Den Rest großer Potenzen mit „Modularem Potenzieren“ berechnen

Beim Potentzieren von zwei Zahlen entstehen schnell große Zahlen, mit denen das Rechnen mühsam oder, wenn die Anzeige des Taschenrechners sie nicht mehr vollständig anzeigen lässt, unmöglich wird. Soll jedoch der **Rest** einer solchen Potenz berechnet werden kann man die Rechnung mit Hilfe von zwei Tricks vereinfachen:

(Regel I) Lässt sich der Exponent als **Summe** zweier kleinerer Zahlen darstellen, so gilt:

$$x^{a+b} = x^a \cdot x^b$$

Soll der Rest der Potenz gebildet werden, so kann die Restfunktion bereits auf Zwischenergebnisse angewendet werden, denn bezüglich der Restbildung zur Division durch d gilt:

$$x^{a+b} \bmod d = ((x^a \bmod d) \cdot (x^b \bmod d)) \bmod d$$

(Regel II) Lässt sich der Exponent als **Produkt** zweier kleinerer Zahlen darstellen, so gilt:

$$x^{a \cdot b} = (x^a)^b$$

Soll der Rest der Potenz gebildet werden, so kann die Restfunktion bereits auf Zwischenergebnisse angewendet werden, denn bezüglich der Restbildung zur Division durch d gilt:

$$x^{a \cdot b} \bmod d = (x^a \bmod d)^b \bmod d$$

Beispiel:

Es soll der Rest der Division von $16^{31} : 71$ berechnet werden. 16^{31} ist ausgeschrieben 830767497367172420564879412675215 36 – eine Zahl, die man wegen ihrer Länge bestimmt nur ungern schriftlich dividieren wird und die sich in viele handelsübliche Taschenrechner nicht vollständig eingeben lassen. Wir wollen daher die Berechnung in zwei Schritten vereinfachen:

Schritt 1: 31 lässt sich in 3 + 28 zerlegen (Es ging auch 1+30 oder andere Summen). Nach Regel I gilt:

$$16^{31} \bmod 71 = ((16^3 \bmod 71) \cdot (16^{28} \bmod 71)) \bmod 71$$

Schritt 2: 28 lässt sich in 4 · 7 zerlegen (Es ginge auch 2 · 14 oder andere Produkte). Nach Regel II gilt:

$$16^{28} \bmod 71 = ((16^4 \bmod 71)^7 \bmod 71$$

$$= (65.536 \bmod 71)^7 \bmod 71 = 3^7 \bmod 71$$

$$16^{31} \bmod 71 = ((16^3 \bmod 71) \cdot (16^{28} \bmod 71)) \bmod 71$$

$$= ((4.096 \bmod 71) \cdot (2.187 \bmod 71)) \bmod 71$$

$$= (49 \cdot 57) \bmod 71$$

$$= 2.793 \bmod 71 = \underline{\underline{24}}$$

Aufgabe: Berechne $13^{19} \bmod 47$ mit modularem Potenzieren! ($13^{19} = 1461920290375446110677$)

Wie führt ein Computer modulares Potenzieren durch?

Wir haben zur Vereinfachung der Berechnung einige willkürliche Entscheidungen getroffen. Will man das Verfahren für einen Computer programmieren, so braucht man ein Verfahren, das immer zu einem Ergebnis kommt. Ein Ansatz wäre, zunächst zu prüfen, ob der Exponent gerade ist oder ungerade. Ist er ungerade, so kann Regel I angewendet werden, um x^p in $x^1 \cdot x^{p-1}$ zu wandeln. Anschließend kann so lange der Exponent nach Regel II durch 2 geteilt werden, bis er den Wert 1 annimmt:

$$x^5 = x^1 \cdot \left(\left(x^1\right)^2 \right)^2$$

Wie kann ich meine Rechenergebnisse überprüfen?

Mit einigen Computer-Programmen lassen sich auch große Potenzen berechnen. Beispiele sind:

- „Taschenrechner"-Programme der Betriebssysteme.
  z.B. bei Windows unter Start -> Programme -> Zubehör
  Tipp: Für weitere Funktionen im Menü *Ansicht* auf „wissenschaftlich" umschalten!
- Computeralgebra-Programme wie z.B. *Derive*.
- Interpreter für Skriptsprachen wie Python. Z.B. unter http://python.org herunterladen und installieren oder unter http://sagemath.org anmelden und den Online-Interpreter nutzen. Nützliche Funktionen sind z.B. für die Restfunktion *modulus(x, d)* , zum Potenzieren *pow(x, p)* und zum modularen Potenzieren *pow(x, p, d)*.