Assignment 3- Solutions 2500 Winter 2014

1. (a) $3053 = 43 \cdot 71$

so $\phi(3053) = 42 \cdot 70 = 2940$

now $2321\,d \equiv 1 \mod 2940$

$2940 = 2321(1) + 619$

$2321 = 619(3) + 464$

$619 = 464(1) + 155$

$464 = 155(2) + 154$

$155 = 154(1) + 1$

$154 = 1(154) + 0$

So $1 = 155 + 154(-1) = 155 + [464 + 155(-2)](-1)$

$= 464(-1) + 155(3) = 464(-1) + [619 + 464(-1)](3)$

$= 619(3) + 464(-4) = 619(3) + [2321 + 619(-3)](-4)$

$= 2321(-4) + 619(15) = 2321(-4) + [2940 + 2321(-1)](15)$

$= 2940(15) + 2321(-19)$

so $d \equiv -19 \equiv 2921 \mod 2940$

So 2921 is the decrypt key.

(b) $2993 = 41 \cdot 73$

So $\phi(2993) = 40 \cdot 72 = 2880$

now $227d \equiv 1 \mod 2880$

$2880 = 227(12) + 156$

$227 = 156(1) + 71$

$156 = 71(2) + 14$

$71 = 14(5) + 1$

$14 = 1(14) + 0$

So $1 = 71 + 14(-5) = 71 + [156 + 71(-2)](-5)$

$= 156(-5) + 71(11) = 156(-5) + [227 + 156(-1)](11)$

$= 227(11) + 156(-16) = 227(11) + [2880 + 227(-12)](-16)$

$= 2880(-16) + 227(203)$

hence $d \equiv 203 \mod 2880$

So 203 is the decrypt key.

(c) $3233 = 53 \cdot 61$

so $\phi(3233) = 52 \times 60 = 3120$

now $1013\, d \equiv 1 \mod 3120$

$3120 = 1013(3) + 81$

$1013 = 81(12) + 41$

$81 = 41(1) + 40$

$41 = 40(1) + 1$

$40 = 1(40) + 0$

So $1 = 41 + 40(-1) = 41 + [81 + 41(-1)](-1)$

$= 81(-1) + 41(2) = 81(-1) + [1013 + 81(-12)](2)$

$= 1013(2) + 81(-25) = 1013(2) + [3120 + 1013(-3)](-25)$

$= 3120(-25) + 1013(77)$

So $d \equiv 77 \mod 3120$

So 77 is the decrypt key.

2 (a) $S_0 = 105 = 3 \cdot 5 \cdot 7$

$S_1 = \sigma(S_0) - S_0$

$= \sigma(3)\sigma(5)\sigma(7) - 105$

$= 4 \cdot 6 \cdot 8 - 105 \quad = 192 - 105$

$= 87 \qquad (= 3 \times 29)$

$S_2 = \sigma(S_1) - S_1$

$= \sigma(3)\sigma(29) - 87$

$= 4 \times 30 - 87 \quad = 120 - 87$

$= 33 \qquad (= 3 \times 11)$

$S_3 = \sigma(33) - 33$

$= \sigma(3)\sigma(11) - 33$

$= 4 \cdot 12 - 33 \quad = 48 - 33$

$= 15 \qquad (= 3 \times 5)$

$S_4 = \sigma(15) - 15$

$= \sigma(3)\sigma(5) - 15$

$= 4 \cdot 6 - 15 = 24 - 15$

$= 9 \qquad (= 3^2)$

$S_5 = \sigma(9) - 9$

$= \sigma(3^2) - 9$

$= 13 - 9$

$= 4 \qquad (= 2^2)$

$S_6 = \sigma(4) - 4$

$= \sigma(2^2) - 4$

$= 7 - 4$

$= 3$

$S_7 = \sigma(3) - 3$

$= 4 - 3 = 1$

So the sequence goes 105, 87, 33, 15, 9, 4, 3, 1.

2(b) $S_0 = 445 = 5 \times 89$

$S_1 = \sigma(445) - 445$

$= \sigma(5)\sigma(89) - 445$

$= 6 \cdot 90 - 445 = 540 - 445$

$= 95 \qquad (= 5 \times 19)$

$S_2 = \sigma(95) - 95$

$= \sigma(5)\sigma(19) - 95$

$= 6 \cdot 20 - 95 = 120 - 95$

$= 25 \qquad (= 5^2)$

$S_3 = \sigma(25) - 25$

$= \sigma(5^2) - 25$

$= 31 - 25 = 6$

< Since 6 is perfect, this repeats; $\sigma(6) - 6 = 6$ >

So the sequence goes 445, 95, 25, 6, 6, 6, 6, 6.

(c) $S_0 = 5020 = 2^2 \cdot 5 \cdot 251$

$S_1 = \sigma(5020) - 5020$

$= \sigma(2^2)\sigma(5)\sigma(251) - 5020$

$= 7 \cdot 6 \cdot 252 - 5020 = 10584 - 5020$

$= 5564 \qquad (= 2^2 \cdot 13 \cdot 107)$

$S_2 = \sigma(5564) - 5564$

$= \sigma(2^2)\sigma(13)\sigma(107) - 5564$

$= 7 \cdot 14 \cdot 108 - 5564 = 10584 - 5564$

$= 5020$

< so 5020 & 5564 are an amicable pair, and the sequence repeats >

So the sequence goes 5020, 5564, 5020, 5564, 5020, 5564, 5020, 5564.

3(a)

$$\begin{aligned}\sigma(12n) &= \sigma(12)\,\sigma(n) && \text{since } (n,12)=1\\ &= \sigma(2^2)\,\sigma(3)\,\sigma(n)\\ &= 7\times 4\times 3n && \text{(since } n \text{ is 3perfect)}\\ &= 7\times 12n\end{aligned}$$

Hence $12n$ would be 7 perfect.

(b) $$\begin{aligned}\sigma(14n) &= \sigma(14)\,\sigma(n) && \text{since } (n,14)=1\\ &= \sigma(2)\sigma(7)\,\sigma(n)\\ &= 3\times 8\times 7n && \text{(since } n \text{ is 7perfect)}\\ &= 12\times 14n\end{aligned}$$

Hence $14n$ would be 12 perfect.

(c) $$\begin{aligned}\sigma(pn) &= \sigma(p)\,\sigma(n) && \text{since } (n,p)=1\\ &= (p+1)\,[pn] && [\text{since } n \text{ is } p\text{-perfect}]\end{aligned}$$

Hence pn is $p+1$ perfect.

4. (For each of the following, we use the fact that ϕ is multiplicative)

a) If n is odd then $(2,n)=1$

so $\phi(2n) = \phi(2)\,\phi(n) = \phi(n)$.

b) If n is even, then we can write

$n = 2^e m$ where m is odd and $e \geq 1$.

Now $\phi(n) = \phi(2^e)\,\phi(m)$ $\quad (2,m)=1$

$= 2^{e-1}\,\phi(m)$

and $\phi(2n) = \phi(2^{e+1} m)$ $\quad$ (again $(2,m)=1$)

$= \phi(2^{e+1})\,\phi(m)$

$= 2^e \phi(m)$

$= 2(\phi(n))$

c) We do the similar thing with $3n$, considering the seperate cases of $n \equiv 0 \bmod 3$ and $n \not\equiv 0 \bmod 3$.

If n is not divisible by 3 $(n \not\equiv 0 \bmod 3)$

then $\phi(3n) = \phi(3)\,\phi(n)$

$= 2\,\phi(n)$.

If n is divisible by 3, then we write

$n = 3^e m$ where $\not\equiv 0 \bmod 3$, $e \geq 1$

[So now $(m, 3) = 1$]

So $\phi(n) = \phi(3^e)\,\phi(m)$

$= 2(3^{e-1})\,\phi(m)$

and $\phi(3n) = \phi(3^{e+1} m)$

$= \phi(3^{e+1})\,\phi(m)$

$= 2(3^e)\,\phi(m)$

$= 3(\phi(n))$

(c) The only overlap in the previous two cases was when $\phi(2n) = \phi(3n) = 2\phi(n)$

Hence we need n to be even, but not divisible by 3.

So $n \equiv 2$ or $4 \bmod 6$.