THE FERMAT-EULER THEOREM AND ITS APPLICATION TO PUBLIC KEY CRYPTOGRAPHY

YUTONG LI

Abstract. This paper discusses definitions in Number Theory such as GCD, divisor, coprimeness, and modular arithmetic and proves elementary results such as the Euclidean algorithm, the Chinese Remainder Theorem, and the Fermat-Euler Theorem. The Euclidean Algorithm gives an efficient method for computing the GCD of two integers and writing it as a linear combination of those integers. The Chinese Remainder Theorem states that, under certain coprimeness conditions, if one knows the remainders of Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers. Finally, the Fermat-Euler Theorem says that for every integer a coprime to an integer n, $a^{\text{number of integers coprime to } n}$ has remainder 1 when dividing it by n. This paper culminates with an application of these results to Public Key Cryptography.

Contents

1. Introduction

Number Theory is a branch of pure mathematics devoted to the study of integers. The origin of Number Theory as a branch dates all the way back to the B.Cs, specifically to the lifetime of one Euclid. [1] Around 300 B.C, Euclid unleashed his classic Elements book series; a series of ten books spanning a range of topics from integers, to line segments and surface areas. An extraordinary mathematician, Euclid of Alexandria, also known as the "Father of Geometry," put forth one of the oldest algorithms recorded, which will be studied in this paper. [2]

In §2, we will review the basic definitions such as equivalence relation, group, and ring. They serve as a foundation of our studies in Number Theory. In §3, we will study the basic lemmas in Number Theory and state and prove the Euclid's Algorithm, which gives us a method to compute the greatest common divisor of two integers a and b. In §4-5, we will define modular arithmetic, then look at rings and groups that are related to it. In §6, we will use all the concepts from previous sections to prove the Fermat-Euler's Theorem. This tells us facts about the number of positive integers less than or equal to n and coprime to n. Finally, in §7, we will examine an application of Number Theory in Cryptography. Using the fact that large primes are hard to factorize, we see a method that allows us to transmit messages using public key.

2. Some Basic Algebraic Definitions

In this section, we review the basic definitions that will be used in this paper. We start from equivalence relation and equivalence class, which is widely used in modular arithmetic. We then look at group and ring, which describes the quality of a set. In the end, we review the definition of homomorphism, which defines a quality of the laws of composition.

Definition 2.1. Let X be a nonempty set. A *relation* R on X is a subset of $X \times X$. The statement $(x, y) \in R$ is read as 'x is related to y by the relation R,' and is often denoted $x \sim y$.

A relation is

- *reflexive* if $x \sim x$ for all $x \in X$.
- *symmetric* if $y \sim x$ whenever $x \sim y$.
- *transitive* if $x \sim z$ whenever $x \sim y$ and $y \sim z$.
- an *equivalence relation* if it is reflexive, symmetric and transitive.

For example, the relation "=" on any set is an equivalence relation because it is reflexive, symmetric, and transitive. The relation "<" is not an equivalence relation because it is not symmetric. In other words, when $y > x$ is true, $x > y$ is not necessarily true.

Definition 2.2. Let R be an equivalence relation on a set X. An *equivalence class* of an element $x \in X$ is the set

$$[x] := \{y \in X \mid (x, y) \in R\}.$$

Remark 2.3. For an equivalence relation R on a nonempty set X, with $x, y \in X$, we have $x \sim y$ if and only if $[x] = [y]$.

Definition 2.4. A *group* is a set G together with a law of composition, i.e. a map $G \times G \to G$, that has the following properties:

- The law of composition is associative: $(ab)c = a(bc)$ for all a, b, c in G.
- G contains an identity element 1, such that $1a = a$ and $a1 = a$ for all $a \in G$.
- Every element a of G has an inverse, and element b such that $ab = 1$ and $ba = 1$.

Definition 2.5. An *abelian group* is a group whose law of composition is commutative.

Example 2.6. Here are some examples of what a group looks like.

(1) The set $\mathbb{Q} \setminus \{0\}$ is an abelian group under $\times$, which is often denoted as $\mathbb{Q}^*$.
(2) Any vector space forms an abelian group under $+$.
(3) The set of invertible $n \times n$ matrices, the general linear group, forms a group under matrix multiplication. It is not abelian unless $n = 1$.

Definition 2.7. A *ring* R is a set with two laws of composition $+$ and $\times$, called addition and multiplication respectively, that has the following properties:

- Under the law of composition $+$, R is an abelian group that we denote by $R+$; its identity is denoted by 0.
- Under the law of multiplication $\times$, R is associative, and has an identity denoted by 1.
- distributive law: For all a, b, and c in $R, (a + b)c = ac + bc$.

Example 2.8. Here are some examples of what a ring looks like.

(1) The set of integers $\mathbb{Z}$ is a ring.
(2) A polynomial in x with coefficients expressed as
$$a_n x^n + \cdots + a_1 x + a_0$$
with $a_i \in \mathbb{R}$ is a ring.

Definition 2.9. Let G and G' be groups, written with multiplicative notation. A *homomorphism* $\psi : G \to G'$ is a map such that for all a and b in G,
$$\psi(ab) = \psi(a)\psi(b).$$
Intuitively, a homomorphism is a map that is compatible with the laws of composition in the two groups, and it provides a way to relate different groups.

3. Euclid's Algorithm

In this section, we study the greatest common divisor of integers. First, we give a rigorous definition of the concept and study some basic lemmas derived from the unique factorization of integers into prime numbers. Then, we look at Euclid's Algorithm, which gives us a generalized method to find the greatest common divisor of two integers.

Definition 3.1. If a and b are integers, we say that a *divides* b, or $a \mid b$, if there is a positive integer c such that $ac = b$.

Definition 3.2. If $a, b \in \mathbb{Z}$, then the *greatest common divisor* (GCD) of a and b, written (a, b), is the greatest positive integer d such that $d \mid a$ and $d \mid b$.

Definition 3.3. We say that a and b are *coprime* if there does not exist a prime p dividing both a and b. More generally, we say that integers $a_1, ..., a_k$ are *pairwise coprime* if no prime divides more than one of the a_i.

We now state some basic facts about greatest common divisors and coprime integers. All of these facts follow from the definitions above and unique factorization of integers into prime numbers.

Lemma 3.4. *Suppose that a, b are positive and that $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where the p_i are distinct primes. Then $(a, b) = p_1^{min(\alpha_1,\beta_1)} \cdots p_k^{min(\alpha_k,\beta_k)}$*

Lemma 3.5. *Suppose that a, b are coprime and that $b \mid ax$. Then $b \mid x$.*

Lemma 3.6. *Suppose that $q_1, \cdots, q_k$ are pairwise coprime. Then $q_1 \cdots q_k$ divides x if and only if q_i divides x for $i = 1, \cdots, k$.*

Lemma 3.7. *Suppose that a and b are both coprime to q. Then so is ab.*

We now investigate the Euclid's Algorithm. It gives us an efficient method for computing GCD and writing the GCD of integers a and b as an integral linear combination of themselves.

Theorem 3.8. (Euclid's Algorithm) *Suppose that a, b are integers. Then there are integers m, n such that $am + bn = (a, b)$.*

Proof. We show that there are integers n, m such that $am + bn = (a, b)$. Without loss of generality, we may assume $a \geq b \geq 0$ (Switch a by $-a$ and b by $-b$ and the role of a, b if necessary). Perform the Euclid's algorithm on a and b :

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\vdots$$

$$r_k = q_{k+2} r_{k+1} + 0$$

where the quotients q_i are nonnegative integers and the remainders r_1 are nonnegative integers and satisfy $r_{i+1} < r_i$. This last property guarantees that the algorithm does terminate.

Now, we want to show that $(a, b) = r_{k+1}$.

First, we show that $r_{k+1} \mid (a, b)$ by showing $r_{k+1} \mid r_i$ for all i by induction.

Base Case: For the Base Case, let $i = k$. By the last equation of the Euclid's Algorithm, $r_k = q_{k+2} r_{k+1}$. So, we have $r_{k+1} \mid r_k$.

Inductive Step: Assume by the inductive hypothesis that $r_{k+1} \mid r_i$ for all $j \geq i$ where $i \in \{2, 3, \cdots, \}$ Now we want to show that $r_{k+1} \mid r_{i-1}$. Notice that for $i \in \{1, \cdots, k\}$ we have the general formula $r_i = q_{i+2} \cdot r_{i+1} + r_{i+2}$. So,

$$\begin{aligned} r_{i-1} &= q_{i+1} r_i + r_{i+1} \\ &= q_{i+1} q_{i+2} r_{i+1} + r_{i+1} \\ &= (q_{i+1} q_{i+2} + 1) r_{i+1} \end{aligned}$$

So, $r_{i+1} \mid r_{i-1}$.

Thus, by induction, $r_{k+1} \mid r_i$ for all $i \in \{1, 2, \cdots, k\}$. Since $b = q_2 r_1 + r_2$, $r_{k+1} \mid b$ by defnition. Similarly, $r_{k+1} \mid a$. So, $r_{k+1} \mid (a, b)$.

Now, let $d = (a, b)$. Then, $d \mid a$ and $d \mid b$ by definition.

Then, similar to the process above, we have $(a, b) \mid r_{k+1}$.

Since we have also have $r_{k+1} \mid (a, b)$, we know $(a, b) = r_{k+1}$.

So, we substitute $(a, b) = r_{k+1}$ in the equation and work from the bottom up to get.

$$\begin{aligned}(a, b) &= r_{k+1} \\ &= r_{k-1} - q_{k+1} r_k \\ &= r_{k-1} - q_{k+1}(r_{k-2} - q_k r_{k-1}) \\ &\vdots \\ &= ma + nb\end{aligned}$$

for some integers m, n. □

4. Modular Arithmetic and The Ring $\mathbb{Z}/q\mathbb{Z}$

In this section, we will define modulo of two integers and the equivalence class of modulo. We will then verify that modulo arithmetic, which is the computation done to the equivalence classes, is well-defined.

First, we need to introduce some definitions.

Definition 4.1. Let $q \geq 1$ be an integer. We write $a \equiv b (\text{mod } q)$ if and only if q divides $a - b$. This statement is read as '*a is equivalent to b modulo q.*'

For example, $357 \equiv 5 (\text{mod } 11)$ since $357 - 5 = 352 = 11 \times 32$.

Remark 4.2. The relation $\sim$ on the set $\mathbb{Z}$, defined by $x \sim y$ if and only if $x \equiv y (\text{mod } q)$, is easily seen to be an equivalence relation. So, the equivalence for $x \in \mathbb{Z}$ is the set $\{x + kq \mid q \in \mathbb{Z}\}$. We denote this equivalence class by $x + q\mathbb{Z}$. Now, we will conduct addition and multiplication on the equivalence classes. This is called modular arithmetic.

A complete set of distinct equivalence classes is $\{\overline{0}, \overline{1}, \cdots, \overline{q-1}\}$. After $\overline{q-1}$ the set starts to repeat because $\overline{q} = 0 + q = \overline{0}, \overline{q+1} = 1 + q = \overline{1}, \cdots$. For integers less than 0 we also have $\overline{-1} = (q-1) + q = \overline{q-1}, \overline{-2} = (q-2) + q = \overline{q-2}, \cdots$. We write $\mathbb{Z}/q\mathbb{Z}$ for this set of equivalence classes.

Example 4.3. $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ or more formally $\{\overline{0} + 4\mathbb{Z}, \overline{1} + 4\mathbb{Z}, \overline{2} + 4\mathbb{Z}, \overline{3} + 4\mathbb{Z}\}$. For every integer, we can find its equivalence class using the definition. For example, $9 = 1 (\text{mod } 4)$, so 9 is in the equivalence class of $\overline{1}$ or $\{\overline{1} + 4\mathbb{Z}\}$.

We want to show that this set is a ring. So, according to Definition 2.7, we need to show that this set is closed under addition and multiplication. (This also implies that this set is closed under subtraction, defined by additive inverse.)

Lemma 4.4. *Suppose that $x \equiv a (\text{mod } q)$ and that $y \equiv b (\text{mod } q)$. Then $x + y \equiv a + b (\text{mod } q)$.*

Proof. Suppose that $x - a = k_1 q$ and $y - b = k_2 q$ for integers k_1, k_2. Then we have $(x + y) - (a + b) = (x - a) + (y - b) = k_1 q + k_2 q = (k_1 + k_2) q$. So, $(x + y) - (a + b)$ divides q. □

This tells us that this set is closed under addition. So, we have a well-defined addition given by

$$(x + q\mathbb{Z}) + (y + q\mathbb{Z}) = (x + y) + q\mathbb{Z}$$

Lemma 4.5. *Suppose that $x \equiv a(mod\ q)$ and that $y \equiv b(mod\ q)$. Then $xy \equiv ab(mod\ q)$.*

Proof. Suppose that $x - a = k_1 q$ and $y - b = k_2 q$ for integers k_1, k_2. Then we have $xy - ab = xy - xb + xb - ab = x(y-b) + b(x-a) = xk_2 q + bk_1 q = q(xk_2 + bk_1)$. So, $xy - ab$ divides q. □

This tells us that this set is closed under multiplication. So, we have a well-defined multiplication given by

$$(x + q\mathbb{Z})(y + q\mathbb{Z}) = xy + q\mathbb{Z}$$

Thus, modular arithmetic is closed under addition and multiplication, and the set $\mathbb{Z}/q\mathbb{Z}$ is a ring.

Next, we verify cancellation for module arithmetic.

Corollary 4.6. *Let $a, b, c, q \in \mathbb{Z}$ with $q \geq 0$. Suppose that $ac \equiv bc(mod\ q)$, and that q is coprime to c. Then $a \equiv b(mod\ q)$.*

Proof. We know that $ac - bc$ divides q by definition. So, $(a-b)c$ divides q. Since q is coprime to c, by Lemma 3.5, $(a-b)$ divides q. So, $a \equiv b(\text{mod } q)$. □

5. The Multiplicative Group

Now, we define multiplicative group, a concept that is build on top of modulo arithmetic. Then, we will study an important bijective map that will lead to the Chinese Remainder Theorem.

Definition 5.1. We define the *multiplicative group of residues mod q* $(\mathbb{Z}/q\mathbb{Z})^\times$ as

$$(\mathbb{Z}/q\mathbb{Z})^\times := \{x + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z} : (x, q) = 1\} = \{\overline{x} : (x, q) = 1\}.$$

For example,

$$(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\}, (\mathbb{Z}/7\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}, (\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}.$$

Lemma 5.2. *Let $q \in \mathbb{Q}$ with $q \geq 0$. $(\mathbb{Z}/q\mathbb{Z})^\times$ is a group under multiplication.*

Proof. We know that there is an identity element $1 + q\mathbb{Z}$.

First, we want to show that $(\mathbb{Z}/q\mathbb{Z})^\times$ is closed under multiplication. By Lemma 3.7, we know that if $\overline{x} \in (\mathbb{Z}/q\mathbb{Z})^\times$ and $\overline{y} \in (\mathbb{Z}/q\mathbb{Z})^\times$, then $\overline{xy}$ is coprime to q. Thus, $\overline{xy} \in (\mathbb{Z}/q\mathbb{Z})^\times$. Thus, $(\mathbb{Z}/q\mathbb{Z})^\times$ is closed under multiplication.

Next, we also need to show that multiplicative inverse exists. For any integer c such that $c + q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z})^\times$. Then by Theorem 3.8 there are integers m, n such that $cm + qn = 1$, so $cm \equiv 1(\text{mod } q)$. Since $(\mathbb{Z}/q\mathbb{Z})^\times$ is closed under multiplication, m is coprime to q. Hence, $m + q\mathbb{Z}$ is inverse to c. □

Theorem 5.3. (The Chinese Remainder Theorem) *Suppose that $q_1, q_2, \cdots, q_k$ are pairwise coprime positive integers. Then the map*

$$\psi : \mathbb{Z}/q_1 \cdots q_k\mathbb{Z} \to \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$$

given by

$$\psi(x + q_1 \cdots q_k\mathbb{Z}) = (x + q_1\mathbb{Z}, \cdots, x + q_k\mathbb{Z})$$

is a bijection.

Proof. By Lemma 3.6, if $x \equiv y (\text{mod } q_1 \cdots q_k)$, then $x \equiv y (\text{mod } q_i)$ for all $i = 1, 2, \cdots, k$. This proves that the map ϕ is well-defined.

Notice that the domain and range of ψ have the same cardinality $q_1 \cdots q_k$. Thus, to show that ψ is a bijection, it suffices to show that it is an injection.

We prove by contradiction. Assume that ψ is not an injection. Then there is some distinct x and y such that $\psi(x) = \psi(y)$. Then, $x \equiv y (\text{mod } q_i)$ for all i. Then $q_i \mid (y - x)$ for all i. By Lemma 3.6, since all q_i are pairwise coprime, $q_1 q_2 \cdots q_k \mid (y - x)$. So, $x \equiv y (\text{mod } q_1 q_2 \cdots q_k)$. This means that x and y are in a equivalence relation. Thus, our assumption is wrong and this map is an injection, and hence a bijection. □

Remark 5.4. When we say that x is unique, we mean that x' also satisfies this condition if and only if $x' \equiv x (\text{mod } q_1 \cdots q_k)$. For example, there is an integer satisfying $x \equiv 3 (\text{mod } 7)$ and $x \equiv 2 (\text{mod } 5)$, namely $x = 17$, and this x is unique (mod 35). For example, $x' = 52$ also satisfies this condition, but $52 \equiv 17 (\text{mod } 35)$.

Remark 5.5. Notice that this result is not true if q_i are not coprime. For example, there is no x such that $x \equiv 1 (\text{mod } 8)$ and $x \equiv 3 (\text{mod } 16)$.

We can interpret Theorem 5.3 as the follows.

Suppose that $q_1, q_2, \cdots, q_k$ are pairwise coprime positive integers. Suppose that $a_1, a_2, \cdots, a_k$ are integers. Then there is an integer x such that $x \equiv a_i (\text{mod } q_i)$ for $i = 1, 2, \cdots, k$. Moreover, x is unique (mod $q_1 \cdots q_k$).

Here's a way to construct an x explicitly.

For each i, write

$$Q_1 := \frac{q_1 q_2 \cdots q_k}{q_i} = q_1 q_2 \cdots q_{i-1} q_{i+1} q_k.$$

Since the q_i are pairwise coprime, lemma 2.7 tells us that Q_i is also coprime to q_i. Use the Euclidian algorithm to find m_i such that m_i is an integer inverse to Q_i in $(\mathbb{Z}/q_i\mathbb{Z})^\times$: thus $m_i Q_i \equiv 1 (\text{mod } q_i)$.

Finally, set

$$x = a_1 m_1 Q_1 + \cdots + a_k m_k Q_k.$$

Notice that all of the Q_i except for Q_1 are divisible by q_1. Therefore,

$$x \equiv a_i m_i Q_i \equiv a_i (\text{mod } q_i).$$

We will prove the Chinese Remainder Theorem by proving a stronger version of it, given by the theorem below.

Now we provide two examples below using the method above.

Example 5.6. We find an integer x such that $x \equiv 5 (\text{mod } 11)$ and $x \equiv 11 (\text{mod } 31)$.

In this problem, we have $q_1 = 11, q_2 = 31$. So,

$$Q_1 = \frac{11 \cdot 31}{11} = 31$$
$$Q_2 = \frac{11 \cdot 31}{31} = 11$$

Now, we want to find m_1 such that m_1 is an inverse to 31 mod 11. Since $31 = 11 \cdot 2 + 9$, we are looking for the inverse to 9 mod 11. We use Theorem 3.8 to get:

$$11 = 9 \cdot 1 + 2$$
$$9 = 2 \cdot 4 + 1$$

$$4 = 1 \cdot 4 + 0$$

So, we rewrite this equation from the bottom up to get

$$\begin{aligned} 1 &= 9 - 2 \cdot 4 \\ &= 9 - (11 - 9) \cdot 4 \\ &= 5 \cdot 9 - 4 \cdot 11 \end{aligned}$$

So, $m_1 = 5$. We use similar method to find $m_2 = -14$. Thus,

$$x = 5 \cdot 5 \cdot 31 + 11 \cdot (-14) \cdot 11 = -919.$$

To make it positive, we add multiples of $11 \cdot 31$ to get $-919 + 3 \cdot 11 \cdot 31 = 104$.

Example 5.7. We find a positive integer x such that $x \equiv 3 (\text{mod } 4)$, $2x \equiv 5 (\text{mod } 9)$, $7x \equiv 1 (\text{mod } 11)$.

Notice that the difference between Example 5.6 and Example 5.7 is that the residues are not given in terms of x, but multiples of x. So, we need to convert the conditions into residues in terms of x to use our methods to compute x using the Chinese Remainder Theorem.

First, we look at the part where $2x \equiv 5 (\text{mod } 9)$. Let $x \equiv a (\text{mod } 9)$. Then $x \equiv 2a (\text{mod } 9)$. Since 5 is an odd number, we know that $2a$ must be larger than 9. This leaves us the numbers $5, 6, 7, 8$. We calculate the result for all four of these numbers: $2 \cdot 5 \equiv 1 (\text{mod } 9), 2 \cdot 6 \equiv 3 (\text{mod } 9), 2 \cdot 7 \equiv 5 (\text{mod } 9), 2 \cdot 8 \equiv 7 (\text{mod } 9)$. Notice that 2 is coprime to 9, so there is only one possible solution, which is consistent with the result we have. So, we know that $x \equiv 7 (\text{mod } 9)$.

Similarly, we can convert $7x \equiv 1 (\text{mod } 11)$ into $x \equiv 8 (\text{mod } 11)$. Now, we use the Chinese Remainder Theorem to get

$$Q_1 = 9 \cdot 11 = 99, Q_2 = 4 \cdot 11 = 44, Q_3 = 4 \cdot 9 = 36.$$

We can also find the inverse of them using the Euclidean algorithm.

$$m_1 = 3, m_2 = 8, m_3 = 4.$$

So, $x = 3 \cdot 3 \cdot 99 + 7 \cdot 8 \cdot 44 + 8 \cdot 4 \cdot 36 = 4507$

We subtract multiples of $4 \cdot 9 \cdot 11$ to get

$$4507 - (4 \cdot 9 \cdot 11) \cdot 11 = 151.$$

Theorem 5.8. (Fermat's Little Theorem) *Let p be a prime number. Suppose that a is not a multiple of p. Then $a^{p-1} \equiv 1 (\text{mod } p)$.*

Proof. Consider the set of numbers $\{1, 2, \cdots, p-1\}$. These numbers are mutually incongruent to p. Now, consider the set of numbers $\{a, 2a, \cdots, (p-1)a\}$. We claim that the second set of numbers are also incongruent to p. We prove by contradiction. Assume that there are some distinct $m, n \in \{1, 2, \cdots, p-1\}$ such that $ma \equiv na (\text{mod } p)$. Since a is coprime to $p, m \equiv n (\text{mod } p)$ by Corollary 4.6. This is a contradiction. Thus, our assumption is wrong and $a, 2a, \cdots, (p-1)a$ are incongruent to p. Thus, they much be $\overline{1}, \overline{2}, \cdots, \overline{p-1}$ in some order. Thus, the product of $\{1, 2, \cdots, p-1\}$ is equal to the product $\{a, 2a, \cdots, (p-1)a\} (\text{mod } q)$ because they are in essence the same numbers. Thus,

$$(p-1)! \equiv a \cdot 2a \cdots (p-1)a \equiv a^{p-1}(p-1)! (\text{mod } p).$$

By Corollary 4.6, we can divide both sides by $(p-1)!$ to get

$$1 \equiv a^{p-1} (\text{mod } p).$$

□

Remark 5.9. This theorem is not true for the other way around. This is to say that if $a^{p-1} \equiv 1 (\text{mod } p)$, it is not necessarily true that p is prime. For example, for $p = 341, a^{340} \equiv 1 (\text{mod } 341)$, but $341 = 11 \cdot 31$.

6. Fermat-Euler's Theorem

In this section, we will defined a new function, Euler's ϕ-Function, which gives the number of positive integers less than or equal to n and coprime to n. We will then study the relationship between the $\phi-$Function and modular arithmetic.

Definition 6.1. (Euler's ϕ-Function) We define $\phi(n)$, the *Euler's ϕ-Function,* to be the number of positive integers less than or equal to n and coprime to n.

For example,

$$\phi(12) = 4(1, 5, 7, 11), \phi(13) = 12(1, 2, \cdots, 12).$$

Lemma 6.2. *We have $\#(\mathbb{Z}/q\mathbb{Z})^\times = \phi(q)$.*

Proof. Every element of $\mathbb{Z}/q\mathbb{Z}$ is congruent to precisely one element of $\{1, 2, \cdots, q\}$. The elements of $(\mathbb{Z}/q\mathbb{Z})^\times$ correspond to the elements of this set which are coprime to q. Since the two sets have a bijection map, they also have the same cardinality. □

Proposition 6.3. *The ϕ-function is multiplicative, that is to say for coprime integers m, n, $\phi(mn) = \phi(m)\phi(n)$.*

Proof. This is given by the definition of homomorphism. Simply apply Theorem 5.3 with $m = q_1$ and $n = q_2$. □

Corollary 6.4. *Suppose that n is a positive integer and that its prime factorisation is $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Then*

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1) = n \prod_{p|n} (1 - \frac{1}{p}).$$

Proof. This follows immediately from Proposition 6.3. Notice that $\phi(p^a) = p^{a-1}(p-1)$, this being the number of integers $\leq p^a$ which are not multiples of p. □

Theorem 6.5. (Fermat-Euler's Theorem) *Suppose that q is a positive integer, and that a is coprime to q. Then $a^{\phi(q)} \equiv 1 (\text{mod } q)$.*

Proof. Let $x_1, \cdots, x_{\phi(q)}$ be a complete set of residues coprime to q. This means two things. First, they are mutually incongruent modulo q, so for any x_i and x_j, $x_i \not\equiv x_j (\text{mod } q)$. Second, every x_i is coprime to q. Therefore, by definition, the $x_i + q\mathbb{Z}$ are precisely the elements of $(\mathbb{Z}/q\mathbb{Z})^\times$.

Now, we consider the integers $ax_1, \cdots, ax_{\phi(q)}$. Recall that a is coprime to q. By Lemma 3.7, $ax_1, \cdots, ax_{\phi(q)}$ are also coprime to q. We also want to show that they are mutually incongruent modulo q. We prove by contradiction. Assume that there is some x_i and x_j such that $ax_i \equiv ax_j (\text{mod } q)$. Then by Corollary 4.6, $x_i \equiv x_j (\text{mod } q)$. This contradicts the fact that all x_i are mutually incongruent modulo q. Thus, our assumption is wrong and $ax_1, \cdots, ax_{\phi(q)}$ are also incongruent modulo q. Thus, $ax_1, \cdots, ax_{\phi(q)}$ is also a complete set of residues coprime to q.

This tells us the product of all x_i and all ax_1 are in fact the same. Thus, we have

$$\prod_{i=1}^{\phi(q)} x_i \equiv \prod_{i=1}^{\phi(q)} (ax_i) \equiv a^{\phi(q)} \prod_{i=1}^{\phi(q)} x_i (\text{mod } q).$$

Notice that $\prod_{i=1}^{\phi(q)} x_i$ is coprime to q. By Corollary 4.6, we can divide both sides bby $\prod_{i=1}^{\phi(q)} x_i$ to get

$$1 \equiv a^{\phi(q)} (\text{mod } q).$$

□

7. Applications on Public Key Cryptography

In this section, we are going to see an application of the Euclidean algorithm and Fermat-Euler's Theorem in cryptography.

7.1. **Introduction.** The RSA Public Key Cryptosystem, invented by Rivest, Shamir and Adleman in 1977 allows messages to be sent securely without the need to exchange a "key" secretly.

7.2. **Set-Up.** Let us suppose that we have two people named Alice and Bob, and that Alice wants to send a message to Bob. A malicious eavesdropper will appear later by the name of Eve.

Bob chooses two large primes p and q (typically with hundreds of digits) and an integer e such that $(e, \phi(n)) = 1$, where $n = pq$. So, $\phi(n) = (p-1)(q-1)$. This is equivalent to $(e, p-1) = (e, q-1) = 1$. He then publishes the product n and e, but keeps the numbers p and q secretly.

7.3. **Decryption.** Assume that Alice wants to transmit a number M. Alice computes $M^e (\text{mod } n)$, which is an integer between 0 and $n-1$.

Now Bob has the encrypted method $M^e (\text{mod } n)$. Since Bob knows p and q, he can compute $\phi(n) = (p-1)(q-1)$. Since e is coprime to $\phi(n)$, he can use the Euclidean algorithm to find d such that $de \equiv 1 (\text{mod } \phi(n))$. So, there is some integer k such that $de = k\phi(n) + 1$. By Fermat-Euler's Theorem, we know that

$$M^{de-1} = M^{k\phi(n)} \equiv 1 (\text{mod } n).$$

So,

$$(M^e)^d = (M^{\phi(n)})^k M \equiv M (\text{mod } n).$$

Since the unencrypted message M is known to be a natural number $< n$, this allows it to be recovered uniquely.

There is an issue here if it happens that M is not coprime to n. However, since p and q are extremely large primes, this is exceptionally unlikely to happen.

7.4. **Security.** The decryption method we presented above depends on having the number d. To calculate this, we needed $\phi(n)$. Eve, the eavesdropper, could read the message if she had $\phi(n)$.

However, in order to obtain $\phi(n)$, we need to factorize $n = pq$, which is widely believed to be hard.

7.5. **Example.** For the sake of calculation, we will pick two prime numbers that are significantly less than the actual ones used in the real world. Let

$$p = 13, q = 17.$$

So, $n = 13 \cdot 17 = 221, \phi(n) = (13-1)(17-1) = 192$. Let

$$e = 5.$$

We then publish $n = 221$ and $e = 5$.

Now, assume we receive an encrypted number from Alice 15. Using the Euclidean algorithm, we have

$$\begin{aligned} 192 &= 38 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

So,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (192 - 38 \cdot 5) \\ &= 77 \cdot 5 - 2 \cdot 192 \end{aligned}$$

So, we have $d = 77$. Now, we can find the encrypted number

$$M = (15)^{77} (\text{mod } 221) = 19,$$

which is our encrypted number.

References

[1] John J. Watkins. Number Theory: A Historical Approach.
[2] Jesus Najera. Number Theory — History Overview. https://towardsdatascience.com/number-theory-history-overview-8cd0c40d0f01
[3] Ben Green. Oxford Number Theory Lecture Notes
[4] Michael Artin. Algebra (2010). Pearson. Second Edition. ISBN 0132413779.
[5] Richard Earl. Groups and Group Actions. Hilary and Trinity Terms 2014.
[6] Oxford Number Theory Exercise Sheet 2020. ben.green@maths.ox.ac.uk