Math 110 Homework # 1.

Due in class on Friday, April 12. Show your work.

1. Let $a = 602$ and $b = 266$.

(a) Use the Euclidean algorithm to compute $d = \gcd(a, b)$.

(b) Use the "magic box" algorithm to find integers u and v such that $au + bv = d$.

(c) Characterize all solutions to $au + bv = d$.

2. The following two messages were encrypted in English by taking a cyclic shift (modulo 26) and deleting spaces between words. Decipher them and explain how the encoding was done.

(a) thismessagewasencodedusingacyclicshiftbyzero

(b) uijtjtbmtpbofbtzqspcmfn

3. Encrypt the following messages using an affine cipher with the affine function $3x+1 \pmod{26}$.

ilovemath

4. Suppose you encrypt a message using a shift cipher, then encrypt the encryption using another shift cipher (both are working modulo 26). Is there any advantage to doing this, rather than using a single shift cipher? Why or why not? What about if you replace shift cipher in each instance above by an affine cipher?

4. Show that for any integers n, m, k with $\gcd(n, m) = 1$ that

$$\gcd(k, nm) = \gcd(k, n)\gcd(k, m).$$

5 Use the Fast Powering Algorithm to compute $7^{1033} \pmod{17}$.

6. Define $2 \uparrow n$ by $2 \uparrow 0 = 1$ and $2 \uparrow n = 2^{2 \uparrow (n-1)}$. In other words,

$$2 \uparrow n = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \quad \text{(a tower of } n \text{ twos)}.$$

Compute $2 \uparrow 100$ modulo 17. Hint: use Fermat's Little Theorem.

7. Suppose a positive integer n has at least four distinct prime factors and satisfies $n < 1000$. Must n be even? Why? You should use a theorem from class.