CRYPTOGRAPHY HANDOUT 15

NUMBER THEORY PRACTICE

1. Use the Euclidean Algorithm to find the gcd for the following pairs of numbers:

   a. $\gcd(14129, 9353)$

   b. $\gcd(30073, 12749)$

2. Compute the Euler Phi Function for the following:

   a. $\varphi(25)$

   b. $\varphi(40)$

   c. $\varphi(29)$

d. $\varphi(17)$

e. $\varphi(p)$ where p is a prime

3. Use Fermat's Little Theorem to evaluate the following:

a. $11^{12} \bmod 13$

b. $11^{13} \bmod 13$

c. $88^{100} \bmod 101$

d. $a^{100} \bmod 101$ for some number a

e. $88^{203} \bmod 101$

4. Use Euler's Theorem to evaluate the following:

a. $23^{20} \bmod 25$

b. $23^{21} \bmod 25$

c. $31^{16} \bmod 40$

d. $a^{16} \bmod 40$ for some number a

e. $17^{55} \bmod 40$

5. Determine the order of the following numbers a and primes p (recall the order is the smallest power k in which $a^k \equiv 1 \bmod p$):

a. $a = 3, p = 7$

b. $a = 2, p = 7$

c. $a = 3, p = 23$

d. $a = 7, p = 13$

6. In the previous question, which values are primitive roots (i.e. the order is $p-1$)?

7. Given an integer a and an odd prime p, determine if a is a square mod p (use Euler's Criterion).

a. $a = 3, p = 7$

$3^{\frac{7-1}{2}} \equiv -1 \bmod 7$ so 3 is not a square mod 7.

b. $a = 10, p = 13$

c. $a = 10, p = 17$

d. $a = 45, p = 199$

8. Use the Legendre symbol $\left(\frac{a}{p}\right)$ to determine whether $a = -1$ is a square or not for the following primes p:

a. $p = 17$

b. $p = 59$

c. $p = 83$

9. First, complete the following table. Then use Euler's Criterion and Quadratic Reciprocity to determine the next questions.

Prime p	Congruent to 1 mod 4 or 3 mod 4?
19	
29	
61	
67	

a. $\left(\frac{19}{29}\right)$

b. $\left(\frac{29}{19}\right)$

c. $\left(\frac{29}{61}\right)$

d. $\left(\frac{61}{29}\right)$

e. $\left(\frac{67}{19}\right)$

f. $\left(\frac{19}{67}\right)$