Math 310/3~~8~~01DH H.W #2 Solutions

7. Show that for $a,b,k \in \mathbb{Z}$ and $k \geq 0$, $a+b \mid a^{2k+1}+b^{2k+1}$.

(1) $k=0$; $a^{2k+1}+b^{2k+1} = a+b = (a+b)(1)$ so true for $k=0$. ✓

(2) Suppose $a^{2k+1}+b^{2k+1} = (a+b)M$; then

$$a^{2(k+1)+1}+b^{2(k+1)+1} = a^{2k+3}+b^{2k+3} = a^2a^{2k+1}+b^2b^{2k+1}$$
$$= a^2(a^{2k+1}+b^{2k+1}) - a^2b^{2k+1}+b^2b^{2k+1}$$
$$= a^2(a+b)M + (b^2-a^2)b^{2k+1} = (a+b)a^2M + (a+b)(b-a)b^{2k+1}$$
$$= (a+b)(a^2M+(b-a)b^{2k+1}) = (a+b)N.$$

So if $a+b \mid a^{2k+1}+b^{2k+1}$, then $a+b \mid a^{2(k+1)+1}+b^{2(k+1)+1}$

So by P.M.I, $a+b \mid a^{2k+1}+b^{2k+1}$ for all $k \geq 0$.

So if $a \geq 2$ and k is odd ($k=2l+1$) $a+1 \mid a^{2l+1}+1^{2l+1} = a^k+1$

Since $1 < a+1 < a^k+1$ ($a < a^k$ for $k \geq 2$ by induction!),

$a+1$ is a proper factor, so a^k+1 can't be prime. ///

8. If $n \geq 1$ and 2^n+1 is prime, then n is a power of 2.

If p is a prime factor of n and $p \neq 2$, then p is odd,

so $n = pq$ with q odd. But then

$$2^n+1 = 2^{pq}+1 = (2^q)^p+1 = a^p+1 \text{ with } a = 2^q \geq 2 \text{ and}$$

$p \geq 3$ odd. So by problem 7, $2^n+1 = a^p+1$ is not prime.

So if 2^n+1 is prime, every prime factor of n is 2,

so n is a power of 2. ///

9. Show that for any 3 consecutive integers $n, n+1, n+2$, exactly one is a multiple of 3.

By the division algorithm, n is exactly one of $3q$, $3q+1$, or $3q+2$. Then

If $n=3q$, then $n+1=3q+1$, $n+2=3q+2$, so only n is a mult of 3.

If $n=3q+1$, then $n+1=3q+2$, $n+2=3(q+1)$, so only $n+2$ is a mult of 3.

If $n=3q+2$, then $n+1=3(q+1)$, $n+2=3(q+1)+1$, so only $n+1$ is a mult of 3.

10. Show that if $a|c$ and $b|d$ then $ab|cd$.

$a|c$ means $c=ar$ for $r\in\mathbb{Z}$. $b|d$ means $d=bs$ for $s\in\mathbb{Z}$.

Then $cd=(ar)(bs)=(ab)(rs)$ with $rs\in\mathbb{Z}$, so $ab|cd$.

11. Show that if $a|b$ and $a|c$, then $a|rb+sc$ for $r,s\in\mathbb{Z}$

$a|b$ means $b=ax$; $a|c$ means $c=ay$; but then

$rb+sc=r(ax)+s(ay)=a(rx+sy)$ with $rx+sy\in\mathbb{Z}$.

So $a|rb+sc$.

12. Show that if $a|c$ and $b|c$, ~~then~~ and $(a,b)=1$, then $ab|c$

$a|c$ means $c=ax$; $b|c$ means $c=by$

$(a,b)=1$ implies $1=ar+bs$ for some $r,s\in\mathbb{Z}$. But

then $c=c\cdot 1=c(ar+bs)=car+cbs=(by)ar+(ax)bs$
$=(ab)(yr)+(ab)(xs)=ab(yr+xs)$ with

$yr+xs \in \mathbb{Z}$; So $ab \mid c$. ∎

H1: Show that if $a \mid (b+c)$ and $(b,c)=d$, then $(a,b) \leq d$ and $(a,c) \leq d$.

$(b,c)=d$ implies that $d = br + cs$ for some $r,s \in \mathbb{Z}$

$a \mid b+c$ means $b+c = ax$ for some $x \in \mathbb{Z}$. Then

$c = ax - b$, so $d = br + (ax-b)s = b(r-s) + a(xs)$

So $d = br' + as'$ for some $r', s' \in \mathbb{Z}$, so $(b,a) = (a,b) \mid d$

In particular, $(a,b) \leq d$.

Similarly, $b = ax - c$, so $d = (ax-c)r + cs = a(xr) + c(s-r)$

So $d = ar'' + cs''$ for some $r'', s'' \in \mathbb{Z}$, so $(a,c) \mid d$. In particular, $(a,c) \leq d$. ∎