

**MATH 332 - ALGEBRA AND NUMBER THEORY**  
**- FIRST MIDTERM - 10/02/2007**

**Show all work. No calculators. There are 2 theory questions and 4 additional problems.** You may assume the following axioms and theorems:

- (1) **Axiom:** The natural numbers  $\mathbb{N}$  satisfy the Well Ordering Principle, i.e. every non-empty subset of natural numbers contains a least element.
- (2) **Theorem:** Let  $a, b, c$  be integers. The linear equation  $ax + by = c$  has a solution if and only if  $\gcd(a, b)$  divides  $c$ .
- (3) **Theorem:** Let  $p$  be a prime and let  $a, b$  be any integers. If  $p|ab$  then  $p|a$  or  $p|b$ . More generally, if  $p|a_1a_2 \cdots a_k$  then  $p$  divides some  $a_i$ .

**Theory Question 1.** (20 points) Prove the **uniqueness** part of the **Fundamental Theorem of Arithmetic**, i.e. assume that every natural number  $n$  has a factorization and then prove that this factorization is unique up to the order of the factors.

*Proof.* Assume that all numbers have at least one factorization into primes and let  $S$  be the set of all natural numbers which have two distinct factorizations. Then either  $S$  is empty and we would be done, or  $S$  is a non-empty set of natural numbers. By the Well Ordering Principle, the set  $S$  has a least element  $n$  and so there are two distinct factorizations:

$$n = p_1^{a_1} \cdots p_r^{a_r} = q_1^{b_1} \cdots q_s^{b_s}.$$

But then  $p_1$  divides  $q_1^{b_1} \cdots q_s^{b_s}$  and so, by Theorem (b) above, there is some  $i$  such that  $p_1$  divides  $q_i^{b_i}$  (assume  $i = 1$ ) and therefore  $p_1$  divides  $q_1$ . Since they are both primes they should be the same prime, hence  $p_1 = q_1$ . But then:

$$\frac{n}{p_1} = p_1^{a_1-1} \cdots p_r^{a_r} = q_1^{b_1-1} \cdots q_t^{b_t}$$

are two distinct factorizations of  $n/p_1$  but  $n/p_1$  is less than  $n$ , so  $n/p_1$  should not be an element of  $S$ . This is a contradiction, therefore  $S$  must be empty in the first place.  $\square$

**Theory Question 2.** (20 points) You may assume the fundamental theorem of arithmetic and any property about congruences proved in class.

- (1) Justify: if  $p \equiv 1 \pmod{4}$  and  $q \equiv 1 \pmod{4}$  then  $pq \equiv 1 \pmod{4}$ .
- (2) Show that if  $N \equiv 3 \pmod{4}$  then  $N$  has a prime factor  $p$  such that  $p \equiv 3 \pmod{4}$ .
- (3) Suppose  $q_1, \dots, q_k$  are primes such that  $q_i \equiv 3 \pmod{4}$  for all  $1 \leq i \leq k$ . Let us define  $N = 4q_1 \cdots q_k - 1$ . Show that  $N$  has a prime factor  $p$  such that  $p \equiv 3 \pmod{4}$  and  $p$  is distinct from any of the primes  $q_1, \dots, q_k$ .
- (4) Prove that there exist infinitely many primes  $p$  of the form  $p \equiv 3 \pmod{4}$ .

*Proof.* (1) We know from class that if  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$  then  $ac \equiv bd \pmod{m}$ . Therefore if  $p \equiv q \equiv 1 \pmod{m}$  then

$$pq \equiv 1 \cdot 1 \equiv 1 \pmod{m}.$$

- (2) By part (1), if two numbers are congruent to 1 modulo 4 then their product also is. Let  $N \equiv 3 \pmod{4}$  have a prime factorization  $N = p_1 \cdots p_r$ . Note that since  $N \equiv 3 \pmod{4}$  then  $N$  is odd, so 2 does not divide  $N$ . Thus, by part (1), some prime divisor  $p_i$  must be  $\equiv 3 \pmod{4}$ , otherwise  $N \equiv 1 \pmod{4}$ .

- (3) Let  $N = 4q_1 \cdots q_k - 1$  with  $q_i \equiv 3 \pmod{4}$ . Note that  $N \equiv -1 \equiv 3 \pmod{4}$ . Thus, by part (2) there is a prime divisor  $p$  of  $N$  such that  $p \equiv 3 \pmod{4}$ . Suppose  $p = q_i$ . Then  $p$  divides  $N$  and  $p$  divides  $4q_1 \cdots q_k$ , and so  $p$  divides  $-1$ , hence a contradiction and  $p \neq q_i$ .
- (4) Suppose that there are only finitely many primes  $q_1, \dots, q_k$  which are congruent to 3 modulo 4. Then  $N = 4q_1 \cdots q_k - 1$  has a prime divisor  $p \equiv 3 \pmod{4}$  which is distinct from all  $q_1, \dots, q_k$ . Contradiction. □

**Problem 1.** (15 points) Use Euclid's algorithm to:

- (1) Find the greatest common divisor of 5 and 13.
- (2) Find all solutions of the linear diophantine equation  $5x + 13y = 1$ .
- (3) Solve the congruences  $5x \equiv 1 \pmod{13}$  and  $13x \equiv 1 \pmod{5}$ .

*Proof.* (1) One has  $13 = 5 \cdot 2 + 3$  and  $5 = 3 + 2$  and  $3 = 2 + 1$ . Therefore the gcd is 1.

- (2) Now work backwards. One has

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5.$$

Hence

$$1 = (-5) \cdot 5 + 2 \cdot 13$$

is a solution. Since  $\gcd(5, 13) = 1$  by a theorem in class all solutions to  $1 = 5x + 13y$  are given by:

$$x = -5 - 13t, \quad y = 2 + 5t, \quad \text{for any } t \in \mathbb{Z}.$$

- (3) Since  $1 = (-5) \cdot 5 + 2 \cdot 13$  we get  $(-5) \cdot 5 \equiv 1 \pmod{13}$ , so  $-5 \equiv 8 \pmod{13}$  is the multiplicative inverse of 5. Similarly  $13 \cdot 2 \equiv 3 \cdot 2 \equiv 1 \pmod{5}$ , so the multiplicative inverse of 13 is 2 modulo 5. □

**Problem 2.** (15 points) Let  $N = 9 \cdot 78^7 + 5 \cdot 78^5 + 7 \cdot 78^2 + 7$ .

- (1) Is  $N$  divisible by 3? Explain.
- (2) Is  $N$  divisible by 7 or 11? Explain.
- (3) Is  $N$  divisible by 79? Explain.
- (4) It turns out that  $N - 1 \equiv 16! \pmod{17}$ . Find another prime divisor of  $N$  (and justify).

*Proof.* (1) Note that  $78 \equiv 15 \equiv 0 \pmod{3}$ . Thus  $N \equiv 0 + 0 + 0 + 7 \equiv 1 \pmod{3}$ . Thus, 3 does not divide  $N$ .

- (2) Notice that  $78 = 1 + 77 = 1 + 7 \cdot 11$ , thus  $78 \equiv 1$  modulo 7 or 11. Now:

$$N \equiv 9 + 5 + 7 + 7 \equiv 14 + 14 \equiv 3 + 3 \equiv 6 \pmod{11}$$

$$N \equiv 9 + 5 + 7 + 7 \equiv 14 + 0 + 0 \equiv 0 \pmod{7}$$

and so  $N$  is not divisible by 11 but 7 divides  $N$ .

- (3) Here we use the fact that  $78 \equiv -1 \pmod{79}$  to calculate:

$$N \equiv 9(-1)^7 + 5(-1)^5 + 7(-1)^2 + 7 \equiv -9 - 5 + 7 + 7 \equiv 0 \pmod{79}.$$

Hence  $79|N$ .

- (4) Last, if  $N - 1 \equiv 16! \pmod{17}$  then by Wilson's theorem (since 17 is prime) we get that  $N - 1 \equiv -1 \pmod{17}$ , therefore  $N \equiv 0 \pmod{17}$  and  $17|N$ . □

**Problem 3.** (15 points) What is the smallest possible number of monkeys in a cage if the number leaves a remainder of 2 when divided by 4 or 9 but leaves a remainder of 1 when divided by 37? (You do not need to simplify your answer).

*Proof.* Let  $x$  be the number of monkeys in the cage. Then we are trying to solve the system:

$$x \equiv 2 \pmod{4}, \quad x \equiv 2 \pmod{9}, \quad x \equiv 1 \pmod{37}.$$

Notice that by the Chinese Remainder Theorem there is a solution (because 4, 9, 37 are pairwise coprime) and unique modulo  $4 \cdot 9 \cdot 37$ .

We first solve  $x \equiv 2 \pmod{4, 9}$ . Notice that 2 is a solution. Thus the any solution is of the form  $x = 2 + 4 \cdot 9k = 2 + 36k$  for some integer  $k$ . We also need  $x \equiv 1 \pmod{37}$ , which implies that  $2 + 36k \equiv 1 \pmod{37}$  and so  $k \equiv 1 \pmod{37}$ . Hence  $k = 1$  is the smallest positive solution and  $x = 2 + 36 = 38$ .  $\square$

**Problem 4.** (15 points) Let  $\phi(m)$  be the Euler  $\phi$ -function.

(1) Verify  $\phi(100) = 40$ .

(2) Find the last two digits of the decimal expansion of  $1032103^{2007}$ .

(Knowing some powers of three may help:

$$3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 27, \quad 3^4 = 81, \quad 3^5 = 243, \quad 3^6 = 729, \quad 3^7 = 2187, \dots)$$

*Proof.* (1) First, we factor  $100 = 4 \cdot 25$ . Hence by the properties of the Euler  $\phi$ -function:

$$\phi(100) = \phi(4)\phi(25) = 2(2-1)5(5-1) = 2 \cdot 5 \cdot 4 = 40.$$

(2) It suffices to find  $1032103^{2007} \pmod{100}$ , because the last two digits of a decimal expansion are the remainder of division by 100. Notice first that  $1032103 \equiv 3 \pmod{100}$ . Moreover:

$$2007 = 40 \cdot 50 + 7.$$

Finally, since  $\gcd(3, 100) = 1$ , Euler's Theorem states that  $3^{40} \equiv 1 \pmod{100}$ . Putting all this together we obtain:

$$1032103^{2007} \equiv 3^{2007} \equiv (3^{40})^{50} \cdot 3^7 \equiv 3^7 \equiv 2187 \equiv 87 \pmod{100}.$$

Hence, the last two digits are 87.  $\square$