UNIVERSITY OF MANITOBA

DATE: December 7, 2012

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

FINAL EXAMINATION

TIME: 3 hours
EXAMINER: M. Davidson

---

[10] 1. (a) Find $(2002, 897)$.

(b) Find all integer solutions to $2002\,x + 897\,y = (2002, 897)$.

[10] 2. For each of the following linear congruences, find out how many solutions there are. If solutions exist, you need *NOT* find them, but you should state a reason for your answer.

(a) $3388\,x \equiv 42 \pmod{7413}$

(b) $2500\,x \equiv 42 \pmod{2012}$

[8] 3. Given the public information of an RSA encryption is $(n, e) = (2599, 107)$, find the decrypt key d.
[Hint: One of the two prime factors of n is less than 30.]

[12] 4. Recall $d(n)$ is the number of divisors of n, $\sigma(n)$ is the sum of the divisors of n and $\phi(n)$ is the Euler phi function. $(229320 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13)$

(a) What is $d(229320)$? $\sigma(229320)$? $\phi(229320)$?

(b) Show that if n is a square then $d(n)$ is odd.

(c) Under what conditions is $\phi(2n) = \phi(n)$? (Justify your answer.)

[8] 5. (a) Define what is meant for a number n to be *abundant*.

(b) Define what is meant for a number n to be *deficient*.

(c) For what values of a is $2^a \cdot 11$ abundant?

(d) Show that there are infinitely many deficient numbers.

[10] 6. (a) Use Wilson's Theorem to find the least residue of $235! \pmod{239}$.

(b) Use Gauss's Lemma to decide if 3 is a quadratic residue or quadratic non-residue modulo 31.
(No credit will be given for any other method.)

[18] 7. (a) How many primitive roots does the prime 71 have?

(b) What are the possible orders a modulo 71 when $(a, 71) = 1$?

(c) Show that 7 is a primitive root of 71.

(d) List two other primitive roots. (How do you know they are primitive roots?) These should be in least residue.

(e) Given that $7^6 = 117649 = 71(1657) + 2$, what is the order of 2 modulo 71? What is the order of 14 mod 71?

[6] 8. Suppose that a has order $t \pmod{m}$. What is the order of a^2 if:

(a) t is odd? (Justify your answer.)

(b) t is even? (Justify your answer.)

[12] 9. Calculate the following Legendre Symbols:
Note: 1723 is prime.

(a) $\left(\dfrac{499}{1723}\right)$

(b) $\left(\dfrac{113616}{997}\right)$

---

[8] 10. We note that for the prime number $p = 2819$, that $2p + 1 = 5639$ is also prime.

Use Euler's Criterion for quadratic residues (together with calculation of Legendre symbols) to decide which, if any, of $2, 3, 5$, or 7 are primitive roots of 5639.

[8] 11. (a) Give a formula for finding integer solutions to $x^2 + y^2 = z^2$.

(b) Under what conditions is this solution fundamental?

(c) Find a Pythagorean triple where one of the values is:

i. 11.

ii. 14.