McGill University
Math 240: Discrete Structures 1
Solutions to Assignment 4

1. (a) The following table gives the computation of the gcd of $a = 13422$ and $b = 10001$. The second and fourth columns give (after the first 2 rows) the remainder r and quotient q after applying the division algorithm to the previous two entries in column 2. The entries of the third and fourth columns are then obtained by subtracting q times the previous entry from the entry before that one.

i	r	m	n	q
-1	13422	1	0	
0	10001	0	1	
1	3421	1	-1	1
2	3159	-2	3	2
3	262	3	-4	1
4	15	-38	51	12
5	7	649	-871	17
6	1	-1336	1793	2

Since $r_i = am_i + bn_i$, we have $1 = a(-1336) + b(1793)$.

(b) Since $1 = (13422)(-1336) + (10001)(1793)$ we have $\gcd(a, b) = 1$ since any divisor of a, b must divide 1.

(c) From (b) we have $(10001)(1793) \equiv 1 \bmod 13422$ so we can take $c = 1793$. Since c is the inverse of 10001 mod 13422 it is unique mod 13422.

(d) Since $10001x \equiv 2341 \bmod 13422$ and $(10001)(1793) \equiv 1 \bmod 13422$ we have $x \equiv (2341)(1793) \equiv 9749 \bmod 13422$.

(e) Let $x = 25(13422)(-1336) + 36(10001)(1793) = 197249748$. Then $x \equiv 25 \bmod 10001$ and $x \equiv 36 \bmod 13422$ and is unique mod $(13422)(10001) = 134233422$. The smallest such x is $197249748 - 134233422 = 63233422$.

2. We have $1 = (3)(5)+(-2)(7)$ so that the solution to the first two congruences is $x = (-2)(7)(2)+(3)(5)(3) \equiv 17 \bmod 35$. Since $1 = (3)(12)+(-1)(35)$ we have $x = (17)(3)(12)+4(-1)(35) = 472 \equiv 52 \bmod 420$ as the solution of all three congruences.

3. (a) Using the Euclidean algorithm we find 43 as the inverse of 67 mod $\phi(91) = 72$. Then $b^{43} = a^{(67)(43)} = a^{1+72k} = a \cdot a^{72k} \equiv a \bmod 91$ by Euler's Theorem. which says that $a^{\phi(n)} \equiv 1 \bmod n$.

(b) By (a) $a \equiv 53^{43} \bmod 91$. Now $43 = 32+8+2+1 \implies 53^{43} = (53)(53^2)(53^8)(53^{32}) \equiv (53)(79)(79)(79) \equiv 53 \bmod 91$. So $a = 53$.

4. (a) Since $302 \equiv 2 \bmod 4$, we have $3^{302} \equiv 3^2 \equiv 4 \bmod 9$ by the Little Fermat Theorem. Similarly, $302 \equiv 2 \bmod 6 \implies 3^{302} \equiv 3^2 \equiv 2 \bmod 7$ and $302 \equiv 2 \bmod 11 \implies 3^{302} \equiv 3^2 \equiv 9 \bmod 11$.

(b) Using the Chinese Remainder Theorem, we have $3^{302} \equiv 9 \bmod 5, 7, 11 \implies 3^{302} \equiv 9 \bmod (5)(7)(11) = 385$.