MATH342 Feedback and Solutions 6

1. The divisors of 12 are 1, 2, 3, 4, 6 and 12. We have

$$\phi(1) = 1 = \phi(2) = 1,\ \phi(3) = \phi(4) = 2, \phi(6) = 2,\ \phi(12) = 4$$

and

$$1 + 1 + 2 + 2 + 2 + 4 = 12.$$

2. By Fermat's Little Theorem, if $a \in \mathbb{Z}_+$ is coprime to 3 then $a^2 \equiv 1 \mod 3$ and hence $a^n \equiv 1 \mod 3$ whenever n is even. All of 58, 26 and 6 are even, and 5 is coprime to 3. So

$$5^{58} + 5^{26} + 5^6 \equiv 1 + 1 + 1 \equiv 0 \mod 3,$$

that is, 3 divides $5^{58} + 5^{26} + 5^6$.

3.

a) $\phi(5) = 4$ and $1 < 3 < 5$ So $|3|_5 = 2$ or 4. Since $3^2 \equiv -1 \mod 5$ we have $3^4 \equiv 1 \mod 5$ and $|3|_5 = 4$.

b) Since $9 \equiv 1 \mod 4$ we have $|9|_4 = 1$

c) $\phi(7) = 6$ and $1 < 2 < 7$. So $|2|_7 = 2$, 3 or 6. Since $2^2 = 4$ and $2^3 \equiv 1 \mod 7$ we have $|2|_7 = 3$

d) $10 \equiv -1 \mod 11$, so $|10|_{11} = 2$.

e) $|24|_{11} = |2|_{11}$. Since $\phi(11) = 10$ and $1 < 2 < 11$, we must have $|2|_{11} = 2$, 5 or 10. Since $2^2 = 4$ and $2^5 = 32 \equiv -1 \mod 11$, we have $|24|_{11} = |2|_{11} = 10$.

So only $3 \mod 5$ and $24 \mod 11 = 2 \mod 11$ are primitive

It really helps to use $24 \equiv 2 \mod 11$. Also in order to show $|2|_{11} = 10$ we only need to show that $|2|_{11}$ is not equal to 2 or 5.

4. Since $\phi(9) = 6$ and $\phi(6) = 2$, there must be two primitive roots mod 9, and if a is one of them, a^5 must be the other, because 1 and 5 are the numbers ≥ 1 and < 6 which are coprime to 6. We have $2^2 = 4$ and $2^3 \equiv -1 \mod 9$. So 2 is a primitive root and $2^5 = 32 \equiv 5 \mod 9$ is the other one.

5. Since $G_{35} \cong G_7 \times G_5$, the number of elements of G_{35} of order 12 is the same as the number of elements (x, y) of $G_7 \times G_5$ of order 12. Let n_1 be the order of x and n_2 the order of y. Then n_1 is a divisor of 6 and n_2 is a divisor of 4. The order of (x, y) is $lcm(n_1, n_2)$, which is 12 if and only if $n_2 = 4$ and $n_1 = 3$ or 6. There are $2 = \phi(4)$ elements of G_5 of order 4, and $2 = \phi(3)$ elements of G_7 of order 3, and $2 = \phi(6)$ of order 6. So there are 8 elements of $G_7 \times G_5$ of order 12 and 8 elements of G_{35} of order 12.

It was not necessary to identify elements of G_{35} of order 12, nor was it necessary to identify the elements of G_5 of order 4, or the number of elements of G_7 of order 3 or 6. All that was needed was: the number of elements of G_5 of order 4 and the number of elements of G_7 of order 3 or 6.

6. In each case the solution x must be in G_9 because if x is not coprime to 9 then x^n cannot be either, for any $n \geq 1$. Since $\phi(9) = \phi(3^2) = 6$, we have $x^6 \equiv 1$ for all $x \in G_9$ and hence

a) $x^7 \equiv 1 \mod 9 \Rightarrow x \equiv 1 \mod 9$.

b) $x^{15} \equiv 1 \mod 9 \Rightarrow x^3 \equiv 1 \mod 9$. There are $\phi(6/3) = 2$ elements of order 3 and one element of order 1 (which) divides 3 Since 2 is a primitive root we have $4^3 \equiv 1 \mod 9$ and $(-2)^3 \equiv 1 \mod 9$. So the solutions are

$$x \equiv 4 \mod 9,\quad x \equiv -2 \equiv 7 \mod 9,\quad x \equiv 1 \mod 9.$$

It really helps with the computation, in both parts, to use $x^6 \equiv 1 \mod 9$ — which follows from Euler's Theorem, of course.

7. We have $8 = 2^3 \equiv -1 \mod 9$ So $8^2 \equiv 1 \mod 9$ and $|8|_9 = 2$. So $|8|_{27} = 2$ or $3 \times 2 = 6$. But $8^2 = 64 \equiv 10 \mod 27$. So $|8|_{27} = 6$.

It is necessary to check that $|8|_{27} \neq 2$. But this is true because $8^2 = 64 \equiv 10 \mod 27$.

We have $14 \equiv -3 \mod 17$. Since $\phi(17) = 16 = 2^4$ the possible values of $|14|_{17}$ are 2^k for $1 \le k \le 4$. We have

$$(-3)^2 = 9,\ 9^2 \equiv -4 \mod 17,\ (-4)^2 \equiv -1 \mod 17,\ (-1)^2 = 1.$$

So $|14|_{17} = 16$ and $|14|_{289} = 16$ or 16×17. Now we show that $|14|_{289} \neq 16$. We have

$$14^{16} = (17-3)^{16} \equiv (-3)^{16} + 16 \times 17 \times (-3)^{15} \equiv (5 \times 17 - 4)^4 + 17 \times 3^{15} \mod 289$$

$$\equiv 256 - 20 \times 17 \times 64 + 17 \times 6 \equiv -33 + 17(-3 \times 64 + 6) \equiv 1 - 34 + 17(3 \times 4 + 6)$$

$$\equiv 1 + 17 \times 16 \equiv 273 \mod 289$$

At one stage we used $3^15 \equiv 3^{-1} \equiv 6 \mod 17$. So

$$|14|_{289} = 16 \times 17 = 272.$$

Once again, even for computing $|14|_{17}$ it helps to work with numbers as small as possible. So it is easier to compute with $-3 \mod 17$ than with $14 \mod 17$. To show that $|14|_{17} = |-3|_{17}| = 16$ we only need to show that $|-3|_{17}$ is not equal to 2, 4 or 8. The solution above shows how it is possible to do the calculation "by hand". But it was OK to use the Big Number Calculator (or any calculator, but it is a bit long-winded with the university calculator).

8.

a) First we consider divisibility by 3. Since $\phi(3) = 2$, and p is prime and not 3, by Fermat's Little Theorem, $p^2 \equiv 1 \mod 3$ and hence $p^n \equiv 1 \mod 3$ if n is even and $p^n \equiv p \mod 3$ if n is odd. Now let $p \equiv 2 \mod 3$. Then $3 \mid (p^n - 1)$ if and only if n is even. Since 3 does not divide $p-1$ and $p-1$ does divide $p^n - 1$, it is also true that $3 \mid (p^n-1)/(p-1)$ if and only if n is even. Now let $p \equiv 1 \mod 3$. Then $p^k \equiv 1 \mod 3$ for all $k \ge 0$ and

$$\frac{p^n - 1}{p - 1} = \sum_{k=0}^{n-1} p^k \equiv n \mod 3.$$

So in this case 3 divides $(p^n-1)/(p-1)$ if and only if $3 \mid n$.

b) Now we consider divisibility by 9. Note that $p \equiv -1 \mod 3$ splits into the cases $p \equiv -1 \mod 9$ or $p \equiv 2 \mod 9$ or $p \equiv 5 \mod 9$. Let $p \equiv -1 \mod 9$. Then $p^2 \equiv 1 \mod 9$ and $p^n \equiv 1 \mod 9$ if and only if n is even. Since 3 does not divide $p-1$, it follows that 9 divides $(p^n-1)/(p-1)$if and only if n is even. The case of $p \equiv 2$ or 5 mod 9 is similar. By question 4, $|2|_9 = |5|_9 = 6$ and so in these cases $p^n \equiv 1$ if and only if n is divisible by 6, and since $p-1$ is not divisible by 3, it follows that $p^n-1)/(p-1)$ is divisible by 9 if and only if n is divisible by 6.

The case $p \equiv 1 \mod 3$ splits into the cases of $p \equiv 1 \mod 9$ or $p \equiv 4 \mod 9$ or $p \equiv 7 \mod 9$ If $p \equiv 1 \mod 9$, then as in the case of $p \equiv 1 \mod 3$ in part a) we have $(p^n-1)/(p-1) \equiv n \mod 9$, and hence $(p^n-1)/(p-1)$ is divisible by 9 if and only if n is. If $p \equiv 4$ or $7 \mod 3$ then by part a), if $(p^n-1)/(p-1)$ is divisible by 3 then $3 \mid n$ and $p^3 \equiv 1 \mod 3$ and we can write $n = 3k$ for some $k \in \mathbb{Z}_+$. But then $(p^n-1)/(p^3-1) = k \mod 3$. We can check that

$$(p^3-1)/(p-1) \equiv 3 \mod 9.$$

So

$$(p^{3k}-1)/(p-1) \equiv 3k \mod 9$$

and so $(p^n-1)/(p-1)$ is divisible by 9 if and only if k is divisible by 3, that is, if and only if n is divisible by 9.

As the answer shows, this was a longer question. Most of the others were quite short – or, at least, it was possible to give short correct answers.