ASSIGNMENT 3 - MATH235, FALL 2007

Submit by 16:00, Monday, October 1 (use the designated mailbox in Burnside Hall, 10^{th} floor).

1. *The ring of 2×2 matrices over a field $\mathbb{F}$.*
Let $\mathbb{F}$ be a field. (In a first read you may as well assume $\mathbb{F}$ is $\mathbb{R}$, but solve the question in general). We consider the set

$$M_2(\mathbb{F}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{F} \right\}.$$

It is called the two-by-two matrices over $\mathbb{F}$. We define the addition of two matrices as

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}.$$

We define multiplication by

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

Prove that this is a ring. For each of the following subsets of $M_2(\mathbb{F})$ determine if they are subrings or not.

⟨A⟩ The set $\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{F}) \right\}$.

⟨B⟩ The set $\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{F}) \right\}$.

⟨C⟩ The set $\left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in M_2(\mathbb{F}) \right\}$.

⟨D⟩ The set $\left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in M_2(\mathbb{F}) \right\}$.

⟨E⟩ The set $\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbb{F}) \right\}$.

Remark: One defines in a very similar way the ring of $n \times n$ matrices with entries in a field $\mathbb{F}$.

2. Find the quotient and remainder when a is divided by b:
(1) $a = 302, b = 19$.
(2) $a = -302, b = 19$.
(3) $a = 0, b = 19$.
(4) $a = 2000, b = 17$.
(5) $a = 2001, b = 17$.
(6) $a = 2002, b = 17$.

3. Prove that the square of any integer a is either of the form $3k$ or of the form $3k + 1$ for some integer k. (Hint: write a in the form $3q + r$, where $r = 0, 1$ or 2.)

4. Prove of disprove: If $a|(b + c)$ then $a|b$ or $a|c$.

5. If $r \in \mathbb{Z}$ and r is a nonzero solution of $x^2 + ax + b$ (where $a, b \in \mathbb{Z}$) prove that $r|b$.

6. If $n \in \mathbb{Z}$, what are the possible values of
(1) $(n, n + 2)$;
(2) $(n, n + 6)$.

7. Find the following gcd's. In each case also express (a, b) as $ua + vb$ for suitable integers $u, v \in \mathbb{Z}$.
(1) $(56, 72)$.
(2) $(24, 138)$.
(3) $(143, 227)$.
(4) $(314, 159)$.

8. If $a|c$ and $b|c$, must ab divide c? What if $(a, b) = 1$?