

Diophantische Gleichungen

- A1:**
Berechne mit dem Euklidischen Algorithmus:
a. $\text{ggT}(150, 54)$ b. $\text{ggT}(300, 468)$ c. $\text{ggT}(44, 18)$ d. $\text{ggT}(992, 999)$
- A2:**
Berechne den ggT der Zahlen a und b und stelle ihn in der Form $ax + by$ dar.
a. $a = 531, b = 93$ b. $a = 753, b = 64$

- A3:**
Bestimme - falls möglich - eine Lösung (x/y) der angegebenen Gleichung:
a. $96x + 66y = 6$ b. $96x + 66y = 18$
d. $119x + 143y = 4$ e. $91x + 35y = 12$.

- A4:**
Vereinfache die Gleichung und finde möglichst viele Lösungen:
a. $42x + 126y = 84$ b. $81x + 54y = 27$ c. $77x + 121y = 44$

Kongruenzen

- A5:**
Bestimme möglichst alle ganzzahligen Lösungen x der folgenden Gleichungen:
a. $5 + x \equiv 2 \pmod{7}$ b. $5 \cdot x \equiv 2 \pmod{7}$
c. $5 \cdot x \equiv 2 \pmod{10}$ d. $-34 \equiv x \pmod{5}$

- A6:**
Beweise die folgenden Aussagen:
a. Wenn $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$, dann $a + c \equiv b + d \pmod{m}$.
b. Wenn $a \equiv b \pmod{m}$, dann $-a \equiv -b \pmod{m}$.
c. Wenn $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$, dann $a \equiv c \pmod{m}$.

Restklassen

- A7:**
Bestimme mit dem erweiterten Euklidischen Algorithmus:
a. $\frac{5}{33}$ in \mathbb{Z}_{37} . b. $\frac{7}{20}$ in \mathbb{Z}_{89} .
- A8:**
Bestimme mit dem kleinen Satz von Fermat:
a. 4^{-11} in \mathbb{Z}_{13} . b. 6^{31} in \mathbb{Z}_{29} . c. 6^{32} in \mathbb{Z}_{29} .

- A9:**
Berechne in \mathbb{Z}_{23} die folgenden Brüche:
a. $\frac{1}{5^{21}}$ b. $\frac{1}{10^{13}}$ c. $\frac{7}{10^{12}}$ d. $\frac{7}{22}$

Diffie-Hellman

- A10:**
a. Alice und Bob vereinbaren die Primzahl p und die Primitivwurzel g . Alice wählt a , Bob wählt b . Welche Zahlen werden veröffentlicht und wie heißt der gemeinsame Schlüssel?
a. $p = 7, g = 3, a = 3, b = 4$.
b. $p = 23, g = 7, a = 15, b = 17$.

- A11:**
Alice und Bob vereinbaren $p = 11$ und $g = 2$. Alice schickt an Bob $A = 5$ und Bob meldet an Alice $B = 8$. Da die Zahlen klein sind, kann die Diffie-Hellman Verschlüsselung geknackt werden. Nutze die Potenztabelle für \mathbb{Z}_{11} . Wie heißt der Schlüssel K ?

		Spalte hoch Zeile									
		1	2	3	4	5	6	7	8	9	10
1	1	1	2	3	4	5	6	7	8	9	10
2	1	4	9	5	3	3	5	9	4	1	
3	1	8	5	9	4	7	2	6	3	10	
4	1	5	4	3	9	9	3	4	5	1	
5	1	10	1	1	1	10	10	10	1	10	
6	1	9	3	4	5	5	4	3	9	1	
7	1	7	9	5	3	8	6	2	4	10	
8	1	3	5	9	4	4	9	5	3	1	
9	1	6	4	3	9	2	8	7	5	10	
10	1	1	1	1	1	1	1	1	1	1	

RSA

- A12:**
Bob wählt p, q und Verschlüsselungsexponent e . Warum ist e ein zulässiger Verschlüsselungsexponent? Wie heißt der öffentliche, wie der private Schlüssel von Bob? Alice will an Bob die Nachricht n verschlüsselt übermitteln. Welche Zahl schickt sie an Bob? Wie entschlüsselt Bob die Nachricht?
a. $p = 3, q = 11, e = 7, n = 6$.
b. $p = 7, q = 11, e = 47, n = 2$