1. Euclidian Division Algorithm

We are interested in finding the greatest common divisor between two numbers \(a\) and \(b\), and Euclidian division algorithm is an effective way of doing that.

Originally the algorithm must have been discovered in geometry, where we take a rectangle with sides \(a\) and \(b\), and we try to tile this rectangle with square tiles as large as possible. For example to find \(\text{gcd}(5, 8)\), we take an \(8 \times 5\) rectangle and begin the tiling with a \(5 \times 5\) tile, and we will be left with an empty \(3 \times 5\) rectangle. Then we use a \(3 \times 3\) tile, then a \(2 \times 2\) and to complete, we need 2 of the \(1 \times 1\) tiles. The size of the smallest tile we use is the \(\text{gcd}(5, 8)\).

Here is the Euclidian division algorithm with 326 and 78 in algebraic terms:

**Example**

\[
\begin{align*}
326 &= 4 \times 78 + 14 \\
78 &= 5 \times 14 + 8 \\
14 &= 1 \times 8 + 6 \\
8 &= 1 \times 6 + 2 \\
6 &= 3 \times 2 + 0
\end{align*}
\]

The circled numbers are the remainders in each division. On the second line, we use the remainder 14 from first line as a divisor, on the third line we use the remainder 8 from second line as a divisor...etc and each time the remainders are getting smaller. Eventually this process is going to end when we hit zero as a remainder.
remainder. Our gcd is the divisor in the last line, or you can see it as the remainder in the line one above the last one.

I recommend thinking about how the algebraic version and geometric version of the algorithm are related to each other.

Now we will start looking at a seemingly different problem. Let’s try to see which integers can we get as a linear combination of 326 and 78. At the end, we will see that the minimum positive linear combination of 326 and 78 is exactly the gcd(78, 326).

**Example** $1 \times 326 - 4 \times 78 = 14$ by the first line in the division algorithm above. Let’s see if we can get a smaller number.

$6 \times 326 - 24 \times 78 = 84$ it seems like we can take out another 78 now:

$6 \times 326 - 25 \times 78 = 6$ and now we can use a combination of the first equation and the third to obtain $14 - 2 \times 6 = 2$ as follows:

$1 \times 326 - 4 \times 78 - 2 \times (6 \times 326 - 25 \times 78) = (-13) \times 326 + 46 \times 78 = 2$

In class, you showed that the minimum positive element of the set

$S = \{a \times 326 + b \times 78 | a, b \in \mathbb{Z}\}$

is the gcd(78, 326).

Euclid’s division algorithm gives a method of writing the gcd(78, 326) as a linear combination of 78 and 326. All you have to do is follow the algorithm backwards.

The geometric reasoning, the algebraic algorithm and the minimum positive linear combination of two numbers are all describing the same concept, gcd. As is the case in general mathematics, the more perspectives you have on a topic, the stronger you are.

## 2. Primes

Now we will be looking at integers more closely to understand what they are really made of. If we look at any material with a strong enough microscope, we will see that they are all made of elementary physical particles that are described in today’s standard model in physics. This is a quite new discovery compared to our discoveries about integers.

**Definition** An integer $n \geq 1$ is called a prime number if it’s only divisors are 1 and itself.

Notice that we are casting out 1 for no particular reason, or at least we can’t see that reason right now.

**Euclid’s lemma** If $p$ is a prime number and $p | ab$, then $p | a$ and $p | b$. The converse is also true.

Euclid’s lemma gives us a complete characterization of prime numbers. You can check if a number is prime using the above criteria, and conversely any number satisfying the above criteria must be prime.

**Example** Here is a non-example: $4 | 2 \times 2$, but $4 \nmid 2$. Not satisfying the above criteria, 4 is not a prime number.

**Fundamental theorem of Arithmetic** And natural number $a \geq 2$ is either a prime, or a product of primes.

Using this fact, we can get a complete factorisation of any natural number into prime factors, possibly with some powers:

$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$
Moreover this factorisation into primes is unique up to reordering. Therefore prime numbers are the building blocks of all natural numbers. If we want to understand all numbers, it is enough to understand the prime numbers. This is a good philosophy, however there are still infinitely many prime numbers. So we have quite a lot of work ahead of us.

**Remark** Now we can why we don’t 1 to be a prime number: If 1 was a prime, we would lose the uniqueness in prime factorization since you can always multiply any number with some copies of 1.

3. **Congruences, or Modular Arithmetic**

We saw how the division works

\[
a = qb + r
\]

with much of our attention being on the remainder \( r \). Now we will shift our attention to the divisors \( q \) or \( b \). We will declare \( a \) and the remainder \( r \) to be equivalent modulo \( b \) or modulo \( q \):

\[
(1) \quad a \equiv b \pmod{n} \iff a = b + kn \text{ for some integer } k
\]

Of course you are used to modular arithmetic we use in clocks(modulo 12, modulo 24), in calendars(modulo 7 for days of the week, modulo 52 to count the weeks of a year...etc). Maybe you are less familiar with modular arithmetic that is being used in error detection in digital world(ISBN uses modulo 10 or modulo 13, IBAN uses modulo 97 arguments ). Also the encryption algorithm RSA depends on modular arithmetic, computers do arithmetic modulo 2.

**Multiplication in modular arithmetic**

If \( a \equiv b \pmod{n} \) and \( a' \equiv b' \pmod{n} \), then \( aa' \equiv bb' \pmod{n} \).

This makes modular arithmetic remarkably simpler than usual arithmetic.

**Example**

\[
\begin{align*}
10 & \equiv 1 \pmod{3} \\
100 & \equiv 10 \times 10 \equiv 1 \times 1 \pmod{3} \\
1000 & \equiv 100 \times 10 \equiv 1 \times 1 \pmod{3}
\end{align*}
\]

Therefore to see if a number is divisible by 3, or in other words is a number is equivalent to zero modulo 3, it is enough to consider the sum of its digits modulo 3: \( 67254 \equiv 6 \times 10000 + 7 \times 1000 + 2 \times 100 + 5 \times 10 + 4 \times 1 \equiv 6 + 7 + 2 + 5 + 4 \equiv 24 \equiv 0 \pmod{3} \)

You can easily figure out such division rules by using simple modular arithmetic.

**Solving equations in modular arithmetic**

Eventually this is an algebra class and algebra aims to solve polynomial equations. Let’s try to solve some linear equations in modular arithmetic:

**Example** Consider the equation \( 2x = 1 \pmod{13} \). We are looking for an unknown \( x \) such that 2 times \( x \) will be a multiple of 13 plus 1. In other words, we need \( a, b \in \mathbb{Z} \) such that

\[
2a = 13b + 1
\]

or
so we are trying to see if we can write 1 as a linear combination of 2 and 13. But such linear combinations are related to gcd. Since gcd(2,13)=1, we can certainly find such $a$ and $b$. One way to obtain such $a$ and $b$ was using Euclidian division. In this case, it is not too difficult to see that

$$2 \times 7 \equiv 14 \equiv 1 \pmod{13}$$

so our solution is $x \equiv 7 \pmod{13}$. We have infinitely many solutions.

**Example** It is easy to see that the equation

$$6x = 3 \pmod{8}$$

doesn’t have a solution since gcd(6,8) = 2 and 3 is not a multiple of gcd(6,8), therefore 3 cannot be written as a linear combination of 6 and 8.

Finally here is a treat:

**Freshman’s dream**

For $p$ prime, $(a + b)^p \equiv a^p + b^p \pmod{p}$.

This is not a difficult result for people familiar with the binomial theorem

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

It is enough to show that the binomial coefficients are divisible by $p$, except the first one and the last one, which are zero. We leave this as an exercise after providing the formula

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$