Elliptic Curve Cryptography

Nandana Madhukara

San Diego Math Circle

May 28, 2024

Euler's Theorem

A Counting Problem

Question

How many positive integers less than n are relatively prime to n?

A Counting Problem

Question

How many positive integers less than n are relatively prime to n?

This is hard! We call this number $\phi(n)$ where ϕ is called the Euler Totient Function.

A Counting Problem

Question

How many positive integers less than n are relatively prime to n?

This is hard! We call this number $\phi(n)$ where ϕ is called the Euler Totient Function.

Question

What if n is

1. *2, 4, or 8*
2. *3, 9, or 27*
3. *5, 25?*

Any patterns?

A pattern?

Solution

We can see the pattern is that $\phi(p^k) = p^k - p^{k-1}$ *for a prime p. Can we prove this?*

A pattern?

Solution

We can see the pattern is that $\phi(p^k) = p^k - p^{k-1}$ for a prime p. Can we prove this?

Proof.

1. Let $m \leq p^k$ be any positive integer.
2. Since p is prime, the only possible values for $\gcd(m, p^k)$ are $1, p, ..., p^k$.
3. $\gcd(m, p^k) > 1 \implies m \in \{p, 2p, ..., p^{k-1}p = p^k\}$.
4. There are p^{k-1} numbers in this set which are the numbers that are not relatively prime with p^k
5. Therefore, total is $p^k - p^{k-1}$

■

More patterns

Question

What if n is 3, 4, or 12? What about if n is 3, 6, or 18? Any patterns?

More patterns

Question

What if n is 3, 4, or 12? What about if n is 3, 6, or 18? Any patterns?

Solution

We can see the pattern is $\phi(mn) = \phi(m)\phi(n)$ *only if* $\gcd(m, n) = 1$.

More patterns

Question

What if n is 3, 4, or 12? What about if n is 3, 6, or 18? Any patterns?

Solution

We can see the pattern is $\phi(mn) = \phi(m)\phi(n)$ *only if* $\gcd(m, n) = 1$.

Proof.

It's too complicated :) It uses the Chinese Remainder Therorem if you want to think about it. ∎

A formula for $\phi(n)$

Question

Using these properties, can you find a formula for $\phi(n)$*?*

A formula for $\phi(n)$

Question

Using these properties, can you find a formula for $\phi(n)$?

Solution

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

A formula for $\phi(n)$

Question

Using these properties, can you find a formula for $\phi(n)$?

Solution

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Proof.

We know that

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$$

Now we can see the formula works by the multiplicative property. ∎

Euler's Theorem

Theorem (Euler)

If $\gcd(a, n) = 1$, *then*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Euler's Theorem

Theorem (Euler)

If $\gcd(a, n) = 1$, *then*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof.

1. Let $R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$ be the integers less than n relatively prime to n.
2. $aR = \{ax_1, ax_2, \ldots, ax_{\phi(n)}\} \equiv R \pmod{n}$
3. $$\prod_{i=1}^{\phi(n)} x_i \equiv \prod_{i=1}^{\phi(n)} ax_i \equiv a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

∎

RSA Cryptosystem

The Basics of Cryptography

Remark (Kerkoff)

When assessing the security of a cryptosystem, one must always assume that the enemy knows the method being used.

The Basics of Cryptography

Remark (Kerkoff)

When assessing the security of a cryptosystem, one must always assume that the enemy knows the method being used.

Definition

1. *Symmetric Key Encryption* is when both the encryption and decryption key must be kept a secret between Alice and Bob.
2. *Asymmetric Key Encryption* is when the encryption key is made public but the decryption key is kept a secret by Bob.

The RSA Cryptosystem

RSA

1. Bob chooses two distinct primes p and q and computes $n = pq$.
2. Bob chooses e such that $\gcd(e, (p-1)(q-1)) = 1$.
3. Bob computes the d such that $de \equiv 1 \pmod{(p-1)(q-1)}$. (Bob can use the Euclidean Algorithm for speed).
4. Bob makes n and e public while keeping p, q, and d private.
5. Alice encrypts her message $0 \leq m < n$ as $c \equiv m^e \pmod{n}$ where c is the ciphertext she sends to Bob. (If m is not in range, she breaks it into smaller blocks).
6. Bob recovers the message by computing $c^d \equiv m \pmod{n}$

Why does this work?

Question

Why can Bob recover the message so easily?

Why does this work?

Question

Why can Bob recover the message so easily?

Solution

First we claim that $c^d \equiv m \pmod{p}$ *and* $(mod\ q)$

Why does this work?

Question

Why can Bob recover the message so easily?

Solution

First we claim that $c^d \equiv m \pmod{p}$ *and* $(mod\ q)$

Proof.

1. WLOG we only consider modulo p.
2. $c^d = (m^e)^d = m^{de}$.
3. $$m^{de} = m^{1+k\phi(n)} = m \cdot m^{k\phi(p)\phi(q)} = m \cdot \left(m^{\phi(p)}\right)^{k\phi(q)}.$$

∎

Why does this work? (cont.)

Proof.

1. If $\gcd(m, p) = 1$, by Euler's Theorem

$$m \cdot (m^{\phi(p)})^{k\phi(q)} \equiv m \cdot 1^{k\phi(q)} \equiv m \pmod{p}.$$

2. If $\gcd(m, p) \neq 1$, since p is prime, we have $m = m'p$, so

$$m \cdot (m^{\phi(p)})^{k\phi(q)} \equiv 0 \equiv m \pmod{p}$$

completing our proof of our claim. ∎

Why does this work? (cont.)

Proof.

1. If $\gcd(m, p) = 1$, by Euler's Theorem

$$m \cdot (m^{\phi(p)})^{k\phi(q)} \equiv m \cdot 1^{k\phi(q)} \equiv m \pmod{p}.$$

2. If $\gcd(m, p) \neq 1$, since p is prime, we have $m = m'p$, so

$$m \cdot (m^{\phi(p)})^{k\phi(q)} \equiv 0 \equiv m \pmod{p}$$

completing our proof of our claim. ∎

Solution

Now our claim tells us

$$c^d = k_1 p + m, \; c^d = k_2 q + m$$

Why does this work? (cont.)

Solution

Multiplying the first equation by q and the second by p and adding the two, we get

$$(p+q)c^d = (k_1 + k_2)pq + (p+q)m.$$

Another way of writing this is

$$(p+q)c^d \equiv (p+q)m \pmod{n}.$$

Now $p+q$ cannot be 1, p, q or n so this means that

$$c^d \equiv m \pmod{n}.$$

Try to hack this

Remark

One thing Eve can try do is trying to take the eth root of $c \equiv m^e \pmod{n}$ to find m. However, this isn't as simple as plugging the expression into a calculator since $c^{1/e}$ is not an integer most of the time so reducing this modulo n is impossible.

Try to hack this

Remark

One thing Eve can try do is trying to take the eth root of $c \equiv m^e \pmod{n}$ to find m. However, this isn't as simple as plugging the expression into a calculator since $c^{1/e}$ is not an integer most of the time so reducing this modulo n is impossible.

Remark

Another thing Eve can try doing is finding the decryption exponent with

$$de \equiv 1 \pmod{\phi(n)}.$$

This requires the knowledge of $\phi(n)$ and this is essentially the same as knowing p and q which is very hard.

Discrete Logarithms

The basics

Definition

Let p be a prime and let α and β be nonzero integers modulo p. Additionally, let n be the smallest positive integer such that $\alpha^n \equiv 1 \pmod{p}$. The *discrete logarithm* of β with respect to α denoted with $L_\alpha(\beta)$ is the integer x modulo n such that

$$\alpha^x \equiv \beta \pmod{p}.$$

The basics

Definition

Let p be a prime and let α and β be nonzero integers modulo p. Additionally, let n be the smallest positive integer such that $\alpha^n \equiv 1 \pmod{p}$. The *discrete logarithm* of β with respect to α denoted with $L_\alpha(\beta)$ is the integer x modulo n such that

$$\alpha^x \equiv \beta \pmod{p}.$$

Definition

A *primitive root* of a modulo p is an α such that every β modulo p is a power of α.

The basics

Definition

Let p be a prime and let α and β be nonzero integers modulo p. Additionally, let n be the smallest positive integer such that $\alpha^n \equiv 1 \pmod{p}$. The *discrete logarithm* of β with respect to α denoted with $L_\alpha(\beta)$ is the integer x modulo n such that

$$\alpha^x \equiv \beta \pmod{p}.$$

Definition

A *primitive root* of a modulo p is an α such that every β modulo p is a power of α.

These computations are very hard to do (efficiently)!

ElGamal Cryptosystem

ElGamal

1. Bob chooses a prime p and a primitive root α. He also chooses a secret number b and computes $\beta = \alpha^b \pmod{p}$. He then makes (p, α, β) public.
2. Alice chooses a message $1 \leq m < p$ (breaking the message up if it is not in this range) and records Bob's public key.
3. Alice chooses a secret integer a and computes $r \equiv \alpha^a \pmod{p}$.
4. Alice also computes $t \equiv \beta^a m \pmod{p}$.
5. Alice sends (r, t) to Bob.
6. Bob decrypts by computing $tr^{-b} \equiv m \pmod{p}$. (He can compute the modular inverse quickly with the Euclidean Algorithm).

Why? and How to hack?

Solution

The reason this works is because

$$tr^{-b} \equiv \beta^a m(\alpha^a)^{-b} \equiv (\alpha^b)^a m\alpha^{-ab} \equiv m \pmod{p}.$$

Why? and How to hack?

Solution

The reason this works is because

$$tr^{-b} \equiv \beta^a m(\alpha^a)^{-b} \equiv (\alpha^b)^a m\alpha^{-ab} \equiv m \pmod{p}.$$

Remark

One thing to note is that Alice must choose a different secret integer a every time she sends a message because if Alice sends two messages m_1 and m_2 with the same a, Eve can find m_2 if she finds m_1. This is because r will be the same and Eve will know (r, t_1) and (r, t_2). Notice that

$$\frac{t_1}{m_1} \equiv \beta^a \equiv \frac{t_2}{m_2} \pmod{p}$$

so $m_2 \equiv t_2 m_1 / t_1 \pmod{p}$.

Elliptic Curves

The basics

Definition

Let K be any field of characteristic not 2 and let $a, b, c \in K$. An elliptic curve E is the set of points

$$E = \{(x, y) : x, y \in K, y^2 = x^3 + ax^2 + bx + c\}.$$

We also add the point (∞, ∞) to this set to represent the "point at infinity" in this curve. We denote this point with ∞.

Example

We can also consider elliptic curves in modulo p since the set of integers modulo p is field of characteristic not 2. For example, E can be the set of points that satisfy

$$y \equiv x^3 + 2x - 1 \pmod 5.$$

Extended Example

Example

This would mean that the elements of E are

$$E = \{(0,2),(0,3),(2,1),(2,4),(4,1),(4,4),\infty\}$$

where we have included the point at infinity. These are the elliptic curvues useful in cryptography.

Extended Example

Example

This would mean that the elements of E are

$$E = \{(0,2),(0,3),(2,1),(2,4),(4,1),(4,4),\infty\}$$

where we have included the point at infinity. These are the elliptic curvues useful in cryptography.

Definition (Addition)

Let P_1 and P_2 be points on an elliptic curve E with $K = \mathbb{R}$. We define the sum of P_1 and P_2 to be the point P_3 with obtained through the following construction: we draw a line through P_1 and P_2 and see where it interesects E. We then take the reflection of this point across x-axis to get P_3.

The Addition Law

Definition (Addition Law)

Let E be the elliptic curve $y^2 = x^3 + bx + c$ and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Then the sum

$$P_1 + P_2 = P_3 = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$$

where

$$m = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2 \\ (3x_1^2 + b)/(2y_1) & \text{if } P_1 = P_2. \end{cases}$$

If the slope is undefined or infinite, $P_3 = \infty$. Finally, the last addition law is

$$P + \infty = P.$$

Elliptic Curve ElGamal Cryptosystem

Elliptic Curve ElGamal

1. Bob chooses an elliptic curve E modulo p, so $K = \mathbb{Z} \backslash p\mathbb{Z}$, and a point α on E. He then chooses a secret number b and computes
$$\beta = b\alpha = \alpha + \alpha + \cdots + \alpha$$
where we are adding α b times. Finally, Bob makes (E, α, β).
2. Alice takes her message m and encodes it as a point on the elliptic curve. She chooses her secret number a and computes $r = a\alpha$ and $t = m + a\alpha$ and sends (r, t) to Bob.
3. Bob takes this pair and decrypts the message by computing
$$t - ar = m.$$

The End

Fin