~~29~~ 40

9. Let m and n be integers, and let d be the greatest common divisor of m and n. Prove that there exists integers r and s with $d = rm + sn$.

Let $H = \{rm + sn \mid r, s \in \mathbb{Z}\}$
Let h be the smallest positive element in H. Observe that every element of H has the form ah for some $a \in \mathbb{Z}$. Indeed, if $k \in H$, then divide h into k to get

$$k = ah + \rho$$

where a and ρ are in $\mathbb{Z}$ and $0 \le \rho \le h-1$
(In other words h went into k a times with a remainder of ρ
We see that ρ is also in H. But h is the smallest positive element of H so ρ must be 0.

We claim that h is the g.c.d of m + n.
m is in H and every element of H is divisible by h so $h \mid m$.
The same argument shows $h \mid n$. So h is a common divisor of m and n. On the other hand $h = rm + sn$ for some integers r + s. The gcd of m and n divides both m and n so it must also divide h. We have shown that $h \le$ g.c.d (m,n) and g.c.d $(m,n) \le h$. It follows that $h =$ g.c.d (m,n) and of course $h = rm + sn$ for some integers r and s.