HW #2

1.(*) Let $a, b \in \mathbf{Z}^+$. Repeated use of the Division Algorithm gives the Euclidean Algorithm, viz., a system of equations

$$\begin{array}{lcll} a & = & bq_1 + r_1 & 0 < r_1 < b \\ b & = & r_1 q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2 q_3 + r_3 & 0 < r_3 < r_2 \\ & \vdots & & \vdots \\ r_{k-3} & = & r_{k-2} q_{k-1} + r_{k-1} & 0 < r_{k-1} < r_{k-2} \\ r_{k-2} & = & r_{k-1} q_k + r_k & 0 < r_k < r_{k-1} \\ r_{k-1} & = & r_k q_{k+1} + 0 & \end{array}$$

Show this ends. Show that $r_k = gcd(a, b)$. Plugging in backwards gives $r_k = ax + by$ for some integers x, y. Do all of this for $a = 39493$ and $b = 19853$ (including finding an appropriate x and y).

2. Let a, b, c be non-zero integers. Let $d = gcd(a, b)$. Show the equation $ax + by = c$ has a solution x, y in integers if and only if $d|c$. Moreover, show if $d|c$ and x_o, y_o is a solution in integers then the general solution in integers is $x_o + \frac{b}{d}k, y_o - \frac{a}{d}k$ for all integers k.

3. In the proof of the uniqueness of the Fundamental Theorem of Arithmetic, give two proofs to finish after showing $p_1 = q_1$.

4.(*) Show the following.
(i) Let R be an equivalence relation on A. Then show that the equivalence classes $\overline{A}$ under this equivalence relation partitions A. Conversely, if $\mathcal{C}$ partitions A, define $\sim$ on $A \times A$ by $a \sim b$ if a, b belong to the same set in $\mathcal{C}$. Then $\sim$ is an equivalence relation on A.
(ii) Through each integer point on the x-axis in the plane $\mathbf{R}^2$ draw a line perpendicular to the x-axis and the same with the y-axis. Define a (systematic) partition of the plane that this defines. [Be careful with points on the various lines.] (Of course, there are many such. I like the one(s) that give nice geometric objects – when looked it at correctly.)

5. Let $m > 1$ be an integer. Show all of the following:
(i) Congruence modulo m is an equivalence relation. In particular,

$$\mathbf{Z} = \overline{0} \vee \overline{1} \vee \ldots \vee \overline{m-1}$$

i.e., there are m equivalence classes. Let $\mathbf{Z}/m\mathbf{Z} = \mathbf{Z}/\equiv \bmod m = \{\overline{0}, \ldots, \overline{m-1}\}$.

(ii) Let $a, b, c, d \in \mathbf{Z}$ satisfy

$$a \equiv c \pmod{m} \text{ and } b \equiv d \pmod{m}$$

then

$$a + b \equiv c + d \pmod{m} \text{ and } a \cdot b \equiv c \cdot d \pmod{m}$$

(i.e., $\overline{a+b} = \overline{c+d}$ and $\overline{a \cdot b} = \overline{c \cdot d}$).

(iii) Now define a $+$ and $\cdot$ on $\mathbf{Z}/m\mathbf{Z}$ by $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.
Show that this is *well-defined*, i.e., if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$ then $\overline{a+b} = \overline{a'+b'}$ and $\overline{a \cdot b} = \overline{a' \cdot b'}$.

(iv) This $+$ and $\cdot$ make $\mathbf{Z}/m\mathbf{Z}$ into a *commutative ring*.
That is the following axioms are satisfied for all $\overline{a}, \overline{b}, \overline{c} \in \mathbf{Z}/m\mathbf{Z}$:

1. $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$ [*Associativity*]
2. $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ [*Commutativity*]
3. $\overline{a} + \overline{0} = \overline{a}$ [*Existence of zero*]
4. $\overline{a} + (\overline{-a}) = \overline{0}$ [*Existence of additive inverses*]
5. $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$ [*Associativity of Multiplication*]
6. $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ [*Commutativity of Multiplication*]
7. $\overline{a} \cdot \overline{1} = \overline{a} = \overline{1} \cdot \overline{a}$ [*Existence of one*]
8. $\overline{c} \cdot (\overline{a} + \overline{b}) = \overline{c} \cdot \overline{a} + \overline{c} \cdot \overline{b}$ [*Distributative Law*]
9. $(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$ [*Distributative Law*]

6. Let c_1, c_2, and c_3 be integers. Find an integer x such that $x \equiv c_1 \pmod{11}$, $x \equiv c_2 \pmod{12}$, and $x \equiv c_3 \pmod{13}$. Find the smallest positive integer x satisfying these equations if $c_1 = 3$, $c_2 = 2$, and $c_3 = 1$.

7. Prove that there exist infinitely many primes congruent to 3 modulo 4.

8.(*) Let p be a prime number. Show that $a^p \equiv a \pmod{p}$ for all integers a.