Square & Multiply: Potenzen modulo m

Bei X^k mod m verbietet sich eine direkte Berechnung von X^k auf jeden Fall, denn wenn X und k jeweils 1000-stellige Zahlen sind, was in der Kryptographie nichts Ungewöhnliches ist, dann hätte X^k etwa 10^{3000} Bits – und dies ist eine Zahl, die die Anzahl der Atome im Weltall bei weitem überschreitet. Glücklicherweise liefert uns Folgerung S1-4 einen Trick, mit dem wir die Berechnung durchführen können:

1. Berechne vorab die Zweierpotenzen von X durch fortgesetztes Quadrieren
   $X^2 = \quad = Y \pmod m$
   $X^4 = Y^2 = Z \pmod m$
   $X^8 = Z^2 = A \pmod m$
   …
   Dies kann man für festes X vorab machen und in einer Tabelle ablegen.
2. Zerlege k in seine Binärdarstellung: $k = \sum_{i=0}^{n-1} k_i 2^i$. Die k_i sind entweder 0 oder 1.
3. Multipliziere die (vorab berechneten) Zweierpotenzen $X^{k_i 2^i}$ deren $k_i=1$ ist.
4. Halte dabei die Zahlen durch fortgesetztes "mod m" klein (s. Folgerung S1-4)

Beispiel: Berechne 2208^5 mod 7.

1. Es gilt 2208 mod 7 = 3. Damit rechnen wir aus:
   $2208^2 = 3 \cdot 3 = 2 \pmod 7$
   $2208^4 = 2^2 = 4 \pmod 7$
2. Wir zerlegen $5 = \mathbf{1} \cdot 2^2 + \mathbf{0} \cdot 2^1 + \mathbf{1}$ [$5 = \mathbf{101}_{\text{binär}}$]
3. $2208^5 = 2208^{4+0+1} = 2208^4 \cdot 2208^1 = 4 \cdot 3 = 12 = \mathbf{5} \pmod 7$

[s. auch **„Square-and-Multiply“**-Algorithmus im CyrpTool-Skript S. 96f]

Übung: Berechne analog 324^{37} mod 11.