CRYPTOGRAPHY HANDOUT 15

NUMBER THEORY PRACTICE SOLUTIONS

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

   a. $\gcd(14129, 9353)$

$\gcd(14129, 9353) = 199$

   b. $\gcd(30073, 12749)$

$\gcd(30073, 12749) = 61$

2. Compute the Euler Phi Function for the following:

   a. $\varphi(25)$

20

   b. $\varphi(40)$

16

   c. $\varphi(29)$

28

   d. $\varphi(17)$

16

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

$p - 1$

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

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

$1 \bmod 13$

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

$11^{12} \cdot 11 \bmod 13 \equiv 1 \cdot 11 \bmod 13 \equiv 11 \bmod 13$

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

$1 \bmod 101$

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

$1 \bmod 101$

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

$(88^2)^{100} \cdot 88^3 \bmod 101 \equiv 88^3 \bmod 101 \equiv 25 \bmod 101$

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

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

$1 \bmod 25$

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

$23^{20} \cdot 23 \bmod 25 \equiv 1 \cdot 23 \bmod 25 \equiv 23 \bmod 25$

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

$1 \bmod 40$

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

$1 \bmod 40$

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

$(17^3)^{16} \cdot 17^7 \bmod 40 \equiv 17^7 \bmod 40 \equiv 33 \bmod 40$

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. $a = 3, p = 7$

$k = 6$

b. $a = 2, p = 7$

$k = 3$

c. $a = 3, p = 23$

$k = 11$

d. $a = 7, p = 13$

$k = 12$

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

3 is a primitive root when $p = 7$. Also, 7 is a primitive root when $p = 13$.

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. $a = 10, p = 13$

$10^{\frac{13-1}{2}} \equiv 1 \bmod 13$ so 10 is a square mod 13.

c. $a = 10, p = 17$

$10^{\frac{17-1}{2}} \equiv -1 \bmod 7$ so 10 is not a square mod 17.

d. $a = 45, p = 199$

$45^{\frac{199-1}{2}} \equiv 1 \bmod 199$ so 45 is a square mod 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. $p = 17$

17 mod 4 $\equiv$ 1 mod 4, so it is a square.

b. $p = 59$

59 mod $4 \equiv 3$ mod 4, so it is not a square.

c. $p = 83$

83 mod $4 \equiv 3$ mod 4, so it is not a square.

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	3
29	1
61	1
67	3

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

-1

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

-1

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

-1

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

-1

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

-1

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

1