Math 3502: Combinatorial Optimisation. Solutions 5.

1. $n = 77, = 7.11$, so $\phi(n) = 6 \cdot 10 = 60$. $a = 7$. $gcd(60, 7)$=1 and $2.60 - 7.17 = 1$, using extended Euclid or extended Binary gcd.

60	7	1	0	0	1
7	4	0	1	1	-8
4	3	1	-8	-1	9
3	1	-1	9	2	-17
1	0	2	-17	-7	60

so $b = -17, = 43(\text{mod } 60)$. In order to read the message Bob computes $60^{43}(\text{mod } 77)$. Now $60 = -17(\text{mod } 77)$, so $60^2 = 17^2 = 58$, $60^4 = 58^2 = -24$, $60^8 = 24^2 = 37$, $60^{16} = 37^2 = 60 = -17$, and $60^{32} = 17^2 = 58$, all (mod 77). As $58 = 32 + 8 + 2 + 1$ one has that the message is $-19.37. - 19. - 17$ (mod 77), $= 4$ (mod 77).

2. The square root of 62821427 is 7926 to the nearest integer. And $7926^2 - 7^2 = 62821427$. So $p = 7933$, $q = 7919$ and $(p - 1)(q - 1) = 62805576$. Now we must find the multiplicative inverse of 5 (mod 62805576), which we do by using the extended Euclid algorithm.

62805576	5	1	0	0	1
5	1	0	1	1	-12561115
1	0	1	-12561115	-5	62805576

So b, the inverse of 5 (mod 62805576) is $-12561115, = 50244461$.

3. We check the values of b^7 for $b \in \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Note that $14 \equiv -1(\text{mod } 15)$, $13 \equiv -2(\text{mod } 13)$, $11 \equiv -4(\text{mod } 15)$ and $8 \equiv -7(\text{mod } 15)$.

Clearly $1^7 \equiv 1$. $2^7 = 128 \equiv 8(\text{mod } 15)$. $4^7 = (2^2)^7 = (2^7)^2 \equiv 8^2(\text{mod } 15) \equiv 4(\text{mod } 15)$. and $8^7 \equiv (2^7)^3 \equiv 2(\text{mod } 15)$. So (exactly) 3/4 of the values are neither 1 or -1.

4. There is some k such that $(2/3)^k.n \leq 1$. Specifically this holds for any k which is at least as big as $\log(n)/\log(3/2)$ (just take logs and rearange).

Let $t(1) = d$. We have that $t(n) \leq t(2n/3) + c$ for some constant c. Thus (assuming that t is increasing) we have that $t(n) \leq d + (\log(n)/\log(3/2) + 1).c$.