1. Übungsblatt zu Computeralgebra I, WS 1995/96

JOACHIM VON ZUR GATHEN, JÜRGEN GERHARD

Abgabe: Di, 31. 10. 1995 in der Vorlesung

Aufgabe 1 (Arithmetische Schaltkreise) *(3 Punkte)*

Sei F ein Körper. Zeichne arithmetische Schaltkreise über F für die folgenden Algorithmen:

i. Multiplikation zweier Polynome aus $F[x]$ vom Grad kleiner als 4 nach der Schulmethode. Eingaben sind dabei die 8 Koeffizienten der beiden Polynome, Ausgaben die 7 Koeffizienten des Produktpolynoms.

ii. Multiplikation zweier Polynome aus $F[x]$ vom Grad kleiner als 4 nach Karazuba-Ofman.

Aufgabe 2 (Komplexe Division) *(3 Punkte)*

Wie kann mit höchstens 7 reellen Multiplikationen und Divisionen der Quotient $\frac{z_1}{z_2}$ zweier komplexer Zahlen $z_1 = a_0 + a_1 i$, $z_2 = b_0 + b_1 i$ berechnet werden? Gegeben sind dabei die Real- und Imaginärteile a_0, a_1, b_0, b_1, gesucht Real- und Imaginärteil von $\frac{z_1}{z_2}$. Gib Deine Lösung auch in Form eines arithmetischen Schaltkreises an.

Anmerkung: Man kann zeigen, daß mindestens 6 nötig sind. Es ist aber nicht so einfach, einen Algorithmus zu finden, der tatsächlich mit 6 auskommt.

Aufgabe 3 (Karazuba-Ofman mit mehreren Blöcken) *(4 Punkte)*

Die in der Vorlesung vorgestellte Methode zur Multiplikation von Polynomen nach Karazuba-Ofman läßt sich verallgemeinern: Über dem Körper $\mathbb{F}$ seien die beiden Polynome $a = \sum_{0\leq i<n} a_i x^i, b = \sum_{0\leq i<n} b_i x^i \in \mathbb{F}[x]$, $n \in \mathbb{N}_{>0}$, zu multiplizieren. Dazu werden a und b in je m Blöcke ($m \in \mathbb{N}$, $m \geq 2$) der Größe $k = \lceil \frac{n}{m} \rceil$ zerlegt:

$$a = \sum_{0\leq i<m} A_i x^{ki}, \quad \deg A_i < k \ (0 \leq i < m)$$
$$b = \sum_{0\leq i<m} B_i x^{ki}, \quad \deg B_i < k \ (0 \leq i < m)$$

und anschließend $ab = \sum_{0\leq i<2m-1} C_i x^{ki}$ berechnet, wobei $C_i = \sum_{0\leq j\leq i} A_j B_{i-j}$ $(0 \leq i < 2m-1)$. Dabei sei $A_j, B_j = 0$ für $j \geq m$.

i. *Entwirf für* $m = 3$ *eine Vorschrift für die Berechnung von* $C_0, \ldots, C_4$, *die höchstens* 6 *Multiplikationen von Polynomen vom Grad kleiner als* k *benötigt. Konstruiere unter Verwendung dieser Vorschrift einen rekursiven Algorithmus à la Karazuba-Ofman und bestimme dessen Kosten, gemessen in der Anzahl* $\mathbb{F}$*-Operationen, für den Fall, daß* n *eine* 3*er-Potenz ist!*

ii. *Wieviele Multiplikationen von Polynomen vom Grad* $< k$ *darf die Berechnung von* $C_0, \ldots, C_{2m-2}$ *im allgemeinen Fall höchstens benötigen, damit ein darauf basierendes rekursives Verfahren asymptotisch besser ist als Karazuba-Ofman? Vergleiche mit Deinem Ergebnis aus i.!*

Aufgabe 4 (Programmieraufgabe) *(10 Punkte)*
(Bearbeitungszeit: bis Di, 14. 11. 1995)

i. *Programmiere den klassischen Multiplikationsalgorithmus und den Algorithmus von Karazuba-Ofman für Polynome über dem endlichen Körper* $\mathbb{F}_p$ *in einem Computeralgebrasystem! Die Programme sollen dabei so ausgelegt sein, daß prinzipiell Polynome beliebigen Grades multipliziert werden können.*

ii. *Entwirf eine geeignete Testreihe von Polynomen mit steigenden Graden und überprüfe, ob bzw. ab welchem Grad Karazuba-Ofman für* $p = 32003$ *schneller ist! Dabei brauchen nur Fälle berücksichtigt zu werden, deren Laufzeit im Minutenbereich liegt. Vergleiche die Zeiten auch mit denen der eingebauten Multiplikationsroutine für Polynome. Beschreibe die Testreihe und bewerte das Ergebnis. Stelle die Laufzeiten graphisch und/oder tabellarisch dar.*

iii. *Von welchen Faktoren (Hardware, Software, etc.) hängt es in der Praxis ab, wann der eine oder der andere Algorithmus schneller ist?*

Schnittstellenbeschreibung: Es sind zwei Prozeduren `plainmult` *und* `karazuba` *zu erstellen, die als Eingabeparameter eine Primzahl* `p` *und zwei Koeffizientenarrays* `l1` *und* `l2` *nehmen und als Ergebnis das Koeffizientenarray des Produktpolynoms zurückliefern. Die Anordnung der Koeffizienten soll dabei aufsteigend sein, d.h. das erste Element des Arrays ist der konstante Koeffizient des jeweiligen Polynoms. Für die Messung der Laufzeiten ist z.B. in Maple oder MuPAD die Funktion* `time` *zu verwenden. Bitte den Code kommentieren!*

Der Quellcode ist per e-mail an

`jngerhar@uni-paderborn.de`

zu schicken (bitte dazuschreiben, welches Computeralgebra-System Ihr gewählt habt), die schriftliche Bearbeitung spätestens in der Vorlesung am ?. 11. abzugeben.

Bemerkung: Dies ist eine experimentelle Aufgabe, d.h. es gibt nicht eine *richtige Lösung. Es ist gar nicht klar, ob sich das Karazuba-Verfahren in der Programmiersprache eines Computeralgebrasystems für „vernünftige" Größenordnungen (d.h. Laufzeiten im Bereich weniger Minuten) überhaupt lohnt – das sollt Ihr selbst herausfinden! Bewertet wird, ob das Programm läuft (andernfalls Punktabzug), aber auch die schriftliche Berbeitung der Teilaufgaben ii. und iii.*

Hinweise: Entsprechend gekennzeichnete Rechenaufgaben dürfen / sollen mit einem Computeralgebrasystem gelöst werden, wenn der Quelltext (z.B. „worksheet“ in Maple) und ein Protokollauf mit abgegeben wird. Empfohlen wird die Verwendung von MuPAD oder Maple, die beide bei allen Mathematik- und Informatik-Logins installiert sind. Maple wird mit `xmaple` und MuPAD mit `xmupad` aufgerufen.

Sollte MuPAD so nicht funktionieren, die folgenden Zeilen in Euer `.cshrc` einfügen:

```
setenv MuPAD_ROOT_PATH /usr/local/MuPAD
setenv FONT_PATH $MuPAD_ROOT_PATH/share/doc/hytex/fonts
setenv MANPATH ${MANPATH}:${MuPAD_ROOT_PATH}/share/doc/man
set path = ($path $MuPAD_ROOT_PATH/share/bin)
```

Spätestens beim nächsten Mal einloggen sollte es dann wie beschrieben funktionieren.

Bei Fragen und Problemen bitte an Jürgen Gerhard (`jngerhar@mathematik`) oder die jeweilige Rechnerbetreuung wenden!

Die AG Algorithmische Mathematik ist über WWW entweder von der Mathematik-Homepage

`http://math-www.uni-paderborn.de/`

oder direkt über

`http://www.uni-paderborn.de/cs/gathen.html`

erreichbar. Dort sind auch jeweils aktuelle Versionen von für die Computeralgebra-Vorlesung interessanten Dokumenten wie z.B. das Skript zu finden.

2. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Di, 7. 11. 1995 in der Vorlesung

Aufgabe 5 (Faltung) *(4 Punkte)*

i. *Zeige, daß die Faltungsoperation für diskrete Signale kommutativ ist, d.h.* $x * y = y * x$ *für alle Signale* $x, y : \mathbb{Z} \longrightarrow \mathbb{R}$. *Dabei darf angenommen werden, daß alle vorkommenden Summen absolut konvergieren.*

ii. *Seien* $n \in \mathbb{N}_{>0}$ *und* $\alpha_0, \beta_0, \ldots, \alpha_{n-1}, \beta_{n-1}$ *reelle Zahlen. Die diskreten Signale* $x, y : \mathbb{Z} \longrightarrow \mathbb{R}$ *sind gegeben durch*

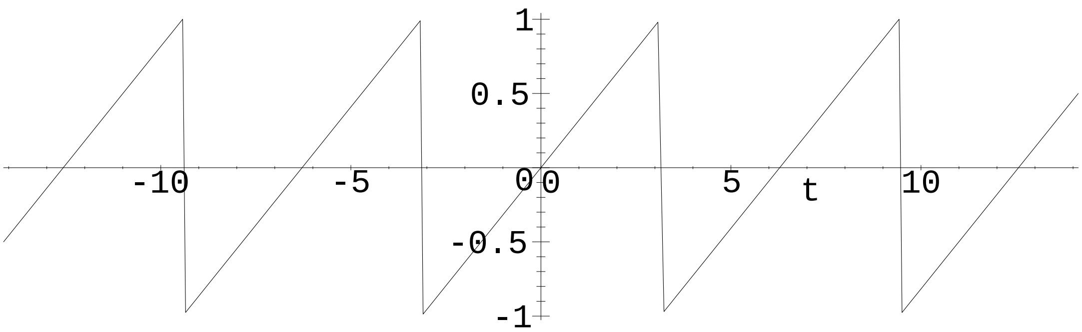
$$x(k) = \begin{cases} \alpha_k & (0 \le k < n) \\ 0 & \text{sonst} \end{cases} \quad \text{bzw. } y(k) = \begin{cases} \beta_k & (0 \le k < n) \\ 0 & \text{sonst} \end{cases}$$

Berechne das gefaltete Signal $z = x * y$. *Woran erinnert Dich das?*

iii. *Zeige, daß für zwei analoge Signale* $f, g : [0, 2\pi] \longrightarrow \mathbb{C}$, *die absolut integrierbar sind (d.h.* $f, g \in L^1([0, 2\pi])$*), gilt:* $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$.

Aufgabe 6 (Fourier-Reihen) *(4 Punkte)*

i. *Berechne die komplexen Fourierkoeffizienten* b_k $(k \in \mathbb{Z})$ *in der Reihenentwicklung* $f(t) = \sum_{k \in \mathbb{Z}} b_k e^{ikt}$ *für die* 2π*-periodische Sägezahn-Schwingung* $f(t) = \frac{t}{\pi}$ $(-\pi \le t < \pi)$:



ii. *Berechne die Fourierkoeffizienten von* $f(t) = e^{int}$ *für ein festes* $n \in \mathbb{Z}$.

Aufgabe 7 (Primitive Einheitswurzeln) *(3 Punkte)*

Seien R ein Ring (kommutatuv, mit Einselement), $n \in \mathbb{N}_{>0}$ und $\omega \in R$ eine primitive n-te Einheitswurzel (n-PEW). Zeige:

i. *$\omega \in R^\times$, und ω^{-1} ist ebenfalls eine n-PEW.*

ii. *Für jeden Teiler $m \in \mathbb{N}_{>0}$ von n ist ω^m eine $\frac{n}{m}$-PEW.*

Aufgabe 8 (Einheitswurzeln in Körpern) *(6 Punkte)*

*Sei $n \in \mathbb{N}_{>0}$ und K ein Körper, dessen Charakteristik kein Teiler von n ist. Ein Element $\omega \in K$ heißt n-*te Einheitswurzel, *wenn $\omega^n = 1$ ist. Zeige:*

i. *Die Menge K_n aller n-ten Einheitswurzeln ist eine Untergruppe der multiplikativen Gruppe $K^\times$.*

ii. *Für eine n-te Einheitswurzel $\omega \in K$ sind äquivalent:*

   (a) ω ist eine primitive n-te Einheitswurzel (n-PEW),

   (b) $\omega^k \neq 1$ für $0 < k < n$,

   (c) $\omega^k \neq 1$ für $0 < k < n$ mit $k \mid n$.

Für die Teilaufgaben iii. und iv. enthalte K eine primitive n-te Einheitswurzel. Zeige:

iii. *K_n ist zyklisch und isomorph zur additiven Gruppe $\mathbb{Z}/n\mathbb{Z}$ (insbesondere ist also $\#K_n = n$).*

iv. *Es gibt genau $\varphi(n)$ primitive n-te Einheitswurzeln, wobei φ die Euler'sche φ-Funktion mit $\varphi(n) = \#\{0 \leq k < n : \mathrm{ggT}(k, n) = 1\}$ ist.*

v. *Zeichne die 12-ten Einheitswurzeln für $K = \mathbb{C}$ und markiere die primitiven!*

3. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Di, 14. 11. 1995 in der Vorlesung

Aufgabe 9 (PEW modulo einer Mersenne-Zahl) *(4 Punkte)*

Für zwei Zahlen $a, b \in \mathbb{N}$, $b \neq 0$, bezeichne $\mathrm{rem}(a,b)$ *den Rest bei Division von a durch b mit Rest, d.h. diejenige Zahl* $r \in \mathbb{N}$ *mit* $a \equiv r \bmod b$ *und* $0 \leq r < b$.

i. *Seien $a, m, n \in \mathbb{N}_{>0}$, $a \geq 2$, $r = \mathrm{rem}(n,m)$ und $g = \mathrm{ggT}(n,m)$. Zeige, daß* $\mathrm{rem}(a^n - 1, a^m - 1) = a^r - 1$ *ist, und folgere daraus* $\mathrm{ggT}(a^n - 1, a^m - 1) = a^g - 1$.

ii. *Für Zahlen $a \in \mathbb{N}$ und $m \in \mathbb{N}_{>0}$ gilt:* $a \bmod m$ *ist Nullteiler* $\Longleftrightarrow$ $\mathrm{ggT}(a,m) \neq 1$.

iii. *Sei $n \in \mathbb{N}$, $n \geq 2$. Die Zahl $M_n = 2^n - 1$ heißt* n-te Mersenne-Zahl. *Zeige (unter Verwendung von i. und ii.), daß 2 in $\mathbb{Z}/M_n\mathbb{Z}$ genau dann eine n-PEW ist, wenn n prim ist.*

Bemerkung *Falls M_n prim ist, heißt M_n eine* Mersenne-Primzahl. *Aus i. folgt, daß das nur der Fall sein kann, wenn n prim ist. Diese Bedingung ist jedoch nicht hinreichend. Das kleinste Gegenbeispiel liefert $n = 11$: $M_{11} = 2047 = 23 \cdot 89$.*

Aufgabe 10 (FFT m-adisch) *(4 Punkte)*

Wie bei Karazuba-Ofman kann auch die schnelle Fouriertransformation verallgemeinert werden durch Aufteilen des Polynoms in m Blöcke. Sei R ein Ring, n eine Potenz von m, $\omega \in R$ eine n-PEW und $a = \sum_{0 \leq i < n} a_i x^i \in R[x]$ ein Polynom.

i. *Beschreibe einen Divide-and-conquer-Algorithmus zur Berechnung von* $\mathrm{DFT}_\omega(a)$ *durch Aufteilen von a in m Blöcke der Größe $\frac{n}{m}$. Beweise, daß der Algorithmus partiell korrekt ist.*

ii. *Zeichne einen arithmetischen Schaltkreis für den Algorithmus im Fall $m = 3$, $n = 9$.*

iii. *Stelle die Rekursionsgleichung für die Kosten auf und löse sie.*

Aufgabe 11 (Schnelle Faltung von Polynomen) *(3 Punkte)*

Sei F ein algebraisch abgeschlossener Körper der Charakteristik $\neq 2$. Dann hat F für jedes $k \in \mathbb{N}$ eine 2^k-PEW. Für $n \in \mathbb{N}$ und $a = \sum_{0 \leq i < n} a_i x^i, b = \sum_{0 \leq j < n} b_j x^j \in F[x]$ sei $a *_n b = \sum_{0 \leq k < n} c_k x^k \in F[x]$ mit

$$c_k = \sum_{\substack{0 \leq i,j < n \\ i+j \equiv k \bmod n}} a_i b_j$$

die Faltung von a und b. In dieser Aufgabe soll gezeigt werden, daß für beliebiges *$n \in \mathbb{N}$ die Faltung $*_n$ mit $O(n \log n)$ Körperoperationen berechnet werden kann.*

Seien $n \in \mathbb{N}$ und $a, b \in F[x]$ wie oben und $m \in \mathbb{N}$ eine Potenz von 2 mit $\frac{m}{2} < 2n \leq m$. Setze $A = a \cdot (1 + x^{m-n})$ und $B = b$. Zeige, daß die Koeffizienten von $a *_n b$ aus denen von $A *_m B$ berechnet werden können und folgere daraus die Behauptung.

Aufgabe 12 (FFT und Faltung über einem endlichen Körper) *(8 Punkte)*

i. *Zeige, daß $\omega = 14 \in \mathbb{F}_{41}$ eine 8-te PEW ist. Gib* alle *8-ten PEW in $\mathbb{F}_{41}$ an.*

ii. *Seien $\eta = \omega^2$ und*

$$\begin{aligned} a = (a_0, \ldots, a_7) &= (6, 2, 0, 0, 3, 0, 2, 1) \in \mathbb{F}_{41}^8, \\ b = (b_0, \ldots, b_7) &= (1, 0, 0, 35, 0, 12, 0, 1) \in \mathbb{F}_{41}^8. \end{aligned}$$

Berechne $A = \mathrm{DFT}_\omega(a)$ und $B = \mathrm{DFT}_\omega(b)$ explizit durch Anwendung der FFT. Du brauchst dabei nur einen Rekursionsschritt durchführen, danach kannst Du DFT_η direkt durch Auswerten von Polynomen an den Potenzen von η berechnen.

iii. *Berechne $C = A \cdot B$ durch komponentenweise Multiplikation und $c = \mathrm{DFT}_\omega^{-1}(C)$.*

iv. *Berechne $\overline{a} \cdot \overline{b}$, wobei $\overline{a} = \sum_{0 \leq i < 8} a_i x^i, \overline{b} = \sum_{0 \leq i < 8} b_i x^i \in \mathbb{F}_{41}[x]$ die zu a bzw. b gehörigen Polynome sind. Berechne die Faltung $a * b$ aus dem Produktpolynom $\overline{a} \cdot \overline{b}$. Vergleiche das Ergebnis mit dem der vorherigen Teilaufgabe.*

<u>*Hinweis:*</u> *Zur Lösung der Aufgabe darf ein Computeralgebrasystem verwendet werden. In diesem Fall bitte den Quelltext und/oder ein Ablaufprotokoll mit abgeben.*

4. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Di, 28. 11. 1995 in der Vorlesung

Aufgabe 13 (Frobenius-Abbildung) *(3 Punkte)*

Seien p eine Primzahl, $q = p^k$ für ein $k \in \mathbb{N}_{>0}$ und $\mathbb{F}_q$ ein endlicher Körper mit q Elementen. Zeige:

i. *Für Unbestimmte x, y über $\mathbb{F}_q$ und alle $l \in \mathbb{N}$ gilt $(x+y)^{p^l} = x^{p^l} + y^{p^l}$.*

ii. *Für alle Polynome $f \in \mathbb{F}_q[x]$ gilt $f^q = f(x^q)$.*

iii. *Für $f \in \mathbb{F}_q[x]$ ist $f^q - f = \prod_{u \in \mathbb{F}_q}(f-u)$.*

Aufgabe 14 (Linearisierte Polynome) *(5 Punkte)*

Seien q eine Primpotenz, $m \in \mathbb{N}_{>0}$, $\mathbb{F}_q$ ein endlicher Körper mit q Elementen, $\mathbb{F}_{q^m}$ ein Erweiterungskörper von $\mathbb{F}_q$, $(\beta_1, \ldots, \beta_m)$ eine $\mathbb{F}_q$-Vektorraumbasis von $\mathbb{F}_{q^m}$ über $\mathbb{F}_q$, $W_i = \operatorname{span}\{\beta_1, \ldots, \beta_i\} \subseteq \mathbb{F}_{q^m}$ und $s_i = \prod_{\alpha \in W_i}(x-\alpha) \in \mathbb{F}_{q^m}[x]$ für $0 \le i \le m$ wie in der Vorlesung. Vervollständige den Beweis des Lemmas aus der Vorlesung:

i. *Für $1 \le i \le m$ gilt die Rekursionsformel*

$$s_i = s_{i-1}^q - s_{i-1}(\beta_i)^{q-1} \cdot s_{i-1}.$$

ii. *Für $0 \le i \le m$ und alle $c \in \mathbb{F}_q$ gilt $s_i(cx) = cs_i(x)$.*

iii. *Ein Polynom $f \in \mathbb{F}_{q^m}[x]$ heißt* q-Polynom, *wenn es von der Form $f = \sum_{0 \le j \le n} f_j x^{q^j}$ mit $f_j \in \mathbb{F}_{q^m}$ für alle j ist. Folgere aus der vorigen Teilaufgabe, daß s_i für $0 \le i \le m$ ein q-Polynom ist, und gib eine Rekursionsformel für die Berechnung der Koeffizienten von s_i aus den Koeffizienten von s_{i-1} an.*

Aufgabe 15 (Division mit Rest durch dünne Polynome) *(4 Punkte)*

Seien F ein Körper und $g = x^n + \sum_{0 \le i < n} g_i x^i \in F[x]$, $g_i \in F$, ein normiertes Polynom n-ten Grades. Das Gewicht *$w(g)$ ist die Anzahl von 0 verschiedener Koeffizienten von g außer dem Leitkoeffizienten:*

$$w(g) = \#\{0 \le i < n : g_i \ne 0\}.$$

i. *Zeichne einen möglichst kleinen arithmetischen Schaltkreis für die Division von Polynomen vom Grad < 9 durch das Polynom $g = x^6 - 3x^4 + 2$ mit Rest nach der Schulmethode.*

ii. *Sei $m \geq n$. Zeige: Polynome vom Grad $< m$ können unter Verwendung von je $w(g) \cdot (m - n)$ Multiplikationen und Subtraktionen in F mit Rest durch g dividiert werden (dabei sind sowohl der Quotient als auch der Divisionsrest zu berechnen).*

Aufgabe 16 (Auswerten von Polynomen über $\mathbb{F}_{16}$) *(8 Punkte)*

Der endliche Körper $\mathbb{F}_{16}$ wird im folgenden repräsentiert als $\mathbb{F}_2[t]/(m)$, wobei $m = t^4 + t + 1 \in \mathbb{F}_2[t]$ ein irreduzibles Polynom ist. Sei $y = t \bmod m \in \mathbb{F}_2[t]/(m)$. Jedes Element $a \in \mathbb{F}_{16}$ hat die Form $a = a_0 + a_1 y + a_2 y^2 + a_3 y^3$ mit $a_0, \ldots, a_3 \in \mathbb{F}_2$ und wird repräsentiert durch das Polynom $a_0 + a_1 t + a_2 t^2 + a_3 t^3 \in \mathbb{F}_2[t]$ vom Grad < 4, genannt der kanonische Repräsentant von *a. Die Addition bzw. Multiplikation zweier Elemente entspricht der Addition bzw. Multiplikation ihrer kanonischen Repräsentanten mit anschließender Reduktion modulo m.*

Diese Aufgabe soll überwiegend mit MuPAD gelöst werden (bitte Ablaufprotokoll mit abgeben). Dazu gibt man nach dem Start (mit `xmupad`*) zunächst folgendes ein:*

```
>> loadlib("domains"): export(domains):
>> F16 := AlgebraicExtension(IntegerMod(2), y^4+y+1=0, y):
```

Danach können Elemente von $\mathbb{F}_{16}$ z.B. mit

```
>> a := F16(y^3+y+1);
```

definiert werden und mit Hilfe der üblichen arithmetischen Operatoren `+,*,/` *addiert, multipliziert und dividiert werden.*

Polynome über $\mathbb{F}_{16}$ in der Variablen x werden z.B. mit

```
>> p := poly(x^3+(1+y^2)*x+(1+y+y^3), [x], F16);
```

definiert und können mit `+,*` *addiert und multipliziert werden. Der Aufruf* `divide(p,q)` *liefert den Quotienten und den Rest bei Division von* `p` *durch* `q` *zurück. Ein Polynom* `p` *kann mit* `p(a)` *an einem Element* `a` *von $\mathbb{F}_{16}$ ausgewertet werden.*

i. *Zeige: y ist eine 15-PEW in $\mathbb{F}_{16}$.*
ii. *Definiere $\beta_1 = 1$, $\beta_2 = y^2 + y$, $\beta_3 = y^2$ und $\beta_4 = y^3 + y$ in $\mathbb{F}_{16}$. Beweise (ohne MuPAD!), daß $(\beta_1, \beta_2, \beta_3, \beta_4)$ eine Basis von $\mathbb{F}_{16}$ über $\mathbb{F}_2$ ist.*
iii. *Gib die Elemente von $W_i = \operatorname{span}\{\beta_1, \ldots, \beta_i\}$ für $0 \leq i \leq 4$ an.*
iv. *Berechne die Polynome $s_i = \prod_{\alpha \in W_i}(x - \alpha) \in \mathbb{F}_{16}[x]$ für $0 \leq i \leq 4$ und die Elemente $s_i(\beta_j) \in \mathbb{F}_{16}$ für $0 \leq i < j \leq 4$.*
v. *Sei*

$$\begin{aligned} f \quad = \quad & \left(y + y^2 + y^3\right) x^{15} + x^{14} + \left(y^2 + y^3\right) x^{11} + x^{10} + \left(y + y^2 + y^3\right) x^9 \\ & + \left(1 + y^2 + y^3\right) x^8 + \left(y + y^3\right) x^7 + \left(1 + y^2 + y^3\right) x^5 + y x^2 + y^2 x \end{aligned}$$

in $\mathbb{F}_{16}[x]$. Protokolliere den Algorithmus aus der Vorlesung zum Auswerten von f an allen Punkten von $\mathbb{F}_{16}$. Es genügt, dies bis zur Rekursionstiefe 2 zu tun, d.h. das Auswerten von Polynomen vom Grad < 4 an 4 Punkten darf direkt (ohne weitere rekursive Aufrufe) durchgeführt werden.

5. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Do, 7. 12. 1995 in der Vorlesung

Aufgabe 17 (Divide-and-conquer-Rekursion) *(4 Punkte)*

Seien $S, T : \mathbb{N}_{>0} \longrightarrow \mathbb{R}_{\geq 0}$ *Funktionen, die den Ungleichungen*

$$\begin{aligned} T(1) &\leq d, \\ T(n) &\leq aT(\frac{n}{b}) + cS(n) \quad \text{für } n = b^k, k \in \mathbb{N}_{>0}, \\ S(bn) &\geq bS(n) \text{ für alle } n \in \mathbb{N}_{>0} \end{aligned}$$

mit Konstanten $b \in \mathbb{N}_{>0}$ *und* $a, c, d \in \mathbb{R}_{\geq 0}$ *genügen. Solche Funktionen treten häufig als Laufzeitschranken von divide-and-conquer-Algorithmen auf.*

i. *Zeige, daß sich* $T(n)$ *für* $n = b^k$, $k \in \mathbb{N}$, *durch*

$$T(n) \leq An^{\log_b a} + BS(n)n^{\log_b a - 1} + CS(n)\log_b n + DS(n) + E$$

nach oben abschätzen läßt, und berechne – in Abhängigkeit von a, b, c, d *– die zugehörigen Konstanten* $A, B, C, D, E \in \mathbb{R}$*! (Hinweis: Abwickeln der Rekursion) Unterscheide dabei die drei Fälle* $a < b$, $a = b$ *und* $a > b$.

ii. *Seien nun* S, T *monoton wachsend, und gelte ferner* $S(bn) \leq b^2 n$ *und* $S(n) \geq en$ *für alle* $n \in \mathbb{N}_{>0}$ *und eine weitere Konstante* $e \in \mathbb{N}_{>0}$*. Folgere aus i. eine möglichst gute O-Abschätzung (nur der dominante Term ist wichtig) für* $T(n)$*, die für* alle $n \in \mathbb{N}_{>0}$ *gilt! (Hinweis:* n *liegt in einem geeigneten Intervall* $[b^{k-1} + 1, b^k]$*)*

Aufgabe 18 (Inverse modulo 3^8) *(3 Punkte)*

Berechne $94^{-1} \bmod 6561$ *mit dem Newton-Verfahren (Rechenweg!).*

Aufgabe 19 (Kubikwurzeln modulo x^n) *(4 Punkte)*

i. *Sei* $n \in \mathbb{N}_{>0}$*. Wieviele Kubikwurzeln* $h \in \mathbb{F}_7[x]$ *von* $b = 1 - x + x^2 - x^3 \in \mathbb{F}_7[x]$ *modulo* x^n *mit* $\deg h < n$ *gibt es (Begründung!), und wie berechnet man sie?*

ii. *Berechne eine solche für* $n = 4$.

Aufgabe 20 (Kosten des Newton-Verfahrens für Polynome)

(4 Punkte)

Seien $R = F[x]$ *der Polynomring über einem Körper,* $f \in R[y]$ *mit* $\deg f = d > 0$, $h_0 \in R$ *mit* $f(h_0) \equiv 0 \bmod x$ *und* $f'(h_0) \not\equiv 0 \bmod x$, *wobei* $'$ *die formale Ableitung nach* y *bezeichnet,* $k \in \mathbb{N}$ *und* $n = 2^k$. *Zeige, daß das Newton-Verfahren zur Berechnung von* $h \in R$ *mit* $f(h) \equiv 0 \bmod x^n$ *und* $h \equiv h_0 \bmod x$ *mit* $O(d \cdot \mathsf{M}(n))$ *Körperoperationen auskommt (*$\mathsf{M}(n)$ *ist die „Multiplikationszeit" für Polynome vom Grad* n *über* F*). Das* <u>*richtige*</u> *Ergebnis aus Aufgabe 17 darf verwendet werden.*

Hinweis: Zeige zunächst, daß die Berechnung von $g(u) \bmod x^m$ *für* $g \in R[y]$, $u \in R$ *und* $m \in \mathbb{N}_{>0}$ $O(\deg g \cdot \mathsf{M}(m))$ *Operationen in* F *benötigt (denke dabei an das Auswerten von Polynomen).*

6. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Di, 19. 12. 1995 in der Vorlesung

Aufgabe 21 (Euklidische Funktion in $\mathbb{Z}[i]$) *(3 Punkte)*

Zeige, daß die Norm $N : \mathbb{Z}[i] \to \mathbb{N}_0$; $N(\alpha) = \alpha\overline{\alpha}$ auf dem Ring der Gaußschen Zahlen $\mathbb{Z}[i]$ mit $i = \sqrt{-1} \in \mathbb{C}$ eine euklidische Funktion ist! Hinweis: Betrachte den exakten Quotienten zweier Zahlen $\alpha, \beta \in \mathbb{Z}[i]$ in $\mathbb{C}$.

Aufgabe 22 (Anwendungen des (E)EA) *(4 Punkte)*

Seien $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ der endliche Körper mit 7 Elementen, $f = x^7 - x - 1 \in \mathbb{F}_7[x]$ und $a = x^6 - x^5 \in \mathbb{F}_7[x]$.

i. *Das Polynom f ist irreduzibel und daher der Restklassenring $F = \mathbb{F}_7[x]/(f)$ ein endlicher Körper mit 7^7 Elementen. Berechne $a^{-1} \bmod f$ in F.*

ii. *Berechne die Kettenbruchentwicklung der rationalen Funktion $\frac{f}{a} \in \mathbb{F}_7(x)$.*

Bei den Aufgaben ist jeweils der Rechenweg anzugeben.

Aufgabe 23 (Fibonacci-Polynome) *(5 Punkte)*

Die Folge $f_0, f_1, f_2, \ldots \in \mathbb{Q}[x]$ normierter Polynome ist durch die folgenden Eigenschaften definiert:

1. $\mathrm{ggT}(f_n, f_{n-1}) = 1$ *für alle $n \geq 1$,*
2. *für jedes $n \geq 1$ hat das Euklidische Schema für f_n und f_{n-1} die Länge n, und sämtliche n Quotienten sind gleich x.*

i. *Welches sind die Reste im Euklidischen Schema für f_n und f_{n-1}? Gib eine Rekursionsformel, einschließlich geeigneter Startwerte, für die f_n an (Begründung). Welchen Grad hat f_n?*

ii. *Formuliere und beweise einen Satz, der besagt, daß f_n und f_{n-1} die „längstmögliche" (was das heißt, ist dabei natürlich zu explizieren) Quotientenfolge haben. Welche weiteren Polynompaare haben diese Eigenschaft?*

7. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Do, 11. 1. 1996 in der Vorlesung

Aufgabe 24 (Kongruenzensystem) *(3 Punkte)*

Wieviele Lösungen $x \in \mathbb{Z}$ mit $0 \le x \le 10^6$ hat das folgende Kongruenzensystem?

$$\begin{aligned} x &\equiv 2 \bmod 11, \\ x &\equiv -1 \bmod 13, \\ x &\equiv 10 \bmod 17. \end{aligned}$$

Aufgabe 25 (Kubikwurzeln modulo n) *(8 Punkte)*

Für $n \in \mathbb{N}$, $n \ge 2$ und $a \in \mathbb{Z}$ bezeichnen wir mit $N_n(a)$ die Anzahl Lösungen der Kongruenz $x^3 \equiv a \bmod n$ mit $0 \le x < n$.

i. *Zeige, daß für eine ungerade Primzahl p gilt:*
   - $N_p(a) \le 3$,
   - $N_p(a) = 1$ *falls* $p \mid a$ *oder* $p = 3$,
   - $N_p(a) \ne 2$ *falls* $3 \ne p \nmid a$, *und für jeden Wert* $N \in \{0, 1, 3\}$ *gibt es eine ungerade Primzahl* p *und* $a \in \mathbb{Z}$ *mit* $3 \ne p \nmid a$ *und* $N_p(a) = N$.

   Bitte jeweils Beispiele bzw. Begründung angeben.

ii. *Sei p^e ($e > 0$) eine Primpotenz und $p > 3$. Begründe, daß $N_{p^e}(a) = N_p(a)$ für $p \nmid a$ gilt, und gib ein Gegenbeispiel für den Fall $p \mid a$ an. (Hinweis: Newton-Iteration)*

iii. *Sei nun $n \in \mathbb{N}$ mit $\mathrm{ggT}(n, 6) = 1$ und $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ seine Primfaktorzerlegung ($e_i > 0$ für $1 \le i \le r$, $r > 0$). Berechne $N_n(a)$ in Abhängigkeit von $N_{p_1}(a), \ldots, N_{p_r}(a)$ für den Fall, daß a und n teilerfremd sind. (Hinweis: Chinesischer Restsatz)*

iv. *Berechne <u>alle</u> Kubikwurzeln von 11 modulo 225625 im Bereich $\{0, 1, \ldots, 225624\}$! Dazu gehören der Rechenweg und eine Begründung, warum es keine weiteren gibt. Zwischenrechnungen dürfen mit einem Computeralgebrasystem durchgeführt werden; in diesem Fall bitte ein Ablaufprotokoll mit abgeben.*

Aufgabe 26 (Subresultanten) *(8 Punkte)*

Diese Aufgabe ist etwas umfangreicher und verfolgt zwei Ziele: Zum einen soll der Umgang mit einem Computeralgebrasystem geübt, zum anderen der Zusammenhang zwischen Subresultanten und dem Erweiterten Euklidischen Schema für Polynome verdeutlicht werden.

Seien

$$\begin{aligned} f &= x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5 \\ g &= 3x^6 + 5x^4 - 4x^2 - 9x + 21 \end{aligned}$$

Polynome über $\mathbb{Z}$.

i. *Berechne alle Einträge* a_i, q_i, s_i, t_i *für* $1 \leq i \leq l$ *des Erweiterten Euklidischen Schemas für* $a_0 = f = \sum_{0 \leq j \leq 8} f_j x^j$, $a_1 = g = \sum_{0 \leq j \leq 6} g_j x^j$ *über* $\mathbb{Q}[x]$.

   Für $0 \leq k < 6$ *sei* $P_k \in \mathbb{Z}^{(14-2k)\times(14-2k)}$ *die Matrix*

$$\left(\begin{array}{cccccccc} f_8 & 0 & 0 & \cdots & g_6 & 0 & 0 & \cdots \\ f_7 & f_8 & 0 & \ddots & g_5 & g_6 & 0 & \ddots \\ f_6 & f_7 & f_8 & \ddots & g_4 & g_5 & g_6 & \ddots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \ddots & \ddots \end{array}\right)$$
$$\underbrace{\qquad\qquad\qquad}_{6-k} \quad \underbrace{\qquad\qquad\qquad}_{8-k}$$

   wie in der Vorlesung.

ii. *Rechne die Richtigkeit der Polynomgleichung* $s_i f + t_i g = a_i$ *für* $2 \leq i \leq l$ *nach. „Übersetze" die Gleichung in ein nichtsinguläres lineares Gleichungssystem der Form* $P_k x_k = u_k$ *mit einem Vektor* x_k *von* $14 - 2k$ *Unbestimmten. Dabei ist* $k \in \{0, \ldots, 5\}$ *und* $u_k \in \mathbb{Q}^{14-2k}$ *in Abhängigkeit von i geeignet zu wählen. Berechne* $\det P_k$. *Welche k kommen für* $2 \leq i \leq l$ *vor und warum?*

iii. *Gib die Lösung* $v_k \in \mathbb{Q}^{14-2k}$ *für* x_k *in jedem der Gleichungssysteme unter ii. an und begründe ohne Rechnung, warum es sich um eine Lösung handelt. Rechne das zusätzlich nach.*

iv. *Für welche der* $k \in \{0, \ldots, 5\}$, *die nicht in ii. vorkommen, ist* P_k *singulär und warum? Gib für diese k einen Vektor* $0 \neq v_k \in \mathbb{Q}^{14-2k}$ *mit* $P_k v_k = 0$ *an (Begründung ohne Rechnung). Rechne die Aussage zusätzlich nach.*

Wir wünschen allen Studierenden ein frohes Weihnachtsfest und einen guten Rutsch!

8. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Di, 23. 1. 1996 in der Vorlesung

Aufgabe 27 (Durchschnitt zweier Kurven) *(5 Punkte)*

Gegeben sind die beiden ebenen Kurven

$$\mathcal{C} = \{(x,y) \in \mathbb{R}^2\colon\ y - x^3 + 7x - 5 = 0\},$$
$$\mathcal{D} = \{(x,y) \in \mathbb{R}^2\colon\ 20x^2 - 5xy - 4y^2 + 35x + 35y - 21 = 0\}$$

in $\mathbb{R}^2$. Bestimme unter Verwendung von Resultanten auf zwei Arten alle Punkte der Schnittmenge $\mathcal{C} \cap \mathcal{D} \subseteq \mathbb{R}^2$: einmal mit Projektion auf die x-Achse, und auch mit Projektion auf die y-Achse. Was fällt beim Vergleich der beiden Methoden auf? Plotte die beiden Kurven und markiere die gefundenen Schnittpunkte. Für die Aufgabe darf ein Computeralgebrasystem verwendet werden. Zum Plotten impliziter Funktionen ist einmalig in Maple `with(plots):` *bzw. in Mupad* `loadlib("plotlib"): export(plotlib):` *einzugeben; danach ist der Befehl* `implicitplot` *verfügbar.*

Aufgabe 28 (Potenzen in endlichen Körpern) *(10 Punkte)*

Seien $p \in \mathbb{N}$ eine Primzahl, $\mathbb{F}_p$ der endliche Körper mit p Elementen und $n \in \mathbb{N}_{>0}$. Zeige:

i. Für $a \in \mathbb{F}_p^\times$ ist $\operatorname{ord}_p(a^n) = \dfrac{\operatorname{ord}_p(a)}{\operatorname{ggT}(n, \operatorname{ord}_p(a))}$.

ii. Zeichne je einen gerichteten Graphen mit Knotenmenge $\mathbb{F}_{17}^\times$ für die Quadratabbildung $x \mapsto x^2$ und die Kubikabbildung $x \mapsto x^3$ in $\mathbb{F}_{17}^\times$. In dem jeweiligen Graphen soll es genau dann eine Kante von a nach b geben, wenn $a^2 = b$ bzw. $a^3 = b$ ist. Schreibe die Ordnungen an die Knoten. Was fällt beim Vergleich der beiden Graphen auf?

Seien nun n ein Teiler von $\#\mathbb{F}_p^\times = p-1$, $P_n = \{a \in \mathbb{F}_p^\times : \exists b \in \mathbb{F}_p^\times\ b^n = a\}$ die Menge der n-ten Potenzen in $\mathbb{F}_p^\times$ und $E_n = \{b \in \mathbb{F}_p^\times : b^n = 1\}$ die Menge der n-ten Einheitswurzeln in $\mathbb{F}_p^\times$. Zeige:

iii. Die Abbildung $\varphi : \left\{ \begin{array}{ccc} \mathbb{F}_p^\times & \longrightarrow & \mathbb{F}_p^\times \\ b & \mapsto & b^n \end{array} \right.$ ist ein Gruppenendomorphismus mit $\ker\varphi = E_n$ und $\operatorname{im}\varphi = P_n$.

iv. E_n ist eine Untergruppe von $\mathbb{F}_p^\times$ der Ordnung n (Hinweis: $\mathbb{F}_p^\times$ ist zyklisch) und P_n ist eine Untergruppe von $\mathbb{F}_p^\times$ der Ordnung $\frac{p-1}{n}$.

v. *Gib einen Gruppenendomorphismus* ψ *von* $\mathbb{F}_p^\times$ *mit* $\ker \psi = P_n$ *und* $\operatorname{im} \psi = E_n$ *an (Begründung). Was ist* $\varphi \circ \psi$*?*

vi. *Sei* $g \in \mathbb{F}_p^\times$ *ein primitives Element, d.h. ein Erzeuger von* $\mathbb{F}_p^\times$*. Dann gilt* $P_n = < g^n >$*, die von* g^n *erzeugte Untergruppe von* $\mathbb{F}_p^\times$*. Wovon wird* E_n *erzeugt?*

vii. *Bestimme* P_n *und* E_n *und jeweils einen Erzeuger von* P_n *und* E_n *im Fall* $p = 17$ *für* $n = 1, 2, 4, 8, 16$.

Aufgabe 29 (Potenzen in $\mathbb{Z}_N$) *(6 Punkte)*

Für natürliche Zahlen $n, N \in \mathbb{N}$ *bezeichne* $\pi_n : \mathbb{Z}_N^\times \longrightarrow \mathbb{Z}_N^\times$ *die* n*-te Potenzabbildung mit* $\pi_n(a) = a^n$.

i. *Faktorisiere* N *und berechne* $T_N = \operatorname{im} \pi_{(N-1)/2}$ *für* $N = 561, 581, 631$ *und* 729.

ii. *Wieviele Urbilder haben* 1 *und* -1 *für die unter i. genannten Werte von* N*? Wie groß ist also die Wahrscheinlichkeit, daß für ein zufällig gewähltes* $a \in \mathbb{Z}_N^\times$ *gilt* $a^{(N-1)/2} \notin \{-1, 1\}$*? Kommentiere die Unterschiede.*

Für die Lösung darf ein Computeralgebrasystem verwendet werden.

Aufgabe 30 (Carmichael-Zahlen) *(7 Punkte)*

Eine Zahl $N \in \mathbb{N}$ *mit* $N > 1$ *heißt* Carmichael-Zahl, *falls sie keine Primzahl ist, aber trotzdem Fermats kleinen Satz erfüllt:* $a^{N-1} = 1$ *für alle* $a \in \mathbb{Z}_N^\times$*. Zeige:*

i. *Sei* $N = p_1^{e_1} \cdots p_r^{e_r}$ *die Primfaktorzerlegung einer Carmichael-Zahl* N*. Dann gilt* $e_i = 1$ *für* $1 \leq i \leq r$*, d.h. Carmichael-Zahlen sind quadratfrei. Hinweis: Konstruiere für jedes* i *mit* $e_i \geq 2$ *ein Element* $a_i \in \mathbb{Z}$ *mit* $\operatorname{ggT}(a_i, N) = 1$ *und* $a_i \equiv 1 + p_i \bmod p_i^2$.

ii. *Eine quadratfreie Nicht-Primzahl* N *ist genau dann eine Carmichael-Zahl, wenn für jeden Primteiler* p *von* N *gilt* $(p-1) \mid (N-1)$.

iii. *Eine Carmichael-Zahl ist ungerade und hat mindestens* 3 *verschiedene Primteiler.*

iv. *Welche der folgenden Zahlen sind Carmichael-Zahlen (Begründung):* 561, 663, 935, 1105, 1547, 1729, 2077, 2465, 2647, 2821, 172081, $10^{600} + 1$. *Computeralgebrasystem als Hilfe ist erlaubt.*

9. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Di, 30. 1. 1996 in der Vorlesung

Aufgabe 31 (Primtest) *(3 Punkte)*

Welche der beiden Zahlen $10^{200} + 349$ *und* $10^{200} + 357$ *sind wahrscheinlich prim und welche sicher nicht (Begründung)? Berechnungen dürfen mit einem Computeralgebrasystem durchgeführt werden, die Ergebnisse von „isprime" und „ifactor" (oder vergleichbaren eingebauten Routinen) reichen nicht aus. Miß die Laufzeiten Deiner Testläufe.*

Warnung: Nicht jede Exponentiationsroutine in einem Computeralgebrasystem ist zur Lösung dieser Aufgabe geeignet.

Aufgabe 32 (Pratt-Zertifikat) *(6 Punkte)*

Diese Aufgabe beruht auf dem Beweis von Pratt (1975), daß die Menge PRIMES $\subseteq \mathbb{N}$ *der Primzahlen in* $\mathcal{NP}$ *liegt. Sei* $N \in \mathbb{N}_{\geq 2}$. *Zeige:*

i. *Für* $a \in \mathbb{Z}_N$ *sind äquivalent:*

- $a \in \mathbb{Z}_N^\times$ *und* a *hat die multiplikative Ordnung* $N-1$,
- $a^{N-1} = 1$ *und* $a^{(N-1)/p} \neq 1$ *für alle Primteiler* p *von* $N-1$.

Ein solches a *heiße im Folgenden ein* Pratt-Zeuge *für* N.

ii. N *ist genau dann eine Primzahl, wenn es einen Pratt-Zeugen für* N *gibt.*

Sei nun N *prim. Ein* Pratt-Zertifikat Z *für die Primalität von* N *ist wie folgt rekursiv definiert:*

- $Z = (\mathbf{2}, \mathit{1})$ *falls* $N = 2$,
- $Z = (N, a; p_r, e_r, \ldots, p_1, e_1; Z_r, \ldots, Z_1)$ *falls* $N \geq 3$, *wobei folgendes gilt:*
  - a *ist ein Pratt-Zeuge für* N,
  - $p_1 < \cdots < p_r \in \mathbb{N}_{\geq 2}$ *sind Primzahlen,* $e_1, \ldots, e_r \in \mathbb{N}_{\geq 0}$ *und* $N - 1 = p_1^{e_1} \cdots p_r^{e_r}$ *ist die Primfaktorzerlegung von* $N-1$,
  - *für* $1 \leq i \leq r$ *ist* Z_i *ist ein Pratt-Zertifikat für* p_i.

Zum Beispiel sind

$$\Big(\mathbf{7}, \mathit{3}; 3, 1, 2, 1; (\mathbf{3}, \mathit{2}; 2, 1; (\mathbf{2}, \mathit{1})), (\mathbf{2}, \mathit{1})\Big),$$
$$\Big(\mathbf{7}, \mathit{5}; 3, 1, 2, 1; (\mathbf{3}, \mathit{2}; 2, 1; (\mathbf{2}, \mathit{1})), (\mathbf{2}, \mathit{1})\Big)$$

sämtliche Pratt-Zertifikate für die Primalität von 7.

iii. *Berechne je ein Pratt-Zertifikat für die Primzahlen* 19, 23 *und* 31*. Stelle die rekursive Struktur der Zertifikate in Baum-Form dar.*

iv. *(Bonusaufgabe)* *(2 Punkte)*
Zeige, daß jedes Pratt-Zertifikat für die Primalität von N polynomiale Länge in $\log N$ hat.

Aufgabe 33 (RSA) *(6 Punkte)*

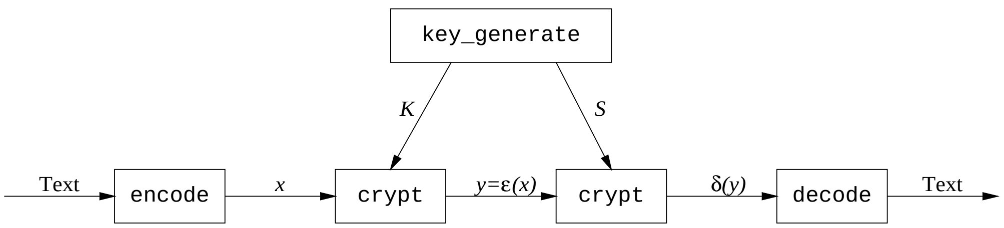
Für diese Aufgabe soll ein Computeralgebrasystem verwendet werden.

i. *Entwirf eine Prozedur* `key_generate`*, die ein Schlüsselpaar (K, S) für das RSA-Verfahren generiert. Dabei sollen $K = (N, e)$ der öffentliche Schlüssel, $S = (N, d)$ der private Schlüssel, $N \in \mathbb{N}$ das Produkt zweier zufällig gewählter Primzahlen mit je* 100 *Dezimalstellen, $e \in \{2, \ldots, \varphi(N)-1\}$ mit $\mathrm{ggT}(e, \varphi(N)) = 1$ zufällig gewählt und $d \in \{2, \ldots, \varphi(N) - 1\}$ mit $de \equiv 1 \bmod \varphi(N)$ sein.*

ii. *Überlege Dir eine Codierung für kurze englische Textstücke mit weniger als* 100 *Zeichen (incl. Satzzeichen, Klammern und Leerzeichen) als natürliche Zahlen im Bereich $0, \ldots, N-1$ und schreibe Prozeduren* `encode` *und* `decode` *für die Codierung und Decodierung.*

iii. *Entwirf eine Prozedur* `crypt` *zum Ver- und Entschlüsseln mit dem RSA-Verfahren, deren Argumente ein Schlüssel und eine zu ver- bzw. entschlüsselnde Nachricht (in der entsprechenden Codierung) sind. Was passiert, wenn die codierte Nachricht nicht teilerfremd zu N ist? Kann man diesen Fall vermeiden, und wenn ja, wie? Wie „wahrscheinlich" ist es, daß so etwas überhaupt eintritt?*

iv. *Berechne mit Deinen Prozeduren ein Schlüsselpaar (K, S), die Codierung $x \in \{0, \ldots, N - 1\}$ der ersten Textzeile des „Computeralgebra I"-Skripts, den mit K verschlüsselten Chiffretext $y = \epsilon(x) \in \{0, \ldots, N - 1\}$, den mit S entschlüsselten Klartext $\delta(y) \in \{0, \ldots, N - 1\}$, und decodiere $\delta(y)$ anschließend. Miß jeweils die Laufzeiten Deiner Prozeduren.*



v. *(Bonusaufgabe)* *(2 Punkte)*
Zeige, daß ein Eindringling, der außer dem öffentlichen Schlüssel noch $\varphi(N)$ kennt, die Zahl N schnell faktorisieren und damit das Kryptosystem knacken kann.

10. Übungsblatt zu Computeralgebra I, WS 1995/96

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Do, 8. 2. 1996 in der Vorlesung

Aufgabe 34 (Quadratfreie Faktorisierung) *(3 Punkte)*

Sei $f \in \mathbb{F}_2[x]$ ein Polynom, dessen Zerlegung in irreduzible Faktoren durch $f = ab^2c^2d^6e^8$ gegeben ist. Dabei sind $a, b, c, d, e \in \mathbb{F}_2[x]$ paarweise verschiedene nichtkonstante irreduzible Polynome. Führe die Berechnung des quadratfreien Teils von f auf symbolischer Ebene mit dem Algorithmus aus der Vorlesung durch.

Aufgabe 35 (Verschiedengradige Faktorisierung) *(3 Punkte)*

Berechne die verschiedengradige Faktorisierung des quadratfreien Polynoms

$$f = x^{19} - x^{18} - x^{17} + x^{15} - x^{14} + x^{12} + x^9 - x^8 - x^7 + x^6 - x^4 - x^3 + x^2 + 1 \in \mathbb{F}_3[x]$$

mit dem Algorithmus aus der Vorlesung. Wieviele irreduzible Faktoren vom Grad i hat f für $1 \leq i \leq 19$? Für die Berechnung darf ein Computeralgebrasystem verwendet werden.

Aufgabe 36 (Gleichgradige Faktorisierung) *(3 Punkte)*

Das Polynom

$$\begin{aligned} f \;=\; & x^{18} - 7\,x^{17} + 4\,x^{16} + 2\,x^{15} - x^{13} - 7\,x^{12} + 4\,x^{11} + 7\,x^{10} + 4\,x^9 \\ & -3\,x^8 - 3\,x^7 + 7\,x^6 - 7\,x^5 + 7\,x^4 + 7\,x^3 - 3\,x^2 + 5\,x + 5 \in \mathbb{F}_{17}[x] \end{aligned}$$

zerfällt in 3 irreduzible Faktoren vom Grad 6. Berechne diese mit dem Algorithmus von Cantor und Zassenhaus! Für die Berechnung darf ein Computeralgebrasystem verwendet werden.

Aufgabe 37 (Irreduzibilitätstest) *(2 Punkte)*

Seien $q \in \mathbb{N}$ eine Primpotenz und $\mathbb{F}_q$ ein endlicher Körper mit q Elementen. Zeige: Ein Polynom $f \in \mathbb{F}_q[x]$ vom Grad n ist genau dann irreduzibel, wenn $f \mid (x^{q^n} - x)$ gilt und $\mathrm{ggT}(x^{q^{n/t}} - x, f) = 1$ ist für jeden Primteiler t von n.

Klausur zu Computeralgebra I, Wintersemester 1995/96

15. 2. 1996, 14.00 bis 16.00

<u>Zulässige Hilfsmittel:</u>

- Vorlesungsskript (wie angegeben),
- Taschenrechner,
- Zwei Blätter (vier Seiten) handgeschriebene Notizen; keine Kopien!

Gesamtpunktzahl: 36 Punkte + 8 Bonuspunkte
Alle Antworten sind zu begründen!

Aufgabe 1 (Quadratfreier Teil) *(4 Punkte)*
Beweise oder widerlege:

i. *Das Polynom $x^{1000} + 2 \in \mathbb{F}_5[x]$ ist quadratfrei.*

ii. *Seien F ein Körper und $f, g \in F[x]$ nichtkonstante Polynome. Dann gilt: Der quadratfreie Teil von fg ist das Produkt der quadratfreien Teile von f und von g.*

Aufgabe 2 (FFT 3-adisch) *(8 Punkte)*
Sei R ein Ring, der zu jedem $k \in \mathbb{N}$ eine primitive 3^k-te Einheitswurzel enthält.

i. *Entwirf einen rekursiven FFT-Algorithmus, der als Eingabe $k \in \mathbb{N}$, ein Polynom $f \in R[x]$ vom Grad kleiner als $n = 3^k$ und eine Liste der Potenzen $1, \omega, \omega^2, \ldots, \omega^{n-1}$ einer primitiven n-ten Einheitswurzel $\omega \in R$ nimmt und $f(1), f(\omega), f(\omega^2), \ldots, f(\omega^{n-1})$ berechnet. Beweise die Korrektheit Deines Algorithmus.*

ii. *Seien $T(n)$ die Kosten Deines Algorithmus, gemessen in R-Operationen, bei Eingabegröße $n = 3^k$ für $k \in \mathbb{N}$. Stelle eine Rekursionsgleichung für $T(n)$ auf (Anfangsbedingung nicht vergessen) und bestimme deren Lösung im O-Kalkül.*

Aufgabe 3 (Quadratwurzeln) *(12 Punkte)*

Seien $n \in \mathbb{N}$ *ungerade,* $n = p_1^{e_1} \cdots p_r^{e_r}$ *seine Primfaktorzerlegung mit* $e_1, \ldots, e_r > 0$ *und* $a \in \mathbb{N}$ *mit* $\operatorname{ggT}(a, n) = 1$.

i. *Welche Bedingung, die nur von* a *und* $p_1, \ldots, p_r$*, aber nicht von* $e_1, \ldots, e_r$ *abhängt, ist notwendig und hinreichend dafür, daß* a *eine Quadratwurzel modulo* n *hat?*

ii. *Welche der Zahlen*

$$10001, 42814, 31027, 17329$$

haben eine Quadratwurzel modulo 50625*?*

iii. *Wieviele Quadratwurzeln modulo* 50625 *hat* 1*? Berechne alle.*

Aufgabe 4 (Interpolation) *(12 Punkte)*

Seien $p_1, p_2 \in \mathbb{N}$ *unterschiedliche Primzahlen,* $m = p_1p_2$, $n \in \mathbb{N}$ *und* $u_0, \ldots, u_{n-1}, \gamma_0, \ldots, \gamma_{n-1} \in \mathbb{Z}$. *Zeige:*

i. *Ein Interpolationspolynom* $f \in \mathbb{Z}[x]$ *mit*

$$\begin{array}{c} f \textit{ hat Koeffizienten in } \{0, \ldots, m-1\},\ \deg f < n \textit{ und} \\ f(u_i) \equiv \gamma_i \bmod m \textit{ für } 0 \leq i < n \end{array} \tag{1}$$

existiert genau dann, wenn

$$u_i \equiv u_j \bmod p_k \Longrightarrow \gamma_i \equiv \gamma_j \bmod p_k$$

für alle $0 \leq i < j < n$ *und* $k = 1, 2$ *gilt.*

ii. *Die Lösung der Interpolationsaufgabe (1) ist genau dann eindeutig, wenn*

$$u_i \not\equiv u_j \bmod p_k$$

für alle $0 \leq i < j < n$ *und* $k = 1, 2$ *gilt.*

iii. *Berechne alle Interpolationspolynome* $f \in \mathbb{Z}[x]$ *mit Koeffizienten in* $\{0, \ldots, 14\}$, $\deg f < 3$ *und*

$$f(1) \equiv 2 \bmod 15,\ f(2) \equiv 5 \bmod 15,\ f(4) \equiv -1 \bmod 15.$$

Aufgabe 5 (Bonusaufgabe) *(8 Punkte)*

Seien $f, g \in \mathbb{Z}[x]$, $r = \operatorname{res}(f, g) \in \mathbb{Z} \setminus \{0\}$ *und* $u \in \mathbb{Z}$. *Dann ist* $\operatorname{ggT}(f(u), g(u))$ *ein Teiler von* r.

Viel Erfolg!

Lösungsvorschlag Klausur CA I, WS 1995/96

Aufgabe 1

i. *Sei* $f = x^{1000} + 2 \in \mathbb{F}_5[x]$. *Dann ist* $f' = 0$ *und* $\mathrm{ggT}(f, f') = f \neq 1$, *also* f *nicht quadratfrei. Genauer: aus* $f' = 0$ *folgt, daß* f *eine 5-te Potenz ist, nämlich*

$$f = (x^{200} + 2)^5 = (x^8 + 2)^{5^3}.$$

ii. *Die Behauptung ist falsch. Gegenbeispiel:* $f = g = x$. *Dann ist* x *der quadratfreie Teil von* f *und von* g *und von* fg, *aber das Produkt der quadratfreien Teile von* f *und von* g *ist* x^2. *Die richtige Aussage in diesem Zusammenhang lautet: Wenn* $\overline{f}$ *den quadratfreien Teil von* f *bezeichnet, analog* $\overline{g}$, $\overline{fg}$, *dann gilt*

$$\overline{fg} = \mathrm{kgV}(\overline{f}, \overline{g}).$$

Aufgabe 2

i. **Algorithmus** FFT.
Eingabe: $k \in \mathbb{N}$, $f \in R[x]$ *mit* $\deg f < n = 3^k$, *und die Potenzen* $1, \omega, \omega^2, \ldots, \omega^{n-1}$ *einer* n*-PEW* $\omega \in R$.
Ausgabe: $f(1), f(\omega), f(\omega^2), \ldots, f(\omega^{n-1}) \in R$.

1. *Falls* $k = 0$, *gib* f *zurück.*
2. *Schreibe* $f = f_0(x^3) + x \cdot f_1(x^3) + x^2 \cdot f_2(x^3)$ *mit* $f_0, f_1, f_2 \in R[x]$ *vom Grad kleiner als* $\frac{n}{3}$.
3. *Berechne rekursiv*

$$\begin{aligned} (\alpha_i)_{0 \le i < n/3} &= \mathrm{FFT}(k-1, f_0, 1, \omega^3, \omega^6, \ldots, \omega^{n-3}), \\ (\beta_i)_{0 \le i < n/3} &= \mathrm{FFT}(k-1, f_1, 1, \omega^3, \omega^6, \ldots, \omega^{n-3}), \\ (\gamma_i)_{0 \le i < n/3} &= \mathrm{FFT}(k-1, f_2, 1, \omega^3, \omega^6, \ldots, \omega^{n-3}). \end{aligned}$$

4. *Für* $0 \le i < \frac{n}{3}$ *setze*

$$\begin{aligned} \delta_i &= \alpha_i + \omega^i \beta_i + \omega^{2i} \gamma_i, \\ \delta_{i+n/3} &= \alpha_i + \omega^{i+n/3} \beta_i + \omega^{2(i+n/3)} \gamma_i, \\ \delta_{i+2n/3} &= \alpha_i + \omega^{i+2n/3} \beta_i + \omega^{2(i+2n/3)} \gamma_i. \end{aligned}$$

5. *Gib* $\gamma_0, \ldots, \gamma_{n-1}$ *zurück.*

Korrektheit: *Beweis per Induktion über* k. *Für* $k = 0$ *ist* f *konstant und* $f(1) = f$. *Sei nun* $k > 0$. *Nach Schritt 3. gilt mit der Induktionshypothese*

$$\alpha_i = f_0(\omega^{3i}),\ \beta_i = f_1(\omega^{3i}),\ \gamma_i = f_2(\omega^{3i})$$

für $0 \leq i < \frac{n}{3}$, *denn* ω^3 *ist eine* $\frac{n}{3} - PEW$. *Wegen* $\omega^n = 1$ *gilt auch* $\alpha_i = f_0(\omega^{3(i+n/3)}) = f_0(\omega^{3(i+2n/3)})$ *für* $0 \leq i < \frac{n}{3}$, *analog für die* β_i *und* γ_i. *Also ist*

$$\delta_i = f_0(\omega^{3i}) + \omega^i f_1(\omega^{3i}) + \omega^{2i} f_2(\omega^{3i}) = f(\omega^i)$$

für $0 \leq i < n$.

ii. *Schritte 1, 2 und 5 sind kostenlos. Die Kosten für Schritt 3 und 4 betragen* $3T(\frac{n}{3})$ *bzw.* $4n$ *Operationen in* R. *Daraus ergibt sich die Rekursionsgleichung*

$$\begin{aligned} T(1) &= 0, \\ T(n) &= 3T(\frac{n}{3}) + 4n \text{ für } n = 3^k,\ k \geq 1 \end{aligned}$$

für die Kosten, welche die Lösung $T(n) = 4n \log_3 n \in O(n \log n)$ *hat.*

Aufgabe 3

i. *a hat genau dann eine Quadratwurzel modulo n, wenn a modulo jedem Primteiler* p_i *von* n *für* $1 \leq i \leq r$ *eine Quadratwurzel hat. Beweis:*

"$\Rightarrow$" *Aus* $b^2 \equiv a \bmod n$ *folgt natürlich* $b^2 \equiv a \bmod p_i$ *für alle* i.

"$\Leftarrow$" *Seien* $b_1, \ldots, b_r \in \mathbb{Z}$ *mit* $b_i^2 \equiv a \bmod p_i$. *Wegen* $\mathrm{ggT}(a, n) = 1$ *gilt* $a_i \not\equiv 0 \bmod p_i$ *und damit auch* $b_i \not\equiv 0 \bmod p_i$. *Mit* $f = x^2 - a \in \mathbb{Z}[x]$ *gilt* $f'(b_i) = 2b_i \not\equiv 0 \bmod b_i$, *und das Newtonverfahren liefert* $c_i \in \mathbb{Z}$ *mit* $c_i \equiv b_i \bmod p_i$ *und* $c_i^2 \equiv a_i \bmod p_i^{e_i}$ *für alle* i. *Aus den* c_i *kann mit dem CRA ein* $c \in \mathbb{Z}$ *mit* $c \equiv c_i \bmod p_i^{e_i}$ *für* $1 \leq i \leq r$ *konstruiert werden, und dieses* c *ist eine Quadratwurzel von* a *modulo* n.

ii. *Es gilt* $50625 = 3^4 \cdot 5^4$ *und*

$$\begin{aligned} 10001 &\equiv 2 \bmod 3, & 10001 &\equiv 1 \bmod 5, \\ 42814 &\equiv 1 \bmod 3, & 42814 &\equiv 4 \bmod 5, \\ 31027 &\equiv 1 \bmod 3, & 31027 &\equiv 2 \bmod 5, \\ 17329 &\equiv 1 \bmod 3, & 17329 &\equiv 4 \bmod 5. \end{aligned}$$

Da 2 *keine Quadratwurzel modulo* 3 *und modulo* 5 *hat, folgt mit i., daß nur* 42814 *und* 17329 *eine Quadratwurzel modulo* 50625 *haben.*

iii. *Wegen der Eindeutigkeit des Newtonverfahrens hat* 1 *modulo* $3^4 = 81$ *genauso viele Quadratwurzeln wie modulo* 3 *und modulo* $5^4 = 625$ *genauso viele wie modulo* 5. *Deshalb sind* $1, -1$ *alle Quadratwurzeln von* 1 *modulo* 81 *und modulo* 625. *Mit dem Chinesischen Restsatz ergeben sich daraus genau vier Quadratwurzeln* $c \in \mathbb{Z}$ *von* 1 *modulo* 50625, *nämlich durch* $c \equiv \pm 1 \bmod 81$ *und* $c \equiv \pm 1 \bmod 625$. *Die beiden offensichtlichen Lösungen sind* 1 *und* -1, *wenn in beiden Kongruenzen dasselbe Vorzeichen gewählt wird. Die restlichen Lösungen liefert der CRA. Dazu bestimmt* *man zunächst* $s, t \in \mathbb{Z}$ *mit* $s \cdot 81 + t \cdot 625 = 1$ *mit dem EEA. Es ergibt sich* $s = -54$ *und* $t = 7$*. Die Lösung der Kongruenzen* $c \equiv 1 \bmod 81$ *und* $c \equiv -1 \bmod 625$ *lautet dann*

$$c = 1 \cdot 7 \cdot 625 + (-1) \cdot (-54) \cdot 81 = 8749,$$

und die vierte Quadratwurzel von 1 *modulo* 50625 *ist* -8749*.*

Aufgabe 4

i. *Nach dem Chinesischen Restsatz gibt es genau dann ein Interpolationspolynom mit (1), wenn modulo* p_1 *und modulo* p_2 *ein Interpolationspolynom existiert. Sei nun* $k \in \{1, 2\}$ *fest. Wenn es Indices* $i \neq j$ *gibt mit* $u_i \equiv u_j \bmod p_k$ *und* $\gamma_i \not\equiv \gamma_j \bmod p_k$*, dann existiert kein Interpolationspolynom modulo* p_k*, da ein solches keine zwei verschiedenen Werte an einer Stelle annehmen kann.*

   Ist umgekehrt die Bedingung von Teilaufgabe i. erfüllt, dann entferne man alle modulo p_k *doppelten Paare* (u_i, γ_i)*. Für die übriggebliebenen Paare (das sind höchstens* n *Stück) sind dann alle verbleibenden Interpolationspunkte modulo* p_k *verschieden, und z.B. die Lagrange-Formel liefert ein Interpolationspolynom modulo* p_k *vom Grad kleiner als* n*.*

ii. *Wiederum nach dem Chinesischen Restsatz ist das Interpolationspolynom modulo* m *genau dann eindeutig, wenn es modulo* p_1 *und modulo* p_2 *eindeutig ist. Seien* $k \in \{1, 2\}$ *fest und* $f \in \mathbb{Z}[x]$ *mit* $\deg f < n$ *ein Interpolationspolynom modulo* p_k*. Wenn es Indices* $i \neq j$ *mit* $u_i \equiv u_j \bmod p_k$ *gibt, dann ist das Polynom*

$$f + \prod_{0 \leq l < n,\, l \neq i} (x - u_l) \in \mathbb{Z}[x]$$

   modulo p_k *verschieden von* f*, hat Grad kleiner als* n *und ist ebenfalls ein Interpolationspolynom modulo* p_k*.*

   Sei nun die Bedingung von Teilaufgabe ii. erfüllt und g *ein weiteres Interpolationspolynom modulo* p_k *vom Grad kleiner als* n*. Dann hat das Polynom* $f - g$ *die* n *modulo* p_k *verschiedenen Punkte* $u_0, \ldots, u_{n-1}$ *als Nullstellen und ist mithin das Nullpolynom modulo* p_k*.*

iii. *Das Interpolationsproblem modulo* 3 *reduziert sich auf*

$$f(1) \equiv 2 \bmod 3, \;\; f(2) \bmod 2 \bmod 3,$$

   und die offensichtliche gradminimale Lösung ist $f = 2$*. Die Menge* aller *Interpolationspolynome hat die Form* $\{2 + g(x-1)(x-2) : g \in \mathbb{F}_3[x]\}$*. Es gibt also genau drei Interpolationspolynome modulo* 3 *vom Grad kleiner als* 3*, nämlich*

$$\begin{aligned}
f_0 &\equiv 2 + 0 \cdot (x-1)(x-2) \equiv 2 \bmod 3, \\
f_1 &\equiv 2 + 1 \cdot (x-1)(x-2) \equiv 2 + (x^2 + 2) \equiv x^2 + 1 \bmod 3, \\
f_2 &\equiv 2 + 2 \cdot (x-1)(x-2) \equiv 2 + 2(x^2 + 2) \equiv 2x^2 \bmod 3.
\end{aligned}$$

Das Interpolationsproblem modulo 5 *ist*

$$f(1) \equiv 2 \bmod 5,\ f(2) \equiv 0 \bmod 5,\ f(4) \equiv 4 \bmod 5.$$

Es gibt also genau ein Interpolationspolynom modulo 5 *vom Grad kleiner als* 3*. Die Langrange-Formel etwa liefert*

$$\begin{aligned} f &\equiv 2 \cdot \frac{(x-2)(x-4)}{(1-2)(1-4)} + 0 \cdot \frac{(x-1)(x-4)}{(2-1)(2-4)} + 4 \cdot \frac{(x-1)(x-2)}{(4-1)(4-2)} \\ &\equiv 4(x^2+4x+3) + 4(x^2+2x+2) \equiv 3x^2+4x \bmod 5. \end{aligned}$$

Also gibt es genau 3 *Interpolationspolynome modulo* 15 *vom Grad kleiner als* 3*, die durch das Kongruenzensystem*

$$f \equiv f_i \bmod 3,\ f \equiv 3x^2+4x \bmod 5$$

für $i = 0,1,2$ *bestimmt sind. Die Lösungen liefert der CRA. Zunächst erhält man durch Probieren (oder systematisch mit dem EEA)* $s,t \in \mathbb{Z}$ *mit* $s \cdot 3 + t \cdot 5 = 1$*, z.B.* $s = 2$ *und* $t = -1$*. Danach kann man entweder das Kongruenzensystem koeffizientenweise und für* $i = 0,1,2$ *lösen, oder "simultan" wie folgt:*

$$\begin{aligned} f &\equiv f_i \cdot (-1) \cdot 5 + (3x^2+4x) \cdot 2 \cdot 3 \\ &\equiv (2 + i(x^2+2)) \cdot 10 + (3x^2+4x) \cdot 6 \\ &\equiv (3+10i)x^2 + 9x + (5+5i) \bmod 15 \end{aligned}$$

für $i = 0,1,2$*, und die drei modulo* 15 *verschiedenen Lösungen vom Grad kleiner als* 3 *sind*

$$3x^2+9x+5,\ 13x^2+9x+10,\ 8x^2+9x.$$

Aufgabe 5 *Wir zeigen zunächst, daß sich* r *als Linearkombination von* f *und* g *mit Polynomen aus* $\mathbb{Z}[x]$ *schreiben läßt. Wegen* $r \neq 0$ *sind* f *und* g *über* $\mathbb{Q}$ *teilerfremd. Also gibt es Polynome* $s,t \in \mathbb{Q}[x]$ *mit* $\deg s < \deg g = m$*,* $\deg t < \deg f = n$ *und* $sf + tg = 1$ *in* $\mathbb{Q}[x]$*. Schreibt man diese Polynomgleichung als lineares Gleichungssystem über* $\mathbb{Q}$ *in den Koeffizienten von* s *und* t*, so ist die zugehörige Koeffizientenmatrix* $P \in \mathbb{Q}^{(n+m)\times(n+m)}$ *gerade die Sylvestermatrix von* f *und* g*, und die "rechte Seite"* $v \in \mathbb{Q}^{n+m}$ *der* $(n+m)$*-te Einheitsvektor. Wegen* $\det P = \operatorname{res}(f,g) \neq 0$ *ist das Gleichungssystem eindeutig lösbar, und nach der Cramer'schen Regel läßt sich jeder Koeffizient von* s *und von* t *als Quotient zweier Determinanten schreiben:* $\det P = r$ *im Nenner und die Determinante der Matrix, die aus* P *durch Ersetzen einer passenden Spalte durch den Vektor* v *entsteht, im Zähler. Also sind* $\overline{s} = rs$ *und* $\overline{t} = rt$ *Polynome mit Koeffizienten in* $\mathbb{Z}$*, und es gilt* $\overline{s}f + \overline{t}g = r$ *in* $\mathbb{Z}[x]$*.*

Nach Einsetzen von $u \in \mathbb{Z}$ *erhalten wir* $\overline{s}(u)f(u) + \overline{t}(u)g(u) = r$ *in* $\mathbb{Z}$*, und nachdem* $\operatorname{ggT}(f(u), g(u))$ *die linke Seite dieser Gleichung teilt, folgt die Behauptung.*