MATH342 Feedback and Solutions 5

1.

a) Since
$$348 = 3 \times 116 = 3 \times 2^2 \times 29,$$
we have
$$\phi(348) = 2 \times 2(2-1) \times 28 = 112.$$

b) Since
$$34606 = 2 \times 17303 = 2 \times 11 \times 1573 = 2 \times 11^2 \times 143 = 2 \times 11^3 \times 13,$$
we have
$$\phi(34606) = 1 \times 11^2 \times 10 \times 12 = 14520.$$

2. Since 7 is prime, by Fermat's Little Theorem, $n^7 \equiv n \mod 7$ for any $n \in \mathbb{Z}$. So $n^{13} = n^6 \times n^7 \equiv n^6 \times n \mod 7 \equiv n^7 \mod 7 \equiv n \mod 7$.

On this and other questions I had a number of answers that were correct, but used calculation rather than referring to Fermat's Little Theorem or Euler's Theorem.

3. If 3 does not divide n then by Fermat's Little Theorem, since 3 is prime, $n^2 \equiv 1 \mod 3$ and hence also $n^6 = (n^2)^3 \equiv 1 \mod 3$. But $1091 = 1089 + 2 \equiv 2 \mod 3$. So if 3 does not divide n we have $n^6 + 1091 \equiv 1 + 2 \equiv 0 \mod 3$, that is, 3 divides $n^6 + 1091$.

4. Both 2 and 3 are coprime to 13, and 13 is prime. So by Fermat's Little Theorem, $2^{12} = 1 \mod 13$ and $3^{12} \equiv 1 \mod 13$. So
$$2^{70} = 2^{60+10} \equiv 2^{10} = 1024 = 10 + 1014 = 10 + 13 \times 78 \equiv 10 \mod 13$$
and
$$3^{70} = 3^{60+10} \equiv 3^{10} = (3^3)^3 \times 3 \equiv 1 \times 3 \mod 13$$
So
$$2^{70} + 3^{70} \equiv 10 + 3 \mod 13 \equiv 0 \mod 13$$
that is, 13 divides $2^{70} + 3^{70}$.

I was expecting some detail in the calculation of 2^{10} and 3^{10} above. However it does help to use Fermat's Little Theorem

5. We have $1000 = 5^3 \times 2^3$ and so
$$\phi(1000) = \phi(2^3) \times \phi(5^3) = 4 \times 5^2 \times 4 = 400.$$
So since both 7 and 3 are coprime to 1000, Euler's theorem gives
$$7^{400} \equiv 1^4 \equiv 1 \mod 1000$$
and similarly for 3^{400}. So
$$7^{400} - 3^{400} \equiv 1 - 1 \equiv 0 \mod 1000.$$

Here it was expected that Euler's Theorem would be used. Otherwise it is a very heavy calculation.

6. We have $100 = 5^2 \times 2^2$. Since $\phi(5^2) = 5 \times 4 = 20$ and $\phi(4) = 2$, we have $b^{20} = 1$ for all $b \in G_{25}$ and $c^2 = 1$ for all $c \in G_4$ by Euler's Theorem, and hence, since 2^2 and 5^2 are coprime, $a^{20} = 1$ for all $a \in G_{100}$.

As the hint suggested, this comes out easily if Euler's Theorem is used $\mod 4$ *and* $\mod 25$*, rather than jusr* $\mod 100$.

7. Suppose that p is prime and $p \mid n$ where $n = 2^{17} - 1 = 131071$. Then $2^{17} \equiv 1 \mod p$. Since 17 is prime, the order of 2 must be 17. But by Fermat's Little Theorem, since 2 is coprime to p (because p must be an odd prime), we have $2^{p-1} \equiv 1 \mod p$, and hence $17 \mid p - 1$, that is, $p \equiv 1 \mod 17$. Now $\sqrt{n}$ is between 362 and 363. So if n is not prime it must be divisible by some prime $p \leq 361$ with $p \equiv 1 \mod 17$, and $p \equiv 1 \mod 2$ (since p is odd) so that $p \equiv 1 \mod 34$. So p must be one of:
$$35,\ 69,\ 103,\ 137,\ 171,\ 205,\ 239,\ 273,\ 307,\ 341.$$
Of these the only primes are
$$103,\ 137,\ 239,\ 307.$$

All the others are divisible by 3 or 5 or 11 (with $341 = 31 \times 11$). None of the primes divides $n = 2^{17} - 1$ In fact

$$n = 1272 \times 103 + 55 = 137 \times 956 + 99 = 548 \times 239 + 99 = 426 \times 307 + 289.$$

I was expecting the four primes that have to be considered to be identified, and some sort of explanation – and some explanation of why they do not divide $2^{17} - 1$*. Writing down the first one or two decimal places after dividing by them was enough.*

8. Let

$$n = \prod_{k=1}^{r} p_k^{m_k}$$

be the prime factorisation of n with $p_k < p_{k+1}$ for all k. The general formula for $\phi(n)$ is

$$\phi(n) = \prod_{k=1}^{r} p_k^{m_k - 1}(p_k - 1).$$

If $p_k \geq 5$ then $p_k - 1$ is even and $p_k - 1 = 2 \times (p_k - 1)/2$ where $(p_k - 1)/2 \geq 2$. So $p_k - 1$ has at least 2 prime factors whenever $p_k \geq 5$.

(i) Suppose that $r \geq 3$. Then for at least one k, say $k = 3$, we have $p_3 \geq 5$. There is at least one other, say $k = 2$, for which $p_2 \geq 3$. Then $p_3 - 1$ factorises as the product of at least 2 prime factors, and $p_2 - 1$ as a product of at least one (and at least two if $p_2 > 3$). So then $\phi(n)$ has at least 3 prime factors, which is a contradiction. So $r \leq 2$.

(ii) Now suppose $r = 2$. Then $(p_1 - 1)(p_2 - 1)$ still has at least 3 prime factors if $p_1 \geq 3$ and $p_2 - 1 \geq 5$. So without loss of generality $p_1 = 2$ and $p_2 \geq 3$. If $p_2 \geq 5$ and $n_2 \geq 2$ then $p_2(p_2 - 1)$ has at least 3 prime factors and divides $\phi(n)$. So $n_2 = 1$ if $p_2 \geq 5$. If $p_2 \geq 5$ then $2^{n_1 - 1}(p_2 - 1)$ divides $\phi(n)$, and so there are at least $n_1 + 1$ factors. So if $r = 2$ and $p_2 \geq 5$ we have $n_1 = n_2 = 1$. If $p_1 = 2$ and $p_2 = 3$ then $2^{n_1 - 1}3^{n_2 - 1}(3 - 1)$ has $n_1 + n_2 - 1$ prime factors, so we have $n_1 + n_2 \leq 3$ and at most one of n_1 and n_2 can be 2.

(iii) Suppose that $r = 1$. Then $p_1^{n_1 - 1}(p_1 - 1)$ has at least $n_1 + 1$ prime factors if $p_1 \geq 5$, at least n_1 prime factors if $p_1 = 3$ and at least $n_1 - 1$ if $p_1 = 2$. So we have $n_1 = 1$ if $p_1 = 5$, $n_1 \leq 2$ if $p_1 = 3$ and $n_1 \leq 3$ if $p_1 = 2$.

Hence if $\phi(n)$ has at most two factors then the possible values of $n \geq 2$ are

$$2,\ 4,\ 8,\ 3,\ 6,\ 12,\ 9,\ 18,\ p,\ 2p$$

where p is a prime ≥ 5.

This was a long question and a number of people who submitted homework left it out. But those who did tackle it did pretty well.

9. We have

$$\phi(2) = 1,\ \pi(4) = \phi(3) = \phi(6) = 2,\ \phi(8) = 4 = \phi(12),\ \phi(9) = \phi(18) = 6,\ \phi(p) = \phi(2p) = p - 1.$$

So if $\phi(n) = 6$ we have $n = 9$ or $n = 18$ or $n = p$ or $2p$ for a prime p such that $p - 1 = 6$. The unique such prime is $6 + 1 = 7$. So the n such that $\phi(n) = 6$ are

$$9,\ 18,\ 7,\ 14.$$

If n is such that $\phi(n) = 14$ then $n = p$ or $2p$ for a prime p such that $p - 1 = 14$. But $14 + 1 = 15 = 3 \times 5$ is not prime and so there is no such p and no such n.