MATH342 Feedback and Solutions 1

1. The largest prime $\leq \sqrt{113}$ is 7 because $11^2 = 121 > 113$. The largest prime $\leq \sqrt{127}$ is 11. Clearly neither 113 nor 127 is divisible by 2 or 5, nor by 3 since in each case the sum of the digits is not divisible by 3. Also $113 = 1 \bmod 7 = 127$, so neither of them is divisible by 7. Since $127 = 6 \bmod 11$, it is not divisible by 11 either. So 113 does not have a prime factor $\leq \sqrt{113}$ and 127 does not have a prime factor $\leq \sqrt{127}$. So both 113 and 127 are prime.

For the prime decompositions of numbers in the prime gap $G(113, 127)$, we have

$$114 = 2 \times 3 \times 19, \quad 115 = 5 \times 23, \quad 116 = 2^2 \times 29, \quad 117 = 3^2 \times 13, \quad 118 = 2 \times 59, \quad 119 = 7 \times 17,$$

$$120 = 2^3 \times 3 \times 5, \quad 121 = 11^2, \quad 122 = 2 \times 61, \quad 123 = 3 \times 41, \quad 124 = 2^2 \times 31, \quad 125 = 5^3, \quad 126 = 2 \times 3^2 \times 7.$$

This question was well done, though some marks were lost because I decided to require evidence of non-divisibility by 3, 5, 7 etc. I am pretty sure those who did not write full detail on this could have done so.

2. $G(2, 3) = \emptyset$. Apart from 2 every prime is odd. So if $p < q$ are consecutive primes with $p > 2$ then $q - p$ is even, that is, $G(p, q)$ has even length.

Since $k \mid n!$ for all $k \in \mathbb{N}$ with $2 \leq k \leq n$, we have $k \mid n! + k$, and hence $n! + k$ is composite for $2 \leq k \leq n$ So if p is the largest prime $< 2 + n!$ and q is the smallest prime $> n! + n$ we have $q - p \geq n! + n + 1 - n! - 1 = n$ and $G(p, q)$ has length $\geq n$.

I required some identification of the primes at either end of the gap, as given above. There is no reason why $n! + 1$ or $n! + n + 1$ should be prime, the direct length of this prime gap cannnot be determined

3. Let $p \in \mathbb{N}$. Then $p \equiv 0$ – in which case 3 divides p — or , $p \equiv 1 \mod 3$ or $p \equiv 2 \mod 3$. If $p \equiv 1 \mod 3$ then $p + 2 \equiv 0 \mod 3$ and if $p \equiv 2 \mod 3$ then $p + 4 \equiv 0 \mod 3$. So either p or $p + 2$ or $p + 4$ is divisible by 3. So if $p > 3$, at least one of p, $p + 2$ and $p + 4$ is composite, that is, not prime.

Use of algebraic notation seems to be pretty good this year. Use of modulo arithmetic seems to help most people– in this question and in others.

4. Suppose that $n = km$ for k, $m \in \mathbb{Z}_+$ both ≥ 2. then $2^k - 1 > 1$ and

$$2^n - 1 = (2^k - 1)(1 + 2^k + \cdots 2^{(m-1)k}).$$

So if n is composite, $2^n - 1$ is too. So if $2^n - 1$ is prime, n must be too. Alternatively, if $n = km$, then $2^k \equiv 1 \mod 2^k - 1$, and hence $2^n = 2^{km} \equiv 1^m \equiv 1 \mod 2^k - 1$, that is, $2^k - 1 \mid 2^n - 1$.

5. We have

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127.$$

These are all prime. The last of these was proved in question 1. However $2047 = 23 \times 89$ is composite.

6. Write $n = 3k + r$ with $k \geq 1$ and $r = 1$ or 2, since n is prime and not divisible by 3. We have $r \neq 0$ since n is prime. We have $2^3 \equiv 1 \mod 7$ and hence $2^{3k} \equiv 1 \mod 7$ for any $k \in \mathbb{Z}_+$. (THis is a special case of question 4 so we can use question 4 for this.) So $2^{3k+1} \equiv 2 \mod 7$ and $2^{3k+2} \equiv 4 \mod 7$. So $2^{3k+1} - 1 \equiv 1 \mod 7$ and $2^{3k+2} - 1 \equiv 3 \mod 7$. So $2^{3k+1} - 1$ and $2^{3k+2} - 1$ are not divisible by 7. But if p is prime and $p > 3$ then $p = 3k + 1$ or $3k + 2$ and so $2^p - 1$ is not divisible by 7.