

Elementary Number Theory — Math 364.3 (02) T2, 1998-99

Final Exam (Saturday, April 24, 1999)**Time: 3 hours****This is a “closed book” examination.**

Show all your work to receive full credit! For the solution of a problem, you may use the assertion of every foregoing part of a problem. The marks are indicated in square brackets []. The maximum number of marks you may earn is 100.

1) Give the definition of:

- a) “prime number”, [3]
 b) “least common multiple of a and b ”, [3]
 c) “primitive root modulo m ”. [5]

2) a) Prove by induction that the following formula holds for all positive integers n : [5]

$$1 \cdot 1! + 2 \cdot 2! + \dots + n \cdot n! = (n + 1)! - 1.$$

b) Prove that $3 \mid (4^n - 1)$ for all positive integers n . [5]

3) a) Compute: [3]

$$i) \varphi(11), \quad ii) \varphi(100), \quad iii) \varphi(2^3 \cdot 3^4 \cdot 7^2 \cdot 11).$$

b) How many elements in any reduced residue system (mod m) have

- a) order 6 for $m = 13$, b) order 8 for $m = 17$,
 c) order 5 for $m = 19$, d) order 4 for $m = 8$? [6]

4) Make a table of indices for modulus 11 and primitive root 2. [4]

Using these indices, solve the following problems:

a) Compute the least residues (mod 11) of the following integers: [5]

$$i) 8 \cdot 9 \quad ii) 3 \cdot 5 \cdot 8 \quad iii) 5^{10} \quad vi) 5^7 \quad v) 7^5.$$

b) Find the inverses of 2, 3, 5 and 7 (mod 11) (explain!). [3]

c) Find all primitive roots (mod 11) between 0 and 11. [3]

d) Find all positive integers below 11 which have order 5 (mod 11). Then find **all** integers which have order 5 (mod 11). [3]

e) Solve the congruence $5x \equiv 8 \pmod{11}$. [2 bonus]

/...2

5) a) Solve the following systems the easiest possible way: [6]

$$\begin{array}{ll} i) & x \equiv 2 \pmod{3} \\ & x \equiv 2 \pmod{5} \\ & x \equiv 2 \pmod{7} \\ & 0 < x < 200 \\ ii) & z \equiv 0 \pmod{9} \\ & z \equiv 3 \pmod{2} \\ & z \equiv 10 \pmod{5} \\ & 0 < z < 90 \end{array}$$

b) The University of Saskatchewan was given some extra money by the government of Saskatchewan. It was given to the College of Arts and Science, the College of Engineering, and the College of Education in order to improve mathematics education. When the three colleges divided it as evenly as possible among themselves (working only with multiples of a thousand Dollars in order to keep computations simple), \$1000 was left over. They gave them to the USSU, who immediately used them to buy a new TV for Louis'. But then the library spoke up, demanding its share of the money in order to buy math books. So they divided the money by four. When they did this as evenly as possible, \$2000 was left over, which was immediately invested in the new math help center. In the meanwhile, the College of Arts and Science had split into a College of Arts and a College of Science. So they had to divide the money by five. Now \$3000 was left over. Assuming that the government always gives the least possible amount of money to universities, determine how much money the university had received. [8]

c) Solve the following system: [4 bonus]

$$\begin{array}{l} 3x \equiv 9 \pmod{6} \\ 2x \equiv 1 \pmod{5} \\ x \equiv 2 \pmod{7} \\ 0 \leq x \leq 210. \end{array}$$

6) Do either part (A) or part (B) or part (C). [12]

(A): Prove Wilson's Theorem.

(B): Describe in up to 5 sentences the connection of Euler's Theorem with the theory of groups. Which theorem on subgroups can be used to prove Euler's Theorem? State both theorems.

(C): Describe in up to 5 sentences the basic ideas of the RSA cryptosystem. (Do not describe the procedures in detail.) What does the security of the system rely on? What is meant by "public key"?

7) Let p be any prime. Show that

$$X^p - X - 1 \equiv 0 \pmod{p}$$

has no solution. (Hint: Fermat.) [4 bonus]

/...3

8) Do either part (A) or part (B).

(A): a) Define “Quadratic Residue modulo m ”. [3]

b) Determine for which of the following moduli -1 is a quadratic residue: 5, 7, 8, 13, 17, 19. Explain. [6]

c) Determine for which of the moduli m in part b) the congruence $x^4 \equiv -1 \pmod{m}$ has a solution. [4]

(B): a) State the Quadratic Reciprocity Law. [5]

b) Compute

$$i) \left(\frac{17}{19}\right) \quad ii) \left(\frac{15}{17}\right) \quad iii) \left(\frac{-15}{17}\right)$$

[8]

9) Do either part (A) or part (B).

(A): a) Use the extended Euclidean algorithm to find the greatest common divisor of 301 and 48 and to determine integers m and n such that

$$m \cdot 301 + n \cdot 48 = 1 .$$

[6]

b) Solve the congruence $48x = 1 \pmod{301}$, $0 \leq x \leq 300$. [3]

c) Solve the congruence $48x = 5 \pmod{301}$, $0 \leq x \leq 300$. [2]

d) Find the least common multiple of 96 and 602. [2]

(B): a) Using the fact that $50 = 5^2 + 5^2$ and $52 = 4^2 + 6^2$, express 2600 as a sum of two squares. [3]

b) Express 800 as a sum of two squares. [2]

c) Can $8 \cdot 9 \cdot 17$ be written as a sum of two squares? What about $8 \cdot 9 \cdot 13 \cdot 17$? Explain! [4]

d) Show that no integer congruent to 2 (mod 4) can be written in the form $u^2 - v^2$ where u, v are integers. [4]

10) Determine all multiplicative units, squares and cubes in $\mathbb{Z}/8\mathbb{Z}$. Show that every element in $\mathbb{Z}/8\mathbb{Z}$ is a sum of two cubes, but not every element is a sum of two squares. [5 bonus]

11) Suppose m is a positive integer such that there exists a primitive root (mod m). Then how many distinct primitive roots can be found in any reduced residue system (mod m)? [3 bonus]

* * * THE END * * *