Proving facts about numbers.... Number Theory.

— Some applications of number theory are applicable to modern life

eg internet security.

The mathematical interest in integers, not in (Country) Country, but in their use in the arithmetical system.

e.g. $9/4 = 2$ (quotient)
1 (remainder)

Division Theorem: Let a, b be integers, $b > 0$

then there are unique integers q, r such that $a = q \cdot b + r$ and $0 \leq r < b$.

Two parts to the theorem:

1) Existence part ("there are")
2) Uniqueness part (unique)

Proof: we prove existence first, then uniqueness

① Existence: look at all non-negative integers of the form $a - kb$, where k is an integer, and show that one of them is less than b.

So, the theorem says: among the integers $a = qb + r$ (or $a - qb$ or $a - kb$), namely the integers r, there is one with r between 0 and b

- so the k that will satisfy the condition, is the q in our theorem.

- Need to show that such integers exist

Eg. Take $k = -|a|$ → absolute value of a

then since $b \geq 1$

$$\therefore a - kb = a + |a| \cdot b \geq a + |a| \geq 0.$$

Let r be the smallest such integer.

Let q be the value of k for which it occurs

i.e. $r = a - qb$

To complete the proof, we show that $r < b$.

Suppose on contrary, that $r \geq b$ [using proof by Contradiction]

Then: $a - (q+1)b = a - qb - b = r - b \geq 0$

Thus $a-(q+1)b$ is a non-negative integer of the form $a - kb$. But r is the smallest such, and yet $a-(q+1)b < a - qb = r$

- this is Contradiction!

Hence $r < b$

This proof existence.

Now lets prove uniqueness!

Uniqueness: We show that if there are two representations of a,

$$a = qb + r = q'b + r', \quad 0 \le r, r' < b,$$

then $r = r'$ and $q = q'$.

[q will denote quotient
r will denote remainder]

Rearranging the above equation:

$$1) \quad r' - r = b(q - q')$$

Taking absolute value in 1)

$$2) \quad |r' - r| = b\,|q - q'|$$

But $\quad -b < -r \le 0 \quad$ and $\quad 0 \le r' < b$

$$\therefore \quad -b < r' - r < b$$

$$\therefore \quad |r' - r| < b.$$

So by 2) $\quad b \cdot |q - q'| < b$

Hence $|(q-q')| < 1$

Hence $q = q'$.

Then by i), $r = r'$ that proves uniqueness

→ ∎ ✓

Example like the Hilbert Hotel demostrate the use of rigorous proofs in mathematics

↳ which deals with infinity, rigorous proofs are the only thing we can rely.

↳ how we are not familiar with

Perus Division theorem, it only apply to division of positive numbers, but there is a more general version

Theorem: (General Division Theorem): Let a, b be integers, $b \neq 0$, then there are unique integers q, r such that $a = qb + r$ and $0 \leq r < |b|$

Proof: We have proved the result in the case $b > 0$,

so assume $b < 0$

Then, since $|b| > 0$, the previous theorem tells us

there are unique integers q', r' such that

$$a = q' \cdot |b| + r' \quad \text{and} \quad 0 \leq r' < |b|$$

Let $q = -q'$, $r = r'$. Then, since $|b| = -b$,

we get $a = q \cdot b + r$, $0 \leq r < |b|$

⇒ With general division theorem established, we can give formally name to q & r

* The number q is called quotient of a by b

* r is called the remainder

Trivial proof but powerful for issues we not familiar with e.g. Hilbert's Hotel