# Chapter 5

# Mathematical Background 1

In order to understand some of the cryptographic algorithms dealt with throughout this course, it is necessary to have some background in two areas of mathematics: Abstract Algebra and Number theory. It will be attempted to keep the level of mathematics to the minimum required for a basic understanding of these algorithms.

As an example, the algorithm for the new Advanced Encryption Standard (AES) relies on the subject of finite fields which forms a part of abstract algebra. It is therefore necessary to understand some of the concepts of finite fields and the notation used to describe them. Students new to these areas of mathematics may find some of the ideas difficult to grasp at first however this will be remedied once some familiarity is obtained.

## 5.1 Number Theory

As it's name suggests, number theory deals with the theory of numbers and is probably one of the oldest branches of mathematics. It is divided into several areas including elementary, analytic and algebraic number theory. These are distinguished more by the methods used in each than the type of problems posed. To understand some of the topics discussed in this course, a number of elements from these different areas are needed. The relevant ideas are discussed here and include prime numbers, the greatest common divisor, the modulus operator, the modular inverse, Euler's Theorem and Fermat's little Theorem. A rigorous approach is purposely avoided but can be found in the recommended text.

### 5.1.1 Prime Numbers

A **prime** number $p$ is simply an integer greater than 1 with only two *positive* divisors, 1 and itself. This means that it's entire set of divisors (i.e. its factors) consist only of four integers $\pm 1$ and $\pm p$. It is therefore seen that 1 is *not* a prime number. Prime numbers are of the utmost importance to certain cryptographic algorithms and most of the techniques used will not work without them.

An interesting point to note is that any positive integer $I \geq 2$ is either a prime or can be expressed as the product of primes[1]:

[1] This is known as the fundamental theorem of arithmetic.

$$I = P_N^{\epsilon_N} \times P_{N-1}^{\epsilon_{N-1}} \times, \ldots, \times P_1^{\epsilon_1}, \qquad P_N > P_{N-1} > \ldots > P_1 \tag{5.1}$$

or another way of looking at this would be:

$$I = \prod_S P_n^{\epsilon_n}, \qquad \epsilon_n \geq 0 \tag{5.2}$$

where S is the set of all prime numbers[2].

As a result of equations 5.1 or 5.2, any integer $> 1$ that is not a prime is known as a **composite** number. It can be seen from this and the definition of a prime number above, that 1 is neither prime nor composite. As an example, the first ten prime numbers are: $2, 3, 5, 7, 11, 13, 17, 19, 23$ and 29.

### 5.1.2 Division

Any integer can be expressed as $n = q \times m + r$, where $n$, $q$, and $r$ are integers, $m$ is a positive integer and $0 \leq r < m$. An important point to note is that the **remainder** (also known as **residue**) $r$, must be *nonnegative* (i.e. either positive or $0$). This is seen by two restrictions: $0 \leq r < m$ and $q = \left\lfloor \frac{n}{m} \right\rfloor$[3]. For example, $24 \div 10$ is $2$ with a remainder of $4$ however, $-24 \div 10$ is $-3$ with a remainder of $6$ and not $-2$ with a remainder of $-4$ as might be expected. If $r = 0$ then $n$ is said to be a multiple of $m$. This is also the same as saying that $m$ divides $n$, is a divisor of $n$ or is a factor of $n$ and the notation used to express this is $m|n$.

The **greatest common divisor**, $m_{max}$, of two integers $a$ and $b$ is the largest *positive* integer that will divide both $a$ and $b$ without a remainder. Therefore, $m_{max}|a$, $m_{max}|b$ and $m_n|m_{max}$ for any divisor $m_n$ of $a$ and $b$. The notation generally used to represent this is $gcd(a, b) = m_{max}$.

If $gcd(a, b) = 1$, this means that $a$ and $b$ have no common factors other than 1. Such pairs of integers are known as **relatively prime** or **co-prime**. Along with prime numbers, numbers that are relatively prime have considerable importance in cryptography as will be seen later.

The greatest common divisor of two positive integers $a$ and $b$ ($gcd(a, b)$), can be determined by a procedure known as Euclid's Algorithm. It is based on the theorem that $gcd(a, b) = gcd(b, a \bmod b)$ a proof of which will not be given here. It is sufficient to know that it exists. The expression "$\mathrm{mod}$" is used in modular arithmetic which is a special kind of arithmetic involving remainders as will be seen next.

[2] Clearly in this case however, most of the exponents $\epsilon_n$ will be 0.

[3] The notation $\lfloor x \rfloor$ is known as the **floor** of the integer $x$ and is the greatest integer $\leq x$. Similarly, the notation $\lceil x \rceil$ is the **ceiling** of the integer $x$ and is the least integer $\geq x$.

### 5.1.3 Modular Arithmetic

Modular arithmetic is a form of arithmetic that will generally have been encountered before but may not have been recognised as such. An example given regularly is that of a 12 hour clock, where it is recognised that 3 hours after 11 o'clock it will be 2 o'clock (and not 14 o'clock). Modular arithmetic may seem a little confusing when first encountered but in fact has many parallels with ordinary arithmetic. The symbol used $(\equiv)$ is known as the **congruence** symbol and was invented by the German mathematician Karl Friedrich Gauss around the beginning of the 19th century. It resembles the equality symbol $(=)$ quite closely as was likely to be Gauss's intention.

Modular relationships are of the form $n \equiv R \pmod{m}$ (spoken as "n is congruent to R mod m") where $n$ and $R$ are integers and $m$ is a positive integer known as the modulus. If this congruence relationship holds, then it is said that $n$ is congruent to $R$ modulo $m$. The modulus operator $(\mathrm{mod})$ produces the remainder when the integer on it's left is divided by the modulus. Thus, the term $(R \bmod m)$ is equal to the remainder, $r$, when $R$ is divided by $m$.

If two remainders are equal then it can be written that $(n \bmod m) = (R \bmod m)$ - a standard equality. However, if the modulus is equal on both sides of the equation, then the mod $m$ term can be removed from the left hand side and the equality symbol replaced with a congruence symbol (along with a slight rearrangement of the brackets). Assuming $n \neq r$, it would be *incorrect*[4] to say $n = (R \bmod m)$ however it is *correct* to say that $n \equiv R \pmod{m}$ and this basically states that the same remainder (in this case $r$) results when both $n$ and $R$ are divided by $m$.

As was mentioned briefly above, the remainder $r$ is also known as a **residue** (remember that $0 \leq r < m$). If $R = r$ (i.e. $0 \leq R < m$) then $R$ is known as a **least residue**. The set of integers congruent to $r \pmod{m}$ is known as a **residue class** (also known as a congruence class). As $0 \leq r < m$, this means there are $m$ possible values of $r$ and hence there are $m$ possible residue classes.

The congruence relationship $n \equiv R \pmod{m}$ is only true if $m|(n-R)$. To understand why, it must be remembered that the integers $n$ and $R$ can be expressed as $q_{\{n,R\}} \times m + r_{\{n,R\}}$, where the subscript $\{n, R\}$ represents the fact that $q$ and $r$ will generally take on different values for $n$ and $R$. Only if $r_n = r_R$ will $m|(n-R)$ because in this case the two remainders cancel each other in the $(n-R)$ term: $(q_n \times m + r_n - q_R \times m - r_R) = (q_n \times m - q_R \times m)$. Because $m|(q_n \times m)$ and $m|(q_r \times m) \Rightarrow m|(q_n \times m - q_R \times m)$. If $n - R$ is not divisible by $m$ then the notation used to represent this is $\not|$ and therefore, $m \not| (n-R)$. In this case $n \not\equiv R \pmod{m}$.

[4] Some texts don't use the congruence symbol but instead write $n = R \pmod{m}$ where the brackets are placed only around the modulus operator and the modulus to identify congruency. This approach will not be used here however.

### 5.1.4 Modular Inverse

The idea of an inverse is important both in ordinary arithmetic and modular arithmetic. In any set of numbers, the inverse of a number contained in that set is another number which when combined with the first under a particular operation will give the Identity element[5] for that operation. Two examples of inverses are the additive inverse and a multiplicative inverse.

It must be noted that the Identity element under different operations will be different. For example, under addition it is 0, as any number added to 0 will remain unchanged. However, under *normal* multiplication the Identity element is 1 as any number multiplied by 1 will remain unchanged.

In ordinary arithmetic if the number is $x$ then the additive inverse is $-x$ and the multiplicative inverse is $\frac{1}{x}$. The idea is the same in modular arithmetic however if $x$ is an integer then its multiplicative inverse would not be $\frac{1}{x}$ as there is no such thing as a fraction in modular arithmetic. In this case it would be a number which, when multiplied by the original number, would give a result that is congruent 1 modulo $m$ (again, $m$ is the modulus). A number $x$ can only have a multiplicative inverse if it is relatively prime to the modulus (i.e., $gcd(x, m) = 1$).

When one number is operated on modulo some other number, it is said that the first number has been reduced modulo the second and the operation is called a modular reduction.

### 5.1.5 Euler's Theorem

Euler's Theorem which will be stated here without proof can be stated mathematically as

$$a^{\phi(m)} \equiv 1 \pmod{m}, \qquad gcd(a, m) = 1 \tag{5.3}$$

where $a$ is any integer and $m$ is the modulus (which, again, is restricted to being a positive integer). The symbol $\phi(m)$ is known as Euler's phi (or totient) function and is the number of positive integers $\leq m$ and relatively prime to it.

A few points should be noted about $\phi(m)$:

- The value of $\phi(1)$ is defined as being equal to 1.
- If $p$ is some prime, then $\phi(p) = p - 1$ as there are $p - 1$ positive integers $< p$ and relatively prime to it.
- If $p$ and $q$ are prime numbers and $n = pq$, then $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$. The reason for this is that the integers *not* relatively prime to $p$ and $q$ are $\{0, p, 2p, ..., (q - 1)p\}$ and $\{0, q, 2q, ..., (p - 1)q\}$ respectively. The number of

[5] This is a number that will leave the original number unchanged under that operation.

integers relatively prime to n is then $pq - (q + p - 1)$, where the 1 is subtracted so as not to include $0$ twice.

As an example take $4^{10} = 1,048,576 \equiv 1 \pmod{11}$ because $11 \times 95,325 + 1 = 4^{10}$.

### 5.1.6 Fermat's Little Theorem

Fermat's Little Theorem is really a specific case of Euler's theorem where $m$ is prime[6]. It can be stated as follows:

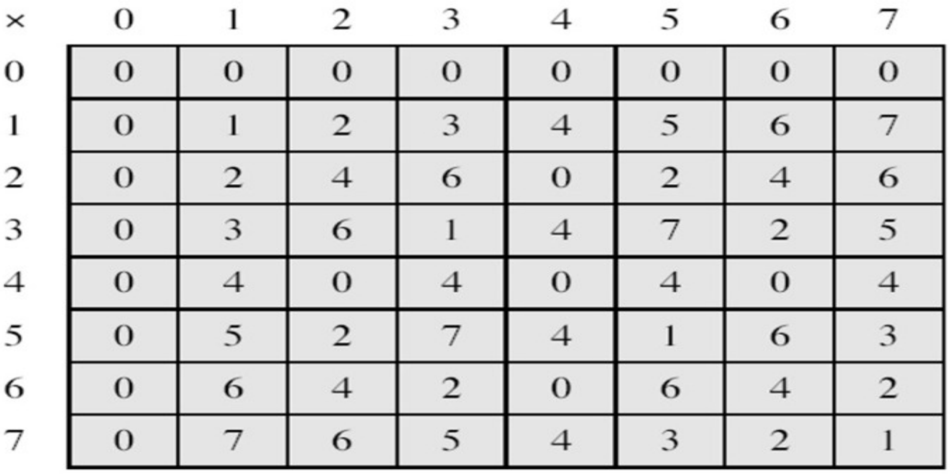
$$a^{m-1} \equiv 1 \pmod{m}, \quad \text{where } m \text{ is a prime and } m \not| a \tag{5.4}$$

If Euler's theorem is taken to be true, then this can also be seen to work because of the fact that $\phi(m) = m - 1$ for a prime number as mentioned above.

[6] Historically though, Fermat's little theorem was discovered long before Euler's Theorem.

## 5.2 Extended Euclid Algorithm

It was stated earlier that the greatest common divisor of two numbers can be found using Euclid's algorithm. This algorithm can be extended so that it not only finds the greatest common divisor but also calculates the inverse of some number $b$ modulo some other number $m$ (assuming it exists). In other words, it finds the value $b^{-1}$. For small values of $m$ it is easy enough to find the inverse. You simply construct a table as in figure 5.1 and read off the value for which the result is 1. For example, in the table it can be seen that for this particular example (multiplication modulo 8) each value is its own inverse[7] (for the values that have inverses) because $5 \times 5 \equiv 1 \pmod 8$ and $7 \times 7 \equiv 1 \pmod 8$ etc.



| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Figure 5.1: Arithmetic modulo 8

However for large numbers this approach is not practical. Luckily there is an extended form of Euclid's algorithm that will allow us to find the inverse of a number $b \bmod m$ assuming gcd$(m, b) = 1$. It is given as follows:

```
EXTENDED EUCLID($m$,$b$)
    1. $(A_1, A_2, A_3) \leftarrow (1, 0, m)$; $(B_1, B_2, B_3) \leftarrow (0, 1, b)$
    2. if $B_3 = 0$      return $A_3 =$ gcd$(m, b)$; no inverse
    3. if $B_3 = 1$      return $B_3 =$ gcd$(m, b)$; $B_2 = b^{-1} \bmod m$
    4. $Q = \lfloor \frac{A_3}{B_3} \rfloor$
```

[7] This obviously isn't always the case.

```
5. $(T_1, T_2, T_3) \leftarrow (A_1 - QB_1, A_2 - QB_2, A_3 - QB_3)$
6. $(A_1, A_2, A_3) \leftarrow (B_1, B_2, B_3)$
7. $(B_1, B_2, B_3) \leftarrow (T_1, T_2, T_3)$
8. Goto 2
```

This is seen to work because $bB_2 = 1 - mB_1$ implies that $bB_2 \equiv 1 \pmod{m}$. Therefore the value of $B_2$ is a number when multiplied by $b$ will give a value which is congruent to $1$ modulo $m$ (in other words it gives a value that when divided by $m$ will leave a remainder of $1$).

We can therefore say:

$$bB_2 = 1 - mB_1 \tag{5.5}$$

which means

$$mB_1 + bB_2 = 1 \tag{5.6}$$

In other words we are trying to find two values $B_1$ and $B_2$ that solve equation 5.6. These values will be revealed when another value $B_3$ is equal to $1$ in the above algorithm:

$$mB_1 + bB_2 = B_3 \tag{5.7}$$

In order to find this multiplicative inverse we need to keep track of $A_1$, $A_2$ and $A_3$ also. The values $T_1, T_2, T_3$ are only used for temporary storage. Looking at steps $5$ and $7$ it can be seen the $B_3 \leftarrow A_3 - QB_3$. This equation is a consequence of Euclid's algorithm and it leaves the remainder when $A_3$ is divided by $B_3$ (you are subtracting $B_3$ away from $A_3$ as many times as you can, remember $Q = \lfloor \frac{A_3}{B_3} \rfloor$).

Throughout the algorithm, the following relationships hold:

$$\begin{aligned} mT_1 + bT_2 &= T_3 \\ mA_1 + bA_2 &= A_3 \\ mB_1 + bB_2 &= B_3 \end{aligned}$$

These equations are why the initial assignments are $(1, 0, m)$ and $(0, 1, b)$. If you work them out you will get the above for $A_3$ and $B_3$. The last equation is the one we are interested in and when $B_3 = 1$ then $B_2 = b^{-1} \bmod m$.

For example to find the multiplicative inverse of $550$ modulo 1759 we have:

| $Q$ | $A_1$ | $A_2$ | $A_3$ | $B_1$ | $B_2$ | $B_3$ |
|---|---|---|---|---|---|---|
| - | 1 | 0 | 1759 | 0 | 1 | 550 |
| 3 | 0 | 1 | 550 | 1 | -3 | 109 |
| 5 | 1 | -3 | 109 | -5 | 16 | 5 |
| 21 | -5 | 16 | 5 | 106 | -339 | 4 |
| 1 | 106 | -339 | 4 | -111 | $\boxed{355}$ | 1 |

where it can be seen that 355 is the multiplicative inverse of 550 modulo 1759.

## 5.3 Discrete Logarithms

Discrete logarithms are fundamental to a number of public key algorithms as we shall see later. It is therefore imperative that we gain an understanding of them.

Considering equation 5.3 above which is Euler's theorem and generalising we have:

$$a^{\epsilon} \equiv 1 \pmod{m}, \qquad gcd(a, m) = 1 \tag{5.8}$$

From Euler's theorem we know that this holds for $\phi(m) = \epsilon$. However the least positive exponent $\epsilon$ for which this holds is known as the **order** of $a \bmod m$. If this value ends up being equal to $\phi(m)$ then it is said that $a$ is a **primitive root** of $m$. This basically says that the set of numbers $\{a, a^2, \ldots, a^{\phi(m)}\}$ are distinct modulo $m$ and relatively prime to it. If $m$ is prime then this means they form the set $\{1, 2, \ldots (m-1)\}$ in some order.

For example it is true that $7^{18} \equiv 1 \pmod{19}$ because $\phi(19) = 18$ and Euler's theorem holds. However $\phi(19)$ is not the *order* of $7 \pmod{19}$ because it is not the least positive exponent for which equation 5.8 holds. The set of values for which this equation does hold are $\epsilon = \{18, 15, 12, 9, 9, 6, 3\}$. It can be seen that the least positive value of this set is 3 and this is therefore the order of 7 $\bmod m$. It isn't a coincidence that the set is a multiple of the order as $7^{3+j} \equiv 7^3 7^j \equiv 7^j \pmod{19}$ which says that any two powers whose exponents differ by 3 are congruent modulo 19 (in other words this is a sequence with a period of 3). However, if we consider a base of 2 (rather than 7), then we can see that the only value of epsilon for which equation 5.8 now holds is phi(m). Therefore it can be seen that 2 is a primitive root of the modulus 19.

So if we have a primitive root $a$ for some number $m$ then we know that the powers of $a$ from 1 to $\phi(m)$ produce a set of distinct integers that are relatively prime to $m$. In particular if $m = p$ for some prime $p$, the set produced is {1,2,...,(p-1)} in some order. Now we know that any integer $b$ can be expressed in the form:

$$b \equiv r \pmod{p} \qquad 0 \leq r \leq (p-1)$$

Therefore given any $b$ and $a$ we can find $i$ such that:

$$b \equiv a^i \pmod{p} \qquad 0 \leq i \leq (p-1)$$

The exponent $i$ is referred to as the **index** or **discrete logarithm** of the number $b$ for the base $a \bmod p$ and is denoted by $\text{ind}_{a,p}(b)$. If we consider two values:

$$\begin{aligned} x &= a^{\text{ind}_{a,p}(x)} \bmod p \\ y &= a^{\text{ind}_{a,p}(y)} \bmod p \end{aligned}$$

then due to the rules of modular arithmetic we can say:

$$\begin{aligned} xy \bmod p &= [(x \bmod p)(y \bmod p)] \bmod p \\ a^{\text{ind}_{a,p}(xy)} \bmod p &= [(a^{\text{ind}_{a,p}(x)} \bmod p)(a^{\text{ind}_{a,p}(y)} \bmod p)] \bmod p \\ &= a^{\text{ind}_{a,p}(x)+\text{ind}_{a,p}(y)} \bmod p \end{aligned}$$

Any positive integer $z$ can be expressed as $z = q+k\phi(m)$ therefore by Euler's theorem:

$$a^z \equiv a^q \pmod{m} \qquad \text{if} \quad z \equiv q \pmod{\phi(m)}$$

Applying this to the above:

$$\text{ind}_{a,p}(xy) \equiv [\text{ind}_{a,p}(x) + \text{ind}_{a,p}(y)] \pmod{\phi(p)}.$$

Generalising we have:

$$\text{ind}_{a,p}(y^r) \equiv [r \times \text{ind}_{a,p}(y)] \pmod{\phi(p)}$$

As can be seen there is a distinct analogy here between true logarithms and indices. For this reason, the latter are often referred to as discrete logarithms.