Zahlentheorie und Kryptologie, WS 2008/09

Michael Hortmann

Aufgabenblatt 7

1. Man zeige: Es gibt genau zwei Körperautomorphismen $\varphi:\mathbb{C}\to\mathbb{C}$, für welche $\varphi|\mathbb{R}=\mathrm{id}_R$.

2. Das Polynom $f=X^3+X+1$ ist irreduzibel in $\mathbb{Z}_5[X]$, so daß $K=\mathbb{Z}_5[X]/<f>$ ein Körper ist. Die Elemente von *K* werden bekanntlich durch Polynome vom Grad kleiner als 3 repräsentiert, und wir benutzen die Schreibweise 345 für das Polynom $3X^2+4X+5$.

a) Finden Sie drei Nullstellen x_1, x_2, x_3 von f in *K* und rechnen Sie nach, daß $f=(X-x_1)(X-x_2)(X-x_3)$

b) Finden Sie ein Polynom dritten Grades in $\mathbb{Z}_5[X]$, welches 111 als Nullstelle besitzt.

3. Berechnen Sie mit Hilfe des quadratischen Reziprozitätsgesetzes das Jacobi-Symbol $\left(\frac{76}{117}\right)$. Können Sie dadurch feststellen, ob 76 ein Quadrat in $\mathbb{Z}_{117}$ ist? Wieso?

4. Sei *p* prim und $Q_p\subset\mathbb{Z}_p^*$ die Untergruppe der Quadrate. Untersuchen Sie, für welche *p* die durch $x\to x^2$ gegebene Abbildung $Q_p\to Q_p$ bijektiv ist und für welche nicht.

5. Der österreichische Briefbombenattentäter Franz Fuchs hatte dummerweise angenommen, es würde mehrere Wochen dauern, die mit dem RSA-Modul *n*=

```
630548215070129547156718332495889632234434145411971275888376987603
260225252787926135276738944105689100036295535868141424386536403649
578707699128189491432138631900590774729214990015369102760964884776
344849717811484309528915040117952098061886881
```

und dem öffentlichen Exponenten *e*=

```
508075310835159009812633969174411123496728859672737076695139826186
257647581337481521676692825102982808222076238747753504407
```

verschlüsselte Botschaft, deren erste Zeile lautete *c*=

```
463316335616613937318842101415083702006628892795168389554894402706
884035322375721126316678871052346087047872057770161604068825594947
480777575090664841774749749032122958886916388656231305149413112661
671360620310298582755616480043108904735117491
```

zu entschlüsseln. Die Dezimalzahl, die beim RSA-Entschlüsseln dieser Zeile entsteht, ist übrigens von hinten beginnend in dreiziffrige Gruppen aufzuteilen, deren jede als Ascii-Code zu interpretieren ist.
Man faktorisiere nun *n* mit Hilfe des Fermat-Verfahrens und entschlüssle die letztlich wirre Botschaft. Worin genau lag der Fehler bei der Wahl von *n*?

5. Schreiben Sie ein Pari-Programm für den Pollard-Rho-Test und faktorisieren Sie damit Zahlen, die aus zwei etwa gleich großen Primfaktoren bestehen. Bis zu welcher Größe der Zahlen schaffen Sie es?