6.1

Question: Find the orders of the elements of U_9 and of U_{10}.

Solution:

$U_9 = \{1, 2, 4, 5, 7, 8\}$ which have order respectively 1,6,3,6,3,2

$U_{10} = \{1, 3, 7, 9\}$ which have order respectively 1,4,4,2

6.2

Question: Show that if l and m are positive integers with highest common factor h, then $gcd(2^l-1, 2^m-1)$ divides $2^h - 1$.

Solution:

Let k be the order of the element 2 in the group U_n. Since h divides $2^l - 1$, $2^l = 1$ in U_n which implies that $k|l$. Similarly k divides m, so $k|gcd(l, m) = h$. Then $2^n = 1$ in U_n since $2^k = 1$ and $k|h$ which implies that $n|2^n - 1$. $\square$

6.3

Question: The groups U_{10} and U_{12} both have order 4; show that exactly one of them is cyclic.

Solution:

By Homework Problem 6.1 we know that the elements $\{1, 3, 7, 9\}$ of U_{10} are generated by 3 since $3^4 = 1$, $3^1 = 3$, $3^3 = 7$, $3^2 = 9$. Thus U_{10} is generated by 3. In U_{12} $1^2, 5^2, 7^2, 11^2 = 1$, thus no element has order $\phi(12) = 4$.

6.4

Question: Find primitive roots in U_n for n = 18, 23, 27 and 31.

Solution:

Recall that by a previous Lemma, we have that an element $a \in U_n$ is a primitive root if and only if $a^{\frac{\phi(n)}{q}} \neq 1$ in U_n for each q dividing $\phi(n)$.

For the case of n = 18 we consider a = 5 since a=2, a=3, a=4 are not units mod(18). Meanwhile, $5^{\frac{\phi(18)}{q}} \neq 1$ in U_18 for q dividing $\phi(18)$

For n = 23 we take a = 5 again since a=2, a=3, a=4 are not units mod(23). $5^{\frac{\phi(23)}{q}} \neq 1$ in U_23 for q dividing $\phi(23)$

For n = 27 we can instead take a = 2 since a=2 is a unit mod(27). Furthermore $2^{\frac{\phi(27)}{q}} \neq 1$ in U_27 for q dividing $\phi(27)$

For n = 31 we can not take a = 2 but instead must go to a = 3 to get $3^{\frac{\phi(31)}{q}} \neq 1$ in U_31 for q dividing $\phi(31)$

6.5

Question: Show that if U_n has a primitive root then it has $\phi(\phi(n))$ of them.

Solution:

Suppose a is a primitive root of U_n. Then we know that U_n is cyclic and can be generated by a. The order of U_n can be written as $m = \phi(n)$. Thus, we see that U_n can be generated by a^k if and only if k and m are relatively prime. The number of primitive roots a^k is $\phi(m) = \phi(\phi(n))$. $\square$

6.6

Question: Verify that the element 5 is a generator of U_7

To verify that the element 5 is a generator of U_7, consider the powers of 5 in U_7 : $5^1 = 5, 5^2 = 4, 5^3 = 6, 5^4 = 2, 5^5 = 3, 5^6 = 1$. Thus, every element of U_7 can be written as a power of 5, which implies that the element 5 generates U_7. $\square$

6.7

Question: Find the elements of order d in U_{11}, for each d dividing 10; which elements are generators?
Solution:
Elements which divide 10 are: $\{1, 2, 5, 10\}$ and the elements of order d form the sets $\{1\}$, $\{10\}$, $\{3, 4, 5, 9\}$, and $\{2, 6, 7, 8\}$. The generators are $\{2, 6, 7, 8\}$.

6.8

Question: Verify that 2 is a primitive root mod(25) by calculating its powers.
Solution:
To verify that 2 is a primitive root mod(25), we consider the powers of 2 in the unit group U_25. The powers of 2 are $\{2, 4, 8, 16, 7, 14, 3, 6, 12, 24 = -1, -2 = 23, -4 = 21, -8 = 17, -16 = 9, 18, 11, 22 = -3, -6 = 19, -12 = 13, 1\}$. Thus 2 has order $20 = \phi(25)$ which implies that 2 is a primitive root mod(25).

6.9

Question: Show that 2 is a primitive root mod (3^e) for all $e \geqslant 1$.
Solution:
To show that 2 is a primitive root mod (3^e) given $e \geqslant 1$ we first consider it as a primitive root mod (3^2). If we can show that 2 is a primitive root mod (3^2) in U_{3^2}, it will follow that it is also a primitive root mod (3^e) for all e. Now, 2 has order $\phi(3^2) = 6$ in U_{3^2} which implies that 2 is a primitive root mod(3^2). Thus, we conclude that 2 is a primitive root mod (3^e) for all $e \geqslant 1$. $\square$

6.10

Question: Find an integer which is a primitive root $mod(7^e)$ for all $e \geqslant 1$.
Solution:
3 is a primitive root mod(7). $3^6 = 729 \neq 1 \bmod (7^2)$ thus 3 is a primitive root mod (7^e) for e = 2 and therefore all e.

Problem 2

Question: Check that 3 is a primitive root modulo 17 by constructing an explicit isomorphism between $Z/16Z$ and $(Z/17Z)^x$ mapping the class of 1 on the class of 3. Use this map to solve the congruence equations
Solution:
$3^1 = 3 \neq 1, 3^2 = 9 \neq 1, 3^4 = (3^2)^2 = 81 = 13 \neq 1, 3^8 = (3^4)^2 = 13^2 = 169 = 16 \neq 1.$. By Fermat's little theorem and Lagrange Theorem, 3 is a primitive root modulo 17.

(a)

$z^{12} \equiv 16 \bmod 17$
Solution:
First note that any solution z must be a unit mod (17), so z, like 16 is an element of U_17. By corollary, this group is cyclic so both z and 16 can be expressed as powers of a primitive root g mod(17). Since we know that 3 is a primitive root mod(17) we take g = 3. The powers of 3 (mod 17) are 3,9,10,13,15,11,16,15,8,7,4,12,2,6,1. We see that $3^7 = 16$ in U_17 so we write z = 3^i where the exponent i is unknown. Then $z^{12} = 3^{12i}$ so our congruence becomes $3^{12i} = 3^{12}$ in U_17. 3, because it is a primitive root has order $\phi(17) = 16$ so $3^{12i} = 3^{12}$ if and only if $12i \equiv 12 \bmod (16)$ or equivalently $i \equiv 1 \bmod (16)$. The relevant values of i are 1 and 13 so the solutions of the original congruence are $z \equiv 3, 3^13 \bmod (17)$. $3^13 \equiv 2$. There are two congruence classes of solutions, namely $z \equiv 3, 2 \bmod (17)$.

(b)

$x^{20} \equiv 13 \bmod 17$
Solution:
Any solution x must be a unit mod (17), so x, like 13 is an element of U_17. This group is cyclic so both x and 13 can be expressed as powers of a primitive root 3 mod(17). The powers of 3 (mod 17) are again: 3,9,10,13,15,11,16,15,8,7,4,12,2,6,1. We see that $3^4 = 13$ in U_17 so we write z = 3^i where the exponent i is unknown. Then $x^{20} = 3^{20i}$ so our congruence becomes $3^{20i} = 3^{20}$ in U_17. $3^{20i} = 3^{20}$ if and only if $20i \equiv 20$ mod(16) or equivalently $i \equiv 1$ mod (16). The relevant values of i are 1, 5, 9 and 13 so the solutions of the original congruence are $x \equiv 3, 3^4$ mod (17). $3^4 \equiv 13$. We further notice that $x \equiv -3 \equiv 14 and x \equiv -5 \equiv 12$. Thus there are four congruence classes of solutions, $x \equiv 3, 5, 12 and 14$ mod (17).

(c)

$x^{48} \equiv 9 \bmod 17$
Solution:
Any solution x must be a unit mod (17), so x, like 9 is an element of U_17. This group is cyclic so both x and 9 can be expressed as powers of a primitive root 3 mod(17). The powers of 3 (mod 17) are 3,9,10,13,15,11,16,15,8,7,4,12,2,6,1. We see that $3^2 = 9$ in U_17 so we write z = 3^i where the exponent i is unknown. Then $x^{48} = 3^{48i}$ so our congruence becomes $3^{48i} = 3^{48}$ in U_17. $3^{48i} = 3^{48}$ if and only if $48i \equiv 48$ mod(16) or equivalently $i \equiv 1$ mod (16). The relevant values of i are 1, 3, 5, 7, 9, 11, 13 and 15 so the solutions of the original congruence are $x \equiv 3, 3^2$ mod (17). $3^2 \equiv 9$. There are 8 congruence classes of solutions.

(d)

$x^{11} \equiv 9 \bmod 17$
Solution:
Solutions of x must be unit mod (17), so x and 9 are elements of U_17. This group is cyclic so both x and 9 can be expressed as powers of a primitive root 3 mod(17). The powers of 3 (mod 17) are 3,9,10,13,15,11,16,15,8,7,4,12,2,6,1. We see that $3^2 = 9$ in U_17 so we write z = 3^i where the exponent i is unknown. Then $x^{11} = 3^{11i}$ so our congruence becomes $3^{11i} = 3^{11}$ in U_17. $3^{11i} = 3^{11}$ if and only if $11i \equiv 11$ mod(16) or equivalently $i \equiv 1$ mod (16). The relevant values of i are 1, 3, 5, 7, 9, 11, 13 and 15 so the solutions of the original congruence are $x \equiv 3, 3^2$ mod (17). $3^2 \equiv 9$. There are 8 congruence classes of solutions.

7.1

Question: Find all solutions in Z_{15} of the congruence $x^2 - 3x + 2 \equiv 0$ mod (15).
Solution:
Recall the formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{1}$$

which can be rewritten

$$(2ax + b)^2 = b^2 - 4ac \tag{2}$$

Applying formula we get that x = 1,2,7,11 in Z_{15}

7.2

Question: What square roots do the elements 5 and 16 have in Z_{21}? Hence find all solutions of the congruences $x^2 + 3x + 1 \equiv 0$ mod (21) and $x^2 + 2x - 3 \equiv 0$ mod (21).

Solution: 5 has no square roots in Z_{21} and therefore no solutions. 16 has square roots $\pm 4, \pm 10$ and therefore has solutions 1,-3,4 and -6.