

Lösungsvorschläge zum 10. Tutorium – Diskrete Strukturen

Während ihr euch unbemerkt dem EN-Gebäude nähert, merkt ihr, dass die umliegenden Gebäude zum Teil in Ruinen stehen und fragt euch, ob das in den letzten Tagen passiert ist oder, ob die Gebäude der TU schon lange dem Verfall geweiht sind.

Aufgabe 1

Finden Sie die kleinste natürliche Zahl, welche folgende Kongruenzen erfüllt:

$$\begin{aligned}x &\equiv 4 \pmod{7} \text{ und} \\x &\equiv 2 \pmod{8} \text{ und} \\x &\equiv 2 \pmod{5}\end{aligned}$$

Aufgabe 2

Berechne die eulersche φ -Funktion für die folgenden Werte:

- (i) $2^1 \cdot 3^2 \cdot 5^3$
- (ii) $15 \cdot 25$
- (iii) $5!$

Aufgabe 3

- (i) Zeigen Sie: Für jede Primzahl p und jedes $n \in \mathbb{N}^+$ mit $n < p$ gilt, dass $\binom{p}{n} \equiv 0 \pmod{p}$.
- (ii) Zeigen Sie per Induktion: Für jede Primzahl p und jedes $m \in \mathbb{N}_0$ gilt, dass $m^p \equiv m \pmod{p}$.¹
(Dies ist der kleine Satz von Fermat, siehe VL 10 Slide 23.)
- (iii) Seien p und q zwei unterschiedliche Primzahlen. Zeigen Sie: Wenn $x \equiv a \pmod{p}$ und $x \equiv a \pmod{q}$, dann gilt auch $x \equiv a \pmod{p \cdot q}$.

Hieraus können Sie nun Folgendes ableiten.

- (iv) Sei $n = p \cdot q$ für zwei Primzahlen p, q und seien $k, m \in \mathbb{N}_0$, sodass $m < n$. Zeigen Sie:

$$m^{k \cdot \varphi(n)+1} \equiv m \pmod{n}.$$

Nun können Sie in voller Allgemeinheit die Korrektheit des RSA-Verfahrens beweisen.

- (v) Sei (e, n) der öffentliche Schlüssel und sei (d, n) der private Schlüssel für das RSA-Verfahren. Zeigen Sie: Wenn $M \in \mathbb{N}_0$ mit $M < n$, dann gilt $(M^e)^d \equiv M \pmod{n}$.

¹Folgende Definition für binomische Formeln kann Ihnen hier helfen: $(a+b)^n = \sum_{k=0}^n (\binom{n}{k} \cdot a^{n-k} \cdot b^k)$.

Chinesischer Restsatz

Betrachte für

$$\cdot b_1, b_2, b_3 \in \mathbb{Z}$$

$$\cdot m_1, m_2, m_3 \in \mathbb{N}_{\geq 2} \text{ mit } \text{ggT}(m_i, m_j) = 1, i \neq j$$

das Kongruenzsystem

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

$$x \equiv b_3 \pmod{m_3}$$

Gesucht ist nun $x \in \mathbb{Z}$, sodass obiges System erfüllt ist.

Lösungsstrategie: oBdA gelte $b_i \in \{0, \dots, m_i - 1\}$ (also $b_i \pmod{m_i} = b_i$)

1) Finden wir $T_i \in \mathbb{N}$ mit $T_i \equiv b_i \pmod{m_i}$ und $T_i \equiv 0 \pmod{m_j}$ für $i \neq j$,

so gilt nach den bekannten Rechenregeln z.B. (analog für m_2, m_3)

$$x := T_1 + T_2 + T_3 \Rightarrow x \pmod{m_1} = [\underbrace{(T_1 \pmod{m_1})}_{\equiv b_1 \pmod{m_1}} + \underbrace{(T_2 \pmod{m_1})}_{=0} + \underbrace{(T_3 \pmod{m_1})}_{=0}] \pmod{m_1}$$

und damit insgesamt $x \equiv b_i \pmod{m_i} \quad \forall i$.

2) Konstruktion der T_i :

$$\text{Setze } M := m_1 \cdot m_2 \cdot m_3$$

↳ dann ist schonmal $M \equiv 0 \pmod{m_i} \quad \forall i$

Weiter gilt

$$M_i := \frac{M}{m_i} \Rightarrow M_i \equiv 0 \pmod{m_j} \text{ für } i \neq j$$

aber i.A. noch nicht $M_i \equiv b_i \pmod{m_i}$

Also probieren wir $M_i \cdot b_i$.

Dann ist immer noch $M_i \cdot b_i \equiv 0 \pmod{m_j}, i \neq j$

aber lediglich $M_i \cdot b_i \pmod{m_i} = [(M_i \pmod{m_i}) \cdot (b_i \pmod{m_i})] \pmod{m_i}$

Beobachtung: Wäre $M_i \equiv 1 \pmod{m_i}$, dann wäre $(M_i \cdot b_i) \pmod{m_i} = b_i$.

Lösung: Modulares Inverse!

(*) Ist $\text{ggT}(a, c) = \text{ggT}(b, c) = 1$, dann ist

auch $\text{ggT}(a \cdot b \cdot c) = 1$

↳ Suche $w_i \pmod{m_i}$ mit $M_i \cdot w_i \pmod{m_i} = 1$.

Diese Zahl existiert, da $\text{ggT}(m_i, M_i) = 1$ gilt (klar?) (*)

und kann mit dem erweiterten eukl. Algo. berechnet werden (~ Tut 9, Aufgabe 4)

Jetzt sind wir fertig!

$$\text{Setze } T_i := M_i \cdot w_i \cdot b_i.$$

$$\Rightarrow T_i \pmod{m_i} = [\underbrace{(M_i \cdot w_i \pmod{m_i})}_{=1} \cdot (b_i \pmod{m_i})] \pmod{m_i} = b_i$$

$$\text{und weiter } T_i \pmod{m_j} = [\underbrace{(M_i \pmod{m_j}) \cdot ((w_i \cdot b_i) \pmod{m_j})}_{=0}] \pmod{m_j} = 0$$

Bemerkung: Es gibt genau eine Lösung $x \in \{0, \dots, M-1\}$

• alle Lösungen sind Kongruent bzgl. M .

Aufgabe 1

Finden Sie die kleinste natürliche Zahl, welche folgende Kongruenzen erfüllt:

$$\begin{aligned}x &\equiv 4 \pmod{7} \text{ und} \\x &\equiv 2 \pmod{8} \text{ und} \\x &\equiv 2 \pmod{5}\end{aligned}$$

1. Berechne $M = m_1 \cdot m_2 \cdot m_3 = 7 \cdot 8 \cdot 5 = 280$.

$$\hookrightarrow M_1 = 8 \cdot 5 = 40$$

$$\hookrightarrow M_2 = 7 \cdot 5 = 35$$

$$\hookrightarrow M_3 = 7 \cdot 8 = 56$$

2. Berechne (rate :D) Modulare Inverse

Gesucht: w_i mit $40 \cdot w_i \pmod{7} = 1$

$$\begin{array}{c} \text{Erw-Euklid}(40, 7): \\ \begin{array}{l} 40 - 5 \cdot 7 = 5 \\ 7 - 1 \cdot 5 = 2 \\ 5 - 2 \cdot 2 = 1 \\ 1 = 5 - 2 \cdot 2 \\ 1 = 3 \cdot 5 - 2 \cdot 7 \\ 1 = 3 \cdot 40 - 17 \cdot 7 \end{array} \end{array}$$

$$2 \geq 7 - 5 = 7 - (40 - 5 \cdot 7) = 6 \cdot 7 - 40$$

$$\begin{aligned}1 &= 40 - 5 \cdot 7 - 2 \cdot (6 \cdot 7 - 40) \\&= 3 \cdot 40 - 17 \cdot 7\end{aligned}$$

Das modular inverse von 40 bezüglich 7 ist 3.

$$40 - 5 \cdot 7 = 5$$

$$7 - 1 \cdot 5 = 2 \Leftrightarrow 2 = 7 - 40 + 5 \cdot 7 = -7 \cdot 40 + 6 \cdot 7$$

$$5 - 2 \cdot 2 = 1 \Leftrightarrow 1 = 40 - 5 \cdot 7 - 2(-7 \cdot 40 + 6 \cdot 7)$$

$$= 40 - 5 \cdot 7 + 2 \cdot 40 - 12 \cdot 7$$

⋮

$$\Rightarrow w_1 = 3$$

$$\text{Erw-Euklid}(35, 8):$$

Analog: $35 - 4 \cdot 8 = 3$

$$8 - 2 \cdot 3 = 2$$

$$3 - 1 \cdot 2 = 1$$

$$1 = 3 - 1 \cdot 2$$

$$1 = 3 \cdot 3 - 1 \cdot 8$$

$$1 = 3 \cdot 35 - 13 \cdot 8$$

Das modular inverse von 35 bezüglich 8 ist 3.

$$\text{Erw-Euklid}(56, 5):$$

$$56 - 11 \cdot 5 = 1$$

Das modular inverse von 56 bezüglich 5 ist 1.

$$\Rightarrow w_2 = 3$$

$$\Rightarrow w_3 = 1$$

3. Berechne T_i und $x \in \{0, \dots, M-1\}$

$$T_1 := M_1 \cdot w_1 \cdot b_1 = 40 \cdot 3 \cdot 4 = 480$$

$$T_2 := M_2 \cdot w_2 \cdot b_2 = 35 \cdot 3 \cdot 2 = 210$$

$$T_3 := M_3 \cdot w_3 \cdot b_3 = 56 \cdot 1 \cdot 2 = 112$$

$$\Rightarrow x := (T_1 + T_2 + T_3) \pmod{M} = 802 \pmod{280} = 242.$$

Eulersche φ -Funktion

Für $n \in \mathbb{N}_{\geq 2}$ ist $\varphi(n) := |\{1 \leq a \leq n : \text{ggT}(a, n) = 1\}|$

↳ # teilerfremde Zahlen zw. 1 und n

Beobachtungen:

- 1) Für p prim gilt $\varphi(p) = p - 1$
- 2) Für p prim und $e \geq 1$ gilt $\varphi(p^e) = p^e - p^{e-1}$
↳ Sei $A := \{m \in \mathbb{N} \mid 1 \leq m \leq p^e, \text{ggT}(p^e, m) > 1\}$
• Klar ist: $\{p, 2p, 3p, \dots, \underbrace{p^{e-1} \cdot p}_=\} \subseteq A$

Lemma von Euklid

Sind $a, b, c \in \mathbb{N}$, so gilt:

$$\text{ggT}(a, b) = 1 \text{ und } a | b \cdot c \Rightarrow a | c$$

• Sei $m \in A$. Dann existiert ein $k \in \mathbb{N}_{\geq 2}$ mit $k | m$ und $k \nmid p^e$

Sei q ein PF von k und ang. $q \neq p$. Dann gilt $q | p^e$ aber wegen $\text{ggT}(q, p) = 1$

folgt durch wiederholte Anwendung des Lemmas von Euklid, dass $q | p^e$ (zu $p \neq q$)

Also ist jeder PF von k gleich $p \Rightarrow k = p^l$, $1 \leq l \leq e$

$$\Rightarrow p | m \Rightarrow m \in \{p, 2p, \dots, p^{e-1} \cdot p\}$$

Also ist $A = \{p, 2p, \dots, p^{e-1} \cdot p\}$

Da es $\left\lfloor \frac{p^e}{p} \right\rfloor = p^{e-1}$ viele solcher Vielfachen gibt, ist $|A| = p^{e-1}$

Da es p^e viele Zahlen $1 \leq i \leq p^e$ gibt, folgt, dass

$$\begin{aligned} |\{m \mid 1 \leq m \leq p^e, \text{ggT}(m, p^e) = 1\}| &= |\{m \mid 1 \leq m \leq p^e\} \setminus \{m \mid 1 \leq m \leq p^e, \text{ggT}(m, p^e) > 1\}| \\ &= p^e - |A| = p^e - p^{e-1} = (p-1) \cdot p^{e-1} \end{aligned}$$

Bemerkung: Sind $m, n \in \mathbb{N}_{\geq 2}$ mit $\text{ggT}(m, n) = 1$, dann gilt: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$!

Daraus folgt zusammen mit 2) von oben:

$$\varphi(n) = \prod_{i=1}^{\ell} (p_i - 1) \cdot p_i^{e_i - 1}, \text{ wobei: } n = \prod_{i=1}^{\ell} p_i^{e_i} \text{ PFZ von } n \text{ ist } (p_i \neq p_j \text{ für } i \neq j)$$

Aufgabe 2

Berechne die eulersche φ -Funktion für die folgenden Werte:

$$(i) 2^1 \cdot 3^2 \cdot 5^3$$

$$(ii) 15 \cdot 25$$

$$(iii) 5!$$

Ansatz: Zerlege Zahl in PF und wende Formel an

Lösung zu Aufgabe 2

$$(i) \varphi(2^1 \cdot 3^2 \cdot 5^3) = (2-1) \cdot 2^0 \cdot (3-1) \cdot 3^1 \cdot (5-1) \cdot 5^2 = 600$$

$$(ii) \varphi(15^1 \cdot 25^1) = \varphi(3^1 \cdot 5^3) = (3-1) \cdot 3^0 \cdot (5-1) \cdot 5^2 = 200$$

$$(iii) \varphi(5!) = \varphi(2^3 \cdot 3^1 \cdot 5^1) = (2-1) \cdot 2^2 \cdot (3-1) \cdot (5-1) = 32$$

Aufgabe 3

(i) Zeigen Sie: Für jede Primzahl p und jedes $n \in \mathbb{N}^+$ mit $n < p$ gilt, dass $\binom{p}{n} \equiv 0 \pmod{p}$.

(i) Wir stellen zuerst fest, dass p zu allen $n \in \mathbb{N}^+$ mit $n < p$ teilerfremd ist, da p eine Primzahl ist. Dies bedeutet aber auch insbesondere, dass p zu $n!$ und zu $(p-n)!$ teilerfremd ist, da alle Primfaktoren von $n!$ kleiner oder gleich n sind. Betrachten wir nun die Binomialzahl

$$\binom{p}{n} = \frac{p!}{n! \cdot (p-n)!} = \frac{p \cdot (p-1)!}{n! \cdot (p-n)!} = p \cdot \frac{(p-1)!}{n! \cdot (p-n)!},$$

so stellen wir fest, dass $n! \cdot (p-n)!$ die Zahl $(p-1)!$ ganzzahlig teilen muss, da $\binom{p}{n}$ eine natürliche Zahl ist (siehe Blatt 9 Aufgabe 3) und p teilerfremd zum Nenner ist. Also existiert ein $k \in \mathbb{N}^+$, sodass

$$\binom{p}{n} \equiv k \cdot p \equiv 0 \pmod{p}.$$

(ii) Zeigen Sie per Induktion: Für jede Primzahl p und jedes $m \in \mathbb{N}_0$ gilt, dass $m^p \equiv m \pmod{p}$.¹
(Dies ist der kleine Satz von Fermat, siehe VL 10 Slide 23.)

Sei p eine bel. Primzahl.

IA: Für $m=0$ gilt $0^p \equiv 0 \pmod{p}$.

IV: Gelte nun $m^p \equiv m \pmod{p}$ für ein $m \in \mathbb{N}_0$.

$$\text{IS: } (m+1)^p \equiv \sum_{k=0}^p \binom{p}{k} \cdot m^k \cdot 1^{p-k} \stackrel{?}{=} \binom{p}{0} \cdot m^0 \cdot 1^p + \binom{p}{1} \cdot m^p \cdot 1^0 \equiv 1 + m^p \stackrel{\text{IV}}{\equiv} 1+m \pmod{p}$$

(iii) Seien p und q zwei unterschiedliche Primzahlen. Zeigen Sie: Wenn $x \equiv a \pmod{p}$ und $x \equiv a \pmod{q}$, dann gilt auch $x \equiv a \pmod{p \cdot q}$.

Aus der VL:

Seien $a, b, c \in \mathbb{N}$. Dann gilt:

$$a|bc \text{ und } \text{ggT}(a,b)=1 \Rightarrow a|c \quad (\star)$$

Es gilt

- $x \equiv a \pmod{p} \Rightarrow \exists k: x-a=k \cdot p$
- $x \equiv a \pmod{q} \Rightarrow q|(x-a) \Leftrightarrow q|k \cdot p$
und mit (\star) folgt wegen $\text{ggT}(p,q)=1: q|k$

Also ist $k \equiv 0 \pmod{q}$ und damit

$$x-a \equiv k \cdot p \equiv 0 \pmod{p \cdot q} \Rightarrow x \equiv a \pmod{p \cdot q}$$

$\downarrow \quad k \cdot p = l \cdot q \cdot p \text{ für ein } l \in \mathbb{Z}$

Hieraus können Sie nun Folgendes ableiten.

- (iv) Sei $n = p \cdot q$ für zwei Primzahlen p, q und seien $k, m \in \mathbb{N}_0$, sodass $m < n$. Zeigen Sie:

$$m^{k \cdot \varphi(n)+1} \equiv m \pmod{n}.$$

$$\text{zz: } m^{k \cdot \varphi(n)+1} \equiv m \pmod{p \cdot q}$$

$$\text{Idee: Zeige } m^{k \cdot \varphi(n)+1} \equiv m \pmod{p}$$

$$m^{k \cdot \varphi(n)+1} \equiv m \pmod{q}$$

denn dann folgt Aussage aus iii)

$$\text{zz: } m^{k \cdot \varphi(n)+1} \equiv m \pmod{p} \quad (\text{das sollte euch an den Satz von Fermat erinnern!})$$

$$\text{Falls } p \mid m \text{ gilt, ist } m \equiv 0 \equiv 0^{k \cdot \varphi(n)+1} \quad \checkmark$$

Sei also $p \nmid m$.

$$\text{Wegen } \varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1) \text{ gilt}$$

$$m^{k \cdot \varphi(n)+1} = m \cdot m^{k \cdot \varphi(n)} = m \cdot m^{k \cdot (p-1)(q-1)} = m \cdot (m^{p-1})^{k \cdot (q-1)} \equiv ?$$

Wunsch: $m^{p-1} \equiv 1 \pmod{p}$, denn dann ist

$$(m^{p-1})^{k \cdot (q-1)} \equiv 1^{k \cdot (q-1)} \equiv 1 \pmod{p}$$

$$\Rightarrow m^{k \cdot (p-1)(q-1)} \cdot m \equiv 1 \cdot m \equiv m \pmod{p}$$

Der Satz von Fermat liefert: $m^p \equiv m \pmod{p}$ (da p Primzahl)

Wegen $p \nmid m$ (nach Annahme) ($\Rightarrow \text{ggT}(p, m) = 1$)

$$m \cdot m^{p-1} \equiv m \pmod{p} \Rightarrow m^{p-1} \equiv 1 \pmod{p} \quad (\text{Rechenregel aus VL})$$

Nun können Sie in voller Allgemeinheit die Korrektheit des RSA-Verfahrens beweisen.

- (v) Sei (e, n) der öffentliche Schlüssel und sei (d, n) der private Schlüssel für das RSA-Verfahren. Zeigen Sie: Wenn $M \in \mathbb{N}_0$ mit $M < n$, dann gilt $(M^e)^d \equiv M \pmod{n}$.

Für e und d gilt nach Konstruktion

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

$$\Rightarrow \exists k \in \mathbb{N}: e \cdot d = 1 + k \cdot \varphi(n)$$

$$\text{Also gilt: } (M^e)^d \equiv M^{e \cdot d} \equiv M^{1+k \cdot \varphi(n)+1} \stackrel{(iv)}{\equiv} M \pmod{p \cdot q}$$

Lösungsvorschläge zur 10. freiwilligen Übung – Diskrete Strukturen

Aufgabe 4

Sie haben herausfinden können, dass für die Zahl $n = 14803$, welche in einem öffentlichen Schlüssel verwendet wird, die eulersche φ -Funktion folgenden Wert annimmt $\varphi(n) = 14560$. Ermitteln Sie mit Hilfe dieser Erkenntnis nun die Primfaktoren p, q von n .

Aufgabe 5

Bestimmen Sie die niedrigstwertige Ziffer von 9^{9^9} . Begründen Sie Ihre Berechnung durch nachvollziehbare Schritte, die keine explizite Berechnungen mit Zahlen höher als 100 enthalten.

Aufgabe 6

Sei $n \in \mathbb{N}$ mit $n \geq 2$. Zeigen Sie: Wenn $a^{n-1} \equiv 1 \pmod{n}$ für alle $a \in \{1, \dots, n-1\}$ gilt, dann ist n eine Primzahl.

Anmerkung: Dies ist die Rückrichtung des kleinen Satz von Fermat.

Aufgabe 7

Casey, die Informatikerin, möchte einen verschlüsselten Nachricht M an Alice, Bob und Dennis schicken. Ihre öffentliche Schlüssel lauten $(3, N_a)$, $(3, N_b)$ und $(3, N_d)$, wobei N_a, N_b und N_d paarweise relativ prim sind und M kleiner als N_a, N_b und N_d ist.

Eve hat, wie üblich, die chiffrierten Texte abgefangen. Wie kann nun Eve den Nachricht M rekonstruieren, ohne die Primzahl faktorzerlegung der öffentlichen Schlüsseln berechnen zu müssen?

Aufgabe 1

Finden Sie die kleinste natürliche Zahl, welche folgende Kongruenzen erfüllt:

$$\begin{aligned}x &\equiv 4 \pmod{7} \text{ und} \\x &\equiv 2 \pmod{8} \text{ und} \\x &\equiv 2 \pmod{5}\end{aligned}$$

Wir nutzen den chinesischen Restsatz. Es sagt uns, dass es für dieses Kongruenzsystem genau eine Lösung x mit $0 \leq x \leq 7 \cdot 8 = 280 = m$ gibt, da $5, 7, 8$ teilerfremd sind.

Seien $m_1 = 7, m_2 = 8, m_3 = 5$, sowie $b_1 = 4, b_2 = 2, b_3 = 2$

Wir lösen das System indem wir, für jedes m_i , einen Term T_i finden, sodass gilt:

$$\begin{aligned}T_i &\equiv b_i \pmod{m_i} \\T_i &\equiv 0 \pmod{m_j} \text{ für } j \neq i\end{aligned}$$

Sei $M_i = \frac{m}{m_i}$.

Wir erstellen T_i wie folgt:

$$T_i = M_i \cdot W_i \cdot b_i$$

Dabei ist W_i das modular Inverse von M_i bezüglich m_i . Dann gilt $T_i \equiv b_i \pmod{m_i}$, denn

$$\begin{aligned}T_i &\equiv M_i \cdot W_i \cdot b_i \pmod{m_i} \\&\equiv 1 \cdot b_i \pmod{m_i} \\&\equiv b_i \pmod{m_i}.\end{aligned}$$

Es gilt

$$\begin{aligned}M_1 &= 40, M_2 = 35, M_3 = 56 \\&= \frac{m}{m_1} \quad = \frac{280}{8} \quad = \frac{280}{5} \\&= \frac{280}{7}\end{aligned}$$

wir berechnen nun die modularen Inversen von den M_i :

$$\begin{aligned}\text{Erw-Euklid}(40, 7): \quad &40 - 5 \cdot 7 = 5 \\&7 - 1 \cdot 5 = 2 \\&5 - 2 \cdot 2 = 1 \\&1 = 5 - 2 \cdot 2 \\&1 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7 \\&1 = 3 \cdot (40 - 5 \cdot 7) - 2 \cdot 7 = 3 \cdot 40 - 17 \cdot 7\end{aligned}$$

das modular inverse von 40 bezüglich 7 ist 3

$$\begin{aligned}\text{Erw-Euklid}(35, 8): \quad &35 - 4 \cdot 8 = 3 \\&8 - 2 \cdot 3 = 2 \\&3 - 1 \cdot 2 = 1 \\&1 = 3 - 1 \cdot 2 \\&1 = 3 - 8 + 2 \cdot 3 = 3 \cdot 3 - 8 \\&1 = 3 \cdot (35 - 4 \cdot 8) - 8 \\&= 3 \cdot 35 - 13 \cdot 8\end{aligned}$$

das modular inverse von 35 bezüglich 8 ist 3

Erw-Euklid (§6.5): $56 - 11 \cdot 5 = 1$
das modular inverse von 56 bezüglich 5 ist 1

$$\Rightarrow \begin{aligned} T_1 &= 40 \cdot 3 \cdot 4 = 480 \\ T_2 &= 35 \cdot 3 \cdot 2 = 210 \\ T_3 &= 56 \cdot 1 \cdot 2 = 112 \end{aligned}$$

Die Summe der T_i hat somit alle erwünschten Eigenschaften

$$\begin{aligned} T_1 + T_2 + T_3 &= 802 \\ 802 \bmod 280 &= 242 \\ 242 &= 34 \cdot 7 + 4 \\ 242 &= 30 \cdot 8 + 2 \\ 242 &= 48 \cdot 5 + 2 \end{aligned}$$

Aufgabe 2

Berechne die eulersche φ -Funktion für die folgenden Werte:

$$(i) 2^1 \cdot 3^2 \cdot 5^3$$

$$(ii) 15 \cdot 25$$

$$(iii) 5!$$

$$(i) \varphi(2^1 \cdot 3^2 \cdot 5^3) = 1 \cdot 2^0 \cdot 2 \cdot 3^1 \cdot 4 \cdot 5^2 = 600$$

$$(ii) \varphi(3 \cdot 5^3) = 2 \cdot 3^0 \cdot 4 \cdot 5^2 = 200$$

$$(iii) \varphi(5!) = \varphi(5 \cdot 4 \cdot 3 \cdot 2) = \varphi(2^3 \cdot 3 \cdot 5) = 2^2 \cdot 2 \cdot 3^0 \cdot 4 \cdot 5^0 = 32$$

Eulersche φ -Funktion: Grundlagen

Eine einfache Berechnungsmethode für φ ist bekannt.

Primzahlen p haben nur sich selbst und 1 als positive Teiler, somit sind sie teilerfremd zu allen Zahlen in $\{1, \dots, p-1\}$ und es gilt

$$\varphi(p) = p - 1$$

Primzahlpotenzen p^e haben nur die Vielfachen von p als Teiler und es gilt

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

Allgemein gilt für eine Zahl n mit der Primfaktorzerlegung $n = \prod_{i=1}^k p_i^{e_i}$:

$$\varphi(n) = \prod_{i=1}^k (p_i - 1)p_i^{e_i - 1}$$

Aufgabe 3

(i) Zeigen Sie: Für jede Primzahl p und jedes $n \in \mathbb{N}^+$ mit $n < p$ gilt, dass $\binom{p}{n} \equiv 0 \pmod{p}$.

(ii) Zeigen Sie per Induktion: Für jede Primzahl p und jedes $m \in \mathbb{N}_0$ gilt, dass $m^p \equiv m \pmod{p}$.¹
(Dies ist der kleine Satz von Fermat, siehe VL 10 Slide 23.)

(iii) Seien p und q zwei unterschiedliche Primzahlen. Zeigen Sie: Wenn $x \equiv a \pmod{p}$ und $x \equiv a \pmod{q}$, dann gilt auch $x \equiv a \pmod{p \cdot q}$.

Hieraus können Sie nun Folgendes ableiten.

(iv) Sei $n = p \cdot q$ für zwei Primzahlen p, q und seien $k, m \in \mathbb{N}_0$, sodass $m < n$. Zeigen Sie:

$$m^{k \cdot \varphi(n)+1} \equiv m \pmod{n}.$$

Nun können Sie in voller Allgemeinheit die Korrektheit des RSA-Verfahrens beweisen.

(v) Sei (e, n) der öffentliche Schlüssel und sei (d, n) der private Schlüssel für das RSA-Verfahren. Zeigen Sie: Wenn $M \in \mathbb{N}_0$ mit $M < n$, dann gilt $(M^e)^d \equiv M \pmod{n}$.

Lösung zu Aufgabe 3

(i) Wir stellen zuerst fest, dass p zu allen $n \in \mathbb{N}^+$ mit $n < p$ teilerfremd ist, da p eine Primzahl ist. Dies bedeutet aber auch insbesondere, dass p zu $n!$ und zu $(p-n)!$ teilerfremd ist, da alle Primfaktoren von $n!$ kleiner oder gleich n sind. Betrachten wir nun die Binomialzahl

$$\binom{p}{n} = \frac{p!}{n! \cdot (p-n)!} = \frac{p \cdot (p-1)!}{n! \cdot (p-n)!} = p \cdot \frac{(p-1)!}{n! \cdot (p-n)!},$$

so stellen wir fest, dass $n! \cdot (p-n)!$ die Zahl $(p-1)!$ ganzzahlig teilen muss, da $\binom{p}{n}$ eine natürliche Zahl ist (siehe Blatt 9 Aufgabe 3) und p teilerfremd zum Nenner ist. Also existiert ein $k \in \mathbb{N}^+$, sodass

$$\binom{p}{n} \equiv k \cdot p \equiv 0 \pmod{p}.$$

(ii) Wir beweisen die Aussage per Induktion über m , angefangen bei $m = 0$.

Der Induktionsanfang gilt, da $0^p \equiv 0 \pmod{p}$.

Die Induktionsvoraussetzung ist nun, dass für ein festes m gilt, dass $m^p \equiv m \pmod{p}$.

Durch die vorherige Aussage können wir nun leicht den Induktionsschritt beweisen, denn es gilt

$$\begin{aligned} (m+1)^p &\equiv \binom{p}{0} m^p 1^0 + \binom{p}{1} m^{p-1} 1^1 + \binom{p}{2} m^{p-2} 1^2 + \dots + \binom{p}{p-1} m^1 1^{p-1} + \binom{p}{p} m^0 1^p \\ &\equiv m^p + \binom{p}{1} m^{p-1} + \binom{p}{2} m^{p-2} + \dots + \binom{p}{p-1} m + 1 \equiv m^p + 1 \pmod{p} \end{aligned}$$

und laut der Induktionsvoraussetzung $m^p + 1 \equiv m + 1 \pmod{p}$. Somit ist die Aussage bewiesen.

¹Folgende Definition für binomische Formeln kann Ihnen hier helfen: $(a+b)^n = \sum_{k=0}^n (\binom{n}{k}) \cdot a^{n-k} \cdot b^k$.

(iii) Aus $x \equiv a \pmod{p}$ folgt, dass $x = (k \cdot p) + a$ für ein $k \in \mathbb{N}^+$ und, da $x \equiv a \pmod{q}$, muss $k \equiv 0 \pmod{q}$ gelten, da p und q teilerfremd sind. Somit folgt $x - a \equiv k \cdot p \equiv 0 \pmod{p \cdot q}$ und auch $x \equiv a \pmod{p \cdot q}$.

(iv) Um (iii) benutzen zu können, möchten wir folgendes Paar von Kongruenzen beweisen:

$$m \equiv m^{k \cdot \varphi(n)+1} \pmod{p} \text{ und } m \equiv m^{k \cdot \varphi(n)+1} \pmod{q}.$$

Angenommen $p|m$, so gilt $0 \equiv m \equiv m^{k \cdot \varphi(n)+1} \pmod{p}$ und wir haben für p die gewünschte Gleichung. Analog gilt dies auch für q . Also können wir annehmen, dass p und q nicht m teilen.

Nun hilft uns folgende Aussage, die aus dem kleinen Satz von Fermat folgt:

$$m^{p-1} \equiv 1 \pmod{p}.$$

Dies gilt, da p und m teilerfremd sind und somit $m^{p-1} \cdot m \equiv 1 \cdot m \pmod{p}$. Also erhalten wir

$$m^{k \cdot \varphi(n)+1} \equiv m^{k(p-1)(q-1)} \cdot m \equiv (m^{p-1})^{k(q-1)} \cdot m \equiv 1^{k(q-1)} \cdot m \equiv m \pmod{p}.$$

Analog lässt sich dies auch für q beweisen. Also folgt die Aussage aus (iii).

(v) Wir erinnern uns zuerst, dass e und d so gewählt wurden, dass $e \cdot d \equiv 1 \pmod{\varphi(n)}$ gilt. Das bedeutet insbesondere, dass es ein $k \in \mathbb{N}^+$ gibt mit $e \cdot d = k \cdot \varphi(n) + 1$. (Die obige Beobachtung wird auch auf den Folien gemacht.)

Nun können wir direkt den gerade bewiesenen Satz verwenden, da

$$(M^e)^d \equiv M^{e \cdot d} \equiv M^{k \cdot \varphi(n)+1} \equiv M \pmod{n}.$$

