1. [20 points] Let a, b, $c \in \mathbb{Z}$ with $(a, b) = 1$. Prove (without assuming the Fundamental Theorem of Arithmetic) that if $a \mid c$ and $b \mid c$ then $ab \mid c$.

HINT: Since $(a, b) = 1$ there are integers x, y such that $ax + by = 1$.

2. [20 points] Let a, b, $c \in \mathbb{Z}$ and assume that a and b are not both zero and let $d = (a, b)$. Prove that

$$ax + by = c$$

for some integers x and y if and only if $d \mid c$.

HINT: Use the result that

$$(a, b) = \min\{ma + nb \,:\, m, n \in \mathbb{Z}, ma + nb > 0\}.$$

3. [5 + 15 = 20 points] (i) Define *pseudoprime*.

(ii) Prove that $161038 = (2)(73)(1103)$ is a pseudoprime.

4. [5 + 15 = 20 points] (i) State Euler's Theorem.

(ii) Let m, n be positive relatively prime integers. Prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

5. [4 × 5 = 20 points] (i) Define what it means for an arithmetic function to be *multiplicative*.

(ii) Prove that if f is a multiplicative function and $f(1) = 0$ then $f(n) = 0$ for all n.

(iii) Prove that if f is a multiplicative function and $f(1) \neq 0$ then $f(1) = 1$.

(iv) Suppose $f(n)$ and $g(n)$ are multiplicative functions. Prove that $h(n) = f(n)g(n)$ is multiplicative.

6. [15 + 5 = 20 points]

(i) Let m, n be positive integers with $m \mid n$. Prove that

$$\phi(m) \mid \phi(n).$$

(ii) Prove or disprove the converse of (i).

7. [20 points] Let $n \in \mathbb{Z}$ with $n > 1$. If f is a multiplicative arithmetic function and f is not the zero function and $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ is the prime factorization of n, prove that

$$\sum_{d|n, d>0} \mu(d)\, f(d) = \prod_{i=1}^{m} (1 - f(p_i)).$$

8. [$4 \times 5 = 20$ points] (i) Define the Legendre symbol $\left(\frac{a}{p}\right)$.

(ii) Find the quadratic residues modulo 5.

(iii) State the Law of Quadratic Reciprocity.

(iv) Find $\left(\frac{115}{131}\right)$. *WARNING:* 115 is NOT prime!

9. [$8 + 12 = 20$ points] Let p be an odd prime.

(i) For $1 \leq a \leq p-1$, let a' denote the multiplicative inverse of a modulo p; i.e., $aa' \equiv 1 \pmod{p}$. Prove that

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

(ii) Prove that

$$\left(\frac{1 \cdot 2}{p}\right) + \left(\frac{2 \cdot 3}{p}\right) + \left(\frac{3 \cdot 4}{p}\right) + \cdots + \left(\frac{(p-2)(p-1)}{p}\right) = -1.$$

10. [20 points] Do either (A) or (B) but NOT BOTH.

(A) Explain what the RSA algorithm is and give a proof of the decoding procedure.

OR

(B) State the a-test for primality and prove that p passes the a-test for any given a, for all primes $p > a$.