

**MATH 332 - ALGEBRA AND NUMBER THEORY**  
**FIRST MIDTERM - PRACTICE TEST**

Note:

- (1) Calculators are not allowed in the exam.
- (2) You may assume the following axioms and theorems:
  - (a) **Axiom:** The natural numbers  $\mathbb{N}$  satisfies the Well Ordering Principle, i.e. every non-empty subset of natural numbers contains a least element.
  - (b) **Theorem:** Let  $a, b, c$  be integers. The linear equation  $ax + by = c$  has a solution if and only if  $\gcd(a, b)$  divides  $c$ .

**Theory Problem 1.** *Prove that if  $p$  is prime and  $p|ab$  then either  $p|a$  or  $p|b$ . Explain why the previous statement can be re-written as follows: if  $p$  is a prime and  $ab \equiv 0 \pmod{p}$  then  $a \equiv 0 \pmod{p}$  or  $b \equiv 0 \pmod{p}$  (or equivalently, if  $ab \equiv 0$  in  $\mathbb{Z}/p\mathbb{Z}$  then either  $a \equiv 0$  or  $b \equiv 0$  in  $\mathbb{Z}/p\mathbb{Z}$ ).*

*Proof.* Suppose  $p$  divides  $ab$  but  $p$  does not divide  $a$ . Then  $\gcd(p, a) = 1$  (otherwise, there is  $d > 1$  such that  $d|p$  and  $d|a$ , and since  $p$  is prime  $d = p$  but  $p$  does not divide  $a$ ). By the theorem above, there exist  $x, y \in \mathbb{Z}$  such that

$$ax + py = 1.$$

Multiplying this equation by  $b$  gives:

$$abx + pyb = b.$$

Since  $p$  divides  $ab$  and  $p$  obviously divides  $pyb$ , then  $p$  divides any linear combination of  $ab$  and  $pyb$ . Hence  $p$  divides  $b = (ab)x + (pyb)y$ .

The rest of the problem follows from the fact that  $p|a$  if and only if  $a \equiv 0 \pmod{p}$ . □

**Theory Problem 2.** *Prove the Fundamental Theorem of Arithmetic, i.e. every natural number  $n > 1$  is a product of primes, and the representation is unique, except for the order of factors.*

*Proof.* See the book or your class notes. □

**Theory Problem 3.** *Prove Euclid's theorem on the infinitude of primes, i.e. prove that there exist infinitely many prime numbers.*

*Proof.* See the book or your class notes. □

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

- (1) *Wilson's Theorem.*
- (2) *Fermat's Little Theorem.*

*Proof.* See the book or your class notes. Remember that in class we said that Wilson's theorem is an if-and-only-if statement. □

**Problem 1.** *Use Euclid's algorithm to:*

- (1) *Find the greatest common divisor of 13 and 50.*
- (2) *Find all solutions of the linear diophantine equation  $13x + 50y = 2$ .*

- (3) Find the multiplicative inverse of 13 modulo 50. Find the multiplicative inverse of 50 modulo 13. Can you use your previous work to find the multiplicative inverse of 7 modulo 27?
- (4) Find all solutions to  $26x \equiv 4 \pmod{100}$ .

*Proof.* (1)  $50 = 13 \cdot 3 + 11$ ,  $13 = 11 + 2$ ,  $11 = 2 \cdot 5 + 1$ . Thus, the gcd is 1.

- (2) One particular solution is found by reversing Euclid's algorithm (and then multiplying through by 2). In particular,  $13 \cdot 4 - 50 = 2$ . By a theorem in class, since  $\gcd(50, 13) = 1$ , all the solutions of  $13x + 50y = 2$  are given by:

$$x = 4 + 50t, \quad y = -1 + 13t, \quad \text{for all } t \in \mathbb{Z}.$$

- (3) A solution to the equation  $13x + 50y = 1$  is given by  $x = 27$  and  $y = -7$ . The equation  $13 \cdot 27 - 7 \cdot 50 = 1$  implies that

$$13 \cdot 27 \equiv 1 \pmod{50}$$

and so, 27 is a multiplicative inverse of 13 modulo 50. Also,  $-7 \equiv 6 \pmod{13}$  is a multiplicative inverse of 50 modulo 13. And  $-50 \equiv 4 \pmod{27}$  is the inverse of 7 modulo 27.

- (4) We first solve  $13x \equiv 2 \pmod{50}$ . In fact, we have already seen that  $13 \cdot 4 - 50 = 2$ . Thus  $x \equiv 4 \pmod{50}$  is the unique solution. Thus, all solutions to  $26x \equiv 4 \pmod{100}$  are  $x = 4$  and  $x = 4 + 50 = 54$  modulo 100 (again by a theorem proved in class).  $\square$

**Problem 2.** Prove that the equation  $x^2 - 7y^3 + 21z^5 = 3$  has no solution with  $x, y, z$  in  $\mathbb{Z}$  (Hint: Calculate all possible squares modulo 7).

*Proof.* Since the set  $\{0, 1, 2, 3, 4, 5, 6\}$  is a complete residue system modulo 7 and since  $a^2 = (-a)^2$ , we can conclude that  $\{0^2, 1^2, 2^2, 3^2\} = \{0, 1, 4, 2\}$  is a complete system of squares modulo 7 (i.e. the squares are congruent to either 0, 1, 2 or 4 modulo 7).

Now, suppose that there are integers  $x, y, z$  such that  $x^2 - 7y^3 + 21z^5 = 3$ . Then:

$$3 = x^2 - 7y^3 + 21z^5 \equiv x^2 \pmod{7}$$

but this,  $x^2 \equiv 3 \pmod{7}$  is impossible by our previous remark.  $\square$

**Problem 3.** Show that 257 divides  $100 \cdot 2^{25} - 57 = 3355443143$ .

*Proof.* Notice that  $2^8 = 256 \equiv (-1) \pmod{257}$ . Thus,  $2^{25} = (2^8)^3 \cdot 2 \equiv -2 \pmod{257}$ . Finally:

$$100 \cdot 2^{25} - 57 \equiv -200 - 57 \equiv -257 \equiv 0 \pmod{257}.$$

$\square$

**Problem 4.** What time does a clock read 100 hours after it reads 2 o'clock?

*Proof.* We need to find the remainder of 102 modulo 12:

$$102 = 12 \cdot 8 + 6, \quad \text{and so} \quad 102 \equiv 6 \pmod{12}.$$

Thus, the time is 6 o'clock. By the way, is that in the PM or AM? Suppose the time now is 2AM. Then we need to find the remainder modulo 24:

$$102 = 24 \cdot 4 + 6, \quad \text{and so} \quad 102 \equiv 6 \pmod{24}$$

and the time is 6 AM.  $\square$

**Problem 5.** Show that  $2^{2^n} + 5$  is composite for every positive integer  $n$ .

*Proof.* First, we try a few numbers. For  $n = 1$ ,  $2^2 + 5 = 9 = 3 \cdot 3$ . For  $n = 2$ ,  $2^4 + 5 = 21 = 3 \cdot 7$ . For  $n = 3$ ,  $2^8 + 5 = 261$  which is divisible by 3. Let us prove that every number  $2^{2^n} + 5$  is divisible by 3 and therefore composite. Since  $2^2 \equiv 1 \pmod{3}$ , we also have  $2^{2^n} = (2^2)^{2^{n-1}} \equiv 1 \pmod{3}$  for all  $n > 0$ . Hence:

$$2^{2^n} + 5 \equiv 6 \equiv 0 \pmod{3}.$$

□

**Problem 6.** Find the smallest positive integer  $n$  such that

$$n \equiv 7 \pmod{3}, \quad n \equiv 5 \pmod{5}, \quad n \equiv 3 \pmod{7}.$$

*Proof.* Simplifying, we need to solve the system:

$$n \equiv 1 \pmod{3}, \quad n \equiv 0 \pmod{5}, \quad n \equiv 3 \pmod{7}.$$

Since  $n \equiv 0 \pmod{5}$ , then  $n = 5a$ . Since  $n \equiv 1 \pmod{3}$  and  $n \equiv 3 \pmod{7}$  then  $n \equiv 10 \pmod{21}$  (use Chinese remainder theorem or any other technique here). Hence, we need to solve:

$$5a \equiv 10 \pmod{21}$$

and clearly  $a = 2$  works. Thus,  $n \equiv 10 \pmod{105}$  and  $n = 10$  is the smallest valid solution. □

**Problem 7.** Find the smallest positive integer that leaves remainders of 2, 4, 6 when divided by 3, 5, 7, respectively.

*Proof.* We need to solve the system:

$$x \equiv 2 \pmod{3}, \quad x \equiv 4 \pmod{5}, \quad x \equiv 6 \pmod{7}$$

or

$$x \equiv -1 \pmod{3}, \quad x \equiv -1 \pmod{5}, \quad x \equiv -1 \pmod{7}.$$

Clearly  $x = -1$  works. Thus,  $x \equiv -1 \pmod{105}$  works. The smallest positive integer is 104. □

**Problem 8.** A troop of 17 monkeys store their bananas in 11 piles of equal size with a twelfth pile of 6 left over. When they divide the bananas into 17 equal groups, none remain. What is the smallest number of bananas they can have?

*Proof.* Let  $x$  be the number of bananas. Then:

$$x \equiv 6 \pmod{11}, \quad \text{and} \quad x \equiv 0 \pmod{17}.$$

Hence,  $x = 17a$  for some integer  $a$ . Thus, we need to solve  $17a \equiv 6 \pmod{11}$  or  $17a + 11b = 6$ . Clearly,  $a = 1, b = -1$  work. Thus  $a = 1$  and  $x \equiv 17 \pmod{187}$ . The smallest possible number is 17. □

**Problem 9.** The seven digit number  $n = 72x20y2$ , where  $x$  and  $y$  are digits, is divisible by 72. What are the possibilities for  $x$  and  $y$ ?

*Proof.* Notice that  $72 = 2^3 \cdot 3^2$ . Thus, 8 divides  $n$  and so 8 divides the three last digits  $0y2 = y2$ . The only two digit numbers divisible by 8 and ending in 2 are 32 or 72, so  $y = 3$  or 7.

The number  $n$  is also divisible by 9, thus the sum of its digits  $7+2+x+2+0+y+2 = x+y+13$  is a multiple of 9. So  $x+y+4$  is a multiple of 9. If  $y = 3$  then  $x+7$  must be a multiple of 9, and the only possibility is  $x = 2$ . If  $y = 7$  then  $x+11$  must be a multiple of 9, which implies that  $x = 7$ . Therefore:

$$n = 7222032 = 72 \cdot 100306, \quad \text{or} \quad n = 7272072 = 72 \cdot 101001.$$

□

**Problem 10.** Show that  $37^{100} \equiv 13 \pmod{17}$ .

*Proof.* By Fermat's Little Theorem,  $a^{16} \equiv 1 \pmod{17}$  for all  $a \not\equiv 0 \pmod{17}$ . Also,  $37 \equiv 3 \pmod{17}$  and  $100 = 16 \cdot 6 + 4$ . Thus:

$$37^{100} \equiv (3^{16})^6 \cdot 3^4 \equiv 3^4 \equiv 3^3 \cdot 3 \equiv 10 \cdot 3 \equiv 30 \equiv 13 \pmod{17}.$$

□

**Problem 11.** Show that  $42|n^7 - n$  for all positive  $n$ .

*Proof.* Note that  $42 = 6 \cdot 7$ . By Fermat's Little Theorem we know that  $n^7 \equiv n \pmod{7}$  for all  $n$ . It remains to show that  $n^7 \equiv n \pmod{6}$  for all  $n$ . Note that  $n^7 \equiv n \pmod{2}$  and FLT also implies that  $n^3 \equiv n \pmod{3}$ , thus  $n^7 \equiv (n^3)^2 \cdot n \equiv n \pmod{3}$ .

Thus, since  $n^7 \equiv n \pmod{7}$  and  $n^7 \equiv n \pmod{6}$  and  $\gcd(6, 7) = 1$ , we obtain  $n^7 \equiv n \pmod{42}$ , for all  $n$ . □

**Problem 12.** Show that  $5555^{2222} + 2222^{5555}$  is divisible by 7.

*Proof.* Note that  $5555 + 2222 = 7777 \equiv 0 \pmod{7}$ . Thus,  $5555 \equiv -2222 \pmod{7}$  and  $2222 = 2100 + 122 \equiv 122 \equiv 105 + 17 \equiv 3 \pmod{7}$ . One also calculates  $2222 \equiv 2 \pmod{6}$  ( $2222$  is 0 modulo 2 and is 2 modulo 3) and  $5555 \equiv 5 \pmod{6}$ . Finally, by Fermat's Little Theorem:

$$(-3)^{2222} + 3^{5555} \equiv (-3)^2 + 3^5 \pmod{7} \equiv 2 + 2 \cdot 2 \cdot 3 \equiv 2 + 5 \equiv 0 \pmod{7}.$$

□

**Problem 13.** Prove that for any natural number  $n \geq 1$ ,  $3^{6n} - 2^{6n}$  is divisible by 35 (Hint: work modulo 5 and modulo 7, separately).

*Proof.* Let us begin working modulo 5 and 7 separately. One calculates (using FLT):

$$3^6 \equiv 3^4 \cdot 3^2 \equiv 9 \equiv 4 \pmod{5}, \quad 2^6 \equiv 2^2 \equiv 4 \pmod{5}, \quad 3^6 \equiv 2^6 \equiv 1 \pmod{7}.$$

Thus:

$$3^{6n} - 2^{6n} \equiv 4^n - 4^n \equiv 0 \pmod{5}, \quad 3^{6n} - 2^{6n} \equiv 1 - 1 \equiv 0 \pmod{7}.$$

Thus, since 5 and 7 are relatively prime,  $3^{6n} - 2^{6n} \equiv 0 \pmod{35}$ . □

**Problem 14.** Show that if  $p$  and  $q$  are distinct primes then  $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ .

*Proof.* Since  $p$  and  $q$  are distinct (and therefore relatively prime), it suffices separately modulo  $p$  and modulo  $q$ . By Fermat's Little theorem one has  $n^{p-1} \equiv 1 \pmod{p}$  and  $n^{q-1} \equiv 1 \pmod{q}$  for all  $n$  not equivalent to 0 modulo  $p$  or  $q$  respectively. Thus:

$$p^{q-1} + q^{p-1} \equiv 1 + 0 \equiv 1 \pmod{q}, \quad p^{q-1} + q^{p-1} \equiv 0 + 1 \equiv 1 \pmod{p}.$$

□

**Problem 15.** Find the remainder when  $14!$  is divided by 17.

*Proof.* By Wilson's Theorem  $16! \equiv -1 \pmod{17}$ . Thus:

$$16 \cdot 15 \cdot 14! \equiv -1 \pmod{17}$$

and

$$14! \equiv -16^{-1} \cdot 15^{-1} \pmod{17}.$$

It suffices to find the inverse of  $16 \cdot 15 \pmod{17}$ . Since  $16 \cdot 15 \equiv (-1)(-2) \equiv 2 \pmod{17}$  and  $2 \cdot 9 \equiv 1 \pmod{17}$ :

$$14! \equiv -(16 \cdot 15)^{-1} \equiv -2^{-1} \equiv -9 \equiv 8 \pmod{17}.$$

□

**Problem 16.** Use Euler's theorem to find the last digit of the decimal expansion of  $7^{1000}$ .

*Proof.* It suffices to find the residue of  $7^{1000}$  modulo 10. Notice that:

$$\varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4.$$

Therefore, by Euler's theorem, if  $\gcd(n, 10) = 1$  then  $n^4 \equiv 1 \pmod{10}$ . Finally:

$$7^{1000} \equiv (7^4)^{250} \equiv 1 \pmod{10}.$$

□