Arithmetics.

Question 1.
Find integers $s, t \in \mathbb{Z}$ such that the equation $gcd(a, b) = s \cdot a + t \cdot b$ holds for the following pairs:

a) $(a, b) = (45, 10)$

b) $(a, b) = (13, 11)$

c) $(a, b) = (13, 12)$

Question 2.
Show that $gcd(n, m) = gcd(n + m, m)$ for all $n, m \in \mathbb{N}$.

Question 3.
Find the set of all solutions to the congruence $17(2x + 5) - 4 \equiv 2x + 4 \pmod 5$. Then project the congruence into $\mathbb{Z}_5$ and solve the resulting equation in $\mathbb{Z}_5$. Compare the results.

Question 4.
Consider modular 5 arithmetic, and the set $S = \{(0, 0), (1, 1), (2, 2), (3, 2)\}$. Find a polynomial $P \in \mathbb{Z}_5[x]$ such that $P(x_i) = y_i$ for all $(x_i, y_i) \in S$.

Algebra.

Question 5.
Consider the multiplicative group $\mathbb{Z}^*_{13}$ of modular 13 arithmetic. Choose a set of 3 generators of $\mathbb{Z}^*_{13}$, define its associated Pedersen hash function, and compute the Pedersen hash of $(3, 7, 11) \in \mathbb{Z}_{12}$.

Question 6.
Consider the ring of modular 6 arithmetics $(\mathbb{Z}_6, +, \cdot)$. Show that $(\mathbb{Z}_6, +, \cdot)$ is not a field.

Question 7.
Consider the prime field $\mathbb{F}_{13}$. Compute the Legendre symbol $\left(\frac{x}{13}\right)$ and the set of roots $\sqrt{x}$ for all elements $x \in \mathbb{F}_{13}$.

Elliptic Curves.

Question 8.
Look up the definition of curve `BLS12-381`, implement it in SageMath, and compute the number of all curve points.

Question 9.
Compute the following expression for projective points on $E_1(\mathbb{F}_5\mathrm{P}^2)$ using the projective goup law:

a) $[0 : 1 : 0] \oplus [4 : 3 : 1]$

b) $[0 : 3 : 0] \oplus [3 : 1 : 2]$

c) $-[0 : 4 : 1] \oplus [3 : 4 : 1]$

d) $[4 : 3 : 1] \oplus [4 : 2 : 1]$

and then solve the equation $[X : Y : Z] \oplus [0 : 1 : 1] = [2 : 4 : 1]$ for some point $[X : Y : Z]$ from the projective short Weierstrass curve $E_1(\mathbb{F}_5\mathrm{P}^2)$.

Question 10.
Consider the elliptic curve `secp256k1` and show that `secp256k1` is not a Montgomery curve.

Question 11.
Consider the `Tiny-jubjub` curve. Show that the polynomial $t^4 + 2 \in \mathbb{F}_{13}[t]$ is irreducible. Then write a SageMath program to implement the finite field extension $\mathbb{F}_{13^4}$, implement the curve extension $TJJ\_13(\mathbb{F}_{13^4})$ and compute the number of curve points.

Question 12.
Consider the curve `alt_bn128` and the generators g_1 and g_2 of $\mathbb{G}_1[p]$ and $\mathbb{G}_2[p]$. Write a SageMath program that computes the Weil pairing $e(g_1, g_2)$.

Statements.

Question 13.
Consider modular 6 arithmetic (working in $\mathbb{Z}_6$), the alphabet $\Sigma = \mathbb{Z}_6$ and the following decision function:

$$R : \Sigma^* \to \{true, false\} \; ; \; < x_1, \ldots, x_n > \mapsto \begin{cases} true & n = 1 \text{ and } 3 \cdot x_1 + 3 = 0 \\ false & else \end{cases}$$

Compute all words in the associated language L, provide a constructive proof for the statement "There exists a word in L" and verify the proof.

Question 14.
Consider the `Tiny-jubjub` curve together with its twisted Edwards addition law.

a) Define an instance alphabet Σ_I, a witness alphabet Σ_W, and a decision function R_{add} with associated language L_{add} such that a string $(i\,; w) \in \Sigma_I^* \times \Sigma_W^*$ is a word in L_{add} if and only if i is a pair of curve points on the `Tiny-jubjub` curve in Edwards form, and w is the sum of those curve points.

b) Choose some instance $i \in \Sigma_I^*$, provide a constructive proof for the statement "There is a witness $w \in \Sigma_W^*$ such that $(i\,; w)$ is a word in L_{add}", and verify that proof.

c) Find some instance $i \in \Sigma_I^*$ such that i has no knowledge proof in L_{add}.

d) Define an R1CS such that words in L_{add} are in 1:1 correspondence with solutions to this R1CS.

Circuit compilers.

Question 15.
Let $\mathtt{F} = \mathbb{F}_{13}$ be the modular 13 prime field and $x \in \mathtt{F}$ some field element. Define a statement in the `PAPER` language from the MoonMath Manual such that given instance x a field element $y \in \mathtt{F}$ is a witness for the statement if and only if y is the square root of x.

Brain-compile the statement into a circuit and derive its associated Rank-1 Constraint System. Consider the instance $x = 9$ and compute a constructive proof for the statement.

Question 16.
Let $\mathbb{F}$ be a finite field. Derive algebraic circuits and associated Rank-1 Constraint Systems for the following operators: NOR, XOR, NAND, EQU.

Question 17.
Let $\mathbb{F}$ be a field. Define a circuit that enforces field inversion for a point of a twisted Edwards curve over $\mathbb{F}$.