Potenzieren im Modul: Info und Lösungen

Aufgabe: Stellen Sie die Potenztafeln von und $\mathbb{Z}_5^*$ und $\mathbb{Z}_{10}^*$ auf.

Berechnen Sie einige hohe Potenzen unter Ausnutzung der Elementordnung.
Prüfen Sie mit Excel.

Einnerung: $\mathbb{Z}_m^*$ ist die Menge der zum m teilerfremden Zahlen.

"**Teilerfremd**" zu m ist eine Zahl, die keinen gemeinsamen Teiler mit m hat. Den trivialen Teiler 1 zählt man da nicht mit.
Teilerfremde Zahlen sind auch dadurch charakterisiert, dass sie den "**größten gemeinsamen Teiler**" 1 haben.

$$a \text{ teilerfremd zu } m \Leftrightarrow ggt(a,m)=1 \Leftrightarrow gcd(a,m)=1$$

gcd ist die englische Bezeichnung "greatest common divisor".

Beispiele:
9 ist teilerfremd zu 10, denn 9 hat nur die Teiler 1,3, 9 und 10 hat nur die Teiler 1,2,5,10. Damit haben 9 und 10 die 1 als größten gemeinsamen Teiler.
8 ist nicht teilerfremd zu 10, denn 8 und 10 haben den gemeinsamen Teiler 2.

Lösung

Potenztafel $\mathbb{Z}_5^*$	Potenztafel $\mathbb{Z}_{10}$ ohne 0	Potenztafel $\mathbb{Z}_{10}^*$
$\begin{pmatrix}1\\2\\3\\4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&4&4&1\\1&3&2&4\\1&1&1&1\end{pmatrix}$ 1. Extra-Spalte Exponent 2. 1. Zeile Basis	$\begin{pmatrix}1\\2\\3\\4\\5\\6\\7\\8\\9\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&4&9&6&5&6&9&4&1\\1&8&7&4&5&6&3&2&9\\1&6&1&6&5&6&1&6&1\\1&2&3&4&5&6&7&8&9\\1&4&9&6&5&6&9&4&1\\1&8&7&4&5&6&3&2&9\\1&6&1&6&5&6&1&6&1\\1&2&3&4&5&6&7&8&9\end{pmatrix}$	$\begin{pmatrix}1\\2\\3\\4\end{pmatrix}, \begin{pmatrix}1&3&7&9\\1&9&9&1\\1&7&3&9\\1&1&1&1\end{pmatrix}$

Sie sehen hier auch, warum nur die teilerfremden Zahlen interessant sind. Nur bei ihnen gibt es in ihrer Spalte überhaupt eine 1. Und diese 1 ist bei Berechnungen in der Kyptografie nötig.

Berechnungen $a^b \bmod m = c$ oder $a^b \underset{m}{\equiv} c$

Im Modul $\mathbb{Z}_{10}^*$ gilt:		
ord(3)=4 ord(7)=4 ord(9)=2	$3^{20} = (3^4)^5 \underset{10}{\equiv} 1^5 = 1$ $3^{1732} \underset{10}{\equiv} 1$ weil $1732 \underset{4}{\equiv} 0$ $7^5 = 7^4 \cdot 7 \underset{10}{\equiv} 1 \cdot 7 = 7$ $7^6 = 7^5 \cdot 7 \underset{10}{\equiv} 7 \cdot 7 = 49 \underset{10}{\equiv} 9$	$9^9 = 9^8 \cdot 9 = (9^2)^4 \cdot 9 \underset{10}{\equiv} 1^4 \cdot 9 = 9$ $9^7 = 9$ weil $7 \underset{2}{\equiv} 1$ $9^{12345} = 9$, Exponent ungerade

Befehle in Excel **Rest(a^b ; m)**
Befehl in vielen Computersprachen und CAS **mod(a^b,m)**
(Pascal, C++, Java, Dephi, ...// MuPAD, Mathematica, Maple, Derive, Taschenrechner)
Befehl in vielen CAS(etwa) **powermod(a, b, m)** (MuPAD, Mathematica, Maple)