Mathematik 3 für CMS, FHS Hagenberg
11. Übungsblatt für den 20.12.2005

1. Bestimmen Sie jeweils 2 primitive Elemente (Erzeuger der multiplikativen Gruppe) der folgenden Körper:

   (a) $\mathbb{Z}_{29}$

   (b) $\mathbb{Z}_5[x]/(x^2 + x + 1)$

2. Sei p eine Primzahl, var eine Variable, $w, f \in \mathbb{Z}_p[var]$, wobei f irreduzibel ist. Die Mathematica-Funktion `PrimitiveQ[w_,f_,var_,p_]` soll `True` zurückgeben, falls $[w]_f$ ein primitives Element im Körper $\mathbb{Z}_p[var]/f$ ist. Vervollständigen Sie die Auslassung im Code der Funktion (siehe auch ue11ws05.nb). Verwenden Sie die Funktion `PolynomialPowerMod` zum Potenzieren von Polynomen.

```
PrimitiveQ[w_, f_, var_, p_] :=

    (* returns True if the element w from the field
        Z_p[var]/f is primitive, returns False otherwise *)

    Module[{size, factors, n, i, canStillBePrimitive, r},
      size = p^Deg[f, var];
      factors = FactorInteger[size - 1];
      n = Length[factors];
      i = 1;
      canStillBePrimitive = True;
      While[canStillBePrimitive && i <= n,
        r = (size - 1)/factors[[i]][[1]];
        canStillBePrimitive =  .......
        .......
      ];
      canStillBePrimitive];
```

3. Zur Schlüsselerzeugung für ElGamal: Finden Sie ein primitives Element des Körpers $\mathbb{Z}_2[x]/(1 + x^2 + x^6 + x^7 + x^9 + x^{10} + x^{11} + x^{12} + x^{16})$. Wählen Sie dazu zufällig ein Polynom und testen Sie es mit der Funktion aus Aufgabe 2 auf Primitivität.

4. Erzeugen Sie einen öffentlichen und einen privaten ElGamal-Schlüssel unter Verwendung der multiplikativen Gruppe des Körpers aus Aufgabe 3.