Math 2500 Assignment #2 Solutions Winter 2013

Q1 (a)

$$3164 = 1003(3) + 155$$
$$1003 = 155(6) + 73$$
$$155 = 73(2) + 9$$
$$73 = 9(8) + 1$$
$$9 = 1(9) + 0$$

$$\begin{aligned}
1 &= 73 + 9(-8) \\
&= 73 + [155 + 73(-2)](-8) \\
&= 155(-8) + 73(17) \\
&= 155(-8) + [1003 + 155(-6)](17) \\
&= 1003(17) + 155(-110) \\
&= 1003(17) + [3164 + 1003(-3)](-110) \\
&= 3164(-110) + 1003(347)
\end{aligned}$$

So $3164(-110) + 1003(347) = 1$

$3164(-5720) + 1003(18044) = 52$

All solutions are $x = 18044 + 3164t$

$y = -5720 - 1003t$

Q1 (b) $3633 = 1540(2) + 553$

$1540 = 553(2) + 434$

$553 = 434(1) + 119$

$434 = 119(3) + 77$

$119 = 77(1) + 42$

$77 = 42(1) + 35$

$42 = 35(1) + 7$

$35 = 7(5) + 0$

Since $(3633, 1540) = 7$ and $7 \nmid 52$, the equation $3633x + 1540y = 52$ has no solutions.

Q1 (c) $4381 = 1352(3) + 325$

$1352 = 325(4) + 52$

$325 = 52(6) + 13$

$52 = 13(4) + 0$

$$\begin{aligned}13 &= 325 + 52(-6) \\ &= 325 + [1352 + 325(-4)](-6) \\ &= 1352(-6) + 325(25) \\ &= 1352(-6) + [4381 + 1352(-3)](25) \\ &= 4381(25) + 1352(-81)\end{aligned}$$

So $4381(25) + 1352(-81) = 13$

$4381(100) + 1352(324) = 52$

All solutions are $x = 100 + 104t$

$y = 324 + 337t$

Q2(a) $16416x \equiv 328 \mod 36012$

$$36012 = 16416(2) + 3180$$
$$16416 = 3180(5) + 516$$
$$3180 = 516(6) + 84$$
$$516 = 84(6) + 12$$
$$84 = 12(7) + 0$$

Since $(36012, 16416) = 12$ and $12 \nmid 328$, the congruence $16416x \equiv 328 \mod 36012$ has no solutions

(b) $1158x \equiv 732 \mod 3660$

$$3660 = 1158(3) + 186$$
$$1158 = 186(6) + 42$$
$$186 = 42(4) + 18$$
$$42 = 18(2) + 6$$
$$18 = 6(3) + 0$$

So $1158x \equiv 732 \mod 3660$ [cancel out 6's]

$193x \equiv 122 \mod 610$ [and note $(193, 610) = 1$]

$$610 = 193(3) + 31$$
$$193 = 31(6) + 7$$
$$31 = 7(4) + 3$$
$$7 = 3(2) + 1$$
$$3 = 1(3) + 0$$

$$\begin{aligned}
1 &= 7 + 3(-2) \\
&= 7 + [31 + 7(-4)](-2) \\
&= 31(-2) + 7(9) \\
&= 31(-2) + [193 + 31(-6)](9) \\
&= 193(9) + 31(-56) \\
&= 193(9) + [610 + 193(-3)](-56) \\
&= 610(-56) + 193(177)
\end{aligned}$$

cont'd →

Q2 (b) cont'd

Since $610(-56) + 193(177) = 1$

Then 177 is the inverse of 193 modulo 610.

From $193x \equiv 122 \mod 610$

$(177)193x \equiv (177)122 \mod 610$

$x \equiv 21594 \mod 610$

$x \equiv 244 \mod 610$

So all solutions are 244, 854, 1464, 2074, 2684, and 3294.

Q2 (c) $113x \equiv 107 \mod 248$

$248 = 113(2) + 22$

$113 = 22(5) + 3$

$22 = 3(7) + 1$

$3 = 1(3) + 0$

$1 = 22 + 3(-7)$

$= 22 + [113 + 22(-5)](-7)$

$= 113(-7) + 22(36)$

$= 113(-7) + [248 + 113(-2)](36)$

$= 248(36) + 113(-79)$

Since $248(36) + 113(-79) = 1$

The we can use -79 as the inverse of 113 mod 248

So $(-79)113x \equiv (-79)107 \mod 248$

$x \equiv -8453 \equiv 227 \mod 248$

So the solution is 227.

Q 3a

$x \equiv 2 \mod 5$

$x = 2 + 5k_1$

$x \equiv 13 \mod 22$

$2 + 5k_1 \equiv 13 \mod 22$

$5k_1 \equiv 11 \mod 22$

$22 = 5(4) + 2$

$5 = 2(2) + 1$

$2 = 1(2) + 0$

$1 = 5 + 2(-2)$

$= 5 + [22 + 5(-4)](-2)$

$= 22(-2) + 5(9)$

So $\bar{5} \equiv 9 \mod 22$

$(9)\, 5k_1 \equiv (9)\, 11 \mod 22$

$k_1 \equiv 99 \mod 22$

$k_1 \equiv 11 \mod 22$

$k_1 = 11 + 22k_2$

$x = 2 + 5(11 + 22k_2)$

$x = 57 + 110k_2$

cont'd →

Q3(a) cont'd

$$x \equiv 20 \mod 49$$
$$57 + 110 k_2 \equiv 20 \mod 49$$
$$8 + 12 k_2 \equiv 20 \mod 49$$
$$12 k_2 \equiv 12 \mod 49$$
$$k_2 \equiv 1 \mod 49$$

$\ulcorner$ $49 = 12(4) + 1$
so $(12, 49) = 1$ $\lrcorner$

$$k_2 = 1 + 49 k_3$$
$$x = 57 + 110(1 + 49 k_3)$$
$$x = 167 + 5390 k_3$$

Hence $x \equiv 167 \mod 5390$

Q3(b) $x \equiv 22 \mod 153$
$$x = 22 + 153 k_1$$

$$x \equiv 41 \mod 119$$
$$22 + 153 k_1 \equiv 41 \mod 119$$
$$34 k_1 \equiv 19 \mod 119$$

$\ulcorner$ $119 = 34(3) + 17$
$34 = 17(2) + 0$ $\lrcorner$

Since $(119, 34) = 17$ and $17 \nmid 19$, this system has no solution, and so cannot be written as a single congruence.

Q3 (c) $x \equiv 17 \mod 39$

$x = 17 + 39k_1$

$x \equiv 43 \mod 91$

$17 + 39k_1 \equiv 43 \mod 91$

$39k_1 \equiv 26 \mod 91$

$3k_1 \equiv 2 \mod 7$

$(-2)3k_1 \equiv (-2)2 \mod 7$

$k_1 \equiv -4 \mod 7$

$k_1 \equiv 3 \mod 7$

$k_1 = 3 + 7k_2$

$91 = 39(2) + 13$

$39 = 13(3) + 0$

$7 = 3(2) + 1$

$1 = 7 + 3(-2)$

$x = 17 + 39(3 + 7k_2)$

$x = 134 + 273k_2$

So as a single congruence, $x \equiv 134 \mod 273$.

Q4 $1743 \equiv 2406 \mod m$ if and only if m is positive and

$m \mid 1743 - 2406$ or

$m \mid -663$

The positive divisors of -663 are the same as 663,

$663 = 3 \cdot 13 \cdot 17$

So the possible values of m are

1, 3, 13, 17, 39, 51, 221 and 663.

Q5 (a) Since $d \mid m$, $m = ds$ for some integer s.

$a \equiv b \bmod m$, so $a = b + mk$

$$a = b + d(sk)$$

Hence $a \equiv b \bmod d$.

(b) First we consider primes greater than 3;

If P_1 is a prime then

$P_1 \not\equiv 0 \bmod 6$ since $6 \mid 6k$

$P_1 \not\equiv 2 \bmod 6$ since $2 \mid 6k+2$

$P_1 \not\equiv 3 \bmod 6$ since $3 \mid 6k+3$

$P_1 \not\equiv 4 \bmod 6$ since $2 \mid 6k+4$

For any primes greater 3, Either $P_1 \equiv 1 \bmod 6$ or $P_1 \equiv 5 \bmod 6$

If p and q are twin prime, then $q = p+2$ (or $p = q+2$, then we can simply switch their order)

Since p is prime $p \equiv 1 \bmod 6$ or $p \equiv 5 \bmod 6$

If $p \equiv 1 \bmod 6$ then $q \equiv p+2 \equiv 3 \bmod 6$ cannot be prime.

Hence $p \equiv 5 \bmod 6$ and $q \equiv p+2 \equiv 7 \equiv 1 \bmod 6$.

And so $pq \equiv (5)(1) \equiv -1 \bmod 6$.