

28.6 (iii): Suppose $x = qy + r$, where $x, y, q, r \in \mathbb{Z}$ (you do not need to assume that y does not divide x). We want to prove that $\gcd(x, y) = \gcd(y, r)$. Let $d := \gcd(x, y)$. This means that d divides x and y . By the relation $r = x - qy$, it follows from Theorem 27.5 that d divides r . So d is a common divisor of y and r , and hence $d \leq \gcd(y, r)$.

Next, we want to prove that d is the greatest integer that divides y and r . For this, we follow Houston's suggestion to prove by contradiction (however, there is a direct approach which also works). Then we assume there is some e which divides y and r , and $d < e$. Then e also divides $x = qy + r$, and so $e \leq \gcd(x, y) = d$, which is a contradiction.

Here is an alternative way to finish the proof after the first paragraph: By definition, $\gcd(y, r)$ divides y and r , so it must divide $x = qy + r$ by Theorem 27.5. This implies $\gcd(y, r) \leq d = \gcd(x, y)$, which proves $\gcd(x, y) = \gcd(y, r)$.

28.19 (i): $\gcd(14592, 6468) = 12$ and $\gcd(-12870, 4914) = 234$.