

## 1. Aufgabe

Berechnen Sie hohe Potenzen mod  $p$ . Verwenden Sie dabei den „kleinen Fermat“. Genauer: Geben Sie  $x$  mit  $0 \leq x < p$  an, sodass

$$\begin{aligned} \text{a.} \quad x &\equiv 5^{25416} \pmod{7} \\ 5^{25416} \pmod{7} &\equiv 5^{4236 \cdot 6} \pmod{7} \equiv (5^6)^{4236} \pmod{7} \equiv 1 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{b.} \quad x &\equiv 3^{132463} \pmod{7} \\ 3^{132463} \pmod{7} &\equiv 3^{22077 \cdot 6 + 1} \pmod{7} \equiv (3^6)^{22077} \cdot 3 \pmod{7} \equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{c.} \quad x &\equiv 3^{12003627} \pmod{13} \\ 3^{12003627} \pmod{13} &\equiv 3^{1000302 \cdot 12 + 3} \pmod{13} \equiv (3^{12})^{1000302} \cdot 3^3 \pmod{13} \equiv 1 \pmod{13} \end{aligned}$$

$$\begin{aligned} \text{d.} \quad x &\equiv 7^{120036270} \pmod{11} \\ 7^{120036270} \pmod{11} &\equiv 7^{12003627 \cdot 10} \pmod{11} \equiv (7^{10})^{12003627} \pmod{11} \equiv 1 \pmod{11} \end{aligned}$$

$$\begin{aligned} \text{e.} \quad x &\equiv 7^{987654321} \pmod{11} \\ 7^{987654321} \pmod{11} &\equiv 7^{98765432 \cdot 10 + 1} \pmod{11} \equiv (7^{10})^{98765432} \cdot 7^1 \pmod{11} \equiv \\ &\equiv 7 \pmod{11} \end{aligned}$$

## 2. Aufgabe

Berechnen Sie  $\varphi(x)$  auf eine der zwei folgenden Arten (diejenige, welche Ihnen einfacher vorkommt):

Erstens: durch Zählen der teilerfremden Zahlen

Zweitens: durch Berechnung der Primzahlzerlegung

Mir kommt – außer vielleicht bei 6 – die Berechnung mit Hilfe der Primzahlzerlegung einfacher vor. Ich wende sie bei allen Aufgabenteilen an:

a.  $\varphi(6)$

$$\varphi(6) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = 2$$

b.  $\varphi(49)$

$$\varphi(49) = \varphi(7^2) = 7 \cdot 6 = 42$$

c.  $\varphi(98)$

$$\varphi(98) = \varphi(2) \cdot \varphi(7^2) = 1 \cdot 42 = 42$$

d.  $\varphi(196)$

$$\varphi(196) = \varphi(2^2) \cdot \varphi(7^2) = 2 \cdot 1 \cdot 42 = 84$$

e.  $\varphi(392)$

$$\varphi(392) = \varphi(2^3) \cdot \varphi(7^2) = 2^2 \cdot 1 \cdot 42 = 168$$

f.  $\varphi(1176)$

$$\varphi(1176) = \varphi(2^3 \cdot 3 \cdot 7^2) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(7^2) = 2^2 \cdot 1 \cdot 2 \cdot 42 = 336$$

### 3. Aufgabe

Machen Sie diese Aufgabe erst, wenn Sie Aufgabe 2 gerechnet haben

- a. Stellen Sie fest, ob  $3^{180126} - 1$  durch 7 teilbar ist.  
Es ist  $3^{180126} = 3^{30021 \cdot 6} = (3^6)^{30021} \equiv 1 \pmod{7}$ , also ist  $3^{180126} - 1$  durch 7 teilbar.
- b. Stellen Sie fest, ob  $37^{8442126} - 1$  durch 49 teilbar ist.  
Es war  $\varphi(49) = 42$ . Es ist:  
 $37^{8442126} = 37^{201003 \cdot 42} = (37^{42})^{201003} \equiv 1 \pmod{49}$ , also ist  $37^{8442126} - 1$  durch 49 teilbar.
- c. Folgern Sie:  $37^{8442126} - 1$  ist auch durch 98 teilbar  
Das folgt aus der Tatsache, dass auch  $\varphi(98) = 42$  ist.
- d. Stellen Sie fest, ob  $25^{84168252} - 1$  durch 196 teilbar ist.  
Es war  $\varphi(196) = 84$ . Es ist:  
 $25^{84168252} = 25^{1002003 \cdot 84} = (25^{84})^{1002003} \equiv 1 \pmod{196}$ , also ist  $25^{84168252} - 1$  durch 196 teilbar.

### 4. Aufgabe

Machen Sie auch diese Aufgabe erst, wenn Sie Aufgabe 2 gerechnet haben. Berechnen Sie hohe Potenzen mod  $q$ . Verwenden Sie dabei den Satz von Euler. Genauer: Geben Sie  $x$  mit  $0 \leq x < q$  an, sodass

- a.  $x \equiv 5^{84} \pmod{49}$   
 $5^{84} \pmod{49} \equiv (5^{42})^2 \pmod{49} \equiv (5^{\varphi(49)})^2 \pmod{49} \equiv 1 \pmod{49}$ , also  $x = 1$
- b.  $x \equiv 5^{127} \pmod{98}$   
 $5^{127} \pmod{98} \equiv (5^{42})^3 \cdot 5 \pmod{98} \equiv (5^{\varphi(98)})^3 \cdot 5 \pmod{98} \equiv 5 \pmod{98}$ , also  $x = 5$
- c.  $x \equiv 5^{254} \pmod{196}$   
 $5^{254} \pmod{196} \equiv (5^{84})^3 \cdot 5^2 \pmod{196} \equiv (5^{\varphi(196)})^3 \cdot 25 \pmod{196} \equiv 25 \pmod{196}$ , also  $x = 25$

- d.  $x \equiv 5^{169} \pmod{392}$   
 $5^{169} \pmod{392} \equiv 5^{168} \cdot 5 \pmod{392} \equiv 5^{\varphi(392)} \cdot 5 \pmod{392} \equiv 5 \pmod{392}$ , also  
 $x = 5$
- e.  $x \equiv 5^{336} \pmod{1176}$   
 $5^{336} \pmod{1176} \equiv 5^{\varphi(1176)} \pmod{1176} \equiv 1 \pmod{1176}$ , also  $x = 1$

## 5. Aufgabe

- a. Zeigen Sie: Das Gleichungssystem

- $x \equiv 12 \pmod{15}$
- $x \equiv 7 \pmod{16}$

hat genau eine Lösung mod  $15 \cdot 16$ , also mod 240. Geben Sie die Lösung an.

Ich argumentiere entlang dem Beweis des chinesischen Restsatzes:

Es ist  $16 - 15 = 1$ , wenn ich also:

$x = 12 \cdot 16 - 7 \cdot 15 = 87$  setze, dann ist:

- $87 = 12 \cdot 16 - 7 \cdot 15 \equiv 12 \cdot 16 - 12 \cdot 15 \pmod{15}$   
 $\equiv 12 \cdot (16 - 15) \pmod{15} \equiv 12 \pmod{15}$
- $87 = 12 \cdot 16 - 7 \cdot 15 \equiv 7 \cdot 16 - 7 \cdot 15 \pmod{16}$   
 $\equiv 7 \cdot (16 - 15) \pmod{16} \equiv 7 \pmod{16}$

Sei jetzt  $y$  eine andere Zahl, für die gilt:

- $y \equiv 12 \pmod{15}$ , also  $87 - y \equiv 0 \pmod{15}$
- $y \equiv 7 \pmod{16}$ , also  $87 - y \equiv 0 \pmod{16}$

Es folgt:  $87 - y \equiv 0 \pmod{\text{kgV}(15, 16)} \equiv 0 \pmod{240}$

Das bedeutet: 87 ist die einzige Lösung mod 240.

b. Zeigen Sie: Das Gleichungssystem

- $x \equiv 8 \pmod{15}$
- $x \equiv 11 \pmod{12}$

hat 3 Lösungen mod  $15 \cdot 12$ , also mod 180. Geben Sie die Lösungen an.

Es ist  $15 - 12 = 3$ , wenn ich also:

$x = 11 \cdot 5 - 8 \cdot 4 = 23$  setze, dann ist:

- $23 = 11 \cdot 5 - 8 \cdot 4 = 8 \cdot 5 - 8 \cdot 4 + 3 \cdot 5 \equiv$   
 $\equiv 8 \cdot (5 - 4) \pmod{15} \equiv 8 \pmod{15}$
- $23 = 11 \cdot 5 - 8 \cdot 4 = 11 \cdot 5 - 11 \cdot 4 + 3 \cdot 4 \equiv$   
 $\equiv 11 \cdot (5 - 4) \pmod{12} \equiv 11 \pmod{12}$

Es gilt:  $\text{kgV}(15, 12) = 60$ .

Damit sind auch  $23 + 60 = 83$  und  $23 + 120 = 143$  eine Lösungen des obigen Gleichungssystems, die alle mod 180 verschieden sind.

c. Zeigen Sie: Das Gleichungssystem

- $x \equiv 8 \pmod{15}$
- $x \equiv 10 \pmod{12}$

hat keine Lösungen mod  $15 \cdot 12$ , also mod 180.

Wir nehmen an, es gebe eine Lösung  $x$ . Es folgt, dass es  $r, s \in \mathbb{Z}$  gibt, so dass:

$8 + r \cdot 15 = 10 + s \cdot 12$  gilt. Daraus würde folgen:

$$2 = r \cdot 15 - s \cdot 12$$

Und damit wäre  $3 = \text{ggT}(15, 12)$  ein Teiler von 2. Das ist ganz offensichtlich nicht der Fall und daher gibt es auch keine Lösung bei dem obigen Gleichungssystem.

- d. Wie vereinbaren sich die Ergebnisse von Teil b) und Teil c) mit dem Chinesischen Restsatz?

Bei Teil b) und Teil c) kann der chinesische Restsatz nicht angewendet werden, da die modulo-Zahlen 15 und 12 nicht teilerfremd sind. Das wird aber im chinesischen Restsatz verlangt.

## 6. Aufgabe

Hinweis: Zu dieser Aufgabe beachten Sie bitte das Programm

- **RSACodierung**

auf meiner Homepage bzw. auf der Seite des Verlags. Es ist im Ordner „Kapitel08“ im Verzeichnis der Programme zu diesem Buch zu finden.

Gegeben der Text „Eintreffen Freitag zehn Uhr“. Verschlüsseln Sie diesen Text, indem Sie

- Zunächst jedem Buchstaben gemäß seiner Reihenfolge im Alphabet eine Zahl zuordnen
- Und anschließend jede dieser Zahlen gemäß dem public-key-Tupel  $(n, e)$  verschlüsseln.

Machen Sie das für die public-key-Tupel

- a.  $(n, e) = (65, 7)$

Text	e	i	n	t	r	e	f	f	e	f	r
Zahlen	5	9	14	20	18	5	6	6	5	6	18
Codes	60	9	14	45	47	60	46	46	60	46	47

Text	e	i	t	a	g	z	e	h	n	u	h	r
Zahlen	5	9	20	1	7	26	5	8	14	21	8	18
Codes	60	9	45	1	58	26	60	57	14	31	57	47

b.  $(n, e) = (239117, 4973)$  (Hinweis:  $239117 = 487 \cdot 491$ )

Text	e	i	n	t	r	e
Zahlen	5	9	14	20	18	5
Codes	173088	166122	130809	103254	183020	173088

Text	f	f	e	f	r	e
Zahlen	6	6	5	6	18	5
Codes	47778	47778	173088	47778	183020	173088

Text	i	t	a	g	z	e
Zahlen	9	20	1	7	26	5
Codes	166122	103254	1	184509	162316	173088

Text	h	n	u	h	r
Zahlen	8	14	21	8	18
Codes	13878	130809	9104	13878	183020

c.  $(n, e) = (60491, 3851)$

Es ist 60491 das Produkt der beiden Primzahlen 241 und 251

Text	e	i	n	t	r	e
Zahlen	5	9	14	20	18	5
Codes	38157	13640	46238	1526	18244	38157

Text	f	f	e	f	r	e
Zahlen	6	6	5	6	18	5
Codes	33252	33252	38157	33252	18244	38157

Text	i	t	a	g	z	e
Zahlen	9	20	1	7	26	5
Codes	13640	1526	1	55498	34496	38157

Text	h	n	u	h	r
Zahlen	8	14	21	8	18
Codes	48953	46238	5636	48953	18244



## 7. Aufgabe

Hinweis: Zu dieser Aufgabe beachten Sie bitte das Programm

- **RSADecodierung**

auf meiner Homepage bzw. auf der Seite des Verlags. Es ist im Ordner „Kapitel08“ im Verzeichnis der Programme zu diesem Buch zu finden.

Finden Sie zu jedem der public-key-Tupel  $(n, e)$  aus Aufgabe 6 den zugehörigen Wert  $d$ , mit dem die Texte wieder entschlüsselt werden können. Führen Sie jeweils die Entschlüsselung durch.

a.  $(n, e) = (65, 7)$

$$\phi(65) = \phi(5) \cdot \phi(13) = 4 \cdot 12 = 48, d = 7^{-1} \text{ in } \mathbf{Z}_{48} = 7.$$

Mit diesen Werten funktioniert die Entschlüsselung. Beispiel: Der Zahlenwert von ‚e‘ war 5, der Code von 5 war 60.  $60^7 \equiv 5 \cdot 60^4 \pmod{65} \equiv 25 \cdot 60 \pmod{65} \equiv 5 \pmod{65}$

b.  $(n, e) = (239117, 4973)$  (Hinweis:  $239117 = 487 \cdot 491$ )

$$\phi(239117) = \phi(487) \cdot \phi(491) = 486 \cdot 490 = 238140, d = 4973^{-1} \text{ in } \mathbf{Z}_{238140} = 48557.$$

Mit diesen Werten funktioniert die Entschlüsselung.

c.  $(n, e) = (60491, 3851)$

$$\phi(60491) = \phi(241) \cdot \phi(251) = 240 \cdot 250 = 60000, d = 3851^{-1} \text{ in } \mathbf{Z}_{60000} = 23651.$$

Mit diesen Werten funktioniert die Entschlüsselung.

## 8. Aufgabe

Hinweis: Auch zu dieser Aufgabe beachten Sie bitte das Programm

- **RSADecodierung**

auf meiner Homepage bzw. auf der Seite des Verlags. Es ist im Ordner „Kapitel08“ im Verzeichnis der Programme zu diesem Buch zu finden.

Entschlüsseln Sie die folgenden Texte:

- a. 1, 31, 46, 4, 60, 47, 52, 1, 31, 60, 47 (verschlüsselt mit (65, 7))

Codes	1	31	46	4	60	47	52	1	31	60	47
Zahlen	1	21	6	4	5	18	31	1	21	5	18
Text	a	u	f	d	e	r	m	a	u	e	r

Also: **Auf der Mauer**

- b. 1, 9104, 47778, 115539, 173088, 183020, 205002, 1, 9104, 173088, 183020  
(verschlüsselt mit (239117, 4973))

Codes	1	9104	47778	115539	173088	183020
Zahlen	1	21	6	4	5	18
Text	a	u	f	d	e	r

Codes	205002	1	9104	173088	183020
Zahlen	12	1	21	5	18
Text	l	a	u	e	r

Also: **auf der Lauer**

- c. 15205, 13640, 1526, 34496, 1526, 46238, 38157, 7750, 36635, 38157, 13640, 46238, 38157, 32719, 1, 46238, 34496, 38157 (verschlüsselt mit (60491, 3851))

Codes	15205	13640	1526	34496	1526	46238
Zahlen	19	9	20	26	20	14
Text	s	i	t	z	t	n

Codes	38157	7750	36635	38157	13640	46238
Zahlen	5	11	12	5	9	14
Text	e	k	l	e	i	n

Codes	38157	32719	1	46238	34496	38157
Zahlen	5	23	1	14	26	5
Text	e	w	a	n	z	e

Also: **sitzt** `ne kleine Wanze