Aufgaben zur Zahlentheorie und Kryptologie WS 2004/05, Blatt 2

Michael Hortmann

Nutzen Sie Pari oder ein anderes Computer-Algebra- oder -Arithmetik Programm bei der Bearbeitung der folgenden Aufgaben.

Aufgabe 1

Ein Polynom in $\sum_{i=0}^{n} a_i X^i \in \mathbb{Z}_p[X]$ werde dargestellt durch den Koeffizientenstring $a_n \ldots a_0$.
Das Polynom *f*=100011011 ist irreduzibel in $\mathbb{Z}_2[X]$. Man benutze den Euklidischen Algorithmus, um im zugehörigen Restklassenkörper $\mathbb{Z}_2[X]/(f)$ das Inverse von 1011011 zu berechnen.

Berechnen Sie auch die Ordnung des Elements 1011011!

Aufgabe 2

Sei $p \equiv 3 \bmod 4$ eine Primzahl. Begründen Sie, warum die Formel $a^{\frac{p+1}{4}}$ eine Quadratwurzel aus *a* in $\mathbb{Z}_p$ liefert, falls eine solche existiert.

Aufgabe 3

Der Chinesische Restesatz besagt, daß die durch $k \to (k \% p, k \% q)$ gegebene Abbildung

$\Phi : Z_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$ ein Ringisomorphismus ist. Wenn wir $k_1, k_2 \in \mathbb{Z}_{pq}$ finden können mit $\Phi(k_1)=(1,0), \Phi(k_2)=(0,1)$, dann ist offenbar $\Phi(r_1 k_1 + r_2 k_2)=(r_1, r_2)$.

a) Nutzen Sie den Euklidischen Algorithmus, um k_1, k_2 für $n=1019 \cdot 1103$ zu bestimmen.
b) In $\mathbb{Z}_n$ gilt $(\pm 3)^2 = 9$. Es muß aber noch zwei weitere Wurzeln aus 9 geben. Berechnen Sie diese mit Hilfe des chinesischen Restesatzes, also a) und dem Ergebnis von Aufg. 2.

Aufgabe 4

a) Benutzen Sie eine Art „Sieb des Erathosthenes“, um unzerlegbare Elemente des Gaußschen Zahlenringes $\mathbb{Z}[i]$ zu finden. Dabei sind natürlich nur solche interessant, die nicht assoziiert sind, also nicht durch Multiplikation mit einer Einheit $\pm 1, \pm i$ auseinander hervorgehen. Offenbar kann man durch geeignete Multiplikationen mit Einheiten die entsprechenden Element in den ersten Quadranten legen. Nachdem Sie so ca. 20 nichtassoziierte Primelemente gefunden haben, stellen Sie eine Vermutung über ihre allgemeine Form auf.

b) Die analoge Aufgabe für $\mathbb{Z}[\omega]$ mit $\omega = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$.