Mathematics 466 Midterm (50 points) Due 10/24/08, 10am

Points (leave blank)  
1 2 3 4 5 ∑  

Name: (clearly, please)

This exam is my own work. Sources (apart from the textbooks and my lecture notes) are indicated.

Signature

Notes

• Put your name on this cover sheet and sign it.

• You are permitted to use your notes and any publication (book, journal, web page). You are not permitted to consult persons. Results which are quoted from a publication (apart from the course textbooks and your lecture notes) should be indicated.

• Unless specified otherwise, you may use a computer for arithmetic (including extended Euclidean algorithm).

  Computer commands, which render the problem trivial (for example using factorization to show that a polynomial is irreducible over \( \mathbb{Z} \)), however are not considered a sufficient solution.

• If you need extra sheets, staple them to this exam. (You do not need to submit scrap paper.)
1) Show that $R := \mathbb{Z}[\sqrt{3}] = \{ a + b\sqrt{3} \mid a, b \in \mathbb{Z} \}$ is an integral domain (you may use, without proof, that $\mathbb{C}$ is a field) and that $2 + \sqrt{3}$ is a unit in $R$. 
2) Construct a field with 16 elements and show that it is a field. (**Hint:** Consider \( \mathbb{F}_2[x]/(p(x)) \) for a suitable polynomial of degree 4.)
3) Let $F$ be a field and $A \in M_n(F)$ an $n \times n$ matrix. Show that the map $\theta: F[x] \to M_n(F)$, $p(x) \mapsto p(A)$ (the polynomial evaluated at the matrix) is a ring homomorphism. Conclude that there is a polynomial $m_A(x) \in F[x]$, such that every polynomial $p(x) \in F[x]$ for which $p(A) = 0_{n \times n}$ is a multiple of $m_A$. ($m_A$ is called the minimal polynomial of $A$.)
4) Let $R$ be a commutative ring with 1. show that $R$ is a field if and only if $\{0\}$ and $R$ are the only ideals of $R$. 
5) (The Chinese Remainder Theorem)
a) Let $R$ be a ring and $I, J \triangleleft R$. Show that the map

$$\vartheta : R \to R/I \times R/J, \quad r \mapsto (I + r, J + j)$$

is a ring homomorphism with kernel $I \cap J$. Show that if $I + J = R$, then $\vartheta$ is surjective.

b) Show that for $\gcd(m, n) = 1$, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. (Hint: Let $I = m\mathbb{Z}$ and $J = n\mathbb{Z}$, and use a))

c) Let $m, n$ as in b). Let $\tilde{m}$ be the multiplicative inverse of $m$ modulo $n$ and $\tilde{n}$ the multiplicative inverse of $n$ modulo $m$. Show that the map

$$(I + a, I + b) \to (I \cap J) + (a \cdot \tilde{n} \cdot n + b \cdot \tilde{m} \cdot m)$$

is an inverse to $\vartheta$.

d) Determine all integers $x$ such that $x \equiv 3 \pmod{1000}$ and $x \equiv 5 \pmod{1001}$. 