GAUSS'S LEMMA

Lemma 1 (Gauss's lemma)**.** *Let f be a monic polynomial with coefficients in $\mathbb{Z}$, and suppose that $f = gh$ where g and h are monic polynomials with coefficients in $\mathbb{Q}$. Then g and h actually have coefficients in $\mathbb{Z}$.*

Proof. Let m be the smallest positive integer such that mg has integer coefficients. Then the coefficients of mg have no common divisor greater than 1. Likewise, let n be the smallest positive integer such that nh has integer coefficients. We now show that $m = n = 1$.

Assume that $mn > 1$. We choose any prime p dividing mn, and consider the equation $mnf = (mg)(nh)$. Reducing the coefficients modulo p, we have $0 = \overline{(mg)(nh)}$. Since $\mathbb{Z}_p$ is an integral domain, so is $\mathbb{Z}_p[x]$. We thus have $\overline{mg} = 0$ or $\overline{nh} = 0$. That is, p divides all coefficients of g or all coefficients of h. This contradicts the minimality of m and n. $\square$