Sum of Us 2026

Kryptographie und Zahlentheorie

Aufgaben

8. September 2026

Liebe Teilnehmer*innen,

dieses Dokument enthält die Aufgaben für den ersten Teil des Internationalen Mathematikturniers 2026, die Sum of Us-Runde. Bevor ihr beginnt, empfehlen wir euch, die Anweisungen auf der nächsten Seite gründlich zu lesen.

Die Aufgaben wurden in diesem Jahr von Victor González Alonso, Michael J. Gruber, Thorsten Holm und Florian Leydecker von der Leibniz Universität Hannover gestellt.

Wir wünschen euch viel Erfolg!

Die Organisationsteams,
Stefan Hartmann & Rainer Kaenders (Universität Bonn)
Victor González Alonso, Michael J. Gruber, Thorsten Holm & Florian Leydecker (Leibniz Universität Hannover)
Niels Bonneux & Joeri Van der Veken (KU Leuven)
Manus Visser (Radboud Universiteit Nijmegen)
Michael Eichmair, Robin Gludovatz & Dmytro Rzhemuvskyi (Universität Wien)

Allgemeine Informationen

Antworten

- Schreibt eure Antworten auf die dafür vorgesehenen Antwortblätter.
- Vergesst nicht, auf jedes Antwortblatt eure Tischnummer zu schreiben!
- Reicht eure Antwortblätter bei den Korrektor*innen ein, lasst sie nicht auf dem Tisch liegen!

Punkteverteilung

Abschnitt 1: $10 + 20 + (20 + 30) + (20 + 20) = 120$

Abschnitt 2: $(15 + 25) + (15 + 15) = 70$

Abschnitt 3: $20 + 20 + 30 = 70$

Abschnitt 4: $20 + 20 + 40 = 80$

Abschnitt 5: $(20 + 10) + 30 = 60$

Abschnitt 6: $10 + 25 + 20 + 20 + 25 = 100$

Die Maximalpunktzahl für diese Runde ist 500 Punkte. Die Minimalpunktzahl ist 0. Wenn ihr eine Aufgabe falsch gerechnet habt und bei einer darauf aufbauenden Aufgabe eine folgerichtige Antwort gebt, wird diese Aufgabe trotzdem als falsch gewertet.

Erlaubte Hilfsmittel

- Schmierpapier, Stifte, Bleistift, Lineal.
- Das Vorbereitungsmaterial (ausgedruckt oder auf einem Tablet).

1. Leonhard, Pierre und ihre Tricks [120 Punkte]

Aufgabe 1 (10 Punkte)

Findet die kleinste natürliche Zahl, die durch alle Zahlen von 1 bis 15 teilbar ist. Gebt das Ergebnis in Dezimaldarstellung an.

Aufgabe 2 (20 Punkte)

Sei n eine natürliche Zahl. Bestimmt den größten gemeinsamen Teiler von $2026^{n+1} + 2$ und $2026^n + 2$.

Aufgabe 3 (20 + 30 = 50 Punkte)

(a) Für welche natürliche Zahlen n gilt $\varphi(n) = \frac{n}{3}$? (Gesucht ist eine Beschreibung anhand der Primfaktorzerlegung.)
(b) Findet die kleinste natürliche Zahl n mit $\varphi(n) < \frac{n}{4}$.

Aufgabe 4 (20 + 20 = 40 Punkte)

(a) Bestimmt den Rest bei Division mit Rest von $2^{1000000}$ durch 17.
(b) Bestimmt die letzten zwei Ziffern der Dezimaldarstellung von $7^{(7^7)}$.

2. Jan, Julia und EAN [70 Punkte]

Aufgabe 5 (15 + 25 = 40 Punkte)

(a) In der folgenden „European Article Number“ (EAN) ist eine Ziffer nicht lesbar. Welche Ziffer muss an der Stelle des Fragezeichens stehen, damit eine korrekte EAN entsteht?

9 7 8 ? 6 5 8 3 1 9 4 6 5

(b) Welche Ziffer fehlt in der folgenden Zahlenfolge, damit diese eine mit dem Luhn-Algorithmus erstellte Kreditkartennummer sein kann?

9 8 7 6 5 4 ? 2 1 9 8 7 6 5 4 3

Aufgabe 6 (15 + 15 = 30 Punkte)

Jan und Julia wollen einen Weitsprungwettbewerb organisieren. Für die Weitenmessung haben sie leider kein Maßband oder Zollstock, sondern nur zwei Stäbe der Längen $a = 851$ und $b = 713$ Zentimeter. Sie können also nur diese Abstände ggf. mehrmals nach vorne und nach hinten messen.

(a) Was ist der kleinste (positive) Abstand, den sie messen können?

(b) Sie können den Abstand $c = 276$ messen. Wie oft müssen sie den Stab der Länge 851 dafür einsetzen, wenn sie ihn möglichst selten einsetzen?

3. Annika, Bert und ihr geheimer Plan [70 Punkte]

Für die folgenden Aufgaben beschreiben wir zunächst die Ausgangssituation. Zwei Geschwister, Annika und Bert, wollen ihre Eltern mit einem Geschenk überraschen. Um ihre Ideen geheim austauschen zu können, benutzen sie eine Tausch-Chiffre. Dafür kodieren sie die Buchstaben mit den Zahlen 1 bis 26 nach folgender Tabelle:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Einfachheitshalber wollen sie nicht zwischen Groß- und Kleinbuchstaben unterscheiden, und sie brauchen auch keine Ziffern, Sonder- oder Leerzeichen. Sie wollen nur einzelne Wörter verschlüsseln. Die Verschlüsselungsfunktion ist als

$$\text{encrypt}_{(s,t)}(m) \equiv (m + s) \cdot t \bmod 26$$

gegeben, wobei der Schlüssel aus den festen Zahlen s und t besteht.

Die Geschwister einigen sich auf den Schlüssel $(s, t) = (5, 9)$.

Aufgabe 7 (20 Punkte)

Bert hat „WEIN“ als Idee und will dies Annika verschlüsselt mitteilen. Wie lautet die verschlüsselte Nachricht?

Aufgabe 8 (20 Punkte)

Annika hatte aber auch eine Idee und hat auf Berts Schreibtisch einen Zettel mit dem Wort „HGB“ hinterlassen. Was ist Annikas Idee?

Aufgabe 9 (30 Punkte)

Inzwischen haben die Kinder den Schlüssel geändert. Die Eltern hatten im Papiermüll einen Zettel mit „BZSABSF“ gefunden, und hatten auch gehört, wie Bert voller Aufregung es nicht aushalten konnte und Annika erzählte, dass es bald im THEATER ein wunderschönes Stück gibt. Wie lautet der neue Schlüssel (s, t)? Gebt s und t zwischen 0 und 25 an.

4. Hilda, Inga und ihr Tresor [80 Punkte]

Hilda und Inga haben einen kleinen gemeinsamen Tresor gekauft, der mit einer Kombination von zwei Ziffern gesichert ist. Sie können die Kombination frei auswählen, wollen aber diese weder laut sagen noch zueinander schriftlich senden. Sie beschließen, dafür das Diffie-Hellman-Verfahren zu nutzen, und zwar mit der Primzahl $p = 101$. So können sie die 100 möglichen Kombinationen mit den Zahlen $1, \ldots, 100$ modulo p kodieren (wobei 100 der Kombination 00 entsprechen soll). Als gemeinsame Basis wählen sie $g = 2$. Dann wählt jede von ihnen einen zufälligen Exponenten und schickt der anderen die resultierende Zahl. So haben beide genug Information, um den gemeinsamen Schlüssel zu bestimmen.

Aufgabe 10 (20 Punkte)

Hilda wählt 17 als Exponent. Welche zweistellige Zahl soll sie an Inga schicken?

Aufgabe 11 (20 Punkte)

Inga schickt Hilda die Zahl 53. Was ist die gemeinsame geheime Kombination für den Tresor?

Hilda ist neugierig und möchte wissen, welchen Exponenten Inga ausgewählt hatte, d.h. für welche Zahl x gilt $2^x \equiv 53 \bmod 101$. Dafür beschließt sie, den Babystep-Giantstep-Algorithmus anzuwenden.

Zuerst berechnet sie $m = \sqrt{p-1} = \sqrt{100} = 10$. Das war einfach! Dann soll sie die zwei Spalten der Tabelle ausfüllen, bis sie glücklicherweise schon nach wenigen Schritten in der zweiten Spalte die Lösung findet.

Aufgabe 12 (40 Punkte)

Füllt die Tabelle solange aus, bis Ingas Exponent x gefunden ist. Welche Basis c verwendet ihr in der zweiten Spalte? Wie lautet der Exponent x?

i, j	$2^j \bmod 101$	$bc^i \bmod 101$
0		
1		
2		
3		
4		
5		
6		
7		
8		
9		

5. Jakob, Lisa und ihr geheimes Ziel [60 Punkte]

Jakob und Lisa, die Eltern von Annika und Bert, wollen im Urlaub mit der Familie in ein Land der Europäischen Union reisen. Um das Reiseziel vor den Kindern geheim zu halten, nutzen Sie folgende Codes für die Länder, wandeln jeden Buchstaben in eine Zahl zwischen 1 und 26 laut folgender Tabelle um, und dann verschlüsseln sie die Zahlen mit einem ElGamal-Verfahren.

Österreich	AT	Belgien	BE	Bulgarien	BG
Zypern	CY	Tschechien	CZ	Dänemark	DK
Deutschland	DE	Estland	EE	Griechenland	EL
Spanien	ES	Finnland	FI	Frankreich	FR
Kroatien	HR	Ungarn	HU	Irland	IE
Italien	IT	Litauen	LT	Luxemburg	LU
Lettland	LV	Malta	MT	Niederlande	NL
Polen	PL	Portugal	PT	Rumänien	RO
Schweden	SE	Slovenien	SI	Slovakei	SK

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Für das ElGamal-Verfahren wählen sie die Primzahl $p = 29$ und $g = 3$ als Basis. Sie wählen jeweils einen geheimen Exponenten.

Jakob will Lisa Portugal vorschlagen. Dafür wandelt er die zwei Buchstaben „PT“ in das Paar $(16, 20)$ um, und verschlüsselt jede Zahl. Jakob gibt Lisa einen Zettel mit den zwei Zahlen. Leider ist Jakobs Handschrift sehr schlecht und nur die erste Zahl ist zu erkennen: eine 11. Damit könnt ihr aber auch die zweite Zahl erraten.

Aufgabe 13 (20 + 10 = 30 Punkte)

(a) Was ist die geheime gemeinsame Zahl s von Jakob und Lisa?
(b) Was ist die zweite Zahl auf dem Zettel?

Lisa gefällt der Vorschlag nicht so gut und sie macht einen Gegenvorschlag mit folgenden verschlüsselten Zahlen: $(4, 27)$.

Aufgabe 14 (30 Punkte)

Wohin möchte Lisa lieber reisen? Gebt den Code für das Land an.

6. Carl, Daniel und ihr skate date [100 Punkte]

Carl und Daniel treffen sich jeden Nachmittag nach der Schule zwischen 14 und 15 Uhr am Skaterplatz. Die genaue Uhrzeit entscheiden sie abwechselnd. Wer heute entscheiden darf, gibt dem anderen einen Zettel mit einer Zahl zwischen 0 und 59 (die Minuten nach 14 Uhr). Zum Beispiel bedeutet „17“, dass sie sich um 14:17 treffen.

Seit sie in der Mathe-AG Verschlüsselung mit RSA kennengelernt haben, sind sie davon begeistert und wollen das Verfahren für ihre Treffen nutzen. Sie überlegen, die Zahlen durch das RSA-Verfahren mit Moduln $n \geq 60$ zu verschlüsseln und das Ergebnis auf den Zettel zu schreiben.

Aufgabe 15 (10 Punkte)

Carl will seinen öffentlichen Schlüssel wählen und ist unentschlossen zwischen den Möglichkeiten $(n, e) = (77, 25)$ und $(n, e) = (65, 13)$. Daniel merkt aber, dass nur eine der zwei Möglichkeiten überhaupt in Frage kommen kann. Welche ist es?

Nach einigen Überlegungen wählen sie folgende öffentliche Schlüssel:

$$\text{Carl: } (n_C, e_C) = (65, 5) \quad \text{und} \quad \text{Daniel: } (n_D, e_D) = (77, 37).$$

Aufgabe 16 (25 Punkte)

Was ist der private Schlüssel von Daniel?

Aufgabe 17 (20 Punkte)

Daniel will sich heute um 14:11 treffen. Was soll er auf den Zettel für Carl schreiben?

Aufgabe 18 (20 Punkte)

Carl gibt Daniel am nächsten Tag einen Zettel mit „13“. Wann treffen sie sich?

Carl und Daniel wollen auch Elene mit in ihr System aufnehmen, um auch mal Verabredungen zu dritt zu organisieren. Dafür wählt Elene folgenden öffentlichen Schlüssel:

$$\text{Elene: } (n_E, e_E) = (65, 11).$$

Aufgabe 19 (25 Punkte)

Daniel entscheidet heute die Uhrzeit. Dafür gibt er Carl einen Zettel mit „62“ und Elene einen Zettel mit „23“.
Oscar fängt die Zettel ab und merkt, dass er ohne viel Aufwand die Uhrzeit des Treffens bestimmen kann. Welche Uhrzeit hat Daniel ausgewählt?