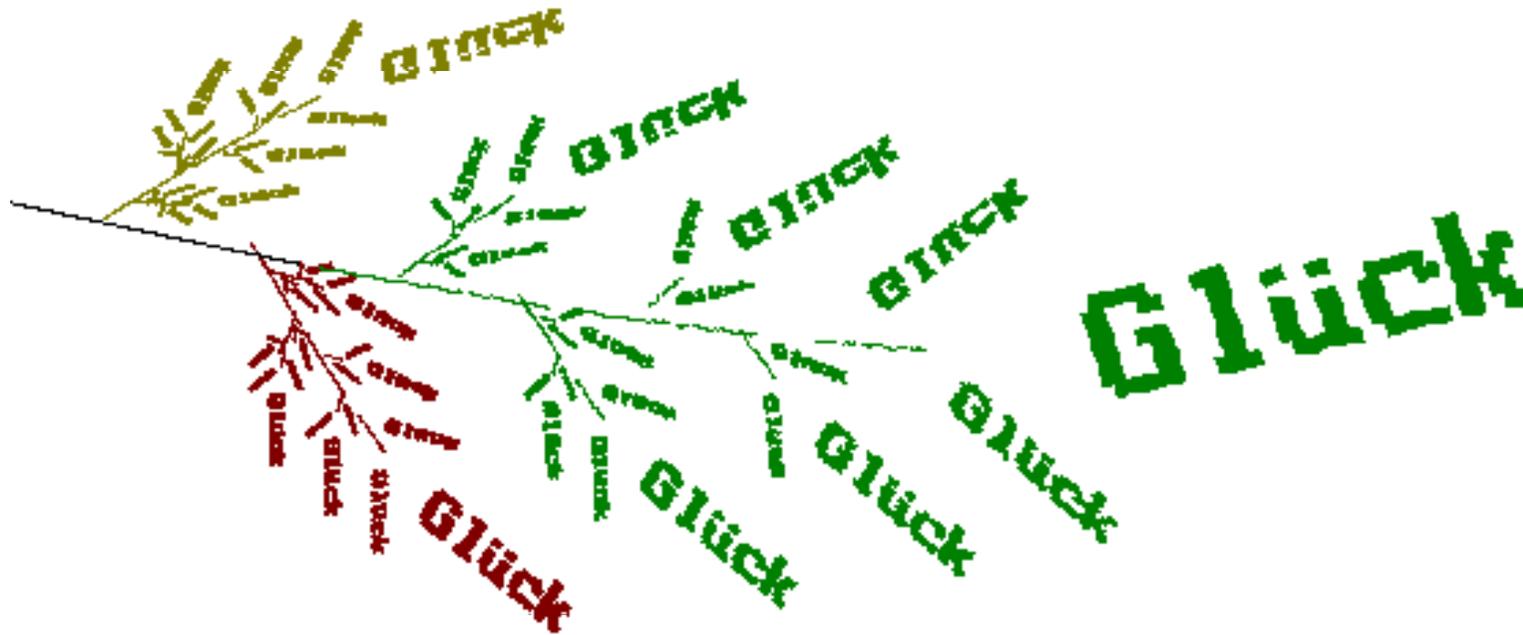


# Mathematik für alle



**LEUPHANA**  
UNIVERSITÄT LÜNEBURG



# Mathematik für Kinder

ganze Familie

**Entziffert die Botschaft:**



auf der Kinderseite  
einer Kundenzeitung



# Cäsarcode, Urtyp der Kryptografie

## MATHE

Schlüssel-  
Buchstabe

über das A stellen

Kryptogramm-Buchstaben



Klartext-Buchstaben

# Cäsarcode Bastelanleitung

MATHE  
DRKYV

Schlüssel-  
Buchstabe

über das A stellen

Kryptogramm-Buchstaben



Klartext-Buchstaben





# 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.

# 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

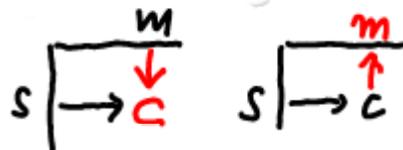
Klartext m 4735544239

Schlüssel s 2846935817

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

*frei erfunden*



# 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

**MATHE**

**4735544239**

Klartext m

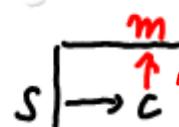
Schlüssel s

**2846935817**

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

65714  
+rechnen



modulo 10

# 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

MATHE

Klartext m 4735544239

Schlüssel s 2846935817

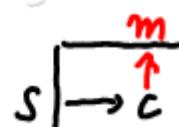
$C = 657147 \dots$

$C = 6781$

$S = 2846$

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



$m =$



# 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

MATHE

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

Klartext  $m$

4735544239

Schlüssel  $s$

2846935817

Ziffernweise ohne Übertrag addieren

$$c = 6571 \dots$$

$$m_z + s_z = c_z$$

Ziffernweise abziehen „modulo 10“

$$c_z - s_z = m_z$$

$$c = 67814697$$

$$s = 28469358$$

$$m = 4945$$

# 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

MATHE

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

Klartext m

4735544239

Schlüssel s

2846935817

Ziffernweise ohne Übertrag addieren

$C = 6571479046$

$$m_z + s_z = c_z$$

Ziffernweise abziehen „modulo 10“

$$C = 67814697$$

$$S = 28469358$$

$$c_z - s_z = m_z$$

$$m = 49455349$$

13

# Kryptografisches 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 ziffernweise „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 Kryptogramm  $c$  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

$$m_z + s_z = c_z$$

$$c_z - s_z = m_z$$

# Vierer-Übung



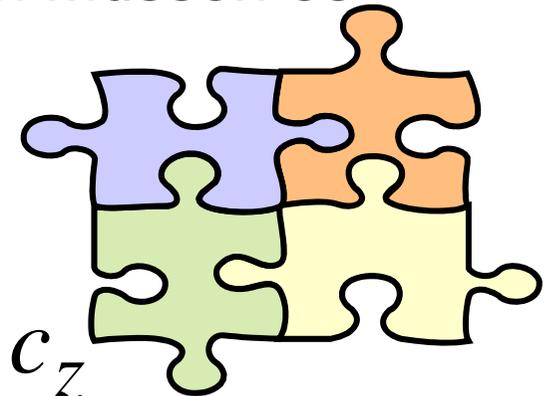
Vier Studis bilden eine Gruppe

Rechts-Unten sagt den Schlüssel an.  
8 Stellen zufällig

Die, die nebeneinander sitzen, verschlüsseln ein Wort mit 3 oder 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

$$m_z + s_z = c_z$$

$$c_z - s_z = m_z$$

# Was ist moderne Kryptografie?

matik: NAME:  
viss. Schein /Note  
chaftlicher Schein

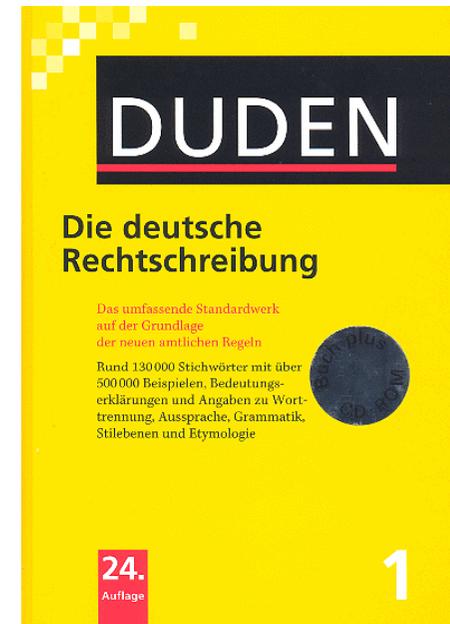
Von Erwachsenen mit  
Absicht erzeugte Kritzel-  
zeichnung (Duden) 

## , Kryptographie

Seite 1 / 2

10. Juli 2007

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



matik: NAME:  
viss. Schein /Note  
chaftlicher Schein

# , Kryptographie

Seite 1 / 2

10. Juli 2007

Von Erwachsenen mit  
Absicht erzeugte Kritz-  
zeichnung (Duden)



## 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  $n$

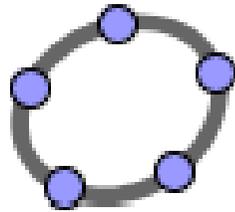
Das wird jetzt erklärt:

17





# modulo n: was bedeutet das?



$$n = 19$$

Die Vielfachen von  
8 modulo 19

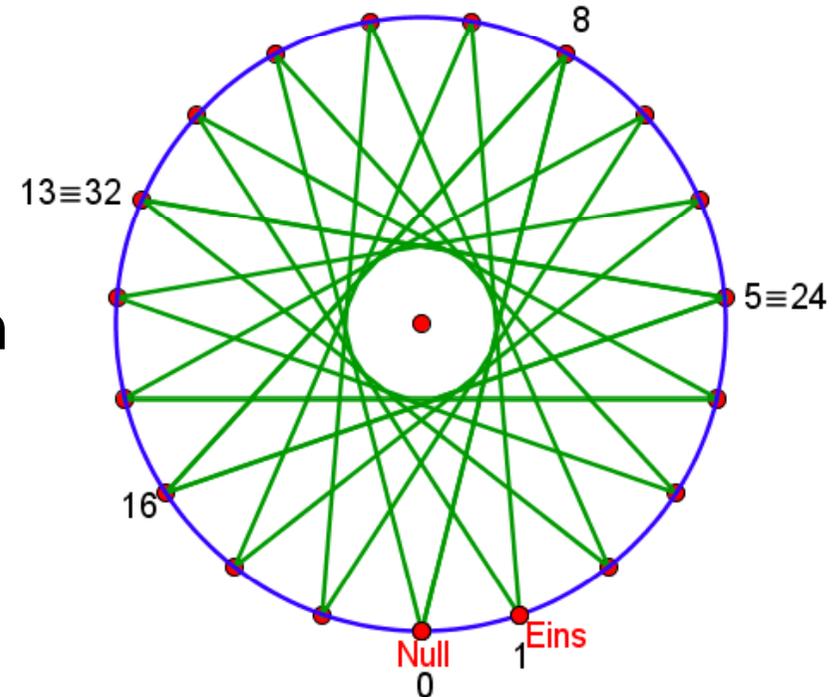
Keine Zahl  $1 < z < 19$  hat einen  
gemeinsamen Teiler mit 19.

Darum wird immer jeder  
Punkt erreicht.

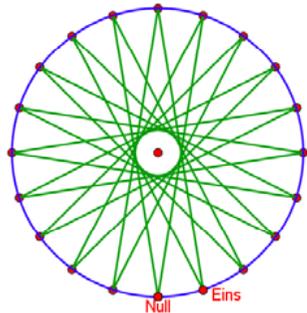
Es bleiben nie Punkte übrig.

## 19 ist eine Primzahl

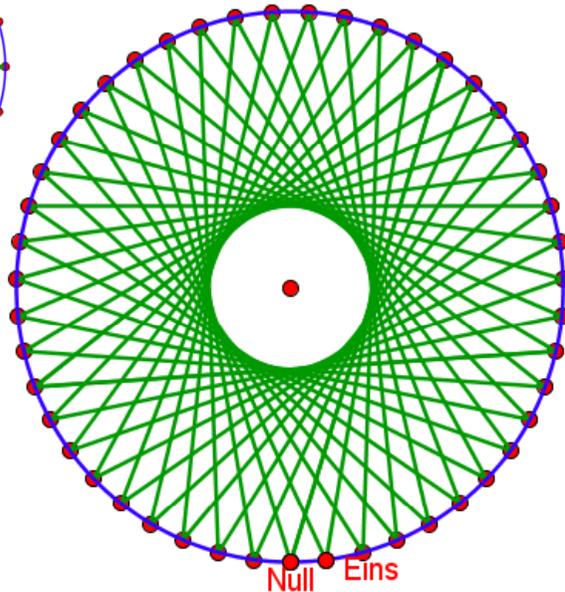
Eine Primzahl  $p$  ist eine Zahl mit genau zwei Teilern: 1 und  $p$ .



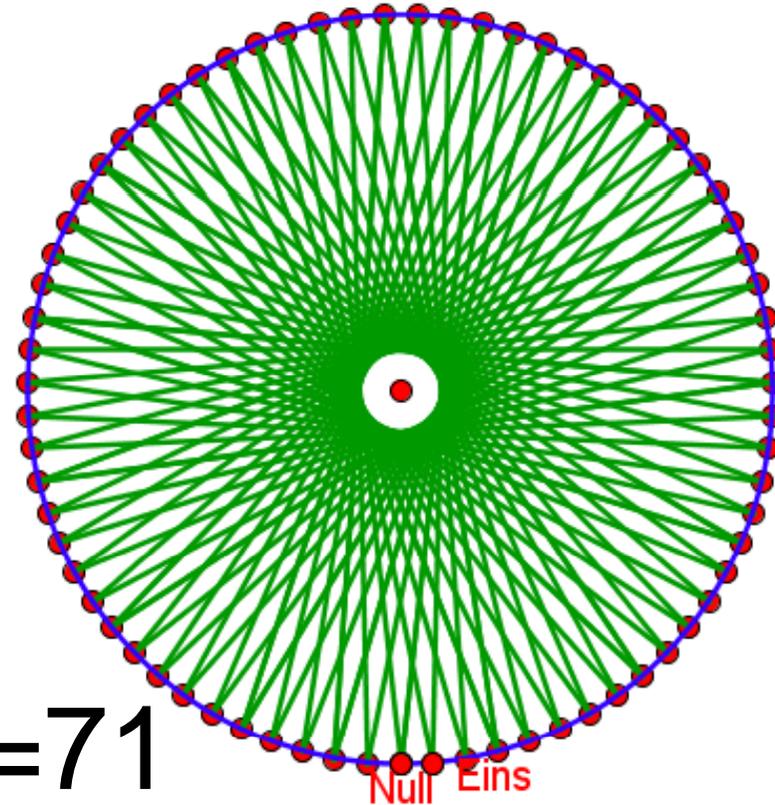
# Die Primzahlen und das modulo-n-Rechnen → Kryptografie



$n = 19$



$n = 47$   $n = 71$

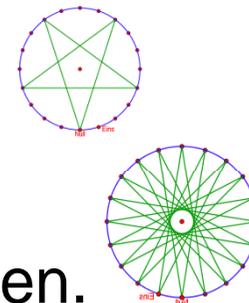


$n = 22154232101339012558196658176407559644$

**1068955439549124678505921927805529849767**

# Erklärung zur letzte Folie:

- Für jede Zahl  $n$  denkt man sich den Kreis der Zahlen als Punkte  $\{0,1,2,3,\dots n-1\}$  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  $n$  so viele Punkte haben, wie im Universum Atome (etwa  $10^{77}$ ) sind.



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

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

$$17 \equiv 2 \pmod{5}$$

5 heißt „Teiler“ oder „modulo-Zahl“

$$54 \equiv 10 \pmod{7}$$

$$54 \equiv 7 \pmod{7}$$

$$73 \equiv 11 \pmod{11}$$

$$777730 \equiv 11 \pmod{11}$$

$$113 \equiv 11 \pmod{11}$$

Ganze Vielfache von n  
weglassen!

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

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

$$17 \equiv 2 \pmod{5}$$

5 heißt „Teiler“ oder „modulo-Zahl“

Handwritten examples:

$$54 \equiv 4 \pmod{10}$$

$$54 \equiv 5 \pmod{7}$$

$$113 \equiv 3 \pmod{11}$$

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

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

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

Ganze Vielfache von n weglassen!

evt. schrittweise

# modulo-rechnen ist einfach

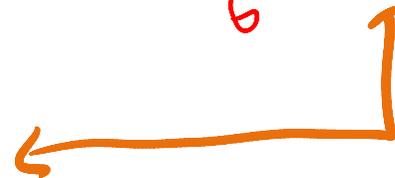
Man rechnet wie immer, lässt aber an beliebigen Stellen in Zahlen Vielfache der modulo-Zahl  $n$  weg oder addiert sie.

$$73 + 56 \equiv_{6} 129 \equiv_{6} 3$$

|||

|||

$$1 + 2 = 3$$



$$13 \cdot 37 \equiv_{5}$$

$$5713 \cdot 68217 \equiv_{5}$$

$$17 - 24 \equiv_{5} 2 - 4 \equiv_{5} -2 \equiv_{5} 3$$

# modulo-Rechnen ist einfach

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

$$73 + 56 \equiv_6 129 \equiv 3$$

III

III

$$1 + 2 = 3$$



$$13 \cdot 37 \equiv_5 3 \cdot 2 \equiv_5 6 \equiv_5 1$$

$$5713 \cdot 68217 \equiv_5 3 \cdot 2 \equiv_5 6 \equiv_5 1$$

$$17 - 24 \equiv_5 2 - 4 \approx -2 \equiv_5 3 \quad \text{weil: } -2+5=3$$

$\mathbb{Z}_m = \mathbb{Z}(m)$  ist die Menge der möglichen Reste beim Teilen durch  $m$ , is the set of all possible rests in division by  $m$

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

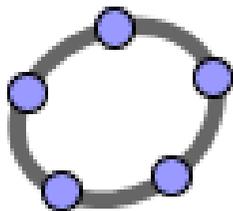


Excel  
Rest(17;5)  $\rightsquigarrow$  2

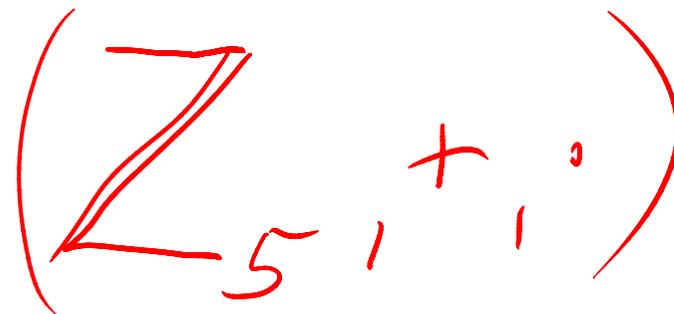
für  $17 \equiv 2 \pmod{5}$

Geogebra Mod [17,5]

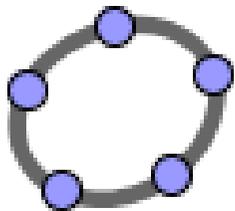
Verknüpfungstabeln  $\rightsquigarrow$  2



*	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



$\mathbb{Z}_m = \mathbb{Z}(m)$  ist die Menge der möglichen Reste beim Teilen durch  $m$ , is the set of all possible rests in division by  $m$



Excel  
Rest(17; 5)  $\rightsquigarrow$  2

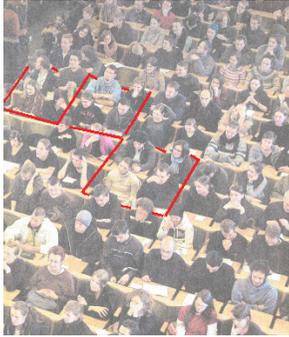
für  $17 \equiv 2 \pmod{5}$

Geometrie Mod [17, 5]

Verknüpfungstabeln  $\rightsquigarrow$  2

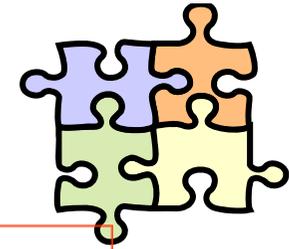
$\mathbb{Z}^*(10)$					$\mathbb{Z}^*(8)$						
*	1	3	7	9	*	1	3	5	7		
1	1	3	7	9	1	1	3	5	7	Gruppe: keine doppelten Werte	
3	3	9	1	7	3	3	1	7	5	keine Nullen innen bei *	
7	7	1	9	3	5	5	7	1	3	und Assoziativgesetz, nicht einfach zu sehen	
9	9	7	3	1	7	7	5	3	1	<b>Kryptografie: Wir brauchen Gruppen</b>	
										weil die <b>Inversen</b> den Rückweg erlaube	
Kleinsche Vierergruppe					Zyklische Gruppe Ordnung 4					mehr Gruppen der Ordnung 4 gibt es nicht	





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  $m$  everywhere. You can add the modulo number  $m$ , if a result is negative.

Muster  
sample

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

$$352 - 710 \equiv_7 2 - 3 \equiv_7 -1 \equiv_7 6$$

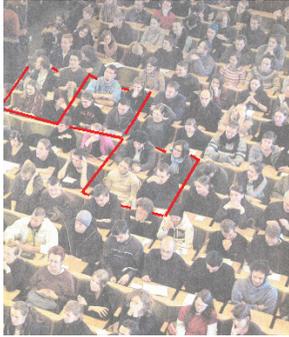
$$993 \cdot 560 \equiv_m$$

$$17 + 22 + 13 + 551 \equiv_5$$

$$109 - 232 \equiv_{20}$$

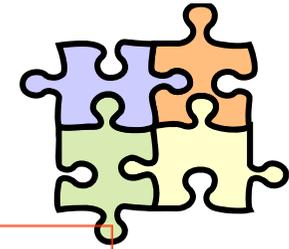
$$12 \cdot 12 \cdot 12 \cdot 12 \equiv_{10}$$

Kopfrechnen  
mental arithmetic



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  $m$  everywhere. You can add the modulo number  $n$ , if a result is negative.

Muster  
sample

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

$$352 - 710 \equiv_7 2 - 3 \equiv_7 -1 \equiv_7 6$$

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

$$17 + 22 + 13 + 551 \equiv_5 2 + 2 + 3 + 1 \equiv_5 3$$

$$109 - 232 \equiv_{20} 9 - 12 \equiv_{20} -3 \equiv_{20} 17 \quad 29 - 12 = 17$$

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

Kopfrechnen  
mental arithmetic

# Gleichungen? Equations?

$$2 + x \equiv 0$$

$$2 \cdot x \equiv 7$$

$$8 + x \equiv 2$$

$$8 \cdot x \equiv 3$$

$$8 \cdot x \equiv 0$$

$$8 \cdot x \equiv 0$$

# Gleichungen? Equations?

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

$$x = 9 \text{ weil } 2 + 9 = 11 \equiv 0 \pmod{11}$$

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

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

$$x = 9 \text{ weil } 2 \cdot 9 = 18 \equiv 7 \pmod{11}$$

only by trial and error

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

$$x = 4$$

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

keine Lösung  
no solution Weil  $k \cdot 10 + 3$  ungerade  
aber  $8 \cdot x$  gerade

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

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

$$x = 5 \text{ weil } 8 \cdot 5 = 40 \equiv 0 \pmod{10}$$

Nullteiler!!!!  
zero divisor

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

keine Lösung  
no solution in  $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$  hat keine Nullteiler  
weil 5 Primzahl ist.

# Was muss ich mir merken?

- Die **Ganzen Zahlen** sind  $\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, 3\dots\}$
- In der Kryptografie geht es um das **Rechnen modulo n** in der Menge  $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$ , 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  $z \cdot n + r$  mit  $z \in \mathbb{Z}$   
Das schreibt man so:
- Im Beispiel

$$r \equiv z \cdot n + r \pmod{n}$$

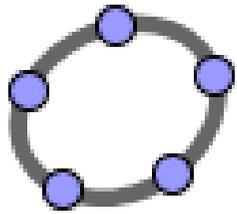
$$\mathbb{Z}_7 = \{0, 1, 2, 3, \dots, 6\}$$

$$\begin{array}{ccccccc} 3 \equiv & z \cdot 7 + 3 & 3 \equiv & 1 \cdot 7 + 3 = 10 & 3 \equiv & 200 \cdot 7 + 3 = 143 & 3 \equiv & -1 \cdot 7 + 3 = -4 \\ 7 & & 7 & & 7 & & 7 & \end{array}$$

Uff, jetzt haben wir  
schon viel gelernt!

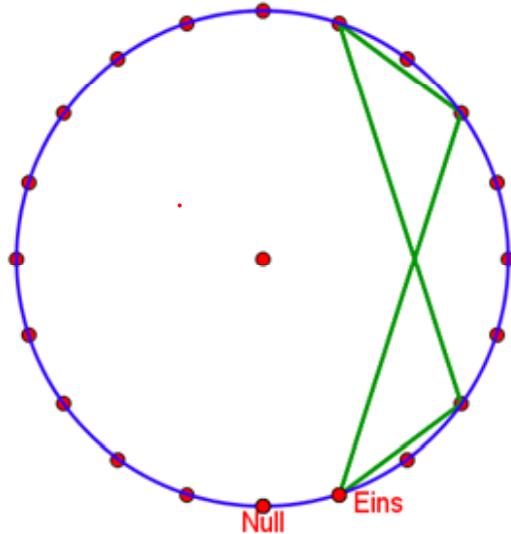
Ziel: Kryptografie verstehen

Weitere Überraschungen beim  
modulo-Rechen folgen!



# Potenzen sind spannend

Die Potenzen von 3 modulo 20



3 hat in  $\mathbb{Z}(20)$  die **Ordnung 4**,  
denn

$$3^4 \equiv 1 \pmod{20} \quad \text{4minimal}$$

Potenzen von 3 in  $\mathbb{Z} = \{1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, \dots\}$

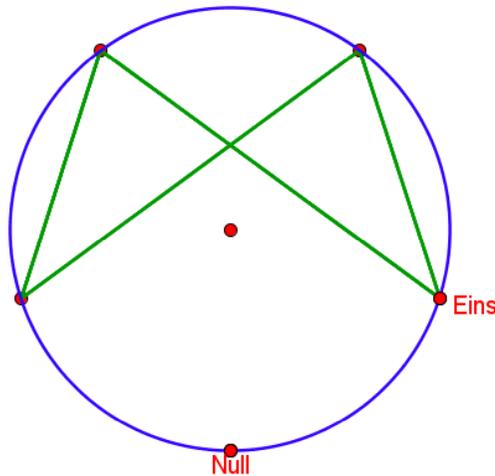
Potenzen von 3 in  $\mathbb{Z}(20) = \{1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1\}$

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

$$a^k \equiv 1 \pmod{n}$$

$k$  ist also die Länge des Polygons

# Rechnen mit Potenzen modulo n



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

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

Potenzen von 2 in  $\mathbb{Z} = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, \dots\}$

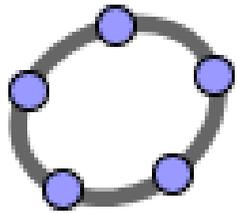
Potenzen von 2 in  $\mathbb{Z}(5) = \{1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1\}$

$$(\mathbb{Z}_5, \cdot) \quad 2^{50} \equiv \underbrace{2^{48}}_1 \cdot 2^2 = 4$$

weil  $4|48$

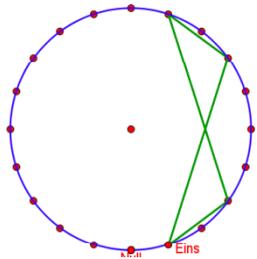
$$2^{7741} \equiv 2 \pmod{5}$$

weil  $4|7740$



# Potenzen in $\mathbb{Z}(m)$

Die Potenzen von 3 modulo 20



$$3^4 \equiv 1 \pmod{20}$$

$$\mathbb{Z}(20)$$

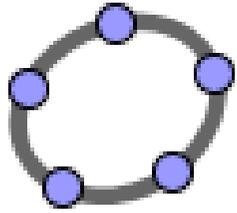
Potenzen von 3 in  $\mathbb{Z} = \{1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, \dots\}$

Potenzen von 3 in  $\mathbb{Z}(20) = \{1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1\}$   
*erste 1 mit*

$$3^{5000} \equiv 3^0 = 1 \pmod{20}$$

$3^k \equiv 1 \pmod{20} \quad k > 0$   
 $\Rightarrow 4$  ist die Ordnung von 3

denn 4 teilt 5000

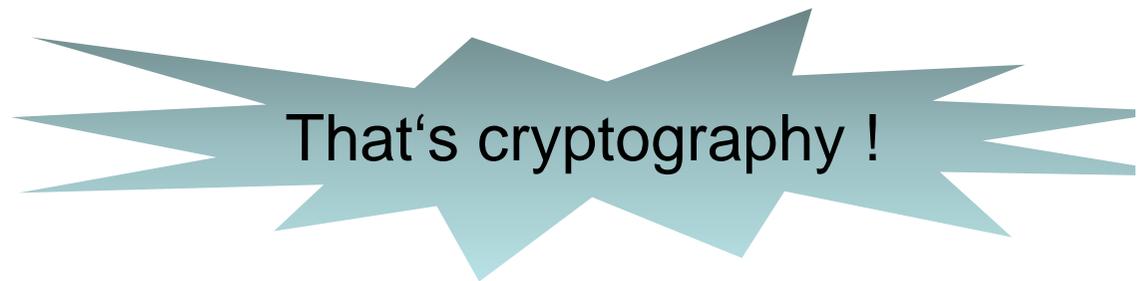


# Potenzen in $\mathbb{Z}(m)$

Die Potenzen von 3 modulo 20

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

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



40389976297871553397008634098150847783944981667 759763748623186628150218442631637244095899912831  
 12221957087037127264409252982112748591787717 0338304034419302831610118 8129043164196698062  
 356902866486896270291486474455107753184811573677 6835487588472583 210948081600792929565527631711  
 04067984120533836065664635950242364928442451805 9950783172484611404441399958188423268629895 33584  
 638540917303432618956468436 267462217689897536939 2215380086837215919461 20333532143917872449136148  
 1975168349141 24865991413224875923799750541915947 12145231739 7071057126304566886323132371593790082  
 148550687072 965753175702655573737129482542935317 5800946829026948 092511256737220542210787053051595  
 8 029812331048560119255525099732 3547989793769 55488078266328549362 70847693205577465760839058922  
 81995269667524 9731286293737861965648227546419290429591462439 038555624893561619568785954150826921  
 892763294299915047701247010852792394608762 8844874010913857489206276252114325178985606399745389659  
 224144433083741307994418 05306974701163924499214361791128 760664708496525819888322565 338880620792  
 950033223059418 285493291048089968257520004746863136622475 618467120568777735579130948166 4752205737  
 723827605017299803707184630307441302672768508598302249090453749312846375484742763 3964464627607892  
 22817645292649569222686897875536855282217 491014801484632774221896808622906058305196961618768384599  
 28035 0429904960585449130847220261622518858769620805308646320741 3261782612698498484353406811946592  
 3915208768348376813643614830773356485071777049891766760174908142141549457854563 07067444808828699  
 697448178044358744 4861500761152862584694865134020872483840686556581145184748378671457545996346098  
 798616081734559377263772534378472230980722996817600668389429061260886477411914141455 248988628956  
 82862959613387393885921344589872176045667983 198603359937253315655 3961929706704163556063532953648  
 89307869133920262536922333502410453259996435324688249532943706881 660939492788636640417954369106567  
 50167596038501554362222214884786870393545144 57890619044805913468089164536163934700023271915388667  
 8836525568811533800230929254497238314075866436365607455976085809437067430000427425918303638570263  
 2776785787325904537009183866802778270050165881888847305210455149967088362881806347999559111106849  
 9262389334270516368681934717001992202623320 857716933794168735052645498039818859137502378346871135  
 9732633600493563136998276100001

# Potenzen in Z(m)

Die Potenzen von 3 modulo 20

3<sup>5000</sup>

403899763 \* 10<sup>12385</sup>

