HOMEWORK ASSIGNMENT # 1
DUE, Friday, October 3

Collaboration: On the homework sets, collaboration is not only allowed but encouraged. However, you must write up and understand your own individual homework solutions, and you may not share written solutions. If you learn how to solve a problem by talking to a classmate, CA, or looking it up in a book, you should cite the source in your homework write-up, just as you would reference your sources in a literature or history class.
Show all your working, and write up your solutions as neatly as possible.

1. (1 point each) Compute the following gcd's using the Euclidean Algorithm (show your steps).
$$\gcd(64, 28), \qquad \gcd(119, 49), \qquad \gcd(144, 89)$$
2. **Efficiency of the Euclidean Algorithm**. Let
$$\phi = \frac{\sqrt{5}-1}{2}$$
be a solution to $\phi^2 + \phi = 1$. Let a_0, a_1 be positive integers such that $a_0 > a_1$, and let
$$a_0 = q_1 a_1 + a_2, \qquad 0 \le a_2 < a_1.$$
   (a) (3 points) Prove that
$$a_0 + \phi a_1 \ge (1+\phi)(a_1 + \phi a_2).$$
   (b) (2 points) Conclude that if a_0 and a_1 each have a billion digits, then the Euclidean Algorithm will terminate in under five billion iterations.
3. (3 points) Find all integral solutions to the following equation:
$$64x + 28y = 12.$$
4. (4 points) Find the *second* smallest positive integer solution to the following simultaneous equations:
$$x \equiv 5 \mod 7$$
$$x \equiv 7 \mod 11$$
$$x \equiv 11 \mod 13$$
5. (3 points) Find a positive integer m and a monic polynomial $f(x) = x^d + \ldots$ of degree d such that $f(x) \equiv 0 \mod m$ has *more* than d distinct solutions modulo m.
6. (2 points) Find all solutions to $\varphi(n) = 2$.