Assignment 4 solutions MATH 2500 Winter 2014

1(a) $\phi(101) = 100$ $\quad 100 = 2^2 \cdot 5^2$

$\phi(100) = \phi(2^2)\,\phi(5^2) = 2(2-1)(5)(5-1) = 40$

The prime 101 has 40 primitive roots.

(b) The order must be a divisor of 100, hence all possible orders are:

1, 2, 4, 5, 10, 20, 25, 50 or 100

(c) We know that $2^{50} \equiv \left(\frac{2}{101}\right) \bmod 101$

and $\left(\frac{2}{101}\right) = -1$ since $101 \equiv 5 \bmod 8$

So the order of 2 is not 50, nor is it a divisor of 50, so not 1, 2, 5, 10 or 25.

Now

$2^4 \equiv 16 \bmod 101$ and

$2^{20} \equiv 1048576 \equiv 95 \bmod 101$

So the order of 2 is also not 4 or 20 either.

Hence the order of 2 is 100, and 2 is a primitive root.

(d) 3, 7 and 11 are relatively prime to 100

$2^3 = 8$, $2^7 \equiv 128 \equiv 27 \bmod 101$, $2^{11} \equiv 2048 \equiv 28 \bmod 101$

So 8, 27 and 28 are primitive roots

1(e) Since $22 \equiv 2^{14} \bmod 101$, the order of 22 is $\frac{100}{(100,14)} = \frac{100}{2} = 50$.
So 22 has order 50.

Since $44 \equiv 2^{15} \bmod 101$, the order of 44 is $\frac{100}{(100,15)} = \frac{100}{5} = 20$
So 44 has order 20.

Since $88 \equiv 2^{16} \bmod 101$, the order of 88 is $\frac{100}{(100,16)} = \frac{100}{4} = 25$
So the order of 88 is 25.

2(a) $2x^2 + 7x + 4 \equiv 0 \bmod 61$

(We find the inverse of 2 mod 61:
$61 = 2(30) + 1$
$1 = 61 + 2(-30)$)

(mult by -30)

$x^2 - 210x - 120 \equiv 0 \bmod 61$

$x^2 + 34x + 2 \equiv 0 \bmod 61$

$(x^2 + 34x + 289) - 289 + 2 \equiv 0 \bmod 61$

$(x+17)^2 \equiv 287 \bmod 61$

$(x+17)^2 \equiv 43 \bmod 61$

$\left(\frac{43}{61}\right) = \left(\frac{61}{43}\right)$ (Since $61 \equiv 1 \bmod 4$)

$= \left(\frac{18}{43}\right)$ (since $61 \equiv 18 \bmod 43$)

$= \left(\frac{2}{43}\right)\left(\frac{9}{43}\right)$ ($18 = 9 \times 2$)

$= \left(\frac{2}{43}\right) = -1$ (9 is 3^2, $43 \equiv 3 \bmod 8$)

Since 43 is a quadratic non residue modulo 61, the original quadratic equation does not have solutions.

2(b) $7x^2 + x + 17 \equiv 0 \mod 73$

(multiply by 21)

$x^2 + 21x + 357 \equiv 0 \mod 73$

$x^2 - 52x + 357 \equiv 0 \mod 73$

$(x^2 - 52x + 676) - 676 + 357 \equiv 0 \mod 73$

$(x-26)^2 \equiv 319 \mod 73$

$(x-26)^2 \equiv 27 \mod 73$

We find the inverse of $7 \bmod 73$

$73 = 7(10) + 3$

$7 = 3(2) + 1$ $\quad 1 = 7 + 3(-2)$

$= 7 + [73 + 7(-10)](-2)$

$= 73(-2) + 7(21)$

$\left(\frac{27}{73}\right) = \left(\frac{3}{73}\right)\left(\frac{9}{73}\right)$ $\quad (27 = 3 \times 9)$

$= \left(\frac{3}{73}\right)$ $\quad (9 = 3^2)$

$= \left(\frac{73}{3}\right)$ $\quad 73 \equiv 1 \mod 4$

$\equiv \left(\frac{1}{3}\right) = 1$ $\quad 73 \equiv 1 \mod 3 \quad (1 = 1^2)$

Since 27 is a quadratic residue mod 73, the original quadratic has solutions.

(c) $x^2 - 77x + 38 \equiv 0 \mod 91$

$x^2 + 14x + 38 \equiv 0 \mod 91$

$(x^2 + 14x + 49) - 49 + 38 \equiv 0 \mod 91$

$(x+7)^2 \equiv 11 \mod 91$

If this has solutions, then so would $(x+7)^2 \equiv 11 \mod 7$, and $(x+7)^2 \equiv 11 \mod 13$.

$\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 1$ $\quad (11 \equiv 4 \mod 7;\ 4 = 2^2)$

$\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1$ $\quad (13 \equiv 1 \mod 4;\ 13 \equiv 2 \mod 11;\ 11 \equiv 3 \mod 8)$

Since 11 is a quadratic nonresidue mod 13, the quadratic has no solutions.

3(a) $\left(\frac{4014}{6551}\right)$ $\quad 4014 = 2 \cdot 3^2 \cdot 223$

$= \left(\frac{2}{6551}\right)\left(\frac{3^2}{6551}\right)\left(\frac{223}{6551}\right)$ $\quad 6551 \equiv 7 \bmod 8$;

$6551 \equiv 223 \equiv 3 \bmod 4$

$= (1)(1)(-1)\left(\frac{6551}{223}\right)$ $\quad 6551 \equiv 84 \bmod 223$

$= (-1)\left(\frac{84}{223}\right)$ $\quad 84 = 2^2 \times 3 \times 7$

$= (-1)\left(\frac{2^2}{223}\right)\left(\frac{3}{223}\right)\left(\frac{7}{223}\right)$ $\quad 223 \equiv 7 \equiv 3 \bmod 4$

$= (-1)(1)(-1)\left(\frac{223}{3}\right)(-1)\left(\frac{223}{7}\right)$ $\quad 223 \equiv 1 \bmod 3$

$227 \equiv -1 \bmod 7$

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

$= (-1)(1)(-1) = 1$

(b) $\left(\frac{3003}{8053}\right)$ $\quad 3003 = 3 \cdot 7 \cdot 11 \cdot 13$

$= \left(\frac{3}{8053}\right)\left(\frac{7}{8053}\right)\left(\frac{11}{8053}\right)\left(\frac{13}{8053}\right)$ $\quad 8053 \equiv 1 \bmod 4$

$= \left(\frac{8053}{3}\right)\left(\frac{8053}{7}\right)\left(\frac{8053}{11}\right)\left(\frac{8053}{13}\right)$ $\quad 8053 \equiv 1 \bmod 3$, $8053 \equiv 3 \bmod 7$

$8053 \equiv 1 \bmod 11$, $8053 \equiv 6 \bmod 13$

$= \left(\frac{1}{3}\right)\left(\frac{3}{7}\right)\left(\frac{1}{11}\right)\left(\frac{6}{13}\right)$ $\quad 7 \equiv 3 \bmod 4$; $6 = 2 \times 3$

$= (1)(-1)\left(\frac{7}{3}\right)(1)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right)$ $\quad 7 \equiv 1 \bmod 3$, $13 \equiv 5 \bmod 8$,

$13 \equiv 1 \bmod 4$

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

(cont'd next)

3(b) (cont'd)

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

3(c) $\left(\frac{3371}{7331}\right)$ $\quad 3371 \equiv 7331 \equiv 3 \bmod 4$

$= (-1)\left(\frac{7331}{3371}\right)$ $\quad 7331 \equiv 589 \bmod 3371$

$= (-1)\left(\frac{589}{3371}\right)$ $\quad 589 = 19 \cdot 31$

$= (-1)\left(\frac{19}{3371}\right)\left(\frac{31}{3371}\right)$ $\quad 19 \equiv 3 \bmod 4\ ;\ 31 \equiv 3 \bmod 4$

$= (-1)(-1)\left(\frac{3371}{19}\right)(-1)\left(\frac{3371}{31}\right)$ $\quad 3371 \equiv 8 \bmod 19\ ;\ 3371 \equiv 23 \bmod 31$

$= (-1)\left(\frac{8}{19}\right)\left(\frac{23}{31}\right)$ $\quad 23 \equiv 3 \bmod 4\ ;\ 8 = 2 \times 4$

$= (-1)\left(\frac{2}{19}\right)\left(\frac{4}{19}\right)(-1)\left(\frac{31}{23}\right)$ $\quad 19 \equiv 3 \bmod 8,\ 4 = 2^2,\ 31 \equiv 8 \bmod 23$

$= (-1)(1)\left(\frac{8}{23}\right)$ $\quad 8 = 2 \times 4$

$= (-1)\left(\frac{2}{23}\right)\left(\frac{4}{23}\right)$ $\quad 23 \equiv 7 \bmod 8,\ 4 = 2^2$

$= (-1)(1) = -1$

4. $\phi(1187) = 1186 = 2 \cdot 593$

So the possible orders are 1, 2, 593 and 1186.

Using Euler's Criterion $a^{593} \equiv \left(\frac{a}{1187}\right) \bmod 1187$.

Now $\left(\frac{3}{1187}\right) = (-1)\left(\frac{1187}{3}\right) = (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1$

$(1187 \equiv 3 \bmod 4)$ $(1187 \equiv 2 \bmod 3)$

So $3^{593} \equiv 1 \bmod 1187$, so 3 is NOT a primitive root of 1187.

$$\left(\frac{5}{1187}\right) = \left(\frac{1187}{5}\right) = \left(\frac{2}{5}\right) = -1$$

$(5 \equiv 1 \bmod 4)$ $(1187 \equiv 2 \bmod 5)$ $(5 \equiv 5 \bmod 8)$

So $5^{593} \equiv -1 \bmod 1187$, so the order of 5 is not 1 or 593.
Also since $5^2 \equiv 25 \bmod 1187$, the order of 5 is not 2
Hence 5 is a primitive root of 1187.

$$\left(\frac{7}{1187}\right) = (-1)\left(\frac{1187}{7}\right) = (-1)\left(\frac{4}{7}\right) = (-1)(1) = -1$$

$(7 \equiv 1187 \equiv 1 \bmod 4)$ $(1187 \equiv 4 \bmod 7)$ $(4 = 2^2)$

So $7^{593} \equiv -1 \bmod 1187$, so the order of 7 is not 1 or 593.
Also, since $7^2 \equiv 49 \bmod 1187$, the order of 7 is not 2
Hence 7 is a primitive root of 1187.

(cont'd)

4. (cont'd)

$$\left(\frac{11}{1187}\right) = (-1)\left(\frac{1187}{11}\right) = (-1)\left(\frac{-1}{11}\right) = (-1)(-1) = 1$$

$(11 \equiv 1187 \equiv 3 \bmod 4)$ $(1187 \equiv -1 \bmod 11)$ $(11 \equiv 3 \bmod 4)$

Since $11^{593} \equiv 1 \bmod 1187$, 11 is NOT a primitive root of 1187.

Hence 5 and 7 are primitive roots, 3 and 11 are <u>not</u> primitive roots.

5(a) Since p is odd, we know p is not congruent to 2, 4, 6, 8 or 10 mod 12. Since $p \neq 3$, p cannot be divisible by 3, so p is not congruent to 3 or 6 or 9. Hence p is congruent to one of 1, 5, 7 or 11 mod 12.

If $p \equiv 1 \bmod 12$ then $p \equiv 1 \bmod 4$ and $p \equiv 1 \bmod 3$

so $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$.

If $p \equiv 5 \bmod 12$ then $p \equiv 1 \bmod 4$ and $p \equiv 2 \bmod 3$

so $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.

(cont'd)

5(a) (cont'd)

If $p \equiv 7 \bmod 12$ then $p \equiv 3 \bmod 4$ and $p \equiv 1 \bmod 3$

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

If $p \equiv 11 \bmod 12$ then $p \equiv 3 \bmod 4$ and $p \equiv 2 \bmod 3$

so $\left(\frac{3}{p}\right) = (-1)\left(\frac{p}{3}\right) = (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1$

So the rule would be

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 12 \text{ or } p \equiv 11 \bmod 12 \\ -1 & \text{if } p \equiv 5 \bmod 12 \text{ or } p \equiv 7 \bmod 12 \end{cases}$$

(b) from Eulers criterion; if $\left(\frac{3}{p}\right) = 1$ then $3^{\frac{p-1}{2}} \equiv 1 \bmod p$, so 3 cannot be a primitive root mod p.
Hence if 3 is a primitive root mod p then $\left(\frac{3}{p}\right) = -1$ and either $p \equiv 5 \bmod 12$ or $p \equiv 7 \bmod 12$.

(c) $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$, and using a similar technique to part (a), we see that an odd prime p ($p \neq 3$) must be congruent mod 24 to one of 1, 5, 7, 11, 13, 17, 19 and 23.

(cont'd)

5(c) (cont'd)

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$$

$p \equiv 1 \bmod 24$; $p \equiv 1 \bmod 8$ AND $p \equiv 1 \bmod 12$ so $\left(\frac{6}{p}\right) = (1)(1) = 1$

$p \equiv 5 \bmod 24$; $p \equiv 5 \bmod 8$ AND $p \equiv 5 \bmod 12$ so $\left(\frac{6}{p}\right) = (-1)(-1) = 1$

$p \equiv 7 \bmod 24$; $p \equiv 7 \bmod 8$ AND $p \equiv 7 \bmod 12$ so $\left(\frac{6}{p}\right) = (1)(-1) = -1$

$p \equiv 11 \bmod 24$; $p \equiv 3 \bmod 8$ AND $p \equiv 11 \bmod 12$ so $\left(\frac{6}{p}\right) = (-1)(1) = -1$

$p \equiv 13 \bmod 24$; $p \equiv 5 \bmod 8$ AND $p \equiv 1 \bmod 12$ so $\left(\frac{6}{p}\right) = (-1)(1) = -1$

$p \equiv 17 \bmod 24$; $p \equiv 1 \bmod 8$ AND $p \equiv 5 \bmod 12$ so $\left(\frac{6}{p}\right) = (1)(-1) = -1$

$p \equiv 19 \bmod 24$; $p \equiv 3 \bmod 8$ AND $p \equiv 7 \bmod 12$ so $\left(\frac{6}{p}\right) = (-1)(-1) = 1$

$p \equiv 23 \bmod 24$; $p \equiv 7 \bmod 8$ AND $p \equiv 11 \bmod 12$ so $\left(\frac{6}{p}\right) = (1)(1) = 1$

Hence the rule is

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 5, 19 \text{ or } 23 \bmod 24 \\ -1 & \text{if } p \equiv 7, 11, 13 \text{ or } 17 \bmod 24 \end{cases}$$

(d) If 6 is a primitive root then $p \equiv 7, 11, 13$ or $17 \bmod 24$.

5 (e) We compare our answers for (b) and (c), and find that if Both 3 and 6 are primitive roots then $p \equiv 7$ or $17 \bmod 24$.
(If $p \equiv 11 \bmod 24$ then 3 is not a primitive root, similarly with $p \equiv 13 \bmod 24$).

(f) It is not possible for 2, 3 and 6 to all be primitive roots of the same prime. If 2 and 3 were both primitive roots, then $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{3}{p}\right) = -1$. Then $\left(\frac{6}{p}\right) = 1$, and so 6 could not also be a primitive root.

(g) This is a generalization of the above; Since we know that primitive roots are quadratic nonresidues, $\left(\frac{g}{p}\right) = -1$ and $\left(\frac{h}{p}\right) = -1$, and so $\left(\frac{gh}{p}\right) = (-1)(-1) = 1$, so gh cannot be a primitive root.