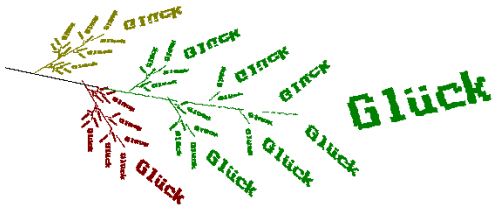
Mathematik für alle

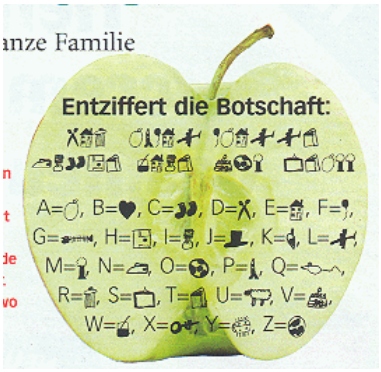
LEUPHANA
UNIVERSITÄT LÜNEBURG



Mathematik für Kinder

auf der Kinderseite
einer Kundenzeitung

Mathematik echt leicht



Cäsarcode, Urtyp der Kryptografie

MATHE

Schlüssel-
Buchstabe

über das A stellen

Kryptogramm-Buchstaben

NOPQRSTUVWXYZABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Klartext-Buchstaben

Cäsarcode Bastelanleitung

MATHE
DRKYV

Schlüssel-
Buchstabe

über das A stellen

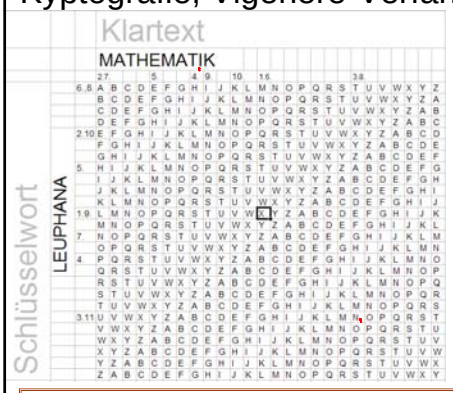
Kryptogramm-Buchstaben

NOPQRSTUVWXYZABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Klartext-Buchstaben

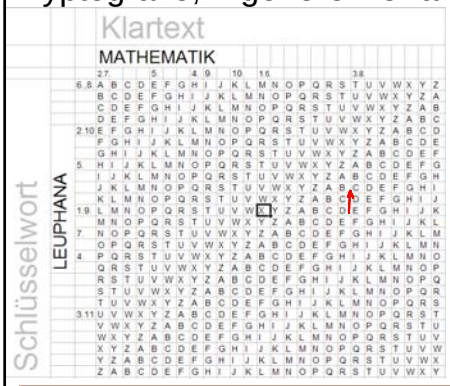
Kyptografie, Vigenère-Verfahren

um 1550



Kryptogramm:

Kyptografie, Vigenère-Verfahren



Kryptogramm:

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.

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

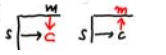
m \ s	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

MATHE

Klartext m 4735544239

Schlüssel s 2846935817

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

Vigenère-Chiffrierung mit Ziffern

m \ s	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

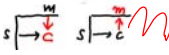
MATHE

Klartext m 4735544239

Schlüssel s 2846935817

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

Vigenère-Chiffrierung mit Ziffern

m \ s	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

Klartext m 4735544239

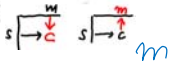
Schlüssel s 2846935817

C = 657147 .....

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

MATHE

Klartext m 4735544239

Schlüssel s 2846935817

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

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

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

$C = 6571479046$

$m_Z + s_Z = c_Z$

$c_Z - s_Z = m_Z$

Ziffernweise abziehen „modulo 10“

$C = 6781469 7$

$S = 2846 9358$

$m = 4945534 9$

Kyptografisches Protokoll

one-time-pad (dezimal)

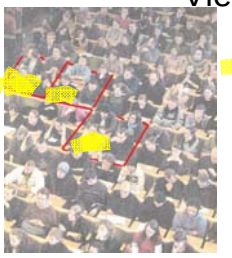
- Vorbereitungsphase
  Anton und Berta vereinbaren einen Schlüssel
- Anwendungsphase: Verschlüsselung (encryption)
  1. Anton übersetzt einen Klartext in eine Zahl m
  2. Er addiert ziffenweise „modulo 10“ (d.h. ohne Übertrag) den Schlüssel s
  3. Das Ergebnis c schickt er Berta.
- Entschlüsselung (decryption)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

$m_Z + s_Z = c_Z$

$c_Z - s_Z = m_Z$

Vierer-Übung

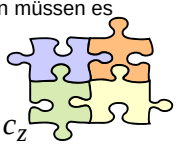


Vier Studis bilden eine Gruppe

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 Kyptografie?

natik: NAME:
viss. Schein /Note
chaftlicher Schein
Von Erwachsenen mit Absicht erzeugte Kritzel-Rechnung (Duden)
, Kryptographie
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)

natik: NAME:
viss. Schein /Note
chaftlicher Schein
Von Erwachsenen mit Absicht erzeugte Kritzel-Rechnung (Duden)
, Kryptographie
Seite 1 / 2 10. Juli 2007

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

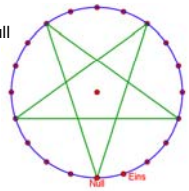
Das wird jetzt erkärt:

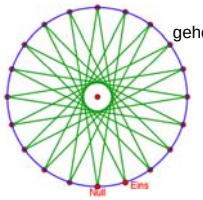
modulo 20
was bedeutet das?

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,

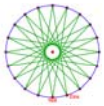
modulo n
was bedeutet das?

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

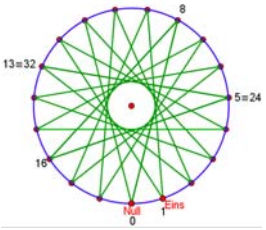
In Z(20) {0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12, 0, 8, 16, 4, 12,

19

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.

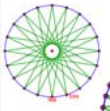
Es bleiben nie Punkte übrig.

19 ist eine Primzahl

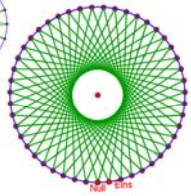
Eine Primzahl p ist eine Zahl mit genau zwei Teilern: 1 und p.

20

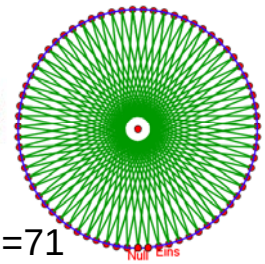
Die Primzahlen und das modulo-n-Rechnen →Kryptografie



n =19



n =47



n =71

n = **221542321013390125581966581764075596 44**

1068955439549124678505921927805529849767

21

Erklärung zur letzte 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 so viele Punkte haben, wie im Universum Atome (etwa 10^{77}) sind.

22

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

$17 \equiv 2 \mod 5$

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“

$54 \equiv 10 \equiv 7$

$54 \equiv 7$

$113 \equiv 11$

$73 \equiv 11$

$7777730 \equiv 11$

Ganze Vielfache von n weglassen!

23

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

$17 \equiv 2 \mod 5$

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“

$54 \equiv 10 \equiv 4$

$54 \equiv 7 \equiv 5$

$113 \equiv 11 \equiv 3$

$73 \equiv 11 \equiv 66+7 \equiv 7$

$7777730 \equiv 11 \equiv 7777700+30 \equiv 30 \equiv 22+8 \equiv 8$

Ganze Vielfache von n weglassen!

evt. schrittweise

24

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.

$73 + 56 \equiv_6 129 \equiv_6 3$

$1 + 2 = 3$

$13 \cdot 37 \equiv_5 3 \cdot 2 \equiv_5 6 \equiv_6 1$

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

$17 - 24 \equiv_5 2 - 4 \equiv -2 \equiv_5 3$ weil: -2+5=3

$\mathbb{Z}_m$ = 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) → 2

für $17 \equiv_5 2$

Geogebra Mod[17,5]

Verknüpfungstafeln → 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

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

$\mathbb{Z}_m$ =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) → 2

für $17 \equiv_5 2$

Geogebra Mod[17,5]

Verknüpfungstafeln → 2

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

Kopfrechnen
mental arithmetic

Muster
sample

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

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

$993 \cdot 560 \equiv_{11}$

$17 + 22 + 13 + 551 \equiv_5$

$109 - 232 \equiv_{20}$

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

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

Kopfrechnen
mental arithmetic

Muster
sample

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

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

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

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

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

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

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?

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

$2 \cdot x \equiv 7 \pmod{11}$ $x=9$ weil $8 \cdot 9 - 18 \equiv 7 \pmod{11}$

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*10+3 ungerade aber 8*x gerade

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

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

$8 \cdot x \equiv 0 \pmod{5}$ 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 $\mathbb{Z}=\{...-2,-1,0,1,2,3...\}$
- 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 $z \cdot n + r$ mit $z \in \mathbb{Z}$ Das schreibt man so: $r \equiv z \cdot n + r \pmod{n}$
- Im Beispiel

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

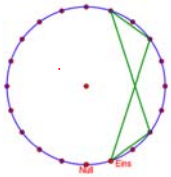
$3 \equiv z \cdot 7 + 3 \pmod{7}$ $3 \equiv 1 \cdot 7 + 3 = 10 \pmod{7}$ $3 \equiv 200 \cdot 7 + 3 = 143 \pmod{7}$ $3 \equiv -1 \cdot 7 + 3 = -4 \pmod{7}$

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 Z (20) die **Ordnung 4,** denn $3^4 \equiv 1 \pmod{20}$ 4minime

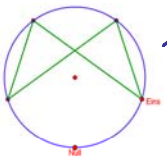
Potenzen von 3 in Z = {1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,

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 heißt **Ordnung von a** modulo n. $a^k \equiv 1 \pmod{n}$

k ist also die Länge des Polygons

Rechnen mit Potenzen modulo n



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

$2^4 = 2^3 \cdot 2 \equiv 3 \cdot 2 \equiv 1 \pmod{5}$ $ord(2)=4$ 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}

$(\mathbb{Z}_5, \cdot)$ $2^{50} \equiv 2^{48} \cdot 2^2 = 4 \pmod{5}$ weil $4 \mid 48$

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

Potenzen in Z(m)

Die Potenzen von 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}

erste 1 mit

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

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

denn 4 teilt 5000

Potenzen in Z(m)

Die Potenzen von 3 modulo 20

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

$3^{5000} \equiv_{20}$

That's cryptography !