Divisibility and Primes

1 Divisibility and Perfect Numbers

If a,b are integers and $a \neq 0$ then a **divides** b iff b=ak for some integer k

a—b means "a is a divisor of b"/"a is a factor of b"/"b is a multiple of a"

A positive integer $p > 1$ is prime if its only positive divisors are 1 and p

2 Properties of divisibility

2.1 Theorem

The following statements about divisibility hold

1. if a—b then a—(bc) for all c
2. if a—b and b—c then a—c
3. If a—b and a—c then a—(sb+tc) for all s,t
4. For all $c \neq 0$, a—b iff $(ca)|(cb)$

2.2 Proof

Let's prove item 2:

- Since a—b, there is k_1 such that $b = ak_1$
- Since b—c there is k_2 such that $c = bk_2$
- Then $c = a(k_1k_2)$ so a—c

3 The division algorithm

3.1 Theorem

Let a be an integer and d a positive integer. Then there exists unique numbers q and r, with $0 \leqslant r < d$, such that $a = qd + r$

3.2 Definition

In the equality in the division algorithm:

- q is the quotient, denoted by $qent(a, d)$ or a div d
- r is the remainder, denoted by $rem(a, d)$ or a mod d

4 Fundamental properties of primes

4.1 Theorem

Every positive integer $n > 1$ can be uniquely represented as $n = p_1 \cdot p_2 \cdots p_k$ where the numbers $p_1 \leqslant p_2 \leqslant ... \leqslant p_k$ are all prime

4.2 Theorem

There are infinitely many prime numbers

4.3 Proof

Assume that there are finitely many primes, say $p_1, ..., p_n$ then consider the number $q = p_1 \cdots p_n + 1$
By the fundamental theorem, q is either prime, or can be written as the product of primes. Hence $p_i | q$ for some i, say $p_1 | q$
But then p_1 divides $q + (-p_2 \cdots p_n)p_1 = 1$, a contradiction

4.4 Theorem

The number of primes not exceeding x approaches $x \ln x$ as x grows infinitely.

5 The greatest common divisor

Let $gcd(a, b)$ denote the greatest common divisor of a and b
A linear combination of a and b is any number of the form $sa + tb$

5.1 Theorem

$gcd(a, b)$ is equal to the smallest linear combination of a and b

5.2 Proof

Let $m = sa + tb$ be smallest positive. We prove that $m = gcd(a, b)$ by showing that $gcd(a, b) \leqslant m$ and $m \leqslant gcd(a, b)$
Any common divisor of a, b divides m, hence $gcd(a, b)|m$ and $gcd(a, b) \leqslant m$

Now show that $m \leqslant gcd(a, b)$. We show that $m|a$
By division algorithm, we have $a = qm + r$ where $0 \leqslant r < m$
As $m = sa + tb$ we have $a = q(sa + tb) + r$, or $r = (1 - qs)a + (-qt)b$
Since m is the smallest positive linear combination of a and b, and $0 \leqslant r < m$ we must have $r = 0$ and hence $m|a$
Similarly one shows m—b and so $m \leqslant gcd(a, b)$

6 Properties of the GCD

6.1 Lemma

The following statements hold:

- gcd(ka,kb)=$k \cdot gcd(a, b)$ for all $k > 0$
- If gcd(a.b)=1 and gcd(a,c)=1 then gcd(a,bc)=1
- if a—bc and gcd(a,b)=1 then a—c

6.2 Proof

We prove item 2, the other parts are similar
Since gcd(a,b)=1 and gcd(a,c)=1, there are number s,t,u,c such that $sa + tb = 1$ and $ua + vc = 1$
Multiplying these together gives $(sa + tb)(ua + vc) = 1$
Rewrite LHS as $a \cdot (sau + tbu + svc) + bc(tv)$
This is a linear combination of a and bc, and is equal to 1
Hence $gcd(a, bc) = 1$

7 Euclid's Algorithm

7.1 Lemma

If $a = qb + r$ then $gcd(a, b) = gcd(b, r)$

7.2 Proof

Suppose d—a and d—b. Then d—r because $r = a - qb$ and so d—gcd(b,r).
Conversely, if d—b and d—r then d—a and so d—gcd(a,b)
Then gcd(a,b) and gcd(b,r) divide each other, so gcd(a,b)=gcd(b,r)

7.3 Method

Suppose $a > b$ are positive numbers. Euclid's algorithm finds gcd(a,b) as follows

- let $r_0 = a$ and $r_1 = b$. Recursively compute numbers r_2, r_3...
- Use division algorithm ($r_i = r_{i+1}q_1 + r_{i+2}$) to find $r_{i+2} = rem(r_i, r_{i+1})$
- Note that $0 \leqslant r_{i+2} < r_{i+1}$. Therefore, for some n, $r_n > 0$ and $r_{n+1} = 0$
- We know that $gcd(r_i, r_{i+1}) = gcd(r_{i+1}, r_{i+2})$ for all i (by the above lemma)
- $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$

7.4 Example

Find gcd(414,662)

$$\begin{aligned}
662 &= 414 \cdot 1 + 248 \\
414 &= 248 \cdot 1 + 166 \\
248 &= 166 \cdot 1 + 82 \\
166 &= 82 \cdot 2 + 2 \\
82 &= 2 \cdot 41
\end{aligned}$$

The last non-zero remainder is 2, so gcd(414,662)=2

7.5 Example 2

How do we modify Euclid's algorithm to express gcd(a,b) as a linear combination of a and b? In every line, express the current remainder as a linear combination of a and b

$$\begin{array}{lll}
662 = 414 \cdot 1 + 248 & 248 = 662 + (-1) \cdot 414 & \\
414 = 248 \cdot 1 + 166 & 166 = 414 + (-1) \cdot 248 & = (-1) \cdot 662 + 2 \cdot 414 \\
248 = 166 \cdot 1 + 82 & 82 = 248 + (-1) \cdot 166 & = 2 \cdot 662 + (-3) \cdot 414 \\
166 = 82 \cdot 2 + 2 & 2 = 166 + (-2) \cdot 82 & = (-5) \cdot 662 + 8 \cdot 414 \\
82 = & 2 \cdot 41 &
\end{array}$$

The last non zero remainder is 2, so $gcd(414, 662) = 2 = (-5) \cdot 662 + 8 \cdot 414$

8 Relatively prime numbers

8.1 Definition

Two numbers a and b are called relatively prime if gcd(a,b)=1

8.2 Example

The value $\phi(n)$ of Euler's ϕ-function on a number n is the number of integers a with $1 \leqslant a \leqslant n$ that are relatively prime with n