Schriftliche Aufgaben

Name:

Aufgabe 5

Gegeben ist die Kongruenzgleichung

$$21x \equiv a \mod 51, \tag{1}$$

wobei $a \in \mathbb{N}$ später gewählt wird.

a) Gib eine zu (1) äquivalente diophantische Gleichung an.

$\boxed{}$ mit $y \in \mathbb{Z}$. (2)

b) Welche Bedingung müssen a und $\mathrm{ggT}(21, 51)$ erfüllen, damit die diophantische Gleichung (2) Lösungen besitzt?

Bedingung: $\boxed{}$.

c) Kreuze in der Tabelle an, für welche der gegebenen Zahlen a die Kongruenzgleichung (1) jeweils Lösungen besitzt.

$a =$	1	3	7	17	21	51
(1) besitzt Lösungen						

Weiter auf Seite 2

Aufgabe 6

Gegeben ist die Kongruenzgleichung

$$e \cdot 7 \equiv 1 \mod 60. \tag{3}$$

a) Gib eine zu (3) äquivalente diophantische Gleichung an.

$\square$ mit $y \in \mathbb{Z}$. (4)

b) Berechne mit Hilfe des erweiterten euklidischen Algorithmus eine Lösung von (4).

Erweiterter euklidischer Algorithmus:

Eine Lösung von (4): $(e \mid y) =$ $\square$.

c) Gib alle ganzzahligen Lösungen von (4) an.

$(e \mid y) =$ $\square$ mit $k \in \mathbb{Z}$.

d) Gib alle Lösungen von (3) an. $e =$ $\square$.

e) Gib die einzige Lösung x von (3) an, für die $1 < x < 60$ gilt.

$e =$ $\square$.

f) Mache die Probe. $e \cdot 7 =$ $\square$ $=$ $\square$ $\cdot 60 + 1$.

Weiter auf Seite 3

Aufgabe 7

Noah möchte sich Nachrichten schicken lassen, die mit dem Elgamal-Verfahren verschlüsselt sind. Er wählt $p = 31$, $g = 11$, $e = 24$ und berechnet

$$\begin{aligned} [11]^2 &= [121 - 124] = [-3], \\ [11]^6 &= [-3]^3 = [-27] = [4], \\ [A] &= [11]^{24} = [4]^4 = [64] \cdot [4] = [2] \cdot [4] = [8] \text{ in } \mathbb{Z}_{31}. \end{aligned}$$

Er veröffentlich also auf seiner Homepage $p = 31$, $g = 11$ und $A = 8$.

a) Anna möchte die Nachricht $n = 10$ für Noah verschlüsseln. Sie wählt den Verschlüsselungsexponent $v = 4$ und berechnet in $\mathbb{Z}_{31}$

$[B] =$ ☐, $[A]^4 =$ ☐, $[N] =$ ☐.

b) Emilia schickt an Noah $B = 4$ und $N = 3$. Berechne

$[B]^{-e} =$ ☐, $[n] =$ ☐ in $\mathbb{Z}_{31}$.

Aufgabe 8

Frank veröffentlicht auf seiner Homepage $m = 77$ und $v = 43$, damit Personen ihre Nachrichten an ihn mit RSA verschlüsseln können..

a) Gib die Werte an, die er gewählt bzw. berechnet hat.

$p =$ ☐, $q =$ ☐, $\widetilde{m} =$ ☐, $e =$ ☐ (beachte die vorigen Aufgaben).

b) Andrew schickt Frank die Zahl $N = 2$. Entschlüssle die Nachricht.

$n =$ ☐.