Homework 4
(Units, Euler's function, RSA, primitive roots.)
Due Wednesday, October 23 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet**.

(1) Calculate $\phi(72)$ and confirm it by finding a reduced set of residues modulo 72.
Since $72 = 9 \cdot 8$ and $\gcd(9, 8) = 1$,

$$\phi(72) = \phi(9)\phi(8) = (3^2 - 3^1)(2^3 - 2^2) = 6 \cdot 4 = 24.$$

One reduced set of residues is

$$\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71\}.$$

(2) Show that if $\gcd(m, n) \neq 1$, then $\phi(mn) > \phi(m)\phi(n)$.

Proof. Suppose that $\gcd(m, n) = d \neq 1$. If

$$m = p_1^{e_1} \cdots p_k^{e_k}$$

and

$$n = p_1^{f_1} \cdots p_k^{f_k}$$

are prime factorizations of m and n where $e_i, f_i \geq 0$, one each of e_i and f_i is nonzero, and p_i are all distinct, then

$$\phi(mn) = mn \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

While

$$\phi(m)\phi(n) = m \prod_{e_i \neq 0} \left(1 - \frac{1}{p_i}\right) n \prod_{f_i \neq 0} \left(1 - \frac{1}{p_i}\right)$$

where we multiply over all i such that $e_i \neq 0$ and $f_i \neq 0$, respectively. Note that each of the p_i appears at least once in the second formula. If, for some i, p_i divides both m and n, then the factor of $\left(1 - \frac{1}{p_i}\right)$ appears twice in the second formula. Since $\left(1 - \frac{1}{p_i}\right) > \left(1 - \frac{1}{p_i}\right)^2$ and since $\gcd(m, n) \neq 1$ implies that there is at least one such p_i, we have that $\phi(mn) > \phi(m)\phi(n)$. □

(3) Show that if m and n are positive integers such that $m \mid n$, then $\phi(m) \mid \phi(n)$.
Hint: Use the prime factorizations of m and n.

Proof. Let m and n be positive integers such that $m \mid n$. Then if n has prime factorization

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

where the p_i are distinct primes and $e_i \geq 1$ for all i, then m has prime factorization

$$m = p_1^{f_1} \cdots p_k^{f_k}$$

where $0 \leq f_i \leq e_i$ for all i. Let $i \in \{1, \ldots, k\}$ and consider the following:

- If $f_i = e_i$, then $\phi(p_i^{e_i}) = \phi(p_i^{f_i})$.
- If $0 < f_i < e_i$, then $\phi(p_i^{f_i}) = p_i^{f_i-1}(p_i - 1)$ since $f_i > 0$. In this case, $p_i^{f_i-1} \mid p_i^{e_i-1}$ since $f_i < e_i$. So because $p_i - 1 \mid p_i - 1$, we have that
$$\phi(p_i^{f_i}) = p_i^{f_i-1}(p_i - 1) \mid p_i^{e_i-1}(p_i - 1) = \phi(p_i^{e_i}).$$
- If $f_i = 0$, then $\phi(p_i^{f_i}) = \phi(1) = 1 \mid \phi(p_i^{e_i})$.

So, for all i, $\phi(p_i^{f_i}) \mid \phi(p_i^{e_i})$. Therefore
$$\prod_{i=1}^{k} \phi(p_i^{f_i}) \mid \prod_{i=1}^{k} \phi(p_i^{e_i}).$$
The right-hand side is clearly $\phi(n)$. The left-hand side is equal to $\phi(m)$ since the instances where $f_i = 0$ only have the effect of multiplying $\phi(m)$ by 1. □

(4) Find all n such that $\phi(n) = 12$.
Answer: 13, 21, 26, 28, 36, 42.
Solution: Suppose that $\phi(n) = 12$ and $n = p_1^{e_1} \cdots p_k^{e_k}$ is a prime-power factorization of n. Then
$$12 = \phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k}).$$
Thus each $\phi(p_i^{e_i})$ divides 12 and so $\phi(p_i^{e_i})$ must be one of
$$1, 2, 3, 4, 6, \text{ and } 12.$$
Recalling that $\phi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$, we compute the following.
- If $\phi(p_i^{e_i}) = 1$, then $p_i^{e_i-1} = p_i - 1 = 1$ and so $p_i = 2$ and $e_i = 1$.
- If $\phi(p_i^{e_i}) = 2$, then either
  (a) $p_i^{e_i-1} = 1$ and $p_i - 1 = 2$, so $p_i = 3$ and $e_i = 1$, or
  (b) $p_i^{e_i-1} = 2$ and $p_i - 1 = 1$, so $p_i = 2$ and $e_i = 2$.
- If $\phi(p_i^{e_i}) = 3$, then either
  (a) $p_i^{e_i-1} = 3$ and $p_i - 1 = 1$, which implies that $p_i = 2$ and a power of 2 cannot be 3, so this cannot occur, or
  (b) $p_i^{e_i-1} = 1$ and $p_i - 1 = 3$, which implies that $p_i = 4$ and so cannot occur since p_i is prime.
- If $\phi(p_i^{e_i}) = 4$, then either
  (a) $p_i^{e_i-1} = 1$ and $p_i - 1 = 4$, so $p_i = 5$ and $e_i = 1$, or
  (b) $p_i^{e_i-1} = 4$ and $p_i - 1 = 1$, so $p_i = 2$ and $e_i = 3$, or
  (c) $p_i^{e_i-1} = 2$ and $p_i - 1 = 2$, which cannot occur(no power of 3 is equal to 2).
- If $\phi(p_i^{e_i}) = 6$, there are four cases to consider, and only two can work:
  (a) $p_i^{e_i-1} = 1$ and $p_i - 1 = 6$, so $p_i = 7$ and $e_i = 1$, or
  (b) $p_i^{e_i-1} = 3$ and $p_i - 1 = 2$, so $p_i = 3$ and $e_i = 2$.
- If $\phi(p_i^{e_i}) = 12$, there are 6 cases to consider, and only one works:
  (a) $p_i^{e_i-1} = 1$ and $p_i - 1 = 12$, so $p_i = 13$ and $e_i = 1$.

Noting that $\phi(p_i^{e_i}) = 3$ does not occur, we look at factorizations of 12 which avoid 3. Note that $p_i = 2$ can only occur once in each product and $p_i = 3$ can only occur once in each product.
- $12 = 2 \cdot 6 = \phi(3)\phi(7) = \phi(21)$
- $12 = 2 \cdot 6 = \phi(2^2)\phi(7) = \phi(28)$
- $12 = 2 \cdot 6 = \phi(2^2)\phi(3^2) = \phi(36)$

- $12 = 1 \cdot 2 \cdot 6 = \phi(2)\phi(3)\phi(7) = \phi(42)$
- $12 = 1 \cdot 12 = \phi(2)\phi(13) = \phi(26)$
- $12 = 12 = \phi(13)$

(5) Consider the groups of units U_{15} and U_7. For each group, complete the following.

(a) List the elements of the group.

$$U_{15} = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$$
$$U_7 = \{[1], [2], [3], [4], [5], [6]\}$$

(b) Match each element with its multiplicative inverse.

For U_{15}:

- [1] is its own inverse.
- [2][8] = [16] = [1], so [2] and [8] are inverses.
- [4][4] = [16] = [1], so [4] is its own inverse.
- [7][13] = [91] = [1], so [7] and [13] are inverses.
- [11][11] = [121] = [15 · 8 + 1] = [1], so [11] is its own inverse.
- [14][14] = [196] = [15 · 13 + 1] = [1], so [14] is its own inverse.

For U_7:

- [1] is its own inverse.
- [2][4] = [8] = [1], so [2] and [4] are inverses.
- [3][5] = [15] = [1], so [3] and [5] are inverses.
- [6][6] = [36] = [1], so [6] is its own inverse.

(c) Find the order of each element. For U_{15}:

- [1] has order 1.
- $2^1 \equiv_{15} 2,\ 2^2 \equiv_{15} 4,\ 2^3 \equiv_{15} 8,\ 2^4 = 16 \equiv_{15} 1$, so [2] has order 4.
- $4^1 \equiv_{15} 4,\ 4^2 = 16 \equiv_{15} 1$, so [4] has order 2.
- $7^1 \equiv_{15} 7,\ 7^2 = 49 \equiv_{15} 4,\ 7^3 \equiv_{15} 7 \cdot 4 = 28 \equiv_{15} -2,$ $7^4 \equiv_{15} 7 \cdot (-2) = -14 \equiv_{15} 1$, so [7] has order 4.
- $8^1 \equiv_{15} 8,\ 8^2 = 64 \equiv_{15} 4,\ 8^3 \equiv_{15} 8 \cdot 4 = 32 \equiv_{15} 2,\ 8^4 \equiv_{15} 8 \cdot 2 = 16 \equiv_{15} 1$, so [8] has order 4.
- $11^1 \equiv_{15} 11,\ 11^2 = 121 \equiv_{15} 1$, so [11] has order 2.
- $13^1 \equiv_{15} 13,\ 13^2 = 169 \equiv_{15} 4,\ 13^3 \equiv_{15} 13 \cdot 4 = 52 \equiv_{15} 7,$ $13^4 \equiv_{15} 13 \cdot 7 = 91 \equiv_{15} 1$, so [13] has order 4.
- $14^1 \equiv_{15} 14,\ 14^2 = 196 \equiv_{15} 1$, so [14] has order 2.

For U_7:

- [1] has order 1.
- $2^1 \equiv_7 2,\ 2^2 \equiv_7 4,\ 2^3 = 8 \equiv_7 1$, so [2] has order 3.
- $3^1 \equiv_7 3,\ 3^2 = 9 \equiv_7 2,\ 3^3 = 27 \equiv_7 -1,\ 3^4 \equiv_7 3 \cdot (-1) = -3,$ $3^5 \equiv_7 3 \cdot (-3) = -9 \equiv_7 -2,\ 3^6 \equiv_7 3 \cdot (-2) = -6 \equiv_7 1$, so [3] has order 6.
- $4^1 \equiv_7 1,\ 4^2 = 16 \equiv_7 2,\ 4^3 = 64 \equiv_7 1$, so [4] has order 3.
- $5^1 \equiv_7 5,\ 5^2 = 25 \equiv_7 4,\ 5^3 \equiv_7 5 \cdot 4 = 20 \equiv_7 -1,\ 5^4 \equiv_7 5 \cdot -1 = -5 \equiv_7 2,$ $5^5 \equiv_7 5 \cdot 2 = 10 \equiv_7 3,\ 5^6 \equiv_7 5 \cdot 3 = 15 \equiv_7 1$, so [5] has order 6.
- $6^1 \equiv_7 6,\ 6^2 = 36 \equiv_7 1$, so [6] has order 2.

(d) Is the group cyclic? If it is cyclic, find all primitive roots.

Since $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$, and there is no element of order 8 in U_15, it is not cyclic.

Since 7 is prime, we know that U_7 is cyclic. The primitive roots are [3] and [5] since they both have order $\phi(7) = 6$.

(6) Consider the RSA algorithm with $p = 5$ and $q = 11$

(a) Find both the public and private keys.
Public key: $n = 55$ and, say, $e = 3$. (Any e such that $\gcd(e, 40) = 1$ will do.)
Private key: $d = 27$. (This should be the mutliplicative inverse of e modulo $\phi(55) = 40$.)

(b) Encrypt the value $n = 8$. (Use successive squaring and a calculator, if needed.)

$$n^e = 8^3 = 8 \cdot 64 \equiv_{55} 8 \cdot 9 = 72 \equiv_{55} 17$$

So the ciphertext is 17.

(c) Decrypt the value $c = 3$. (Use successive squaring and a calculator, if needed.) We need to compute $c^d = 3^{27}$ modulo 55. We'll use successive squaring:

$$\begin{aligned} 3^2 &\equiv_{55} 9 \\ 3^4 = 81 &\equiv_{55} 26 \\ 3^8 &\equiv_{55} (26)^2 = 676 \equiv_{55} 16 \\ 3^{16} &\equiv_{55} (16)^2 = 256 \equiv_{55} 36 \end{aligned}$$

So

$$\begin{aligned} 3^{27} = 3^{16+8+2+1} &\equiv_{55} 36 \cdot 16 \cdot 9 \cdot 3 \\ &= 36 \cdot 144 \cdot 3 \\ &\equiv_{55} 36 \cdot 34 \cdot 3 \\ &= 36 \cdot 102 \\ &\equiv_{55} 36 \cdot (-8) \\ &= -288 \\ &\equiv_{55} -13 \\ &\equiv_{55} 42. \end{aligned}$$

So the original message would have been $n = 42$.

Fun problem (will not be graded): For each of the following statements, produce examples (values of integers x, y, and z) where the statement holds.

(1) $\phi(x) + \phi(y) = \phi(x + y)$.
(2) $\phi(x) + \phi(y) \neq \phi(x + y)$.
(3) $\phi(x^2) + \phi(y^2) = \phi(z^2)$ and $x^2 + y^2 = z^2$.
(4) $\phi(x^2) + \phi(y^2) \neq \phi(z^2)$ and $x^2 + y^2 = z^2$.

Do you think there are infinitely many examples in (1) and (3)?