Quiz 2

Allen Williams

January 31st, 2018

Problem 1. *i) Find the gcd of 203 and 91 using the Euclidean Algorithm.*

$$\begin{aligned}203 &= 91 \cdot 2 + 21\\ 91 &= 21 \cdot 4 + 7\\ 21 &= 7 \cdot 3 + 0\end{aligned}$$

So by the Euclidean Algorithm, gcd(203, 91)=7. Working backwards 7 can be written as a linear combination of 203 and 91.

$$\begin{aligned}7 &= 91 - 21 \cdot 4\\ 7 &= 91 - 4 * (203 - 2 \cdot 91) = 9 \cdot 91 + (-4) \cdot 23\end{aligned}$$

So gcd(203, 91) = 7 = $9 \cdot 91 + (-4) \cdot 23$
ii) Find the gcd of 21 and 8 using the Euclidean Algorithm.

$$\begin{aligned}21 &= 8 \cdot 2 + 5\\ 8 &= 5 \cdot 1 + 3\\ 5 &= 3 \cdot 1 + 2\\ 3 &= 2 \cdot 1 + 1\\ 2 &= 1 \cdot 2 + 0\end{aligned}$$

So by the Euclidean Algorithm, gcd(21, 8)=1. Working backwards 1 can be written as a linear combination of 21 and 8.

$$\begin{aligned}1 &= 3 - 2\\ 1 &= 3 - (5 - 3) = 3 \cdot 2 - 5\\ 1 &= 2(8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5\\ 1 &= 2 \cdot 8 - 3(21 - 2 \cdot 8) = 8 \cdot 8 - 3 \cdot 21\end{aligned}$$

So gcd(21, 8) = 1 $= 8 \cdot 8 - 3 \cdot 21$

Problem 2. *Prove that for* $n \geq 1$, $2 + 2^2 + ... + 2^n = 2^{n+1} - 2$
The proof is by induction. Let $P(n)$ *denote the statement "*$2{+}2^2{+}...{+}2^n = 2^{n+1}{-}2$*".*
Clearly $2^1 = 2(2-1) = 2^2 - 2^1 = 2^{1+1} - 2$ *so* $P(1)$ *is true establishing the basis of induction. Assume* $P(k)$ *is true for some* $k \in \mathbb{N}$*, that is*

$$\begin{aligned}
2 + 2^2 + ... + 2^k &= 2^{k+1} - 2 \text{ so,} \\
2 + 2^2 + ... + 2^k + 2^{k+1} &= 2^{k+1} - 2 + 2^{k+1} \\
&= 2 \cdot 2^{k+1} - 2 \\
&= 2^{(k+1)+1} - 2
\end{aligned}$$

So $P(k+1)$ *is true and by the first principle of mathematical induction* $P(n)$ *is true for all* $n \in \mathbb{N}$*.*

Problem 3. *Prove that for all* $n \geq 1$, $8^n - 3^n$ *is divisible by 5.*
The proof is by induction. Let $P(n)$ *denote the statement "*$8^n - 3^n$ *is divisible by 5."* $8^1 - 3^1 = 5 = 5 \cdot 1$ *so* $P(1)$ *is true, establishing the basis of induction. Assume* $P(k)$ *is true for some* $k \in \mathbb{N}$*, that is*

$$\begin{aligned}
8^k - 3^k &= 5 \cdot j \text{ for some } j \in \mathbb{Z} \text{ so,} \\
8(8^k - 3^k) &= 8 \cdot 5j \\
8 \cdot 8^k - 8 \cdot 3^k &= 8 \cdot 5j \\
(8 \cdot 8^k - 3 \cdot 3^k) - 5 \cdot 3^k &= 5 \cdot 8j \\
8^{k+1} - 3^{k+1} &= 5 \cdot 8j + 5 \cdot 3^k \\
8^{k+1} - 3^{k+1} &= 5(8j + 3^k)
\end{aligned}$$

Since $8j$ *and* $3^k \in \mathbb{Z}$, $8^{k+1} - 3^{k+1}$ *is divisible by 5 so by the first principle of mathematical induction,* $P(n)$ *is true for all* $n \in \mathbb{N}$*.*

Problem 4. *Prove that* $\frac{1}{2}+\frac{1}{6}+...+\frac{1}{n(n+1)}=\frac{n}{n+1}$ *for all* $n \in \mathbb{N}$.
The proof is by induction. Let $P(n)$ *denote the statement* "$\frac{1}{2}+\frac{1}{6}+...+\frac{1}{n(n+1)}=\frac{n}{n+1}$"*.* $\frac{1}{1(1+1)}=\frac{1}{2}=\frac{1}{1+1}$ *so* $P(1)$ *is true, establishing the basis of induction. Assume* $P(k)$ *is true for some* $k \in \mathbb{N}$ *that is,*

$$\frac{1}{2}+\frac{1}{6}+...+\frac{1}{n(n+1)}=\frac{n}{n+1} \text{ then,}$$

$$\begin{aligned}
\frac{1}{2}+\frac{1}{6}+...+\frac{1}{n(n+1)}+\frac{1}{(n+1)((n+1)+1)} &= \frac{n}{n+1}+\frac{1}{(n+1)((n+1)+1)} \\
&= \frac{n}{n+1}+\frac{1}{(n+1)(n+2)} \\
&= \frac{n(n+2)+1}{(n+2)(n+1)} \\
&= \frac{n^2+2n+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} \\
&= \frac{n+1}{(n+1)+1}
\end{aligned}$$

So $P(k+1)$ *is true and by the first principle of mathematical induction,* $P(n)$ *is true for all* $n \in \mathbb{N}$.

Problem 5. *Demonstrate that* $\sqrt{7}$ *cannot be a rational number.*
Assume for contradiction that $\sqrt{7}$ *is rational, that is* $\sqrt{7}=\frac{p}{q}$ *for* $p,q \in \mathbb{Z}$ *with* $q \neq 0$ *and* $gcd(p,q)=1$. *Then* $7=\frac{p^2}{q^2}$ *so* $7q^2=p^2$ *so* $7 \mid p^2$ *and since 7 is a prime number* $7 \mid p$, *that is* $p=7j$ *for some* $j \in \mathbb{Z}$. *Then* $7q^2=(7j)^2$ *so* $7q^2=49j^2$ *so* $q^2=7j^2$ *meaning* $7 \mid q^2$ *and again since 7 is a prime number,* $7 \mid q$. *Then 7 is a common divisor of* p *and* q *which contradicts the assumption that* $1=gcd(p,q)$, *so* $\sqrt{7}$ *cannot be a rational number.*

Problem 6. *Let* $a,b,c \in \mathbb{Z}$. *Prove that if* $gcd(a,b)=1$ *and* $a \mid bc$, *then* $a \mid c$.
Let $a,b,c \in \mathbb{Z}$ *suppose that* $gcd(a,b)=1$ *and* $a \mid b \cdot c$. *Then* $bc=ak$ *for some* $k \in \mathbb{Z}$. *Also by Bezout's identity there exist* $r,s \in \mathbb{Z}$ *such that* $ar+bs=1$. *Then* $car+(bc)s=c$, *so* $car+aks=c$, *so* $a(cr+ks)=c$. *Since c,r,k and s are integers,* $a \mid c$.

Problem 7. *Deleted 1/29/2018*