WEEK 1 Solutions

Q1 Trivial

Q2 *Solution.* Using long division for polynomials, we find that

$$n^3 + 4n^2 + 4n - 14 = (n^2 + 2n + 2)(n + 2) + (-2n - 18).$$

In order for $n^2 + 2n + 2$ to divide $n^3 + 4n^2 + 4n - 14$, it must also divide the remainder:

$$(n^2 + 2n + 2) \mid (-2n - 18).$$

The only way that this is possible is either when $|-2n - 18| \geq |n^2 + 2n + 2|$ or when $-2n - 18 = 0$. In the first case, this inequality only holds when $-4 \leq n \leq 4$. We test all n within this range, and determine that the values of n which work are $n = -4, -2, -1, 0, 1, 4$. In the second case, we additionally find that $n = -9$

Q3 *Outline.* Note that by the Euclidean Algorithm, we have

$$\begin{aligned} \gcd(a^m - 1, a^n - 1) &= \gcd(a^m - 1 - a^{m-n}(a^n - 1), a^n - 1) \\ &= \gcd(a^{m-n} - 1, a^n - 1). \end{aligned}$$

We can continue to reduce the exponents using the Euclidean Algorithm, until we ultimately have $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$. $\square$

Q4 *Solution.* We use induction. For the base case, note that when $n = 1$, we have $a_1 = 1, b_1 = 1$, therefore, $\gcd(a_1, b_1) = 1$.

For the inductive hypothesis, we assume that it holds for $n = k$, therefore, when $a_k + b_k\sqrt{2} = \left(1 + \sqrt{2}\right)^k$, we have $\gcd(a_k, b_k) = 1$. We now show that it holds for $n = k + 1$. Note that

$$\begin{aligned} a_{k+1} + b_{k+1} &= \left(1 + \sqrt{2}\right)^{k+1} \\ &= \left(1 + \sqrt{2}\right)\left(1 + \sqrt{2}\right)^k \\ &= \left(1 + \sqrt{2}\right)\left(a_k + b_k\sqrt{2}\right) \\ &= (a_k + 2b_k) + \sqrt{2}\,(a_k + b_k). \end{aligned}$$

Therefore, $a_{k+1} = a_k + 2b_k$ and $b_{k+1} = a_k + b_k$. It is now left to show that $\gcd(a_{k+1}, b_{k+1}) = 1$. Note that by the Euclidean Algorithm,

$$\gcd(a_k + 2b_k, a_k + b_k) = \gcd(b_k, a_k + b_k) = \gcd(b_k, a_k) = 1.$$

Therefore, by induction, we have shown that $n = k \implies n = k + 1$, and we are done. $\square$

$$\frac{a^p + b^p}{a+b} = a^{p-1} - a^{p-2}b + a^{p-3}b^2 - a^{p-4}b^3 + \cdots - ab^{p-2} + b^{p-1}.$$

In order to invoke the Euclidean Algorithm, we wish to evaluate this expression mod $a+b$. Using the fact that $a \equiv -b \pmod{a+b}$ and that $p-1$ is even, we can simplify as follows:

Q5

$$\begin{aligned} a^{p-1} - a^{p-2}b + a^{p-3}b^2 - \cdots + b^{p-1} &\equiv (-b)^{p-1} - (-b)^{p-2}\,b + (-b)^{p-3}\,b^2 + \cdots \\ &\equiv (-1)^{p-1}\left(\underbrace{b^{p-1} + b^{p-1} + \cdots + b^{p-1}}_{\text{p terms}}\right) \\ &\equiv pb^{p-1} \pmod{a+b}. \end{aligned}$$

Therefore, by the Euclidean Algorithm, we arrive at

$$\gcd\left(\frac{a^p+b^p}{a+b}, a+b\right) = \gcd(pb^{p-1}, a+b).$$

Now, in the problem statement, it was given that a and b are relatively prime. Hence, similarly, $\gcd(b, a+b) = 1$, and we can simplify the above expression further:

$$\gcd(pb^{p-1}, a+b) = \gcd(p, a+b) = 1 \text{ or } p.$$

□

Q6 $a \mid bc$ but $\gcd(a,b) = 1$

Sol^n By Bezout's, $1 = ax + by$

As $a \mid bc$, $bc = ak$ $\Rightarrow$ $ybc = yak$

$\Rightarrow$ $(1-ax)c = yak$

$\Rightarrow$ $c = a(xc + yk)$

$\Rightarrow$ $a \mid c$

□

Q7

Solution. By Bezout's identity, there exist integers a and b such $\gcd(m,n) = am + bn$. Next, notice that

$$\frac{\gcd(m,n)}{n}\binom{n}{m} = \frac{am+bn}{n}\binom{n}{m} = \frac{am}{n}\binom{n}{m} + b\binom{n}{m}.$$

We must now prove that $\dfrac{am}{n}\dbinom{n}{m}$ is an integer. Note that

$$\frac{m}{n}\binom{n}{m} = \frac{m}{n}\left(\frac{n!}{m!(n-m)!}\right) = \frac{(n-1)!}{(m-1)!(n-m)!} = \binom{n-1}{m-1}.$$

Therefore,

$$\frac{\gcd(m,n)}{n}\binom{m}{n} = a\binom{m-1}{n-1} + b\binom{m}{n},$$

which is clearly an integer.

□

Q8 *Solution.* For these conditions to be met, we must have

$$\begin{aligned} a^2+b &\geq b^2-a & b^2+a &\geq a^2-b \\ (a+b)(a-b+1) &\geq 0 & (a+b)(b-a+1) &\geq 0 \\ a &\geq b-1 & b &\geq a-1. \end{aligned}$$

For these two inequalities to be satisfied, we must have $a=b, b-1, b+1$. complete solution set of $(a,b)=(2,2),(3,3),(1,2),(2,3),(2,1),(3,2)$. □

Q9 *Solution.* Since $n \mid p-1$, let $p-1=kn$ for some positive integer k, therefore $p=kn+1$. This satisfies the first condition of the requirement. We now look at the second condition, which is $p \mid n^3-1=(n-1)(n^2+n+1)$. Note that since $p=kn+1$, we have $p \geq n-1$, and because p is a prime, $\gcd(p,n-1)=1$:

$$p \mid (n-1)(n^2+n+1) \implies p=kn+1 \mid n^2+n+1.$$

In order for this to be true, $kn+1 \leq n^2+n+1 \implies k \leq n+1$. Since $n^2+n+1 \mid k(n^2+n+1)$, we also have

$$\begin{aligned} p=kn+1 &\mid kn^2+kn+k \\ \implies kn+1 &\mid kn^2+kn+k-n(kn+1)=kn+k-n. \end{aligned}$$

Similarly, to have this divisibility, $kn+k-n \geq kn+1 \implies k \geq n+1$. However, above we found that $k \leq n+1$, therefore, $k=n+1$. Substituting this in for p gives $p=(n+1)n+1=n^2+n+1$, giving

$$4p-3=4n^2+4n+4-3=4n^2+4n+1=(2n+1)^2.$$

□

Q10

$gcd(n+m, mn+1) = gcd(n+m, mn+1-m(n+m)) = gcd(n+m, 1-m^2) = gcd(n+m, m^2-1)$. Clearly this is periodic in n with a period of m^2-1, but we must show that this is the fundamental period. $gcd(n+m, m^2-1) = m^2-1$ when $m^2-1 | n+m$, meaning that this value cannot occur more frequently than every m^2-1 values of n, proving that the period is fundamental.