INTRODUCTION TO NUMBER THEORY

MAS 4203 — FINAL EXAM - PART 2 — April 20, 2016

NAME:

When giving proofs make sure your reasoning is clearly. Show all necessary work. State clearly any results you used.
There are 5 questions of EQUAL value. Do FOUR complete questions. If you do more than four questions the best four complete questions will be taken. At the end there is also an optional 2 point bonus problem. Only basic and scientific calculators are allowed. A table of primes is supplied.

---

1. [$5 \times 2 = 10$ pts] FIND

(i) $\phi(1155)$

(ii) $\nu(1155)$

(iii) $\sigma(1155)$

(iv) $\mu(1155)$

(v) $F(1155)$ is $F(n) = \sum_{d|n} (\mu(d))^2$.

2. [$3 + 4 + 3 = 10$ pts]

(i) FIND $g(49)$ if $(\nu(n))^2 = \sum_{d|n} g(d)$.

(ii) PROVE that infinitely many positive integers n such that

$$\mu(n) + \mu(n+1) + \mu(n+2) = 0.$$

(iii) A positive integer n is *deficient* if $\sigma(n) < 2n$. PROVE that any prime power p^a is deficient.

3. $[1+2+3+4=10$ pts$]$

(i) DEFINE the Legendre symbol $\left(\frac{a}{p}\right)$.

(ii) EXPLAIN why

$$\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{p-1}{p}\right)=0$$

for any odd prime p.

(iii) Let $a \in \mathbb{Z}$. Suppose $a \not\equiv 0 \pmod{p}$ and $\overline{a}$ is the multiplicative inverse of a mod p. PROVE that

$$\left(\frac{a}{p}\right)=\left(\frac{\overline{a}}{p}\right).$$

(iv) FIND the Legendre symbol $\left(\frac{2591}{2711}\right)$. Show reasoning.

4. $[1+1+6+2=10$ pts$]$

(i) COMPLETE the statement of **Euler's Criterion:** Let p be an odd prime. Let $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$\left(\frac{a}{p}\right) \equiv \_\_\_\ \_\_\_ \pmod{\_\_\_}$$

(ii) COMPLETE the statement: Let p be an odd prime. Then

$$\left(\frac{2}{p}\right)=1 \quad \text{if and only if} \quad p \equiv \_\_\_\ \_\_\_\ \_\_\_ \pmod{\_\_\_}$$

(iii) Let p and q be prime numbers with $p \equiv 3 \pmod{4}$ and $q = 2p+1$. PROVE that

$$q \mid 2^p - 1.$$

(iv) DETERMINE whether $2^{1223}-1$ is a Mersenne prime.

5. [5 + 5 = 10 pts] Do either (A) or (B) but NOT BOTH.

(A) Explain and describe the RSA encryption scheme and give a proof of the decoding procedure.

(B) State the a-test for primality and prove that p passes the a-test for all odd primes $p > a$, where a is any fixed integer $a > 1$.

2 BONUS pts

The guy on the left is L___ ___ ___ ___ L___ ___ ___ ___ ___ ___ ___.
He was a French p ___ ___ ___ ___ ___ ___ ___ ___ ___. The guy on
the right is A___ ___ ___ ___ ___-M___ ___ ___ ___ L___ ___ ___ ___ ___ ___ ___.
He was a French m___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___.
This caricature by J.-L. B ___ ___ ___ ___ ___is the only known pro-
trait of A ___ ___ ___ ___ ___-M___ ___ ___ ___ L ___ ___ ___ ___ ___ ___ ___.
The portrait on the left was mistakenly thought to be that of the math-
emtician. This error was not discovered until the year ___ ___ ___ ___by
two students from the University of S___ ___ ___ ___ ___ ___ ___ ___ ___.