

(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": $\forall z_1, z_2 \in \mathbb{Z}[\omega], z_2 \neq 0 \exists q, r \in \mathbb{Z}[\omega]: z_1 = qz_2 + r$ mit $N(r) \leq N(z_2)$.

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

(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 $x+iy = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A^{-1} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{3}} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, wobei $A = \begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}$,
 $\stackrel{= \omega}{=}$

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

Nun gilt $\underbrace{z_1}_{\in \mathbb{Z}[\omega]} = \underbrace{q \cdot z_2}_{\in \mathbb{Z}[\omega]} + \underbrace{t \cdot z_2}_{=: r \in \mathbb{Z}[\omega]}$. 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 deren Ecken, also $\|\frac{1+\omega}{2}\|_2 = \|\frac{1}{4} + \frac{\sqrt{3}}{4}i\|_2 = \sqrt{\frac{1}{4}} = \frac{1}{2}$, d.h. $\|s\|_2 \leq \frac{1}{2}$ und folglich

$$N(r) = N(t \cdot z_2) = N(t) N(z_2) = (t_1^2 - t_1 t_2 + t_2^2) N(z_2) \\ = \left[\left(s_1 + \frac{s_2}{\sqrt{3}} \right)^2 - \left(s_1 + \frac{s_2}{\sqrt{3}} \right) \left(\frac{2}{\sqrt{3}} s_2 \right) + \left(\frac{2}{\sqrt{3}} s_2 \right)^2 \right] N(z_2)$$

$$\stackrel{(\text{MAPLE})}{=} (s_1^2 + s_2^2) N(z_2) \leq \frac{1}{4} N(z_2) < N(z_2).$$

Daher 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 $a \neq 0$. Weidurs 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, weilers auch $a \geq 1$ und $b < -1$, $a < -1$ und $b \geq 1$; die verbleibenden 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 $\frac{1}{\omega} = \frac{\bar{\omega}}{\omega \bar{\omega}} = \bar{\omega} \in \mathbb{Z}[\omega]$, also ist ω eine Einheit.

Die anderen Fälle gehen genauso.

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

$$(1-w)^2 = 1 - 2w + w^2 \stackrel{!}{=} 1 - 2w - w - 1 = -3w$$

$$\Rightarrow \frac{3}{(1-w)^2} = \frac{3}{-3w} = -\frac{1}{w} = -\frac{\bar{w}}{w\bar{w}} = -\bar{w} = -\frac{1}{2}(-1 - i\sqrt{3}) = \frac{1}{2}(1 + i\sqrt{3})$$

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\frac{\sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor}{n} \leq \frac{1}{p-1} \text{ und daher die gewünschte Ungleichung. } \square$$

② Seien $a, b \in \mathbb{Z}^+$ mit $a|b^2, b^2|a^3, a^3|b^4, \dots$ z.z.: $a=b$.

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

$$v_p(a) \leq v_p(b^2) \leq v_p(a^3) \leq v_p(b^4) \leq \dots \text{ bzw. äquivalent dazu}$$

$$v_p(a) \leq 2v_p(b) \leq 3v_p(a) \leq 4v_p(b) \leq \dots$$

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

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

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

was mit dem Grenzwert für $n \rightarrow \infty$ $v_p(a) = v_p(b)$ folgt. \square

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

Ang., es gäbe ein $p \in P$ mit $p | (n!+1) \wedge p | ((n+1)!+1)$.

Dann gilt auch $p | (n+1)!+1 - (n!+1) = n! \cdot n$

und somit, wegen $p \in P, p \leq n$. Damit erhalten wir aber $p | n!$, im Widerspruch zu $p | (n!+1)$. \square

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

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

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

Offensichtlich gilt $t = s$. Man gilt

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

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

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

⑧ z.z.: $s \notin P \Rightarrow 2^s - 1 \notin P$.

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

$$\begin{aligned} \textcircled{24} \bullet \left(\frac{70}{27}\right) &= \left(\frac{2}{27}\right) \cdot \left(\frac{5}{27}\right)^{1(4)} \cdot \left(\frac{7}{27}\right) = (-1)^{\frac{2 \cdot 2 - 1}{8}} \cdot \left(\frac{5}{5}\right)^{2(5)} \cdot \left(\frac{7}{7}\right)^{6(7)} \\ &\stackrel{\hookrightarrow 9 \in \mathbb{P}}{=} (-1)^{1176} \cdot \left(\frac{2}{5}\right) \cdot \left(\frac{6}{7}\right) = (-1)^3 \cdot \left(\frac{2}{7}\right) \cdot \left(\frac{3}{7}\right) = (-1) \cdot (-1)^6 \cdot \left[\left(\frac{7}{3}\right)\right]^{1(3)} = (-1)^2 \cdot \left(\frac{1}{3}\right) = \underline{1}. \\ \bullet \left(\frac{-14}{83}\right) &= \left(\frac{-1}{83}\right) \cdot \left(\frac{2}{83}\right) \cdot \left(\frac{7}{83}\right) = (-1)^{\frac{83-1}{2}} \cdot (-1)^{\frac{83^2-1}{8}} \cdot \left[-\left(\frac{83}{7}\right)\right]^{6(7)} = -\left(\frac{6}{7}\right) = -\left[\left(\frac{2}{7}\right) \cdot \left(\frac{3}{7}\right)\right]^{1^2=1(3)} \\ &\stackrel{\hookrightarrow 83 \in \mathbb{P}}{=} -\left[(-1)^{\frac{7^2-1}{8}} \cdot \left(-\frac{7}{3}\right)\right] = \left(\frac{7}{3}\right)^{1(3)} = \left(\frac{1}{3}\right) = \underline{1}. \\ \bullet \left(\frac{55}{89}\right) &= \left(\frac{11}{89}\right) \cdot \left(\frac{5}{89}\right) = \left(\frac{89}{11}\right)^{1(44)} \cdot \left(\frac{89}{5}\right) = \left(\frac{1}{11}\right) \cdot \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = (-1)^{2 \cdot \frac{5^2-1}{8}} = (-1)^6 = \underline{1}. \\ &\stackrel{\hookrightarrow 89 \in \mathbb{P}}{=} \equiv 1(4) \quad \equiv 1(4) \quad = 1 \end{aligned}$$

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

Ag., $x^2 = 55k - 1 \Leftrightarrow x^2 + 1 = 55k \Leftrightarrow x^2 \equiv -1 \pmod{55}$. [55 = 5 · 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
Wahrscheinlichkeit	$\frac{1}{8}$	$\frac{2}{8}$	$\frac{5}{11}$

Wann nächstes, übernächstes mal alle zu sehen?

Wir suchen also ein x mit
$$\begin{aligned} x &\equiv -1 \pmod{5} \\ x &\equiv -2 \pmod{8} \\ x &\equiv -8 \pmod{11}. \end{aligned}$$
 5, 8 und 11 sind paarweise

Seiterfreund, also können wir der christlichen Restauration anhängen.

Nur benötigen $b_1 \cdot 8 \cdot 11 \equiv 1 \pmod{5}$
 $b_2 \cdot 5 \cdot 11 \equiv 1 \pmod{8}$
 $b_3 \cdot 5 \cdot 8 \equiv 1 \pmod{11}$.
 Exemplarisch berechnen wir b_1 mit dem
 Euklidischen Algorithmus:

$$\begin{array}{l} 88 = 17 \cdot 5 + 3 \\ 5 = 1 \cdot 3 + 2 \\ 3 = 1 \cdot 2 + 1 \\ 2 = 1 \cdot 2 + 0 \end{array} \quad \begin{array}{l} 1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 5 = \\ = 2 \cdot (88 - 17 \cdot 5) - 5 = 2 \cdot 88 - 35 \cdot 5, \\ \text{also } 2 \cdot 88 \equiv 1 \pmod{5}, \text{ i.e. } b_1 = 2 = (88)^{-1} \pmod{5}. \end{array}$$

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

Da $x \bmod 440$ eindeutig bestimmt ist, ist das nächste gesuchte Jahr in 14 Jahren

und das darauffolgende in $14 + 440 = \underline{454}$.

(xiv.) Sei $p \in \mathbb{P}$, $p \equiv 1 \pmod{2}$ 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 $\text{ord}(g_1^k) = \frac{p-1}{2} < p$.

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

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. $v_p(a) \leq v_p(b) \leq v_p(c)$, dann ist

$$\begin{aligned} v_p\left(\frac{abc(a, b, c)}{(a, b)(b, c)(c, a)}\right) &= v_p(a) + v_p(b) + v_p(c) + \min_{i \in \{a, b, c\}} v_p(i) - \min_{i \in \{a, b\}} v_p(i) - \min_{i \in \{b, c\}} v_p(i) - \min_{i \in \{a, c\}} v_p(i) \\ &= v_p(a) + v_p(b) + v_p(c) + v_p(a) - v_p(a) - v_p(b) - v_p(a) \\ &= v_p(c) = \max_{i \in \{a, b, c\}} v_p(i). \quad \square \end{aligned}$$

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

$$x \equiv 1 \pmod{2}$$

$$x \equiv 3 \pmod{4} \Rightarrow x \equiv 1 \pmod{2} \checkmark$$

$$x \equiv 7 \pmod{8} \Rightarrow x \equiv 1 \pmod{2}, x \equiv 3 \pmod{4} \checkmark$$

$$x \equiv 5 \pmod{6} \Rightarrow x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3} \checkmark$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 8 \pmod{9} \Rightarrow x \equiv 2 \pmod{3} \checkmark$$

$$x \equiv 4 \pmod{5}$$

$$x \equiv 9 \pmod{10} \Rightarrow x \equiv 4 \pmod{5}, x \equiv 1 \pmod{2} \checkmark$$

$$x \equiv 6 \pmod{7}$$

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

$$= -1 \equiv 629 \pmod{630} \text{ und } x \text{ ist eindeutig}$$

$$\text{mod } 630, \text{ also } \boxed{x = 629}.$$

\rightsquigarrow

$$\begin{aligned} x &\equiv 6 \pmod{7} \\ x &\equiv 8 \pmod{9} \\ x &\equiv 9 \pmod{10} \end{aligned}$$

$$\begin{aligned} a_1 &= 6 \\ a_2 &= 8 \\ a_3 &= 9 \end{aligned}$$

$$\begin{aligned} m_1 &= 17 \\ m_2 &= 9 \\ m_3 &= 10 \end{aligned}$$

paarweise teilerfremd

$$b_1 \stackrel{!}{=} 90^{-1} \pmod{7}$$

$$b_2 \stackrel{!}{=} 70^{-1} \pmod{9}$$

$$b_3 \stackrel{!}{=} 63^{-1} \pmod{10}$$

$$\begin{aligned} 90 &= 12 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 7 - 1 \cdot 6 \\ &= 7 - (90 - 12 \cdot 7) \\ &= 13 \cdot 7 - 90 \end{aligned}$$

$$b_1 = -1$$

$$\begin{aligned} 70 &= 7 \cdot 9 + 7 \\ 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3 \cdot (9 - 7) \\ &= 70 - 7 \cdot 3 \cdot (9 - 7) \\ &= 70 \cdot 4 - 9 \cdot 31 \end{aligned}$$

$$b_2 = 4$$

$$\begin{aligned} 63 &= 6 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ &= 10 - 3 \cdot (63 - 6 \cdot 10) \\ &= 19 \cdot 10 - 3 \cdot 63 \end{aligned}$$

$$b_3 = -3$$

xxiii. $\exists \varphi: m, n \in \mathbb{N}: m|n \Rightarrow \varphi(m) | \varphi(n)$

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

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

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

$$\begin{array}{l} 1255 = 7 \cdot 177 + 16 \\ 177 = 11 \cdot 16 + 1 \\ 16 = 16 \cdot 1 + 0 \end{array} \quad \left| \quad \begin{aligned} 1 &= 177 - 11 \cdot 16 = 177 - 11 \cdot (1255 - 7 \cdot 177) \\ &= (-11) \cdot 1255 + 78 \cdot 177 \\ &\stackrel{\text{=: } x}{=} \qquad \qquad \qquad \stackrel{\text{=: } y}{=} \end{aligned}\right.$$

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

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

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

$$\cdot \sum_{k \geq 1} \left\lfloor \frac{500}{5^k} \right\rfloor = 100 + 20 + 4 = 124$$

$$\cdot \sum_{k \geq 1} \left\lfloor \frac{200}{5^k} \right\rfloor = 40 + 8 = 48$$

Somit ergibt $(500!)/(200!)$ auf $124 - 48 = \underline{\underline{76}}$ Stellen.

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

$$\begin{array}{l} 64 = 1 \cdot 40 + 24 \\ 40 = 1 \cdot 24 + 16 \\ 24 = 1 \cdot 16 + 8 \\ 16 = 2 \cdot 8 + 0 \end{array} \quad \left| \quad \begin{array}{l} 8 = 24 - 1 \cdot 16 = 24 - (40 - 24) = -40 + 2 \cdot 24 = -40 + 2 \cdot (64 - 40) \\ = 40 \cdot (-3) + 64 \cdot 2 \end{array} \right.$$

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

$$\bullet \quad 40x + 64y = 0 \Leftrightarrow \frac{x}{y} = -\frac{64}{40} = \frac{64/8}{40/8} = -\frac{8}{5} \Leftrightarrow \exists k \in \mathbb{Z}: x = k \cdot 8, y = -k \cdot 5$$

• Allg. Lsg.: $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -21 \\ 14 \end{pmatrix} + k \begin{pmatrix} 8 \\ -5 \end{pmatrix}$

(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 $(a^3 - b^3, a^2 - b^2) =: d$.

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

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

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 $d = \underline{a-b}$.

(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 $n_0 := \frac{((m+1)a+b)!}{a}$, 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} , $\underbrace{2 \leq k \leq m+1}_{m \text{ Zahlen}} \quad \square$