Einwegfunktionen und Primzahlen

*Eine **Einwegfunktion** ist eine mathematische Funktion, die leicht berechenbar, aber schwer oder praktisch gar nicht umzukehren ist.*

Formale Definition:
Eine Funktion $f: X \rightarrow Y$ heißt Einwegfunktion wenn gilt:

- *Es gibt ein effizientes Verfahren zur Berechnung von $y = f(x)$ für jedes $x \in X$.*
- *Es gibt kein effizientes Verfahren zur Berechnung von $x = f^{-1}(y)$ für jedes $y \in Y$*

Aufgabe 1 Einwegfunktionen im Alltag

Ein Puzzle lässt sich schnell zerstören aber nur sehr langsam wieder aufbauen. Aus einzelnen Zutaten kann eine Suppe gekocht werden, aber die Suppe kann nicht mehr in ihre Bestandteile zurückgeführt werden. Nenne mindestens fünf weitere Alltagsbeispiele für Handlungen, die nur schwer oder gar nicht wieder umzukehren sind.

Aufgabe 2 Produkte und ihre Faktoren

a) Berechne das Produkt aus den Primzahlen 19 und 23.

b) Die Zahl 91 ist als Produkt aus zwei Primzahlen p und q entstanden. Bestimme, welche Zahlen für p und q infrage kommen.

c) Die Zahl 3397 ist als Produkt aus zwei Primzahlen p und q entstanden. Beurteile, ob du in angemessener Zeit, die Primzahlen p und q bestimmen könntest. Beschreibe, wie du dabei vorgehen könntest.

d) Erkläre, warum es sich bei der Multiplikation zweier Primzahlen um eine Einwegfunktion handeln könnte.

*Die Suche nach den Primfaktoren einer Zahl wird als **Faktorisierungsproblem** bezeichnet. Bislang sind keine effizienten Verfahren bekannt, um eine große Zahl in ihre Primfaktoren zu zerlegen.*

Aufgabe 3 Wie war das nochmal?

Löse die folgenden Aufgaben. Recherchiere gegebenenfalls die benötigten Rechengesetze.

a) ggT(5, 15) =

b) ggT(36, 56) =

c) ggT(43, 71) =

d) 53 mod 7 =

e) 121 mod 11 =

f) 4^3 mod 17 =