RECAP $\mathbb{N} = 1, 2, 3, 4, \ldots$

$\mathbb{Z} = \ldots -3, -2, -1, 0, 1, 2, 3, \ldots$

- Operators $+, \times, -$ obey familiar laws.
- There is an order $<$, but take care: if $n<m$ and $a<0$ then $an > am$!
- We say $d$ divides $n$ and write $d \mid n$ if there exists $k \in \mathbb{N}$ such that $n = kd$.
- If $a \mid b$ and $b \mid c$ then $a \mid c$.
- If $a \mid b$ and $a \mid c$ and $b<c$ then $a \mid c-b$.

---

**Definition** Let $n \in \mathbb{N}$, $n \geq 2$. Then $n$ is prime if its only factors are $1$ and $n$. We say $n$ is composite otherwise.

**Lemma 4.3** Let $n \in \mathbb{N}$, $n \geq 2$. Then $n$ has at least one prime factor.

**Proof** Let $P(n)$ be the statement "$n$ has a prime factor".

We prove $P(n)$ by strong induction.

Base case ($n=2$). $2 \mid 2$ and 2 is prime, so $P(2)$ is true.

Inductive step ($n>2$).

- If $n$ is prime then $n \mid n$ and $P(n)$ is true.
- If $n$ is composite, $n$ has a factor $m$ with $1<m<n$. By $P(m)$, $m$ has a prime factor $p$. Then $p \mid m$ and $m \mid n$ and so $p \mid n$ by transitivity (Lemma 4.1). So $P(n)$ holds. ⊠

Repeating this argument we can express any natural number $n \geq 2$ as $n = \overbrace{p_1 p_2 \cdots p_k}^{\text{primes}}$. This observation is one part of the Fundamental Theorem of Arithmetic. The other part is that this decomposition into primes is unique.(*)

Example $84 = 2 \times 2 \times 3 \times 7$

(*) Up to reordering of the factors.

Theorem 4.4 There are infinitely many primes.

Proof We use proof by contradiction. Suppose there are only finitely many primes. List the primes $p_1, p_2, \dots, p_m$. Then let $n = p_1 p_2 \cdots p_m + 1$. By Lemma 4.3, $n$ has a prime factor $p$. By assumption, $p = p_i$ for some $i$. Now, $p \mid n$ and $p \mid p_1 p_2 \cdots p_m$ i.e. $p \mid (n-1)$. By Lemma 4.2, $p \mid (n-(n-1))$ i.e., $p \mid 1$. This is a contradiction. ☒

## 4.3 Greatest common divisor

**Definition** Let $a, b \in \mathbb{N}$. Then $\gcd(a,b)$ is the largest number that divides both $a$ and $b$. We say that $a, b$ are coprime if $\gcd(a,b) = 1$.

**Examples** $\gcd(18,30) = 6$ :

Divisors of 18 are 1, 2, 3, 6, 9 ; of 30 are 1, 2, 3, 5, 6, 10, 15.

A better way is to use unique prime factorisations.

$\gcd(84,70) = 2^1 \times 7^1 = 14$, since:

$84 = 2 \times 2 \times 3 \times 7 = 2^2 \times 3 \times 7$ ; $70 = 2 \times 5 \times 7$

In general, exponent of $p$ is the smaller exponent of $p$ in the prime decompositions of $a$ and $b$.

Final examples: $\gcd(a,1)=1$, $\gcd(a,a)=a$, $\gcd(a,b)=b$, when $b \mid a$.

**Lemma 4.5** Suppose $a,b \in \mathbb{N}$. Then there exist $q,r \in \mathbb{Z}$ such that $a = qb + r$ where $0 \leq r < b$.

Example: $a=30$, $b=8$. Then $q=3$ and $r=6$. $(30 = 3\times 8 + 6)$

*Proof* Let $q$ be the largest number such that $qb \leq a$. Then $r = a - qb$. Note that $r \geq 0$. Now note[+] that $(q+1)b > a$. Rearranging, $b > a - qb = r$. Combining the inequalities, $0 \leq r < b$.

[+] since $q$ is maximal! ☒

**Proposition 4.6** Suppose $a,b \in \mathbb{N}$, $q,r \in \mathbb{Z}$ satisfy $a = qb + r$ with $0 < r < b$. Then $\gcd(a,b) = \gcd(b,r)$.

*Proof* Let $d = \gcd(a,b)$. $d$ is a common divisor, so $d \mid a$ and $d \mid b$. Now $r = a - qb$. Note that $d$ divides the

right hand side (Lemma 4.2). So $d$ divides the left hand side, i.e., $d \mid r$. Observe that $d$ is a common divisor of $b$ and $r$. So $d \leq \gcd(b,r)$, i.e., $\gcd(a,b) \leq \gcd(b,r)$. ⊛

Now let $d = \gcd(b,r)$, so $d \mid b$ and $d \mid r$. Note that $a = qb + r$; $d$ divides the r.h.s, so $d \mid a$. As $d$ is a common divisor of $a$ and $b$, we have $d \leq \gcd(a,b)$, ie. $\gcd(b,r) \leq \gcd(a,b)$. ⊛ Putting ⊛ together, we obtain the result. ⊠

Example

$$\begin{aligned} \gcd(96,66) &= \gcd(66,30) && 96 = 1\times 66 + \underline{30} \\ &= \gcd(30,6) && 66 = 2\times 30 + \underline{6} \\ &= \gcd(6,0) && 30 = 5\times 6 + \underline{0} \\ &= 6 \end{aligned}$$

Explicitly:

Euclid's Algorithm

Find $\gcd(a,b)$

Input: $a, b \in \mathbb{N}$, $[a \geq b]$

- find $q, r$ such that $a = qb + r$, with $0 \leq r < b$.
- If $r = 0$ the stop and return $b$.
- otherwise compute $\gcd(b, r)$.