Math 342 Problem set 6 (due 25/2/09)

$(\mathbb{Z}/m\mathbb{Z})^{\times}$

1. Let p be a prime. We saw in class that $\varphi(p) = p-1$. Now let $k \geq 1$ be an integer.
   (a) What are the positive divisors of p^k? Find a simple way to express the condition "$(a, p^k) > 1''$.
   (b) How many integers between 0 and $p^k - 1$ are multiples of p?
   (c) Show that $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ for all k.
   (d) Show that $\varphi(p \cdot p) \neq \varphi(p)\varphi(p)$.

2. Let p, q be distinct primes. Let $m = pq$.
   (a) What are the positive divisors of m?
   (b) Which integers a, $0 \leq a \leq m-1$ have a common factor with m?
   (c) Show that $\varphi(pq) = (p-1)(q-1)$.
   (d) The conclusion of part (c) can be rephrased as $\varphi(p \cdot q) = \varphi(p)\varphi(q)$. Given the conclusion of part 1(d), your proof of 2(c) must have at some point used the fact that $p \neq q$. Where was it?

3. (§9C.E811) For each integer n below, list the positive divisors of n. For each divisor d find $\varphi(d)$ [by definition, $\varphi(1) = 1$]. Calculate the sum $\sum_{d|n} \varphi(d)$.
   (a) $n = 16$ (you may want to use 2(c) repeatedly).
   (b) $n = 15$,
   (c) $n = 45$.

RSA

- Download the paper by Rivest, Shamir and Adelman from the course website and read it.

Section II describes the idea (novel at the time) of the whole world knowing the encryption method but nevertheless only the receiver knowing the decryption method. In this description the keys (the various integers $d, e, m, \varphi(m)$) are considered part of the functions D, E just like in the lecture.

5. Explain why on the top of page 123, e is chosen to be *relatively prime* to $\varphi(pq)$. This was not emphasized in class, but it is essential.
   Hint: How do we know that d exists?

6. The algorithm in section VII.A has appeared in a previous problem set; it requires about $2\log_2 d$ multiplications to raise a number to the dth power. Could you guess why it was important enough to be mentioned?
   Hint: In applications, d and e will have hundreds of digits.

8. Verify the numerical example in part VIII: for $m = 2773$, $\varphi(m) = 2668$, $d = 157$, $e = 17$.
   (a) Check that $de \equiv 1\,(\varphi(m))$.
   (b) Consider the word "GREEK" from the example, encoded as the three decimal numbers 0718, 0505, 1100. Here $G = 07$, $R = 18$, $E = 05$, $K = 11$. For each of the three numbers x calculate $x^e \mod m$ and compare with the "encyphered" values given.
   (c) Take your resulting three numbers y, calculate $y^d \mod m$ and see that you get your starting values back.

Rings

Let $M_2(\mathbb{Z})$ be the set of 2×2 matrices. We write $A \in M_2(\mathbb{Z})$ as $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$. We define addition component-wise, and multiplication by the usual rule of matrix multiplication:

$$A \cdot B = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12}A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix}.$$

Let $I = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$ denote the identity matrix, 0 the everywhere zero matrix.

8. Using the usual laws of arithmetic in $\mathbb{Z}$, prove that:
   (a) Addition in $M_2(\mathbb{Z})$ is associative.
   (b) I is a neutral element for multiplication in $M_2(\mathbb{Z})$: for all $A \in M_2(\mathbb{Z})$, $I \cdot A = A \cdot I = A$.
   (c) Show that multiplication in $M_2(\mathbb{Z})$ is not commutative. In other words, find 2×2 matrices A, B with integer entries so that $A \cdot B \neq B \cdot A$

Optional

A. Continuing problem 8, prove that multiplication in $M_2(\mathbb{Z})$ is associative.