

Algebra-Zahlentheorie Aufgaben

- (1) Führen Sie den erweiterten euklidischen Algorithmus vollständig von Hand durch für das Zahlenpaar $(223, 70)$
 Prüfen Sie mit TI durch Eingabe von `ggte(223,70)`
 Prüfen Sie in wxMaxima mit `gcdex(223,70)`
gcd=greatest common divisor=ggd, ex=extended=erweitert)
 Bestimmen Sie von Hand 223 modulo 70 .
 TI: `mod(223,70)` wxMaxima `mod(223,70)`
- “von Hand” heißt:
mit allen
Zwischenschritten
- (2) Bestimmen Sie auf alle!!! auf Seite 15 vorgestellten Arten das Inverse von 13 modulo 70 und prüfen Sie von Hand.
- (3) Zerlegen Sie 70 in Primfaktoren (sinnvoll von Hand).
 Mit CAS: `factor(70)`
 Geben Sie begründet (mit systematischer Primfaktoren-Auswahl) alle Teiler von 70 an. Mit TI `teiler(70)` (Ha-Krypto-Tool) wxMaxima `divisors(70)`
- (4) Geben Sie von Hand durch einige Worte begründet die ersten 10 zu 70 teilerfremden Zahlen an.
 Bestimmen Sie mit CAS die Menge $Z^*(70)$.
 Mit TI `zstern(70)` (Ha-Krypto-Tool) mit wxMaxima `zstern(70)` (Ha-entpr. Datei)
- (5) Bestimmen Sie mit CAS die Anzahl der zu 70 teilerfremden Zahlen.
 Mit TI `euler(70)`, wxMaxima `eulerphi(70)` (Ha-entpr. Datei)
- (6) Geben Sie eine Liste der Potenzen von 13 modulo 70 an.
 TI: `seq (mod(13^k ,70) , k, 0,24)` seq=sequence=Folge
 wxMaxima `makelist(mod(13^k, 70) ,k,0,24)`
- (7) Lesen Sie aus ihrer Liste die Ordnung von 13 in $Z^*(70)$ ab.
 Mit TI `ordo(13,17)` (Ha-Krypto-Tool) wxMaxima `ordo(13,70)`
- (8) Taufen Sie die von 13 in $Z^*(70)$ erzeugte Untergruppe `grup`.
 Bestimmen Sie die Nebenklassen von $\langle 13 \rangle$ in $Z^*(70)$
 Verwenden Sie bei TI `mod(a*grup,70)` bei wxMaxima `mod(a*grup,70)`
- (9) Lösen Sie von Hand in $Z^*(70)$ die Gleichung $13 \cdot x = 19$.
- (10) Geben Sie in $Z^*(70)$ einige Quadratzahlen an, die in Z nicht Quadratzahlen sind. (Von Hand)
- (11) Wählen Sie selbst teilerfremde Zahlenpaare (nicht zu klein) entsprechend $(223,70)$ und $(13,70)$, bearbeiten Sie die Seite ebenso. Prüfen Sie alles selbst.