# Number Theory

* Let we say is **divisible** by if for some .
* We write and call a **divisor** of , and a **multiple** of .
* If does not divide , we write

|  |
| --- |
| Definition - Transitivity of Divisibility: |
| **If** |

#### *Proof:*

|  |
| --- |
| Definition – Divisibility by Primes: |
| **Every is divisible by some prime number.** |

#### *Proof: (Strong Induction)*

1. For , suppose every integer is divisible by a prime. Show that is divisible by a prime.

Case 1: is a prime. Then

Case 2: is composite. Then for some ,

By hypothesis, . Since , by transitivity

∴ Every is divisible by a prime.

Exercise:

Find a prime factor:

1. 693



1. 1048



### Theorem:

There are infinitely many primes.

#### *Proof: (by contradiction)*

Suppose there are finitely many Primes, .

Construct a number p defined by .

Clearly is larger than all the primes, so is not equal to any of the primes.

Hence is divisible by a prime.

Without loss of generality (WLOG),



🡨 a contradiction



∴ There are infinitely many primes.

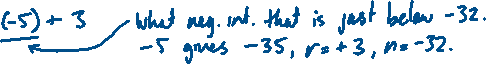
## Quotient-Remainder Theorem

* If and , then there exists a unique such that:

|  |
| --- |
| Definition |
|  |

Exercise:

Find .



## Fundamental Theorem of Arithmetic

* Every can be factorized uniquely in the form:

Where

#### Proof:

The proof requires the following Lemma:

Euclid’s Lemma: Let be prime, . If , then OR .

First, we show that every is either a prime or a product of primes, by strong induction.

1. 2 is prime.
2. Suppose are all either prime or product of primes.  
   Prove that is either prime or product of primes.
   1. If is prime 🡪 there is nothing more to prove.
   2. If not, then it is a composite:

By hypothesis, and are products of primes.

Then is a product of primes.

∴ Ever is either prime or a product of primes.

Now we show uniqueness, by contradiction.

Assume that is the product of primes in two different ways:

Since , Euclid’s Lemma says , divides one of the . Without loss of generality, let . Since , is prime, its divisors are and . Hence, , and:

By the same logic, must divide one of the remaining , WLOQ . Then

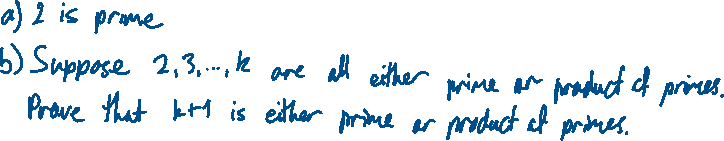
Continuing like this, we find that and .

The same argument with the primes and primes reversed gives us that and .

Therefore, and we have that the two factorizations are the same.

Exercise:

Find the prime factorization.



1. 924



1. 1300
2. 2722
3. 50,193



## Greatest Common Divisor

* Let with at least one of nonzero.
* The **greatest common divisor** of and , denoted by is the number such that:
* is a common divisor of and : and
* If is a common divisor of and , then

|  |
| --- |
| Definition |
|  |

Exercise:

, since and , and there is no bigger integer that divides them both.

Note:

* **Prime factorizations** can be used to find , if:

and (some can be zero), then

Exercise:

Given that and , we have:

## Least Common Multiples (LCM)

* Let with at least one of nonzero.
* The **least common multiple** of and , denoted by , is the number such that:
* is a common multiple of and , i.e., .
* If is a common multiple of and , then .

Exercise:

* We can use **prime factorization** to calculate , if:

(some can be zero), then

Exercise:

Given that and , we have:

Exercise:

1. Find
2. Find



## The Euclidean Algorithm

* The Euclidean Algorithm is a process for finding the greatest common divisor.
* It works because of the Quotient-Remainder Theorem and the following two lemmas:

Lemma 1: For all

#### Proof 1:

Lemma 2: Let , then

#### Proof 2:

Let , we will show that

Since and are integers, we have , so .

Hence, , and we have .

Since and are integers, we have , so .

Hence, , and we have .

Therefore, . So, every common divisor of and is also a common divisor of and , and vice versa.

### Euclidean Algorithm

1. Let
2. Check if . If so, Lemma 1 says
3. If , use Quotient-Remainder Theorem to find with such that .   
   Lemma 2 says .
4. Set and go to step 2.

* This algorithm will terminate with , since each remainder is smaller than the previous one.

Exercise:

Find .



Exercise:

Find .



|  |
| --- |
| Definition |
| **Integers are called coprime (relatively prime, mutually prime) if .** |

Exercise:

True or false? For all there exists such that .

### Bézout's Identity Theorem

* Let , then exists, and there exists such that .

Corollary: if and are relatively prime, then there exist such that .

* How do we find ?
* We use the Euclidean Algorithm in reverse.

Exercise:

Find such that



Exercise:

Find such that .



## The Pigeonhole Principle

* Let
* If pigeons fly into pigeonholes, then some pigeonhole contains at least two pigeons.

#### Proof:

Suppose that each pigeonhole contains at most one pigeon.

Then the total number of pigeons is at most



Therefore, there exists a pigeonhole that contains more than one pigeon.

Examples:

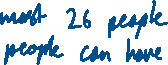
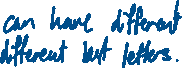
1. You have a drawer full of socks, of 3 different colours. How many socks must you pick at random to be sure you have a matching pair?  
   A: 4. The first 3 could possibly be all 3 different colours, but the fourth will match one or those (or else there’s a previous pair).
2. In a room of 367 people (allowing for leap year), at least 2 of them share a birthday.
3. Humans have a maximum of about 500,000 hairs. Is it guaranteed that 2 residents of Wollongong have exactly the same number of hairs? How about 2 residents of Sydney?

* Some formal equivalent statements to the pigeonhole principle:

1. Let be a set of elements. If is partitioned into pairwise disjoint subsets, where , then at least one subset contains more than one element.
2. A function from one finite set to a smaller set cannot be one-to-one. There must be at least two elements that map to the same point.

Exercise:

In a group of 700 people, must there be two whose first names have the same first and last letters?

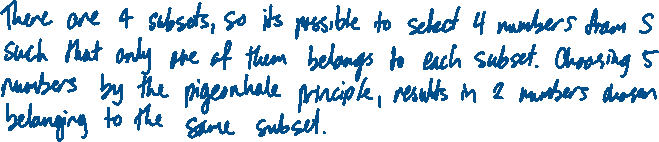


* Problems of this sort involve figuring out how to form the pigeonholes properly (how to partition the set).

Exercise:

5 different numbers are selected from the set . Show that 2 of the selected

numbers sum to 9.



Exercise:

A restaurant serves 3 different salads, 6 different mains and 4 different desserts. How many people must eat there to ensure that at least 2 of them have the same meal.

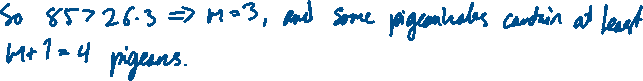


### Generalised Pigeonhole Principle

* If pigeons fly into pigeonholes, and for some , then some pigeonhole contains at least pigeons.

Exercise:

Show that in a group of 85 people, the first name of at least 4 of them must start with the same letter.



Exercise:

We want to assign 70 students to 11 classes so that no class has more than 15 people. Show that there must be at least 3 classes with 5 or more people.

