

MA 341 - Number Theory

Sample Questions from Previous Exams on Exam 3 Topics

1) A number a is a **cubic residue** ($\text{mod } p$) if $x^3 \equiv a \pmod{p}$ has a solution.

- a) Which values of $a \pmod{p}$ are cubic residues when $p \equiv 2 \pmod{3}$?
- b) Prove your answer in a).

2) Consider

$$x^{58} \equiv 1393 \pmod{1453}$$

1453 is prime and 2 is a primitive root ($\text{mod } 1453$). $\text{ind}_2(1393) = 605$.

Does the above congruence have a solution? Why or why not?

If it has a solution give all solution(s) to the above congruence in terms of indices.

3) $p = 313$ is a prime.

- a) Find the value of the Legendre symbol

$$\left(\frac{11}{p}\right)$$

b)

$$11^{104} \equiv 214 \pmod{p}$$

$$11^{24} \equiv 113 \pmod{p}$$

Is 11 a primitive root for p ? Why or why not?

- c) 10 is a primitive root for $p = 313$. Find another primitive root for p , not equal to 10 ($\text{mod } p$) or 11 ($\text{mod } p$).

4) $p = 73553$ is prime. Does the congruence

$$x^2 - 3x + 7 \equiv 0 \pmod{73553}$$

have solutions? Why or why not?

5) $\text{ord}_{121}(2)$ is the **smallest** exponent e such that

$$2^e \equiv 1 \pmod{121}$$

- a) What are the possible values of $\text{ord}_{121}(2)$? Explain.
- b) Determine which of the possible values you gave in a) is the actual value of $\text{ord}_{121}(2)$.

6) Does the congruence

$$x^2 \equiv 58 \pmod{77}$$

have solutions? Why or why not? If it has solutions how many does it have? If there are solutions, find one.

7) Alice wants to use RSA encryption and she chooses $m = 71 \cdot 79$.

a) Calculate the value $\phi(m)$.

b) She decides to choose $e = 7$ as her encryption key. She now needs to find her decryption key d so that

$$(a^e)^d \equiv a \pmod{m}$$

for any message a she is sent. (Assume the message is broken up into blocks so that the numbers representing each block are less than m). Can she do this? If she can find the value of d and if she can't explain why not.

8) For what primes p is -7 a quadratic residue $(\text{mod } p)$?

Note: Your answer should be a set of congruences $(\text{mod } 28)$, and should be explained for general p using quadratic reciprocity.

9) Let p be an odd prime, g a primitive root $(\text{mod } p)$, and $\text{ind}(a) = \text{ind}_g(a)$ be the index of a $(\text{mod } p)$ for base g .

a) What is the value of $\text{ind}(-1)$? Give reasons for your answer that work for any odd prime p .

b) Show

$$x^4 \equiv -1 \pmod{p}$$

has a solution if and only if $p \equiv 1 \pmod{8}$. You must give an argument that works for general primes p .

10) 1279 is prime.

a) Does $x^2 \equiv 23 \pmod{1279}$ have solutions? Why or why not?

b) If there are no solutions find a value a , $a \neq b^2$ for $b \in \mathbf{Z}$ such that $x^2 \equiv a \pmod{1279}$ has solutions.

c) For a value a such that $x^2 \equiv a \pmod{1279}$ has solutions explain how to find them without testing values of x , $1 < x < 1279$ until you find one. Give a **formulain** terms of your value of a , but do **not** apply the method of successive squaring o calculate the exact value.

d) Explain why your formula works.

11) Use the definition of the Jacobi symbol to show the following:

a) Let $n = p^2$ for p an odd prime. Let a be **any** integer satisfying $1 < a < n$ and $\text{gcd}(a, n) = 1$. Show

$$\left(\frac{a}{n}\right) = 1$$

b) Let $n = p_1 \cdot p_2 \cdots p_r$ where the p_i are **distinct** odd primes. Show there is at least one value of a satisfying $1 < a < n$, $\text{gcd}(a, n) = 1$, **and**

$$\left(\frac{a}{n}\right) = -1$$

HINT: Use the Chinese Remainder Theorem.