

**MATH 332 - ALGEBRA AND NUMBER THEORY**  
**SECOND MIDTERM - PRACTICE**

**Theory Question 1.** Write a precise statement for Fermat's Little Theorem and prove it.

**Theory Question 2.** Write a precise statement for Euler's theorem and prove it.

**Theory Question 3.** Prove that every prime number has a primitive root (you may use Lagrange's theorem on the number of roots of polynomials over fields, but you certainly need to state it precisely and correctly).

**Theory Question 4.** Write precise statements for the following theorems/conjectures (you do not need to prove them):

- (1) Law of Quadratic Reciprocity.
- (2) Prime Number Theorem.
- (3) Dirichlet's theorem on primes in arithmetic progressions.
- (4) Goldbach's Conjecture.
- (5) Twin Prime Conjecture.
- (6) Fermat's Last Theorem.

**Theory Question 5.** Write a precise definition of the following:

- (1) Quadratic residue modulo  $m$ .
- (2) Legendre symbol.
- (3) Mersenne prime.
- (4) Perfect number.

**Remark.** You may use any of the theorems stated in Theory Question 4 in solving the following problems. But make sure you name the theorems you use!

**Problem 1.** Find the following values of the Legendre symbol:

$$\left(\frac{113}{127}\right), \quad \left(\frac{113}{131}\right), \quad \left(\frac{113}{137}\right), \quad \left(\frac{210}{229}\right).$$

The numbers 113, 127, 131, 137 are primes.

**Problem 2.** Find all solutions (if any) of the equations:

$$x^2 + 21x + 82 \equiv 0 \pmod{137}, \quad x^2 + 5x + 3 \equiv 0 \pmod{37}, \quad x^2 + 5x + 7 \equiv 0 \pmod{37}$$

**Problem 3.** Find all solutions (if any) of the equation  $x(x + 35) = 22 + 82x^7$  in  $\mathbb{Z}/41\mathbb{Z}$ .

**Problem 4.** Find a primitive root for  $m = 505447028499293771$  without using a calculator. Hint:  $m$  is a power of one prime.

**Problem 5.** The following is a table of powers of 2 modulo 13:

$x$	$x^2$	$x^3$	$x^4$	$x^5$	$x^6$	$x^7$	$x^8$	$x^9$	$x^{10}$	$x^{11}$	$x^{12}$
2	4	8	3	6	12	11	9	5	10	7	1

- (1) Find all primitive roots of 13. How many are there?
- (2) Use the table to find all quadratic residues modulo 13.
- (3) Use the table to construct a table of indices for 13 in base 2.
- (4) Find all solutions to the following congruences:

$$10x^5 \equiv 1 \pmod{13}, \quad 3x^6 \equiv 11 \pmod{13}, \quad 3x^7 \equiv 7x^3 \pmod{13}.$$

(5) Does  $m = 11 \cdot 13$  have a primitive root? Find one solution of the congruence

$$10x^5 \equiv 1 \pmod{143}.$$

**Problem 6.** Let  $C$  be the unit circle in  $\mathbb{R}^2$ , defined by  $x^2 + y^2 = 1$ .

- (1) Find four different rational points in the first quadrant of the unit circle, other than  $(1, 0)$  and  $(0, 1)$ . In other words, find four different solutions of  $x^2 + y^2 = 1$  with  $x, y \in \mathbb{Q}$  and  $x, y > 0$ . Of course  $(a, b)$  and  $(b, a)$  count as the same solution, and  $x, y$  should be fractions in lowest terms.
- (2) Find a formula for **all** the rational points in the unit circle.

**Problem 7.** Find **all** the rational points in the curve  $x^n + y^n = 1$  and prove that you have found all of them. Hint: you may assume any theorem in Chapter 8.

**Problem 8.** Prove that the equation  $x^2 - 137y^2 = 113$  has no integer solutions.

**Problem 9.** For what primes  $p$  is  $-5$  a quadratic residue? For what primes  $p$  is  $-10$  a quadratic residue? Are there infinitely many primes  $p$  such that  $-10$  is a quadratic residue modulo  $p$ ?

**Problem 10.** Are there two odd primes  $p, q$  such that  $p \neq q$ ,  $p \equiv q \equiv 3 \pmod{4}$  and such that  $p$  is a quadratic residue modulo  $q$  and  $q$  is a quadratic residue modulo  $p$ ? What is the smallest odd prime  $q$  such that  $3$  is a quadratic residue modulo  $q$  and  $q$  is a quadratic residue modulo  $3$ ?

**Problem 11.** Use induction to show that, for all  $n$ , there exists a set of  $n$  distinct odd primes  $\{p_1, \dots, p_n\}$  such that

$$\left(\frac{p_i}{p_j}\right) = 1$$

for all  $1 \leq i, j \leq n$  with  $i \neq j$ , i.e. every prime in the list is a quadratic residue modulo any other prime in the list.

**Problem 12.** Assume that  $x^p + y^p = z^p$  has no solutions in non-zero integers for any prime  $p$  and then prove Fermat's Last Theorem. In other words, show that in order to prove Fermat's Last Theorem it suffices to show that  $x^p + y^p = z^p$  has no non-zero solutions for prime exponents.

**Problem 13.** Show that  $x^5 + y^5 = 3 + 11z^5$  has no solutions in integers  $x, y, z$ .

**Problem 14.** Recall that if  $q$  is a divisor of  $2^p - 1$ , for an odd prime  $p$ , then  $q$  is of the form  $2kp + 1$  for some  $k \geq 1$ .

- (1) Explain why the Mersenne numbers  $M_4, M_6, M_9$  and  $M_{11}$  are **not** prime.
- (2) Prove that  $M_{23}$  is not prime.

**Problem 15.** Prove that for any natural number  $n \geq 1$ ,  $3^{6n} - 2^{6n}$  is never prime.

**Problem 16.** Find as many prime factors as possible of the number  $N = 3^{101} - 1$ .

**Problem 17.** Let  $a, n > 0$  be natural numbers. Find as many prime factors as possible of the number  $N = a^{n!} - 1$ .

**Problem 18.** Suppose that  $p$  and  $q$  are twin primes. Is it possible that  $2$  is a quadratic residue for both  $p$  and  $q$ ? Is  $2$  necessarily a quadratic residue of  $p$  or  $q$ ? Find twin primes  $p$  and  $q$  such that  $2$  is a quadratic residue modulo  $p$  but not modulo  $q$ .

**Problem 19.** Are there infinitely many primes of  $p$  such that  $(p, p+2, p+4)$  are all primes? Why? Are there infinitely many primes  $p$  such that  $(p, p+2, p+6, p+8, p+12, p+14)$  are all primes? Why? Make a generalization of the Twin Prime conjecture for 6-tuples, i.e. make an educated conjecture for the existence of 6-tuples of primes.