Kryptologie, SS03 Aufgabenblatt 3

Chinesischer Restesatz

Sind *k,l* teilerfremde natürliche Zahlen und *n=kl*, so ist die Abbildung

$$\varphi:\ \mathbb{Z}_n \to \mathbb{Z}_k \times \mathbb{Z}_l$$
$$m \to (m\%k, m\%l)$$

ein Ringisomorphismus. Um die Umkehrabbildung zu konstruieren, benötigt man Zahlen *M,N* mit $M \equiv 1 \operatorname{mod} k,\ M \equiv 0 \operatorname{mod} l,\ \ N \equiv 0 \operatorname{mod} k,\ N \equiv 1 \operatorname{mod} l$. Dann gilt nämlich für $(x,y) \in \mathbb{Z}_k \times \mathbb{Z}_l$ und $k := (xM + yN)\ \%\ n:\ \varphi(k) = (x,y)$. *M,N* beschafft man sich, indem man mit dem erweiterten Euklidischen Algorithmus die Gleichung $ak + bl = \operatorname{ggT}(k,l) = 1$ löst und *M:=bl*, *N:=ak* setzt.

Wurzelziehen in Z_p, $p \equiv 3 \operatorname{mod} 4$

Aufgabe 1: Sei p eine Primzahl, $p \equiv 3 \operatorname{mod} 4$, $a,b \in \mathbb{Z}_p^*$, $b^2 = a$. Man zeige, daß für $c := a^{\frac{p+1}{4}}$ ebenfalls gilt $c^2 = a$. (Dann ist natürlich $c = b$ oder $c = -b$).

Hinweis: Man zeige zunächst mit Hilfe der Potenzgesetze in $\mathbb{Z}_p^*$, daß $a^{\frac{p-1}{2}} = 1$.

Aufgabe 2

Es gilt $n := 5447693 = 1259 \cdot 4327$. In $\mathbb{Z}_n$ gilt $1234567^2 = 129949$. Mit Hilfe der Wurzel-Formel aus Aufgabe 1 und dem Chinesischen Restesatz finde man alle 4 Quadratwurzeln von 129949 in $\mathbb{Z}_n$.

Aufgabe 3

a) Es sei $n = 121932633334857493$. Benutzen Sie den Fermat-Primzahltest, um zu zeigen, daß *n* keine Primzahl ist.

b) In $\mathbb{Z}_n$ gilt $1234567^2 = 1524155677489$, wie man z.B. mit pari-gp leicht nachrechnet. Man weiß also, daß a:=1524155677489 ein Quadrat in $\mathbb{Z}_n$ ist. Ein Orakel, welches Quadratwurzeln in $\mathbb{Z}_n$ berechnen zu können behauptet, gibt auf Input *a* hin die Zahl 121932633333622926 aus. Benutzen Sie diese Information, um *n* zu faktorisieren!

Aufgabe 4

Eine Carmichael-Zahl ist eine ungerade zusammengesetzte Zahl *n*, für die gilt:
$\forall a \in \mathbb{Z}_n:\ a \neq 0 \Rightarrow a^{n-1} = 1$ in $\mathbb{Z}_n$.

Man kann zeigen, daß i) jeder in der Primfaktorzerlegung von *n* jeder vorkommende Primfaktor nur mit Potenz 1 vorkommt, und daß *n* mindestens 3 Primfaktoren besitzt. Mit Hilfe des Chinesischen Restesatzes überlegt man sich, daß ii) für jeden Primfaktor *p* einer Carmichael Zahl *n* gilt: $(p-1)/(n-1)$. Mit i),ii) sind die Carmichael – Zahlen charakterisiert.

Man zeige (durch Nachweis von i),ii))

a) 561 ist eine Carmichael Zahl.

b)* Sind für $k \in \mathbb{N}$ $6k+1, 12k+1, 18k+1$ Primzahlen, so ist $N := (6k+1) \cdot (12k+1) \cdot (18k+1)$ eine Carmichael Zahl.

c) Mit Hilfe der Aussage von b) finde man eine weitere Carmichael Zahl.