Math 3200 – Midterm
Spring – 2015
Odenthal

You must show and explain your work!!
You will be evaluated on your methods.
It isn't enough to get the correct answer.

---

1. (125 pts) Evaluate Euler's phi function $\phi(6000)$.

2. (125 pts) Use the Euclidean Algorithm to find $d = \gcd(189, 119)$ and find integers x and y so that $d = 189x + 119y$.

   Extra credit: (100 pts) Use the *extended* version of the algorithm.

3. (125 pts) Find the *smallest positive* integer x that solves the following system of simultaneous congruences:

$$x \equiv 5 \pmod{16}$$
$$x \equiv 3 \pmod{7}$$

4. (125 pts) Use one round of the Miller-Rabin Primality Test with (not so random) $a = 12$ to check whether 65 is prime. (Yes, I know that 65 isn't prime, but that's not the point – what does the Miller-Rabin test say?)

5. (125 pts) I'm running the RSA algorithm with modulus $n = 319$. Unfortunately I've chosen p and q too close together. Factor n by the method shown in class (known in some circles as Fermat's algorithm).

6. (125 pts) I'm running the RSA algorithm with modulus $n = 55 = 5 \cdot 11$ and encoding key $e = 3$. Find the decoding key d.

7. (125 pts) I'm running the RSA algorithm with modulus $n = 209$ but you've discovered that $\phi(n) = 180$. Use this information together with the algorithm from class to factor n.

8. (125 pts) Evaluate $5^{35} \pmod{51}$ by hand in an efficient manner.