

## INTRODUCTION TO NUMBER THEORY

## Exam 1

February 16, 2007

The point value of each problem is given in the margin.

- (20) 1. a) Explain why  $\gcd(0, 0)$  is not defined.
- b) What discreteness property of the integers is needed to prove that  $\gcd(a, b)$  exists if  $a, b$  are not both zero.
- c) (Fill in the blank) In the **Fast** Euclidean algorithm one needs the following version of the division algorithm: Given integers  $a, b$  with  $b \neq 0$ , there exist integers  $q, r$  such that  $a = bq + r$  with \_\_\_\_\_ .
- d) State the key lemma needed for proving the uniqueness of factorization of integers. (It involves a prime  $p$ .)
- e) What method of proof is used for proving the existence of factorization of natural numbers.
- (7) 2. Use the Euclidean Algorithm to find the greatest common divisor of 28 and 266.

(12) 3. a) Find the general solution of the linear equation  $23x + 14y = 200$ , in integers  $x, y$ .

b) Then find all solutions with  $x$  and  $y$  both positive.

(15) 4. Use properties of congruences to compute the least residue of the following numbers (mod 7). (Avoid long multiplication in  $\mathbb{Z}$ .)

(a)  $4903 \cdot 69 + 72$

(b)  $78^2 + 72^5$

(c)  $2^{1000}$

(10) 5. Prove the following theorem. If  $a, b, c, d$  are integers such that  $a \equiv c \pmod{m}$  and  $b \equiv d \pmod{m}$  then  $ab \equiv cd \pmod{m}$ .

(16) 6. True, False. Circle T or F. True means that the statement is true for **all** choices of integers  $a, b, c, d$ .  $(a, b) = \text{GCD}$ .  $[a, b] = \text{LCM}$ .

T F a) If  $a|(b+c)$  then  $a|b$  and  $a|c$ .

T F b) If  $a|b$  and  $a|c$  then  $a|(2b-c)$ .

T F c) If  $a|bc$  then either  $a|b$  or  $a|c$ .

T F d) If  $d|a$  and  $d|b$  then  $d|[a, b]$ .

T F e) For any integers  $a, b, c$ ,  $(a, b+ca) = (a, b)$

T F f) If  $m|(a-2b)$  then  $a \equiv 2b \pmod{m}$ .

T F g) If  $p, q$  are distinct primes then there exist integers  $x, y$  such that  $px + qy = 10^{10}$ .

T F h) If  $p$  is an odd prime then there exist integers  $x, y$  such that  $px + p^2y = 4$ .

(10) 7. Prove by induction that  $4^n \equiv 1 + 3n \pmod{9}$ , for any positive integer  $n$ .

(10) 8. Prove that if  $a|bc$  and  $\gcd(a, b) = 1$ , then  $a|c$ .