

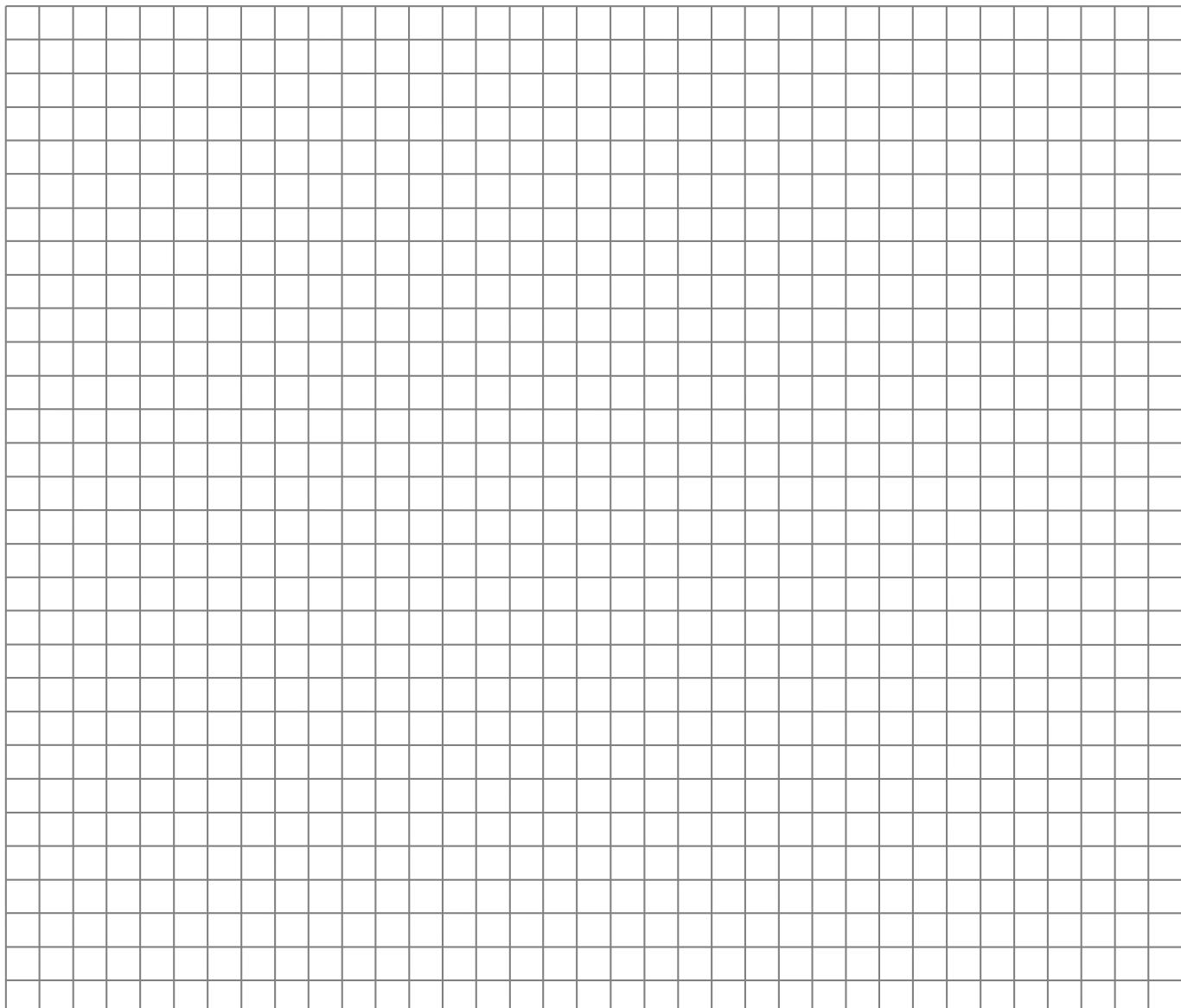
HOCHSCHULE ESSLINGEN

| | |
|---|--|
| Sommersemester 2021 | Zahl der Blätter: 11 Blatt 1 von 11 |
| Studiengang: SWB: Dozent: Strecker | Semester: SWB2 |
| Prüfungsfach: Diskrete Mathematik | Prüfungsnummer: 1052034 |
| Hilfsmittel: Literatur; Manuskript; ausgegebener Taschenrechner Casio FX-87DE PLUS oder Casio FX-87DE PLUS 2nd Edition | Zeit: 90 min. 60 Punkte |

Aufgabe 1 Mengenlehre (6 Punkte)

Seien $A, B, C \neq \emptyset$ Mengen. Zeigen Sie, dass $(A \cup B) \cup C = A \cup (B \cup C)$ gilt, d.h., dass die Vereinigung von Mengen assoziativ ist.

Hinweis: Sie dürfen voraussetzen, dass für die logische Oder-Verknüpfung das Assoziativgesetz gilt, d.h., für die drei Aussagen p, q, r gilt $(p \vee q) \vee r = p \vee (q \vee r)$



| | |
|-----------------------------------|-------------------------|
| Sommersemester 2021 | Blatt 2 von 11 |
| Prüfungsfach: Diskrete Mathematik | Prüfungsnummer: 1052034 |

Aufgabe 2 Induktion (6 Punkte)

Beweisen Sie mit vollständiger Induktion die Formel $(1 + 2 + \dots + n)^2 = 1^3 + 2^3 + \dots + n^3$

Hinweis: $1 + 2 + \dots + n = \frac{n(n+1)}{2}$

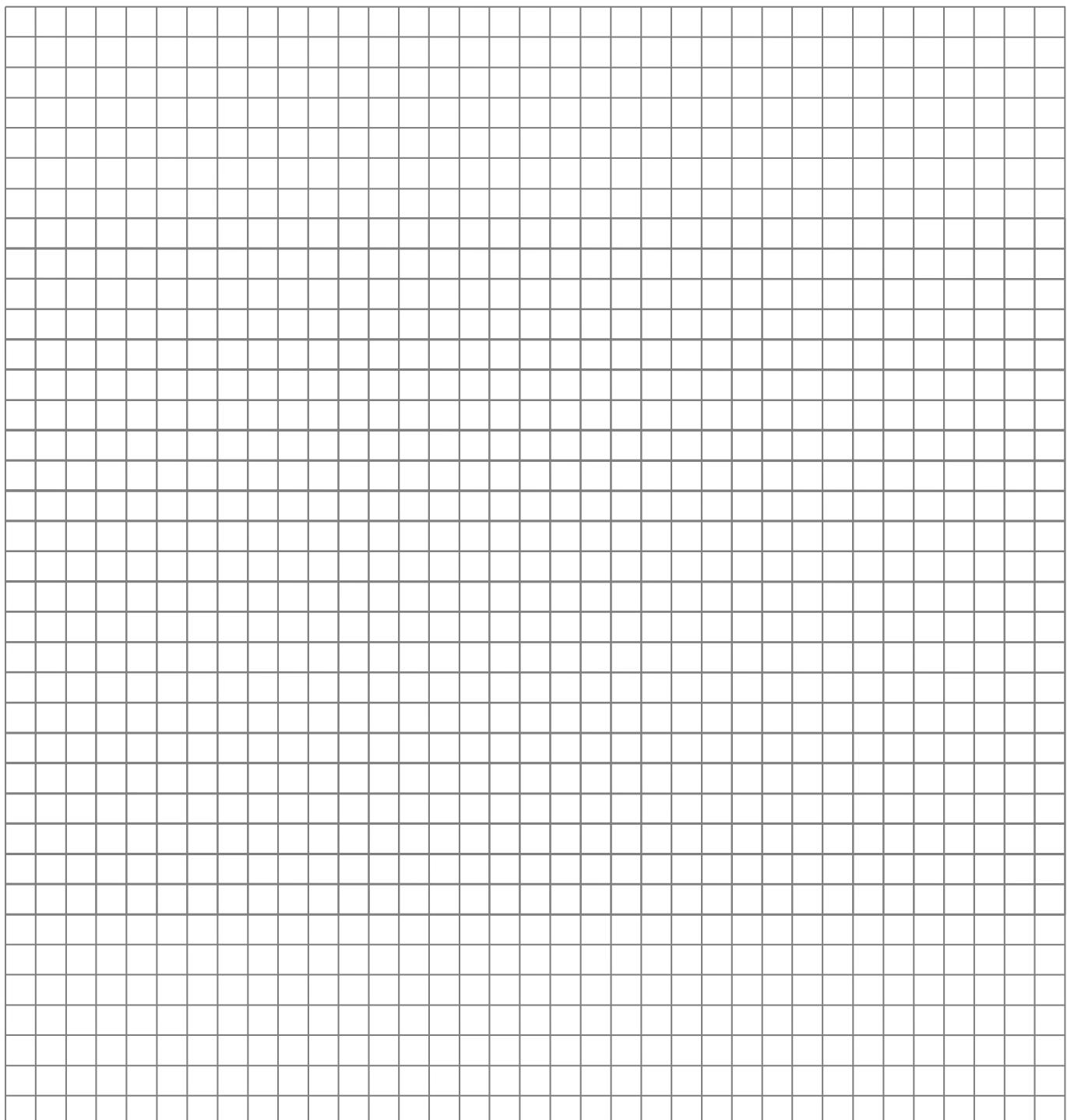
| | |
|-----------------------------------|-------------------------|
| Sommersemester 2021 | Blatt 3 von 11 |
| Prüfungsfach: Diskrete Mathematik | Prüfungsnummer: 1052034 |

Aufgabe 3 Chinesischer Restsatz (6 Punkte)

Gegeben seien die drei simultanen Kongruenzen

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 1 \pmod{5} \\ x \equiv 0 \pmod{4} \end{cases}$$

- a) Begründen Sie, warum das System lösbar ist.
- b) Geben Sie eine Lösung des Systems an.


 A large rectangular grid consisting of approximately 20 columns and 30 rows of small squares, intended for students to work out their calculations for the problem.

Aufgabe 4 Linearkombination des größten gemeinsamen Teilers (6 Punkte)

Bestimmen Sie mit Hilfe des erweiterten Euklidischen Algorithmus die Linearkombination des größten gemeinsamen Teilers d der beiden Zahlen $a = 56$ und $b = 23$

| Gibt nur Rest | | | | |
|---------------|----------------------------|---|-----------------------------------|-----------------------------------|
| i | $r_i = r_{i-1} \% r_{i-1}$ | $q_{i-1} = \frac{r_{i-1} - r_i}{r_{i-1}}$ | $s_i = s_{i-1} - q_{i-1} s_{i-1}$ | $t_i = t_{i-1} - q_{i-1} t_{i-1}$ |
| 0 | $r_0 = 56$ | $q_0 = 0$ | $s_0 = 1$ | $t_0 = 0$ |
| 1 | $r_1 = 23$ | $q_1 = \frac{56 - 23}{23} = 2$ | $s_1 = 0$ | $t_1 = 1$ |
| 2 | $r_2 = 23 \% 23 = 0$ | $q_2 = \frac{23 - 0}{23} = 1$ | $s_2 = 1 - 2 \cdot 0 = 1$ | $t_2 = 0 - 2 \cdot 1 = -2$ |
| 3 | $23 \% 1 = 0$ | $q_3 = \frac{0 - 0}{1} = 0$ | $s_3 = 0 - 2 \cdot 1 = -2$ | $t_3 = 1 - 2 \cdot (-2) = 5$ |
| 4 | $1 \% 1 = 0$ | $q_4 = \frac{0 - 0}{1} = 0$ | $s_4 = 1 - 3 \cdot (-2) = 7$ | $t_4 = -2 - 3 \cdot 5 = -17$ |
| 5 | $1 \% 0 = 0$ | - | - | - |

$$\hookrightarrow \text{folglich gilt: ggT}(56, 23) = 1 \equiv 7 \cdot 56 - 17 \cdot 23$$

Aufgabe 5 Primitivwurzel modulo m (6 Punkte)

Betrachten Sie den Körper $\mathbb{Z}/11\mathbb{Z}$.

- Geben Sie die Anzahl der primitiven Wurzeln in $\mathbb{Z}/11\mathbb{Z}$ an.
- Schreiben Sie die multiplikative Gruppe $(\mathbb{Z}/11\mathbb{Z})^\times$ in Potenzen einer Primitivwurzel w , d.h., $((\mathbb{Z}/11\mathbb{Z})^\times, \cdot) = \{w, w^2, \dots, w^{10}\}$

a) ① $\varphi(p)$ herausfinden:

$$p = 11 \rightarrow \text{also } \varphi(p) = 10$$

② Anzahl der primitiven Wurzeln:

$$\varphi(p-1) = \varphi(10) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$$

\hookrightarrow Anzahl Teiler der primitiven Wurzeln ist 4

b) ③ Teiler d von Ordnung 10 herausfinden:

$$10 = 2 \cdot 5 = (1+1) \cdot (1+1) = 4$$

$$d = \{1, 2, 5, 10\}$$

④ Primzahlen testen:

$$\text{Primzahlen} < 11: \{1, 2, 3, 5, 7\}$$

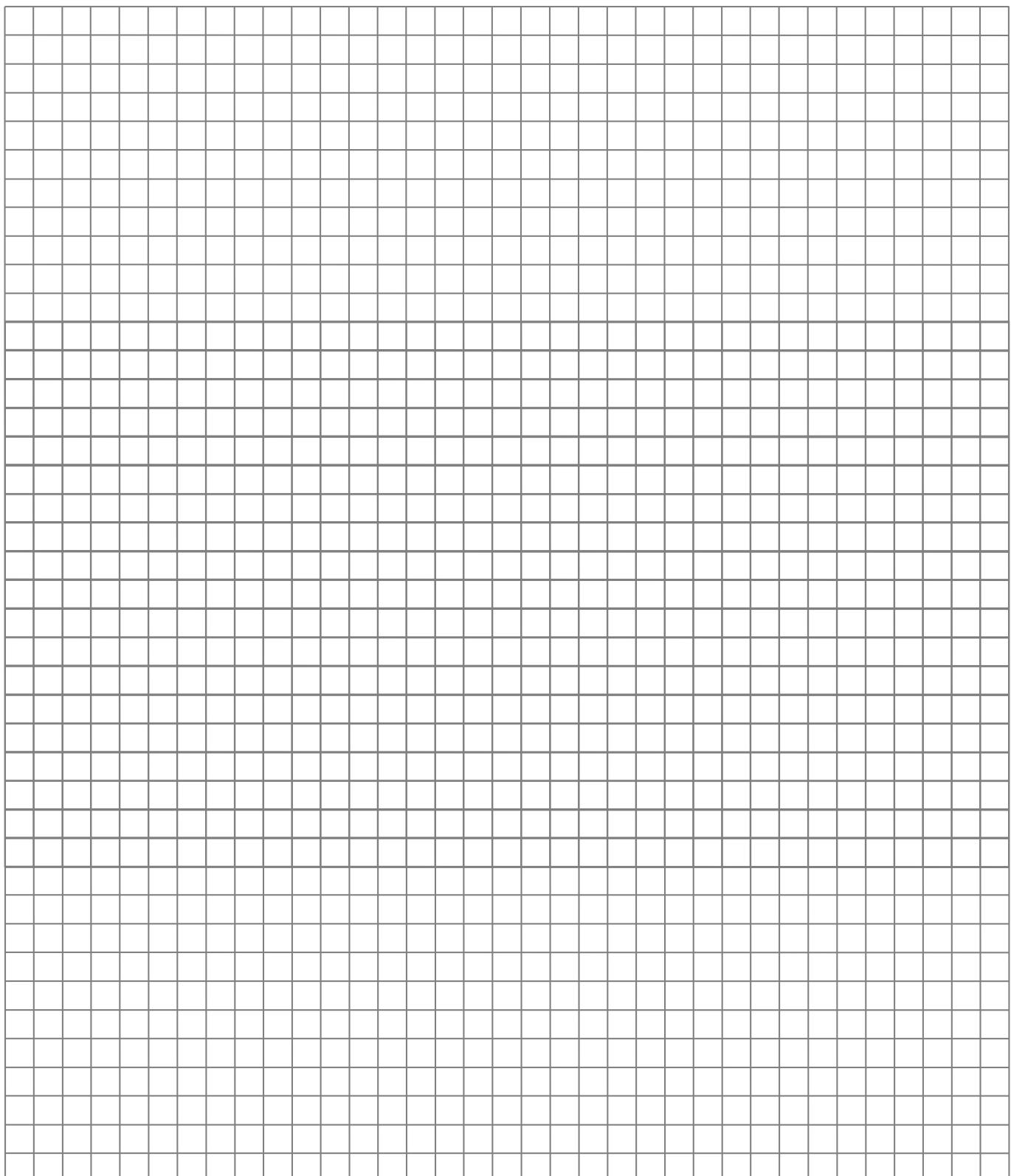
| d | 1 | 2 | 5 | 10 |
|---------------------------------|---|----|------------|------------|
| $\varphi(d)$ | 1 | 1 | 4 | 4 |
| $a \in \mathbb{Z}/11\mathbb{Z}$ | 1 | 10 | 3, 4, 5, 9 | 2, 6, 7, 8 |

\hookrightarrow somit ist z.B. $(\mathbb{Z}/11\mathbb{Z})^\times = \{w^1, \dots, w^{10}\}$, $w = \bar{2}$

| | |
|-----------------------------------|-------------------------|
| Sommersemester 2021 | Blatt 6 von 11 |
| Prüfungsfach: Diskrete Mathematik | Prüfungsnummer: 1052034 |

Aufgabe 6 Linearer Kongruenzgenerator (4 Punkte)

Gegeben sei der lineare Kongruenzgenerator $x_n \equiv 21 \cdot x_{n-1} + 3 \pmod{40}$.
Zeigen Sie, dass die Periode des Generators maximal wird.

A large grid of squares, approximately 20 columns by 20 rows, intended for students to show their work for the assignment.

(Angenommen p, q nicht gegeben, nur Zahl 527, dann Primfaktorzerlegung und schaue, welches Element keinen Rest bei Division gibt)

Aufgabe 7 Schlüsselpaar im RSA (6 Punkte)

Geben Sie ein Paar öffentlicher Schlüssel e und privater Schlüssel d für das Primzahlpaar $(p, q) = (17, 31)$ an. \leftarrow im RSA Verfahren p, q immer Primzahlen

Ansatz:

$$\textcircled{1} \text{ berechnen } n = p \cdot q = 17 \cdot 31 = 527$$

$$\textcircled{2} \text{ berechnen } \varphi(527) = \varphi(17) \cdot \varphi(31) \leftarrow \varphi(527) = 526 \text{ } \cancel{\text{ist w\"ore falsch, da 527 keine Primzahl!!!!}}$$

$$\hookrightarrow \varphi(527) = \varphi(17) \cdot \varphi(31)$$

$$= 16 \cdot 30 \leftarrow \text{da es sich um Primzahlen bei 17 und 31 handelt, 16 und 30 teilerfremde}$$

$$= 480$$

$$\textcircled{3} \text{ Primzahl } e \text{ finden die teilerfremd zu } \varphi(pq), \text{ also teilerfremd zu } 480 \text{ ist:}$$

$$\hookrightarrow \text{ggT}(e, \varphi(pq)) = 1, \text{ dann ist } e \text{ teilerfremd}$$

\rightarrow Ansatz: einfach 480: e und schaue, bei welcher Primzahl Rest r\"uckt

$$\hookrightarrow 480 \equiv 0 \pmod{2}, 480 \equiv 0 \pmod{3}, \dots 480 \equiv 4 \pmod{7}$$

$$\hookrightarrow \text{Rest bei } e=7$$

$$\textcircled{4} \text{ multiplikatives inverse } d \text{ f\"ur } e=7 \text{ finden:}$$

\hookrightarrow allgemeine Formel f\"ur multiplikatives inverses bei RSA:

$$e \cdot d \equiv 1 \pmod{\varphi(n)} \leftarrow \text{nicht f\"ur aufgegebene relevant aber allgemeiner Ansatz f\"ur Primzahlen } rx \equiv 1 \pmod{p} \text{!}$$

$$7 \cdot d \equiv 1 \pmod{480}$$

$\textcircled{5}$ erweiterter euklidischer Algorithmus:

| i | $r_i = r_{i-2} \% r_{i-1}$ | $q_{i-1} = \frac{r_{i-2} - r_i}{r_{i-1}}$ | $s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$ | $t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$ |
|---|----------------------------|---|---|---|
| 0 | $r_0 = 480$ | $q_0 = 0$ | $s_0 = 1$ | $t_0 = 0$ |
| 1 | $r_1 = 7$ | $q_1 = \frac{480 - 7}{7} = 68$ | $s_1 = 0$ | $t_1 = 1$ |
| 2 | $r_2 = 480 \% 7 = 1$ | $q_2 = \frac{7 - 1}{7} + 1 = 1$ | $s_2 = 1 - 68 \cdot 0 = 1$ | $t_2 = 0 - 68 \cdot 1 = -68$ |
| 3 | $1 \% 1 = 0$ | $q_3 = \frac{1 - 0}{1} = 1$ | $s_3 = 0 - 1 \cdot 1 = -1$ | $t_3 = 1 - 1 \cdot (-68) = 69$ |
| 4 | $0 \% 1 = 0$ | $q_4 = \frac{0 - 0}{1} = 0$ | $s_4 = 1 - 1 \cdot (-1) = 2$ | $t_4 = -68 - 1 \cdot 69 = -137$ |

$$\hookrightarrow \text{folglich gilt: } \text{ggT}(480, 7) = 1 = 2 \cdot 480 - 137 \cdot 7 \leftarrow -137 \text{ multiplikatives inverses zu 7}$$

$$\textcircled{5} \text{ } d = -137 \text{ soll positiv sein! } \rightarrow d = -137 \equiv 343 \pmod{480}$$

$$\hookrightarrow \text{Schl\"usselpaar: } (e, d) = (7, 343)$$

Standardwerte \rightarrow

| | |
|-----------------------------------|-------------------------|
| Sommersemester 2021 | Blatt 8 von 11 |
| Prüfungsfach: Diskrete Mathematik | Prüfungsnummer: 1052034 |

Aufgabe 8 Zykel und Transpositionen in der symmetrischen Gruppe (6 Punkte)

- a) Gegeben seien die Zykel $\rho = (134), \sigma = (143)$ und $\tau = (1256)$ aus der symmetrischen Gruppe S_6 . Berechnen Sie Produkte $\sigma\rho, \rho\tau$ und $\sigma\tau\rho$.
- b) Gegeben sei der Zykel $\sigma = (23785) \in S_8$. Stellen Sie σ als Produkt von Transpositionen dar.

A large grid of squares, approximately 20 columns by 25 rows, intended for students to work out their solutions to the problems.

Aufgabe 9 Russische Bauern-Multiplikation (4 Punkte)

Multiplizieren Sie mit dem Algorithmus der Russischen Bauern-Multiplikation die beiden Zahlen $a = 56$ und $b = 23$

| a | b | p | Wertetabelle |
|---------------------|---------------------|------------------------|---|
| 56 | 23 | 0 | a gerade $\hookrightarrow a = \frac{a}{2}$, $b = 2b$ |
| $\frac{56}{2} = 28$ | $23 \cdot 2 = 46$ | 0 | a gerade $\hookrightarrow a = \frac{a}{2}$, $b = 2b$ |
| $\frac{28}{2} = 14$ | $46 \cdot 2 = 92$ | 0 | a gerade |
| $\frac{14}{2} = 7$ | $92 \cdot 2 = 184$ | 0 | a ungerade $\hookrightarrow a = \frac{a}{2}$ (abgerundet), $b = 2b$ $\Rightarrow a = q + b$ |
| $\frac{7}{2} = 3$ | $184 \cdot 2 = 368$ | $0 + 184$ $= 184$ | a ungerade |
| $\frac{3}{2} = 1$ | $368 \cdot 2 = 736$ | $368 + 184$ $= 582$ | a ungerade |
| $\frac{1}{2} = 0$ | - | $= 1788$ | |

$$\hookrightarrow p = 1788 = 56 \cdot 23$$

man schaut
immer bei 1

Aufgabe 10 Rechnen im Galois-Feld $GF(3^2)$ (10 Punkte)

Gegeben sei die Tabelle der Diskreten Logarithmen des Galois-Felds $GF(3^2)$ mit dem Generatorpolynom $g(X) = 2X$ ← das hier soll das erzeugende Element sein

| $a \in GF(3^2) \setminus \{(0, 0, 0)\}$ | a als Polynom | $\log_{2X} a$ der Exponent |
|---|-----------------|----------------------------|
| (0, 1) | 1 | Dies ist die Basis 8 |
| (0, 2) | 2 | 4 |
| (1, 0) | X | 5 |
| (1, 1) | $X + 1$ | 2 |
| (1, 2) | $X + 2$ | 3 |
| (2, 0) | $2X$ | 1 |
| (2, 1) | $2X + 1$ | 7 |
| (2, 2) | $2X + 2$ | 6 |

3 bedeutet $\mathbb{Z}/3\mathbb{Z}$ also Nullstellen

können 0, 1, 2 sein

2 bedeutet Polynom 2-1 grades, also

1. Grades möglich

z.B. $(ax+b)$

a stellt sowohl den Exponenten dar, es gibt

insgesamt 9 Elemente also $3^2 = 9$

Elemente, aber die 0 wird hier

nicht mitgerechnet also $9 - 1 = 8$

Elemente ohne 0

} Es werden die Elemente
gesucht für $2x^a$

- Zeigen Sie, dass das Polynom $p(X) = X^2 + 2X + 2$ irreduzibel in $\mathbb{Z}/3\mathbb{Z}[X]$ ist. ← in $\mathbb{Z}/3\mathbb{Z}$ gibt es Nullstellen 0, 1, 2, diese einsetzen in $p(x)$ um checken ob Nullstellen
- Berechnen Sie die fehlenden Diskreten Logarithmen in der Tabelle oben.
- Berechnen Sie für $a = (1, 1), b = (2, 2)$ mit Hilfe der Tabelle das Produkt ab und das Inverse a^{-1} von a ← Hier Exponenten von a und b ablesen, addieren, schon was vorbereitet

a) Ansatz:

↪ Polynom $p(x) = x^2 + 2x + 2 \rightarrow$ Polynom 2 Grades, da x^2

↪ Faktor Grad muss ≥ 1 sein, also sowohl $2 = 1+1$.

① Überprüfen auf Nullstellen:

↪ Polynom 2. Grades irreduzibel, wenn es keine Nullstelle besitzt. Wenn Polynom 2. Grades

reduzibel wäre könnte in Linearfaktoren (also als Produkt zweier Polynome p, q ersten Grades)

↪ Diese Linearfaktoren entsprechen Nullstellen des Polynoms

$$\rightarrow p(0) = 0^2 + 2 \cdot 0 + 2 = 2 \not\equiv 0 \pmod{3} \leftarrow \text{Nullstelle in } \mathbb{Z}/3\mathbb{Z} \text{ alle } 0, 3, 6 \text{ etc., d.h. } 2 \text{ keine!}$$

$$p(1) = 1^2 + 2 \cdot 1 + 2 = 5 \not\equiv 0 \pmod{3}$$

$$p(2) = 2^2 + 2 \cdot 2 + 2 = 10 \not\equiv 0 \pmod{3}$$

↪ $p(x)$ besitzt im Körper $\mathbb{Z}/3\mathbb{Z}$ also keine Nullstellen und ist deshalb irreduzibel

→ Schritt der Irreduzibilität war notwendig da man nur irreduzible Polynome vollen Grades

(also hier 3. Grades der x^3) für den reduzieren mit mod verwenden kann

b) ② bestimmen der fehlenden Logarithmen:

↳ was genau ist gesucht?

→ Es sind die passenden Exponenten gesucht zur Basis $2x$.

↳ also $(2x)^2$, $(2x)^3$, $(2x)^5$ Exponenten gehen von 1 bis 8

③ Potenzen ausrechnen und anschließend nach $x^2 + 2x + 2$ reduzieren:

$$(2x)^2 \equiv 4x^2 \text{ mod } 3 \equiv x^2 \text{ mod } x^2 + 2x + 2 \equiv x^2 - (x^2 + 2x + 2) \equiv -2x - 2 \text{ mod } 3 \equiv x + 1$$

↑ außerhalb des Körpers $\mathbb{Z}/3\mathbb{Z}$ nur 0, 1, 2 erhält doch $\text{mod } x^2 + 2x + 2$, da nur x^1 erlaubt, mod ist bei $\text{mod } 3$ zuerst $\text{mod } 3$ rechnen bevor man mit Polynom fortfährt. Polynome gehen das gleiche wie einfach Subtraktion!! wieder umwendlich in positive

↳ Bei höheren Potenzen die größer sind als Grad 2 (also größer als $x^2 + 2x + 2$)

nimmt das Polynom zuerst zerlegt werden in kleinere Polynome:

→ $(2x)^3 = 8x^3 \text{ mod } 3 = 2x^3 \leftarrow 2x^3 \text{ zu groß um direkt } \text{mod } x^2 + 2x + 2 \text{ zu reduzieren}$ deshalb aufteilen

↳ $2x^3 = 2(x \cdot x^2) \leftarrow x^2 \text{ ist mit } \text{mod } x^2 + 2x + 2 \text{ zerlegbar}$

$$\leftarrow x^2 \text{ mod } x^2 + 2x + 2 \equiv x^2 - (x^2 + 2x + 2) \equiv x^2 - x^2 - 2x - 2 \equiv -2x - 2 \text{ mod } 3 \equiv x + 1$$

↳ $x + 1$ einsetzen für x^2 :

$$\rightarrow 2(x \cdot (x+1)) = 2x^2 + 2x \text{ mod } x^2 + 2x + 2 \equiv 2x^2 + 2x - x^2 - 2x - 2 \equiv x^2 - 2$$

$$\equiv x^2 + 1 \text{ mod } 3 \equiv (x+1) + 1 \equiv x + 2$$

→ alternativer schnellerer Weg (einfach direkt immer $x+1$ für x^2 einsehen)

$$2(x \cdot (x+1)) = 2x^2 + 2x = 2(x+1) + 2x = 2x + 2 + 2x = 4x + 2 \equiv x + 2 \text{ mod } 3$$

$$\rightarrow (2x)^5 = 32x^5 \equiv 2x^5 \text{ mod } 3$$

$$\leftarrow 2(x^2 \cdot x^3) \equiv 2((x+1) \cdot (x \cdot (x+1))) \equiv 2((x+1) \cdot (x^2 + x)) \equiv 2((x+1) \cdot ((x+1) + x))$$

$$\equiv 2((x+1) \cdot (2x+1)) \equiv 2(2x^2 + x + 2x + 1) \equiv 2((2(x+1)) + 3x + 1) \equiv 2(2x + 2 + 3x + 1)$$

$$\equiv 2(5x + 3) \equiv 10x + 6 \text{ mod } 3 \equiv x$$

c) Wie findet man das inverse zu a?

↪ man sucht das Element, dessen Logarithmus, wenn zu dem von a addiert

0 ergibt (mod der Größe des Feldes, in diesem Fall 8 weil $GF(3^2)$ 9 Elemente hat)

aber 0 kein inverses besitzt deshalb $g-1=7$ und Log-Elemente nur für nicht 0-Elemente definiert sind)

→ Für den Diskreten Log gilt $g^0 = 1$, das ist grundsätzlich so

↪ wir haben die Exponenten des Log zur Basis $2x$ ja in der Tabelle gegeben.

↪ d.h. wenn diese Exponenten 0 wären, dann hat man $g^0 = 1$ und da das inverse

zu $a \cdot a^{-1} \equiv 1 \pmod{p}$ sein muss wäre die Lösung

↪ wir wissen auch, dass wenn man Exponenten multipliziert diese einfach addiert

$$\hookrightarrow \text{also } (2x)^2 \cdot (2x)^6 = (2x)^{2+6} = (2x)^8$$

$$\hookrightarrow \text{also } 2+6=8=0 \pmod{8} \quad \checkmark$$

→ Erklärung: In Galois Feld rechnet man immer mod 3, für diskrete Logarithmen

in Feld verwendet man aber $p^n - 1 = 3^2 - 1 = 8$, da 8 nicht null Elemente

→ Musterlösung:



→ Man entnimmt der Tabelle $\log_{2x}(1,1) + \log_{2x}(2,2) = 2+6=8 = \log_{2x}(0,1)$.

somit ist das Produkt der vorhale Element und deshalb sind a und b zueinander invers

Erklärung Galois Feld:

→ GF(3):

↪ stellt nichts anderes dar als einer Körper $\mathbb{Z}/3\mathbb{Z}$ mit 0,1,2

↪ GF(2) wäre dementsprechend Körper $\mathbb{Z}/2\mathbb{Z}$ mit 0,1 als Koeffizienten

→ GF(p^n):

↪ p stellt Primzahl dar und n ist eine positive ganze Zahl

↪ Elemente des Feldes:

↪ Elemente von $GF(p^n)$ sind Polynome bis zum Grad $n-1$, wobei die Koeffizienten aus $GF(p)$ stammen

→ Beispiel $GF(2^3)$:

↪ Koeffizienten nur aus $GF(2)$, also Körper $\mathbb{Z}/2\mathbb{Z}$, also 0,1

→ Polynome bis zum Grad $n-1$ möglich aber bis zum Grad $3-1=2$ möglich

↪ jedes Polynom kann also in ax^2+bx+c ausgedrückt werden, wobei a,b,c nur 0 oder 1 sein können

→ insgesamt sind $2^3 = 8$ unterschiedliche Polynome (Elemente) möglich

- ↪ 1. $0x^2 + 0x + 0 = 0$
2. $0x^2 + 0x + 1 = 1$
3. $0x^2 + 1x + 0 = x$
4. $0x^2 + 1x + 1 = x + 1$
5. $1x^2 + 0x + 0 = x^2$
6. $1x^2 + 0x + 1 = x^2 + 1$
7. $1x^2 + 1x + 0 = x^2 + x$
8. $1x^2 + 1x + 1 = x^2 + x + 1$

} (auch für a,b,c=0 ergetzt in ax^2+bx+c)

↪ diese repräsentieren alle möglichen Kombinationen der Koeffizienten

a,b,c in $GF(2^3)$

→ Teilbarkeit mod 2:

↪ Koeffizienten können in Körper $\mathbb{Z}/2\mathbb{Z}$, also GF(2), nur 0,1 sein, d.h. Zahl >1 oder <0 nicht möglich

↪ Beispiel:

↪ wenn nun z.B. 8 erhält, dann ist $8 \bmod 2 \equiv 0 \bmod 2$, $-1 \bmod 2 \equiv 1 \bmod 2$, $3 \bmod 2 \equiv 1 \bmod 2$

→ Polynome dürfen höchstens vom Grad 2 sein (also x^2)

↪ falls diese größer als Grad 2 (z.B. x^3), dann werden diese mit speziellum

Polynom vom Grad 3 reduziert (z.B. x^3+x (nur Beispielhaft))

(dieses Polynom ist dann aber eigentlich immer in Aufgabe gegeben)

→ wie man irreduzible Polynome finden würde:

↪ Liste aller irreduziblen Polynome → Form x^3+ax^2+bx+c , wobei a,b,c entweder 0,1

→ Test auf Irreduzibilität:

→ Polynom 3 Grades ist irreduzibel in GF(2), wenn es keine Nullstellen in GF(2) besitzt

und nicht als Produkt von Polynomen niedrigeren Grades dargestellt werden kann

↪ Bsp. x^3+x+1 oder x^3+x^2+1 könnte man verwenden

↪ also z.B. $\bmod x^3+x+1$

→ Beispiel mod Polynom:

↪ wenn man z.B. Polynome multiplizieren würde, welche in GF(2³) liegen

$$\hookrightarrow (x^2+x) \cdot (x+1) = x^3+x^2+x^2+x$$

$$= x^3+2x^2+x \leftarrow \text{der } \mathbb{Z}/2\mathbb{Z} \text{ nur } 0,1 \text{ wird Koeffizient } 2 \text{ zu } 2 \bmod 2 \equiv 0 \bmod 2 \text{ also zu } 0x^2$$

↪ nun x^3+x durch x^3+x^2+1 teilen:

↪ da Ergebnis bereits von Grad 3 subtrahiert man x^3+x^2+1 von x^3+x

$$\rightarrow (x^3+x) - (x^3+x^2+1) = x^3+x-x^3-x^2+1 = -x^2+x+1$$

mit Addition genau gleich
Hinweis: $= x^3+x+x^3+x^2+1 = 2x^3+x^2+x+1 \bmod 2 = x^2+x+1$

+ und - sind in Körper $\mathbb{Z}/2\mathbb{Z}$ genau das gleiche da $-1 \equiv 1 \bmod 2$ ist deshalb kann man statt - einfach immer + rechnen und sobald Koeffizienten größer 1 oder kleiner 0 kommen einfach mod 2 nehmen!

addieren statt subtrahieren ist nur in GF(2ⁿ) möglich in anderen z.B. GF(3ⁿ) nicht mehr möglich, einfach immer standardmäßig subtrahieren!!

→ also ist das Ergebnis von $(x^2+x) \cdot (x+1) = x^2+x+1$