Arithmetik in endlichen Körpern für den Web-Gauss-Calculator

Studenten

Ali Al-Kubaisi

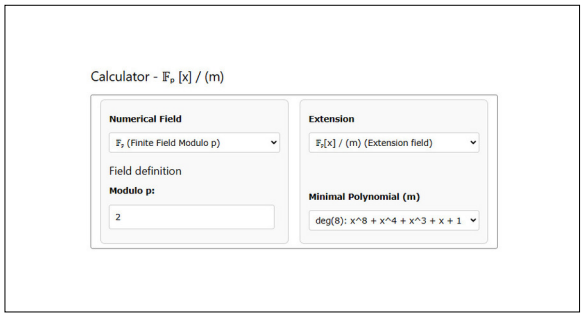
Simon Amberg

Ausgangslage: Das Ziel der Arbeit war, die Arithmetik in endlichen Körpern zu implementieren. Verwendet werden sollte diese dann in einer existierenden Web-Anwendung zum Gauss-Algorithmus (Gauss-Calculator). Die Implementation sollte dabei nicht nur den endlichen Körper F_p unterstützen, sondern auch Erweiterungen davon, wie Polynomringe $F_p[x]$ und die Erweiterung um ein Minimalpolynom zu einem neuen Körper. Diesen Körper sollte man neu über die Benutzeroberfläche wählen und konfigurieren können.

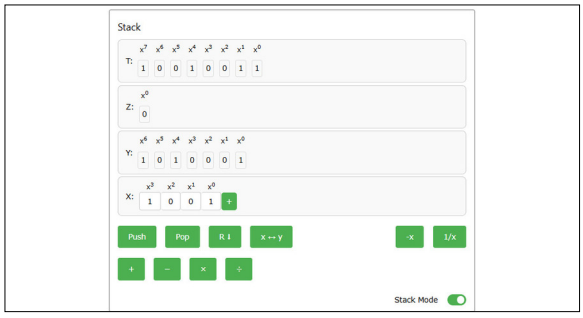
Vorgehen / Technologien: Um die Herausforderungen der Implementierung zu identifizieren, wurde zunächst eine detaillierte Analyse der Problemdomäne durchgeführt. Anschliessend wurde die Implementierung iterativ entwickelt, wobei ein Taschenrechner als erste Anwendung der Arithmetik implementiert wurde. Die Funktionalität des Rechners wurde schrittweise erweitert, um praktische Anwendungsfälle zu ermöglichen. Die Wahl der Reverse Polish Notation (RPN) für den Rechner ermöglicht eine effiziente Umsetzung der mathematischen Operationen. Die ursprünglich geplante Integration der entwickelten Lösung in den Gauss-Calculator wurde dem Auftraggeber überlassen.

Ergebnis: Es gelang eine geeignete Abstraktion zu finden, mit der die Arithmetik und Zahlenformate der verschiedenen Körper und Ringe einfach mit der Benutzeroberfläche verbunden werden konnte. Implementiert wird diese für die einzelnen mathematischen Körper und Ringe in ihren eigenen Klassen. Das Resulat dieser Arbeit ermöglicht es mit langen Ausdrücken in verschiedenen Körpern und Ringen zu rechnen und illustriert den Zusammenhang zwischen diesen Zahlenbereichen.

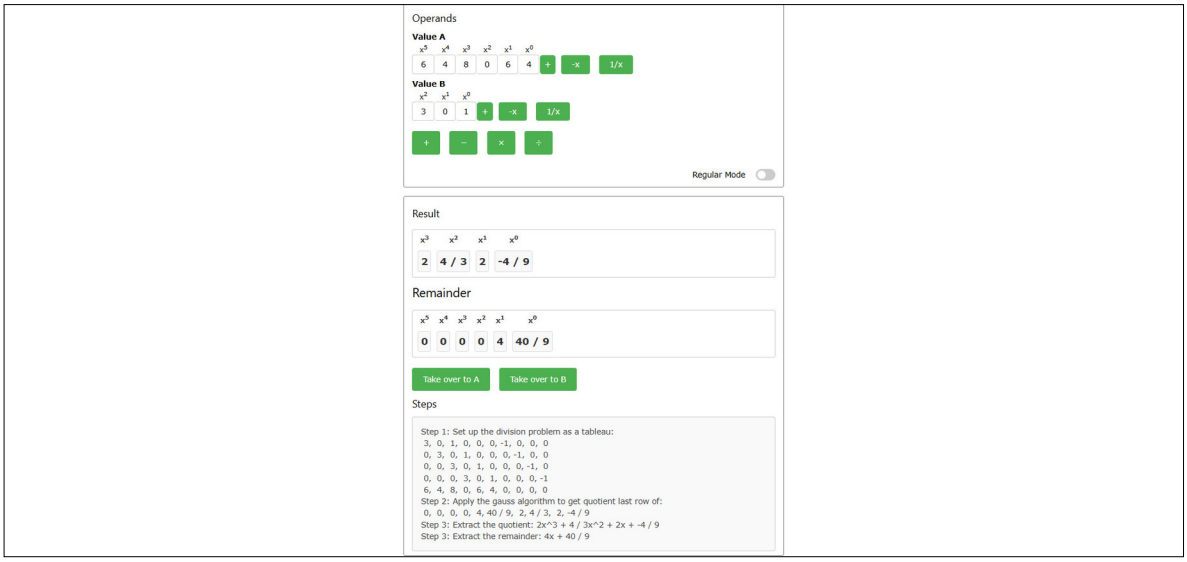
Konfiguration
Eigene Darstellung



RPN Modus
Eigene Darstellung



Normaler Modus mit Resultat
Eigene Darstellung



Referent
Prof. Dr. Andreas Müller

Korreferent
Prof. Dr. Thomas Kämpfer

Themengebiet
Internet-Technologien und -Anwendungen, Software