Universität Dortmund
Fachbereich Mathematik
Prof. Dr. H. M. Möller
Dipl.-Math. C. Scholz

Dortmund, 2.11.2004

Symbolisches Rechnen

4. Übung

Aufgabe 12 Finden Sie das kleinste positive $x \in \mathbb{Z}$ mit

(i) $\phi_8(x) = 5$, $\phi_5(x) = 2$, $\phi_3(x) = 0$,

(ii) $\phi_{11}(x) = 10$, $\phi_7(x) = 0$, $\phi_5(x) = 3$, $\phi_3(x) = 1$,

jeweils mit dem Ansatz von Newton bzw. Lagrange.

Aufgabe 13

(i) Berechnen Sie das Inverse von 222 in $\mathbb{Z}_{32003}$.

(ii) Beim Rechnen modulo $p = x^3 - 2$ in $\mathbb{Q}[x]$ arbeitet man mit Polynomen der Form $a_2x^2 + a_1x + a_0$, mit $a_0, a_1, a_2 \in \mathbb{Q}$. Tritt an die Stelle von x die Nullstelle $\alpha = \sqrt[3]{2}$, so erhält man statt der Polynome Ausdrücke der Form $a_2\sqrt[3]{4} + a_1\sqrt[3]{2} + a_0$. Berechnen Sie das Inverse von $\sqrt[3]{4} + 1$ als Ausdruck in obiger Form.

Aufgabe 14 Seien $m, c, N \in \mathbb{N}$ mit $N \leq m$ und $\mathrm{ggT}(m, c) = 1$. Gesucht sind rationale Zahlen $\frac{p}{q}$ mit $0 \leq p, q \leq N$ und

$$\phi_m(p - cq) = 0.$$

Dazu bestimmt man mit Hilfe des erweiterten Euklidischen Algorithmus zunächst $\tilde{q} = \frac{1}{c} \bmod m$ und bildet anschließend die Brüche $\frac{k}{k\cdot\tilde{q} \bmod m}$ für $1 \leq k \leq N$.

(i) Zeigen Sie, dass man auf diese Weise alle Brüche $\frac{\tilde{p}}{\tilde{q}}$ mit $1 \leq \tilde{p} \leq N$ erhält, welche die obige Gleichung erfüllen.

(ii) Bestimmen Sie p und q mit $1 \leq p, q \leq 10$ und

$$\phi_{13}(p - 5q) = 0,\ \ \phi_{17}(p - 6q) = 0,\ \ \phi_{19}(p - 16q) = 0.$$

Aufgabe 15 Bestimmen Sie die Menge der $f \in \mathbb{Q}[x]$, für die gilt

$$f = x + 1 \bmod x^2 - 2 \ \text{ und}$$
$$f = x^2 - 1 \bmod x^3 + 3.$$

Abgabe: Donnerstag, den 11.11.2004 bis 12.15 Uhr in den Briefkästen im Mathematikgebäude.