18. Vorlesung 23.11.2020

Notiztitel 23.11.2020

Bemerkungen zur 3. Übung

zur 6. Aufgabe Finden Sie Binome bzw. berechnen Sie mit geeigneten Binomen

(a5) 99^2

$$99^2 = (100-1)^2 = 100^2 - 2\cdot 1\cdot 100 + 1^2 = 10\,000 - 200 + 1 = 9801$$

$$(a-b)^2 = a^2 - 2ab + b^2$$

zur 1. Aufgabe: c) $\sum_{i=0}^{10} \binom{10}{i}$

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} \cdot b^i$$

$a=1, b=1, n=10$

$$\sum_{i=0}^{10} \binom{10}{i} = \sum_{i=0}^{10} \binom{10}{i} \cdot 1 \cdot 1 = \sum_{i=0}^{10} \binom{10}{i} \cdot 1^{10-i} \cdot 1^i$$

$$= (\underset{a}{1} + \underset{b}{1})^{10} = 2^{10} = 1024$$

siehe z.B. 8. Vorlesung

d) $(a-b)^n = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} a^{n-k} b^k$

$a=1$, $b=1$

$$\sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} 1^{n-k} \cdot 1^k$$

$$= (1-1)^n = 0^n = 0$$

a) $\sum_{n=4}^{7} \binom{n}{n-2} = \binom{4}{2} + \binom{5}{3} + \binom{6}{4} + \binom{7}{5}$ „stures" Einsetzen dann ausrechnen

2. Variante Symmetrie von Binomialkoeffizienten:

$$\binom{n}{k} = \binom{n}{n-k} \text{ also } \binom{n}{n-2} = \binom{n}{n-(n-2)} = \binom{n}{2}$$

$$\sum_{n=4}^{7} \binom{n}{n-2} = \sum_{n=4}^{7} \binom{n}{2} = \binom{4}{2} + \binom{5}{2} + \binom{6}{2} + \binom{7}{2}$$

$$= \frac{4\cdot 3}{1\cdot 2} + \frac{5\cdot 4}{1\cdot 2} + \frac{6\cdot 5}{1\cdot 2} + \frac{7\cdot 6}{1\cdot 2}$$

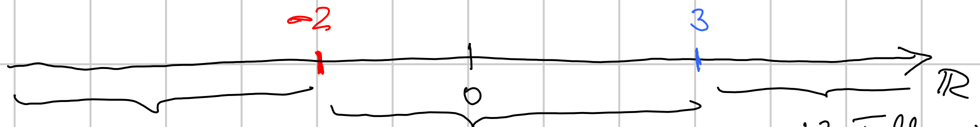
$$= 6 + 10 + 15 + 21 = 52$$

zu Aufgabe 4d: $|x+2| = |x-3|$

Welche Fälle muss man bei der Fallunterscheidung betrachten!

Vorzeichenwechsel bei -2 Vorzeichenwechsel bei $+3$

$\mathbb{R} = (-\infty, -2) \cup [-2, 3) \cup [3, +\infty)$



1. Fall: $x < -2$

d.h. $x \in (-\infty, -2)$

$x < -2 \Rightarrow x+2 < 0 \wedge x-3 < 0$

$|x+2| = |x-3|$ auflösen der Beträge

$-(x+2) = -(x-3)$

$-x-2 = -x+3 \quad | +x+2$

$0 = 5$ ↯

$\mathbb{L}_1 = \emptyset$

2. Fall: $-2 \leq x < 3$

d.h. $x \in [-2, 3)$ ✓

$x+2 \geq 0 \wedge x-3 < 0$

$|x+2| = |x-3|$

$x+2 = -(x-3)$

$x+2 = -x+3 \quad | +x-2$

$2x = 1$

$x = \frac{1}{2} \in [-2, 3)$ ✓

$\mathbb{L}_2 = \left\{ \frac{1}{2} \right\}$

3. Fall: $x \geq 3$

d.h. $x \in [3, +\infty)$

$x+2 \geq 0 \wedge x-3 \geq 0$

$|x+2| = |x-3|$

$x+2 = x-3 \quad | -x-2$

$0 = -5$ ↯

$\mathbb{L}_3 = \emptyset$

insgesamt: $\mathbb{L} = \mathbb{L}_1 \cup \mathbb{L}_2 \cup \mathbb{L}_3 = \left\{ \frac{1}{2} \right\}$

zu Aufgabe 3: Berechnung von Quadratzahlen natürlicher Zahlen, wenn die letzte Ziffer eine 5 ist!

$\underbrace{156}_{n\cdot(n+1)} \cdot 100 + 25$

$125^2 = 15625$

$\underline{12}5 \to n = 12, \; n\cdot(n+1) = 12\cdot 13$

$12 \cdot 10 + 5$

$\underbrace{72}_{n\cdot(n+1)} \cdot 100 + 25$

$85^2 = 7225$

$\underline{8}5 \to n = 8, \; n\cdot(n+1) = 8\cdot 9$

$8 \cdot 10 + 5$

Warum geht das? $\quad a_n a_{n-1} a_{n-2} \ldots a\,5 = z$ gesucht z^2

$$z = a_n a_{n-1} a_{n-2} \ldots a_1 5 = \underbrace{(a_n a_{n-1} a_{n-2} \ldots a_1)}_{n} \cdot 10 + 5$$

$$\Rightarrow \quad z = n \cdot 10 + 5 \quad \Rightarrow \quad z^2 = (n \cdot 10 + 5)^2$$

$(a+b)^2 = a^2 + 2ab + b^2$

$$= (n\cdot 10)^2 + 2\cdot(n\cdot 10)\cdot 5 + 5^2$$

$$= \underbrace{n^2 \cdot 100 + n \cdot 100}_{} + 25$$

$$= \underbrace{(n^2 + n)}_{} \cdot 100 + 25$$

$$= n\cdot(n+1) \cdot 100 + 25 \quad ✓$$

Weiter in der Vorlesung: Rechnen in $\mathbb{Z}_m = \{\overline{k} \mid 0 \le k \le m-1\}$

$\uparrow$ Restklassen beim (ganzz.) Teilen durch m

Aus der 17. Vorlesung ist bekannt:

a) $(\mathbb{Z}_m, +, \cdot)$ ist ein kommutativer Ring mit 1

b) $\overline{k} \in \mathbb{Z}_m$ hat ein inverses Element bezüglich der Multiplikation (also ein $\overline{l} \in \mathbb{Z}_m$ mit $\overline{k} \cdot \overline{l} = \overline{l} \cdot \overline{k} = \overline{1}$), falls k und m teilerfremd sind, d.h. $ggT(k, m) = 1$

$\Rightarrow$ $p \in \mathbb{N}$ Primzahl $\Rightarrow ggT(k,p) = 1 \; \forall k \in \mathbb{Z} \Rightarrow (\mathbb{Z}_p, +, \cdot)$ ist ein Körper, d.h. es gelten die 5 Körperaxiome (wie in $\mathbb{Q}$ und $\mathbb{R}$)

Beispiel: $(\mathbb{Z}_{13}, +, \cdot)$ 13 ist Primzahl $\Rightarrow (\mathbb{Z}_{13}, +, \cdot)$ ist ein Körper

a) Berechnen Sie das inverse Element bezüglich der Multiplikation von $\overline{11} \in \mathbb{Z}_{13}$

b) $(\mathbb{Z}_{13}, +, \cdot)$ ist ein Körper also gelten binomische Formeln! Rechnen Sie dies mal für $(\overline{5} + \overline{7})^2$

zu a) zunächst euklid. Algorithmus für $ggT(11, 13) = 1$

$$13 = 1 \cdot 11 + 2$$
$$11 = 5 \cdot 2 + 1 \leftarrow 1 = ggT(11,13)$$
$$2 = 2 \cdot 1 + 0$$

es gibt $s, t \in \mathbb{Z}$ mit $1 = ggT(11,13) = s \cdot 11 + t \cdot 13$

„Rückwärtsrechnen" (Lemma von Bézout)

$$1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (13 - 1 \cdot 11) = (-5) \cdot 13 + 6 \cdot 11$$

in $\mathbb{Z}_{13}$ gilt also

$$\overline{1} = \overline{(-5) \cdot 13 + 6 \cdot 11} = \overline{(-5)} \cdot \underbrace{\overline{13}}_{=\overline{0}} + \overline{6} \cdot \overline{11} = \overline{6} \cdot \overline{11}$$

$\Rightarrow$ die inverse Zahl zu $\overline{11}$ in $\mathbb{Z}_{13}$ bezüglich der Multiplikation ist $\overline{6}$

<u>Probe:</u> $\overline{6}\cdot\overline{11} = \overline{66} = \overline{65}+\overline{1} = \overline{5}\cdot\underbrace{\overline{13}}_{=\overline{0}}+\overline{1} = \overline{1}$

$65 = 5\cdot 13$

<u>zu b)</u> $(\overline{5}+\overline{7})^2 = \overline{12}^{\,2} = \overline{12}\cdot\overline{12} = \overline{12\cdot 12} = \overline{(12)^2} = \overline{144} = \overline{143}+\overline{1}$

$= \overline{11}\cdot\underbrace{\overline{13}}_{=\overline{0}} + \overline{1} = \overline{1}.$

$\overline{5}^2 + \overline{2}\cdot\overline{5}\cdot\overline{7} + \overline{7}^2 = \overline{25} + \overline{5}\cdot\overline{14} + \overline{49} = \overline{12}+\overline{5}+\overline{10}$

$\overline{25} = \overline{12}$, $\overline{14} = \overline{1}$, $\overline{49} = \overline{10}$

$= \overline{27} = \overline{2}\cdot\underbrace{\overline{13}}_{=\overline{0}}+\overline{1} = \overline{1}$

$\overline{14} = \overline{1}\cdot\underbrace{\overline{13}}_{=\overline{0}}+\overline{1} = \overline{1}$

$\overline{49} = \overline{39+10} = \overline{3}\cdot\underbrace{\overline{13}}_{=\overline{0}}+\overline{10} = \overline{10}$

$(\overline{5}+\overline{7})^2 = \overline{5}^2+\overline{2}\cdot\overline{5}\,\overline{7}+\overline{7}^2$

$\overline{25} = \underbrace{\overline{13}}_{=\overline{0}}+\overline{12} = \overline{12}$

<u>Merke:</u> Potenzieren ist wiederholtes Multiplizieren mit dem selben Faktor
also gilt für $\overline{k}\in\mathbb{Z}_m$: $\overline{k}^{\,n} = \overline{(k^n)}$

<u>Einführung in „simultane Kongruenzen"</u>

a) <u>Bemerkung zu Bezeichnungen:</u>

$\overline{k}\in\mathbb{Z}_m \Rightarrow \overline{k} = \{b\in\mathbb{Z} \mid b \text{ hat beim Teilen durch } m \text{ den Rest } k\}$

$= \{b\in\mathbb{Z} \mid m \mid b-k \text{ d.h. } m \text{ teilt } b-k\}$

$= \{b\in\mathbb{Z} \mid (k,b)\in R_m\}$

Äquivalenzrelation aus der 17. Vorlesung

<u>statt</u> $(k,b)\in R_m$ sagt man auch „k ist kongruent zu b modulo m"
und schreibt dafür $k \equiv b \mod m$

$\equiv$ ist kongruent zu

b) Was sind „simultane Kongruenzen"?

Beispiel: Nikolaus verteilt Geschenke. Wenn er in jeden Haushalt 3 Geschenke abgibt, hat er zum Schluß 2 Geschenke übrig. Wenn er in jeden Haushalt 5 Geschenke abgibt, hat zum Schluß 4 Geschenke übrig.

Wieviele Geschenke hat der Nikolaus mindestens dabei? Gibt es weitere mögliche Anzahlen von Geschenken?

Geschenkesack vom Nikolaus

3 Geschenke / 2 Rest : $S_1 = \{2, 5, 8, 11, 14, \underbrace{17, 20, 23, 26,}_{15 = 3\cdot 5} 29, \underbrace{\ldots}_{15} 44 \}$

5 Geschenke / 4 Rest: $S_2 = \{4, 9, 14, \underbrace{19, 24,}_{15 = 3\cdot 5} 29, \underbrace{34, \ldots}_{15} 44 \}$

Der Nikolaus hat mindestens 14 Geschenke dabei, weitere Möglichkeiten sind $x_k = 14 + k \cdot 3 \cdot 5$, $\tilde{x} = 14$ ist kleinste positive Lösung!

$\overline{x} = \overline{2}$ in $\mathbb{Z}_3 \leftarrow x \equiv 2 \bmod 3$

$\overline{x} = \overline{4}$ in $\mathbb{Z}_5 \leftarrow x \equiv 4 \bmod 5$

2 „simultane Kongruenzen"

Allgemein gilt:

Satz (chinesischer Restsatz für zwei simultane Kongruenzen):
Die simultanen Kongruenzen

$$\overline{x} = \overline{n} \text{ in } \mathbb{Z}_{m_1} \text{ und } \overline{x} = \overline{k} \text{ in } \mathbb{Z}_{m_2}$$

sind lösbar, wenn gilt: $\mathrm{ggT}(m_1, m_2) = 1$.

Es gilt dann: $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$ ist **eine** Lösung, falls gilt $\overline{a} \cdot \overline{m_2} = \overline{1}$ in $\mathbb{Z}_{m_1}$ und $\overline{b} \cdot \overline{m_1} = \overline{1}$ in $\mathbb{Z}_{m_2}$.

Weitere (positive) Lösungen sind $x = x_0 + i \cdot m_1 \cdot m_2$ für $i \in \mathbb{Z}$ (solange $x \geq 0$ gilt).

Bemerkung:

a) $\mathrm{ggT}(m_1, m_2) = 1$ heißt m_1 und m_2 sind teilerfremd

b) $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$ mit $\overline{a} \cdot \overline{m_2} = \overline{1}$ in $\mathbb{Z}_{m_1}$ und $\overline{b} \cdot \overline{m_1} = \overline{1}$ in $\mathbb{Z}_{m_2}$ ist nicht immer sofort die kleinste pos. Lösung sondern auf jeden Fall 1 Lösung von den unendlich vielen Möglichkeiten $x = x_0 + i \cdot m_1 \cdot m_2$, $i \in \mathbb{Z}$

c) Wie sieht das in unserem Beispiel aus:

$n = 2$, $m_1 = 3$
$k = 4$, $m_2 = 5$
gesucht in $\mathbb{Z}_3$: $\overline{a}$ mit $\overline{a} \cdot \overline{5} = \overline{1}$ in $\mathbb{Z}_3$

gesucht in $\mathbb{Z}_5$: $\bar{b}$ mit $\bar{b} \cdot \bar{3} = \bar{1}$ in $\mathbb{Z}_5$

$\bar{b} \cdot \bar{3} = \bar{1}$ in $\mathbb{Z}_5$ $\to$ Lösung durch „Hingucken" $\bar{b} = \bar{2}$

$\bar{a} \cdot \bar{5} = \bar{1}$ in $\mathbb{Z}_3$ $\Rightarrow$ $\bar{a} \cdot \bar{2} = \bar{1}$ in $\mathbb{Z}_3$ $\to$ Lösung durch „Hingucken" $\bar{a} = \bar{2}$

$\bar{5} = \bar{2}$ in $\mathbb{Z}_3$

<u>also</u>: $x_0 = 2 \cdot 2 \cdot 5 + 4 \cdot 2 \cdot 3 = 20 + 24 = 44$