Endterm Test (sample)

programming part

- Maximum 30 points ($\geq$ 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. a) Write a function that calculates the polynomial $p_n = x^{n-1} + \ldots + x^2 + x + 1 \in \mathbb{Z}[x]$ for a given n. (The type of the result must be polynomial.)

b) Print all n between 1 and 20 for which the above p_n is irreducible. (Hint: use the factorization.) What are these numbers? *(9 p)*

4. a) Modify the RSA implementation so that the public exponent is the fixed constant $e = 65537$, and if it doesn't satisfy the criteria of RSA, then generate the prime numbers again. Let the prime numbers be random numbers below $L = 2^{50}$. Encrypt a message using the public key.

b) Break RSA using the `factor()` function, i.e. restore the message from the cyphertext created above, using only the public key. (Note: the given L is small enough for this.) *(9 p)*

5. Let R be a *commutative ring with identity*, given by the list of its elements (e.g. **not** `Zmod(7)`, but `list(Zmod(7))`). Don't use **anything else** about the elements than the two ring operations (`a + b` and `a * b`), equality comparison (`a == b`, `a != b`), and the abstract fact that they form a commutative ring with identity. (In particular, we don't know *which* element is the identity.)

a) Write a function that gets the ring R and two elements $a, b \in R$, and decides whether $a \mid b$. Using this function, print which $a \in \mathbb{Z}_{10}$ are divisible by $\overline{4} \in \mathbb{Z}_{10}$.

b) Write a function that gets the ring R, and it returns the list of *units* in R. Using this function, print the units of $\mathbb{Z}_{10}$. *(9 p)*

6. For all finite fields with at most ten elements, print the polynomial for which all elements of the field are roots (as simple roots, and without any extra factors). *(8 p)*