

Q5a: By corollary 1.2 we have that for any $a, b \in \mathbb{Z}$, there exists unique $q, r \in \mathbb{Z}$ so that $a = qb + r$ and $|r| < |b|$. We check 2 cases. First if $|r| \leq \frac{|b|}{2}$ then we are done. If not, that is if $\frac{|b|}{2} < r < |b|$ then we do the following. If $b > 0$, then we have $a = b(q+1) + (r-b)$. We have that $|r-b| < \frac{|b|}{2}$. Now if $b < 0$, then we have $a = b(q+1) + (r+b)$ and $|r+b| < \frac{|b|}{2}$. We now claim uniqueness. Suppose that $a = q_1b + r_1 = q_2b + r_2$. We have that $b(q_2 - q_1) = r_1 - r_2$. Suppose that $q_1 \neq q_2$, then we have that $|q_2 - q_1| \geq 1$. This implies that $|r_1 - r_2| \geq |b|$. But since $|r_1|, |r_2| < \frac{|b|}{2}$, this can never happen. Hence $q_1 = q_2$ and $r_1 = r_2$. The new updated Euclidean Algorithm is as follows:

$$\begin{aligned} a &= q_1b + r_1 \\ b &= q_2r_1 + r_2 \\ r_1 &= q_3r_2 + r_3 \\ &\vdots \\ r_n &= 0 \end{aligned}$$

At the i 'th step, the remainder term r_i will be bounded above by $\frac{|b|}{2^i}$.

Q5b: We will compute $\gcd(1066, 1492)$ and $\gcd(1485, 1745)$. First, we will use the Euclidean Algorithm:

$$\begin{aligned} 1492 &= 1066 + 426 \\ 1066 &= 2 \cdot 426 + 214 \\ 426 &= 214 + 212 \\ 214 &= 212 + 2 \\ 212 &= 106 \cdot 2 \end{aligned}$$

We see in 5 steps that $\gcd(1066, 1492) = 2$. We will now compute this with our new least remainder algorithm.

$$\begin{aligned} 1492 &= 1066 + 426 \\ 1066 &= 3 \cdot 426 - 212 \\ 426 &= -2 \cdot (-212) + 2 \\ -212 &= -106 \cdot 2 \end{aligned}$$

We get the same result but in 4 steps. Now for $\gcd(1485, 1745)$, we know from previously that the Euclidean algorithm will return 5 as our result in 6 steps. Using the least remainders algorithm;

$$\begin{aligned} 1745 &= 1485 + 260 \\ 1485 &= 6 \cdot 260 - 75 \\ 260 &= -3 \cdot (-75) + 35 \\ 75 &= 2 \cdot 35 + 5 \\ 35 &= 5 \cdot 7 \end{aligned}$$

This terminates in 5 steps. This is faster than the euclidean algorithm.

Q5c: In general, suppose that the algorithm terminates in n steps. Since $r_n = 0$ and $r_i < \frac{|b|}{2^i}$ we will have that $\frac{|b|}{2^n} < 1$ and so $|b| < 2^n$. Therefore the number of steps, n , bounds above the quantity $\log_2(|b|)$. So The number of steps will be $n = \lceil \log_2(|b|) \rceil$