MATH 135 Alexander Maguire
Assignment 4 20396195

1) RTS $m^2 \nmid n^2 \Rightarrow m \nmid n$ STS $m|n \Rightarrow m^2|n^2$ by contrapositive.
Let $m=\prod_i p_i$ where p_i is the *i*-th prime factor of *m*. Now take $m^2=\left(\prod_i p_i\right)^2=\prod_i \left(p_i^2\right)=\prod_i p_i \cdot p_i$. This shows that $p_i|m \Rightarrow p_i^2|m^2$, and therefore that $p_i^2 \nmid m^2 \Rightarrow p_i \nmid m$.

2)

s	t	r	step	euclid
1	0	-5083		-5083=-4*1656+1541
0	1	1656		1656=1*1541+115
1	4	1541		1541=13*115+46
-1	-3	115		115=2*46+23
14	43	46		46=2*23
-29	-89	23		

3) Prove $\forall a:\forall b:\forall c, c>0 \Rightarrow gcd(ac,bc)=c\cdot gcd(a,b)$. Let the multiset of prime factors of *n* be denoted n^* (for example $60^*=\{2,2,3,5\}$). Note that $n=\prod_i n_i^*$. For convenience, we will define $1^*=\emptyset$. Now, let *a*, *b* and *c* be integers, with $c>0$. $ac=a^*\cup c^*$, and $bc=b^*\cup c^*$. The *gcd* function finds the greatest common divisor between two numbers, which by definition is the intersection of prime factors between the two numbers. Thus, we can view *gcd* as $gcd(x,y)=\prod_i \{x^*\cap y^*\}_i$. Therefore, $gcd(ac,bc)^*=(a^*\cup c^*)\cap(b^*\cup c^*)=c^*\cup(a^*\cap b^*)$ .This last result can be rewritten as $gcd(ac,bc)^*=c^*\cup gcd(a,b)^*$, and multiplying through this (to get $gcd(ac,bc)$), we get $gcd(ac,bc)=\left(\prod_i c_i^*\right)\left(\prod_j gcd(a,b)_j^*\right)=c\cdot gcd(a,b)$, by definition. Therefore $\forall a:\forall b:\forall c, c>0 \Rightarrow gcd(ac,bc)=c\cdot gcd(a,b)$.

4) RTS $gcd(ab,c)=gcd(b,c)$ if $gcd(a,c)=1$.
If $gcd(a,c)=1$, then $gcd(a,c)^*=a^*\cap c^*=1^*=\emptyset$.
$gcd(ab,c)^*=(a^*\cup b^*)\cap c^*$
$(a^*\cup b^*)\cap c^*=(a^*\cap c^*)\cup(b^*\cap c^*)$
$(a^*\cap c^*)\cup(b^*\cap c^*)=\emptyset\cup(b^*\cap c^*)=b^*\cap c^*$ as shown above, therefore
$gcd(ab,c)^*=b^*\cap c^*=gcd(b,c)^*$, which of course shows
$gcd(ab,c)=gcd(b,c)$.

However, $gcd(ab,c)=gcd(a,c)\cdot gcd(b,c)$ is not true in general. Take $a=12, b=8, c=24$.
$gcd(ab,c)=gcd(96,24)=24$, but $gcd(12,24)\cdot gcd(8,24)=12\cdot 8=96$.

5) $gcd(a,b)=gcd(2a+b,3a+2b) \Rightarrow \exists x : \exists y : ax+by=(2a+b)x+(3a+2b)y$. Using this, we can expand either side of the equation as $ax+by=2ax+bx+3ay+2by$. Gathering like terms, this simplifies to $ax+by=a(2x+3y)+b(x+2y)$. We can then rewrite this as $gcd(x,y)=gcd(2x+3y,x+2y)=gcd(y,x)=gcd(2y+x,3y+2x)$. Therefore $gcd(a,b)=gcd(2a+b,3a+2b)$.