Math 310 Homework 3 Solutions

13. $(1111, 473)$:

$$1111 = 473 \cdot 2 + 165 \quad (1111 - 946 = 165)$$
$$473 = 165 \cdot 2 + 143 \quad (473 - 330 = 143)$$
$$165 = 143 \cdot 1 + 22$$
$$143 = 22 \cdot 6 + 11$$
$$22 = 11 \cdot 2 + 0$$

So $(1111, 473) = 11$

$$11 = 143 - 22 \cdot 6 = 143 - (165 - 143 \cdot 1) \cdot 6 = 143 \cdot 7 - 165 \cdot 6$$
$$= (473 - 165 \cdot 2) \cdot 7 - 165 \cdot 6 = 473 \cdot 7 - 165 \cdot 20$$
$$= 473 \cdot 7 - (1111 - 473 \cdot 2) \cdot 20 = 473 \cdot 47 - 1111 \cdot 20$$

So $11 = 473 \cdot 47 - 1111 \cdot 20 = 473 \cdot (47) + 1111 \cdot (-20)$

14. $(1357, 2468)$:

$$2468 = 1357 \cdot 1 + 1111$$
$$1357 = 1111 \cdot 1 + 246$$
$$1111 = 246 \cdot 4 + 127 \quad (1111 - 984 = 127)$$
$$246 = 127 \cdot 1 + 119$$
$$127 = 119 \cdot 1 + 8$$
$$119 = 8 \cdot 14 + 7$$
$$8 = 7 \cdot 1 + 1$$
$$7 = 1 \cdot 7 + 0$$

So $(1357, 2468) = 1$

$$1 = 8 - 7 \cdot 1 = 8 - (119 - 8 \cdot 14) \cdot 1 = 8 \cdot 15 - 119 \cdot 1$$
$$= (127 - 119 \cdot 1) \cdot 15 - 119 \cdot 1 = 127 \cdot 15 - 119 \cdot 16$$
$$= 127 \cdot 15 - (246 - 127 \cdot 1) \cdot 16 = 127 \cdot 31 - 246 \cdot 16$$
$$= (1111 - 246 \cdot 4) \cdot 31 - 246 \cdot 16 = 1111 \cdot 31 - 246 \cdot 140$$
$$= 1111 \cdot 31 - (1357 - 1111 \cdot 1) \cdot 140 = 1111 \cdot 171 - 1357 \cdot 140$$
$$= (2468 - 1357 \cdot 1) \cdot 171 - 1357 \cdot 140$$
$$= 2468 \cdot 171 - 1357 \cdot 311$$

So $1 = 2468 \cdot 171 - 1357 \cdot 311 = 2468 \cdot (171) + 1357 \cdot (-311)$

15 If p is prime and $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.

By induction (on n!):

(1) $n=1$ $p \mid a_1$, so $p \mid a_1$! ✓

(2) Assume true for $n-1$, i.e. if $p \mid a_1 \cdots a_{n-1}$ then $p \mid a_i$ for some i. Then since

$a_1 \cdots a_n = (a_1 \cdots a_{n-1}) \cdot a_n$ we have

$p \mid (a_1 \cdots a_{n-1}) \cdot a_n$, so from a result from class, since p is prime, either

$p \mid a_1 \cdots a_{n-1}$ or $p \mid a_n$. But by the inductive hypothesis, we then have either

$p \mid a_i$ for some i $1 \le i \le n-1$, or $p \mid a_n$.

So $p \mid a_i$ for some i, $1 \le i \le n$. //

So by induction, if $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.

16. If $a \in \mathbb{Z}$, $n \ge 1$, p prime and $p \mid a^n$ then $p^n \mid a^n$.

By problem #15, since $p \mid a^n = a \cdot a \cdots a = a_1 \cdots a_n$ we have $p \mid a_i = a$ for some i. So $p \mid a^n$ implies $p \mid a$. So $a = pX$ for some integer X, so

$a^n = (pX)^n = p^n X^n$, so $p^n \mid a^n$. //

17. If n is not prime, then $n = pq$ where p is prime and $p \le \sqrt{n}$.

Since p isn't prime, $p = ab$ with $a > 1$ and $b > 1$.

From class, we know that $n = pX$ for some prime p.

If $p > \sqrt{n}$ and $X > \sqrt{n}$, then $n = p \cdot X > \sqrt{n} \cdot \sqrt{n} = n$, which is impossible. So we must have either

$p \leq \sqrt{n}$ or $X \leq \sqrt{n}$. If $p \leq \sqrt{n}$, stop; p is the prime we want. If $X \leq \sqrt{n}$, then X might be prime; if it is use X instead. But in any event, we know (by the same result from class) that $X = p'Y$ for some prime p'. But then $p' \leq X \leq \sqrt{n}$, so $p' \leq \sqrt{n}$, and $n = pX = p(p'Y) = p'(pY) = p'Z$ with p' prime and $p' \leq \sqrt{n}$.

So in either case, we find some prime p (or p') with $p \mid n$ and $p \leq \sqrt{n}$.

So to check if $n = 239$ is prime: if it is not prime, then it has a prime factor $\leq \sqrt{239} < \sqrt{256} = 16$. So one of 2, 3, 5, 7, 11, or 13 would have to be a factor. But:

$239 = 2 \cdot 119 + 1$ so $2 \nmid 239$
$239 = 3 \cdot 79 + 2$ so $3 \nmid 239$
$239 = 5 \cdot 47 + 4$ so $5 \nmid 239$
$239 = 7 \cdot 34 + 1$ so $7 \nmid 239$
$239 = 11 \cdot 21 + 8$ so $11 \nmid 239$
$239 = 13 \cdot 18 + 5$ so $13 \nmid 239$

So none of the primes, one of which would have to divide it, do; so 239 is prime.

H.2: a, b integers ≥ 1, $(a,b)=1$ and $ab=c^r$, then $a=x^r$ and $b=y^r$ for some x, y.

Proof: By complete induction on c: $ab \geq 1$ so $c \geq 1$.

(1) $c=1$ $ab=1^r=1$, then $a|1$ and $b|1$ so $a=1=1^r$ and $b=1=1^r$; so set $x=y=1$.

(2) Suppose the result is true if $ab=d^r$ for any $d<c$.

Then since we can write $c=pX$ with p prime, we have $ab=c^r=(pX)^r=p^rX^r$, so $p^r|ab$. But! Then $p|a$ or $p|b$. We can't have $p|a$ and $p|b$, since then $1=(a,b) \geq p$. So WLOG $p|a$ and $p \nmid b$, so $(p,b)=1$. But then $(p^r,b)=1$ [Induction? Or: $1=p\alpha+b\beta$ so $1=1^r=(p\alpha+b\beta)^r=p^r\alpha^r+b(\text{lots of junk})$.] So then $p^r|ab$ and $(p^r,b)=1$, so $p^r|a$. Then writing $a=p^rY$, we have $(p^rY)b=p^rX^r=p^r(Yb)$ so $Yb=X^r$ with $X<c$. So the inductive hypothesis implies that $Y=x^r$ and $b=y^r$ for some x and y, so $a=p^rY=p^rx^r=(px)^r$ and $b=y^r$, as desired. ∎

So by complete induction, the result is true. ∎