Einführung in die Algebra und Zahlentheorie
Übungsblatt 12

Abgabetermin Donnerstag, den 27.01.2010 vor der Vorlesung.

0. Wiederholen Sie Abschnitt 5 im Vorlesungsmanuskript.

1. Sei $m \in \mathbb{Z}_{\geq 2}$. Für ein $a \in \mathbb{Z}$ gelte $a^{m-1} \equiv 1 \operatorname{mod} m$ und $a^{\frac{m-1}{p}} \not\equiv 1 \operatorname{mod} m$ für jeden Primteiler p von $m-1$. Zeigen Sie, dass dann m prim ist.

2. Der öffentliche RSA-Schlüssel von Alice ist
$$n_A = 1619358228406467075474914775557010450966972147576529361 9$$
$$e_A = 2^{16} + 1$$
Bob hat eine verschlüsselte Nachricht
$$c = 13319877118067225831682957143105157757730827112934642828$$
an Alice geschickt. Was war der Inhalt der Nachricht?

   Hinweise: Alice hat ungeschickterweise einen Primfaktor p von $n_A = p \cdot q$ gewählt, sodass $\varphi(p)$ nur Primpotenzfaktoren ≤ 200000 hat.

   Um für $a, b, n \in \mathbb{N}$ effizient $a^b \operatorname{mod} n$ zu berechnen, gibt es in Maple das Kommando

   `a&^b mod n`

   (das im Wesentlichen sukzessive a modulo n aufmultipliziert).

   Testen Sie, ob auch die Maple-Funktion `ifactor` zum Ziel führt.

3. Sei $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.
   (a) Zeigen Sie, dass $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$.
   (b) Folgern Sie $[K : \mathbb{Q}] = 4$.
   (c) Zeigen Sie $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.
   (d) Zeigen Sie: Das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ ist
   $$f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$$
   (e) Bestimmen Sie alle Nullstellen von f.

4. Sei $K \subset K[\alpha]$ eine algebraische Körpererweiterung und $g \in K[x]$ das Minimalpolynom von α.
   (a) Geben Sie ein Verfahren an, um das Inverse β^{-1} von $0 \neq \beta \in K[\alpha]$ zu berechnen.
   (b) Bestimmen Sie das Inverse von
   $$\left(\sqrt{2} + \sqrt{3}\right)^2 + \sqrt{2} + \sqrt{3} \in \mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right]$$
   und machen Sie die Probe.

5. (4 Zusatzpunkte) Implementieren Sie
   (a) das Sieb des Eratosthenes,
   (b) die Faktorisierung von ganzen Zahlen mittels Probedivision und
   (c) das Faktorisierungsverfahren von Pollard.

   Testen Sie Ihre Implementierung jeweils an Beispielen, siehe auch Aufgabe 2.