Number Theory and Cryptography
Math UN3020
New York, 2023/04/05

EXERCISE SHEET 11

Quadratic Residues

Exercise 1 (11 points)**.** For an integer n, consider the set of positive divisors of n, defined as

$$\mathrm{Div}_n^+ := \{\ d \in \mathbb{Z} \ \mid\ d > 0 \quad \text{AND} \quad d \mid n\ \}\,.$$

Consider the function

$$\tau(n) := \#\mathrm{Div}_n^+\,.$$

Prove that, if m and n are coprime, we have

$$\tau(mn) = \tau(m)\tau(n)\,.$$

Exercise 2 (11 points)**.** Let p be a prime, and $b \in \mathbb{Z}$ be such that $\gcd(b, p^\alpha) = p^s > 1$. Prove that

1. If $b \equiv 0 \pmod{p^\alpha}$, then b is a quadratic residue modulo p^α.
2. If $b \not\equiv 0 \pmod{p^\alpha}$ and s is odd, then b is not a quadratic residue modulo p^α.
3. If $b \not\equiv 0 \pmod{p^\alpha}$ and s is even, then b is a quadratic residue modulo p^α if and only if $\frac{b}{p^s}$ is a quadratic residue modulo p.

(Hint:) Write the binomial equation $x^2 \equiv b \pmod{p^\alpha}$ and apply the method for the case when b is not invertible.

Exercise 3 (16 points)**.** Use Euler's Criterion to determine if the following are quadratic residues:

(a) 2 modulo 31.

(b) 2 modulo 43.

(c) 3 modulo 31.

(d) 7 modulo 29.

Exercise 4 (11 points)**.** Let n be an even positive integer, and p be a prime such that $p \mid n^2 + 1$. Prove that

$$p \equiv 1 \pmod{4}.$$

(Hint:) First, show that

$$\left(\frac{-1}{p}\right) = \left(\frac{n^2}{p}\right).$$

Exercise 5 (11 points)**.** Prove that there are infinitely many primes congruent to 1 modulo 4.
(Hint:) Write a proof similar to Euclid's proof. Use Exercise 4.