§2. Kongruenzen

Seien $n, a, b \in \mathbb{Z}$. Notation: $a \equiv b \pmod n :\Leftrightarrow n \mid a-b$

"a kongruent b modulo n"

$a \equiv b$ definiert eine Äquivalenzrelation auf $\mathbb{Z}$:

reflexiv: $a \equiv a$, denn: $n \mid a-a$

symmetrisch: $a \equiv b \Rightarrow b \equiv a$, denn: $n \mid a-b \Rightarrow n \mid -(a-b) = b-a$

transitiv: $a \equiv b$ und $b \equiv c \Rightarrow a \equiv c$, denn: $n \mid a-b$ und $n \mid b-c$

$\Rightarrow n \mid (a-b)+(b-c)$

$a \equiv b \pmod n$ bedeutet: Bei Division mit Rest durch n, also

$a = na' + r(a)$ und $b = nb' + r(b)$ gilt $r(a) = r(b)$ nachprüfen

Die Äquivalenzklassen (was ist das?) heißen auch Restklassen.

Notation: $\bar{a} = \{b \in \mathbb{Z} : a \equiv b \pmod n\}$ ist die Restklasse von

$\bar{a} = \{a, a+n, a+2n, \dots\} \cup \{a-n, a-2n, \dots\}$

Dann gilt: $\bar{a} = \overline{a+kn}$ $\forall k \in \mathbb{Z}$ warum?

und $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \dots \cup \overline{n-1}$ (disjunkte Vereinigung)

Notation für die Menge der Restklassen modulo n:

$\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$\mathbb{Z}/n\mathbb{Z}$ ist eine abelsche Gruppe mit Addition $\bar{a}+\bar{b} := \overline{a+b}$

Die Addition ist wohldefiniert: $\bar{a} = \bar{c} \Rightarrow n \mid a-c$, $\bar{b} = \bar{d} \Rightarrow n \mid b-d$

$\Rightarrow n \mid (a-c)+(b-d) = (a+b)-(c+d) \Rightarrow \overline{a+b} = \overline{c+d}$ ✓

neutrales Element: $\bar{0}$

invers zu $\bar{a}$: $-\bar{a} = \overline{n-a}$

assoziativ: $\bar{a}+(\bar{b}+\bar{c}) = \overline{a+b+c} = (\bar{a}+\bar{b})+\bar{c}$

abelsch: $\bar{a}+\bar{b} = \overline{a+b} = \bar{b}+\bar{a}$

nachprüfen

Verknüpfungstafel für $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/5\mathbb{Z}$

Kongruenzen darf man mit ganzen Zahlen multiplizieren:

$a \equiv b \pmod n \Rightarrow la \equiv lb \pmod n$ für $l \in \mathbb{Z}$

aber im Allgemeinen nicht kürzen: $la \equiv lb \pmod n$

$\not\Rightarrow a \equiv b \pmod n$

Gegenbeispiel?

Kürzen ist erlaubt, wenn der zu kürzende Faktor teilerfremd zu n ist:
$ab \equiv ac \pmod n$ und $ggT(n,a) = 1 \Rightarrow b \equiv c \pmod n$
$= (n,a)$ wie folgt das aus einem Ergebnis in Kapitel 1?

Theorie der Kongruenzen: Carl Friedrich Gauss (1801), Disquisitiones Arithmeticae
vorherschon: Goldbach (1730)

Chin Chiu-shao (1247), Mathematische Abhandlung in 9 Kapiteln

Warum betrachtet man Kongruenzen?

- $\mathbb{Z}/2\mathbb{Z} = \{$gerade, ungerade$\} \rightsquigarrow$ Regeln für Addition, Multiplikation
- Teilbarkeitsregeln, z.B durch 3: $a = a_0 + a_1 \cdot 10 + a_2 \cdot 100 + -$, alle $a_i \in \{0, \dots, 9\}$ (Dezimalentwicklung), $10 \equiv 1 \pmod 3$, $(10,3) = 1 \Rightarrow 100 \equiv 10 \equiv 1 \pmod 3$, $10^e \equiv 1 \pmod 3 \; \forall e \Rightarrow a \equiv a_0 + a_1 + -$, d.h. a ist kongruent zur Summe der Ziffern in der Dezimalentwicklung. Insbesondere: $3 \mid a \Leftrightarrow 3 \mid (a_0 + a_1 + -)$
  Teilbarkeit durch 9: analog?
  Teilbarkeit durch 11: $10 \equiv -1 \pmod{11}$ (warum?) $\Rightarrow 100 \equiv 1 \pmod{11}$ usw
  $\Rightarrow a \equiv a_0 - a_1 + a_2 - a_3 + a_4 \pm - \pmod{11}$ gilt $11 \mid 123453$?
- allgemeine Teilbarkeitsaussagen:
  $17^{22} \equiv 1 \pmod{23}$ nachprüfen und verallgemeinern! (oder: abwarten)
- Verschlüsselung von Nachrichten, Kryptographie (Beispiel folgt)

"Gleichungen" für Kongruenzen: (zum Beispiel) n fest, $a, b \in \mathbb{Z}$, $ax \equiv b \pmod n$, gesucht ist x
Das bedeutet $ax - b \equiv 0 \pmod n$, d.h. $\exists y: ax - b = ny$ bzw $ax - ny = b$
Nach Kapitel 1 ist das für alle b lösbar, wenn $ggT(a,n) = 1$ bzw für festes b genau dann, wenn $ggT(a,n) \mid b$.
Direkte Rechnung: Sei $ggT(a,n) = 1$. Wenn x durch $\{\bar{0}, \dots, \overline{n-1}\}$ läuft, läuft auch ax durch ganz $\mathbb{Z}/n\mathbb{Z}$, denn: Falls nicht $\exists x_1 \neq x_2$ mit $ax_1 \equiv ax_2$.
Aber $(a,n) = 1 \Rightarrow$ Kürzen ist erlaubt, also $x_1 \equiv x_2$ ↯ $\Rightarrow \exists x: ax \equiv b \pmod n$
Der euklidische Algorithmus wird also nicht gebraucht.

Wenn $n=p$ prim ist, gilt immer $(a,n)=1$ für $a\neq 0$

$\Rightarrow \forall b\ \exists x: ax\equiv b \pmod p$. Z.B. $b=1$: $\exists x$ mit $ax\equiv 1 \pmod p$, d.h. die Restklasse a hat ein Inverses.

Folgerung: $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper. Axiome prüfen

Wenn $n=c\cdot d$ zusammengesetzt ist ($c,d\geq 2$, $<n$), dann ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper: c invertierbar, d.h. $\exists x: cx\equiv 1 \pmod n \Rightarrow \underbrace{cd}_{n} x\equiv d \pmod n$

$\Rightarrow d\equiv 0 \pmod n$ ↯

Gegeben x: betrachte die Restklassen von $x, x^2, \ldots \pmod n$. Nur endlich viele sind verschieden $\Rightarrow \exists h,j$ mit $h<j$: $x^j\equiv x^h \pmod n$. Falls $ggT(x,n)=1$:

Kürzen $\Rightarrow x^{j-h}\equiv 1 \pmod n$. $\Rightarrow \exists k$ minimal mit $x^k\equiv 1 \pmod n$.

k heißt die (multiplikative) Ordnung von x. Notation: $ord(x)$

Beispiel für $n=11$: $ord(3)$?

$x^{ord(x)}\equiv 1 \pmod n$

Für ℓ beliebig gilt: $x^\ell\equiv 1 \pmod n \Leftrightarrow ord(x) \mid \ell$ Beweis?

Spezialfall: $n=p$ prim, $x\not\equiv 0 \Rightarrow x^2\not\equiv 0$ usw, alle x^k haben Restklassen $\neq \bar{0}$

2.1 Theorem (Kleiner Satz von Fermat, 1640): Sei p eine Primzahl, $a\in\mathbb{Z}$.

Dann gilt $a^p\equiv a \pmod p$. Falls $p\nmid a$, gilt $a^{p-1}\equiv 1 \pmod p$.

Beispiel: $17^{22}\equiv 1 \pmod{23}$

Erster Beweis (Leibniz): $a=\overbrace{1+1+-+1}^{a \text{ Summanden}}\Rightarrow$

$a^p=(1+1+-+1)^p=1^p+1^p+-+1^p+$ Terme, die durch p teilbar sind

$\Rightarrow a^p\equiv a \pmod p$ (warum? a Summanden)

Kürzen $\Rightarrow a^{p-1}\equiv 1 \pmod p$ falls $ggT(a,p)=1$ □

Zweiter Beweis: $1, 2, \ldots, p-1$ repräsentieren die Restklassen $\neq \bar{0}$

Für $(a,p)=1$: $a, 2a, 3a, \ldots, (p-1)a$ repräsentieren diese Restklassen auch (da Kürzen möglich ist)

Also: $1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)\equiv \underbrace{a\cdot 2a\cdot 3a\cdot\ldots\cdot(p-1)a}_{=1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)\cdot a^{p-1}} \pmod p$

Kürzen $\Rightarrow 1\equiv a^{p-1} \pmod p$. (Der andere Fall $p\mid a$ ist klar) □

$(\mathbb{Z}/p\mathbb{Z})^*$

Dritter Beweis (algebraisch): $(\mathbb{Z}/p\mathbb{Z} - \{0\}, \cdot)$ ist eine (multiplikative) Gruppe. $H := \{\bar{a}, \bar{a}^2, \dots\}$ ist die von $\bar{a}$ erzeugte Untergruppe.
Satz von Lagrange $\Rightarrow$ $|H|$ teilt $|\mathbb{Z}/p\mathbb{Z}^*| = p-1$
wie in jeder Gruppe: $a^{|H|} = 1$, d.h. $\operatorname{ord}(a) \mid \operatorname{ord}(H)$
$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$ □

Die Ordnung von a kann kleiner sein als $p-1$, dessen Teiler sie ist.
Beispiel für $p=7$?

Der zweite (und der dritte) Beweis lassen sich verallgemeinern.
2.2 Definition: Die Eulersche φ-Funktion ist definiert durch
$\varphi: \mathbb{Z} \to \mathbb{N}$, $\varphi(n) = |\{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \operatorname{ggT}(a,n) = 1\}|$ wohldefiniert?
Beispiel: $n = p$ prim $\Rightarrow \varphi(p) = p-1$ noch prüfen
2.3 Theorem (Satz von Euler, 1760): Seien $n, a \in \mathbb{Z}$ mit $\operatorname{ggT}(a,n) = 1$. Dann gilt $a^{\varphi(n)} \equiv 1 \pmod{n}$.
(Daraus folgt 2.1 als Spezialfall. wie?)
Beweis: Modifikation des zweiten Beweises von 2.1.
Sei $\ell = \varphi(n)$ und $k_1, \dots, k_\ell$ Repräsentanten der zu n teilerfremden Restklassen.
$(a,n) = 1 \Rightarrow \bar{a}$ invertierbar in $\mathbb{Z}/n\mathbb{Z}$, d.h. die Kürzungsregel gilt
$\Rightarrow ak_1, \dots, ak_\ell$ sind auch Repräsentanten dieser Restklassen
$\Rightarrow k_1 \cdots k_\ell \equiv ak_1 \cdots ak_\ell \pmod{n} \Rightarrow 1 \equiv a^\ell \pmod{n}$ (mit $\ell = \varphi(n)$)
$= k_1 \cdots k_\ell \cdot a^\ell$ □

Kann man $\varphi(n)$ ausrechnen?
Wenn n gegeben ist, kann man die Multiplikation in $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ bestimmen. Damit erhält man $\varphi(2) = 1$ ($\bar{1}$ ist invertierbar)

$\varphi(3) = 2$ $(\bar{1}, \bar{2})$ $\quad$ $\varphi(6) = 2$ $(\bar{1}, \bar{5})$
$\varphi(4) = 2$ (?) $\quad$ $\varphi(20) = 8$ $(\bar{1}, \bar{3}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{17}, \bar{19})$
$\varphi(5) = 4$ (?)

Welche Regeln stecken dahinter?

2.4 Proposition: Die Eulersche φ-Funktion erfüllt:

(a) $\varphi(n) = n-1$, wenn $n = p$ prim

(b) $\varphi(p^a) = p^a - p^{a-1}$, wenn p prim und $a \geq 1$

(c) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, falls $(a,b) = 1$

Beispiel, daß das falsch ist ohne die Voraussetzung?

(d) $\varphi(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_r^{a_r} - p_r^{a_r-1})$, wenn $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen sind und $a_1, \ldots, a_r \in \mathbb{N}$

(e) $\sum_{d|n} \varphi(d) = n$ für jedes n

$\leftarrow$ d läuft durch alle positiven Teiler, inklusive 1 und n

Beweis: (a) $1, \ldots, p-1$ sind alle zu p prim teilerfremd

(b) Der einzige Primteiler von p^a ist p selbst. Für b mit $p \nmid b$ gilt $(b, p^a) = 1$. Welche $b \leq p^a$ erfüllen $(b, p^a) \neq 1$? Alle Vielfachen von p, d.h. alle $p \cdot c$ mit $1 \leq c \leq p^{a-1}$, d.h. $p, 2p, \ldots, p^2, p^2+p, \ldots$ bzw $p \cdot 1, p \cdot 2, p \cdot 3, \ldots, p \cdot p, p(p+1), \ldots$

$\Rightarrow \varphi(p^a) = p^a - p^{a-1}$

(c) ist der schwierigste Teil. Sei $(a,b) = 1$. Für $1 \leq x \leq a$ und $1 \leq y \leq b$ gilt: $(x,a) \neq 1$ oder $(y,b) \neq 1 \Rightarrow (xy, ab) \neq 1$. warum ist das hier relevant?

Aber nicht jede Zahl $z \leq ab$ ist ein Produkt $z = xy$. Deshalb schreiben wir die Bedingungen, wann eine Zahl zu $\varphi(a \cdot b)$, $\varphi(a)$ oder $\varphi(b)$ beiträgt, um in Kongruenzen: Die Grundidee ist ganz allgemein, unter der Voraussetzung $(a,b) = 1$. Aus zwei Kongruenzen mod a bzw mod b machen wir eine Kongruenz mod (ab), und umgekehrt.

Sei $x \equiv c \pmod a$ und $x \equiv d \pmod b$, 1. Kongruenz $\Rightarrow \exists t: x = c + at$.

Einsetzen in die zweite Kongruenz: $c + at \equiv d \pmod b \Leftrightarrow at \equiv d - c \pmod b$.

Wegen $(a,b) = 1$ ist a invertierbar modulo b (d.h. $\bar{a}^{-1}$ existiert in $\mathbb{Z}/b\mathbb{Z}$) ist die Kongruenz $at \equiv d - c \pmod b$ immer nach t auflösbar, d.h. t existiert und x existiert deshalb auch.

Die Gleichung $x \equiv c \pmod a$ hat also eine eindeutige Lösung in Restklassen. D.h. es gibt genau eine Lösung x im Intervall $[1, a]$ ($\subset \mathbb{Z}$).

Im Intervall $[1, ab]$ gibt es natürlich mehr Lösungen, für diese eine Gleichung. Aber $\bar{x}$ ist eine Lösung beider Gleichungen - wie sieht es da mit Eindeutigkeit aus?

Aus der Konstruktion der Lösung beider Kongruenzen folgt, daß man einen Repräsentanten $x \in [1, ab]$ wählen kann. nachprüfen

Sei $y \in [1, ab]$ ebenfalls eine Lösung beider Kongruenzen.

Frage: $x = y$? D.h. ist die Lösung eindeutig modulo ab?

Da x und y Lösungen sind, gilt $x \equiv c \equiv y \pmod a$ und $x \equiv d \equiv y \pmod b$

$\Rightarrow a \mid (x-y)$ und $b \mid (x-y)$

Nach Voraussetzung ist $(a,b) = 1$ $\overset{\text{warum}}{\Rightarrow}$ $ab \mid (x-y) \Rightarrow x \equiv y \pmod{ab}$

$\Rightarrow x = y$, da beide $\in [1, ab]$. Das ist die gewünschte Eindeutigkeit.

Aber $x \equiv cd \pmod{ab}$ kann man nicht erwarten. Gegenbeispiel?

Gezeigt ist (nur): Für festes a und b und gewählter c und d gibt es genau ein $x \in [1, ab]$ mit $x \equiv c \pmod a$ und $x \equiv d \pmod b$.

Anders gesagt: es gibt eine injektive Funktion

$$f: [1,a] \times [1,b] \to [1, ab]$$
$$(c,d) \longmapsto x \text{ (die eindeutige Lösung}$$

Warum injektiv? Für $(c,d) \neq (c',d')$ kann x nicht beide Kongruenzen erfüllen. genauer? ← meint Paare (c,d) und (c',d')

Also ist f auch surjektiv, $x = f(c,d)$ läuft durch ganz $[1, ab]$. warum?

Was wollten wir eigentlich beweisen? Aussage (c), d.h. $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

unter der Voraussetzung $(a,b) = 1$. ← meint $\operatorname{ggT}(a,b) = 1$

Für $\varphi(a)$ zählen wir alle $c \in [1,a]$ mit $(a,c) = 1$ und alle $\overset{d}{\not b} \in [1,b]$ mit $(b,d) = 1$

und vergleichen mit der Anzahl aller $x \in [1, ab]$ mit $(x, ab) = 1$.

Falls c nicht mitgezählt wird, d.h. $(a,c) \neq 1$ ist auch $(a,x) \neq 1$ weil

$x = c + at \Rightarrow (ab, x) \neq 1$. Ebenso wenn $(b,d) \neq 1$.

$\Rightarrow$ Für ~~nicht~~ (c,d) bei denen c oder d nicht mitgezählt wird, wird

auch $x = f(c,d)$ nicht mitgezählt. nicht

Umgekehrt werde $x = f(c,d)$ mitgezählt bei $\varphi(ab)$, d.h. $(ab, x) \neq 1$.

Aber $x \equiv c \pmod a \Rightarrow (a,x) = (a,c)$ warum?

und $x \equiv d \pmod{\not{gd}\, b} \Rightarrow (b,x) = (b,d)$

Und $(a,x) = 1 = (b,x) \overset{\text{warum}}{\Leftrightarrow} (ab, x) = 1$

$\Rightarrow (a,c) \neq 1$ oder $(b,d) \neq 1$

$\Rightarrow$ (c) ist bewiesen

(d) folgt aus (b) und (c). wie?

(e) Sei $1 \le x \le m$. Falls $(x,m)=1$, zählen wir x bei $\varphi(m)$ mit.

Falls $(x,m)=e$, d.h. $x=q\cdot e$ und $m=de$ mit $(q,d)=1$, dann wird q bei $\varphi(d)$ mitgezählt (da $q \le d$ aus $x \le m$ folgt).

Umgekehrt sei d ein Teiler von m und $q \le d$ mit $(q,d)=1$. Sei $e=\frac{m}{d}$ und $x=qe \Rightarrow (x,m)=e$.

Also: auf der rechten Seite, d.h. m, zählen wir alle x mit $1 \le x \le m$.

Auf der linken Seite, $\sum_{d \mid m} \varphi(d)$, zählen wir für festes $d=\frac{m}{e}$ alle q mit $(q,d)=1$, damit auch genau alle $x=qe$. □

Im Beweis von (c) haben wir eine Aussage über die simultane Lösbarkeit mehrerer Kongruenzen mitbewiesen:

2.5 Theorem (Chinesischer Restsatz, Sun-tzu, etwa 3.Jh): Seien $m_1, \dots, m_u$ paarweise teilerfremd. Dann gibt für beliebige $a_1, \dots, a_u \in \mathbb{Z}$:

$$x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_u \pmod{m_u}$$

hat genau eine (simultane) Lösung modulo $m_1 \cdot \dots \cdot m_u$.

wie folgt das genau aus dem Beweis von 2.4(c)?

was hat das mit der algebraischen Aussage

$$\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_u\mathbb{Z} \cong \mathbb{Z}/m_1 \cdot \dots \cdot m_u\mathbb{Z}$$

zu tun, und wird da dieselbe Voraussetzung gebraucht?

2.6 Theorem (Satz von Wilson): Sei p prim. Dann gilt

$$(p-1)! \equiv -1 \pmod{p}$$

Beweis (Gauß): $\mathbb{Z}/p\mathbb{Z}$ Körper $\Rightarrow$ zu $a \in \{1, \dots, p-1\}$ existiert genau ein b mit $ab \equiv 1 \pmod{p}$, d.h. ein Inverses zu a.

Falls $a=b$: $a^2 \equiv 1 \pmod{p}$, d.h. $p \mid (a^2-1) = (a+1)(a-1) \Rightarrow a \in \{1, -1\}$ (warum?)

Für alle $a \neq 1, p-1$ gilt $a \neq b \Rightarrow$ in $2 \cdot \dots \cdot (p-2)$ kommen a und b als zwei verschiedene Faktoren vor, die sich wegkürzen: $2 \cdot \dots \cdot (p-2) \equiv 1 \pmod{p}$.

$\Rightarrow (p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}$ □

Die Umkehrung gilt auch: $(p-1)! \equiv -1 \pmod p \Rightarrow p$ prim.
Denn: Sei n zusammengesetzt, $n = a \cdot b$, $a, b \in \mathbb{N}$, z.B. a prim
$\Rightarrow a \mid (p-1)!$ und ~~$a \nmid p$~~ $a \mid n = ab$
Annahme: $(n-1)! \equiv -1 \pmod n$. Daraus folgt $n \mid (n-1)! + 1$
Aber $a \mid n$ und $a \mid (n-1)! \Rightarrow a$ ist ein Primteiler von 1 $\lightning$

Eine bekannte Anwendung in der Kryptographie ist das RSA-Verfahren (Rivest-Shamir-Adleman, 1978), ein Public Key Verfahren zur verschlüsselten Nachrichten übertragung.
Nachrichten sind Folgen von Elementen in $\mathbb{Z}/n\mathbb{Z}$ (Beispiele: Geheimzahl am Bankautomaten, bei Telefon Karten, digitale Signatur, Chip auf Reisepass –).
Eine Nachricht bzw ein $x \in \mathbb{Z}/n\mathbb{Z}$ soll kodiert (chiffriert), gesendet und vom Empfänger entschlüsselt werden. Die Nachricht kann abgehört werden und Sender und Empfänger können keine Geheimsprache vereinbaren. Es gibt nur einen Empfänger für alle Nachrichten.
Idee: Der Empfänger wählt zwei große Primzahlen p und q, $p \neq q$. Sei $n = pq$.
2.4 $\Rightarrow \varphi(n) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$. Ein $e \in \mathbb{N}$ wird gewählt mit $1 < e < \varphi(n)$ und $\operatorname{ggT}(e, \varphi(n)) = 1$.
Die Zahlen n und e sind der Public Key und können bekannt gegeben werden. Die Primzahlen p und q bleiben geheim, wenn sie groß sind, dauert es lange, sie aus n zu berechnen.
Nun wird die Restklasse $x \in \mathbb{Z}/n\mathbb{Z}$ als x^e kodiert und x^e wird gesendet, kann also abgehört werden. Jemand, der e und n kennt und x^e abhört, müsste die e-te Wurzel aus x^e (modulo n) ziehen können, was lange dauert.
Was macht der rechtmäßige Empfänger? Er/sie kennt $\varphi(n)$ und weiß, daß $(e, \varphi(n)) = 1$ gilt. $\Rightarrow e$ ist in $(\mathbb{Z}/\varphi(n)\cdot\mathbb{Z})^*$ invertierbar: $\exists\, d$ so daß $de \equiv 1 \pmod{\varphi}$. Wenn man $\varphi(n)$ in Primfaktoren zerlegt hat, kann man d mit dem chinesischen Restsatz ausrechnen. Genauer:

Der Empfänger erhält $y = x^e$, hat d schon berechnet und rechnet y^d in $\mathbb{Z}/n\mathbb{Z}$ aus.

Behauptung: $y^d \equiv x \pmod n$, d.h. die Nachricht ist entschlüsselt.

Beweis: Falls $x \equiv 0$ ist nichts zu zeigen (aber die Nachricht ist nicht geheim!)

Sei $x \not\equiv 0$. $n = p \cdot q$, p und q sind beide prim $\Rightarrow ggT(x,n) \in \{1, p, q, n = pq\}$

$ggT(x,n) = n$ bedeutet $x \equiv 0$. Also bleiben drei Fälle: 1, p oder q.

Erster Fall: $ggT(x,n) = 1 \Rightarrow p \nmid x$ und $q \nmid x$.

$de \equiv 1 \bmod \varphi(n) \Rightarrow \exists j: de = 1 + j\,\varphi(n) \Rightarrow x^{de} = x^{1+j\varphi(n)} = x \cdot (x^{\varphi(n)})^j$

Mit dem Satz von Euler (anwendbar wegen $ggT(x,n) = 1$) folgt $x^{\varphi(n)} \equiv 1 \pmod n$, also $x^{de} \equiv x \pmod n$

Zweiter Fall: $ggT(x,n) = p$. Wie im ersten Fall ist $x^{de} = x \cdot (x^{\varphi(n)})^j$

$\varphi(n) = \varphi(p) \cdot \varphi(q) \Rightarrow x^{de} = x\,(x^{\varphi(q)})^{\varphi(p)j}$

$ggT(q,x) = 1$, also ist darauf der Satz von Euler anwendbar $\Rightarrow$

$x^{\varphi(q)} \equiv 1 \pmod q$, also $x^{de} \equiv x \pmod q \Rightarrow q \mid (x^{de} - x)$

Nach Voraussetzung: $p \mid x$, also auch $p \mid x^{de}$, also $p \mid (x^{de} - x)$

$\Rightarrow n = pq \mid (x^{de} - x)$

Dritter Fall: $ggT(x,n) = q$, analog $\square$