstehen
Hans Brüngger, Wahrscheinlichkeitsrechnung mit Pascal
Mario Gerwig, Beweisen verstehen im Mathematikunterricht
Interessante Website: www.lehrkunst.ch
Broschüre:
https://ksalpenquai.lu.ch/dokumente/lehrstuecke_mathematik

philipp.spindler@edulu.ch