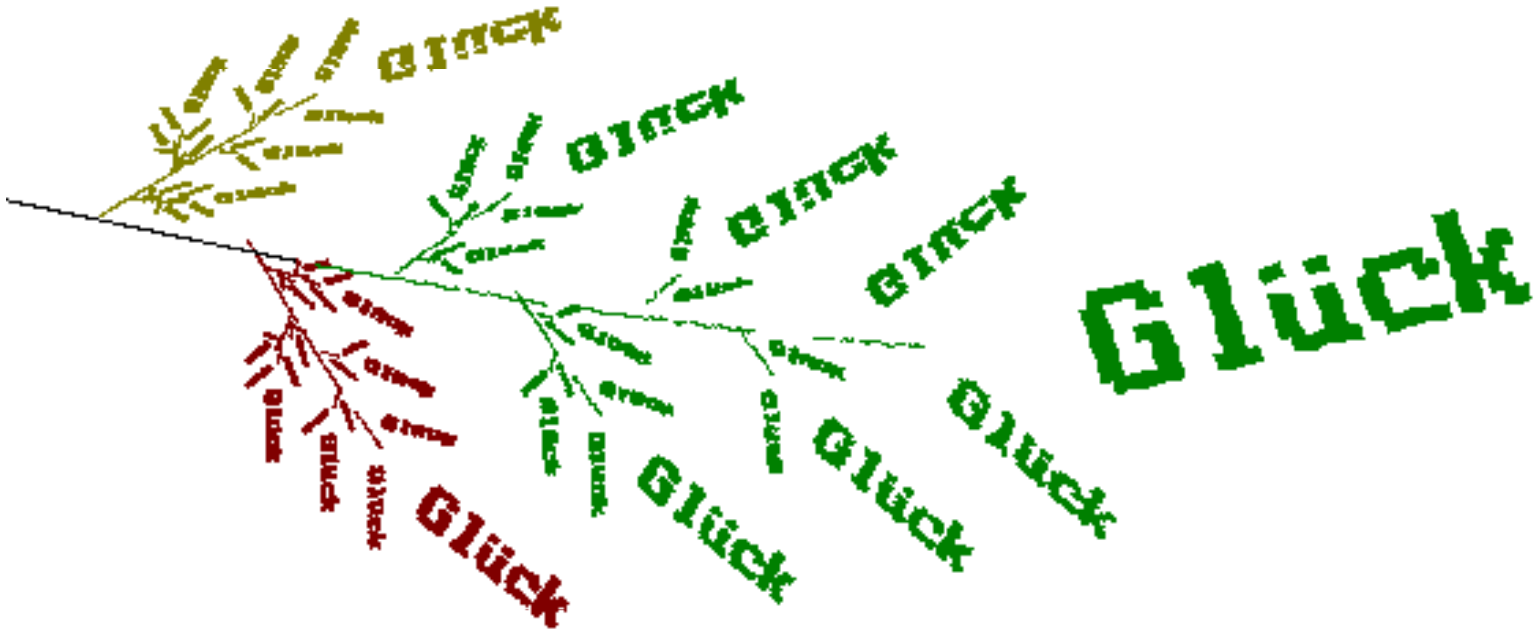
Mathematik für alle

LEUPHANA
UNIVERISITÄT LÜNEBURG

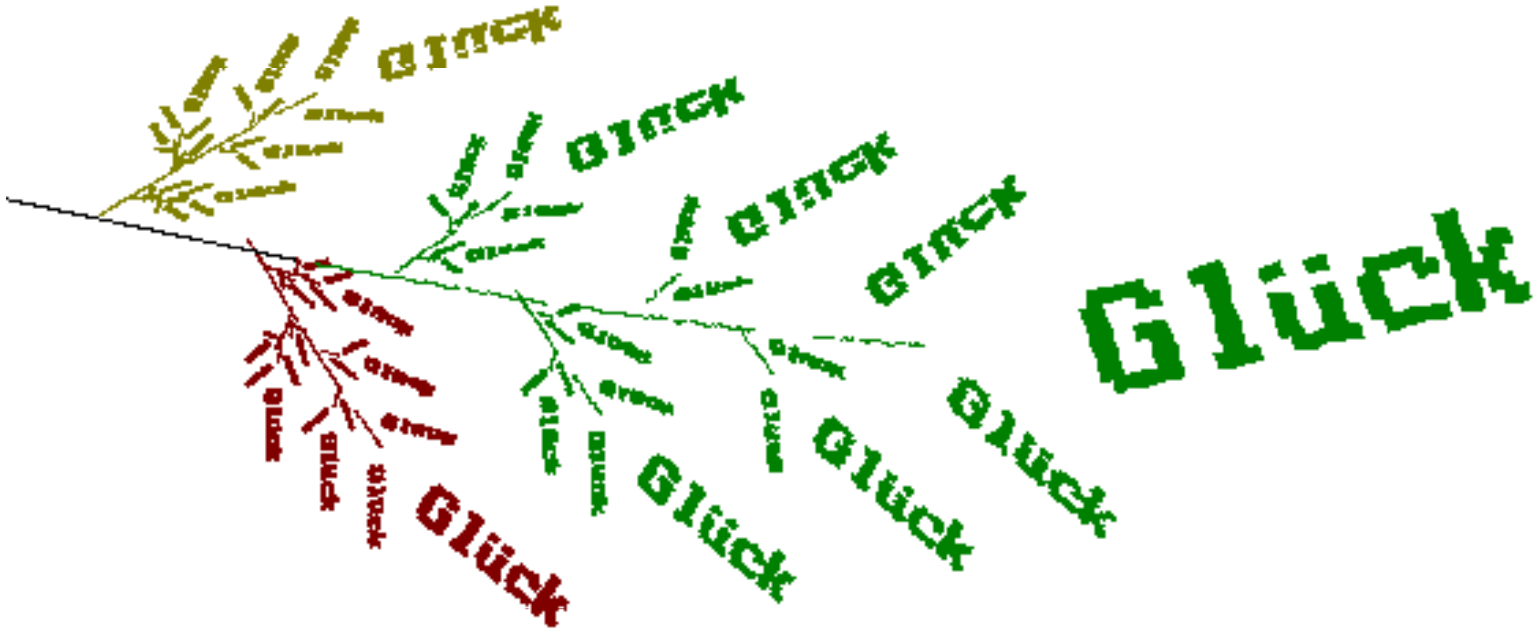


Mathematics for Everyone

LEUPHANA
UNIVERISITÄT LÜNEBURG

This is a fractal with the word

„luck“

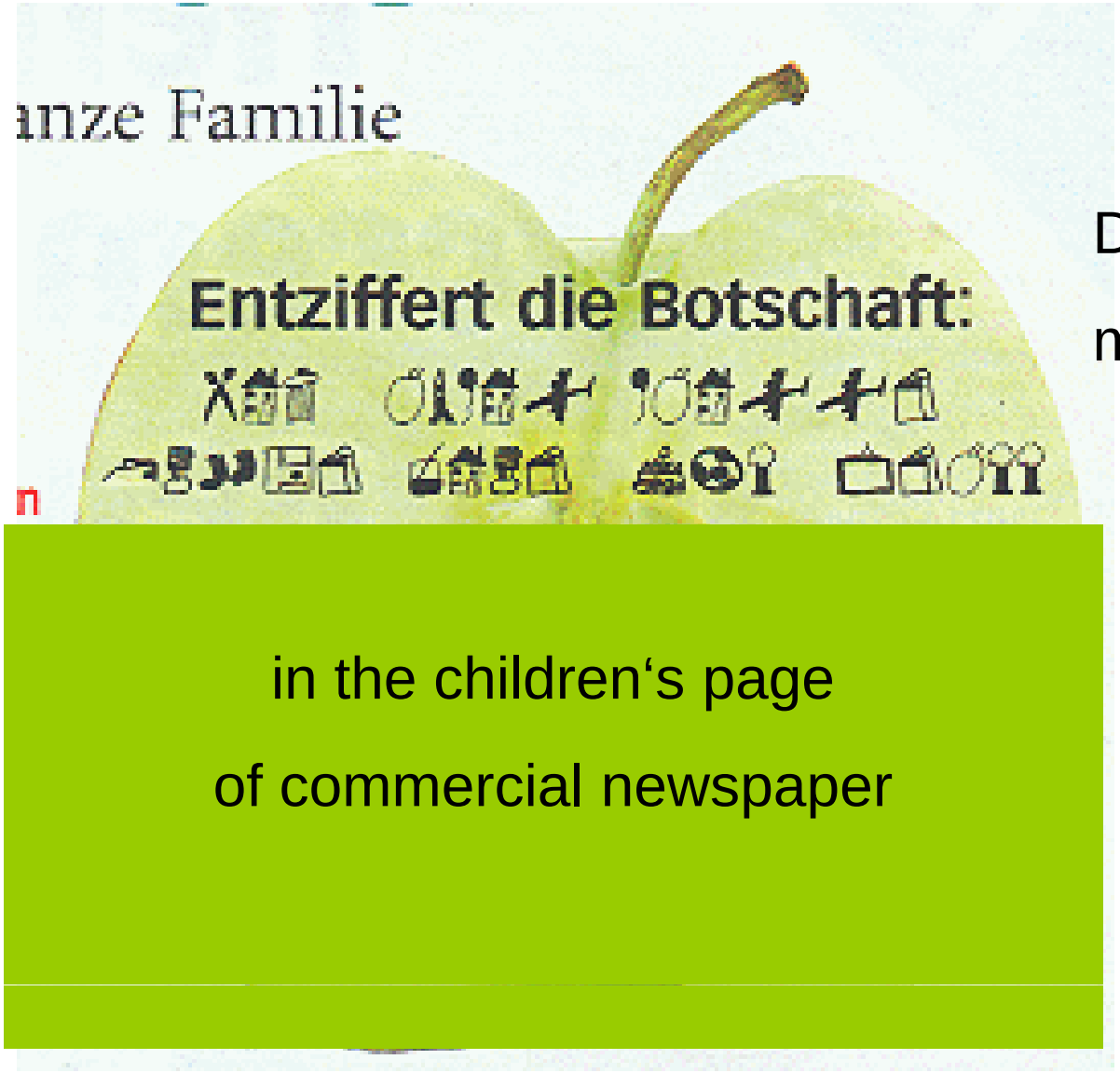


Mathematik für Kinder

auf der Kinderseite

einer Kundenzeitung

Mathematics for Children

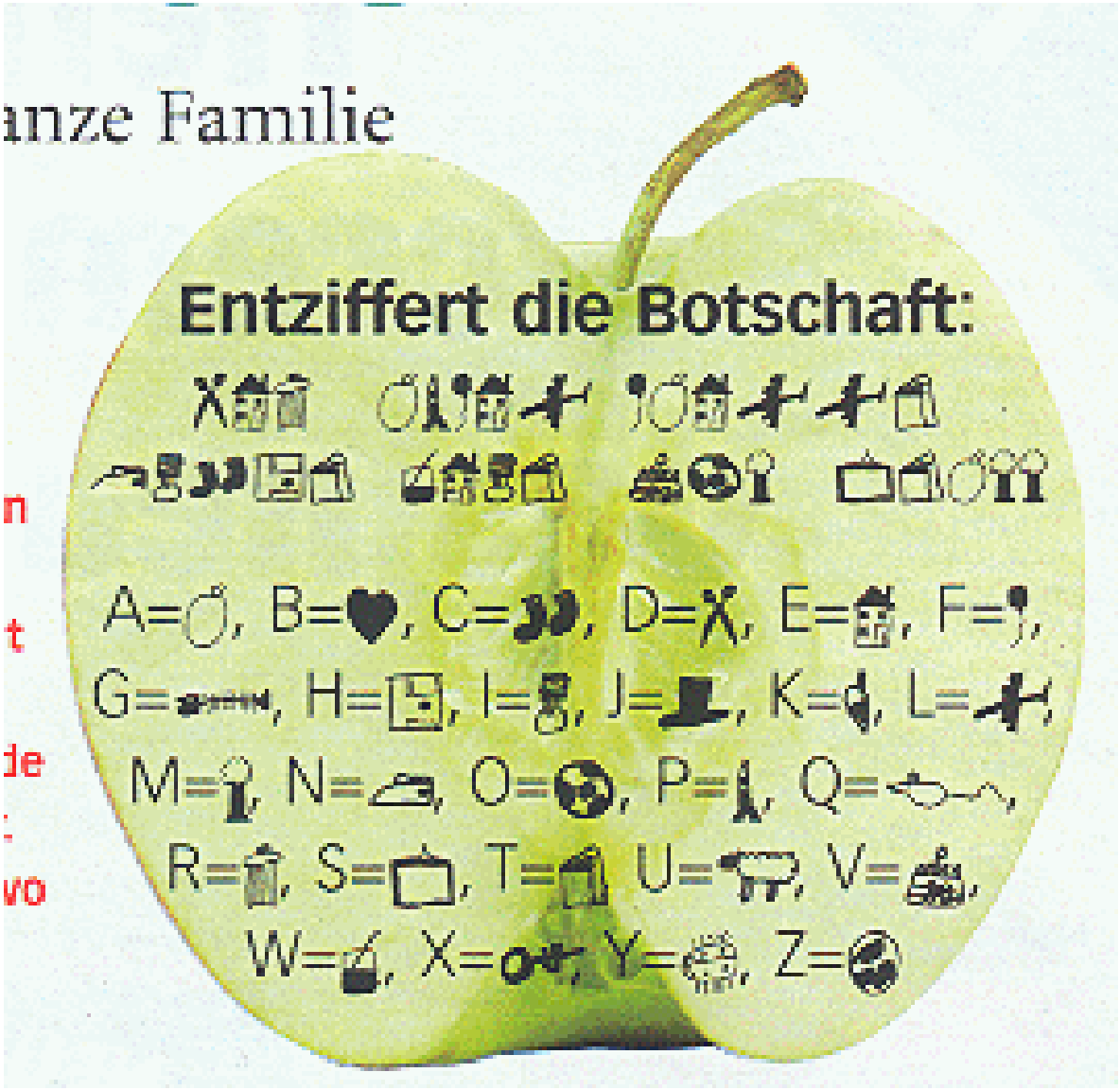


Decode the message:

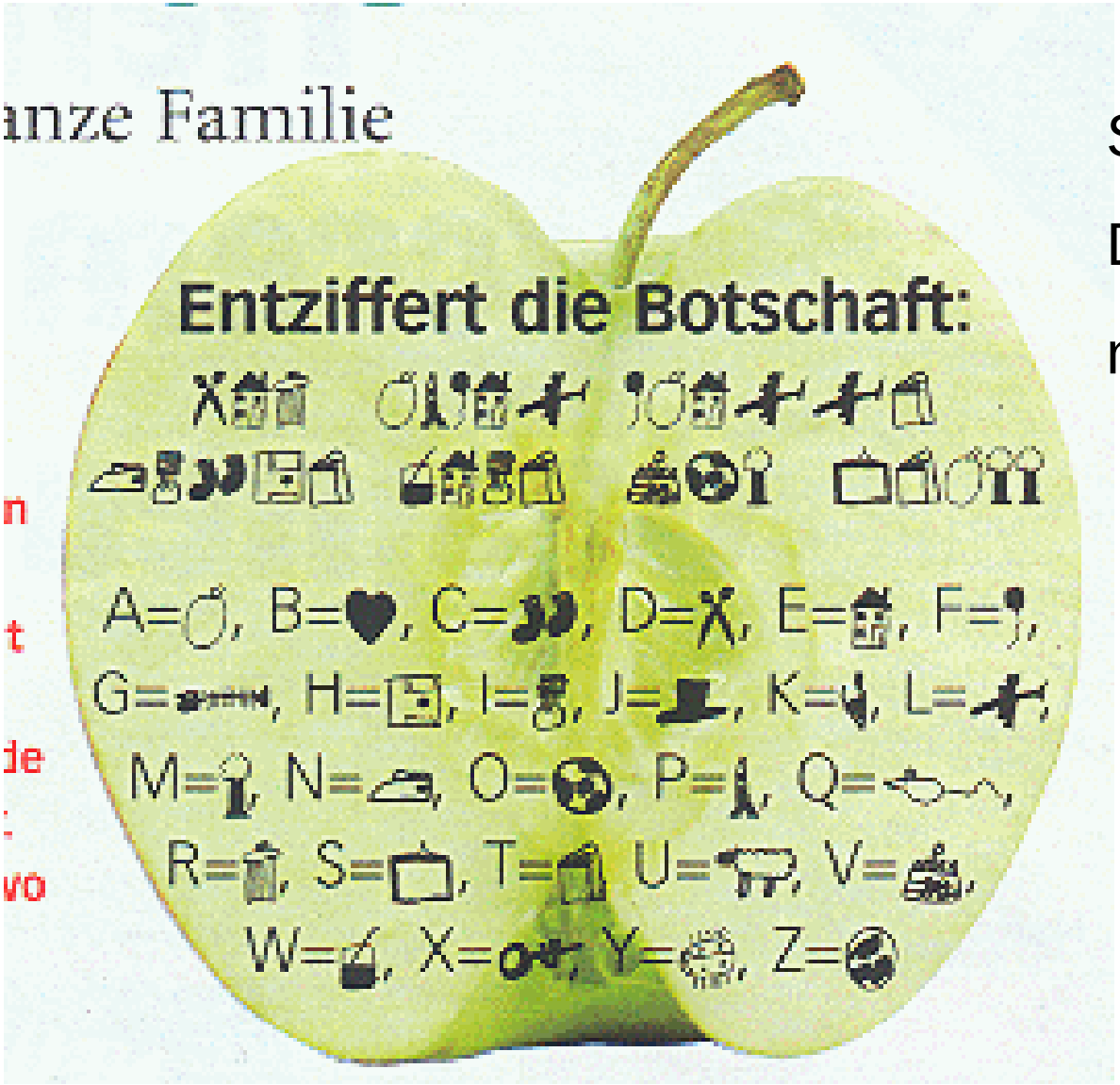
in the children‘s page

of commercial newspaper

Mathematik echt leicht



Mathematics is Easy



Solution:

Der Apfel faellt

nicht weit vom Stamm

a german idiomatic

expression:

The apple falls not

far from the tree

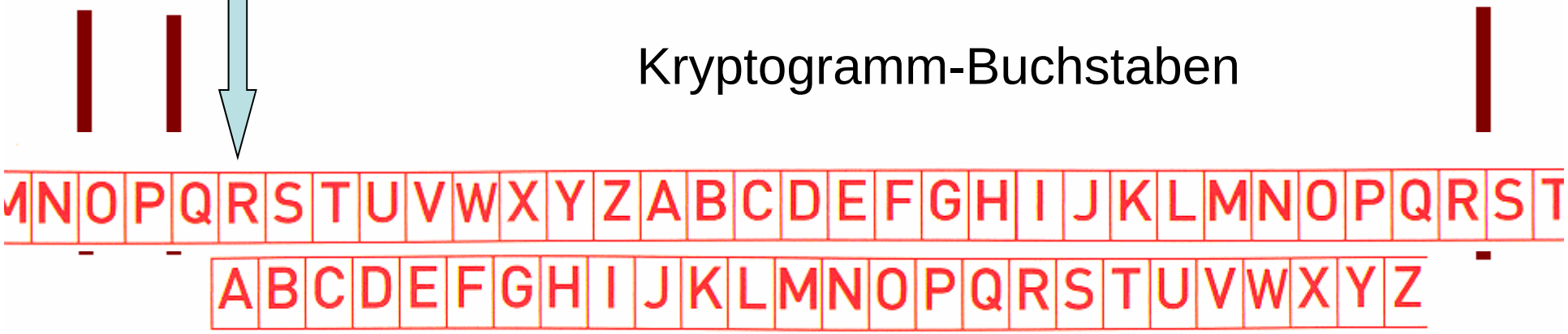
Cäsarcode, Urtyp der Kryptografie

MATHE

Schlüssel-
Buchstabe

über das A stellen

Kryptogramm-Buchstaben



Klartext-Buchstaben

Caesar‘s code, Prototype of the Cryptographic Methods

keyletter

MATHE

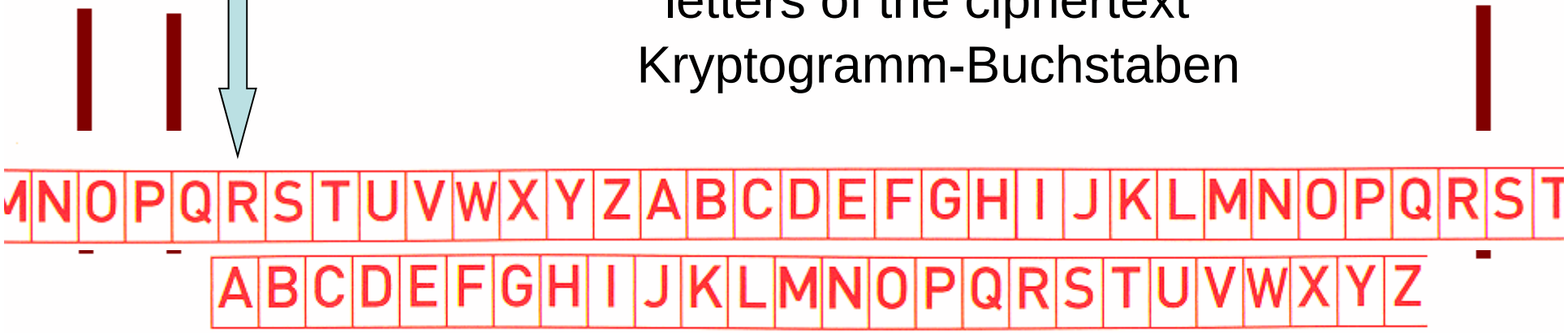
Schlüssel-
Buchstabe

put it over the A

über das A stellen

letters of the ciphertext

Kryptogramm-Buchstaben



Klartext-Buchstaben letters of the plaintext

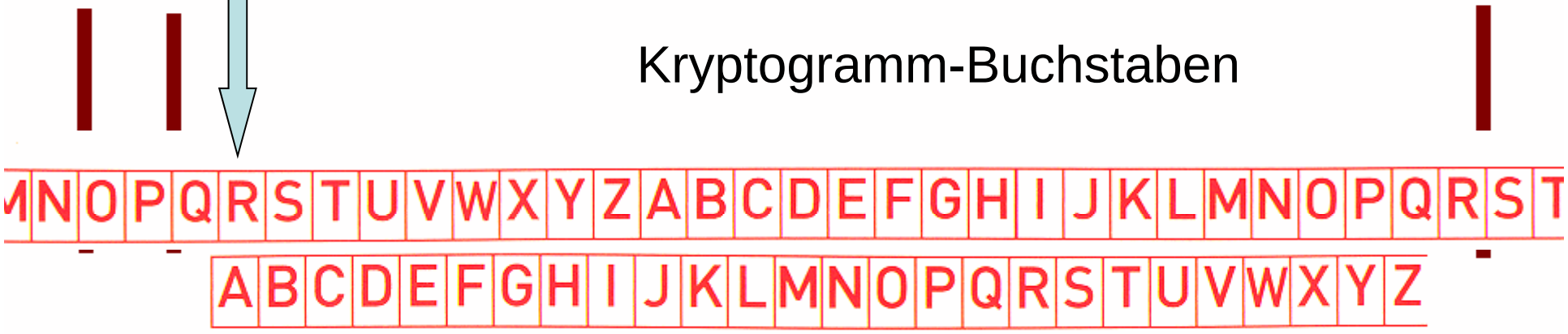
do it yourself: caesarcode

MATHE

DRKYV

Schlüssel-
Buchstabe

über das A stellen



Caesar‘s Code, the Origin of the Cryptography

keyletter

Schlüssel-Buchstabe

MATHE

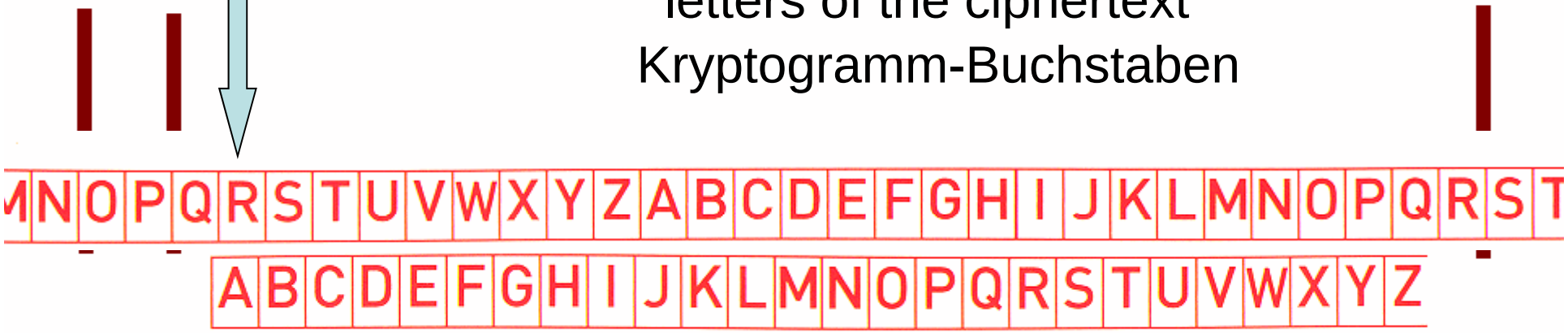
DRKYV

put it over the A

über das A stellen

letters of the ciphertext

Kryptogramm-Buchstaben

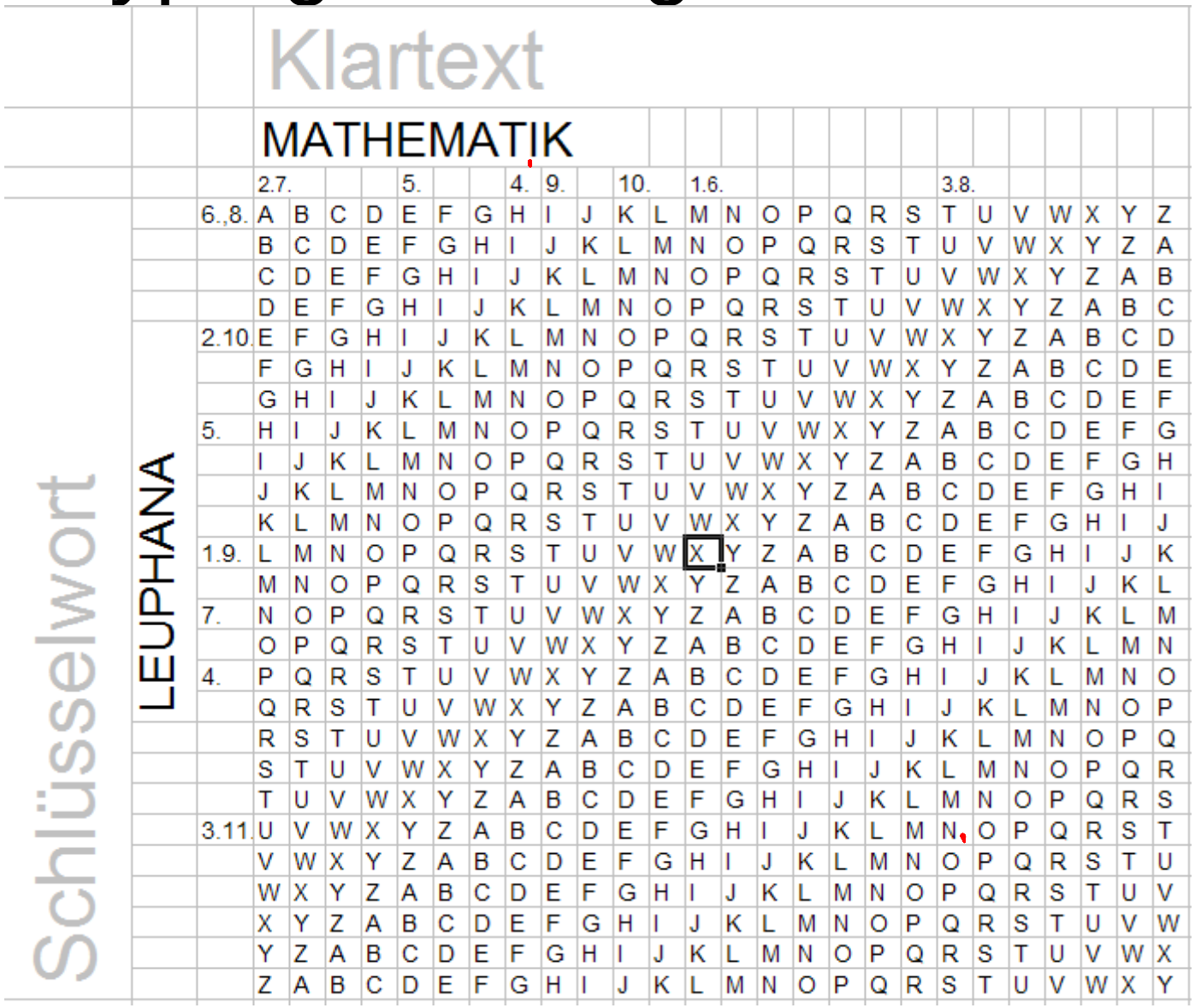


Klartext-Buchstaben letters of the plaintext

Kyptografie, Vigenère-Verfahren

um 1550

Kryptogramm:



Cyptographie, Vigenère‘s Method

um 1550

Klartext plaintext

MATHEMATIK

Schlüsselwort keyword

LEUPHANA

		2.7.			5.			4.	9.		10.		1.6.						3.8.					
6.,8.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
2.10.	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
5.	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
1.9.	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
7.	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
4.	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
3.11.	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Kryptogramm:

ciphertext:

Kyptografie, Vigenère-Verfahren um 1550

Klartext: MATHEMATIK

Schlüsselwort: LEUPHANA

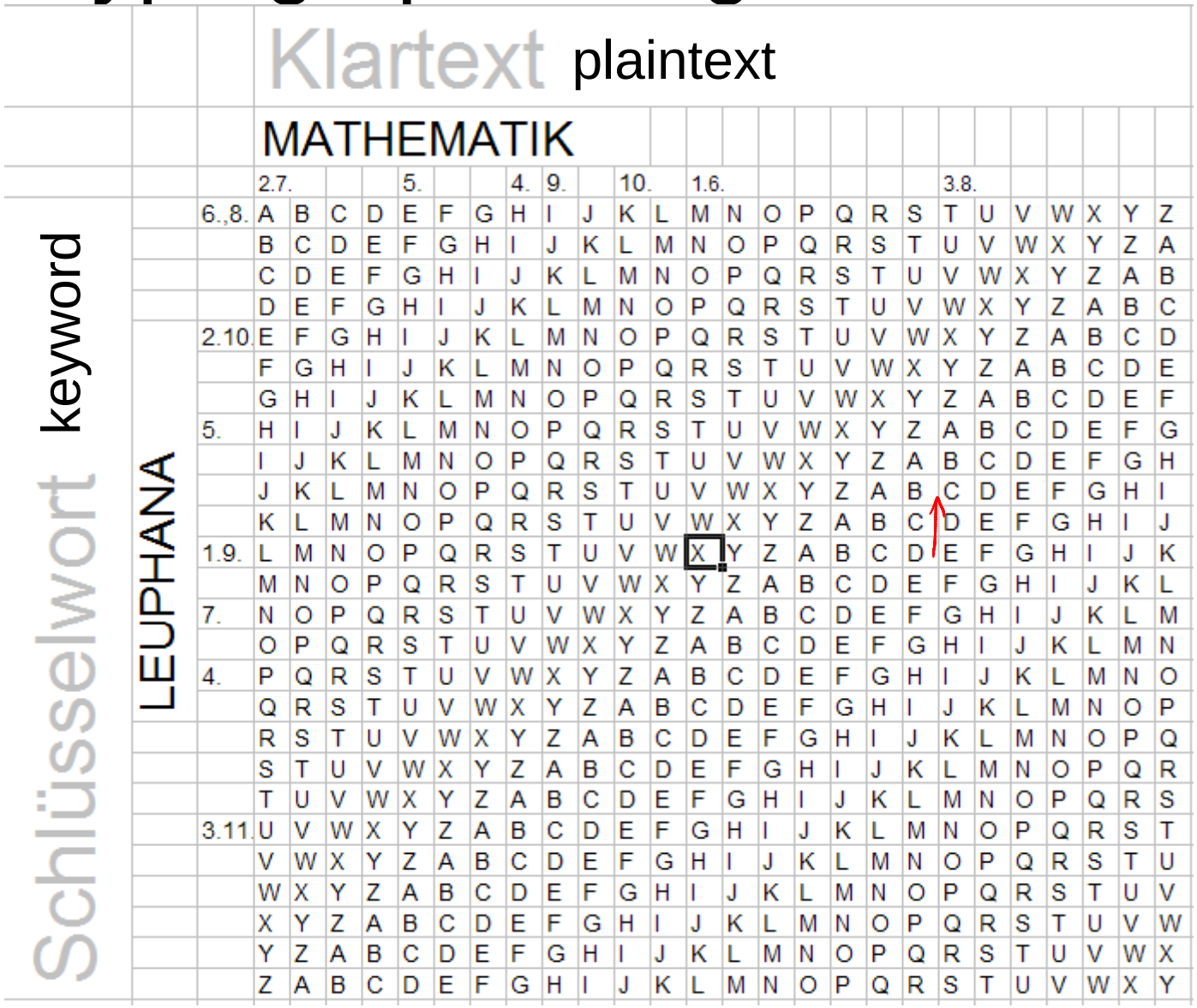
		2.7.			5.			4.	9.		10.		1.6.						3.8.						
6.,8.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
2.10.	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
5.	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
1.9.	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
7.	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
4.	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
3.11.	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Kryptogramm:

XENWLMNTTO

DYJTY

Cyptographie, Vigenère‘s Method



ciphertext:

XENWLMNTTO

DYJTY

Kyptografie macht sich auf den Weg

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

MATHE

4735544239

INFO: Der ASCII-Code ist die übliche Codierung des Alphabetes.

Die großen Buchstaben reichen von 65 bis 90, dann folgen die kleinen Buchstaben.

Hier ist die Zahl 30 vom ASCII-Code abgezogen, damit man zweistellig bleibt.

Cyptography Goes On

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

MATHE

4735544239

INFO: The ASCII-Code is the usual way to realise letters and sign in the computer.

The big Letters have the Mumbers 65 to 90, then the small letters follow.

The number 30 is subtracted from ASCII-Code here, so that two figures are enough.

Kyptografie macht sich auf den Weg

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Vigenère-Chiffrierung mit Ziffern

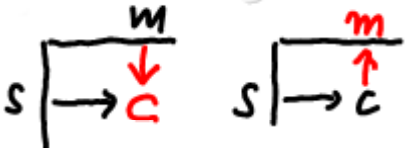
s \ m	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Klartext m MATHE

Schlüssel s 2846935817

4735544239

frei erfunden



Cyptography Goes On

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

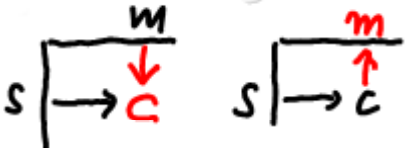
Vigenère-Chiffrierung mit Ziffern

s \ m	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

plaintext m MATHE

key s 2846935817

free chosen



Zahlen ermöglichen gute Kryptografie

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Vigenère-Chiffrierung mit Ziffern

s \ m	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

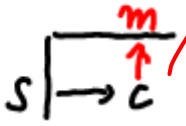
Klartext m: MATHE

4735544239

Schlüssel s: 2846935817

65714

+ rechnen modulo-10



Numbers are Good for Good Cryptography

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Vigenère-Chiffrierung mit Ziffern

s \ m	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

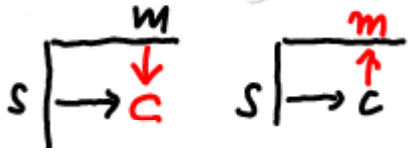
MATHE

plaintext m 4735544239

key s 2846935817

65714

you habe to add it without transfer 10



modulo 10

Zahlen ermöglichen gute Kyptografie

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Vigenère-Chiffrierung mit Ziffern

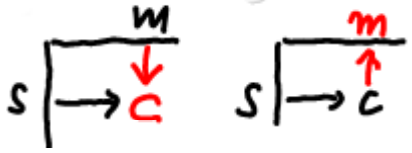
s \ m	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Klartext m MATHE

4735544239

Schlüssel s 2846935817

C = 657147 . . . . . .



C = 6781

S = 2846

m = ?

Numbers are Good for Good Cryptography

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Vigenère-Chiffrierung mit Ziffern

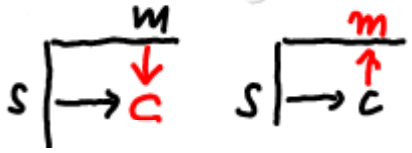
s \ m	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

MATHE

plaintext m 4735544239

key s 2846935817

$c = 657147\ldots$



$c = 6781$

$s = 2846$

$m =$?

Rechnen geht besser als Ablesen

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Die Tabelle können wir vergessen, man kann das ganz einfach auch ausrechnen!

Klartext m MATHE

4735544239

Schlüssel s 2846935817

Ziffernweise ohne Übertrag addieren

$m_Z + s_Z = c_Z$

$c_Z - s_Z = m_Z$

Ziffernweise abziehen „modulo 10“

C = 6571 .....

C = 67814697

S = 28469358

m = 4945

To Add is Better than to Read Vigenère's Table

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Forget the table, it is easier to add it (without transfer the 10)

MATHE

plaintext m 4735544239

key s 2846935817

add the figures and drop the tens

C = 6571 .....

$$m_Z + s_Z = c_Z$$

$$c_Z - s_Z = m_Z$$

subtract the figures
take a 10 if you need
„modulo 10"

C = 67814697

S = 28469358

m = 4945

Rechnen geht besser als Ablesen

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Die Tabelle können wir vergessen, man kann das ganz einfach auch ausrechnen!

Klartext m MATHE

4735544239

Schlüssel s 2846935817

Ziffernweise ohne Übertrag addieren

$m_Z + s_Z = c_Z$

$c_Z - s_Z = m_Z$

Ziffernweise abziehen „modulo 10“

$c = 6571479046$

$c = 67814697$

$s = 28469358$

$m = 4945534 9$

To Add is Better than to Read Vigenère's Table

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

Forget the table, it is easier to add it (without transfer the 10)

plaintext m MATHE

4735544239

key s 2846935817

add the figures and drop the tens

$c = 6571479046$

$m_Z + s_Z = c_Z$

$c_Z - s_Z = m_Z$

subtract the figures take a 10 if you need „modulo 10“

$c = 67814697$

$s = 28469358$

$m = 4945539$

Kyptografisches Protokoll

one-time-pad (dezimal)

- Vorbereitungsphase
  Anton und Berta vereinbaren einen Schlüssel
- Anwendungsphase: Verschlüsselung (encryption)
  1. Anton übersetzt einen Klartext in eine Zahl m
  2. Er addiert ziffenweise „modulo 10“ (d.h. ohne Übertrag) den Schlüssel s
  3. Das Ergebnis c schickt er Berta.
- Entschlüsselung (decryption)
  1. Berta subtrahiert ziffernweise „modulo 10“ den Schlüssel von dem Krytogramm c und erhält m
  2. Sie übersetzt m zurück in Buchstaben und liest.

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

$$m_Z + s_Z = c_Z$$

$$c_Z - s_Z = m_Z$$

Cryptographic Protokoll

one-time-pad (decimal)

- preparation phase
  Anton and Berta agree on a key
- application phase: encryption
  1. Anton translates a plaintext in a Number m
  2. He adds figurewise „modulo 10“ (without take 10) the key s
  3. He sends the result, the ciphertext, c to Berta.
- decryption
  1. Berta subtracts „modulo 10“ the key from the ciphertext. The result ist the message m.
  2. She translates m back in letters ans reads the message.

A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

$$m_Z + s_Z = c_Z$$

$$c_Z - s_Z = m_Z$$

Vierer-Übung

Vier Studis bilden eine Gruppe

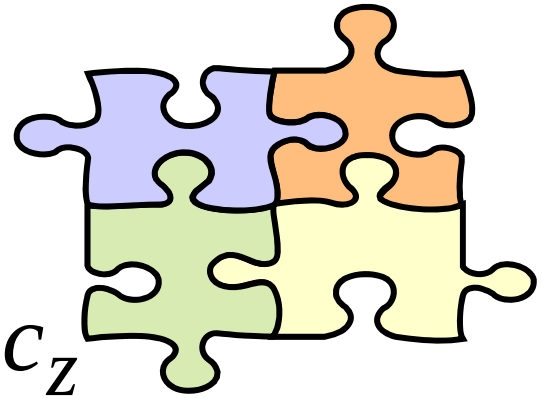
Rechts-Unten sagt den Schlüssel an.

8 Stellen zufällig

Die, die nebeneinander sitzen, verschlüsseln ein Wort mit 4 Buchstaben.

Die beiden anderen müssen es herausbekommen.

6 Minuten



A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

$$m_Z + s_Z = c_Z$$

$$c_Z - s_Z = m_Z$$

Exercises with Four Students

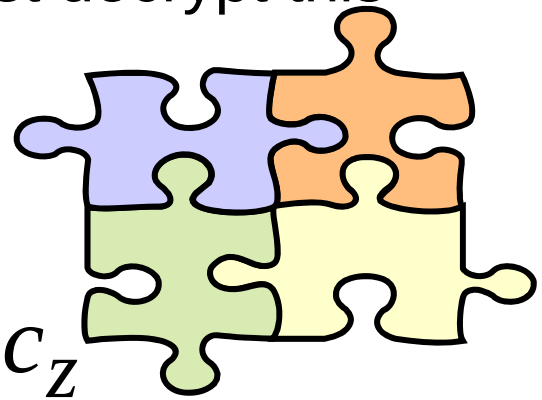
Four students build a group.

Right-down says an arbitrary key.
8 figures randomly

The students, which are neighbours, encrypt one word whith 4 letters.

The two others must decrypt this word.

6 minutes



A	B	C	D	E	F	G	H	I	J	K	L	M
35	36	37	38	39	40	41	42	43	44	45	46	47

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
48	49	50	51	52	53	54	55	56	57	58	59	60

$$m_Z + s_Z = c_Z$$

$$c_Z - s_Z = m_Z$$

Was ist moderne Kyptografie?

natik: NAME:
viss. Schein /Note
chaftlicher Schein

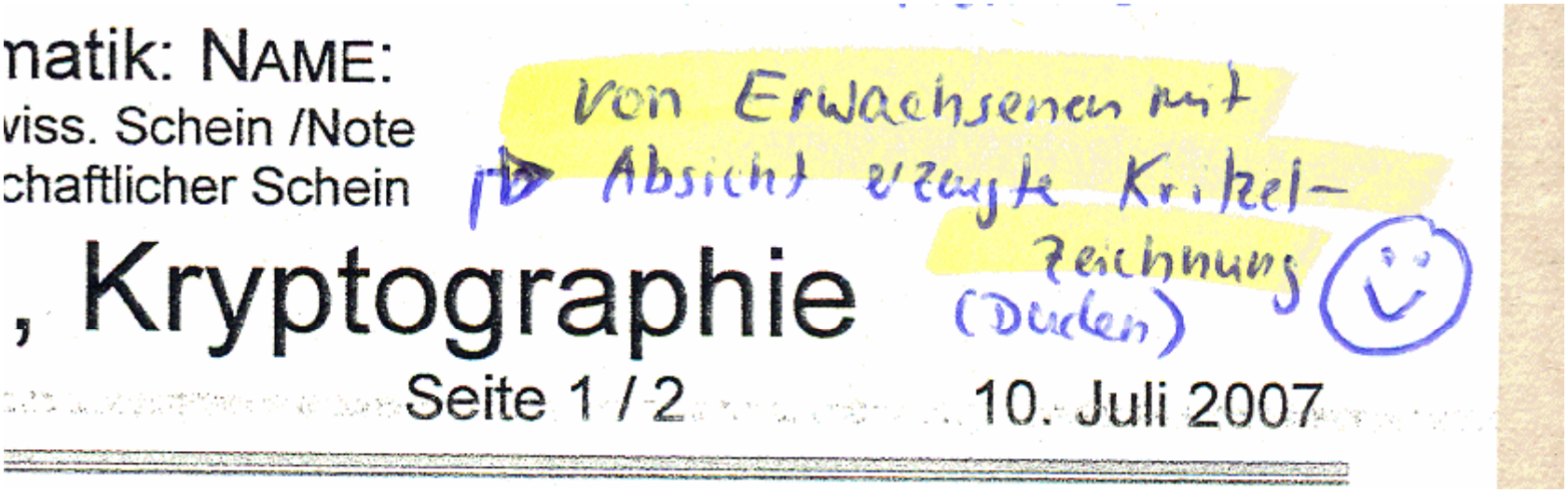
, Kryptographie

von Erwachsenen mit Absicht erzeugte Kritzelzeichnung (Duden)

Seite 1 / 2 10. Juli 2007

Kryp|to|gra|fie, **Kryp|to|gra|phie**, die; -, ...ien (*Psychol.* absichtslos entstandene Kritzelzeichnung bei Erwachsenen; Disziplin der Informatik; *veraltet für* Geheimschrift)

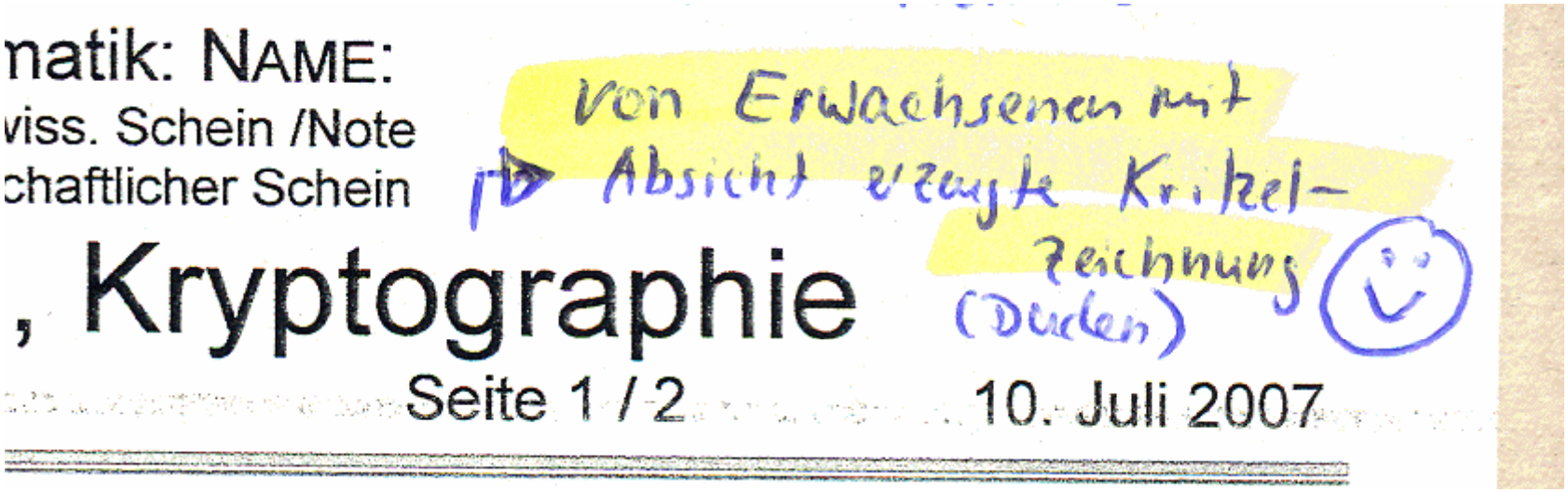
What is Modern Cryptography?



Kryp|to|gra|fie, **Kryp|to|gra|phie**, die; -, ...ien (*Psychol.* absichtslos entstandene Kritzelzeichnung bei Erwachsenen; Disziplin der Informatik; *veraltet für* Geheimschrift)

It ist a very special joke, that one can read important german dictionary: cryptography is a randomly made scratching of adults.

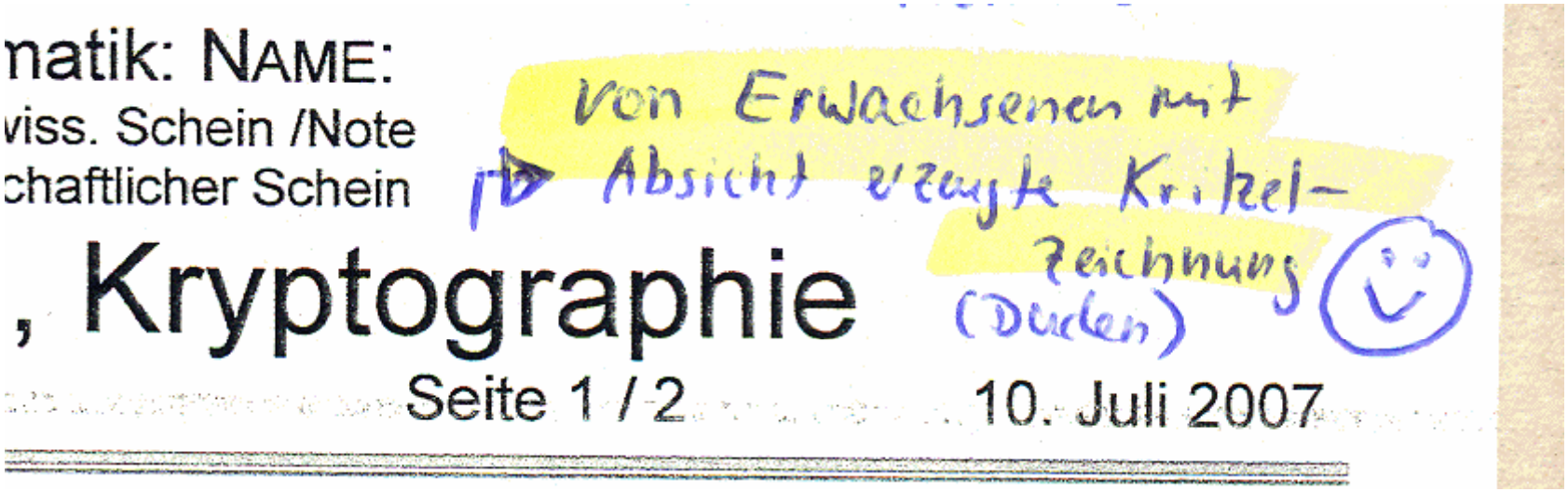
The goal of this lecture is, to enable people to know it better.



Was ist moderne Kryptografie?

- treibt das Rechnen auf die Spitze
- verwendet riesige Zahlen von 200 Stellen Länge
- werkelt mit Primzahlen
- erzeugt das Kryptogramm und die Schlüssel durch Rechnungen
- die Rechnungen laufen „modulo n“, im Restklassenring von n

Das wird jetzt erkärt:

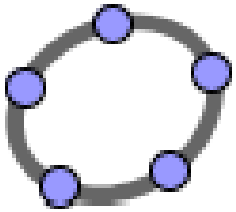


What is modern cryptography?

- high end calculating with numbers
- takes giant numbers with 200 figures
- handles with primnumbers
- produce the ciphertext and the keys
  only with calculating
- calculation is „modulo n“, in residue class ring on n

This will be explained:

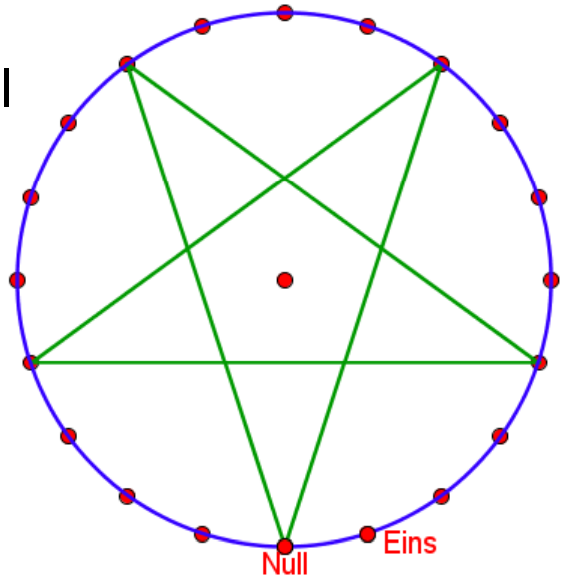
modulo 20
was bedeutet das?

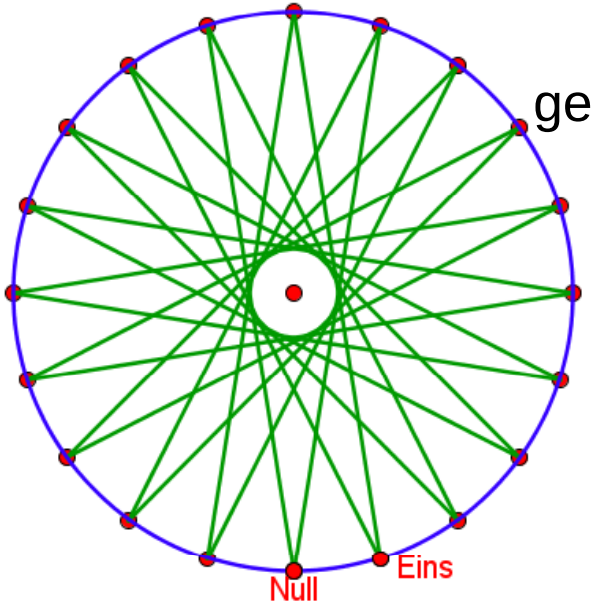


Die Vielfachen von 8 bzw. 9 modulo 20

Es geht nur um die Reste beim Teilen durch 20.

gehe von Null
8 Schritte
und
8 Schritte
u.s.w.
…



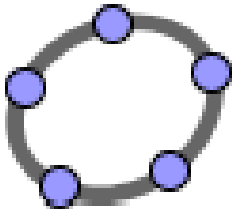


gehe von Null
9 Schritte
und
9 Schritte
u.s.w.
…

In Z {0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 1

In Z(20) {0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12,

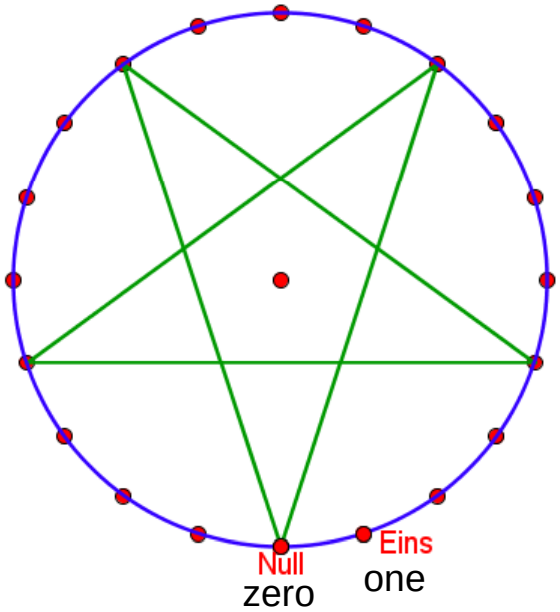
modulo 20
what is it?

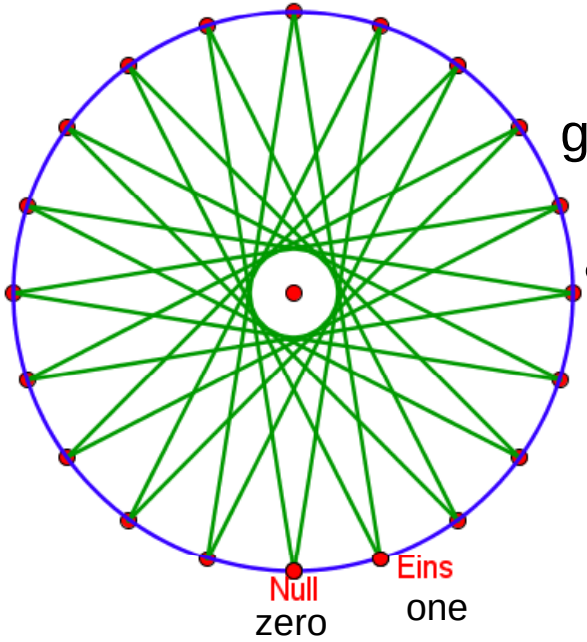


The multiples of 8 (left) and 9 (right) modulo 20

Importend are only the residues in divison by 20.

go from zero
8 steps
and 8 steps
and so on
…



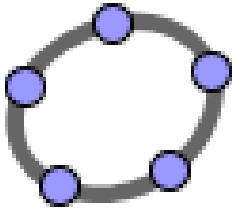


go from zero
9 steps
and 9 steps
and so on
…

In Z {0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 1

In Z(20) {0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12,

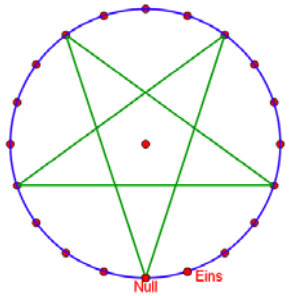
modulo n
was bedeutet das?

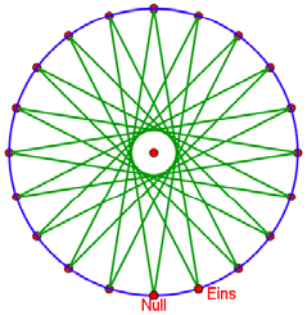


Die Vielfachen von 8 bzw. 9 modulo 20

Es geht nur um die Reste beim Teilen durch 20.

n = 20





8 hat einen gemeinsamen Teiler mit 20, nämlich 4.

Es bleiben Punkte übrig.

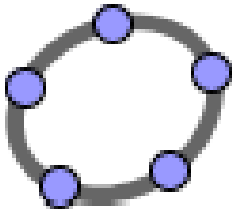
9 hat keinen gemeinsamen Teiler mit 20

Es bleiben keine Punkte übrig.

In Z {0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 1

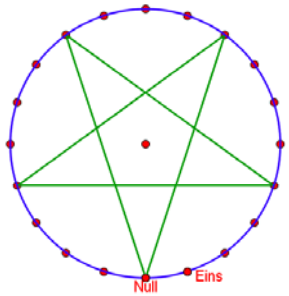
In Z(20) {0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12,

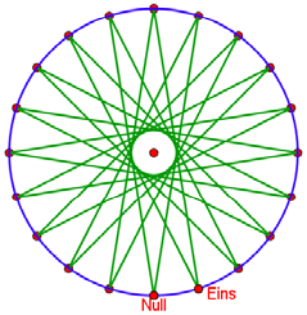
modulo n
what is it?



The multiples of 8 (left) and 9 (right) modulo 20
Importend are only the residues in divison by 20.

n = 20





8 has a common divisor with 20, namely 4.

9 don‘t have a commom divisor with 20

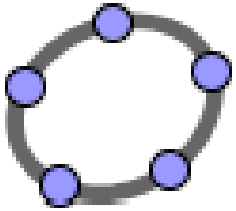
There are points in the circle without lines.

All points in the circle get lines.

In Z {0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 1

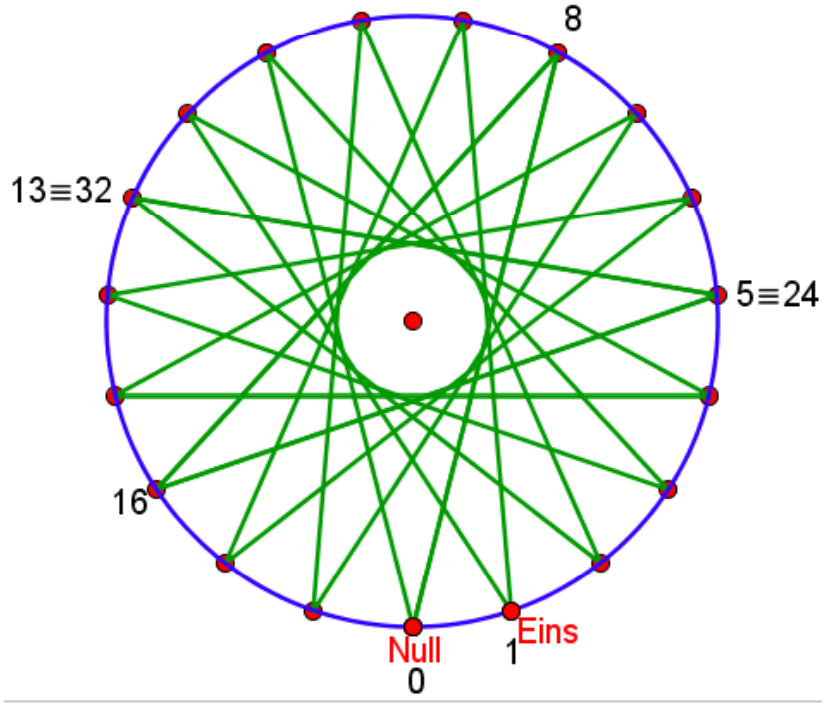
In Z(20) {0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12,

modulo n: was bedeutet das?



n = 19

Die Vielfachen von
8 modulo 19



Keine Zahl $1 < z < 19$ hat einen gemeinsamen Teiler mit 19.

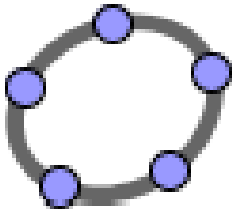
Darum wird immer jeder Punkt erreicht.

Es bleiben nie Punkte übrig.

19 ist eine Primzahl

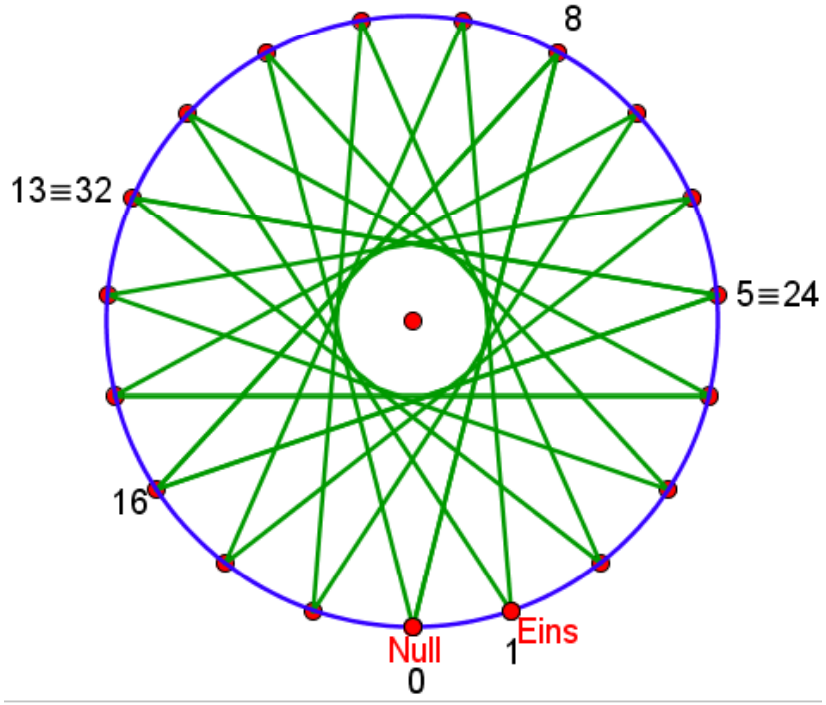
Eine Primzahl p ist eine Zahl mit genau zwei Teilern: 1 und p.

modulo n: what is it?



n = 19

The multiples of 8 modulo 19



No Number $1 < z < 19$ has a common divisor with 19.

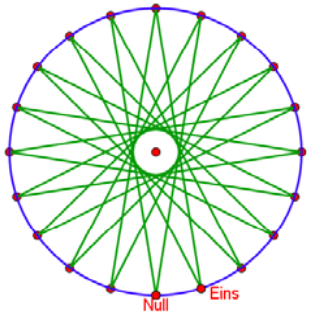
Therefore in all cases every point ist reached.

No points are left.

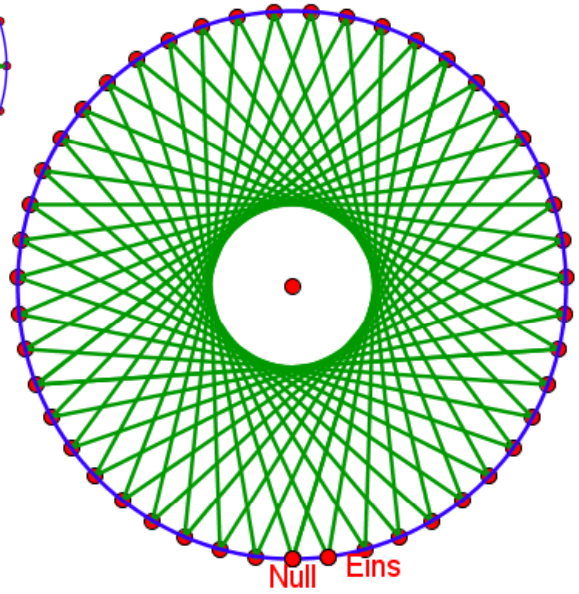
19 is a prime number

A prime number p is a number with exact two divisors: 1 and p.

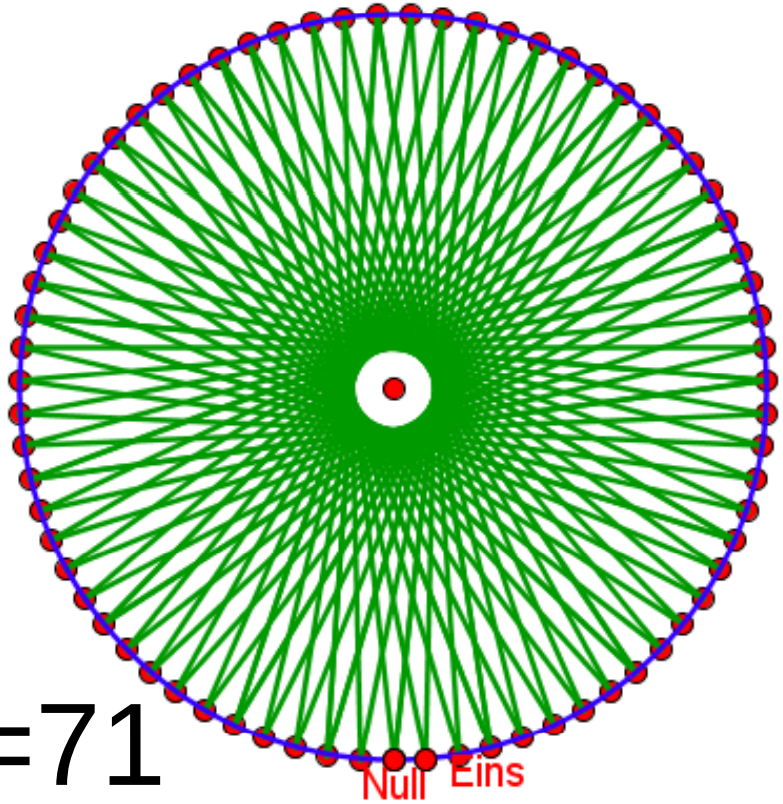
Die Primzahlen und das modulo-n-Rechnen →Kryptografie



n =19



n =47

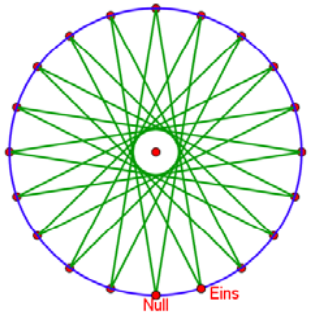


n =71

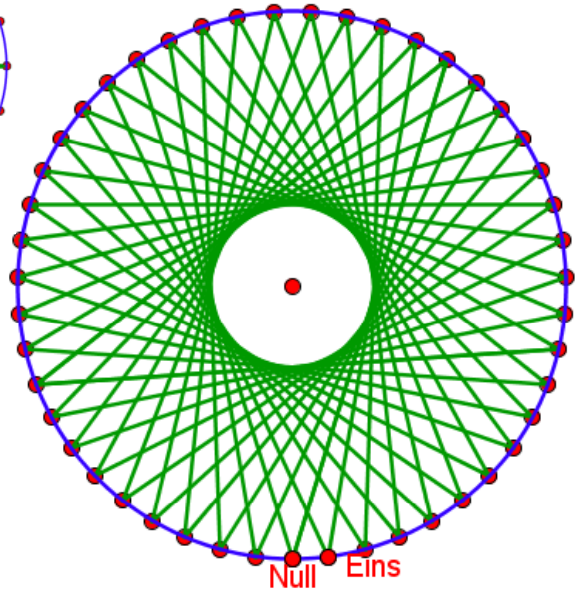
n = **221542321013390125581966581764075596 44**

1068955439549124678505921927805529849767

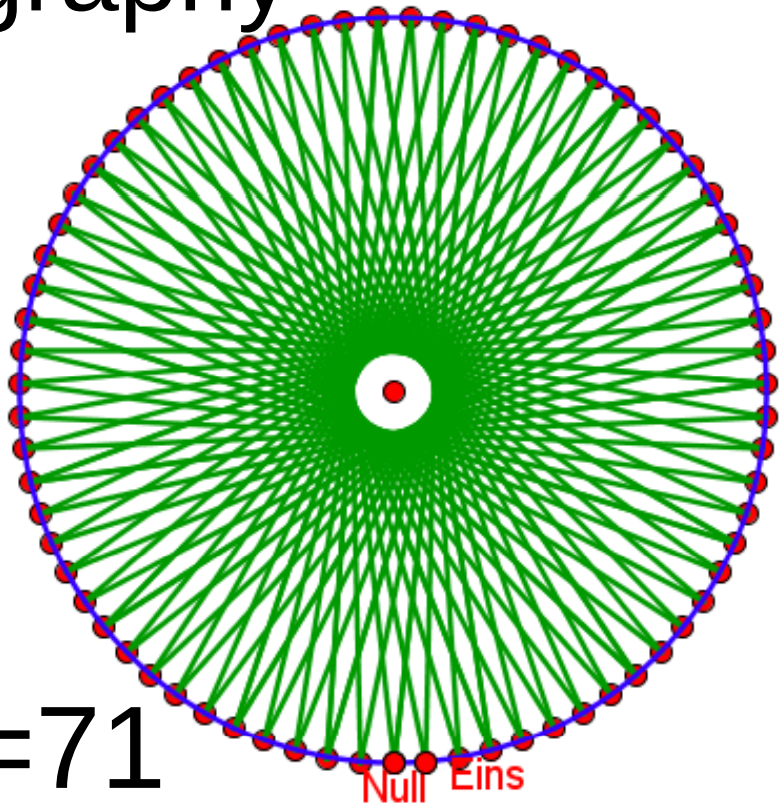
Prime Numbers and the Calulating modulo n →That‘s the New Cryptography



n =19



n =47



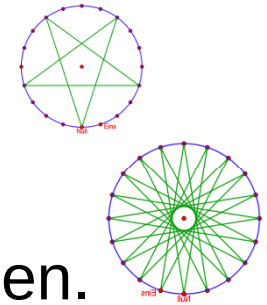
n =71

n =

25153528579505500464455223674991216717754459477884467104369027866457316690323872601396263900552169184402002146582419756137977860863538917211838281136977

Erklärung zur letzten Folie:

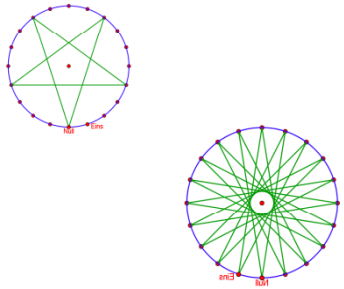
- Für jede Zahl n denkt man sich den Kreis der Zahlen als Punkte {0,1,2,3,….. n-1} auf dem Zifferblatt einer Uhr.
- Beim Rechnen modulo n kommen nur diese Zahlen vor. Ihre Menge bezeichnet man mit $\mathbb{Z}_n$. ($\mathbb{Z}$ sind die ganzen Zahlen)
- Die Vielfachen einer Zahl t lassen manchmal Punkte aus. Das ist für die Kryptografie ungünstig.
- Bei Primzahlen kann das nicht passieren, darum sind Primzahlen so wichtig für die Kryptografie.
- In der Kryptografie verwendet man riesige Primzahlen.



- Der ganz große Kreis rechts müsste für das angegebene n (etwa 10^{150}) viel mehr Punkte haben, als im Universum Atome (etwa 10^{77}) sind.

Explanation of the Last Slide:

- We think for every number n a circle of numbers with points {0,1,2,3,….. n-1} as a face plate of a clock.
- When we calculate modulo n the are only this numbers. We name the set of these numbers $\mathbb{Z}_n$. ($\mathbb{Z}$ are the integers)
- The multiples of a number t sometimes leap some points. This is awkward for cryptography.
- With prime numbers this is impossible. Thats why prime numbers are so important for cryptography



- In cryptography one take giant prime numbers Primzahlen.
- For the given n (ca. 10^{150}) the biggest circle at the right must have more points than the universe has atoms (ca. 10^{77}).

Jetzt: Kopfrechnen mit den Resten beim Teilen durch n: das ist Rechnen modulo-n

$17 \equiv 2 \pmod 5$

17 modulo 5 ist 2

17 ist gleich 2 modulo 5

17 ist kongruent 2 modulo 5

$\mathrm{mod}(17, 5) = 2$

$17 \equiv 2 \mod 5$

5 heißt „Teiler“ oder „modulo-Zahl“

$54 \equiv 10$

$54 \equiv 7$

$113 \equiv 11$

$73 \equiv 11$

$777730 \equiv 11$

Ganze Vielfache von n weglassen!

Now: Mental Arithmetic with the Rests by Dividing by n: That is modulo n Calculation.

$17 \equiv 2 \pmod 5$

17 modulo 5 equals 2

17 equals 2 modulo 5

17 is congruent 2 modulo 5

$\mathrm{mod}(17, 5) = 2$

$17 \equiv 2 \bmod 5$

5 is the „divisor“ or „modulo-number“

$54 \equiv 10$

$54 \equiv 7$

$113 \equiv 11$

$73 \equiv 11$

$777730 \equiv 11$

leave whole multiples of n!

Jetzt: Kopfrechnen mit den Resten beim Teilen durch n: das ist Rechnen modulo-n

$17 \equiv 2 \pmod 5$

17 modulo 5 ist 2

17 ist gleich 2 modulo 5

17 ist kongruent 2 modulo 5

$\mathrm{mod}(17, 5) = 2$

$17 \equiv 2 \mod 5$

5 heißt „Teiler“ oder „modulo-Zahl“

$54 \equiv 4 \pmod{10}$

$54 \equiv 5 \pmod 7$

$113 \equiv 3 \pmod{11}$

$73 \equiv 66 + 7 \equiv 7 \pmod{11}$

$777730 \equiv 777700 + 30 \pmod{11}$

$\equiv 30 \pmod{11}$

$\equiv 22 + 8 \equiv 8 \pmod{11}$

Ganze Vielfache von n weglassen!

evt. schrittweise

Now: Mental Arithmetic with the Rests by Dividing by n: That is modulo n Calculation.

$17 \equiv 2 \pmod 5$

17 modulo 5 equals 2

17 equals 2 modulo 5

17 is congruent 2 modulo 5

$\mathrm{mod}(17, 5) = 2$

$17 \equiv 2 \mod 5$

5 is the „divisor“ or „modulo-number“

$54 \equiv 10 \pmod 5$

$54 \equiv 7 \pmod{11}$

$113 \equiv 11 \pmod{11}$

$73 \equiv 66 + 7 \equiv 7 \pmod{11}$

$777730 \equiv 777700 + 30 \pmod{11}$

$\equiv 30 \equiv 22 + 8 \equiv 8 \pmod{11}$

leave whole multiples of n!

perhaps more steps

modulo-rechnen ist einfach

Man rechnet wie immer, lässt aber an beliebigen Stellen in Zahlen Vielfache der modulo-Zahl n weg oder addiert sie.

$73 + 56 \equiv_6 129 \equiv_6 3$

$\| \quad \|$

$1 + 2 = 3$

$13 \cdot 37 \equiv_5$

$5713 \cdot 68217 \equiv_5$

$17 - 24 \equiv_5 2 - 4 \equiv_5 -2 \equiv_5 3$

modulo Calculating ist Easy

You calculate in the normal manner but in numbers
you can leave multiples of the modulo-number n everywhere.
You can add the modulo number n, if a result is negative.

$73 + 56 \equiv_6 129 \equiv_6 3$

$\| \quad \|$

$1 + 2 = 3$

$13 \cdot 37 \equiv_5$

$5713 \cdot 68217 \equiv_5$

$17 - 24 \equiv_5 2 - 4 \equiv_5 -2 \equiv_5 3$

modulo-Rechnen ist einfach

Man rechnet modulo n wie immer, lässt aber an beliebigen Stellen in den Zahlen Vielfache der Modulzahl n weg.

$$73 + 56 \underset{6}{\equiv} 129 \equiv 3$$

$$\| \qquad \| \qquad \qquad \uparrow$$

$$1 + 2 = 3$$

$$13 \cdot 37 \underset{5}{\equiv} 3 \cdot 2 \underset{5}{\equiv} 6 \underset{5}{\equiv} 1$$

$$5713 \cdot 68217 \underset{5}{\equiv} 3 \cdot 2 \underset{5}{\equiv} 6 \underset{5}{\equiv} 1$$

$$17 - 24 \underset{5}{\equiv} 2 - 4 = -2 \underset{5}{\equiv} 3$$

weil: -2+5=3

modulo Calculating ist Easy

You calculate in the normal manner but in numbers
you can leave multiples of the modulo-number n everywhere.
You can add the modulo number n, if a result is negative.

$73 + 56 \underset{6}{\equiv} 129 \underset{6}{\equiv} 3$

$\| \quad \| \quad \|$

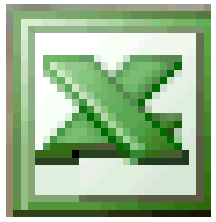
$1 + 2 = 3$

$13 \cdot 37 \underset{5}{\equiv} 3 \cdot 2 \underset{5}{\equiv} 6 \equiv 1$

$5713 \cdot 68217 \underset{5}{\equiv} 3 \cdot 2 \underset{5}{\equiv} 6 \underset{5}{\equiv} 1$

$17 - 24 \underset{5}{\equiv} 2 - 4 \underset{5}{\equiv} -2 \underset{5}{\equiv} 3$ because -2+5=3

$\mathbb{Z}_m$ = Z(m) ist die Menge der möglichen Reste beim Teilen durch m

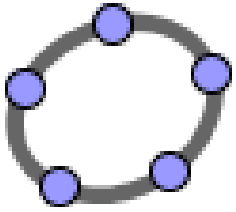


Excel
Rest(17;5) ⇝ 2
für $17 \equiv_5 2$
Geogebra Mod[17,5] ⇝ 2

Verknüpfungstafeln

Rechnen Modulo 5

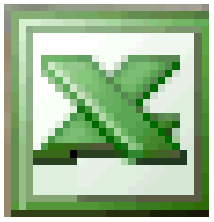
+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3



*	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

$(\mathbb{Z}_5, +, \cdot)$

$\mathbb{Z}_m$ = Z(m) is the Set of all Possible Rests in Division by m



Excel
Rest(17;5) ⇝ 2

für $17 \equiv_5 2$

Geogebra Mod[17,5] ⇝ 2

Rechnen Modulo 5

+	0	1	2	3	4
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

table of operation

Z*(10)

*	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Kleinsche Vierergruppe

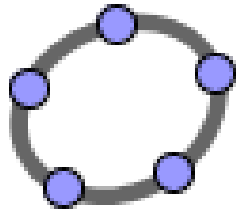
Z*(8)

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Zyklische Gruppe Ordnung 4

Gruppe: keine doppelten Werte
keine Nullen innen bei *
und Assozieativgesetz, nicht einfach zu sehen

Kryptografie: Wir brauchen Gruppen
weil die Inversen den Rückweg erlaube

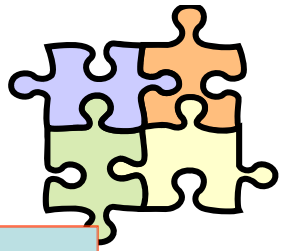


mehr Gruppen der Ordnung 4 gibt es nicht

Vier Studis helfen einander.

Four Studis help eachother.

4 Min



You calculate in the normal manner but in numbers
you can leave multiples of the modulo-number n everywhere.
You can add the modulo number n, if a result is negative.

Kopfrechnen
mental arithmetic

Muster
sample

$187 \cdot 203 \equiv_{20} 7 \cdot 3 \equiv_{20} 1$

$352 - 710 \equiv_{7} 2 - 3 \equiv_{7} -1 \equiv_{7} 6$

$993 \cdot 560 \equiv_{11}$

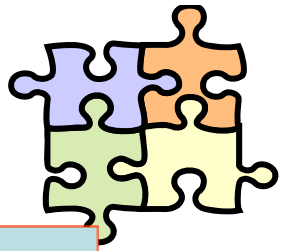
$17 + 22 + 13 + 551 \equiv_{5}$

$119 - 232 \equiv_{20}$

$12 \cdot 12 \cdot 12 \cdot 12 \equiv_{10}$

Vier Studis helfen einander.
Four Studis help each other.

4 Min



You calculate in the normal manner but in numbers
you can leave multiples of the modulo-number n everywhere.
You can add the modulo number n, if a result is negative.

Kopfrechnen
mental arithmetic

Muster
sample

$187 \cdot 203 \equiv_{20} 7 \cdot 3 \equiv_{20} 1$

$352 - 710 \equiv_{7} 2 - 3 \equiv_{7} -1 \equiv_{7} 6$

$993 \cdot 560 \equiv_{11} 3 \cdot 10 \equiv_{11} 30 \equiv_{11} 8$

$17 + 22 + 13 + 551 \equiv_{5} 2 + 2 + 3 + 1 \equiv_{5} 3$

$109 - 232 \equiv_{20} 9 - 12 \equiv_{20} -3 \equiv_{20} 17$

$12 \cdot 12 \cdot 12 \cdot 12 \equiv_{10} 2 \cdot 2 \cdot 2 \cdot 2 \equiv_{10} 16 \equiv_{10} 6$

Gleichungen? Equations?

$2 + x \equiv 0 \pmod{11}$

$2 \cdot x \equiv 7 \pmod{11}$

$8 + x \equiv 2 \pmod{10}$

$8 \cdot x \equiv 3 \pmod{10}$

$8 \cdot x \equiv 0 \pmod{10}$

$8 \cdot x \equiv 0 \pmod{5}$

Gleichungen? Equations?

$2 + x \equiv_{11} 0$ $x = 9$ weil $2 + 9 = 11 \equiv_{11} 0$

$x = -2 \equiv 9 \pmod{11}$

$2 \cdot x \equiv_{11} 7$ $x = 9$ weil $2 \cdot 9 = 18 \equiv_{11} 7$

only by trial and error

$8 + x \equiv_{10} 2$ $x = 4$

$8 \cdot x \equiv_{10} 3$ keine Lösung / no solution — Weil k*10+3 ungerade aber 8*x gerade

$\mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}$ hat außer 0 weitere

$8 \cdot x \equiv_{10} 0$ $x = 5$ weil $8 \cdot 5 = 40 \equiv_{10} 0$

Nullteiler!!!! zero divisor

$8 \cdot x \equiv_{5} 0$ keine Lösung / no solution

$\mathbb{Z}_5^* = \{1,2,3,4\}$ has no zero divisors because 5 is prime.

Was muss ich mir merken?

- Die **Ganzen Zahlen** sind $\mathbb{Z} = \{...-2,-1,0,1,2,3...\}$
- In der Kryptografie geht es um das **Rechnen modulo n** in der Menge $\mathbb{Z}_n = \{0,1,2,3,...,n-1\}$, der Menge der Reste.
- In der Kryptografie hat **n etwa 200 Stellen**. Zum Lernen nehmen wir kleine n und rechnen meist im Kopf.
- Hinter jeder Zahl r in $\mathbb{Z}_n$ muss man sich alle Zahlen vorstellen, die **denselben Rest beim Teilen durch n** ergeben. Sie ergeben sich aus r durch Addition eines beliebigen Vielfachen von n. Also r repräsentiert $z \cdot n + r \quad \text{mit} \quad z \in \mathbb{Z}$
  Das schreibt man so: $r \underset{n}{\equiv} z \cdot n + r$
- Im Beispiel $\mathbb{Z}_7 = \{0,1,2,3,...,6\}$

$3 \underset{7}{\equiv} z \cdot 7 + 3 \qquad 3 \underset{7}{\equiv} 1 \cdot 7 + 3 = 10 \qquad 3 \underset{7}{\equiv} 200 \cdot 7 + 3 = 143 \qquad 3 \underset{7}{\equiv} -1 \cdot 7 + 3 = -4$

What Shall I Have to Keep in My Mind?

- The i**ntegers** are this: $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, 3 \ldots\}$
- In cryptography one **calculate modulo n** in the set $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$, the set of residues, the set of rests.
- In cryptografie **n has ca. 200 digits**. to learn it, we take small modulo-numbers n and mostly we calculate by head.
- behind every number r in $\mathbb{Z}_n$ one must imagine alle numbers with the **same rest in division by n**.
  They are constructed from r by addition of an arbitrary multiple of n. So r represents $z \cdot n + r$ mit $z \in \mathbb{Z}$
  We write in this manner: $r \underset{n}{\equiv} z \cdot n + r$
- In example $\mathbb{Z}_7 = \{0, 1, 2, 3, \ldots, 6\}$

$3 \underset{7}{\equiv} z \cdot 7 + 3 \quad 3 \underset{7}{\equiv} 1 \cdot 7 + 3 = 10 \quad 3 \underset{7}{\equiv} 200 \cdot 7 + 3 = 143 \quad 3 \underset{7}{\equiv} -1 \cdot 7 + 3 = -4$

Uff, jetzt haben wir schon viel gelernt!

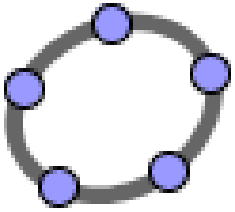
Ziel: Kryptografie verstehen

Weitere Überraschungen beim modulo-Rechen folgen!

Wow, We Have Learned Much in this Short Time!

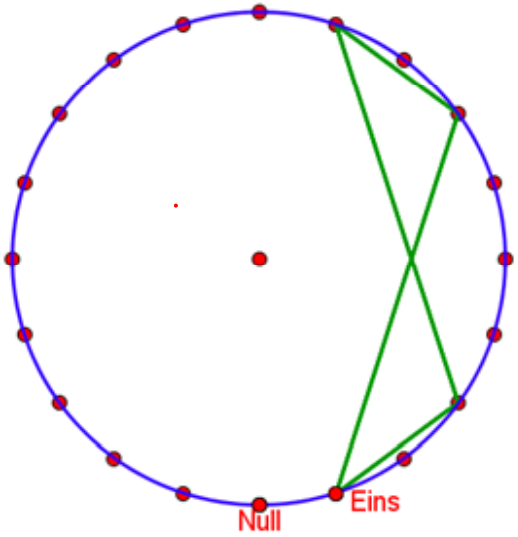
goal: to understand cryptography

Futher surprises with modulo-calculating!



Potenzen sind spannend

Die Potenzen von 3 modulo 20



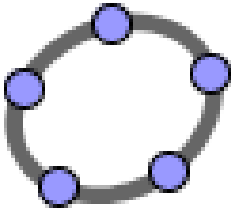
3 hat in Z (20) die **Ordnung 4,**

denn $3^4 \equiv_{20} 1$ 4minimal

Potenzen von 3 in Z = {1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,

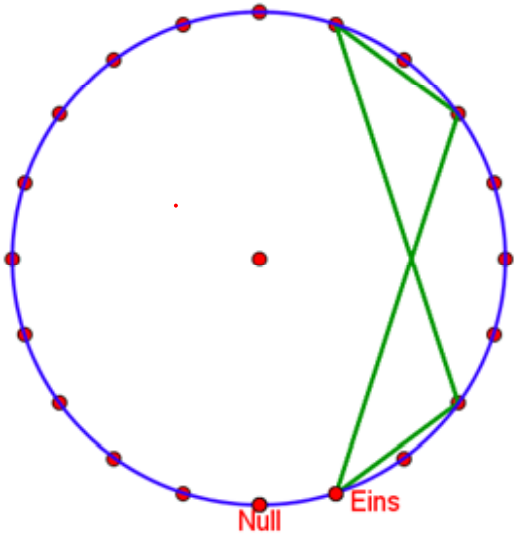
Potenzen von 3 in Z(20)= {1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1}

Nur Zahlen, deren Potenzen in Z(n) wieder 1 erzeugen sind brauchbar. Der kleinste Exponent k von a, mit $a^k \equiv_n 1$ heißt **Ordnung von a** modulo n.



Powers are exciting

The powers of 3 modulo 20



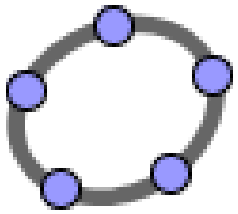
3 has in Z (20) the **Order 4,**

denn $3^4 \equiv_{20} 1$ 4 minimal

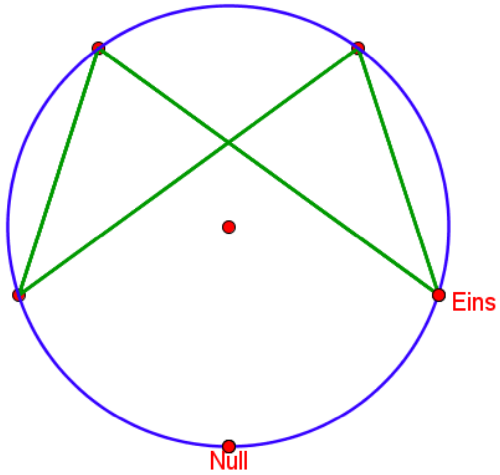
Potenzen von 3 in Z = {1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,

Potenzen von 3 in Z(20)= {1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1}

Numbers are only useful, if the powers in Z(n) equal 1 for any exponent. The smalest exponent k von a, mit $a^k \equiv_n 1$ is named **Order of a** modulo n.



Powers modulo n



$2^3 \underset{5}{\equiv} 8 \underset{5}{\equiv} 3$

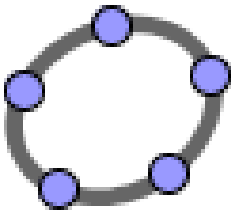
$2^4 = 2^3 \cdot 2 \underset{5}{\equiv} 3 \cdot 2 \underset{5}{\equiv} 1$ $\quad ord(2) = 4$ in $\mathbb{Z}_5$

Potenzen von 2 in Z = {1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048,

Potenzen von 2 in Z(5)= {1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1}

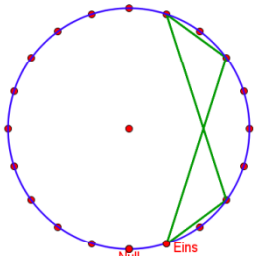
$(\mathbb{Z}_5, \cdot)$ $\quad 2^{50} \underset{5}{\equiv} \underbrace{2^{48}}_{1} \cdot 2^2 = 4$ weil $4 \mid 48$

$2^{7741} \underset{5}{\equiv} 2$ weil $4 \mid 7740$



Powers in Z(n)

The powers of 3 modulo 20



$3^4 \equiv_{20} 1$

$\mathbb{Z}(20)$

Potenzen von 3 in Z = {1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,

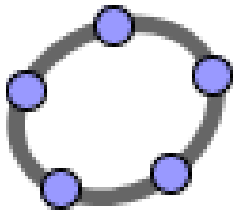
Potenzen von 3 in Z(20)= {1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1}

first 1 with $3^k \equiv_{20} 1 \quad k>0$

$3^{5000} \equiv_{20} 3^0 = 1$

k ist the order of 3 modulo 10

denn 4 teilt 5000



Powers in Z(n)

The powers of 3 modulo 20

$3^{5000} =$ 4.03899763* 10 ^ 2385

$\uparrow 3^{5000} \equiv 20$

Potenzen in Z(n)

Die Potenzen von 3 modulo 20

$3^{5000} = 4.03899763 \cdot 10^{2385}$

4038997629787155339700863409815084778394498166 7 7597637486231866281502184426316372440958999128 31
1222195708703712726440925298211274859178771 7 0338304034419302831610118 8129043164196698062
3569028664868962702914864744551077531848115736 77 6835487588472583 2109480816007929295655276317 11
040679841205338360656646359502423649284424518 05 9950783172484611404441399958188423268629895 33584
638540917303432618956468436 26746221768989753693 9 221538008683721591946 1 2033353214391787244913 6148
1975168349141 2486599141322487592379975054191594 7 12145231739 7071057126304566886323132371593790082
148550687072 96575317570265557373712948254293531 7 5800946829026948 0925112567372205422107870530515 95
8 0298123310985601213525552509973 2 3547989793769 5548807826632854936 2 708476932055774657608390589 22
819952696676524 9731286293737861965648227546419290429591462439 038555624893561619568785954150826921
89276329429991504770124701085279239460876 2 884487401091385748920627625211432517898560639974538965 9
2241444435083741307994418 053069747011639244992143617911 28 760664708496525819888322565 338880620792
9500332235059418 2854932910480899682575200047468631366224 75 6184671205687773557913094816 6 4752205737
72382760501729980370 7 18463030744130267276850859830224909045374931284637548474276 3 39644646276076892
228176452926495692268689787553685528221 7 4910148014846327742218968086229060583051969616187683845 99
28035 042990496058544913084722026162251885876962080530864632074 1 32617826126984984843534068119465 92
3915208768348376813643614830773356485 07 17770498917667601749081421415494578545 63 070674448088286 99
697448178044358744 48615007611528625846948651340208724838406865565811451847483786714575459963460 98
7986160817345593772637725343784722309807229968176006683894290612608864774111914141455 248988628956
8286295961333873938859213445898721760456679830 1986033599372533115655 3961929706704163556063532953648
893078691339202625369223335024104532599964353246882495329437068 81 6609394927886366404179543691065 67
50167596038501554362222214884786870393545144 578906190448059134680891645361639347000232719153886 67
88365255688115338002309292544972383140758664363656074559760858094370674300004274259183036385702 63
277678578732590453700918386680277827005016588188884730521045514996708836288180634799955911110684 9
9262389334270516368681934717001992202623320 857716933794168735052645498039818859137502378346871135
97326336004935631369982761000 01

$\uparrow$ $3^{5000} \underset{20}{\equiv} 1$