Wolfgang K. Seiler
Tel. 2515

B6, B4.08

8. Mai 2025

10. Übungsblatt Kryptologie

Aufgabe 1:

a) Berechnen Sie mit dem Euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $f = X^3 + 4X^2 + 5X + 2$ und $g = X^3 + 6X^2 - X - 6$ in $\mathbb{Q}[X]$!

b) Bestimmen Sie alle größten gemeinsamen Teiler von f und g in $\mathbb{Z}[X]$!

b) Betrachten Sie nun f und g modulo fünf und berechnen Sie ihren ggT in $\mathbb{F}_5[X]$!

Aufgabe 2:

a) Zeigen Sie: Ein Polynom vom Grad zwei oder drei über einem Körper k ist genau dann irreduzibel, wenn es keine Nullstelle in k hat.

b) Finden Sie ein nicht irreduzibles Polynom vom Grad vier über $\mathbb{F}_2$, das keine Nullstelle in $\mathbb{F}_2$ hat, und zeigen Sie, daß es das einzige Polynom mit diesen Eigenschaften ist!

c) Bestimmen Sie alle irreduziblen Polynome vom Grad zwei über $\mathbb{F}_3$!

d) Bestimmn Sie alle irreduziblen Polynome vom Grad drei über $\mathbb{F}_2$!

e) Betrachten Sie für jedes dieser Polynome P den Körper mit acht Elementen, der aus den Polynomen in X vom Grad höchstens zwei über $\mathbb{F}_2$ besteht und in dem die Multiplikation modulo P definiert ist. Berechnen Sie jeweils die Elemente X^4 und X^{-1}!

f) Zeigen Sie, daß in einem Körper k mit acht Elementen jedes von Null verschiedene Element die multiplikative Gruppe $k^\times$ erzeugt!

g) Gilt dies auch in einem Körper mit sechzehn Elementen?

h) Zeigen Sie: Ist k ein endlicher Körper mit q Elementen und erzeugt $g \in k$ die multiplikative Gruppe $k^\times$ von k, so erzeugt eine Potenz g^r von g diese Gruppe genau dann, wenn r teilerfremd zu $q - 1$ ist.

Aufgabe 3:

Im Körper mit 256 Elementen sei die Multiplikation modulo dem Polynom

$$P = X^8 + X^4 + X^3 + X + 1$$

definiert. Berechnen Sie die Potenzen X^n für $-2 \leq n \leq 15$!

Abgabe und Besprechung am Mittwoch, dem 14. Mai 2025, um 15.30 Uhr