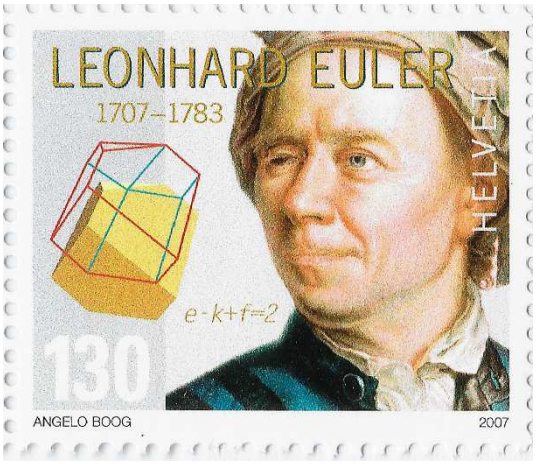
3. Teiler und teilerfremde Zahlen



Euler (1707 - 1783, Gymnasium und Universität in Basel, Professor für Physik und Mathematik in Petersburg und Berlin) war nicht nur einer der produktivsten Mathematiker der Menschheitsgeschichte, sondern auch einer der grössten Gelehrten aller Zeiten (Zitat seines Biographen Emil A. Fehlmann). Obwohl er 1740 an einem Auge, später völlig erblindete, entstand fast die Hälfte seiner Werke in dieser Zeit.

Die Eulersche $\varphi-$Funktion gibt die Anzahl aller natürlichen Zahlen an, die kleiner oder gleich der natürlichen Zahl n sind und deren ggT mit n gleich 1 ist, die also zu n teilerfremd sind.

Beispiele:
zu n = 6 sind 1 und 5 teilerfremd $\varphi(6) = 2$
zur Primzahl 5 sind 1, 2, 3, 4 teilerfremd $\varphi(5) = 4$

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

Eigenschaften:

a) $\varphi(n)$ gerade für n ≥ 3

b) $\varphi(p) = p-1$ für eine Primzahl p.

c) $\varphi(p\cdot q) = (p-1)\cdot(q-1)$ für Primzahlen p und q mit $p \neq q$

Beispiel zu c)
p = 3 und q = 5:
von den 15 Zahlen fallen weg, die Zahl 15 selbst, 4 Vielfache von 3 und 2 Vielfache von 5.
$\varphi(3\cdot 5) = 8 = (\varphi(3)-1)\cdot(\varphi(5)-1) = 2\cdot 4$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Beweis von c):
Von den p q natürlichen Zahlen ist die Anzahl aller Zahlen zu subtrahieren, die mit n einen ggT grösser als 1 haben:
p q selbst
q – 1 Vielfache von p. p, 2p, ... (q - 1)p
p – 1 Vielfache von q: q, 2q, .., (p - 1)q

Damit gilt:
$$\varphi(p\cdot q) = p\cdot q - 1 - (q-1) - (p-1) = p\cdot q - q - p + 1 = p\cdot(q-1) - (q-1) = (p-1)\cdot(q-1)$$

weitere Eigenschaften:

d) $\varphi(p^k) = p^{k-1}(p-1)$

e) $\varphi(ab) = \varphi(a)\cdot\varphi(b)$ sofern ggT(a,b) = 1

Beispiele:
$\varphi(19) = 18$ wegen b)
$\varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2) \cdot \varphi(3^2) = 1 \cdot 3^{2-1}(3-1) = 6$ mit b) und c)
$\varphi(16) = \varphi(2^4) = 2^3(2-1) = 8$ wegen d)

Als Vorbereitung zum Kleinen Fermat betrachten wir eine Tabelle von Potenzen $a^{\varphi(5)}$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$a^{\varphi(5)}$	1	16	81	256	625	1296	2401	4096	6561	10000	14641	20736	28561	38416	50625	65536	83521	104976	130321	160000
mod 5	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0

Es treten offenbar nur die Endziffern 0, 1, 5, 6 auf, d.h. die Fünferreste 0 oder 1. Der Rest 1 tritt genau dann auf, wenn als Basis kein Vielfaches von 5 gewählt wird.

Allgemein gilt der folgende

Kleine Fermatsche Satz:
Für jede Primzahl p und eine beliebige zu p teilerfremde Zahl a gilt:
$a^{p-1} \equiv 1 \bmod p$

3.1

Beim Beweis wird ein Kunstgriff verwendet, der zunächst an einem Beispiel illustriert wird. Multipliziert man die primen Reste der Primzahl p = 11 mit einem festen Faktor (im Beispiel mit a = 6), so entstehen erneut die primen Reste 1, 2, 3, …., 10, nicht unbedingt in der gleichen Reihenfolge (Gruppe der primen Restklassen).

p = 11	1	2	3	4	5	6	7	8	9	10
Faktor a =6	6	12	18	24	30	36	42	48	54	60
mod 11	6	1	7	2	8	3	9	4	10	5

bezüglich des Moduls p = 11 gilt also:
$1 \cdot 2 \cdot 3 \cdot \ldots \cdot 10 \equiv (1 \cdot 6) \cdot (2 \cdot 6) \cdot (3 \cdot 6) \cdot \ldots \cdot (10 \cdot 6) \quad mod\ 11$
Es kann nicht $a_i \equiv a_j \bmod p$ sein für $i \neq j$, denn dann müsste (i – j) durch p teilbar sein, was nicht möglich ist.

Beweis des kleinen Fermat:
allgemein gilt
$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv (1 \cdot a) \cdot (2 \cdot a) \cdot (3 \cdot a) \cdot \ldots \cdot \big((p-1) \cdot a\big) \quad mod\ p$
oder
$(p-1)! \equiv a^{p-1} \cdot (p-1)! \quad mod\ p$
oder
$(a^{p-1} - 1) \cdot (p-1)! \equiv 0 \quad mod\ p$
Da $(p-1)!$ nicht durch p teilbar ist, muss $a^{p-1} - 1$ durch p teilbar sein.□

Im folgenden Beispiel wird als Modul die Nichtprimzahl m = 6 mit $\varphi(6) = 2$ gewählt.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$a^{\varphi(6)}$	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225	256	289	324	361	400
mod 6	1	4	3	4	1	0	1	4	3	4	1	0	1	4	3	4	1	0	1	4

Im Beispiel ist zu erkennen, dass der kleine Fermatsche Satz verallgemeinert werden kann:

Satz von Euler-Fermat:
ggT(a, m) = 1 $\Rightarrow a^{\varphi(m)} \equiv 1 \mod m$ 3.2

Der Beweis des Euler-Fermat-Satzes verläuft entsprechend dem Beweis von 3.1.

Für ein vollständiges Repräsentantensystem aller $\varphi(m)$ primen Restklassen $b_1. b_2, \ldots., b_{\varphi(m)}$ mod m und a ∈ N mit ggT(a, m) = 1 gilt:
$b_1. b_2, \ldots., b_{\varphi(m)} = ab_1 \cdot ab_2 \cdot \ldots \cdot ab_{\varphi(m)}$ mod m.
Daher ist
$b_1. b_2, \ldots., b_{\varphi(m)} = ab_1 \cdot ab_2 \cdot \ldots \cdot ab_{\varphi(m)} = \left(a^{\varphi(m)} - 1\right) \cdot b_1. b_2, \ldots., b_{\varphi(m)} = 0 \mod m$

Da m das Produkt $b_1. b_2, \ldots., b_{\varphi(m)}$ nicht teilen kann, muss m ein Teiler von $\left(a^{\varphi(m)} - 1\right)$ sein.□

Die Umkehrung des Satzes von Fermat ermöglicht es, eine vorgegebene Zahl als zusammengesetzte Zahl zu erkennen:
Ist nämlich für eine Basis a die Zahl $a^{n-1} - 1$ nicht durch n teilbar, dann ist n zusammengesetzt.

Beispiel:
n = 4 und a = 3 $3^{4-1} - 1 = 26$ ist nicht durch 4 teilbar, also ist 4 keine Primzahl.

Ist aber umgekehrt $a^{n-1} - 1$ ein Vielfaches von n, so folgt daraus leider nicht, dass n eine Primzahl sein muss.

Beispiele:
a)
Zwar ist für n = 341
$2^{341-1} - 1 = 2^{340} - 1$ ein Vielfaches von 341.
Die Zahl 341 = 31·11 ist aber zusammengesetzt.
b)
n = 15
$4^{15-1} - 1 = 4^{14} - 1 = 268\,435\,455 = 15 \cdot 17895697$ ein Vielfaches 15.
Die Zahl 15 ist aber zusammengesetzt.

Definition:
Eine Zahl n, die den Fermattest für die Basis a besteht, obwohl sie zusammengesetzt ist, heisst Pseudoprimzahl.

Beim Fermattest stellt sich das Problem, den Rest einer grossen Zahl, z.B. 2^{341-1} bei einer Division zu bestimmen. Diese Aufgabe wird mit der Kongruenzrechnung erleichtert. Dazu wird der Exponenten im Dualsystem dargestellt und die Potenzen von 2 werden schrittweise quadriert.
$2^{341-1} = 2^{340} = 2^{256} \cdot 2^{64} \cdot 2^{16} \cdot 2^{4}$

In der Tabelle sind die Potenzen von 2 mod 341 dargestellt.

Die Rechnung wird vereinfacht, da nur die Reste quadriert werden müssen.
$2^{340} \equiv 64 \cdot 16 \cdot 64 \cdot 16 = 6553 \equiv 1 \mod 341$
Da $2^{340} - 1$ durch 341 teilbar ist, besteht also die Pseudoprimzahl 341 den Fermattest für die Basis 2. Die Zahl 341 = 11·31 ist aber zusammengesetzt.

Basis	Exponent	Zweierpotenz mod	Modul	Rest
2	1	2	341	2
	2	4	341	4
	4	16	341	**16**
	8	256	341	256
	16	65536	341	**64**
	32	4096	341	4
	64	16	341	**16**
	128	256	341	256
	256	65536	341	**64**
		1048576	341	**1**

Übungsaufgabe:
Es ist zu zeigen, dass die Pseudoprimzahl
$n = 561$ den Fermattest für die Basis 2 und 3 besteht.
Lösung:
Basis 2:
$2^{560} = 2^{512} \cdot 2^{32} \cdot 2^{16}$
$2^{560} \equiv 103 \cdot 103 \cdot 460 \equiv 1 \mod 561$
also ist $2^{560} - 1$ durch 561 teilbar, aber 561 = 3·11·17 ist zusammengesetzt.
Basis 3:
$3^{560} = 3^{512} \cdot 3^{32} \cdot 3^{16}$
$3^{560} \equiv 273 \cdot 273 \cdot 69 \equiv 1 \mod 561$
also ist $3^{560} - 1$ durch 561 teilbar.

Bemerkung: 561 ist sogar für jede andere Basis ebenfalls pseudoprim. Diese Eigenschaft ist aber sehr selten (→Carmichael-Zahlen).

4. Der RSA-Algorithmus, ein Verschlüsselungsverfahren

Das Prinzip:
Verschlüsselungsverfahren sind ein wichtiges Mittel des Datenschutzes. Das z.B. von der Telecom eingesetzte RSA-Verfahren wurde im Jahre 1977 von Ron Rivest, Adi Shamir und Leonard Adleman entwickelt.

Die grundlegende Idee:
Es ist einfach das Produkt n von zwei verschiedenen Primzahlen p und q zu berechnen. Hingegen ist es bei genügend grossen Zahlen mit mehr als 200 Stellen zurzeit praktisch unmöglich, aus dem Produkt n die Faktoren p und q zu gewinnen, d.h. n in Primfaktoren zu zerlegen.
Die beiden Seiten müssen keinen geheimen Schlüssel austauschen. Stattdessen besitzt jeder Teilnehmer einen eigenen öffentlichen Schlüssel c und einen dazu passenden geheimen Schlüssel d. Die öffentlichen Schlüssel aller Teilnehmer, die mit diesem Verfahren verschlüsseln, sind frei zugänglich, ebenso der Modul n.
Will nun Beat eine Nachricht m an Anna senden, so verschlüsselt Beat die Nachricht m mit dem öffentlichen Schlüssel c von Anna zu der Nachricht ist $\bar{m} = m^c$ mod n und versendet

diese. Anna entschlüsselt $\bar{m}$ mit ihrem geheimen Schlüssel d. Dieser ist so gewählt, dass $\bar{m}^d \equiv m \mod n$. Ein anderer Teilnehmer Carlo kann $\bar{m}$ nicht entschlüsseln, da er aus dem öffentlichen Schlüssel c von Anna den geheimen Schlüssel d von Anna nicht bestimmen kann.
Der RSA- Algorithmus kann auch zur elektronischen Unterschrift benutzt werden, indem Anna eine mit ihrem geheimen Schlüssel verschlüsselte Nachricht veröffentlicht. Erhält der Empfänger Beat mit Hilfe des öffentlichen Schlüssels von Anna daraus eine sinnvolle Nachricht, so kann diese nur von Anna stammen.

Das Verfahren wird an einem einfachen Beispiel illustriert:

Erzeugung des Schlüssels
1. Anna wählt zwei Primzahlen p und q (beide geheim) und berechnet das Produkt n = p·q (öffentlich) und $\varphi(n) = (p-1)\cdot(q-1)$ (geheim)
Beispiel:
p = 3, q = 5, also n = 3·15 = 15, $\varphi(15) = 2 \cdot 4 = 8$
2. Anna wählt eine Zahl c mit ggT(c, $\varphi(15)) = 1$ (c ist der öffentliche Schlüssel von Anna)
Beispiel:
c = 7, Kontrolle ggT(7, 15) = 1
3. Anna bestimmt ihren geheimen Schlüssel d so, dass $d \cdot c \equiv 1 \mod \varphi(n)$
Beispiel:
d = 7 Kontrolle: $7 \cdot 7 \equiv 1 \mod 8$
4. Anna gibt das Zahlenpaar (n, c) als ihre öffentlichen Schlüssel bekannt.
Beispiel:
n = 15, c = 7
5. Wenn Beat eine Nachricht an Anna schicken will, dann verwandelt er seine Nachricht in eine Zahl m ≤ n.
Beispiel:
m = 8

Verschlüsselung
6. Beat verschlüsselt seine Nachricht m mit dem öffentlichen Schlüssel c von Anna zu $\bar{m} \equiv m^c$ und sendet sie Anna.
Beispiel:
$\bar{m} \equiv 8^7 = 2097152 = 139810 \cdot 15 + 2 \equiv 2 \mod 15$.
Der geheime Text ist $\bar{m} = 2$

Entschlüsselung
7. Anna empfängt die Nachricht $\bar{m}$ und berechnet daraus die dechiffrierte Nachricht $\tilde{m} \equiv \bar{m}^d \equiv m$
Beispiel:
$\tilde{m} = 2^7 = 128 = 8 \cdot 15 + 8 \equiv 8$ damit ist $\tilde{m} = m$

Eine Bemerkung zu 3.
Die Gleichung $d \cdot c \equiv 1 \mod \varphi(n)$ kann mit dem erweiterten Euklidschen Algorithmus gelöst werden. Im Beispiel stimmt d mit c überein, was natürlich zu vermeiden ist.

Aufgabe:
Bekannt sind eine Zahl n = 119 öffentlich (119 = 7·17 bleibt geheim) und der öffentliche Schlüssel c = 37 von Anna.
Beat sendet eine Nachricht m an Anna. Er ordnet dazu den Buchstaben A, B, C, ..., X, Y, Z die Zahlen 1, 2, 3, ..., 24, 25, 26 zu (Variante: ASCII-Code) und verschlüsselt m mit dem öffentlichen Schlüssel c = 37 von A zur verschlüsselten Nachricht

$\overline{m} \equiv m^{37} \mod 119$

Anna erhält die folgende so verschlüsselte Botschaft $\overline{m}$ und versucht sie zu entschlüsseln:
108, 1, 13. 82, 117, 100, 36, 63, 4

Lösung:

Anna berechnet mit ihrem geheimen Schlüssel d = 13

$\overline{m}^{d} \equiv \left(m^{37}\right)^{13} = 108^{13} \mod 119$

Der Rest von 108^{13} mod 119 kann mit der folgenden Zerlegung bestimmt werden:

$108^{13} = 108^{8} \cdot 108^{4} \cdot 108^{1} \equiv 16 \cdot 4 \cdot 108 = 6912 \equiv 10 \mod 119$

Basis	Exp.	Potenz	mod 119
108	1	108	108
	2	11664	2
	4	4	4
	8	16	16
		6912	10

Damit ergibt sich m = 10.
Der erste entschlüsselte Buchstabe heisst also J.

Übungsaufgabe:
Wie heisst die entschlüsselte Nachricht?
JAMES BOND.

Fragen:
Wie kann der Hersteller des Verfahrens den geheimen Schlüssel d von Anna bestimmen?

Da ihm p = 7 und q = 17 bekannt sind, kann er $\varphi(n) = \varphi(p) \cdot \varphi(q) = 6 \cdot 16 = 96$ berechnen und die Lösung von $d \cdot c = d \cdot 37 \equiv 1 \mod 96$ mit dem Euklidschen Algorithmus bestimmen

$96 = 2 \cdot 37 + 22$ $\quad$ $22 = 96 - 2 \cdot 37$
$37 = 1 \cdot 22 + 15$ $\quad$ $15 = 37 - 1 \cdot 22$
$22 = 1 \cdot 15 + 7$ $\quad$ $7 = 1 \cdot 22 - 15$
$15 = 2 \cdot 7 + 1$ $\quad$ $1 = 15 - 2 \cdot 7 = 37 - 1 \cdot 22 - 2 \cdot (1 \cdot 22 - 15)$
$= 37 - 3 \cdot 22 + 2 \cdot 15 = 37 - 3 \cdot 22 + 2 \cdot (37 - 1 \cdot 22)$
$= 3 \cdot 37 - 5 \cdot 22 = 3 \cdot 37 - 5 \cdot (96 - 2 \cdot 37)$
$1 = \mathbf{13} \cdot 37 - 5 \cdot 96$

Der geheime Schlüssel von Anna ist also d = **13**.

Zur Begründung des Verfahrens:
Dass $\widetilde{m}$ mit m übereinstimmt, ist im Wesentlichen eine Folge des Fermatschen Satzes.
Anna erhält die verschlüsselte Nachricht
$\bar{m} \equiv m^c \ mod\, n$ oder auch $m^c = \bar{m} + j_1 \cdot n$
und bestimmt daraus
$\widetilde{m} = (m^c)^d \ \ mod\, n$
Es gilt $(m^c)^d \equiv m^{cd}$ mod n
denn nach dem Binomischen Lehrsatz ist
$\bar{m}^d = (m^c)^d = (\bar{m} + j_1 \cdot n)^d = \bar{m}^d + j_2 \cdot n = m^{cd} + j_2 \cdot n$ da ausser
$\bar{m}^d$ alle Summanden mindestens einen Faktor n enthalten.
Damit ist also $\bar{m}^d \equiv m^{cd} \ \ mod\, n$ oder $\bar{m}^d = m^{cd} + j_2 \cdot n$ 1)
und
$d \cdot c \equiv 1 \ \ mod\, \varphi(n)$ oder$c \cdot d = 1 + k \cdot \varphi(n)$ mit k∈N 2)
Aus 1) und 2) folgt
$\widetilde{m} = \bar{m}^d = m^{cd} + j_2 \cdot n \ = m^{1+k\cdot\varphi(n)} + j_2 \cdot n$ 3)
Sofern der ggT(m, $\varphi(n)$) = 1 ist, gilt nach dem
Kleinen Fermat 3.2
$m^{\varphi(n)} \equiv 1 \bmod n$ und damit auch für eine k–te Potenz
$m^{k\cdot\varphi(n)} \equiv 1 \bmod n)$ und nach Multiplikation mit m
$m^{k\cdot\varphi(n)+1} \equiv m \bmod n$ oder $m^{k\cdot\varphi(n)+1} = m + j_3 \cdot n$ 4)
Aus 4) eingesetzt in 3) ergibt:
$\widetilde{m} = \bar{m}^d = m^{1+k\cdot\varphi(n)} + j_2 \cdot n = m + j_3 \cdot n + j_2 \cdot n = m + j_4 \cdot n$
oder also $\widetilde{m} \equiv m \ \ mod\, n$ □

In der Praxis wird die Botschaft in eine Zahl m ≤ n umgeformt. Als Modul verwendet man Zahlen mit vielen Stellen, die aus genau zwei verschiedenen Primfaktoren bestehen. Es ist zwar einfach zwei Primzahlen zu multiplizieren, aber auch mit den leistungsfähigsten Computern schwierig, eine Zahl mit sehr vielen Stellen in Primfaktoren zu zerlegen. Die wesentliche Hürde für das Auffinden des geheimen Schlüssels d ist also die Primfaktorzerlegung der Zahl n, welche die Grundlage für die Bestimmung von $\varphi(n)$ bildet.

Beim folgenden Beispiel wurde die Software Maple verwendet.
Gewählte Primzahlen: p = 47 und q = 59 also $n = 47 \cdot 59 = 2773$
Wahl des öffentlichen Schlüssels: c = 17
Die in Viererblöcken gegliederte Nachricht lautet:
m = 0920 1900 0112 1200 0718 0505 1100 2015 0013 0500
Sie wird nun mit c = 17 verschlüsselt:
mod$(920^{17}, 2773)$ = 948
mod$(1900^{17}, 2773)$ = 2342
…
$\bar{m} \equiv m^{17}$ mod m : 948 2342 1084 1444 2663 2390 778 774 219 1655

Für das Entschlüsseln wird der geheime Schlüssel d benötigt mit der Eigenschaft
$d \cdot c \equiv 1 \ \ mod\, \varphi(n)$
$\varphi(2773) = 46 \cdot 58 = 2668$
d ist also Lösung der diophantischen Gleichung
$d \cdot 17 \equiv 1 \ \ mod\, 2668$ bzw. $d \cdot 17 + k \cdot 2668 = 1$

Der Maplebefehl
igcdex(17, 2668 , '*d*', '*k*')
ergibt zunächst den grössten gemeinsamen Teiler

$$1$$

und mit
d; *k*

$$157$$

$$-1$$

Die Lösungen für den geheimen Schlüssel d = 157 (und k = -1)

Variante:
msolve(17·d = 1, 2668) ergibt direkt d = 157

Damit kann nun die Nachricht entschlüsselt werden:

> **mod**$(948^{157}, 2773)$

$$920$$

mod$(2342^{157}, 2773)$

$$1900$$

…
Die entschlüsselte Nachricht heisst also
0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

Der Text ist nach der Stellung der Buchstaben im Alphabet codiert, wobei für einen Zwischenraum Nullen gesetzt sind.
09 ist der 9. Buchstabe im Alphabet also i, der 20. ist t, somit ergibt sich als Klartext das Zitat, das Shakespeare dem Julius Cäsar in den Mund legte:

Ist all greek to me
Quelle: Markus Paul TI Nachrichten

Das folgende Maple-Beispiel zeigt, dass die bisher verwendeten Primzahlen für eine Verschlüsselung viel zu klein sind, denn die Software benötigt für die Zerlegung der Zahl n = p·q in Primfaktoren weniger als eine Sekunde. Mit den Primfaktoren ist aber der geheime Schlüssel bereits geknackt.

```
> t1 := time( );
  z := rand( );
  p := nextprime(z);
  q := nextprime(z^2);
  n := p*q;
```

$$t1 := 1.359$$

$$z := 118191465299$$

$$p := 118191465311$$

$$q := 13969222469524721159473$$

$$n := 1651042872928472835576800778541103$$

```
> ifactor(n); "n in Primfaktoren zerlegen"
```

$$(118191465311)\ (13969222469524721159473)$$

```
> t2 := time( ) - t1
```

$$t2 := 0.078$$

Näheres zum RSA-Verfahren siehe
https://de.wikipedia.org/wiki/RSA-Kryptosystem.

Übungsaufgabe:
Anna stellt sich einen RSA-Schlüssel her.
Sie wählt dazu die zwei Primzahlen p =19 und q = 23 (hält beide geheim) und berechnet das Produkt n = 437 (öffentlich) und $\varphi(437) = 18 \cdot 22 = 396$ (geheim) und die Zahl c = 281 als ihren öffentlichen Schlüssel.
Anna gibt Beat das Zahlenpaar n= 437 und c = 281 als ihre öffentlichen Schlüssel bekannt.

a) Welcher geheime Schlüssel d passt zu Annas öffentlichem Schlüssel?
b) Beat schickt Anna die verschlüsselte Nachricht 224.Wie lautet die dechiffrierte Nachricht?

Lösung:
a)
d muss die Bedingung erfüllen $d \cdot 281 \equiv 1 \mod 396$
Mit dem Gausschen Algorithmus erhält man d = 365
b)
Wegen
$\widetilde{m} \equiv \bar{m}^d \equiv m$ ergibt $\widetilde{m} = 224^{365} \equiv 401 = m \bmod 396$
erhält man die gesuchte Nachricht m = 401.