A. Sei $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ mit $\omega = \frac{1}{2}(-1 + i\sqrt{3})$.

(a) z.z.: $\mathbb{Z}[\omega]$ ist euklidischer Ring mit Norm $N(a+b\omega) = a^2 - ab + b^2$.

- $(a+b\omega) + (c+d\omega) = (a+c) + (b+d)\omega$
- $(a+b\omega) \cdot (c+d\omega) = ac + (ad+bc)\omega + bd\omega^2$, und es gilt $\omega^2 \in \mathbb{Z}[\omega]$:
- $\omega^2 = \frac{1}{4}(1 - 2i\sqrt{3} - 3) = \frac{1}{4}(-2 - 2i\sqrt{3}) = -\frac{1}{2}(1 + i\sqrt{3}) = -\frac{1}{2}(-1+i\sqrt{3}) - 1 = -\omega - 1$.
- $\mathbb{Z}[\omega]$ erbt alle Rechengesetze und die Nullteilerfreiheit von $\mathbb{C}$, ist also ein Integritätsbereich.

„Division mit Rest": $\forall z_1, z_2 \in \mathbb{Z}[\omega], z_2 \neq 0\ \exists q, r \in \mathbb{Z}[\omega]: z_1 = q z_2 + r$ mit $N(r) \leq N(z_2)$.

$$\underbrace{\frac{z_1}{z_2}}_{\in \mathbb{C}} = \underbrace{(a + b\omega)}_{\substack{\text{nächstliegende Zahl} \\ \text{in } \mathbb{Z}[\omega]}} + \underbrace{(s_1 + i s_2)}_{s_1, s_2 \in \mathbb{R}} = \underbrace{(a + b\omega)}_{=: q} + \underbrace{(t_1 + t_2\omega)}_{=: t}.$$

(Wir können jedes $z \in \mathbb{C}$ in die Form $t_1 + \omega t_2$, $t_1, t_2 \in \mathbb{R}$ bringen vermöge des Basiswechsels $x + iy = \binom{x}{y} \mapsto A^{-1}\binom{x}{y} = \begin{pmatrix} 1 & 1/\sqrt{3} \\ 0 & 2/\sqrt{3} \end{pmatrix}\binom{x}{y}$, wobei $A = \begin{pmatrix} 1 & \underbrace{\begin{smallmatrix} -1/2 \\ \sqrt{3}/2 \end{smallmatrix}}_{=\omega} \\ 0 & \end{pmatrix}$,

bzw. $x + iy = \left(x + \frac{y}{\sqrt{3}}\right) + \left(\frac{2}{\sqrt{3}} y\right)\omega$.)

Nun gilt $\underbrace{z_1}_{\in \mathbb{Z}[\omega]} = \underbrace{q \cdot z_2}_{\in \mathbb{Z}[\omega]} + \underbrace{t \cdot z_2}_{\Rightarrow =: r \in \mathbb{Z}[\omega]}$. Der max. Abstand von einem $z \in \mathbb{C}$ zu $\mathbb{Z}[\omega]$ ist der Abstand des Mittelpunkts eines der von $\mathbb{Z}[\omega]$ aufgespannten Parallelogramme zu dessen Ecken, also $\left\|\frac{1+\omega}{2}\right\|_2 = \left\|\frac{1}{4} + \frac{\sqrt{3}}{4} i\right\|_2 = \sqrt{\frac{1}{4}} = \frac{1}{2}$, d.h. $\|s\|_2 \leq \frac{1}{2}$ und folglich

$$N(r) = N(t \cdot z_2) = N(t)\, N(z_2) = (t_1^2 - t_1 t_2 + t_2^2)\, N(z_2)$$
$$= \left[\left(s_1 + \frac{s_2}{\sqrt{3}}\right)^2 - \left(s_1 + \frac{s_2}{\sqrt{3}}\right)\left(\frac{2}{\sqrt{3}} s_2\right) + \left(\frac{2}{\sqrt{3}} s_2\right)^2\right] N(z_2)$$
$$\overset{\text{(MAPLE)}}{=} (s_1^2 + s_2^2)\, N(z_2) \leq \frac{1}{4} N(z_2) < N(z_2).$$

Dabei haben wir die Multiplikativität der Norm verwendet, die man leicht nachrechnen kann.

(b) Einheiten von $\mathbb{Z}[\omega]$: $a + b\omega$ Einheit $\Rightarrow N(a+b\omega) = 1$ $[\Leftrightarrow (a-b)^2 + ab = 1]$.

Falls $a, b > 1$, gilt wegen $(a-b)^2 > 0$ $N(a+b\omega) > 1$; dasselbe passiert, wenn $a > 2$ und $b \neq 0$ oder $b > 2$ und $a \neq 0$. Weiters gilt $a, b = 0 \Rightarrow N(a+b\omega) = 0$. Auch $a > 2 \wedge b = 0$ und $b > 2 \wedge a \neq 0$ ist unmöglich. Alle bisher behandelten Fälle mit umgekehrtem Vorzeichen erweisen sich ebenso als unmöglich, weiters auch $a \geq 1$ und $b < -1$, $a \leq -1$ und $b > 1$; die verbliebenen Fälle sind also $a = b = 1$, $a = b = -1$, $a = 0 \wedge b = 1$, $a = 1 \wedge b = 0$, $a = 0 \wedge b = -1$, $a = -1 \wedge b = 0$, also ist $\{1+\omega, -\omega-1 = \omega^2, \omega, 1, -\omega, -1\}$ die Menge der möglichen Einheiten. Es verbleibt die Verifikation, dass es sich tatsächlich um Einheiten handelt.

Zum Beispiel gilt $\frac{1}{\omega} = \frac{\overline{\omega}}{\underbrace{\omega\overline{\omega}}_{=1}} = \overline{\omega} \in \mathbb{Z}[\omega]$, also ist ω eine Einheit.

Die anderen Fälle gehen genauso.

ad (A.) c) z.z.: $(1-\omega)^2 \mid 3$: siehe Teil (a)

$$(1-\omega)^2 = 1-2\omega+\omega^2 \overset{\downarrow}{=} 1-2\omega-\omega-1 = -3\omega$$

$$\Rightarrow \frac{3}{(1-\omega)^2} = \frac{3}{-3\omega} = -\frac{1}{\omega} = -\frac{\overline{\omega}}{\underbrace{\omega\overline{\omega}}_{=1}} = -\overline{\omega} = -\frac{1}{2}(-1-i\sqrt{3}) = \frac{1}{2}(1+i\sqrt{3})$$

$$= \frac{1}{2}(-1+i\sqrt{3})+1 = \omega+1 \in \mathbb{Z}[\omega].$$

(B.) Finde alle $n \in \mathbb{Z}^+$ mit $\varphi(5n) = 5\varphi(n)$. Wir wissen: $\varphi(n) = n \cdot \prod_{\substack{p\in\mathbb{P}\\ p\mid n}} \left(1-\frac{1}{p}\right)$.

Fall 1: $5 \nmid n$. Dann gilt $\varphi(5n) = 5n \prod_{p\mid 5n}\left(1-\frac{1}{p}\right) = \frac{4}{5}\cdot 5n\prod_{p\mid n}\left(1-\frac{1}{p}\right) = 4\varphi(n) \neq 5\varphi(n)$.

Fall 2: $5 \mid n$. Dann gilt $\varphi(5n) = 5n\prod_{p\mid 5n}\left(1-\frac{1}{p}\right) = 5n\prod_{p\mid n}\left(1-\frac{1}{p}\right) = 5\varphi(n)$.

Also gilt $\varphi(5n) = 5\varphi(n) \Leftrightarrow 5 \mid n$.

(6.) w.w.: $\forall n\in\mathbb{N}\ \forall p\in\mathbb{P}$: $v_p(n!) = \sum_{k\geq 1}\left\lfloor \frac{n}{p^k}\right\rfloor$.

a) Auf wieviele Nullen endet $(169!)$?

Auf soviele, wie $169!$ den Primfaktor 10 enthält – also $\min\{v_2(169!), v_5(169!)\}$ mal.

$$v_2(169!) = \sum_{k\geq 1}\left\lfloor\frac{169}{2^k}\right\rfloor = \sum_{k=1}^{7}\left\lfloor\frac{169}{2^k}\right\rfloor = 84+42+21+10+5+2+1 = 165,$$

$$v_5(169!) = \sum_{k=1}^{3}\left\lfloor\frac{169}{5^k}\right\rfloor = 33+6+1 = 40,$$ also auf 40 Nullen.

b) z.z.: $\sqrt[n]{n!} \leq \prod_{p\mid n!} p^{\frac{1}{p-1}}$

$$\sqrt[n]{n!} = \sqrt[n]{\prod_{p\mid n} p^{v_p(n!)}} \leq \sqrt[n]{\prod_{p\mid n!} p^{\sum_{k\geq 1}\left\lfloor\frac{n}{p^k}\right\rfloor}} = \prod_{p\mid n!} p^{\boxed{\frac{\sum_{k\geq 1}\left\lfloor\frac{n}{p^k}\right\rfloor}{n}}}.$$

Nun gilt $\sum_{k\geq 1}\left\lfloor\frac{n}{p^k}\right\rfloor \leq n\sum_{k\geq 1}\left(\frac{1}{p}\right)^k = n\left(\frac{1}{1-\frac{1}{p}}-1\right) = n\left(\frac{1}{p-1}\right)$ also

$$\boxed{\frac{\sum_{k\geq 1}\left\lfloor\frac{n}{p^k}\right\rfloor}{n}} \leq \frac{1}{p-1}$$ und daher die gewünschte Ungleichung. $\square$

(2.) Seien $a, b \in \mathbb{Z}^+$ mit $a \mid b^2,\ b^2 \mid a^3,\ a^3 \mid b^4, \ldots$ z.z.: $a = b$.

Sei $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$, $b = \prod_{p \in \mathbb{P}} p^{v_p(b)}$, dann gilt für jedes $p \in \mathbb{P}$:

$v_p(a) \leq v_p(b^2) \leq v_p(a^3) \leq v_p(b^4) \leq \ldots$ bzw. äquivalent dazu

$v_p(a) \leq 2\,v_p(b) \leq 3\,v_p(a) \leq 4\,v_p(b) \leq \ldots$

Wir zeigen nun $v_p(a) = v_p(b)$. Gilt $v_p(b) = 0$, folgt $v_p(a)=0$ und wir sind fertig.

Andernfalls gilt $\forall n \geq 3$: $(n-1)\,v_p(b) \leq n\,v_p(a) \leq (n+1)\,v_p(b)$, also

$$\frac{n-1}{n} \leq \frac{v_p(a)}{v_p(b)} \leq \frac{n+1}{n},$$

woraus mit dem Einschließungssatz für $n \to \infty$ $v_p(a) = v_p(b)$ folgt. $\square$

(4.) z.z.: $n \geq 1 \Rightarrow (n!+1,\ (n+1)!+1) = 1$.

Ang., es gäbe ein $p \in \mathbb{P}$ mit $p \mid (n!+1) \ \wedge\ p \mid ((n+1)!+1)$.

Dann gilt auch $p \mid (n+1)!+1-(n!+1) = n!\,n$

und somit, wegen $p \in \mathbb{P}$, $p \leq n$. Damit erhalten wir aber

$p \mid n!$, im Widerspruch zu $p \mid (n!+1)$. $\square$

(3.) z.z.: $H_n = \sum_{k=1}^{n} 1/k \notin \mathbb{Z}$ für $n > 1$.

Es gilt $H_n = \left(\sum_{k=1}^{n} \frac{\mathrm{kgV}(1,\ldots,n)}{k}\right) / \mathrm{kgV}(1,\ldots,n)$. Wir zeigen, dass dieser Bruch die Form ungerade / gerade hat und folglich nicht ganzzahlig ist.

Seien dazu $d \in 2\mathbb{N}+1$ und $t \in \mathbb{N}$ mit $\mathrm{kgV}(1,\ldots,n) = 2^t d$ sowie $s := \max\{m \in \mathbb{N} : 2^m \leq n\}$.

Offensichtlich gilt $t = s$. Nun gilt

$$\frac{\mathrm{kgV}(1,\ldots,n)}{k} \in \begin{cases} 2\mathbb{N}+1, & k = 2^s \\ 2\mathbb{N}, & k \neq 2^s. \end{cases}$$

Der Zähler hat also genau einen ungeraden Summanden und ist daher ungerade.

Der Nenner ist für $n > 1$ offenbar gerade. $\square$

(8.) z.z.: $s \notin \mathbb{P} \Rightarrow 2^s - 1 \notin \mathbb{P}$.

Sei $s = ak$, $a, k > 1$. Dann gilt $2^s - 1 = 2^{ak} - 1 = \underbrace{(2^a - 1)}_{p}\underbrace{\left(\frac{2^{ak}-1}{2^a-1}\right)}_{q}$

und $q = \dfrac{(2^a)^k - 1}{2^a - 1} = \sum_{i=1}^{k} (2^a)^{i-1} \in \mathbb{N}$, also $2^s - 1 = p \cdot q$ mit $p, q > 1$. $\square$

(24.)

- $\left(\frac{70}{97}\right) = \left(\frac{2}{97}\right)\cdot\left(\frac{5}{97}\right)\cdot\underbrace{\left(\frac{7}{97}\right)}_{\equiv 1(4)} = (-1)^{\frac{97^2-1}{8}}\cdot\left(\frac{\overset{\equiv 2(5)}{97}}{5}\right)\cdot\left(\frac{\overset{\equiv 6(7)}{97}}{7}\right)$

  ↳ $97 \in \mathbb{P}$

  $= (-1)^{1176}\cdot\left(\frac{2}{5}\right)\cdot\left(\frac{6}{7}\right) = (-1)^3\cdot\left(\frac{2}{7}\right)\cdot\left(\frac{\overset{\equiv 3(4)}{3}}{\underset{\equiv 3(4)}{7}}\right) = (-1)\cdot(-1)^6\cdot\left[-\left(\frac{\overset{\equiv 1(3)}{7}}{3}\right)\right] = (-1)^2\cdot\left(\frac{1}{3}\right) = \underline{\underline{1.}}$

- $\left(\frac{-14}{83}\right) = \left(\frac{-1}{83}\right)\cdot\left(\frac{2}{83}\right)\cdot\left(\frac{\overset{\equiv 3(4)}{7}}{\underset{\equiv 3(4)}{83}}\right) = \underbrace{(-1)^{\frac{83-1}{2}}\cdot(-1)^{\frac{83^2-1}{8}}}_{=1}\cdot\left[-\left(\frac{\overset{\equiv 6(7)}{83}}{7}\right)\right] = -\left(\frac{6}{7}\right) = -\left[\left(\frac{2}{7}\right)\cdot\left(\frac{3}{7}\right)\right]$

  ↳ $83 \in \mathbb{P}$

  $= -\left[(-1)^{\frac{7^2-1}{8}}\cdot\left(-\left(\frac{7}{3}\right)\right)\right] = \left(\frac{\overset{\equiv 1(3)}{7}}{3}\right) = \left(\frac{1}{3}\right) = \underline{1.}$

- $\left(\frac{55}{89}\right) = \left(\frac{11}{\underset{\equiv 1(4)}{89}}\right)\cdot\left(\frac{5}{\underset{\equiv 1(4)}{89}}\right) = \left(\frac{\overset{\equiv 1(11)}{89}}{11}\right)\cdot\left(\frac{89}{5}\right) = \underbrace{\left(\frac{1}{11}\right)}_{=1}\cdot\left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = (-1)^{2\cdot\left(\frac{5^2-1}{8}\right)} = (-1)^6 = \underline{\underline{1.}}$

  ↳ $89 \in \mathbb{P}$

(34.) Gibt es eine Quadratzahl der Form $55k-1$?

Ang., $x^2 = 55k-1 \Leftrightarrow x^2+1 = 55k \Leftrightarrow x^2 \equiv -1\ (55)$. $\boxed{55 = 5\cdot 11}$

Diese Kongruenz ist lösbar, genau dann wenn $x^2 \equiv -1\,(11)$ und $x^2 \equiv -1\,(5)$ lösbar sind.

Wir berechnen $\left(\frac{-1}{11}\right) = (-1)^{\frac{11-1}{2}} = \underline{-1}$, also existiert kein solches x.

(vii.)

Komet A, B, C zuletzt gesehen vor 1, 2, 8 Jahren, alle 5, 8, 11 Jahre. Wann nächstes, übernächstes mal alle zu sehen?

Wir suchen also ein x mit
$$x \equiv -1\ (5)$$
$$x \equiv -2\ (8)$$
$$x \equiv -8\ (11).$$
5, 8 und 11 sind paarweise teilerfremd, also können wir den chinesischen Restsatz anwenden.

Wir benötigen
$$b_1\cdot 8\cdot 11 \equiv 1\ (5)$$
$$b_2\cdot 5\cdot 11 \equiv 1\ (8)$$
$$b_3\cdot 5\cdot 8 \equiv 1\ (11).$$
Exemplarisch berechnen wir b_1 mit dem Euklidischen Algorithmus:

$88 = 17\cdot 5 + 3$	$1 = 3 - 1\cdot 2 = 3 - 1\cdot(5-1\cdot 3) = 2\cdot 3 - 5 =$
$5 = 1\cdot 3 + 2$	$= 2\cdot(88 - 17\cdot 5) - 5 = 2\cdot 88 - 35\cdot 5,$
$3 = 1\cdot 2 + \boxed{1}$	
$2 = 1\cdot 2 + 0$	also $2\cdot 88 \equiv 1\ (5)$, d.h. $b_1 = 2 = (88)^{-1} \bmod 5$.

Genauso erhält man $b_2 = 7$ und $b_3 = 8$ und daher, nach der Formel aus der Vorlesung, $x = \sum_{i=1}^{3} a_i b_i \frac{m}{m_i}$ $(m_i = 5, 8, 11,\ m = 5\cdot 8\cdot 11)$ $= -3506 \equiv 14 \bmod m = 440$.

Da $x \bmod 440$ eindeutig bestimmt ist, ist das nächste gesuchte Jahr in $\underline{14}$ Jahren und das darauffolgende in $14 + 440 = \underline{\underline{454}}.$

(xiv.) Sei $p \in \mathbb{P}$, $p \equiv 1\ (2)$ und seien g_1, g_2 Primitivwurzeln mod p.

z.z.: $g_1 g_2$ ist keine Primitivwurzel mod p.

Weil g_1 eine Primitivwurzel ist, gibt es ein k mit $g_2 = g_1^k$. Für gerades $k = 2l$ kann g_1^k keine Primitivwurzel sein, denn es gilt $(g_1^{2l})^{\frac{p-1}{2}} = (g_1^{l})^{p-1} = 1$, also $\mathrm{ord}(g_1^k) = \frac{p-1}{2} < p$. Also ist k ungerade. Nun ist aber $g_1 g_2 = g_1^{k+1}$, was als Potenz von g_1 mit ungeradem Exponenten nach demselben Argument keine Primitivwurzel sein kann. $\square$

(iii) z.z.: $a, b, c > 0 \implies [a,b,c] = \frac{abc\,(a,b,c)}{(a,b)(b,c)(c,a)}$

Wir wissen bereits, dass $\forall p \in \mathbb{P}: v_p([a,b,c]) = \max\{v_p(a), v_p(b), v_p(c)\}$.

Sei $p \in \mathbb{P}$ und gelte o.B.d.A. $v_p(a) \le v_p(b) \le v_p(c)$, dann ist

$$v_p\left(\frac{abc\,(a,b,c)}{(a,b)(b,c)(c,a)}\right) = v_p(a) + v_p(b) + v_p(c) + \min_{i \in \{a,b,c\}} v_p(i) - \min_{i \in \{a,b\}} v_p(i) - \min_{i \in \{b,c\}} v_p(i) - \min_{i \in \{a,c\}} v_p(i)$$

$$= v_p(a) + v_p(b) + v_p(c) + v_p(a) - v_p(a) - v_p(b) - v_p(a)$$

$$= v_p(c) = \max_{i \in \{a,b,c\}} v_p(i). \quad \square$$

(N.) Finde kleinstes $x \in \mathbb{Z}^+$, sodass $x \equiv i\ (i+1)$, $i = 1, \dots, 9$.

$x \equiv 1\ (2)$
$x \equiv 3\ (4) \Rightarrow x \equiv 1 (2)$ ✓
$x \equiv 7\ (8) \Rightarrow x \equiv 1 (2),\ x \equiv 3 (4)$ ✓
$x \equiv 5\ (6) \Rightarrow x \equiv 1 (2),\ x \equiv 2 (3)$ ✓

$x \equiv 2\ (3)$
$x \equiv 8\ (9) \Rightarrow x \equiv 2 (3)$ ✓

$x \equiv 4\ (5)$
$x \equiv 9\ (10) \Rightarrow x \equiv 4 (5),\ x \equiv 1 (2)$ ✓

$x \equiv 6\ (7)$

$\leadsto$ $\boxed{\begin{aligned} x &\equiv 6\ (7) \\ x &\equiv 8\ (9) \\ x &\equiv 9\ (10) \end{aligned}}$ $a_1 = 6$, $a_2 = 8$, $a_3 = 9$; $m_1 = 7$, $m_2 = 9$, $m_3 = 10$

paarweise teilerfremd

$b_1 \overset{!}{=} 90^{-1}\ (7)$	$b_2 \overset{!}{=} 70^{-1}\ (9)$	$b_3 \overset{!}{=} 63^{-1}\ (10)$
$90 = 12 \cdot 7 + 6$	$70 = 7 \cdot 9 + 7$	$63 = 6 \cdot 10 + 3$
$7 = 1 \cdot 6 + \boxed{1}$	$9 = 1 \cdot 7 + 2$	$10 = 3 \cdot 3 + \boxed{1}$
	$7 = 3 \cdot 2 + \boxed{1}$	
$1 = 7 - 1 \cdot 6$	$1 = 7 - 3 \cdot 2$	$1 = 10 - 3 \cdot 3$
$= 7 - (90 - 12 \cdot 7)$	$= 7 - 3 \cdot (9 - 7)$	$= 10 - 3 \cdot (63 - 6 \cdot 10)$
$= 13 \cdot 7 - 90$	$= 70 - 7 \cdot 9 - 3 \cdot (9 - 70 + 7 \cdot 9)$	$= 19 \cdot 10 - 3 \cdot 63$
	$= 70 \cdot 4 - 9 \cdot 31$	
$b_1 = -1$	$b_2 = 4$	$b_3 = -3$

$x = \sum_{i=1}^{3} a_i b_i \frac{m}{m_i} = 6 \cdot (-1) \cdot 90 + 8 \cdot 4 \cdot 70 + 9 \cdot (-3) \cdot 63$

$= -1 \equiv 629\ (630)$ und x ist eindeutig mod 630, also $\boxed{x = 629}$.

(xxiii.) z.z.: $m, n \in \mathbb{N}$: $\quad m \mid n \Rightarrow \varphi(m) \mid \varphi(n)$

$$m \mid n \Rightarrow [\forall p \in \mathbb{P}: p \mid m \Rightarrow p \mid n]$$

Daher gilt $\varphi(m) = m \cdot \prod_{\substack{p \in \mathbb{P} \\ \underbrace{p \mid m}_{\Rightarrow p \mid n}}} \left(1 - \frac{1}{p}\right) \mid \underbrace{n}_{m \mid} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} \left(1 - \frac{1}{p}\right) = \varphi(n)$. $\square$

(xxxi.) Finde Lösung der Gleichung $1255x + 177y = 1$. Euklidischer Algorithmus:

$$\begin{aligned} 1255 &= 7 \cdot 177 + 16 \\ 177 &= 11 \cdot 16 + \boxed{1} \\ 16 &= 16 \cdot 1 + 0 \end{aligned}$$

$$1 = 177 - 11 \cdot 16 = 177 - 11 \cdot (1255 - 7 \cdot 177)$$
$$= \underbrace{(-11)}_{=: x} \cdot 1255 + \underbrace{78}_{=: y} \cdot 177.$$

(ii.) Auf wieviele Nullen endet $(500!)/(200!)$?

Der Satz von Legendre (Bsp. 5) sagt: $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$.

Offenbar gilt $v_2(n!) \geq v_5(n!)$, daher enthält $n!$ den Faktor 10 $v_5(n!)$ mal.

- $\sum_{k \geq 1} \left\lfloor \frac{500}{5^k} \right\rfloor = 100 + 20 + 4 = 124$
- $\sum_{k \geq 1} \left\lfloor \frac{200}{5^k} \right\rfloor = 40 + 8 = 48$

Daher endet $(500!)/(200!)$ auf $124 - 48 = \underline{\underline{76}}$ Nullen.

(xi.) Gib alle Paare $(x, y) \in \mathbb{Z}^2$ an, sodass $40x + 64y = 56$.

- $$\begin{aligned} 64 &= 1 \cdot 40 + 24 \\ 40 &= 1 \cdot 24 + 16 \\ 24 &= 1 \cdot 16 + \boxed{8} \\ 16 &= 2 \cdot 8 + 0 \end{aligned}$$

$$8 = 24 - 1 \cdot 16 = 24 - (40 - 24) = -40 + 2 \cdot 24 = -40 + 2 \cdot (64 - 40)$$
$$= 40 \cdot (-3) + 64 \cdot 2$$

$56 = 7 \cdot 8 \rightsquigarrow$ partikuläre Lsg.: $x_0 = -3 \cdot 7 = -21$, $y_0 = 2 \cdot 7 = 14$.

- $40x + 64y = 0 \Leftrightarrow \frac{x}{y} = -\frac{64}{40} = \frac{64/8}{-40/8} = \frac{8}{-5} \Leftrightarrow \exists k \in \mathbb{Z}: x = k \cdot 8, \; y = -k \cdot 5$
- Allg. Lsg.: $\underline{\underline{\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -21 \\ 14 \end{pmatrix} + k \begin{pmatrix} 8 \\ -5 \end{pmatrix}}}$

(XXI.) Seien $p,\ 8p-1 \in \mathbb{P}$. Kann auch $8p+1 \in \mathbb{P}$ sein?

Nein: Fall 1, $p=3$: $8\cdot 3+1 = 25 \notin \mathbb{P}$.

Fall 2, $p \neq 3$: Fall 2.1, $p = 3k-1 \Rightarrow 8p-1 = 24k-9 = 3(8k-3) \Rightarrow 8p-1 \notin \mathbb{P}$.

Fall 2.2, $p = 3k+1 \Rightarrow 8p+1 = 24k+9 = 3(8k+3) \Rightarrow 8p+1 \notin \mathbb{P}$. $\square$

(XX.) Seien $a, b \in \mathbb{N},\ (a,b)=1$. Berechne $(a^3-b^3,\ a^2-b^2) =: d$.

$$\left.\begin{aligned} a^3-b^3 &= (a-b)(a^2+ab+b^2) \\ a^2-b^2 &= (a-b)(a+b) \end{aligned}\right\} \Rightarrow d = (a+b,\ a^2+ab+b^2)\cdot(a-b)$$

Sei $p \in \mathbb{P}$ beliebig. Angenommen, $p \mid \underbrace{a+b}_{p\mid} \ \wedge\ p \mid a^2+ab+b^2 = \underbrace{(a+b)^2}_{p\mid} + \underbrace{ab}_{\Rightarrow p\mid}$

$\Longrightarrow p \mid ab \overset{p\in\mathbb{P}}{\Longrightarrow} p\mid a \vee p \mid b$.

O.B.d.A. gelte $p \mid a$, dann gilt wegen $p \mid a+b$ auch $p \mid b$, im Widerspruch zu $(a,b)=1$. Also gilt $(a+b,\ a^2+ab+b^2)=1$ und folglich $d = \underline{\underline{a-b}}$.

(L.) Sei $x_n = a\cdot n + b$ arithmetische Progression, $m \in \mathbb{N}$.

z.z.: $\exists n_0 \in \mathbb{N}\ \forall k = 1,\dots,m:\ x_{n_0+k}$ ist zusammengesetzt.

Wir stellen fest, dass $\forall m \in \mathbb{N}$ die Zahlen $m!+k,\ k = 2,\dots,m$ wegen $m!+k = k\left(\frac{m!}{k}+1\right)$ zusammengesetzt sind. Seien o.B.d.A. $a, b, m > 0$.

Wir wählen $n_0 := \dfrac{((m+1)a+b)!}{a}$, dann gilt

$$x_{n_0+k} = a(n_0+k)+b = ((m+1)a+b)! + (ak+b).$$

Für $2 \leq k \leq m+1$ gilt $2 \leq ak+b \leq (m+1)a+b$. Wegen der obigen Feststellung über die Faktorielle sind $((m+1)a+b)!+i$ für $2 \leq i \leq (m+1)a+b$ alle zusammengesetzt und damit auch

$x_{n_0+k},\ \underbrace{2 \leq k \leq m+1}_{m \text{ Zahlen}}$. $\square$

(5.) z.z.: $\forall n \in \mathbb{N}\ \forall p \in \mathbb{P}$: $v_p(n!) = \sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor$.

Es gilt $v_p(n!) = \sum_{i=1}^{n} v_p(i)$ und $v_p(i) = k \Leftrightarrow i$ ist Vielfaches von p^k.
Weiters ist $m p^k \leq n \Leftrightarrow m \leq \frac{n}{p^k}$, also ist $\lfloor \frac{n}{p^k} \rfloor$ gleich der Anzahl der Vielfachen von p^k unter den Zahlen $1, \dots, n$.
Ist $v_p(i) = l$, dann ist i ein Vielfaches von p^k, $k = 1, \dots, l$, und wird daher in der Summe $\sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor$ genau l Mal gezählt. □

(M.) (a) z.z.: $\forall x, y \in \mathbb{R}$: $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.
Es gilt $\lfloor x \rfloor \leq x$, $\lfloor y \rfloor \leq y$ und folglich $\lfloor x \rfloor + \lfloor y \rfloor \leq x + y$. Deshalb ist
$\lfloor x \rfloor + \lfloor y \rfloor \leq \max\{m \in \mathbb{Z} : m \leq x + y\} =: \lfloor x + y \rfloor$.

(b) z.z.: $n!$ teilt das Produkt von n bel. aufeinanderfolgenden Zahlen.
Seien also $m \in \mathbb{N}$, dann gilt $(m+1) \cdots (m+n) = \frac{(m+n)!}{m!}$ und mit
Bsp. 5 $v_p\left(\frac{(m+n)!}{m!}\right) = v_p((m+n)!) - v_p(m!) = \sum_{k \geq 1} \left\lfloor \frac{m+n}{p^k} \right\rfloor - \sum_{k \geq 1} \left\lfloor \frac{m}{p^k} \right\rfloor$.

Mit (a) gilt $\lfloor n \rfloor = \lfloor m \rfloor + \lfloor n \rfloor - \lfloor m \rfloor \leq \lfloor m + n \rfloor - \lfloor m \rfloor$,
also $\left\lfloor \frac{m+n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor \geq \left\lfloor \frac{n}{p^k} \right\rfloor$ und daher $v_p\left(\frac{(m+n)!}{m!}\right) \geq v_p(n!)$.

(c) Wie kann man (b) mithilfe von Binomialkoeffizienten zeigen?

$$\frac{(m+n)!}{m!} = \frac{(m+n)!\ n!}{m!\ (m+n-m)!} = n! \underbrace{\binom{m+n}{n}}_{\in \mathbb{Z}}. \quad \square$$

(xiii.) Was sind die letzten beiden Ziffern (in Basis 10) von 3^{3333}?
Die entscheidende Beobachtung ist, dass die letzten beiden Ziffern von 3^{n+1} nur von den letzten beiden Ziffern von 3^n abhängen:
$3^{n+1} \bmod 100 = [(3^n \bmod 100) \cdot 3] \bmod 100$. Die letzten beiden Ziffern müssen sich also zyklisch wiederholen. Wir berechnen mit obiger Regel:

$3^0 \equiv 1\ (100)$	$3^{10} \equiv 49$
$3^1 \equiv 3\ (100)$	$3^{11} \equiv 47$
$3^2 \equiv 9\ (100)$	$3^{12} \equiv 41$
$3^3 \equiv 27\ (100)$	$3^{13} \equiv 23$
$3^4 \equiv 81\ (100)$	$3^{14} \equiv 69$
$3^5 \equiv 43\ (100)$	$3^{15} \equiv 7$
$3^6 \equiv 29\ (100)$	$3^{16} \equiv 21$
$3^7 \equiv 87\ (100)$	$3^{17} \equiv 63$
$3^8 \equiv 61\ (100)$	$3^{18} \equiv 89$
$3^9 \equiv 83\ (100)$	$3^{19} \equiv 67$

und schließlich $3^{20} \equiv 1\ (100)$, also hat der Zyklus die Länge 20. Wir berechnen

$3333 \equiv 13\ (20)$

und somit $3^{3333} \equiv \underline{\underline{23}}\ (100)$.