QUESTION

Are the following true or false? Provide either a proof, or a counterexample, as appropriate.

(i) If $\gcd(a, p^2) = p$, then $\gcd(a^2, p^2) = p^2$.

(ii) If $\gcd(a, p^2) = p$ and $\gcd(b, p^2) = p^2$, then $\gcd(ab, p^4) = p^3$.

(iii) If $\gcd(a, p^2) = p$ and $\gcd(b, p^2) = p$ then $\gcd(ab, p^4) = p^2$.

(iv) If $\gcd(a, p^2) = p$ then $\gcd(a + p, p^2) = p$.

ANSWER

(i) TRUE: $\gcd(a, p^2) = p \Rightarrow p^2|a^2$, so $\gcd(a^2, p^2) = p^2$.

(ii) FALSE: $gcd(a, p^2) = p$ shows that $p|a$ but $p \not| a$ so we know the axact power of p that divides a. But $\gcd(b, p^c) = p^2$ only shows that $p^2|b$. It is quite possible that b is divisible by a higher power of p (e.g. $\gcd(p^3, p^2) = p^2$) and it is by exploring this possibility that we find a counterexample, e.g. $a = 2,\ b = 8,\ p = 2$ gives $\gcd(a, p^2)$=$\gcd(2, 4) = 2 = p$ and $\gcd(b, p^2)$=gcd$8, 4) = 4 = p^2$, but $\gcd(ab, p^4)$=$\gcd(16, 16) = 16 = p^4 \neq p^3$.

(iii) TRUE: As explaind in part (ii), we have $p|a$, but $p^2 \not| a$, so $a = pm$, where $p \not| m$. Similarly, $b = np$, where $p \not| n$. We now have $ab = p^2mn$, and lemma 2.2 tells us that if $p|mn$ then $p|m$ or $p|n$. Since we know that p divided neither m or n, we may conclude that $p \not| mn$, so the highest power of p dividing ab is p^2. As the only divisors of p^4 are powers of p, we may conclude that $\gcd(ab, p^4) = p^2$.

(iv) FALSE: The trick here is to take $a = p^2 - p$, so that $a + p$ is divisible by p^2. So to get a numerical counterexample, we may choose, e.g.$p = 3,\ a = 6$ and get $\gcd(a, p^2)$=$\gcd(6, 9) = 3 = p$, but $\gcd(a + p, p^2)$=gcd(9,9)=9.