Midterm Test (sample)

programming part

- Maximum 30 points (≥ 12 required).
- (There are more exercises than 30 points, to allow some room for errors.)
- Allowed: Sage, the class website, your own notes, your class work, Sage website.
- Forbidden: other internet, other person, artificial intelligence.
- Print the result of all exercises.
- The solutions must run quickly (within a couple of seconds).
- Upload the solutions in a single `.sage` file (not `.zip`).

3. Find all pairs of adjacent prime numbers below 1000 whose distance is greater than of any other adjacent prime numbers before: $(2,3),(3,5),(7,11),(23,29),\ldots$. *(8 p)*

4. Two different positive integers, a and b are called *amicable numbers* if the sum of the proper divisors of either number equals the other, i.e. $s(a) = b$ and $s(b) = a$, but $a \neq b$. For example, 220 and 284 are amicable numbers. Print all pairs of amicable numbers up to 10000 (each pair exactly once). *(9 p)*

5. Using the modular inverse, solve multiple linear congruences of the form $ax \equiv b \pmod{m}$ at the same time, where a and m are *coprime*, and they are fixed for all congruences, and only b differs.

- Take advantage of the fact that there a multiple similar congruences, i.e. don't solve each linear congruence separately.
- The function receives three parameters: the single a and m, and the list of possible b's. It returns the list of solutions, each between 0 and $m-1$, corresponding to the list of b values.
- Don't use the mathematical functions of Sage.
- Test the function for $\{3x \equiv 0\ (10),\ 3x \equiv 1\ (10),\ \ldots,\ 3x \equiv 9\ (10)\}$ (i.e. $a = 3$, $m = 10$ and $b \in \{0,1,2,\ldots,9\}$), and also for the following congruences:

$$\{1101200990981x \equiv b \pmod{1234567654321} \mid b = 0,1,\ldots,9\}.$$

(9 p)

6. Break the Diffie–Hellman key exchange (if possible), i.e. write a function that tries to calculate the common secret from only the publicly visible data, using discrete logarithm. Test the solution on multiple set of parameters (with known solution), including for $p = 23, g = 5$ and $p = 12345678923, g = 5$. *(9 p)*