RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Hausübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 12 / 15. Januar 2013 / Abgabe bis spätestens 22. Januar 2013, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (4 Punkte)**:**
Beweisen Sie den 2. Teil von Dicksons Lemma:
Sei $I = \langle x^\alpha \mid \alpha \in A \rangle \subset \mathbb{F}[X_1, \ldots, X_n]$ ein Monomideal für eine beliebige (potenziell unendliche) Erzeugermenge A. Zeigen Sie, dass I stets eine endliche Basis *aus Elementen der gegebenen Erzeugermenge* A besitzt, d.h. $A' \subset A$ existiert mit $I = \langle x^\alpha \mid \alpha \in A' \rangle$, $|A'|$ endlich.
Hinweis: Sie dürfen natürlich den 1. Teil von Dicksons Lemma benutzen. Es kann hilfreich sein, sich die Ascending Chain Condition und deren Beweis anzusehen.

AUFGABE 2 (5 Punkte)**:**
Sei $f = X^2Y^2 + X^2Y - y + 1, f_1 = XY^2 + X, f_2 = XY - Y^3$ in $\mathbb{Q}[X, Y]$. Wir wählen als Monomordnung $>_{\texttt{lex}}$ mit $X > Y$.

(a) Berechnen Sie den Divisionsrest von f, dividiert durch f_1, f_2 mittels des multivariaten Divisionsalgorithmus

(b) Berechnen Sie den Divisionsrest von f, dividiert durch f_2, f_1 mittels des multivariaten Divisionsalgorithmus

Beachten Sie, dass der Divisionsalgorithmus in (a) immer modulo f_1 reduziert und in (b) modulo f_2 reduziert, falls beides möglich ist.
Hinweis: Es ist nur der Divisionsrest gefragt! Sie dürfen den Algorithmus selbstverständlich soweit anpassen, dass er Ihnen nur das gefragte ausrechnet (vorausgesetzt, das Ergebnis wird nicht verändert und die Rechnung nachvollziehbar). Modulare Reduktion modulo f_1 kann man als Ersetzungsschritt auffassen, wobei man XY durch $-X$ ersetzt und modulo f_2 ersetzt XY durch Y^3. Allgemein kann man einen einzelnen Schritt des Divisionsalgorithmus hierbei so interpretieren, dass man ein Vorkommen von $LT(f_i)$ in $LM(f)$ durch $f_i - LT(f_i)$ ersetzt.

AUFGABE 3 (5 Punkte)**:**
Zeigen Sie:

(a) $>_{\texttt{grlex}}$ ist eine Monomordnung auf $\mathbb{N}^n$.

(b) $>_{\texttt{grevlex}}$ ist eine Monomordnung auf $\mathbb{N}^n$.

AUFGABE 4 (6 Punkte)**:**
Sei $\mathbb{F}$ ein Körper, $R := \mathbb{F}[X_1, \ldots, X_n]$ und sei $I \subset R$ ein Ideal mit einer Gröbnerbasis $G \subset I$ bzgl. einer beliebigen Monomordnung $>$.
Sei Q der von allen Monomen, die nicht durch ein Leitmonom von G teilbar sind, aufgespannte $\mathbb{F}$-Vektorraum (Q ist *kein* Ideal).
Wir betrachten die Abbildung $m : R \to Q, m(f) := f \bmod G$, d.h. die Abbildung, die einem Polynom f den (eindeutigen) Rest bei Polynomdivision mit G zuordnet. Zeigen Sie:

(a) m induziert eine wohldefinierte bijektive $\mathbb{F}$-lineare Abbildung $\alpha : R/I \to Q$ mittels $\alpha([f]) = m(f)$. Wie sieht die inverse Abbildung aus?

(b) m ist $\mathbb{F}$-linear.

Hierbei kann man den Quotienten $R/I = \{[f] \mid f \in R\}$ etwa als Menge von Äquivalenzklassen $[f] = f + I$ auffassen.

Hinweis: Da die Linearität von m aus der Definition des Polynomdivisionsalgorithmus heraus zumindest nicht offensichtlich ist, kann man den Homomorphiesatz nicht direkt anwenden, ohne vorher die Linearität zu zeigen. Geschickter ist es, sich zunächst zu überlegen, dass α wohldefiniert, d.h. nicht vom Repräsentanten abhängt und dass α bijektiv ist und dann die Inverse anzugeben. Die Linearität von α folgt dann am Ende aus der Linearität der Inversen. Bei dieser Vorgehensweise benötigt man nur den Satz „Eindeutigkeit des Rests“ und nicht die konkrete Definition der Polynomdivision.