Problem 1. (prove Proposition 7.5) Prove Proposition 7.5 from the lecture, which gives a possibility to generate a primitive element modulo $n$:

Let $p > 3$ be prime, $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ the prime factorization of $p - 1$. Then,

$$a \in \mathbb{Z}_p^*$$

is a primitive element modulo $p$ $\iff$ $a^{p-1} \not\equiv 1 \pmod{p}$ for all $i \in \{1, \ldots, k\}$.

Problem 2. (calculating the basis) Given $a^{13} \equiv 17 \pmod{31}$, calculate the basis $a$.

Problem 3. (Diffie-Hellman key exchange) Alice and Bob perform a Diffie-Hellman key exchange with prime $p = 107$ and primitive element $a = 2$. Alice chooses the random number $x_A = 66$ and Bob the random number $x_B = 33$.

a) Calculate the shared key for both users.

b) Show that $b = 103$ is also a primitive element mod $p$.

Problem 4. (Proof of 8.3) Let $n = p \cdot q$, $p \neq q$ be prime and $x$ a non-trivial solution of $x^2 \equiv 1 \pmod{n}$, i.e., $x \not\equiv \pm1 \pmod{n}$.

Then

$$\gcd(x + 1, n) \in \{p, q\}$$