Alexander Brodbelt s2157837. January 29, 2024

Problem 1. *Given $n > 1$, write the polynomial $x^n - 1$ as a product of two polynomials each of degree less than n*

Solution.
$$x^n - 1 = (x-1)(1 + x^2 + \ldots + x^{n-1}) \quad (1)$$

□

Problem 2. *Deduce that if for integer $d > 1$ the number $d^n - 1$ then $d = 2$ (where $n > 1$)*

Solution. From problem (1) we know we can rewrite $d^n - 1$ as:

$$d^n - 1 = (d-1)(1 + d + d^2 + \ldots + d^{n-1}) \quad (2)$$

For $d^n - 1$ to be prime, we require either $d - 1 = 1$ or $1 + d + d^2 + \ldots + x^{n-1} = 1$. However, $2 < 1 + d < 1 + d + d^2 + \ldots + x^{n-1} \neq 1$. It follows then that $d - 1 = 1$, therefore $d = 2$ □

Problem 3. *Show that if n is composite, say $n = ab$ with $a > 1$ and $b > 1$, then $2^n - 1$ is composite.*

Solution. Given $n = ab$ for $a > 1$ and $b > 1$ we can rewrite $2^n - 1$ to be

$$\begin{aligned} 2^n - 1 = 2^{ab} - 1 \\ &= (2^a)^b - 1 \\ &= (2^a - 1)(1 + 2^a + 2^{2a} + \ldots + 2^{(b-1)a}) \end{aligned}$$

Both factors of $2^n - 1$

1. $2^a - 1 > 2 - 1 = 1$ as $a > 1$
2. $1 + 2^a + 2^{2a} + \ldots + 2^{(b-1)a} > 1$

Therefore $2^n - 1$ must be composite. □

Problem 4. *Deduce that if $2^n - 1$ is prime then n is prime*

Solution. We prove the statement by proving the contrapositive:
Suppose n is not prime, then n is composite. By problem (3) we can then conclude that $2^n - 1$ is composite, or in other words, not prime; and so we are done. □

Problem 5. *Given odd $n > 1$, write the polynomial $x^n + 1$ as a product of two polynomials each of degree less than n.*

Solution. If n is odd then $\exists k \in \mathbb{N}$ such that $n = 2k + 1$. As $x = -1$ is a root of the polynomial $x^{2k+1} + 1 = 0$. By the fundamental theorem of algebra, we can factorize $x^{2k+1} + 1$ as

$$x^{2k+1} + 1 = (x+1)(1 - x + x^2 - \ldots + \ldots - x^{n-2} + x^{n-1}) = (x+1)(\sum_{k=0}^{n-1} (-1)^k x^k) \quad (3)$$

□

Problem 6. *Show that if $2^n + 1$ is prime then n cannot be odd unless $n = 1$*

Solution. Clearly, if $n = 1$ then $2^n + 1 = 3$ which is prime. We prove the rest of the claim by contradiction:
If n is odd and $n \neq 1$ then we have $n = 2m - 1$ with $2 \leq m$. Thus rewriting $2^n + 1$.

$$\begin{aligned}
2^n + 1 &= 2^{2m-1} + 1 \\
&= (2+1)\left(\sum_{k=0}^{n-1}(-1)^k 2^k\right) \\
&= 3\left(\sum_{k=0}^{2m-2}(-1)^k 2^k\right) \\
&\text{Breaking up the sum into the positive terms and the negative terms} \\
&= 3\left(\sum_{k=0}^{m-1} 2^{2k+2} - \sum_{k=0}^{m-1} 2^{2k+1}\right) \\
&= 3\left(4\sum_{k=0}^{m-1} 2^{2k} - 2\sum_{k=0}^{m-1} 2^{2k}\right) \\
&= 3 \cdot 2\left(\sum_{k=0}^{m-1} 2^{2k}\right)
\end{aligned}$$

Which shows $6 \mid 2^n + 1$ and so it is composite, or in other words, not prime; a contradiction. Therefore if $2^n + 1$ is prime then n cannot be odd unless $n = 1$. $\square$

Problem 7. *Show that if $2^n + 1$ is prime then n cannot be divisible by an odd number $q > 1$.*

Solution. We show this by contradiction:
Suppose $q \mid n$ with $q > 1$ being an odd number. Then $n = qm$ for some $1 \leq m$.

- If $m = 1$ then by problem (6) we have shown $2^n + 1$ is composite, as it is divisible by 6.
- Otherwise, if $m > 1$ then we can write $2^n + 1$ in the following way, having $q = 2m - 1$

$$\begin{aligned}
2^n + 1 &= 2^{qm} + 1 \\
&= (2^m)^q + 1 \\
&= (2^m + 1)\left(\sum_{k=0}^{q-1}(-1)^k (2^m)^k\right) \\
&= (2^m + 1)\left(\sum_{k=0}^{2m-2}(-1)^k (2^m)^k\right) \\
&\text{Breaking up the sum into the positive terms and the negative terms} \\
&= (2^m + 1)\left(\sum_{k=0}^{m-1}(2^m)^{2k+2} - \sum_{k=0}^{m-1}(2^m)^{2k+1}\right) \\
&= (2^m + 1)\left(4\sum_{k=0}^{m-1}(2^m)^{2k} - 2\sum_{k=0}^{m-1}(2^m)^{2k}\right) \\
&= (2^m + 1) \cdot 2\left(\sum_{k=0}^{m-1}(2^m)^{2k}\right)
\end{aligned}$$

Which shows $2 \cdot (2^m + 1) \mid 2^n + 1$, showing $2^n + 1$ is not prime and thus a contradiction. Therefore, if $2^n + 1$ is prime then n cannot be divisible by an odd number $q > 1$.

$\square$

Problem 8. *Conclude that if $2^n + 1$ for some m.*

Solution. By problem (7) if $2^n + 1$ is prime then n is not divisible by an odd number $q > 1$, and thus n must be of the form $n = 2^m$ for some $m \in \mathbb{N}$. $\square$