Die Reste von Potenzen in mod

Für unsere späteren Überlegungen benötigen wir Kenntnisse im Umgang mit Potenzen. Diese werden selbst bei kleinen Zahlen recht schnell groß und erfordern spezielle Überlegungen und Kenntnisse bei der Verarbeitung. Diese verschaffen wir uns ausgehend von einem

Beispiel: *Berechne 15^7 mod 13.*

Dies geht ganz handwerklich: Berechne 15^7 (= 170.859.375) und davon mod 13: der Befehl für den Taschenrechner lautet $\boxed{\div R}$ (auf dem WTR rot markiert). 15^7 $\boxed{\div R}$ 13 liefert R = 11.

Potenzen werden jedoch sehr schnell groß und damit für den Taschenrechner nicht mehr handhabbar. Versuche, 21^{14} mod 18 zu berechnen: 21^{14} ist für den WTR nicht mehr exakt zu berechnen. Hierbei hilft uns für gewisse Zeit noch ein Satz weiter:

Es gilt: $\mathbf{a^b \bmod c = (a \bmod c)^b \bmod c}$

a) *Überprüfe den Satz exemplarisch an selbstgewählten Beispielen mit Hilfe des WTR. Achte dabei auch auf die Grenze, ab denen der WTR nicht mehr exakt rechnet (d.h. wenn der WTR das Ergebnis in Fließkommadarstellung … x10 ··· ausgibt).*

a	b	c	a^b	**a^b mod c**	a mod c	$(a \bmod c)^b$	**$(a \bmod c)^b$ mod n**
Individuell							

b)*

$a^b \bmod c$

$= (a \cdot a \cdot a \cdot \ldots \cdot a) \bmod c$ **b Faktoren**

$= (a \bmod c \cdot a \bmod c \cdot \ldots \cdot a \bmod c) \bmod c$ **Satz über modulares Multiplizieren[1]**

$= (a \bmod c)^b \bmod c$ ∎

1 $(a \bmod c \cdot a \bmod c) = (a \cdot a) \bmod c$ von rechts nach links gelesen

Ein Verfahren zur Bestimmung der modulo-Reste bei großen Potenzen

Dies leiten wir an einem ersten, ganz kleinen Beispiel her, um unsere Berechnungen nachvollziehen zu können:

Gesucht ist 5^{11} mod 7.

Dies geht auch noch von Hand bzw. WTR:

5^{11} mod 7 = 48.828.125 mod 7 = 3

Als Grundlage brauchst du:

- Binärdarstellung natürlicher Zahlen
- Potenzrechnung aus Klasse 9
- Rechenregeln für das Multiplizieren in mod

Das selbe nun mit einem Trick nochmals durchgerechnet:

Zunächst schreiben wir den Exponent 11 in Zweierpotenzen. (Tipp: Dabei hilft auch die Binärdarstellung: $11_{10} = 1011_2$): $11 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$

Verdeutliche dir bei jedem Schritt des nun folgenden Verfahrens, welche Rechenregel zur Anwendung kommt. Notiere sie rechts neben dem jeweiligen Schritt. Schreibe am Ende eine kurze Anleitung zum Verfahren in eigenen Worten.

Zunächst sortieren wir den Exponenten „11“ nach *aufsteigenden* Zweierpotenzen:

$11 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3$. Damit ergibt sich folgende Darstellung für 5^{11} mod 7:

$5^{11} \bmod 7 = 5^{2^0 + 2^1 + 2^3} \bmod 7$ Darstellung des Exponenten in Zweierpotenzen

$= (5^{2^0} \cdot 5^{2^1} \cdot 5^{2^3}) \bmod 7$ Potenzgesetz $x^{b+c} = x^b \cdot x^c$

$= (5^{2^0} \bmod 7) \cdot (5^{2^1} \bmod 7) \cdot (5^{2^3} \bmod 7)$ $(x \cdot x) \bmod c = (x \bmod c \cdot x \bmod c) \bmod c$

Berechnung der einzelnen Faktoren:

I. $5^{2^0} \bmod 7 = 5 \bmod 7 = 5$

II. $5^{2^1} \bmod 7 = (5^{2^0})^2 \bmod 7$ Potenzgesetz $(x^b)^c = x^{b \cdot c}$

$= (5^{2^0} \bmod 7)^2 \bmod 7$ $(x^2) \bmod c = (x \bmod c)^2 \bmod c$ (mod. Mult)

$= 5^2 \bmod 7$ (*) $5^{2^0} = 5^1 = 5$; $5 \bmod 7 = 5$

$= 25 \bmod 7 = 4$ $5^2 = 25$

III. $5^{2^2} \bmod 7$ *Dieser Ausdruck wird im Prinzip nicht gebraucht. Allerdings ist dir vielleicht in II. Schon etwas aufgefallen. Wenn nicht, gib jetzt genau acht, was wir tun...*

$5^{2^2} \bmod 7 = (5^{2^1})^2 \bmod 7$ Exponent: $2^2 = 2^1 \cdot 2$; Potenzgesetz $x^{b \cdot c} = (x^b)^c$

$= (5^{2^1} \bmod 7)^2 \bmod 7$ $(x^2) \bmod c = (x \bmod c)^2 \bmod c$

$= 4^2 \bmod 7$ (*) $5^{2^1} \bmod 7 = 25 \bmod 7 = 4$

$= 16 \bmod 7 = 2$ $4^2 = 16$

IV. $5^{2^3} \bmod 7 = (5^{2^2})^2 \bmod 7$ Exponent: $2^3 = 2^2 \cdot 2$; Potenzgesetz $x^{b \cdot c} = (x^b)^c$

$= (5^{2^2} \bmod 7)^2 \bmod 7$ $(x^2) \bmod c = (x \bmod c)^2 \bmod c$

$= 2^2 \bmod 7$ (*) $5^{2^2} \bmod 7 = 625 \bmod 7 = 2$

$= 4 \bmod 7 = 4$ $2^2 = 4$

Nun haben wir alle benötigten Faktoren beisammen und können den letzten Schritt vornehmen:

$5^{11} \bmod 7 = 5^{2^0} \bmod 7 \cdot 5^{2^1} \bmod 7 \cdot 5^{2^3} \bmod 7 = 5 \cdot 4 \cdot 4 = 80.$

Wir erhalten $5^{11} \bmod 7 = 80$.

Jedoch ist $80 > 7$. Da wir mit Restklassen („modulo“) rechnen, gilt: $5^{11} \bmod 7 \equiv 80 \equiv 3$.

Schlussergebnis: $5^{11} \bmod 7 = 3$

Eine weiterführende Betrachtung: Betrachte die mit (*) markierten Zeilen. Was für Zahlen benutzt du hier? Woher bekommst du sie? Welchen Rechenschritt führst du mit ihnen aus? Formuliere deine Erkenntnis in Worten:

Die Umformungen führen stets auf das im vorherigen Schritt berechnete Ergebnis zurück. Dieses wird hier jeweils quadriert und die Restklasse bestimmt: Ist das Ergebnis im vorherigen Schritt a, so berechnet man stets „$a^2 \bmod c$“.

Benutzung des Verfahrens mit technischer Unterstützung

An den mit (*) markierten Zeilen siehst du, dass das Verfahren rekursiv aufgebaut ist: Der neu zu berechnende Faktor wird auf den vorhergehenden zurückgeführt. Mit dem WTR lässt sich das bequem ausnutzen, wenn man seine Speicherfunktionen effektiv benutzt:

Start des Verfahrens:

$5^{2^0} \bmod 7 = 5 \bmod 7 = 5$ belege die Speicher: $5 \rightarrow A$, $7 \rightarrow B$

Betrachte die Zeilen (*): Die Terme haben immer die selbe Form (s.u.).

Was kann man (in Worten) in die Klammer schreiben? Ergänze:

$$(\textit{vorheriges Ergebnis})^2 \bmod 7$$

Teste das Vorgehen mit dem WTR:

- Belege die Speicher A und B mit den Startwerten (s.o.)
- Gib den Term ein: $A^2 - B \cdot (A^2 \div R\ B) \rightarrow A$
- Drücke mehrmals ENTER.
- Das leistet der Term: *Der Speicher a ist zunächst mit der Basis der betrachteten Potenz (hier: 5) belegt. Dann wird dieser Wert quadriert. Vom Quadrat berechnet man mod b und erhält so den nächsten Wert der Rekursion. Dieser wird automatisch in die Variable a gespeichert, so dass in einem neuen Aufruf des Terms automatisch der nächste Schritt berechnet wird. Dies muss so lange durchgeführt werden, bis alle benötigten Faktoren berechnet sind.*

a) $87^{353} \bmod 91 = 68$

b) $523^{792} \bmod 123 = 100$

c) $72802^{2471} \bmod 231 = 4$