Introduction to Algebra **Example sheet 6** **Autumn 2022**

1. Let $n \geq 2$ be an integer and a another such that $(a, n) = 1$. Show that $a^k \equiv 1 \pmod{n}$ if and only if $o_n(a)|k$.

2. As a consequence of the previous exercise show that $a^k \equiv a^l \pmod{n}$ if and only if $k \equiv l \pmod{o_n(a)}$.

3. Show that there is no primitive root modulo 2^a if $a \geq 3$. (Use induction on a. We know that for $a = 3$ there is no.)

4. Show that if $n = n_1 n_2$, where $(n_1, n_2) = 1$ and $(\varphi(n_1), \varphi(n_2)) > 1$ then there is no primitive root modulo n. (Our agrument was as follows: if $(g, n) = 1$ then $g^{\varphi(n_1)} \equiv 1 \pmod{n_1}$ and $g^{\varphi(n_2)} \equiv 1 \pmod{n_2}$, so $g^l \equiv 1 \pmod{n_1}$ and $g^l \equiv 1 \pmod{n_2}$ for the least common multiple $l = [\varphi(n_1), \varphi(n_2)] < \varphi(n_1)\varphi(n_2) = \varphi(n)$.)

5. Show that modulo a prime the product of two quadratic nonresidues is a quadratic residue!

6. Show that -1 is a quadratic residue modulo p for primes $p \equiv 1 \pmod{4}$ and -1 is a quadratic nonresidue if $p \equiv 3 \pmod{4}$.

7. Suppose $o_n(a) = u$; $o_n(b) = v$.

(i) Show that $o_n(a^k) = \frac{u}{(u,k)}$.

(ii) Show that $o_n(ab)|[u, v]$.

(iii) If further $v|u$ and $v < u$ then $o_n(ab) = u$.

8. Show that modulo a prime greater than 3 the sum of quadratic residues is 0.

9. Divide $x^4 - 2x + 5$ with remainder by
a) $x^2 - x + 2$,
b) $x + 1$,
c) $(x + 1)^2$ and
d) $x^2 - 1$!

10. What is the greatest common divisor of $a(x) = x^3 - 2x^2 + x - 1$ and $b(x) = x^2 + 2$? Find polynomials p and q such that $\gcd(a, b) = pa + qb$.

11. What are the irreducible polynomials

(i) of degree 2, 3 and 4 over $\mathbb{F}_2$ and

(ii) of degree 2 and 3 over $\mathbb{F}_3$?

12. What is the gcd and lcm of $(x-2)^2(x+\pi)^5(x-3)(x-4)^2$ and $(x-2)(x+\pi)^2(x-3)^3$?

13. How to choose $a \in \mathbb{R}$ such that $(x + 1)^2 | x^5 - ax^2 - ax + 1$?

14. Show that a polynomial of degree 3 with no root is irreducible.

15. Show that every polynomial in $\mathbb{R}[x]$ of odd degree has at least one real root!