
Math 307
Solutions to the proofs in HW4, question #4

(a) $(\forall a, b, k \in \mathbb{Z})[[k \geq 1 \wedge a|b] \Rightarrow a^k|b^k]$.

Proof:

- (1) Let $a, b, k \in \mathbb{Z}$.
- (2) Assume $k \geq 1$ and $a|b$.
- (3) Since $a|b$, there exists an $r \in \mathbb{Z}$ such that $b = a \cdot r$.
- (4) Then $b^k = (ar)^k = a^k \cdot r^k$.
- (5) So there exists an $s \in \mathbb{Z}$ such that $b^k = a^k \cdot s$.
- (6) Hence, $a^k|b^k$.
- (7) So $(\forall a, b, k \in \mathbb{Z})[[k \geq 1 \wedge a|b] \Rightarrow a^k|b^k]$.

(b) $(\forall a, b, c \in \mathbb{Z})[(a|b \wedge b|c) \Rightarrow a|c]$.

Proof:

- (1) Let $a, b, c \in \mathbb{Z}$.
- (2) Assume $a|b$ and $b|c$.
- (3) Since $a|b$, there exists an $r \in \mathbb{Z}$ such that $b = a \cdot r$.
- (4) Since $b|c$, there exists an $s \in \mathbb{Z}$ such that $c = b \cdot s$.
- (5) Then $c = b \cdot s = (a \cdot r) \cdot s = a \cdot (rs)$.
- (6) So there exists a $t \in \mathbb{Z}$ such that $c = a \cdot t$.
- (7) Hence, $a|c$.
- (8) So $(\forall a, b, c \in \mathbb{Z})[(a|b \wedge b|c) \Rightarrow a|c]$.

(c) $(\forall x \in \mathbb{Z})[3|x^2 \Rightarrow 3|x]$.

Proof:

- (1) Suppose $x \in \mathbb{Z}$.
- (2) Assume $3|x^2$.
- (3) Assume 3 does not divide x .
- (4) Since 3 does not divide x , then when we divide x by 3 we get a remainder of either 1 or 2.
- (5) In other words, there exist $n, e \in \mathbb{Z}$ such that $x = 3n + e$ and e is either 1 or 2.
- (6) Now compute that $x^2 = (3n + e)^2 = 9n^2 + 6ne + e^2 = 3(3n^2 + 2ne) + e^2$.
- (7) So 3 divides $x^2 - e^2$, which means $x^2 \equiv_3 e^2$.
- (8) Since $3|x^2$, this means $x^2 \equiv_3 0$; so $e^2 \equiv_3 0$ as well.
- (9) But e is either 1 or 2, and in neither case is it true that $e^2 \equiv_3 0$. So this is a contradiction.
- (10) Hence $3|x$.
- (11) So we have proven that $(\forall x \in \mathbb{Z})[3|x^2 \Rightarrow 3|x]$.

(d) $(\forall x \in \mathbb{Z})[2|x \Rightarrow [x^4 \equiv_{32} 0 \vee x^4 \equiv_{32} 16]]$

Proof:

- (1) Let $x \in \mathbb{Z}$.
- (2) Suppose $2|x$.
- (3) Assume that $x^4 \not\equiv_{32} 0$.
- (4) Since $2|x$, there is a $k \in \mathbb{Z}$ such that $x = 2k$.
- (5) Then $x^4 = (2k)^4 = 16 \cdot k^4$.
- (6) If k^4 is even, then there exists $n \in \mathbb{Z}$ such that $k^4 = 2n$. Then $x^4 = 16 \cdot k^4 = 32 \cdot n$, and so $x^4 \equiv_{32} 0$; this contradicts our assumption in (3).
- (7) Therefore k^4 is odd. This means $k^4 = 2n + 1$ for some integer n .
- (8) Hence, $x^4 = 16 \cdot k^4 = 16 \cdot (2n + 1) = 32n + 16$.
- (9) So $32|x^4 - 16$, hence $x^4 \equiv_{32} 16$.
- (10) We have proven $x^4 \not\equiv_{32} 0 \Rightarrow x^4 \equiv_{32} 16$.
- (11) The above is equivalent to $x^4 \equiv_{32} 0 \vee x^4 \equiv_{32} 16$.
- (12) So $(\forall x \in \mathbb{Z})[2|x \Rightarrow [x^4 \equiv_{32} 0 \vee x^4 \equiv_{32} 16]]$.