MATH 2500 · Winter 2013 - Assignment 4 Solutions.

1(a) $\phi(89-1) = \phi(88) = \phi(2^3 \cdot 11) = \phi(2^3)\phi(11)$
$= 2^2 \cdot 10 = 40.$
There are 40 primitive roots of 89.

(b) An order must be a divisor of $\phi(89) = 88$. The divisors of 88, and hence the possible orders, are:
1, 2, 4, 8, 11, 22, 44, 88

(c) Since $3^{44} \equiv \left(\frac{3}{89}\right) \bmod 89$
and $\left(\frac{3}{89}\right) = \left(\frac{89}{3}\right) = \left(\frac{2}{3}\right) = -1$ [Note: $89 \equiv 1 \bmod 4$],
we get $3^{44} \equiv -1 \bmod 89$, so the order of 3 is not 44, and it is not a divisor of 44, so also not 1, 2, 4, 11 or 22.

$3^8 \equiv 6561 \equiv 64 \bmod 89$, so 3 also does not have order 8.
Since 3 is not of order 1, 2, 4, 8, 11, 22 or 44, it must be of order 88; and is hence a primitive root.

(d) We note that $(88,3)=1$, $(88,5)=1$, $(88,7)=1$, $(88,9)=1$
so $3^3 \equiv 27 \bmod 89$,
$3^5 \equiv 65 \bmod 89$,
$3^7 \equiv 51 \bmod 89$, and
$3^9 \equiv 14 \bmod 89$.
So 27, 65, 51 and 14 are primitive roots.

(e) Since $4 \equiv 3^{32} \bmod 89$, the order of 4 is $88/(88,32) = 88/8 = 11$,

$12 \equiv 3^{33} \bmod 89$, the order of 12 is $88/(88,33) = 88/11 = 8$

$36 \equiv 3^{34} \bmod 89$, the order of 36 is $88/(88,34) = 88/2 = 44$

2(a) $x^2 + 11x + 6 \equiv 0 \bmod 53$

$x^2 + 64x + 6 \equiv 0 \bmod 53$

$(x^2 + 64x + 1024) - 1024 + 6 \equiv 0 \bmod 53$

$(x+32)^2 \equiv 1018 \bmod 53$

$(x+32)^2 \equiv 11 \bmod 53$

$\left(\frac{11}{53}\right) = \left(\frac{53}{11}\right) = \left(\frac{9}{11}\right) = 1$ (note: $53 \equiv 1 \bmod 4$)

So the quadratic congruence does have solutions

(b) $7x^2 + 3x + 30 \equiv 0 \bmod 71$ $\quad 71 = 7(10) + 1 \Rightarrow 1 = 71 + 7(-10)$

$x^2 - 30x - 300 \equiv 0 \bmod 71$

$(x^2 - 30x + 225) - 225 - 300 \equiv 0 \bmod 71$

$(x-15)^2 \equiv 525 \bmod 71$

$(x-15)^2 \equiv 28 \bmod 71$

$\left(\frac{28}{71}\right) = \left(\frac{7}{71}\right)\left(\frac{4}{71}\right) = (-1)\left(\frac{71}{7}\right)(1) = (-1)\left(\frac{1}{7}\right) = -1$ $\quad (7 \equiv 71 \equiv 3 \bmod 4)$

So the quadratic congruence does not have solutions.

2(c) $6x^2+7x+1 \equiv 0 \mod 37$ $\quad 37 = 6(6)+1;\ 1 = 37+6(-6)$

$x^2-42x-6 \equiv 0 \mod 37$

$(x^2-42x+441)-441-6 \equiv 0 \mod 37$

$(x-21)^2 \equiv 447 \mod 37$

$(x-21)^2 \equiv 3 \mod 37$

$\left(\frac{3}{37}\right) = \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1$ $\quad [37 \equiv 1 \mod 4]$

So the quadratic congruence does have solutions.

3(a) $\left(\frac{3879}{6211}\right) = \left(\frac{3^2}{6211}\right)\left(\frac{431}{6211}\right)$ $\quad 431 \equiv 6211 \equiv 3 \mod 4$

$= (-1)\left(\frac{6211}{431}\right) = -\left(\frac{177}{431}\right) = -\left(\frac{3}{431}\right)\left(\frac{59}{431}\right)$ $\quad 59 \equiv 3 \mod 4$

$= -(-1)\left(\frac{431}{3}\right)(-1)\left(\frac{431}{59}\right) = (-1)\left(\frac{2}{3}\right)\left(\frac{18}{59}\right)$

$= (-1)(-1)\left(\frac{2}{59}\right)\left(\frac{9}{59}\right) = (-1)(1) = -1$ $\quad 59 \equiv 3 \mod 8$

(b) $\left(\frac{2184}{8999}\right) = \left(\frac{2^3}{8999}\right)\left(\frac{3}{8999}\right)\left(\frac{7}{8999}\right)\left(\frac{13}{8999}\right)$

$= \left(\frac{2}{8999}\right)(-1)\left(\frac{8999}{3}\right)(-1)\left(\frac{8999}{7}\right)\left(\frac{8999}{13}\right)$ $\quad 8999 \equiv 7 \equiv 3 \mod 4,\ 13 \equiv 1 \mod 4$

$= (1)\left(\frac{2}{3}\right)\left(\frac{4}{7}\right)\left(\frac{3}{13}\right)$ $\quad 8999 \equiv 7 \mod 8$

$= (-1)(1)\left(\frac{13}{3}\right) = (-1)\left(\frac{1}{3}\right) = -1$

(c) $\left(\frac{3433}{7001}\right) = \left(\frac{7001}{3433}\right) = \left(\frac{135}{3433}\right)$ $\quad 7001 \equiv 1 \mod 4$

$= \left(\frac{3^3}{3433}\right)\left(\frac{5}{3433}\right) = \left(\frac{3}{3433}\right)\left(\frac{5}{3433}\right)$

$= \left(\frac{3433}{3}\right)\left(\frac{3433}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{3}{5}\right)$ $\quad 3433 \equiv 1 \mod 4$

$= (1)\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$ $\quad 5 \equiv 1 \mod 4$

4 For $p = 3623$, $p-1 = 3622 = 2 \cdot 1811$ (1811 is prime),
So the order of an element mod 3623 is 1, 2, 1811 or 3622.

Since $2^2 \equiv 4 \bmod 3623$, $3^2 \equiv 9 \bmod 3623$, $4^2 \equiv 16 \bmod 3623$ and $5^2 \equiv 25 \bmod 3623$; none of 2, 3, 4 and 5 have 2 as their order.

Checking the 1811 power via Euler's Criterion:

$\left(\frac{2}{3623}\right) = 1$ $(3623 \equiv 7 \bmod 8)$ so $2^{1811} \equiv 1 \bmod 3623$

$\left(\frac{3}{3623}\right) = (-1)\left(\frac{3623}{3}\right) = (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1$ so $3^{1811} \equiv 1 \bmod 3623$
$[3623 \equiv 3 \bmod 4]$

$\left(\frac{4}{3623}\right) = 1$ so $4^{1811} \equiv 1 \bmod 3623$

$\left(\frac{5}{3623}\right) = \left(\frac{3623}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ so $5^{1811} \equiv -1 \bmod 3623$
$[5 \equiv 1 \bmod 4]$

Since 2, 3, 4 have an order smaller than 3622, they are not primitive roots (they have order 1811). Since 5 does not have order 1, 2 or 1811, it must have order 3622, and is a primitive root.

5(a) Suppose a has order t, and t is odd.
Then $(t,2)=1$, and by lemma 10.1, a^2 has the same order as a; a^2 has order t.

Suppose a has order t, and t is even. Since $(t,2)=2$, by lemma 10.1, a^2 cannot have order t, so lets say that a^2 has order s.
Since $(a^2)^t \equiv (a^t)^2 \equiv 1^2 \equiv 1 \bmod m$, we know that $s \mid t$. (Theorem 10.1)
Also $(a^2)^s \equiv a^{2s} \equiv 1 \bmod m$, we know that $t \mid 2s$ (also Theorem 10.1)
From $s \mid t$ we get $t = sk_1$ $(s \neq t \Rightarrow k_1 \neq 1)$, and from $t \mid 2s$ we get $2s = tk_2$.
Combining, we get $2s = sk_1k_2 \Rightarrow k_1k_2 = 2$.
Since k_1 & k_2 are positive integers and $k_1 \neq 1$, then $k_1 = 2$, $k_2 = 1$ and $t = 2s \Rightarrow s = t/2$.
So the order of a^2 is $t/2$.

(b) Since $(ab)^{15} \equiv a^{15}b^{15} \equiv (a^3)^5(b^5)^3 \equiv 1 \bmod m$, we know the order of ab divides 15, so it is 1, 3, 5 or 15.
If the order of ab was 3, then
$1 \equiv (ab)^3 \equiv a^3b^3 \equiv b^3 \bmod m$, which would contradict the order of b being 5.

If the order of ab were 5, then

$1 \equiv (ab)^5 \equiv a^5 b^5 \equiv a^5 \mod m$, which would contradict the order of a being 3. (Theorem 10.1, 5 is not a multiple of 3)

If the order of ab were 1, then b would be the inverse of a modulo m. Now

$a^3 \equiv 1 \equiv ab \mod m$, $(a,m) = 1$ so
$b \equiv a^2 \mod m$.

But by part (a), the order of a is odd, so a^2 has the same order as a, this contradicts the order of b being 5.

Hence the order of ab is 15.