Clase 7

René Descartes

Los enteros módulo n: Congruencias

- Definición: Dado n > 0 entero, y a, b enteros, decimos que "a es congruente con b módulo n", y lo denotamos:
- $a \equiv b \pmod{n}$
- Si $n \mid a - b$.
- En particular, si en la división entera entera entre a y n se tiene cociente q y resto r (con $0 \leqq r < n$), como se cumple:
- $a = n \cdot q + r \Longrightarrow a - r = n \cdot q \Longrightarrow n \mid a - r$, luego:
- $a \equiv r \pmod{n}$. Es decir que todo entero a es congruente módulo n con un número $r \in \{0,1,\ldots..,\ n-1\}$. Es fácil ver que lo será con un único r en este intervalo pues si $a \equiv r \pmod{n}$ y $r \in \{0,1,\ldots..,\ n-1\}$ entonces r tiene necesariamente que ser el resto de la división de a entre n.

- La relación de congruencia módulo n es una relación de equivalencia, es decir, es reflexiva, simétrica y transitiva. Las dos primeras son evidentes, respecto a la transitividad:
- Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n} \Longrightarrow n \mid a - b$ y $n \mid b - c \Longrightarrow$
- $n \mid (a - b) + (b - c) = a - c \Longrightarrow a \equiv c \pmod{n}$.
- Luego, los enteros quedan repartidos en las n clases de equivalencia (son n pues recordemos que cada una tiene un representante $r \in \{0, 1, \ldots, n-1\}$, que es un conjunto de cardinal n), a las que llamaremos clases residuales módulo n. Para un $u \in \mathbb{Z}$, denotaremos por $\bar{u}$ a la clase residual que contiene a u. Al conjunto de estas n clases residuales lo denotamos $\mathbb{Z} / n\,\mathbb{Z}$, es decir:
- $\mathbb{Z} / n\,\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots\ldots, \overline{n-1}\}$.

- La suma, resta y producto en $\mathbb{Z}$ inducen análogas operaciones (con idénticas propiedades conmutativa, asociativa y distributiva) en estas clases residuales, pues están bien definidas, es decir, no dependen del elemento cogido en cada clase residual:
- Si $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n} \Longrightarrow a + b \equiv a' + b' \pmod{n}$,
- $a - b \equiv a' - b' \pmod{n}$ y $a \cdot b \equiv a' \cdot b' \pmod{n}$.
- Las dos primeras se deducen fácilmente de $n \mid x, n \mid y \Longrightarrow n \mid x \pm y$. Para el caso del producto, de la propiedad $n \mid x \Longrightarrow n \mid x \cdot z$ (para cualquier z) se deduce que: $a \equiv a' \pmod{n} \Longrightarrow a \cdot b \equiv a' \cdot b \pmod{n}$. Y por otro lado como
- $b \equiv b' \pmod{n} \Longrightarrow a' \cdot b \equiv a' \cdot b' \pmod{n}$. Juntando las dos obtenemos:
- $a \cdot b \equiv a' \cdot b' \pmod{n}$.

- Observación: De lo anterior se sigue que $\forall\, s \geqq 0$: $a \equiv b \pmod{n} \Longrightarrow$
- $a^s \equiv b^s \pmod{n}$. En particular si $a \equiv -1 \pmod{n} \Longrightarrow a^s \equiv (-1)^s \pmod{n}$, que es igual a 1 si s es par y a -1 si s es impar.
- También vemos que si P(x) es polinomio a coeficientes en $\mathbb{Z}$ y se tiene: $a \equiv b \pmod{n}$, entonces: $P(a) \equiv P(b) \pmod{n}$
- Proposición 1: Si $n \geqq 1$ y se tiene enteros a, b, c con:
- $a \cdot c \equiv b \cdot c \pmod{n}$, sea $d = mcd(c, n)$, se tiene:
- $a \equiv b \left(\mod \frac{n}{d}\right)$
- Demostración: Como $d = mcd(c, n)$ si llamamos $c/d = c'$ y $n/d = n'$ se tiene que (c' y n' son enteros y) $mcd(c', n') = 1$. Sustituimos $c = d \cdot c'$ y $n = d \cdot n'$ en la fórmula y nos queda:
- $a \cdot d \cdot c' \equiv b \cdot d \cdot c' \pmod{d \cdot n'}$. Veamos que aquí podemos cancelar todas las apariciones de d (incluída la que aparece en el módulo!):

- La fórmula equivale a:
- $d \cdot n' \mid (d \cdot a \cdot c' - d \cdot b \cdot c') = d \cdot (a \cdot c' - b \cdot c')$, y podemos cancelar d para deducir que: $n' \mid a \cdot c' - b \cdot c'$.
- En este punto tenemos que recordar que $mcd(c', n') = 1$, y como se tiene que $n' \mid c' \cdot (a - b)$, el lema de Euclides implica que $n' \mid a - b$, que nos da: $a \equiv b \pmod{n'}$.
- Q.E.D.
- Corolario: Si a, b, c, n son como antes con la condición extra de que $mcd(c, n) = 1$, entonces vale la cancelativa, es decir:
- $a \cdot c \equiv b \cdot c \pmod{n} \Rightarrow a \equiv b \pmod{n}$

- Lema: Sea R un conjunto de n enteros que representan a todas las clases residuales $\mathbb{Z} / n\mathbb{Z}$. Sea a un entero con mcd(a, n) = 1. Entonces:
- $a \cdot R = \{ a \cdot x$ tal que $x \in R\}$ también cumple que sus elementos representan todas las clases de $\mathbb{Z} / n\mathbb{Z}$.
- Observación: como los n elementos de R representan a las n clases de $\mathbb{Z} / n\mathbb{Z}$, es obvio que todos representan a clases diferentes.
- Demostración: Como R posee n elementos (que sabemos que recorren todas las clases residuales módulo n), $a \cdot R$ también posee n elementos. Luego, como hay n clases residuales módulo n, probar que los elementos de $a \cdot R$ representan a todas las clases residuales es equivalente a probar que ningún par de ellos representa a la misma clase residual.
- Supongamos que se tienen $x, x' \in R$ tales que $a \cdot x \equiv a \cdot x' \pmod n$. Como mcd(a,n)= 1, por el corolario previo: $x \equiv x' \pmod n \Longrightarrow x = x'$. Luego, diferentes elementos de $a \cdot R$ no caen en la misma clase residual módulo n.

- Proposición 2: Si $n > 1$ y a, b enteros con $\mathrm{mcd}(a, n) = 1 \Longrightarrow$
- La ecuación: $a \cdot x \equiv b \pmod{n}$ tiene solución, y es única módulo n.
- Demostración: Si tomamos $R = \{0, 1, \ldots, n-1\}$, como $\mathrm{mcd}(a,n) = 1$ vemos que a y R cumplen las condiciones del lema previo, luego sabemos que
- $a \cdot R = \{0, a, \ldots, a \cdot (n-1)\}$ recorre todas las clases residuales. En particular, algún elemento cae en la clase de b, es decir, existe i tal que:
- $a \cdot i \equiv b \pmod{n}$.
- Para ver la unicidad (como clase módulo n), supongamos que tenemos dos enteros x, x' con:
- $a \cdot x \equiv b \equiv a \cdot x' \pmod{n}$, de aquí por el corolario de la proposición 1 y siendo $\mathrm{mcd}(a,n)=1$ tenemos: $x \equiv x' \pmod{n}$.

- Observación: En el caso particular b=1 vemos que si a es coprimo con n entonces a tiene inverso módulo n, es decir, una clase residual cuyos elementos x cumplen: $a \cdot x \equiv 1 \pmod{n}$. En la siguiente proposición se establece la afirmación recíproca.
- Proposición 3: Si a, b enteros y $n > 1$ se tiene que $a \cdot x \equiv b \pmod{n}$ tiene solución sí y sólo sí $mcd(a,n) \mid b$.
- En particular (caso b=1): a posee inverso módulo n $\Leftrightarrow$ a coprimo con n.
- Demostración: Sea $g = mcd(a,n)$. Supongamos que hay un x entero solución de la congruencia $\Rightarrow n \mid a \cdot x - b$.
- Luego, como $g \mid n \Rightarrow g \mid a \cdot x - b$. Además se tiene que $g \mid a$, y por lo tanto $g \mid a \cdot x$. Por lo tanto $g \mid (a \cdot x - (a \cdot x - b)) = b$.

- Recíprocamente, supongamos que g | b. Entonces, como g | a, g | n y g | b, se tiene la equivalencia:
- $n \mid a \cdot x - b \Leftrightarrow \frac{n}{g} \mid (\frac{a}{g} \cdot x - \frac{b}{g})$.
- Por lo tanto, la ecuación $a \cdot x \equiv b \pmod{n}$ tiene solución sí y sólo sí la ecuación $\frac{a}{g} \cdot x \equiv \frac{b}{g} \pmod{\frac{n}{g}}$ tiene solución. Para esta última, como $\mathrm{mcd}(\frac{a}{g}, \frac{n}{g}) = 1$ sabemos por la proposición previa que tiene solución.
- Observaciones:
- (1) En el caso en que el módulo es un primo p, vemos que a tiene inverso módulo p $\Leftrightarrow$ a no es divisible por p $\Leftrightarrow$ $a \not\equiv 0 \pmod{p}$
- (2) En el caso en que mcd(a,n) | b vemos de la demostración (y de la unicidad en la prop. previa) que, además de existir solución, esta solución es única módulo n/mcd(a,n). Esto implica que hay mcd(a, n) soluciones módulo n.

Clase 8

- Lema: Sean $a_1, a_2, \ldots a_k, n$ enteros con $a_i \mid n$, para i= 1,2,…,k y además tales que los a_i son coprimos dos a dos. Entonces se tiene que:
- $a_1 \cdot a_2 \cdot \ldots\ldots \cdot a_k \mid n$.
- Demostración: Ejercicio.
- Teorema Chino de los Residuos: Dados $m_1, m_2, \ldots, m_k$ enteros positivos coprimos dos a dos, y enteros $c_1, c_2, \ldots, c_k$, el sistema de congruencias:
- $$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \ldots\ldots\ldots \\ x \equiv c_k \pmod{m_k} \end{cases}$$
- Tiene solución, y la solución es única módulo $m = m_1 \cdot m_2 \cdot \ldots\ldots \cdot m_k$

Qin Jiushao

- Demostración: Si definimos $M_i = m/m_i$ para i=1,2,…,k se tiene: $m = m_i \cdot M_i$. Observad que M_i es el producto de todos los m_j con $j \neq i$, $j \in \{1,2,\ldots,k\}$.
- Es fácil ver que mcd(a,b)=1 y mcd(a,c)= 1 $\Longrightarrow$ mcd(a, b·c)=1 (ejercicio: probarlo), y lo mismo para el caso de más de dos factores, por lo tanto al ser los m_i coprimos dos a dos vemos que mcd(m_i , M_i)=1.
- De aquí, por la proposición 2 concluimos que existe n_i tal que:
- $n_i \cdot M_i \equiv 1 \pmod{m_i}$, para todo i=1,2,…,k.
- Consideremos el entero $x = \sum_{i=1}^{k} n_i \cdot M_i \cdot c_i$. Entonces se tiene:
- $x \equiv n_i \cdot M_i \cdot c_i \equiv 1 \cdot c_i \pmod{m_i}$, con lo cual este x resuelve el sistema.

- Para ver la unicidad módulo m, sean x e y soluciones del sistema.
- Entonces: $x \equiv c_i \equiv y \pmod{m_i}$, para todo i=1,2,…,r ⇨ $m_i \mid x - y$, para todo i=1,2,…,r. Como los m_i son coprimos dos a dos, el lema previo implica que $m \mid x - y$, es decir que $x \equiv y \pmod{m}$.
- Observación: La demostración permite calcular, en cualquier ejemplo dado, la solución del sistema. El paso más complejo es el cálculo de inversos para elementos coprimos con el módulo, cosa que se reduce fácilmente a resolver la identidad de Bézout pues: $a \cdot x \equiv 1 \pmod{m} \Leftrightarrow$
- $a \cdot x - 1 = m \cdot y$ (para algún entero y) $\Leftrightarrow a \cdot x - m \cdot y = 1$, que es la identidad de Bézout para a y –m, puesto que mcd(a, -m)=mcd(a,m)=1.

- Pequeño Teorema de Fermat: Sea p un número primo y a un entero no divisible por p. Entonces se tiene:
- $a^{p-1} \equiv 1 \pmod{p}$.
- Demostración: Consideramos R= {0,1,…., p-1}, que cumple que los p elementos de R representan todas las clases residuales módulo p. Como la condición a no divisible por p es equivalente a mcd(a , p) = 1 (pues p es primo) aplicando el lema de la clase anterior vemos que los elementos de:
- $a \cdot R = \{0, a, \ldots, (p-1)\, a\}$ también representan a todas las clases residuales mod p. Consideramos ahora conjuntos análogos pero con el 0 excluído:
- $R' = R \setminus \{0\}$ y $R'' = a \cdot R \setminus \{0\}$. Deducimos que tanto los p-1 elementos de R' como los p-1 elementos de R'' recorren las p-1 clases residuales módulo p distintas de la clase del 0. Por lo tanto si multiplicamos todos los elementos de ambos conjuntos tenemos la congruencia:
- $1 \cdot 2 \cdot \ldots\ldots \cdot (p-1) \equiv a \cdot (2\,a) \cdot \ldots\ldots \cdot (p-1)a \pmod{p}$ ⇨
- $(p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod{p}$. Podemos aplicar la cancelativa, pues (p-1)! es coprimo con p, y
- Obtenemos $1 \equiv a^{p-1} \pmod{p}$.

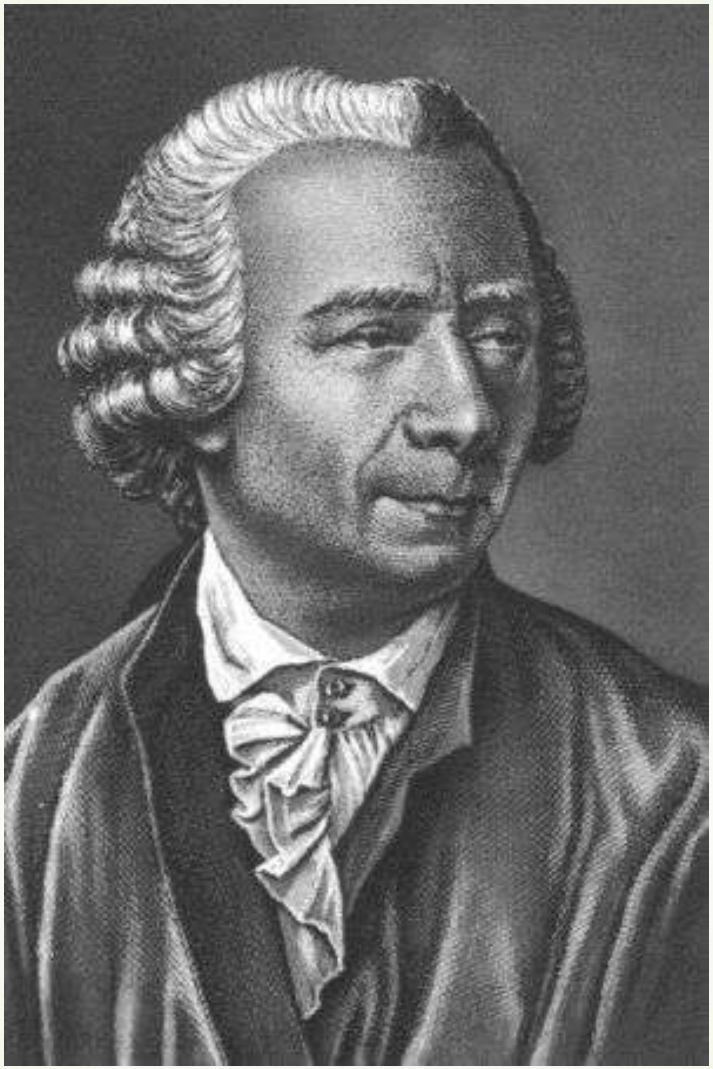
Pierre de Fermat

- Hemos visto en la proposición 3 que la propiedad de que un entero a tenga inverso módulo m equivale a mcd(a , m)=1.
- Obsérvese que el hecho de "tener un inverso módulo m" no depende del representante de una clase módulo n, pues si $a \equiv a' \pmod{m}$ y a tiene un inverso s módulo m, se tiene: $a \cdot s \equiv 1 \pmod{m} \Longrightarrow a' \cdot s \equiv 1 \pmod{m}$. En particular se sigue de la equivalencia mencionada que:
- Si $a \equiv a' \pmod{m}$ y $mcd(a,m)=1 \Longrightarrow mcd(a',m)=1$.
- Llamaremos a las clases residuales módulo m formadas por elementos que tienen inverso módulo m(o equivalentemente, por elementos coprimos con m) "clases inversibles módulo m".

- Definición: Función φ de Euler: Dado n > 1 entero, llamamos $\varphi(n)$ a la cantidad de clases residuales en $\mathbb{Z}$ / n $\mathbb{Z}$ que son inversibles módulo n (equivalentemente, que son coprimos con n).
- Si escogemos como representantes de las clases residuales a los enteros del intervalo [1, n], vemos que $\varphi(n)$ es igual a la cantidad de enteros en dicho intervalo que son coprimos con n.
- Ejemplo:
- (1) $\varphi(6) = 2$. De hecho, sólo los enteros 1 y 5 del intervalo [1,6] son coprimos con 6.
- (2) Si p es primo, $\varphi(p) = p-1$: esto se deduce de que la única clase no inversible módulo p es la de los enteros divisibles por p, es decir, la clase de los congruentes con 0 módulo p.

- Teorema de Euler: Sea n >1 y a entero con mcd(a,n)=1. Entonces se cumple: $a^{\varphi(n)} \equiv 1 \pmod{n}$.
- Demostración: Sea S ={ x_1 , x_2 , …., x_r }, formado por un representante de cada clase inversible módulo n, con #S = r = $\varphi(n)$. Comenzamos probando un análogo al lema de la clase pasada pero ahora para estas clases inversibles.
- Sea x ∈ S. Como mcd(x,n)=1 y mcd(a,n) = 1 ⟹ mcd(a·x, n)=1. Por lo tanto si multiplicamos a todos los elementos de S por a obtenemos:
- $a \cdot S = \{ a \cdot x_1 , a \cdot x_2 , \ldots, a \cdot x_r \}$ y vemos que todos los elementos de este conjunto son de nuevo coprimos con n. Además, # $a \cdot S = r = \varphi(n)$.
- Queremos ver que estos elementos representan todas las $\varphi(n)$ clases inversibles módulo n, para lo cual basta con ver que cada par de ellos no son congruentes módulo n. Para esto, aplicamos la propiedad cancelativa (es decir, el corolario a la Proposición 1), que nos dice que si:
- $a \cdot x_i \equiv a \cdot x_j \pmod{n}$, como mcd(a,n)=1 ⇨ $x_i \equiv x_j \pmod{n}$ ⇨ i = j.

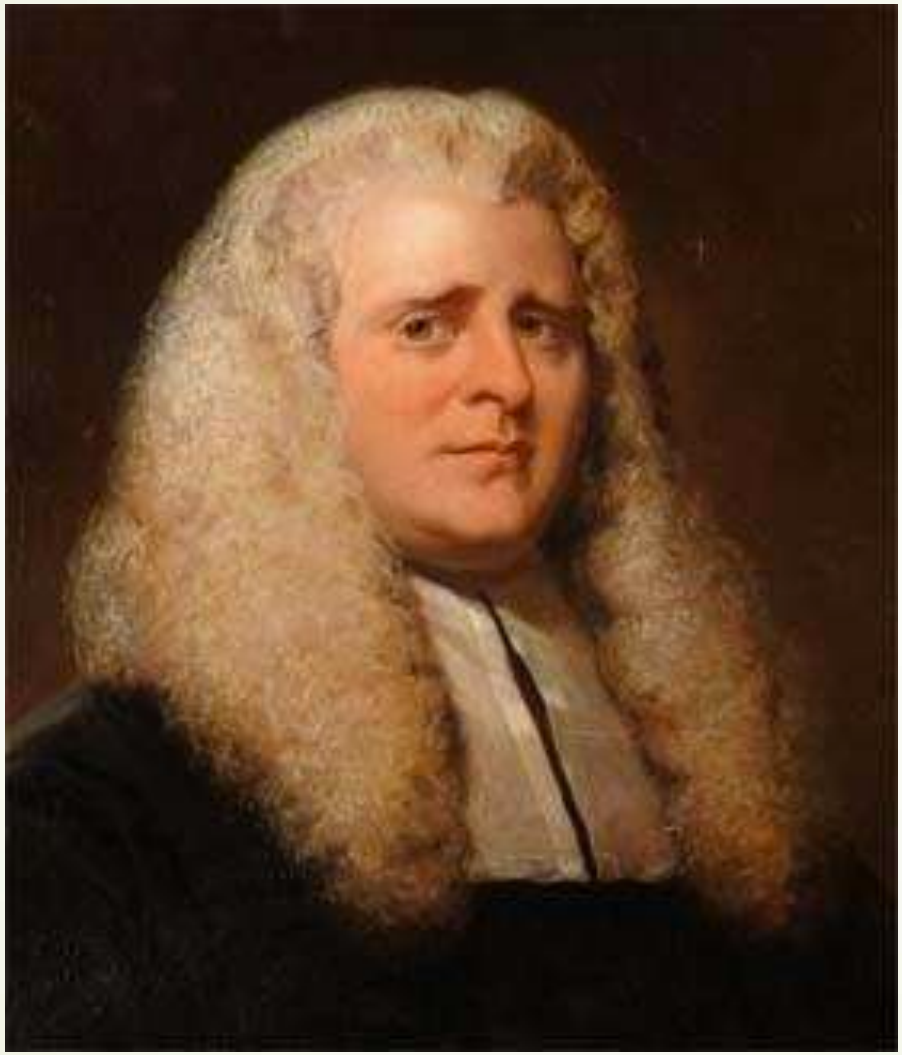
- Por lo tanto, tanto S como $a \cdot S$ están formados por un representante de cada clase inversible módulo n. De aquí se sigue que si multiplicamos todos sus elementos obtenemos la congruencia:
- $x_1 \cdot x_2 \cdot \ldots \cdot x_r \equiv a \cdot x_1 \cdot a \cdot x_2 \cdot \ldots \cdot a \cdot x_r \pmod{n}$, donde $r = \varphi(n)$.
- Si llamamos x al producto de los x_i , con i=1,2,…,r:
- $x \equiv a^{\varphi(n)} \cdot x \pmod{n}$.
- Como los x_i son coprimos con n, también x es coprimo con n, con lo cual podemos cancelarlo y obtenemos:
- $1 \equiv a^{\varphi(n)} \pmod{n}$.



Leonard Euler

- Teorema de Wilson: Sea p un número primo, entonces se tiene:
- $(p-1)! \equiv -1 \pmod{p}$
- Demostración: Si p = 2 la congruencia $1 \equiv -1 \pmod{2}$ prueba el teorema.
- Sea p primo impar. Como p es primo, ya vimos que las clases inversibles módulo p son todas las clases diferentes de la del 0, es decir, que tomando representantes en el intervalo [1, p] para la clases, se obtienen los representantes de las clases inversibles: 1, 2, …., p-1.
- Precisamente por ser inversibles, esto implica que para todo $i \in \{1,2,\ldots, p-1\}$ existe j en el mismo conjunto con: $i \cdot j \equiv 1 \pmod{p}$.
- Antes de proceder a emparejar a cada elemento con su inverso, tenemos que aislar el caso i = j, es decir, hallar aquellos i tales que: $i^2 \equiv 1 \pmod{p}$.

- Vemos que esta ecuación tiene dos soluciones triviales. i=1 y i = p -1:
- $1^2 \equiv 1 \pmod{p}$ y $(p-1)^2 \equiv (-1)^2 \equiv 1 \pmod{p}$.
- Veamos ahora que no posee más soluciones: Sea x tal que $x^2 \equiv 1 \pmod{p}$.
- Luego $x^2 - 1 \equiv 0 \pmod{p} \implies (x + 1) \cdot (x - 1) \equiv 0 \pmod{p}$. Equivalentemente, p divide al producto $(x + 1) \cdot (x - 1)$. Por el lema fundamental de la aritmética, concluímos que $p \mid x+1$ o $p \mid x-1$. Equivalentemente: $x \equiv -1 \equiv p-1 \pmod{p}$ o $x \equiv 1 \pmod{p}$.
- Luego, las únicas $i \in \{1, 2, \ldots, p-1\}$ que cumplen $i^2 \equiv 1 \pmod{p}$ son 1 y p-1.
- Sabemos por lo tanto que los elementos de {1,2, …., p-1} poseen un inverso módulo p en este mismo conjunto, y que sólo 1 y p-1 son inversos de sí mismos. Por lo tanto, al hacer el producto: $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = (p-1)!$ si lo miramos módulo p, excepto por 1 y p-1 el resto se emparejan en pares de inversos i , j con $i \cdot j \equiv 1 \pmod{p}$, de donde $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$.



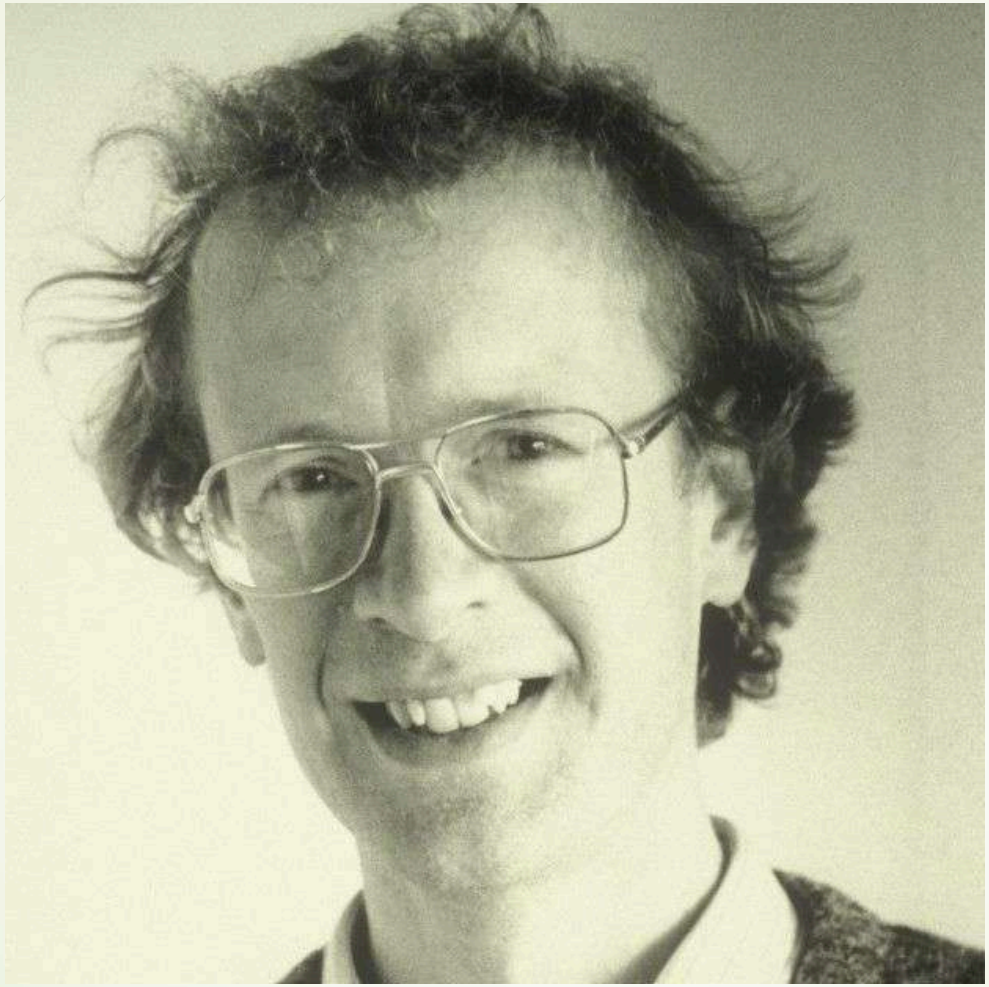
John Wilson

- Demostración alternativa del pequeño teorema de Fermat:
- El enunciado de este teorema nos dice que para p primo y a con p no dividiendo a a se tiene que $a^{p-1} \equiv 1 \pmod{p}$. Veamos que esto equivale a decir que: $a^p \equiv a \pmod{p}$. De hecho, para pasar de la primera a la segunda congruencia basta con multiplicar por a ambos miembros, y para pasar de la segunda a la primera con cancelar a, cosa que se puede hacer pues mcd(a, p)=1. Por lo tanto, el teorema equivale a probar que
- $$a^p \equiv a \pmod{p}.$$
- La ventaja de esta formulación es que para los a divisibles por también es cierta pues se reduce a $0^p \equiv 0 \pmod{p}$, con lo cual es una propiedad que cumplen todos los enteros a.

- Como es evidente que a= 0 cumple la propiedad y que si un entero la cumple su opuesto también, podemos reducirnos al caso a > 0. Queremos probarla para todo a sin restricciones, y eso hace que se pueda intentar demostrarla…. por inducción!
- Si a =1 es evidente. Supongamos que un a ≧ 1 cumple la proposición (hipótesis de inducción) y veamos que también es cierta para a+1.
- Aplicando la fórmula del binomio de Al-Karayí (llamada "de Newton"):
- $(a + 1)^p = \sum_{j=0}^{p} \binom{p}{j} a^j = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} a^j \equiv a^p + 0 + 0 + \ldots + 0 + 1 \pmod p$
- Aplicando la hipótesis de inducción $a^p \equiv a \pmod p$ concluimos que:
- $(a + 1)^p \equiv a + 1 \pmod p$. Esto acaba la prueba por inducción. Esta demostración es de L. Euler.

Al-Karayí

- Una diofántica con mucha historia: Fermat también dejó un resultado sin resolver (aunque en el margen del libro de Diofanto que estaba leyendo donde formuló el resultado él dijo haberlo resuelto, parece poco creíble…) en el año 1637 que se hizo muy famoso pues durante siglos nadie pudo resolverlo, hasta que en 1994 fue resuelto por el matemático inglés Andrew Wiles. Se le conoce como el Último Teorema de Fermat y dice lo siguiente:
- Teorema de Fermat-Wiles: Si n >2, la ecuación:
- $X^n + Y^n = Z^n$ no tiene soluciones enteras positivas.
- O, en el lenguaje que usó Fermat: Un cubo más un cubo no puede dar un cubo, una potencia cuarta más una potencia cuarta no puede dar una potencia cuarta, y así sucesivamente.
- Por cierto, los primeros casos resueltos fueron n=4 (Fermat) y n=3 (Euler).
- Observad que para n=2 es FALSO, por ejemplo: $3^2 + 4^2 = 5^2$, $12^2 + 5^2 = 13^2$.



Andrew Wiles