Algebra-Aufgaben zum Kryptografie-Heft Seiten 13 und 14

kry\malstern(22) und kry\potstern(22) sind hier rechts angegeben.

1	3	5	7	9	13	15	17	19	21
3	9	15	21	5	17	1	7	13	19
5	15	3	13	1	21	9	19	7	17
7	21	13	5	19	3	17	9	1	15
9	5	1	19	15	7	3	21	17	13
13	17	21	3	7	15	19	1	5	9
15	1	9	17	3	19	5	13	21	7
17	7	19	9	21	1	13	3	15	5
19	13	7	1	17	5	21	15	9	3
21	19	17	15	13	9	7	5	3	1

1	1	3	5	7	9	13	15	17	19	21
2	1	9	3	5	15	15	5	3	9	1
3	1	5	15	13	3	19	9	7	17	21
4	1	15	9	3	5	5	3	9	15	1
5	1	1	1	21	1	21	1	21	21	21
6	1	3	5	15	9	9	15	5	3	1
7	1	9	3	17	15	7	5	19	13	21
8	1	5	15	9	3	3	9	15	5	1
9	1	15	9	19	5	17	3	13	7	21
10	1	1	1	1	1	1	1	1	1	1

Stellen Sie jeweils die Maltafel der von a erzeugten Untergruppe auf.

1.) Wählen Sie drei verschiedene a, die die Ordnung 2 , 5 und 10 haben sollen.
Übrigens: seq(mod(a^k,m),k,1,m), aber eine „von Hand“:

2.) Woran erkennen Sie, dass es sich um Gruppen handelt?

3.) Schreiben Sie jeweils alle Nebenklassen auf.

4.) Machen Sie sich klar: Nach der Definition in S.13 (5) ist auch <a> selbst eine Nebenklasse von <a>. Nennen wir die anderen Nebenklassen "echte Nebenklassen".

5.) Wieviele Elemente haben die Nebenklassen aus 3) und wieviele Nebenklassen gibt es jeweils?

6.) Warum kann man wirklich das Wort "Klassen" für die Nebenklassen verwenden?

7.) Machen Sie sich den Zusammenhang zwischen den Anzahlen der Elemente in <a>, Anzahl der Nebenklassen von <a>, Anzahl der Element in G, Anzahl der Elemente in den Nebenklassen, Anzahl der echten Nebenklassen und der Ordnung von a für Ihre drei a oben und allgemein klar.

8.) Gibt es in $\mathbb{Z}_{22}^*$ eine Zahl. die den Kleinen Fermatsche Satz $a^{20} \underset{22}{\equiv} 1$ erfüllt? Suchen Sie in den Potenztafeln der Seiten 12 a,b,c Zahlen, die $a^{m-1} \underset{m}{\equiv} 1$ erfüllen. Können Sie eine Vermutung äußern?

9.) Bestätigen Sie die Behauptung Seite 14 Satz 4b an den Beispielen der Seiten 12 a,b,c. Sehen Sie sich sorgfältig den Beweis dieses Stzes auf Seite 16 an. Geben Sie eine verbale Begründung.