

# Mathematik und Logik

## 8. Übungsaufgaben

2007-01-23

1. Berechnen Sie  $2^{340} \bmod 341$ . Glauben Sie, daß 341 eine Primzahl ist?

*Beweis.* Mittels der Methode des sukzessiven Quadrierend erhält man in ca 8 Schritten (Quadrieren und Multiplizieren von Zahlen bis maximal 340) das Ergebnis  $2^{340} \equiv 1 \pmod{341}$ . Da dieser Sachverhalt nur bei zusammengesetzten Zahlen verletzt ist, ergibt sich damit ein Hinweis, daß 341 tatsächlich eine Primzahl sein dürfte, aber kein Beweis dafür.  $\square$

2. Wiederholen Sie das vorige Beispiel mit der Basis 3. Was stellen Sie fest?

*Beweis.* Wir gehen ähnlich wie im vorigen Beispiel vor und stellen fest  $3^{340} \equiv 56 \not\equiv 1 \pmod{340}$ . Da dies für keine Primzahl gelten kann, können wir uns sicher sein, daß 341 tatsächlich keine Primzahl ist, der Hinweis im vorigen Beispiel also irreführend war.  $\square$

3. Wählen Sie  $p = 11$  und  $q = 23$  als „große“ Primzahlen. Sei  $m = pq$ ; bestimmen Sie  $\varphi$ , und wählen Sie ein  $e$  relativ prim zu  $\varphi$ .

*Beweis.* Wir rechnen:  $m = p \cdot q = 11 \cdot 23 = 253$ ;  $\phi = (p - 1) \cdot (q - 1) = 10 \cdot 22 = 220$ . Nun wählen wir irgendein  $e$  mit  $3 < e < \phi$ , welches zu  $\phi$  relativ prim ist (d.h.  $\text{ggT}(e, \phi) = 1$ ). Wir probieren etwa  $e = 25$ , und überprüfen mit dem Euklidschen Algorithmus; dies liefert  $\text{ggT}(25, 220) = 5$ ; damit ist dieser Versuch fehlgeschlagen, und wir probieren eine andere Zahl, etwa  $e = 17$ ; hier liefert der Euklidsche Algorithmus  $\text{ggT}(17, 220) = 1$ ; somit ist  $e = 17$  eine geeignete Wahl.

Anmerkung: Diese Wahl ist ganz beliebig. Tatsächlich gibt es weitere 75 Möglichkeiten. Oder anders herum: Es gibt 216 Zahlen zwischen

3 und 220; davon sind 78 geeignet (d.h. relativ prim zu 221); wählt man eine Zahl zufällig (gleichverteilt), dann erwischt man mit einer Wahrscheinlichkeit von  $\frac{78}{216} \approx 0.36$  eine geeignete; nach 10 Schritten hat man dann mit einer Wahrscheinlichkeit von 99% eine geeignete gefunden. Dieses Probiervorgehen funktioniert also tatsächlich, nämlich in dem Sinne, daß man mit großer Wahrscheinlichkeit schon nach ein paar Schritten am Ziel ist, und die Wahrscheinlichkeit, daß man wirklich lange probieren muß, extrem niedrig ist.  $\square$

4. Bestimmen Sie zu  $e$  aus dem vorigen Beispiel ein passendes  $d$  mit  $de \equiv 1 \pmod{\varphi}$ .

*Beweis.* Der erweiterte Euklidische Algorithmus liefert hier die Lösung  $d = 13$ . Dies ist leicht nachprüfbar:  $13 \cdot 17 = 221 \equiv 1 \pmod{220}$ .

Damit haben wir kann man RSA-verschlüsseln:  $(253, 17)$  ist der öffentliche Schlüssel,  $(253, 13)$  der geheime.

Anmerkung: Natürlich ist dieses konkrete Verschlüsselungsverfahren leicht zu knacken, weil 253 leicht zu faktorisieren (d.h. in Faktoren zerlegbar) ist. In der Realität verwendet man für  $p$  und  $q$  ca 150-stellige Zahlen, womit  $m$  ca 300 Dezimalstellen hat. Zahlen dieser Größenordnung können mit heutiger Technik und dem aktuellen Stand der Wissenschaft nicht faktorisiert werden. (Unbekannt, obwohl eher unwahrscheinlich, ist aber, ob nicht doch jemand (etwa ein Geheimdienst) ein Wissen, z.B. wie man schneller faktorisieren kann, für sich behält, und damit das RSA-Verfahren knacken kann).  $\square$

5. Wählen Sie ein  $x \in \mathbb{Z}_m$ , bestimmen Sie  $y = x^e$  und rechnen Sie nach, ob  $y^d = x$  ist. Wiederholen Sie das Beispiel für mehrere  $x$ .

*Beweis.* Sei  $x = 118$ ; dann ist  $y = x^e = 118^{17} = 200 \in \mathbb{Z}_{253}$ ; und weiters  $y^d = 200^{13} \equiv 118 \in \mathbb{Z}_{253}$ , so wie es schließlich sein soll.  $\square$

6. Alice verwendet den/die Schlüssel aus den obigen Beispielen. Der öffentliche Schlüssel von Bob sei  $m = 323$ ,  $e = 5$ . Alice will Bob die geheime Nachricht 16 mitteilen. Was muß sie versenden?

*Beweis.* Alice's Schlüssel ist für dieses Beispiel irrelevant. Sie verwendet lediglich Bob's öffentlichen Schlüssel, rechnet  $y = 16^5 = 1048576 \equiv 118 \pmod{323}$ , und versendet daher die Zahl 118.  $\square$

7. Bob hat die Nachricht empfangen; sie überrascht ihn aber, und er hat Zweifel, ob sie tatsächlich von Alice stammt. Er bittet sie daher, ihre Nachricht zusätzlich zu signieren. Was muß Alice nun schicken?

*Beweis.* Bob empfängt also die Nachricht 2. Mit seinem geheimen Schlüssel  $d'$  kann er die ursprüngliche Nachricht rekonstruieren:  $118^{d'} = 16 : \mathbb{Z}_{323}$ ; und das überrascht ihn. Er kennt den öffentlichen Schlüssel von Alice; diese signiert daher die Nachricht (durch Anwendung ihres geheimen Schlüssels), berechnet als  $x' = x^d = 16^{13} = 26 : \mathbb{Z}_{253}$ ; dies ist die signierte Nachricht, welche als Element von  $\mathbb{Z}_{323}$  aufgefaßt wird, und dann wie vorhin verschlüsselt versandt wird:  $y' = x'^{e'} = 26^5 = 144 : \mathbb{Z}_{323}$ . Tatsächlich auf die Reise geht hier somit die Zahl 144.

Bob verwendet kann dann mit seinem privaten Schlüssel  $144^{d'} : \mathbb{Z}_{m'}$  berechnen, um  $x'$  zu erhalten, und mit Alice's öffentlichem Schlüssel erhält er schließlich die Nachricht  $x$  selbst. Da allgemein angenommen wird, daß für die Berechnung von  $x'$  aus  $x$  der geheime Schlüssel  $d$  tatsächlich notwendig ist, nimmt Bob an, daß die Nachricht tatsächlich von Alice stammt. (Genauer, von jemanden, der Zugriff auf Alice's geheimen Schlüssel hat, oder das Verfahren geknackt hat.)  $\square$