Universität Hamburg
Fachbereich Mathematik

Winter 2016/17
Janko Latschev

Grundlagen der Mathematik

Übungsblatt 11

Präsenzaufgaben

(P20) Größter gemeinsamer Teiler

Bestimmen Sie jeweils den größten gemeinsamen Teiler der angegebenen Zahlen. Überlegen Sie vorher, ob die Bestimmung der Primfaktorzerlegung oder der euklidische Algorithmus effizienter sein wird:

a) 63 und 91

b) 5133 und 2146

(P21) Polynomdivision in $\mathbb{Q}[x]$

Polynomdivision mit Rest von Polynomen mit *rationalen* Koeffizienten funktioniert praktisch analog zur schriftlichen Division mit Rest natürlicher Zahlen, wobei die Potenzen der Variablen x die Rolle der "Stellen" eines Stellenwertsystems übernehmen. Bei den Koeffizienten führen wir jeweils eine gewöhnliche Division durch. Quotient und Rest sind eindeutig, wenn man verlangt, dass der Rest strikt kleineren Grad hat als der Divisor.

Beispiel:

$$\begin{array}{l}
(2x^2 + 5x + 1) : (3x) = \frac{2}{3}x + \frac{5}{3} \text{ Rest } 1 \\
\underline{2x^2} \\
\quad 0 + 5x \\
\quad \underline{5x} \\
\qquad\quad 0 + 1
\end{array}$$

Führen Sie die Division mit Rest für folgende Polynome durch:

a) $(3x^2 + 14x + 2) : (5x + 2)$

b) $(18x^4 + 12x^2 + 5x + 9) : (3x^2 + 3x + 8)$

Bitte wenden!

Übungsaufgaben mit Abgabetermin Mo, 16.01.17, zu Beginn der Vorlesung

(A29) Euklidischer Algorithmus mit Polynomen **(3+2 Punkte)**

Den euklidischen Algorithmus kann man in jedem Ring durchführen, in dem die Division mit Rest erklärt ist, also auch in $\mathbb{Q}[x]$. Auf diese Weise kann man dann auch einen größten gemeinsamen Teiler zweier Polynome bestimmen, wobei das Attribut *größter* im Sinne von "größtmöglicher Grad" zu verstehen ist. Ein solcher größter gemeinsamer Teiler ist dann allerdings nur bis auf Multiplikation mit einer von Null verschiedenen rationalen Zahl bestimmt, d.h. es gibt viele größte gemeinsame Teiler.

a) Bestimmen Sie einen größten gemeinsamen Teiler $g(x)$ der beiden Polynome

$$p_1(x) = 3x^5 + 8x^4 + 11x^3 + 14x^2 \quad \text{und} \quad p_2(x) = 3x^3 + 5x^2 + 9x + 7.$$

b) Finden Sie Polynome $a(x)$ und $b(x)$ mit rationalen Koeffizienten, so dass (für Ihr $g(x)$ aus Teil **a)**) die Gleichung

$$g(x) = a(x)p_1(x) + b(x)p_2(x)$$

erfüllt ist.

(A30) Das kleinste gemeinsame Vielfache **(2+2+1 Punkte)**

Analog zum größten gemeinsamen Teiler definiert man das *kleinste gemeinsame Vielfache* zweier **natürlicher** Zahlen x und y als die kleinste natürliche Zahl k mit $x|k$ und $y|k$. Es wird oft mit $\mathrm{kgV}(x, y)$ bezeichnet.

a) Zeigen Sie: Sind

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{und} \quad y = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

die Primfaktorzerlegungen von x und y, so gilt[1]

$$\mathrm{kgV}(x, y) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}.$$

b) Zeigen Sie, dass für beliebige natürliche Zahlen x und y die Beziehung

$$\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) = x \cdot y$$

gilt.

c) Bestimmen Sie $\mathrm{kgV}(5133, 2146)$.

[1] Für beliebige ganze (oder auch reelle) Zahlen a, b gilt $\max(a, b) = \begin{cases} a & \text{falls } a \geq b \\ b & \text{sonst} \end{cases}$.

Siehe nächstes Blatt!

(A31) Rechnen in $\mathbb{Z}_p$ **(1+2+1+1+1+2+2 Punkte)**

Sei p eine Primzahl. In dieser Aufgabe untersuchen wir die Gleichung

$$x^{p-1} = 1 \tag{1}$$

im Ring $\mathbb{Z}_p$ der Restklassen modulo p.
Sei $a \in \mathbb{Z}$ teilerfremd zu p.

a) Zeigen Sie, dass die Elemente $[a]$, $[2a]$, $\ldots [(p-1)a]$ in $\mathbb{Z}_p$ von Null verschieden sind.
Hinweis: Was sagt das Lemma von Euklid?

b) Folgern Sie daraus, dass diese Elemente auch paarweise verschieden sind.

c) Folgern Sie daraus die Kongruenz

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p.$$

d) Folgern Sie daraus die Kongruenz

$$a^{p-1} \equiv 1 \mod p.$$

e) Wieviele Lösungen hat die Gleichung (1) in $\mathbb{Z}_p$?

f) Bestimmen Sie für die natürlichen Zahlen $a \in \{1, 2, 3, 4, 5, 6\}$ jeweils den *kleinsten* Exponenten $k \in \mathbb{N}$ mit $a^k \equiv 1 \mod 7$.

g) Beweisen Sie: Ist p eine Primzahl und a eine natürliche Zahl und ist $k \in \mathbb{N}$ die kleinste natürliche Zahl mit

$$a^k \equiv 1 \mod p,$$

dann teilt k die Zahl $p-1$.

(A32) Noch ein größter gemeinsamer Teiler **(2 BONUS-Punkte)**

Bestimmen Sie den größten gemeinsamen Teiler der Zahlen a und b, wobei die Deziamldarstellung von a eine Folge von 100 Dreien und die Dezimaldarstellung von b eine Folge von 60 Dreien ist. Der Lösungsweg muss klar erkennbar sein.