

CLASE

7

Métodos Numéricos

Integración Numérica II

Educación de calidad

INTRODUCCIÓN

DE LA CLASE

GRADO / POSGRADO / TECNOLOGÍAS

Estudia a tu tiempo
son interrupciones



En esta clase se amplía el estudio de la integración numérica mediante los métodos compuestos, los cuales extienden las reglas básicas al subdividir el intervalo de integración en varios subintervalos para mejorar la precisión, partiendo del concepto de integración compuesta como la aplicación repetida de reglas como el trapecio o Simpson sobre particiones más pequeñas, lo que permite obtener aproximaciones más cercanas al valor real, analizando cómo la reducción del tamaño de paso influye directamente en el error global y en la calidad del resultado, para luego desarrollar la regla del trapecio compuesta y la regla de Simpson compuesta, evaluando su formulación, comportamiento del error y nivel de precisión, y cerrando con una comparación entre ambos métodos en términos de eficiencia, costo computacional y velocidad de convergencia, con el objetivo de que el estudiante pueda aplicar estos métodos y elegir el más adecuado según el problema.

Además, se introduce el estudio de los sistemas de ecuaciones diferenciales como una extensión natural para modelar fenómenos con múltiples variables que interactúan simultáneamente, comunes en áreas como ingeniería, física y economía, comenzando con los sistemas lineales homogéneos que permiten una resolución más directa mediante herramientas como matrices y valores propios, facilitando la comprensión de su estructura y comportamiento, para luego abordar los sistemas no homogéneos que incorporan términos externos y requieren técnicas adicionales para encontrar soluciones particulares, destacando el uso de métodos estructurados que amplían las posibilidades de análisis, permitiendo al estudiante comprender y resolver sistemas dinámicos más complejos y aplicar estos conceptos en la modelación de problemas reales.

Resultado o resultados de aprendizaje que será abordado con el contenido de la clase.

- 1) Analizar problemas matemáticos y computacionales utilizando métodos numéricos adecuados para su solución aproximada.
- 2) Aplicar técnicas numéricas en la resolución de problemas propios de la ingeniería y las ciencias computacionales.
- 3) Evaluar resultados numéricos considerando el error, la estabilidad y la confiabilidad de los métodos empleados.

Reto # (4)

Integración Numérica II

En la Clase 12 vimos las reglas simples del trapecio y Simpson, junto con sus errores. Ahora profundizamos en las versiones compuestas (composite), que dividen el intervalo en múltiples subintervalos para mejorar precisión y estabilidad. También comparamos los métodos.

Presentamos primero la formulación matemática formal, teoremas de error y análisis de convergencia, y luego las aplicaciones en ciberseguridad.

La integración numérica compuesta es una extensión de los métodos de integración numérica que se utiliza cuando el intervalo de integración es grande o cuando se desea mejorar la precisión de los métodos básicos, como la regla del trapecio o la regla de Simpson. En lugar de aplicar un único paso de integración en todo el intervalo, la integración compuesta divide el intervalo en subintervalos más pequeños y aplica los métodos de integración a cada uno de esos subintervalos. Posteriormente, las aproximaciones obtenidas de cada subintervalo se combinan para obtener una estimación del valor total de la integral. Este enfoque es muy útil en situaciones donde el intervalo es grande, ya que permite obtener una mayor precisión sin tener que reducir excesivamente el tamaño de los pasos en la integración.

La regla del trapecio compuesta es una versión extendida de la regla del trapecio que divide el intervalo en varios subintervalos y aplica la regla del trapecio a cada subintervalo de manera independiente. El valor total de la integral es la suma de las aproximaciones de cada subintervalo. Este método es fácil de implementar y mejora la precisión del método de trapecio simple al usar más puntos de evaluación a lo largo del intervalo. Sin embargo, al igual que la regla del trapecio simple, su precisión sigue siendo limitada y depende del número de subintervalos. A medida que el número de subintervalos aumenta, la precisión mejora, pero la mejora no es tan rápida como en otros métodos, como la regla de Simpson. La regla del trapecio compuesta es útil cuando se tiene un gran número de subintervalos y se necesita una solución rápida y relativamente precisa.

Integración compuesta

La integración compuesta divide $[a, b]$ en n subintervalos (n par para Simpson 1/3) de ancho $h = (b - a)/n$, con nodos $x_i = a + ih$, $i = 0, 1, \dots, n$.

La integral total es la suma de integrales en cada subintervalo:

$$\int_a^b f(x) dx = \sum_{k=0}^{n-1} \int_{x_k}^{x_{k+1}} f(x) dx$$

Aplicando una regla simple en cada subintervalo se obtiene la regla compuesta.

Teorema general de convergencia: Si f es suficientemente suave y $h \rightarrow 0$ ($n \rightarrow \infty$), la aproximación compuesta converge al valor exacto de la integral, con orden de precisión igual al de la regla simple (2 para trapecio, 4 para Simpson 1/3).

Regla del trapecio compuesta

Divide $[a, b]$ en n subintervalos ($n \geq 1$) de ancho $h = (b - a)/n$.

$$\int_a^b f(x) dx \approx \frac{h}{2} \left[f(x_0) + 2 \sum_{i=1}^{n-1} f(x_i) + f(x_n) \right]$$

Análisis de error (teorema compuesto): Si $f \in C^2[a, b]$, el error total es:

$$E_T = -\frac{(b-a)h^2}{12} f''(\xi) \text{ para algún } \xi \in [a, b]$$

$$\Rightarrow |E_T| \leq \frac{(b-a)^3}{12n^2} \max_x |f''(x)| = O(1/n^2) = O(h^2)$$

El orden global de precisión es 2, igual que la versión simple.

COMPOSITE TRAPEZIODAL RULE: WEIGITED Sum of Subintervals

Visualizing Area Breakdown with op Weights

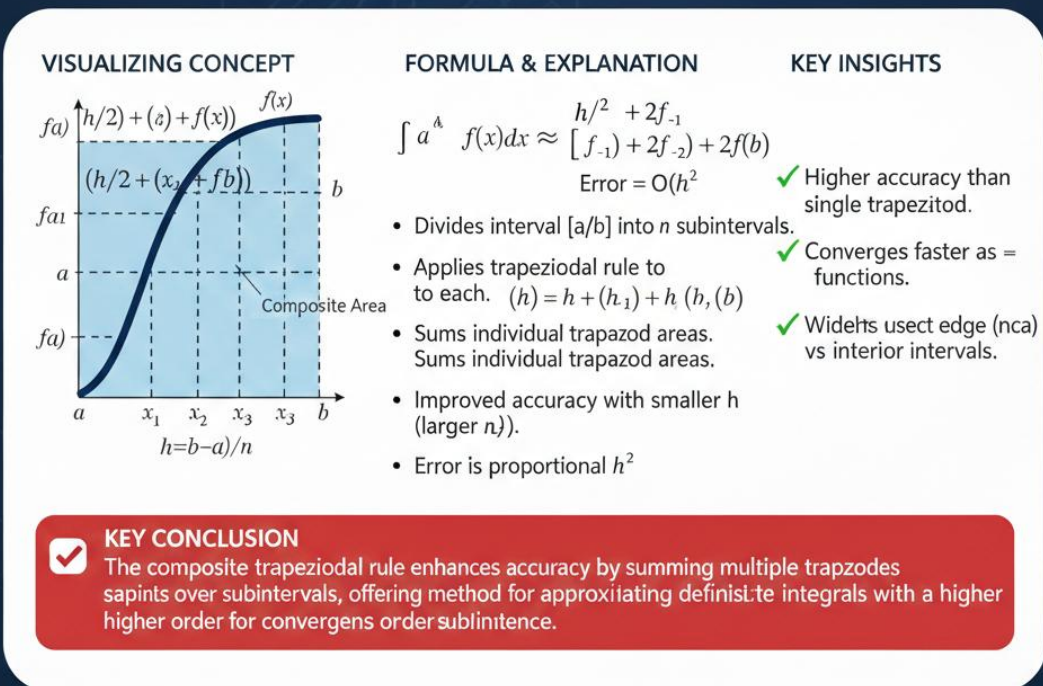


Figura 1: Desglose de la regla del trapecio compuesta en subintervalos con pesos $h/2, h, h/2$.

Creación propia.

Regla de Simpson compuesta

Formulación matemática formal

Requiere n par (número de subintervalos par, número de puntos $n+1$ impar). Divide $[a, b]$ en n subintervalos de ancho $h = (b - a)/n$.

$$\int_a^b f(x) dx \approx \frac{h}{3} \left[f(x_0) + 4 \sum_{k=1}^{n/2-1} f(x_{2k-1}) + 2 \sum_{k=1}^{n/2-1} f(x_{2k}) + f(x_n) \right]$$

Análisis de error (teorema compuesto): Si $f \in C^4[a, b]$, el error total es:

$$E_S = -\frac{(b-a)h^4}{180} f^{(4)}(\xi) \text{ para algún } \xi \in [a, b]$$

$$\Rightarrow |E_S| \leq \frac{(b-a)^5}{180n^4} \max |f^{(4)}(x)| = O(1/n^4) = O(h^4)$$

El orden global de precisión es 4, exacta para polinomios hasta grado 3.

En ciberseguridad: Simpson compuesta ofrece mayor precisión en integración de señales suaves en power/electromagnetic analysis (e.g., correlación acumulada en CPA), estimación de probabilidades en Monte Carlo para riesgo de ataques, y procesamiento forense de señales continuas discretizadas.

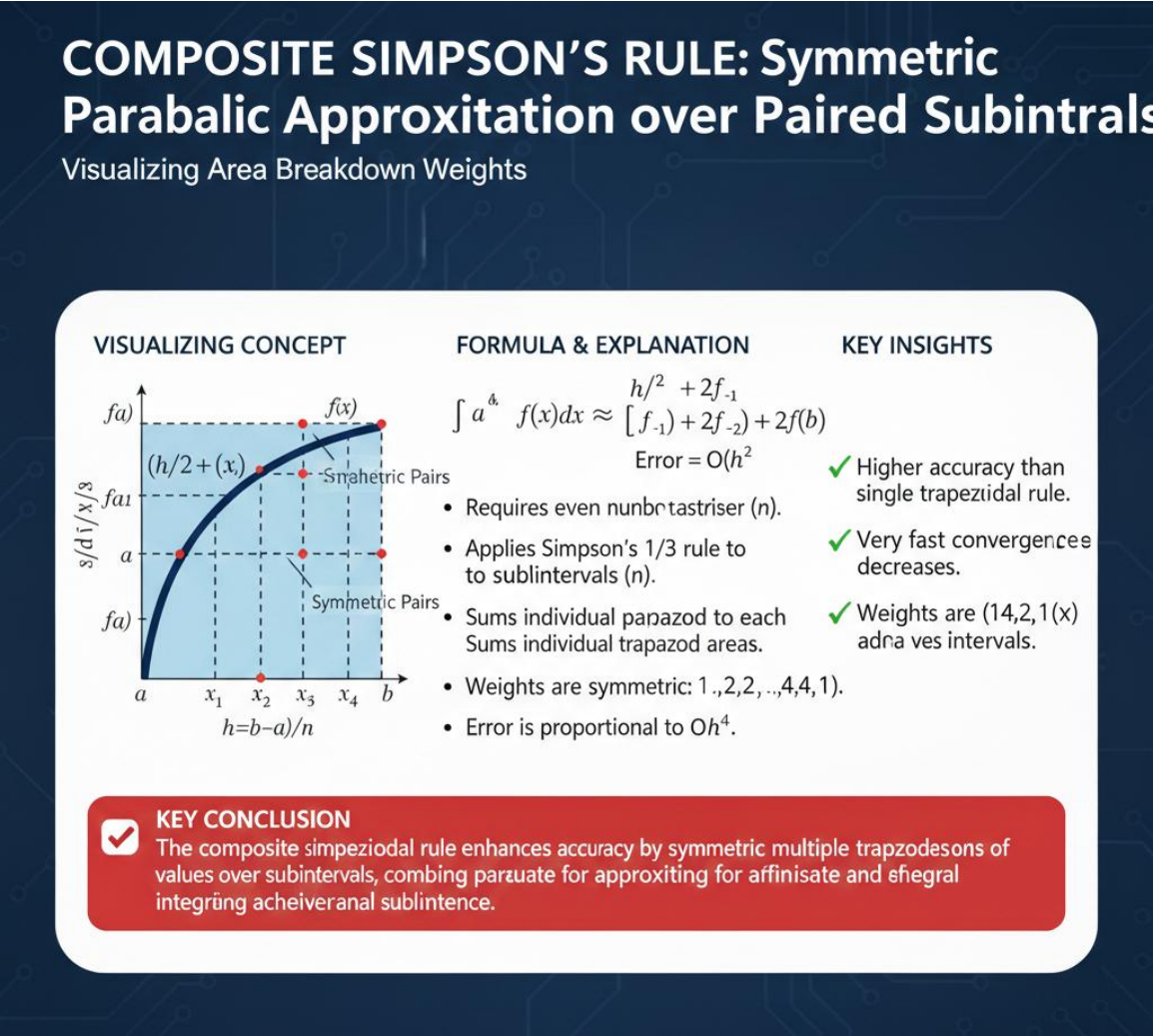


Figura 2: Regla de Simpson compuesta: combinación de parábolas en pares de subintervalos (simétricas).

Creación propia.

Comparación de métodos de integración

Método	Orden de precisión	Error de truncamiento	Costo de evaluación (por intervalo)	Ventajas matemáticas	Desventajas	Aplicación típica en ciberseguridad
Trapezio compuesto	2 ($O(h^2)$)	$-\frac{(b-a)h^2}{12} f''(\xi)$	1 por subintervalo	Simple, estable, converge	Precisión moderada, error $O(h^2)$	Integración rápida de correlación

			o (n+1 total)	para f continua		en trazas ruidosas
Simpson 1/3 compuesto	4 ($O(h^4)$)	- $\frac{(b-a)h^4}{180} f^{(4)}(\xi)$	1 por subintervalo (n+1 total)	Alta precisión con pocos puntos, exacta grado 3	Requiere n par, más sensible a ruido extremo	Análisis preciso de señales en DPA/CPA o forense
Trapezio vs Simpson	Simpson n 4x mejor	Error Simpson ~ h^2 veces menor	Similar (mismo número de puntos)	Simpson converge mucho más rápido	Trapezio más robusto si f'' grande o ruido	Simpson preferido para funciones suaves, trapezio para ruidosas

Tabla 1: Comparación gráfica: En escala log-log (error vs h), trapezio muestra pendiente -2, Simpson -4 (convergencia más rápida).

Creación propia.

Elección:

- Trapecio para funciones con derivadas altas o datos muy ruidosos (menos sensible a outliers).
- Simpson para funciones suaves y cuando se necesita precisión alta con menos evaluaciones.

En ciberseguridad: Simpson compuesta es preferida en integración de funciones de correlación o potencia media (mayor precisión reduce falsos negativos en detección); trapezio en estimaciones rápidas de áreas bajo ROC o Monte Carlo para probabilidad de éxito de ataques.

TRUNCATION ERROR COMPARISON: Trapezoidal vs Simpson (Log-Log Plot)

Visualizing Convergence Rate with Step Size

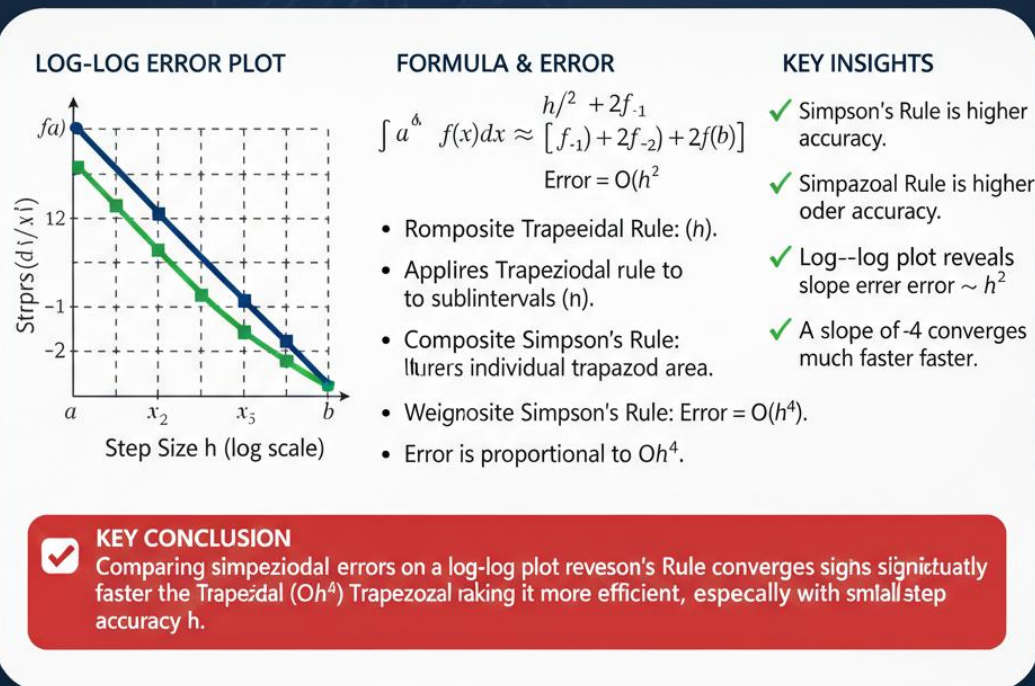


Figura 3: Comparación log-log de error vs tamaño de paso h : pendiente -2 para trapecio compuesto, -4 para Simpson compuesto.

Creación propia.

La figura muestra una comparación log-log del error frente al tamaño del paso h para dos métodos de integración numérica: trapecio compuesto y Simpson compuesto. En el gráfico log-log, el eje vertical representa el error de la aproximación, mientras que el eje horizontal muestra el tamaño del paso h , que es la distancia entre los puntos de evaluación de la función en cada método.

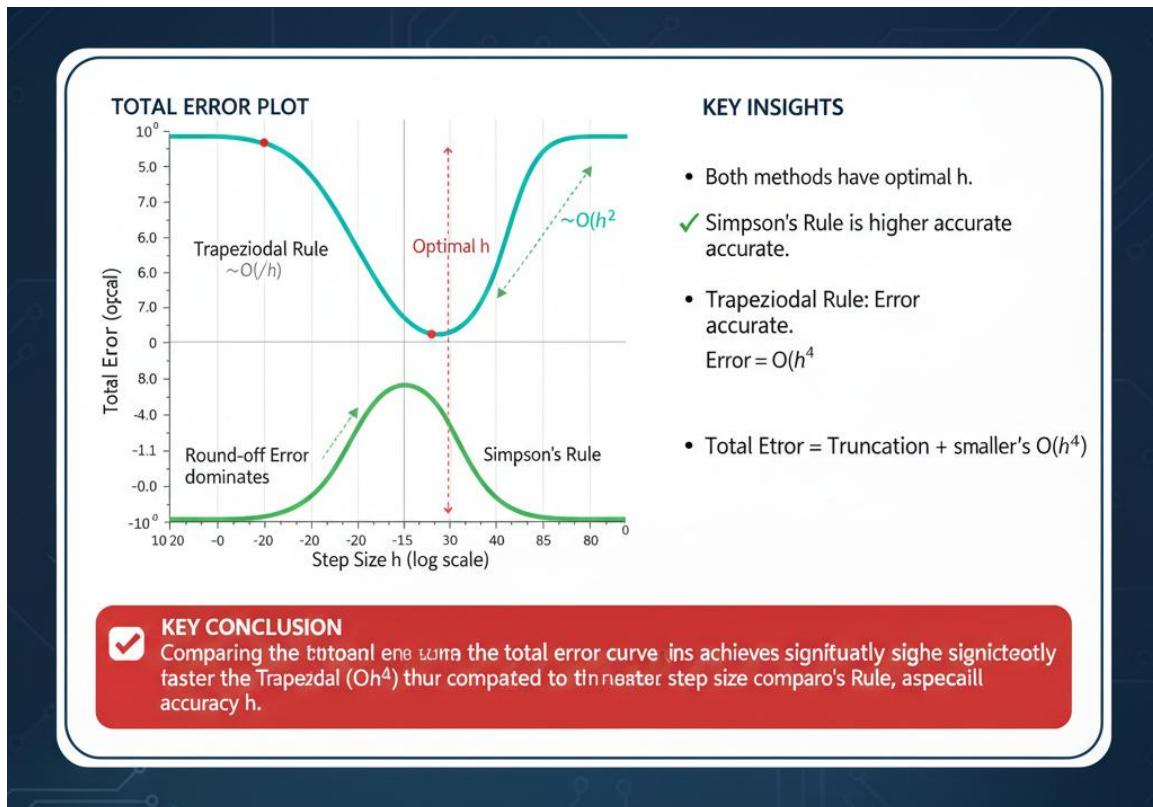


Figura 4: Curva de error total vs h para ambos métodos: mínimo más bajo y a h mayor para Simpson.

Creación propia.

Ecuaciones Diferenciales Ordinarias I

En esta parte de la asignatura pasamos a las ecuaciones diferenciales ordinarias (EDO) de primer orden, que modelan fenómenos dinámicos en el tiempo o en una variable independiente. En ciberseguridad, las EDO aparecen en modelado de propagación de malware (modelos SIR/SEIR adaptados), análisis de timing en side-channel (dinámica de ejecución), y simulación de ataques persistentes o difusión de vulnerabilidades en redes.

Presentamos primero la formulación matemática formal, métodos de resolución numérica de un paso y análisis de error, y luego las aplicaciones en ciberseguridad.

Las ecuaciones diferenciales ordinarias (EDO) son fundamentales para modelar fenómenos dinámicos en diversas áreas de la ciencia y la ingeniería. Estas ecuaciones describen cómo cambian una o más variables dependientes en función de una variable independiente, generalmente el tiempo. La formulación de problemas con EDO implica definir la ecuación diferencial que describe el comportamiento del sistema y las condiciones iniciales que determinan el estado del sistema al inicio del proceso. El objetivo es encontrar una función que satisfaga la ecuación diferencial y las condiciones iniciales, pero en muchos casos, especialmente cuando no se puede obtener una solución exacta, se recurre a métodos numéricos para aproximar la solución. Los métodos numéricos, como el método de Euler y el

método de Euler mejorado, son ampliamente utilizados para resolver EDOs de manera aproximada.

El método de Euler es uno de los métodos más sencillos y básicos para resolver ecuaciones diferenciales ordinarias de primer orden. Este método aproxima la solución de la EDO utilizando un enfoque de "pasos discretos" a lo largo de la variable independiente, normalmente el tiempo. En cada paso, el valor de la función se actualiza utilizando la derivada en el punto actual y un tamaño de paso (h), que determina cuánto se avanza en cada iteración. Aunque el método de Euler es fácil de implementar y computacionalmente eficiente, su precisión es limitada, especialmente cuando el tamaño del paso es grande. Esto se debe a que el método es de primer orden, lo que significa que el error en la aproximación disminuye de manera lineal con el tamaño del paso.

El método de Euler mejorado, también conocido como el método de Heun, es una versión más precisa del método de Euler. En lugar de utilizar solo la derivada en el punto actual, el método de Euler mejorado realiza una predicción inicial con el método de Euler y luego corrige esta predicción utilizando la derivada en el siguiente paso. Este enfoque reduce el error y mejora la precisión, ya que utiliza una aproximación más precisa para la pendiente en cada paso. Aunque no es tan preciso como métodos más avanzados, como el método de Runge-Kutta de cuarto orden, el método de Euler mejorado ofrece una buena precisión a un costo computacional relativamente bajo, siendo ideal para problemas donde se requiere una mejora significativa respecto al método de Euler sin un aumento drástico en los cálculos.

El análisis del error en métodos de un paso, como los métodos de Euler y Euler mejorado, es esencial para entender la precisión de las soluciones numéricas obtenidas. El error en estos métodos generalmente depende del tamaño del paso (h), y el método de Euler, al ser de primer orden, tiene un error que disminuye proporcionalmente al tamaño del paso, es decir, el error es directamente proporcional a (h). En cambio, el método de Euler mejorado, que es de segundo orden, tiene un error que disminuye más rápidamente, siendo proporcional a (h^2). Esto significa que, a medida que se reduce el tamaño del paso, el error disminuye de forma más eficiente con el método mejorado en comparación con el método básico de Euler. Sin embargo, en ambos métodos, un tamaño de paso demasiado pequeño puede generar problemas de estabilidad y aumentar los costos computacionales, por lo que es importante encontrar un balance adecuado entre precisión y eficiencia en función del problema específico.

Formulación de problemas con EDO

Una ecuación diferencial ordinaria de primer orden tiene la forma general:

$$y'(t) = f(t, y(t)), \quad y(t_0) = y_0$$

Donde:

- t es la variable independiente (tiempo o parámetro),
- $y(t)$ es la función desconocida (estado del sistema),
- $f(t, y)$ es la función dada (velocidad de cambio),
- (t_0, y_0) es la condición inicial.

Teorema de existencia y unicidad (Picard-Lindelöf): Si f es continua en un rectángulo alrededor de (t_0, y_0) y Lipschitz continua en y (es decir, existe K tal que $|f(t, y_1) - f(t, y_2)| \leq K|y_1 - y_2|$ para todo t en intervalo), entonces existe una única solución $y(t)$ en algún intervalo $[t_0 - \delta, t_0 + \delta]$.

En ciberseguridad: las EDO modelan la tasa de infección en redes ($y' = \beta y (1 - y/N)$ en modelo logístico), dinámica de propagación de ransomware, o evolución temporal de métricas de ataque (e.g., número de hosts comprometidos).

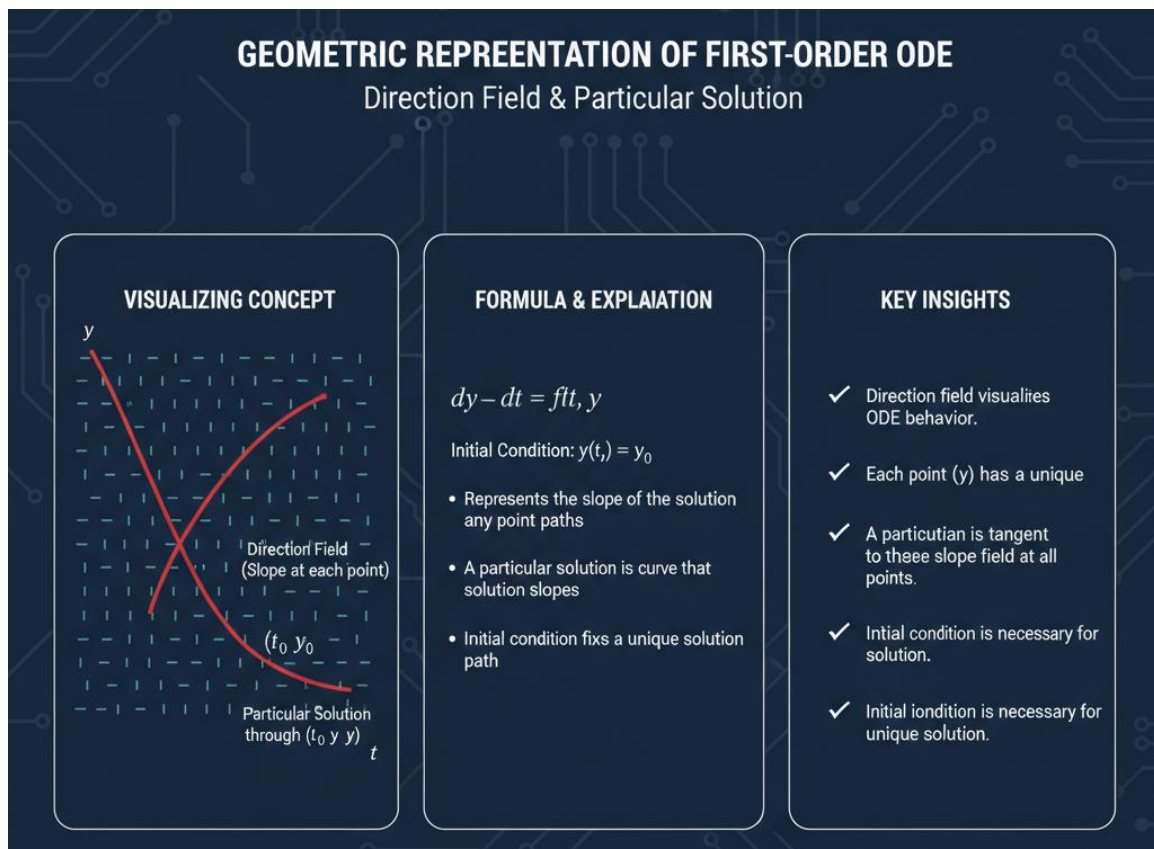


Figura 5: Representación geométrica de una EDO de primer orden: campo de direcciones (slopes) y solución particular que pasa por (t_0, y_0) .

Creación propia.

Método de Euler

Formulación matemática formal

El método de Euler (forward Euler) es el más simple de los métodos de un paso. Aproxima la derivada por la diferencia hacia adelante:

$$y'(t_k) \approx \frac{y_{k+1} - y_k}{h} = f(t_k, y_k)$$

$$\Rightarrow y_{k+1} = y_k + hf(t_k, y_k)$$

con $t_{k+1} = t_k + h$, h paso de tiempo.

Análisis de error local (truncamiento): Por expansión de Taylor: $y(t_k + h) = y(t_k) +$

$$hy'(t_k) + \frac{h^2}{2}y''(\xi_k) \Rightarrow \text{error local} = y(t_{k+1}) - y_{k+1} = \frac{h^2}{2}y''(\xi_k) = O(h^2)$$

Error global: acumulación de errores locales $\rightarrow O(h)$ (orden de precisión 1).

Condición de estabilidad: para ecuaciones rígidas (stiff), Euler forward puede ser inestable a menos que h sea muy pequeño.

En ciberseguridad: Euler se usa en simulaciones simples de propagación de malware (modelo SIR discreto), estimación rápida de evolución de amenazas en redes, y prototipado de ataques temporales.

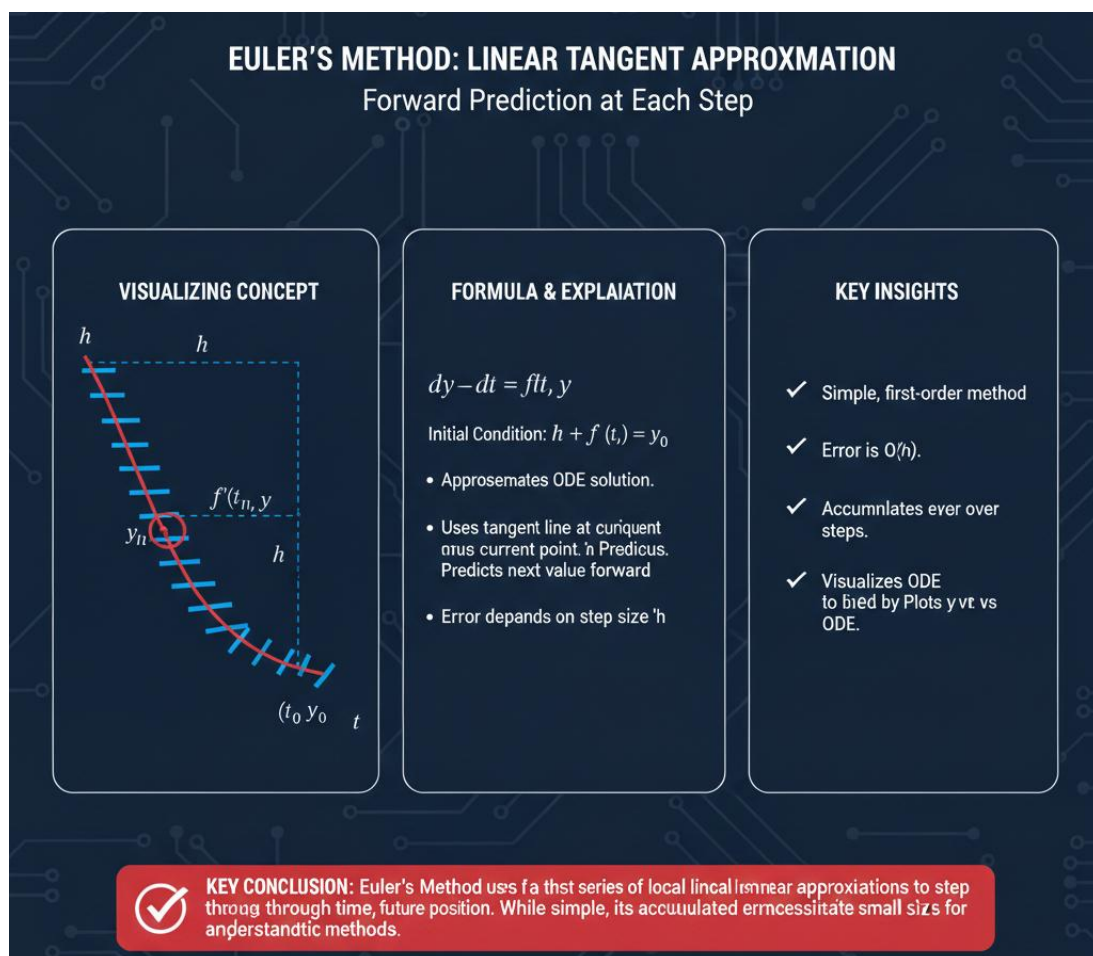


Figura 6: Método de Euler: aproximación lineal tangente en cada paso (predicción forward).

Creación propia.

Enlace 1: <https://www.youtube.com/watch?v=7jC2k5v5K8w> Ver en YouTube: Método de Euler para Ecuaciones Diferenciales – Explicación paso a paso y ejemplo Este video muestra la derivación, implementación y comparación con solución exacta.

Método de Euler mejorado

Formulación matemática formal

El método de Euler mejorado también conocido como método de Heun o Euler modificado (predictor-corrector de dos etapas):

1. **Predictor** (Euler estándar): $\hat{y}_{k+1} = y_k + hf(t_k, y_k)$
2. **Corrector** (promedio de pendientes): $y_{k+1} = y_k + \frac{h}{2}[f(t_k, y_k) + f(t_{k+1}, \hat{y}_{k+1})]$

Análisis de error:

- Error local: $O(h^3)$ (por expansión de Taylor en ambas evaluaciones y promedio).
- Error global: $O(h^2)$ (orden de precisión 2).

Teorema: Si f es Lipschitz en y y continua en t , el método converge con orden 2.

En ciberseguridad: Euler mejorado ofrece mejor precisión en simulaciones de dinámica de amenazas (e.g., propagación de botnets o worms) sin costo mucho mayor que Euler simple, y en modelado de side-channel temporal (evolución de consumo de potencia).

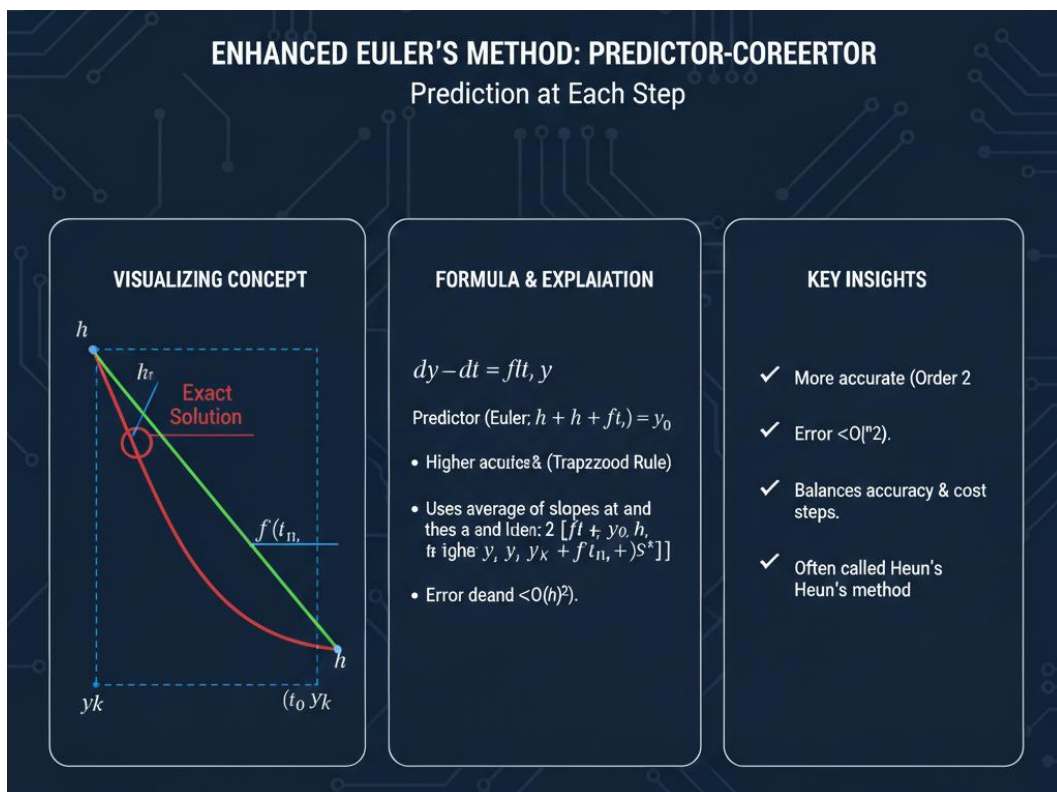


Figura 7: Euler mejorado: predictor (Euler) + corrector (promedio de pendientes en t_k y t_{k+1}).

Creación propia.

La figura muestra el método de Euler mejorado, que es una mejora del método de Euler simple. El método de Euler mejorado combina dos pasos: un predictor y un corrector, para obtener una mejor aproximación de la solución de la ecuación diferencial.

Predictor (Euler):

El primer paso, conocido como el predictor, es el mismo que el método de Euler simple. Consiste en utilizar la fórmula de Euler para estimar el valor de la solución en el siguiente paso y_{k+1} utilizando el valor de la pendiente en el punto t_k :

$$y_{k+1}^{(p)} = y_k + hf(t_k, y_k)$$

donde $y_{k+1}^{(p)}$ es la predicción de la solución en el siguiente paso, h es el tamaño del paso, y $f(t_k, y_k)$ es la pendiente de la solución en el punto (t_k, y_k) .

Corrector (promedio de pendientes):

El paso del corrector mejora la predicción obtenida en el predictor tomando el promedio de las pendientes en los puntos t_k y t_{k+1} . Esto se hace para corregir la aproximación, ya que la predicción inicial realizada por el predictor solo utiliza la pendiente en t_k , lo que puede no ser exacto si la pendiente cambia mucho en el intervalo.

La fórmula para el corrector es:

$$y_{k+1} = y_k + \frac{h}{2} \left(f(t_k, y_k) + f(t_{k+1}, y_{k+1}^{(p)}) \right)$$

Aquí, $y_{k+1}^{(p)}$ es el valor predicho del paso anterior, y $f(t_{k+1}, y_{k+1}^{(p)})$ es la pendiente evaluada en el punto $(t_{k+1}, y_{k+1}^{(p)})$, que es el valor de la predicción.

El promedio de pendientes tiene como objetivo mejorar la precisión de la aproximación, ya que utiliza una evaluación de la pendiente en dos puntos del intervalo, en lugar de solo en un punto.

Resultado final:

La combinación del predictor y el corrector en el método de Euler mejorado produce una aproximación de la solución más precisa que el método de Euler simple. El error se reduce, y el método tiene un orden de precisión de $O(h^2)$, lo que significa que la precisión mejora más rápidamente a medida que se reduce el tamaño del paso h , en comparación con el método de Euler simple, que tiene un error de $O(h)$.

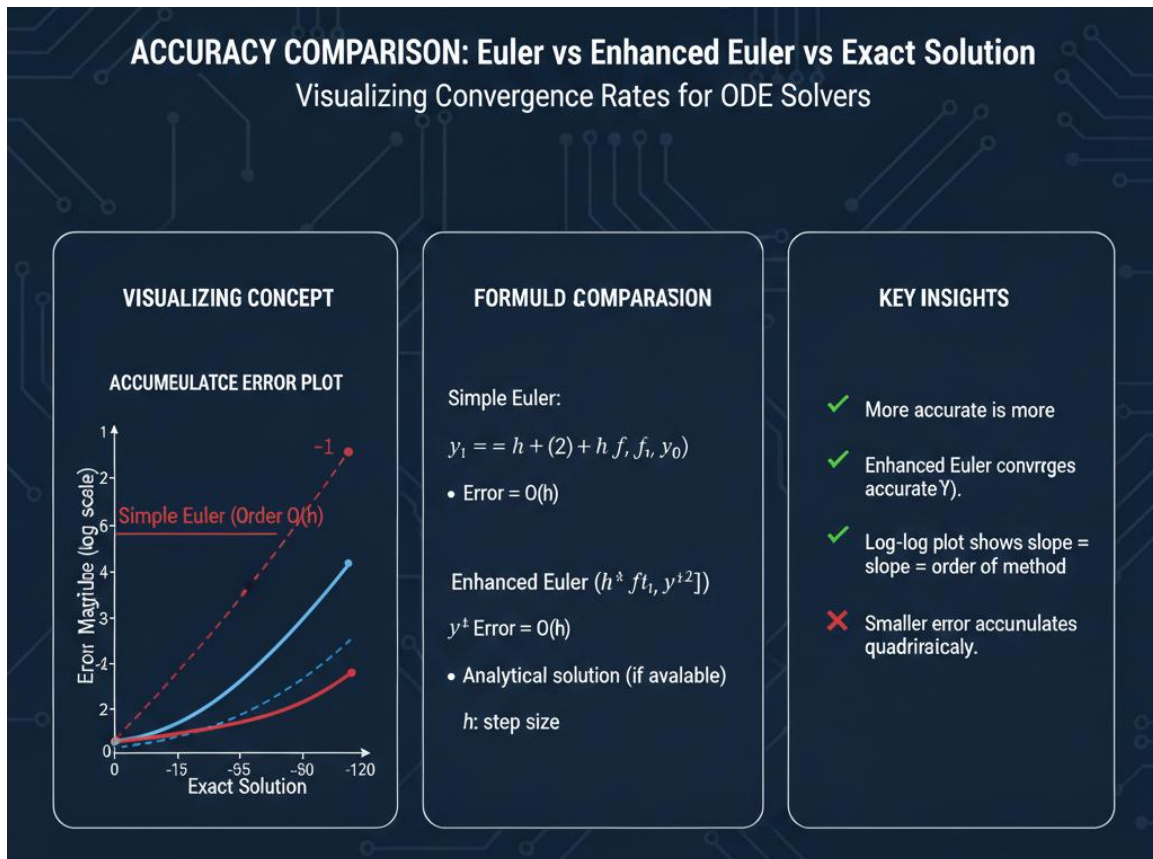


Figura 8: Comparación de precisión: Euler simple ($O(h)$) vs Euler mejorado ($O(h^2)$) vs solución exacta.

Creación propia.

Enlace 2: https://www.youtube.com/watch?v=Stf__2m3z0U Ver en YouTube: Método de Euler Mejorado (Heun) – Fórmula, error y ejemplo resuelto Este recurso explica el predictor-corrector, análisis de error $O(h^2)$ y ventajas sobre Euler simple.

Análisis del error en métodos de un paso

Error local de truncamiento (LTE): diferencia entre la solución exacta y la aproximada en un paso, asumiendo y_k exacto.

- Euler: $LTE = O(h^2)$
- Euler mejorado: $LTE = O(h^3)$

Error global (GTE): acumulación de errores locales a lo largo de todos los pasos. Para métodos de un paso consistentes y estables: $GTE = O(h^p)$ si $LTE = O(h^{p+1})$.

Teorema de convergencia (Lax equivalence): Un método consistente + estable $\Rightarrow$ convergente. Euler es consistente de orden 1, Euler mejorado de orden 2.

Error de redondeo y estabilidad:

- Error de redondeo acumulado $\approx n \cdot \epsilon_{\text{machine}} \cdot \max |y|$ ($n = (b - a)/h$).

- Estabilidad absoluta: región en el plano complejo donde $|1 + h \lambda| < 1$ (para $y' = \lambda y$).
Euler forward tiene región pequeña (disco de radio 1 centrado en -1).

En ciberseguridad: análisis de error es crítico para confiar en simulaciones de propagación de amenazas (error bajo evita subestimar riesgos), y en optimización numérica de ataques (gradientes de funciones de costo en ML para detección).

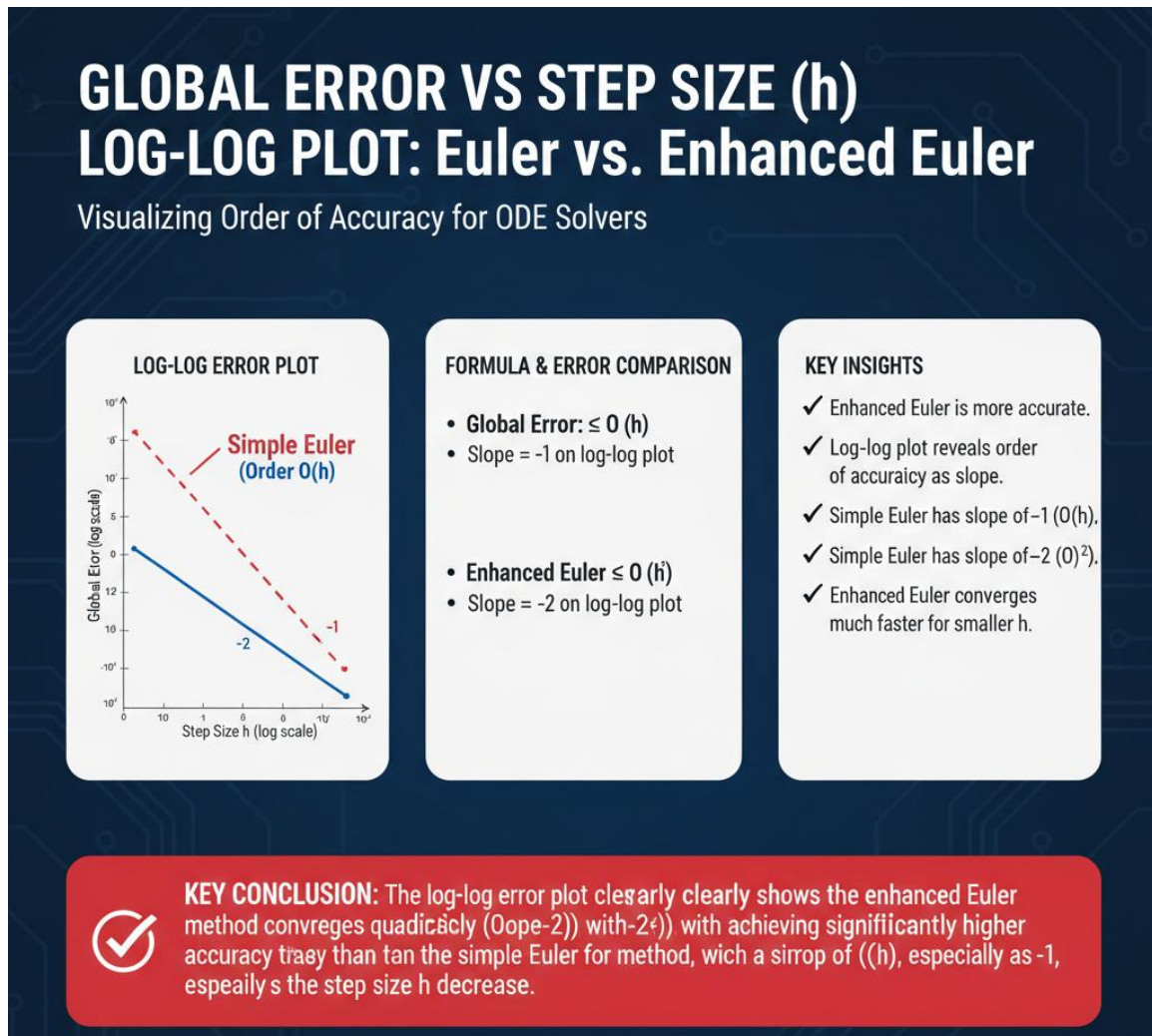


Figura 9: Error global vs paso h (log-log): pendiente -1 para Euler ($O(h)$), -2 para Euler mejorado ($O(h^2)$).

Creación propia.

RE FE REN CIAS

Glosario:

- Burden, R. L., Faires, J. D., & Burden, A. M. (2015). Numerical analysis (10ª ed.). Cengage Learning.
- Higham, N. J. (2002). Accuracy and stability of numerical algorithms (2ª ed.). SIAM.
- Atkinson, K. E. (1989). An introduction to numerical analysis. Wiley.
- Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer.
- Boneh, D., & Shoup, V. (2020). A graduate course in applied cryptography.
<https://toc.cryptobook.us>



síguenos en:



www.pucevirtual.puce.edu.ec