Satz von Euler und RSA-Verfahren

Außermathematische Anwendungen im Mathematikunterricht
WS 2011/12
Franz Embacher, Universität Wien

Satz von Euler

(in einer für das RSA-Verfahren zurechtgeschneiderten Form):

> Seien p und q zwei verschiedene Primzahlen, k eine natürliche Zahl und x eine natürliche Zahl $< p\,q$. Dann gilt
>
> $$x^{k(p-1)(q-1)+1} \bmod p\,q = x\,.$$

(Wir beweisen ihn nicht, sondern erwähnen nur, dass er eine Verallgemeinerung des „kleinen Fermatschen Satzes“ ist.)

Beispiel:

> Mit $p=13,\ q=11,\ k=2,\ x=97$ lautet die Aussage des Satzes
>
> $$97^{2\cdot 12\cdot 9+1} \bmod 13\cdot 11 \equiv 97^{241} \bmod 143 = 97\,.$$

Anwendung im **RSA-Verfahren**:

1. Alice wählt zwei verschiedene Primzahlen p und q.
2. Sie berechnet
   $$n = p\,q$$
   $$m = (p-1)(q-1)$$
3. Sie wählt eine zu m teilerfremde natürliche Zahl a.
4. Sie gibt die Zahlen n und a als „öffentlichen Schlüssel“ bekannt.

5. Bob drückt seine Nachricht (den „Klartext“) als natürliche Zahl $x < n$ aus.
   (Beachten Sie: Der Schlüssel n muss genügend lang sein!)
6. Bob verschlüsselt seine Nachricht gemäß der Formel $y = x^a \bmod n$.
7. Er gibt y (den „Geheimtext“) öffentlich bekannt.

8. Alice ermittelt $b = a^{-1} \bmod m$.
   b existiert genau dann, wenn a und m teilerfremd sind – was laut Voraussetzung der Fall ist – und ist jene (eindeutig bestimmte) natürliche Zahl zwischen 1 und $m-1$, für die $a\,b \bmod m = 1$ gilt. In der Praxis wird b mit Hilfe des **erweiterten Euklidischen Algorithmus** berechnet.
   Als Folge gibt es eine natürliche Zahl k mit $a\,b = k\,m+1$.
9. Alice berechnet $X = y^b \bmod n$.
   Es gilt:

$$X = y^b \bmod n = \left(x^a \bmod n\right)^b \bmod n =$$
$$= x^{a\,b} \bmod n = x^{k\,m+1} \bmod n \underbrace{=}_{\text{Satz von Euler}} x$$

   Das ist aber genau Bobs Klartext!

Der wesentliche Punkt ist, dass zur Entschlüsselung die Zahl m bekannt sein muss! Da n öffentlich bekannt ist, ist das wegen

$$n = p\,q$$
$$m = (p-1)(q-1) = p\,q - p - q + 1 = n + (p+q) + 1$$

de facto gleichbedeutend damit, p und q, also die Primfaktoren von n, zu kennen.