Zahlentheorie, Algebra, Kryptographie

Aufgabe 1 Zahlentheorie

a) Führen Sie für 1761 und 50 den erweiterten Euklidischen Algorithmus vollständig von Hand durch.
b) Geben Sie begründet das Inverse von 50 modulo 1761 an.
c) Zerlegen Sie 480 mit Kopfrechnen nachvollziehbar in Primfaktoren.
d) Zeigen Sie am Beispiel 480 und 504 wie die Primfaktorzerlegung für eine systematische Bestimung von ggT und kgV genutzt werden kann und bestimmen Sie diese dadurch.

Aufgabe 2 Algebra

a) Für welche n ist $(\mathbb{Z}_n, +)$ Gruppe?

b) Für welche n ist $(\mathbb{Z}_n, +, \bullet)$ nur Ring und nicht Körper? Für welche ist dies ein Körper?

c) Welche Menge wird mit $\mathbb{Z}^*_n$ bezeichnet, wieviele Elemente sind darin?

Zeigen Sie, dass $(\mathbb{Z}^*_6, \bullet)$ Gruppe ist, aber nicht $(\mathbb{Z}^*_6, +)$.

Aufgabe 3 Gruppentheorie

Es folgen die Gruppentafel und die Potenztafel von $\mathbb{Z}^*_{13}$

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	4	9	3	12	10	10	12	3	9	4	1
3	1	8	1	12	8	8	5	5	1	12	5	12
4	1	3	3	9	1	9	9	1	9	3	3	1
5	1	6	9	10	5	2	11	8	3	4	7	12
6	1	12	1	1	12	12	12	12	1	1	12	1
7	1	11	3	4	8	7	6	5	9	10	2	12
8	1	9	9	3	1	3	3	1	3	9	9	1
9	1	5	1	12	5	5	8	8	1	12	8	12
10	1	10	3	9	12	4	4	12	9	3	10	1
11	1	7	9	10	8	11	2	5	3	4	6	12
12	1	1	1	1	1	1	1	1	1	1	1	1

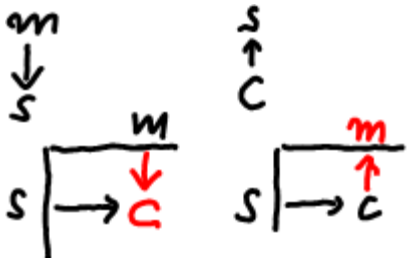
a) Woran erkennt man erzeugende Elemente und welche hat $\mathbb{Z}^*_{13}$?
b) Woran erkennt man die Ordnung der Elemente? Welche Elemente haben welche Ordnung?
c) Bilden Sie die von 8 erzeugte Untergruppe und ihre Nebenklassen. Welchen gruppentheoretischen Satz beweist man mit einer solchen -dann aber verallgemeinerten- Betrachtung.
d) Berechnen Sie unter Verwendung der Ordnung von 8 von Hand $8^{110} \bmod 13$.
e) Zeigen Sie an einem Beispiel mit der Potenztafel: Wenn g nicht erzeugendes Element ist, dann gibt es zwei Zahlen a und b mit $g^{ab} \underset{13}{\equiv} 1$.
f) Zeigen Sie dieses allgemein in $\mathbb{Z}^*_n$.

Aufgabe 4 Kryptographie, Diffie-Hellmann-Verfahren

Protokoll: Anton und Berta vereinbaren offen eine Primzahl p und eine Grundzahl g. Dann wählen sie sich geheim eine Zahl a, bzw. b, bilden $g^a \underset{p}{\equiv} : \alpha$, bzw. $g^b \underset{p}{\equiv} : \beta$ und senden sich offen das Ergebnis zu. Berta bildet dann $\alpha^b \underset{p}{\equiv} : k_b$ und Anton bildet $\beta^a \underset{p}{\equiv} : k_a$. Diffie und Hellmann nennen ihr Verfahren "Schlüsselvereinbarung" und empfehlen nun die Verwendung eines symmetrischen kryptographischen Verfahrens.

a) Wählen Sie p=13 und g als ein erzeugendes Element aus $\mathbb{Z}^*_{13}$. (->Aufgabe 3a).
b) Stellen sie graphisch mit selbst gewählten a und b dar, wer wem was sendet und was beim Berechnen herauskommt.
c) Zeigen Sie allgemein die Durchführbarkeit des Verfahrens.
d) In mathematisch ambitionierteren Kryptographie-Büchern wird erwähnt, dass g eine Primitivwurzel von $\mathbb{Z}^*_p$ sein sollte. Verwenden Sie 3e) und 3f) um diesen Anspruch zu begründen.

Aufgabe 5 Vigenère-Verfahren



Früher wurde das Vigenère-Verfahren mit Buchstaben durchgeführt, heute wird die Nachrricht in eine Zahl übersetzt, die dann **ziffernweise** mit einem symmetrischen als Zahl gegebenen Schlüssel codiert wird.

Führen Sie das für die Nachricht m und Schüssel s hier durch. Zeigen Sie **eine** Tabellenablesung deutlich.

m 3 1 1 2 8 7 9 3
s 5 0 3 4 8 5 4 3

Mathix behauptet, man müsse nur zum Verschlüsseln modulo 10 addieren und zum Entschlüsseln modulo 10 subtrahieren. Nehmen Sie Stellung.

Vigenère-Chiffrierung mit Ziffern

s \ m	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Führen Sie die Entschlüsselung von c=276 auf beide Arten durch und vergleichen Sie. Zeigen Sie **eine** Tabellenablesung deutlich.