Índice

Introducción.....2

Capítulo 1. Divisibilidad.....3

1.1. Definición y propiedades básicas..... 3

1.2. División entera y algoritmo de Euclides.....4

1.3. Los números primos. El teorema fundamental de la Aritmética..... 7

1.3. Aplicaciones inmediatas del TFAr..... 9

Ejercicios..... 12

Capítulo 2. Congruencias..... 13

2.1 Definición y propiedades básicas..... 13

2.2. Reglas de divisibilidad.....14

2.3. Anillos de restos..... 16

2.4. Teoremas de Euler, Fermat, Lagrange, Wilson y Wolstenholme.....19

Introducción

En este curso de teoría de números abordaré una pequeña introducción, en general suficiente para resolver problemas de cierta complejidad, pero sin llegar a matemática avanzada. Partiremos de una base mínima, en la que ya están construidos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ pero no serán necesarios conocimientos de cálculo diferencial ni integral, al menos hasta nuevo aviso y sólo en caso de demanda al respecto.

En el primer capítulo expondré nociones básicas de divisibilidad, normalmente incluidas en el currículo de la ESO, aunque tratadas sólo superficialmente, lo mínimo para que el alumno pueda operar con fracciones. Aquí se tratarán en profundidad y por supuesto con demostraciones.

En el segundo algo sobre anillos de restos (también conocido como *congruencias*), ecuaciones modulares y diofánticas.

Por último trataré las funciones aritméticas, en especial las multiplicativas, que se considera el último escalón antes de meterse de lleno en la teoría de números analítica avanzada.

Capítulo 1. Divisibilidad

En este curso se considerará que el conjunto de los números naturales es {1,2,3,...}, es decir, que el 0 *no* es natural.

1.1. Definición y propiedades básicas.

Definición: Sean a y b dos números enteros. Si existe otro entero c tal que $ac=b$ se dice que a divide a b, que a es un divisor de b o que b es múltiplo de a. Se representa $a|b$.

Inmediatamente surgen las primeras propiedades, algunas más conocidas que otras.

Proposición: Para enteros cualesquiera a, b y c se cumple:

1. Si $a|b$ y $b\neq 0$ entonces $|a|\leq|b|$.
2. Si $a|b$ y $b|c$ entonces $a|c$.
3. Si $a|b$, entonces $a|bc$.
4. $|a|$ divide a $|b|$ si y sólo si $a|b$.
5. Si $a|b$ y $b|a$ entonces $|a|=|b|$.
6. Si $a|b$, entonces $a|(b+c)\Leftrightarrow a|c$.
7. $a|0$, $1|a$
8. Si $ab|ac$ y $a\neq 0$ entonces $b|c$.

Demostración:

1. En estas condiciones, existe $k\in\mathbb{Z}$ tal que $ak=b$. Como $b\neq 0$, entonces $k\neq 0$, y por tanto $|k|\geq 1$. Entonces $|b|=|ak|\geq|a|$.
2. Existen $r, s\in\mathbb{Z}$ tales que $ar=b, bs=c$, de donde $a(rs)=c$.
3. Es claro que $b|bc$. Ahora aplíquese el apartado anterior.
4. Si $|a|$ divide a $|b|$ entonces existe $k\in\mathbb{Z}$ tal que $k|a|=|b|$. Si a tiene el mismo signo que b, será $ka=b$, y si no, $-ka=b$. Recíprocamente, si $a|b$, existe $k\in\mathbb{Z}$ tal que $ka=b$ y por tanto $|k||a|=|b|$.
5. Por el apartado anterior tenemos que $|a|$ y $|b|$ se dividen el uno al otro y por el apartado 1, queda $|a|=|b|$.
6. Si $a|b$ y $a|c$ existen $r, s\in\mathbb{Z}$ tales que $b=ar$, $c=as$, y por tanto $b+c=a(r+s)$. Para el recíproco basta darse cuenta de que $c=(b+c)+(-b)$.
7. $a\cdot 0=0$, $1\cdot a=a$

8. Existe $d \in \mathbb{Z}$ tal que $adb = ac$.

1.2. División entera y algoritmo de Euclides.

Ahora introducimos la división euclídea, que nos permitirá demostrar el teorema fundamental de la aritmética. Pero antes es necesario probar un resultado estructural de $\mathbb{Z}$, que es el que permite en el fondo efectuar tal división. Diremos que un subconjunto $A \subseteq \mathbb{Z}$ es acotado si existe $n \in \mathbb{N}$ tal que $|a| < n \; \forall a \in A$. Pues bien,

Proposición 1.2.1: Todo subconjunto acotado de $\mathbb{Z}$ es finito.

Demostración: Sea A un subconjunto acotado de $\mathbb{Z}$, y sea $n \in \mathbb{N}$ tal que $|a| < n \; \forall a \in A$. Sea $B = \{a + n, a \in A\}$. Es obvio que $card(A) = card(B)$ y, como $B \subseteq \{1, 2, \ldots, 2n\}$, está claro que $card(A) \leq 2n$.

Teorema. División euclídea. Sean $a, b \in \mathbb{N}$ con $a < b$. Si $a \nmid b$ existen naturales q, r únicos tales que $0 < r < a$ y $b = aq + r$.

Demostración: Sea $A = \{ak, k \in \mathbb{N}\}$, que es infinito (pruébelo el lector). Por la proposición anterior no está acotado, y como todos sus elementos son positivos, existe $k \in \mathbb{N}$ tal que $ak > b$. Sea $B = \{k \in \mathbb{N}, ak > b\}$. Éste es un subconjunto no vacío de $\mathbb{N}$ y por tanto tiene un primer elemento q'; además, como $a < b$ es $q' > 1$. Sea $q = q' - 1$. Por la elección de q, es claro que $aq \leq b$, y como $a \nmid b$, $aq < b$. Además, si hacemos $r = b - aq$, es $r > 0$, y si fuera $r \geq a$ tendríamos $b = aq + r \geq aq + a = a(q+1) = aq' > b$, una contradicción; por tanto $r < a$. Supongamos ahora que existen q_0, r_0 con las condiciones indicadas. Entonces $q_0 \notin B$ y como $a(q_0 + 1) = aq_0 + a > aq_0 + r_0 = b$, resulta que $q_0 + 1 \in B$. Es claro que los elementos de B son todos consecutivos, así que $q_0 = q$. Se sigue fácilmente que $r_0 = r$.

Surge ahora la necesidad de extender este resultado a $\mathbb{Z}$.

Teorema 1.2.2: Sean $a, b \in \mathbb{Z}$. Si $a \nmid b$ y $a \neq 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $0 < r < |a|$ y $b = aq + r$.

Demostración: Para la existencia, considérense los casos:

- $b > a > 0$. Ya probado.
- $a > b > 0$. Tómese $q = 0, r = b$.
- $-b > -a > 0$. Aplicando el teorema anterior, sabemos que existen $q, r \in \mathbb{N}$ únicos tales que $-b = -aq + r$ y $0 < r < -a = |a|$. Entonces $b = aq - r = a(q+1) + (-a - r)$. Por otro

lado $0=a-a>a+r>a$, por lo que $0<-a-r<-a=|a|$.

- $-a>-b>0$. Basta tomar $q=-1, r=b-a$.
- $-b>a>0$. Queda $-b=aq+r \Rightarrow b=a(-q)-r=a(-q-1)+(a-r)$. Por otro lado $0=a-a<a-r<a$.
- $b>-a>0$. Ahora $b=-aq+r=a(-q)+r$.

Para la unicidad supongamos que existen dos pares q, r y q', r' con las propiedades exigidas. Entonces $aq+r=aq'+r'$, es decir, $a(q-q')=r'-r$. Por tanto $a|(r'-r)$, y como $|a|>|r-r'|$ debe ser $r-r'=0$, y entonces $r=r'$ y $q=q'$.

Los números r y q a los que se refiere este teorema se denominan respectivamente *resto* y *cociente* de la división, que permite hallar mediante un sencillo algoritmo el máximo común divisor de dos enteros. Lo definimos con precisión.

Definición 1.2.3: Dados dos enteros a, b se dice que d es *un* máximo común divisor de a y b (mcd en adelante), si $d|a$, $d|b$ y para cualquier otro entero d' que sea divisor de a y de b se tiene que $|d'|\leq|d|$.

Es inmediato el siguiente resultado:

Proposición 1.2.4: Sean $a, b\in\mathbb{Z}$. Si d y d' son mcd de a y b, entonces $|d|=|d'|$.

Dados dos enteros no nulos a la vez, la existencia de su mcd está garantizada, ya que dos números enteros siempre tienen un divisor común (a saber, el 1) y el conjunto de los divisores de un número no nulo está acotado. La proposición anterior implica que existen dos mcd, uno positivo y otro negativo. En adelante, salvo que se especifique lo contrario asumiremos que *el* mcd de dos enteros a, b es el positivo de los dos que hay, y escribiremos $d=(a, b)$ para indicar que d es el mcd de a y b.

Ahora damos una caracterización importante del mcd.

Teorema 1.2.5: Sean $a, b, d\in\mathbb{N}$. Son equivalentes:

1. $d=(a, b)$
2. Todo divisor común a a y b divide a d.

Demostración (incompleta): La implicación $2\Rightarrow 1$ es muy sencilla: si $d'|a$ y $d'|b$, por hipótesis $d'|d$ y entonces $|d'|\leq|d|$. Pero para demostrar el recíproco necesitamos antes describir el algoritmo de Euclides y probar la identidad de Bezout.

Sean a, b números naturales, con $a > b$. Si $b|a$ es obvio que $(a, b) = b$. Si no, podemos efectuar la división euclídea y escribir $a = qb + r$. Observamos que cualquier número que divida a a y a b dividirá también a r, y además $r < b$. Esto sugiere el siguiente algoritmo[1], llamado *algoritmo de Euclides*:

Entrada: Dos números naturales a, b con $a > b$.

Funciones auxiliares: Dados dos naturales x, y con $x > y$, $y \nmid x$, $R(x, y)$ será el resto de la división de x entre y, y $Q(x, y)$ su cociente.

$r_0 = a$;

$r_1 = b$;

$n = 1$;

mientras $r_n \nmid r_{n-1}$,

$q_n = Q(r_{n-1}, r_n)$;

$r_{n+1} = R(r_{n-1}, r_n)$;

$n = n + 1$;

fin mientras

Salida: r_n.

Primero, obsérvese que la sucesión $\{r_n\}$ es una sucesión decreciente de números naturales, lo que muestra que el algoritmo acaba, es decir, que en algún momento $r_n | r_{n-1}$; Sea m el máximo valor que alcanza n, y sea $d = r_m$, es decir, la salida del algoritmo. Segundo, como hemos apuntado antes, cualquier divisor de r_{n+1} divide también a r_n y a r_{n-1} (para todo n entre 1 y $m-1$). Pero $d | r_{m-1}$, y por tanto $d | r_{m-2}$, y por tanto $d | r_{m-3}$, etc. Entonces $d | a$ y $d | b$. Además, si $d' | a$ y $d' | b$, $d' | r_2$, etc y vemos que $d' | d$. Esto, junto con la implicación ya probada del teorema, demuestra que $d = (a, b)$.

Quizá se haya preguntado el lector por qué nos hemos molestado en "guardar" la sucesión $\{q_n\}$. Ahora mismo hallará la respuesta. Podemos escribir:

$$r_0 = q_1 r_1 + r_2$$

$$r_1 = q_2 r_2 + r_3$$

$$\vdots$$

$$r_{m-2} = q_{m-1} r_{m-1} + d$$

1 Para el lector sin unos mínimos conocimientos de programación, doy aquí una explicación del algoritmo. Dividimos *a* entre *b,* obteniendo un cociente *q* y un resto *r*. Después dividimos *b* entre *r* obteniendo otro cociente y otro resto. Seguimos así, hasta que la división sea exacta y formamos dos sucesiones, una con los cocientes y otra con los restos. La parte comprendida entre las palabras "mientras" y "fin mientras" es la que se repite hasta que la división sea exacta. No pretendo sustituir el algoritmo con esta explicación, sino complementarlo.

o equivalentemente,

$r_2 = r_0 - q_1 r_1$

$r_3 = r_1 - q_2 r_2$

$\vdots$

$d = r_{m-2} - q_{m-1} r_{m-1}$.

Sustituyendo, podemos obtener r_3 en función de r_0 y r_1 (concretamente, $r_3 = r_1 - q_2(r_0 - q_1 r_1) = (1 + q_1 q_2) r_1 - q_2 r_0$). Y también r_4, etc. También, por supuesto, d. Hemos probado:

Teorema (identidad de Bezout): Sean $a, b \in \mathbb{N}$. Sea $d = (a, b)$. Entonces existen números enteros x, y tales que $d = ax + by$.

Ahora podemos completar la demostración del teorema anterior. Si $d = (a, b)$, $d' | a$ y $d' | b$, escribimos $ax + by = d$, lo que implica inmediatamente que $d' | d$.

Es necesario, aunque fácil y algo tedioso, extender estos teoremas para valores enteros (quizá distintos de cero en algunos casos) de a, b. El lector no convencido puede intentarlo como ejercicio. Viene bien para asimilar las características del algoritmo de Euclides.

1.3. Los números primos. El teorema fundamental de la Aritmética.

Presento aquí una de las familias de objetos matemáticos más caóticas y fascinantes: los números primos.

Definición 1.3.1: Sea $p \in \mathbb{N}$. Se dice que p es primo si $p \neq 1$ y los únicos divisores naturales de p son 1 y p. Se dice que un entero p es primo si $|p|$ es natural primo (el 0 no es primo). Salvo que se indique lo contrario, al decir que p es primo, se sobreentenderá que p es natural. Si un natural distinto de 1 no es primo, se dice que es compuesto.

Definición 1.3.2: Sean a, b enteros. Se dice que son primos entre sí o que a es primo con b si $(a, b) = 1$.

Proposición 1.3.3: Si los enteros a, b son primos entre sí, entonces existen x, y enteros tales que $ax + by = 1$.

Demostración: Es consecuencia inmediata de la identidad de Bezout.

Proposición 1.3.4: Si p es primo, $a\in\mathbb{Z}$, y $p\nmid a$, entonces a y p son primos entre sí.
Demostración: Sea $d=(a,p)$. Entonces $d\in\{1,p\}$, por ser p primo. Como $p\nmid a$, $d=1$.

Teorema 1.3.5: Sea p un primo y $a,b\in\mathbb{Z}$. Si $p|ab$ entonces $p|a$ ó $p|b$.
Demostración: En las condiciones del teorema, existe un entero c tal que $cp=ab$. Supongamos que $p\nmid a$. Entonces, en virtud de lo anterior, existen dos enteros x,y tales que $ax+py=1$. Entonces, $cpx=abx=(1-py)b$, o sea, $p(cx+by)=b$, por lo que $p|b$.

Es fácil probar por inducción que si un primo divide a un producto de enteros, divide al menos a uno de ellos. Ya estamos en condiciones de demostrar el teorema fundamental de la aritmética.

Proposición 1.3.6: Todo número natural mayor que 1 se puede expresar como producto de primos.
Demostración: Razonamos por inducción. El número 2 cumple el enunciado por ser él mismo primo. Sea $n\in\mathbb{N}$ y supongamos que todo natural menor que n (y mayor que 1) se puede expresar como producto de primos. Si n es primo no hay nada que probar, y si no, al ser mayor que 1, será compuesto, es decir, existen dos naturales a,b mayores que 1 tales que $ab=n$. Por la hipótesis de inducción, estos dos naturales se pueden expresar como producto de primos, y por tanto n también.

Teorema fundamental de la Aritmética (TFAr): La descomposición a la que alude la proposición anterior es única para cada natural mayor que 1, salvo en el orden de los primos. Más precisamente, si $n=\prod_{k=1}^{r} p_k=\prod_{k=1}^{s} q_k$, donde $\{p_k\}$ y $\{q_k\}$ son familias de primos no necesariamente distintos, entonces $r=s$ y existe una aplicación biyectiva σ de $\{1,2,\ldots,r\}$ en sí mismo tal que para cada $k\in\{1,2,\ldots,r\}$, $p_k=q_{\sigma(k)}$.
Demostración: Sea n un natural con las dos descomposiciones citadas en el enunciado. Por simetría podemos suponer $r\le s$. Se tiene que $p_1|\prod_{k=1}^{s} q_k$, y como p_1 es primo existe $\sigma(1)\in 1,2,\ldots,s$ tal que $p_1|q_{\sigma(1)}$. Elegimos el menor posible. Al ser $q_{\sigma(1)}$ primo debe ser $p_1=q_{\sigma(1)}$ y queda $\prod_{k=2}^{r} p_k=\prod_{\substack{1\le k\le s\\ k\neq\sigma(1)}} q_k$. Razonando del mismo modo con todos los primos p_k

llegamos a que $1=\prod_{\substack{1\le k\le s\\ k\neq\sigma(1)\\ k\neq\sigma(2)\\ \vdots\\ k\neq\sigma(r)}} q_k$, de donde se ve claramente que $r=s$. La aplicación biyectiva queda así correctamente construida y el teorema probado.

La importancia de este teorema radica en que si tenemos por ejemplo la descomposición $72=2^3\cdot 3^2$, eso quiere decir que *ningún otro primo* puede dividir a 72.

1.3. Aplicaciones inmediatas del TFAr.

El TFAr permite definir funciones[2] sobre los números naturales que resultan de gran utilidad a la hora de formalizar ciertos razonamientos. Llamaremos en adelante P al conjunto de los números primos (naturales).

Espectro primo: Si $n\in\mathbb{N}$, se define $S(n)=\{p\in P, p|n\}$.

Función *p*-multiplicidad: Para cada $p\in P$ definimos la función m_p de este modo: $m_p(n)$ es el número de veces que aparece p en la factorización de n. Así, podemos escribir $n=\prod_{p\in P} p^{m_p(n)}=\prod_{p\in S(n)} p^{m_p(n)}$. Nótese que $m_p(n)>0\Leftrightarrow p\in S(n)$.

Función longitud: Para cada $n\in\mathbb{N}$ definimos $l(n)=\sum_{p\in P} m_p(n)=\sum_{p\in S(n)} m_p(n)$.

Se deja como ejercicio comprobar que para todo par de naturales a, b:

- $m_p(ab)=m_p(a)+m_p(b)$ para todo $p\in P$.
- Si $p\in P$, entonces $m_p(a+b)\ge\min(m_p(a), m_p(b))$ y si $m_p(a)\neq m_p(b)$ entonces se alcanza la igualdad.
- $l(ab)=l(a)+l(b)$
- $S(ab)=S(a)\cup S(b)$. En particular $S(a^n)=S(a)$ para todo $n\in\mathbb{N}$.
- $S(a)\cap S(b)\subseteq S(a+b)$

Así como estas funciones se "comportan bien" con los productos, resultan terriblemente caóticas con las sumas, siendo hasta la fecha imposible de determinar de un modo sencillo por ejemplo $l(a+b)$ en función de $l(a), l(b), a$ y b. De hecho, un descubrimiento al respecto,

2 Es posible que en la literatura estas funciones no se usen, o tengan otros símbolos y nombres.

seguramente traería como consecuencia la resolución de muchos de los problemas más célebres que hay planteados en teoría de números. Por ejemplo, Goldbach planteó el siguiente problema a Euler en una carta: "Demostrar que todo número entero mayor que 2 es la suma de tres[3] primos". Aunque hay fundadas sospechas de que esto es cierto, el problema lleva más de dos siglos abierto, y se conoce como la conjetura de Goldbach. Obsérvese que el problema se podría formular de este modo.

"Demostrar que $a+b+c$ recorre todos los números naturales mayores que 2 cuando $l(a)\leq 1$ y $l(b)\leq 1$ y $l(c)\leq 1$ ".

Podemos citar también en este sentido la conjetura de los primos de Mersenne. Los primos de Mersenne son aquéllos que se pueden escribir como 2^n-1. Es fácil probar que para que este número sea primo es necesario que n sea primo. Así, para los primeros primos tenemos $2^2-1=3$, $2^3-1=7$, $2^5-1=31$, $2^7-1=127$ pero enseguida nos topamos con una excepción: $2^{11}-1=2047=23\cdot 89$. El primo de Mersenne más grande conocido hasta la fecha es $2^{32582657}-1$, que tiene cerca de diez millones de cifras, descubierto el 4 de septiembre de 2006. Se sospecha, pero no se ha demostrado, que hay infinitos primos de este tipo. Imagínese el lector cuánto facilitaría las cosas poder descomponer la expresión $l(2^p-1)$.

Quizá haya observado que los factores 23 y 89 de $2^{11}-1$ tienen la propiedad de que al restarles 1 da justamente un múltiplo de 11. Este hecho no es casual, sino que es generalizable a todos los divisores primos (y también a los no primos) de un número de la forma 2^p-1. Estaremos en condiciones de probarlo cuando estudiemos las congruencias.

En la wikipedia hay bastante información -sobre todo en inglés- acerca de éstas y de otras conjeturas.

Proposición 1.4.1: Sean a, b naturales. Los siguientes enunciados son equivalentes:

1. a y b son primos entre sí.
2. $S(a)\cap S(b)=\varnothing$.

Demostración: La implicación $1\Rightarrow 2$ es evidente. Supongamos entonces 2 y hagamos $d=(a,b)$. Si algún primo p dividiera a d, tendríamos que $p|a$ y $p|b$, en contra de 2. Por tanto $d=1$.

Proposición 1.4.2: Si $a\in\mathbb{N}$, $(a,a+1)=1$.

Demostración: Sea $d=(a,a+1)$. Entonces $d|a$ y $d|a+1$, por tanto $d|1$ y $d=1$.

Sobre el conjunto de los números primos y su distribución a lo largo de $\mathbb{N}$, nos

3 En aquella época se consideraba al 1 como número primo.

conformaremos de momento con el siguiente resultado, ya conocido por los griegos:

Teorema 1.4.3: El conjunto de los números primos es infinito.

Demostración: Sea $n\in\mathbb{N}$. Probaremos que existe algún primo mayor que n. El número $n!+1$ es primo con $n!$, y por tanto $m_p(n!+1)=0$ para cualquier primo $p\leq n$. Así, todos los divisores primos de $n!+1$ son mayores que n.

Proposición 1.4.4: Sean $a,b\in\mathbb{N}$. Son equivalentes:

1. $b|a$
2. $m_p(b)\leq m_p(a)$ para todo $p\in P$.
3. $m_p(b)\leq m_p(a)$ para todo $p\in S(b)$.

Además, cualquiera de ellos implica que $S(b)\subseteq S(a)$.

Demostración: Sea $c=\frac{a}{b}\in\mathbb{Q}$. Aplicando el TFAr tenemos que $c=\prod_{p\in P} p^{m_p(a)-m_p(b)}$. Es claro que $c\in\mathbb{N}$ si y sólo si $m_p(a)\geq m_p(b)$ para todo $p\in P$. Vemos así que 1 y 2 son equivalentes.
Es obvio que 2 y 3 también son equivalentes, puesto que si $p\in P-S(b)$, entonces $m_p(b)=0$.
Para demostrar la última parte tomamos $p\in S(b)$. Deducimos sucesivamente $p|b$, $p|a$ y $p\in S(a)$.

Teorema 1.4.5: Sean $a,b,c\in\mathbb{N}$. Si $a|bc$ y $(a,b)=1$ entonces $a|c$.

Demostración: Sea $p\in S(a)$. Como $S(a)\cap S(b)=\emptyset$, $p\notin S(b)$, es decir, $m_p(b)=0$. Entonces $m_p(a)\leq m_p(b)+m_p(c)=m_p(c)$.

Teorema 1.4.6: Sean $a,b\in\mathbb{N}$. Entonces $(a,b)=\prod_{p\in S(a)\cap S(b)} p^{\min(m_p(a),m_p(b))}$. O, lo que es lo mismo, $m_p((a,b))=\min(m_p(a),m_p(b))$ para todo $p\in P$.

Demostración: Se sigue inmediatamente de la proposición anterior.

Ésta es la forma de calcular el mcd que generalmente se estudia en la infancia: "Factores comunes con el menor exponente".

Teorema 1.4.7: Sea $p\in P$. Entonces $\sqrt{p}\notin\mathbb{Q}$.

Demostración: Supongamos que $\sqrt{p}\in\mathbb{Q}$. Entonces existen $a,b\in\mathbb{N}$ tales que $\sqrt{p}=\frac{a}{b}$, es decir, $b^2p=a^2$. Entonces $2m_p(b)+1=2m_p(a)$, una contradicción, ya que el miembro izquierdo es

impar y el derecho par.

Del mismo modo se puede probar que $\sqrt{n}\in\mathbb{Q}$ si y sólo si $m_p(n)$ es par para todo $p\in P$, o lo que es lo mismo, si y sólo si n es producto de cuadrados de primos. En este caso es claro que $\sqrt{n}\in\mathbb{N}$, por lo que

Teorema 1.4.8: Sea $n\in\mathbb{N}$. La raíz cuadrada positiva de n es natural o irracional.

También de modo análogo se puede ver:

Teorema 1.4.9: Sean $m, n\in\mathbb{N}$. El número $\sqrt[m]{n}$ es natural o irracional.

Ejercicios*

1. Encontrar dos enteros x, y tales que $36x+49y=1$.

2. Sean $a,b\in\mathbb{N}$, $x,y\in\mathbb{Z}$. Probar que si $a\nmid b$, $b\nmid a$ y $ax+by=(a,b)$ entonces los enteros x, y tienen signo distinto.

3. Sea $n\in\mathbb{N}$. Probar que en todo conjunto con n enteros consecutivos hay un múltiplo de *n*.

4. Sean $a,b\in\mathbb{N}$. Probar que existe un único natural, que denotaremos por $[a,b]$, que es múltiplo de a y de b, y que divide a cualquier otro múltiplo común de a y de b. Probar que $ab=(a,b)[a,b]$. Hallar, para cada $p\in P$ el valor de $m_p([a,b])$.

5. Sean $a,b,c\in\mathbb{N}$. Probar que si $c|ab$ entonces existe al menos un par de naturales c_a, c_b tales que $c_a|a$, $c_b|b$ y $c=c_a c_b$. ¿Se pueden siempre elegir c_a y c_b primos entre sí? Probar que si $(a,b)=1$ la respuesta es afirmativa y este par es único.

6. Sean $a,b,c,d\in\mathbb{N}$. Probar que si $ab=cd$ entonces $a+b+c+d$ es compuesto.

7. Sean $a,b\in\mathbb{N}$. Probar que $(a,b)=(a+b,[a,b])$.

---

* Los ejercicios podrían contener definiciones, notaciones o resultados usados más adelante en la teoría.

Capítulo 2. Congruencias.

Empezamos este capítulo probando un resultado sin interés teórico, ya que se trata de un simple caso particular, pero servirá para ilustrar el resto del contenido.

Vamos a suponer que $a, b \in \mathbb{N}$. Si al dividir estos números entre 7 da como resto 6 y 3 respectivamente, entonces al dividir $a+b$ entre 7 da de resto 2 y al dividir ab, 4. En efecto, aplicando la división euclídea podemos escribir que $a = 7q+6$ y $b = 7q'+3$.

Entonces es fácil ver que $a+b = 7(q+q'+1)+2$ y $ab = 7(7qq'+6q'+3q+2)+4$. Lo interesante de esto es que en particular, para $a=6$ y $b=3$, también se cumple, obviamente. Esto sugiere que podemos operar con los restos de las divisiones por 7 como si fueran los dividendos. Es decir, si para cada $n \in \mathbb{N}$ definimos $f_7(n)$ como el resto de dividir n entre siete[4], se tendría (y se tiene, como probaremos en breve):

$$f_7(mn) = f_7(f_7(m) f_7(n))$$
$$f_7(m+n) = f_7(f_7(m) + f_7(n))$$

En el método que hemos usado para probar el resultado anterior no parece muy relevante el hecho de que el divisor sea 7, parece como si se hubiera podido probar para cualquier otro número, y de hecho así es.

Para evitar tratar casos separadamente, en adelante, si $a|b$, diremos que el resto de la división euclídea de b entre a es 0 y el cociente $\frac{b}{a} \in \mathbb{Z}$.

2.1. Definición y propiedades básicas.

Definición 2.1.1: Sean $a, b, m \in \mathbb{Z}$, con $m \geq 1$. Se dice que $a = b + (m)$ (y se lee "a es congruente con b módulo m") si $m|(b-a)$.

Teorema 2.1.2: Sean $a, b, m \in \mathbb{Z}$ con $m \geq 1$. Son equivalentes:

1. $a = b + (m)$
2. El resto de la división euclídea de a entre m es el mismo que el de la división b entre m.

Demostración: Aplicando la división euclídea tenemos que $a = qm + r$, $b = q'm + r'$. Si $r = r'$ entonces $b - a = (q'-q)m$. Recíprocamente, si $m|(b-a)$ entonces $m|[m(q'-q)+(r-r')]$, y por tanto $m|(r-r')$. Como $|(r-r')| < m$ resulta que $r = r'$.

Corolario: La relación "ser congruente módulo *m*" es de equivalencia para todo $m \geq 1$, e induce

4 La notación f_7 ni es estándar ni se usará en el resto del libro. Sólo se introduce aquí con fines didácticos.

una partición de $\mathbb{Z}$ en m clases. Los enteros $\{0,1,2,\ldots,m-1\}$ están en clases diferentes, y las clases a las que pertenecen estos números son todas las que hay.

Teorema 2.1.3: Sean $a,b,a',b',m\in\mathbb{Z}$ con $m\geq 1$. Supongamos que $a=a'+(m)$ y $b=b'+(m)$. Entonces $a+b=a'+b'+(m)$ y $ab=a'b'+(m)$.

Demostración: Tenemos que $m|(a-a')$ y $m|(b-b')$. Por tanto divide a la suma, es decir, $m|(a+b-a'-b')$. Por otra parte $ab-a'b'=(a-a')b+a'(b-b')$, y por tanto $m|(ab-a'b')$.

Corolario: Con la notación y condiciones del teorema anterior, si f es un polinomio con una variable y coeficientes enteros, entonces $f(a)=f(a')+(m)$.

Proposición 2.1.4: Sea $a\in\mathbb{Z}$, $m\geq 1$. Si $(a,m)=1$ entonces existe $a'\in\mathbb{Z}$ tal que $aa'=1+(m)$.

Demostración: Por la identidad de Bezout existen enteros a',b tales que $aa'+bm=1$, y entonces $(aa'-1)|m$.

Proposición 2.1.5: Sean $a,b,c\in\mathbb{Z}$, $m,n\geq 1$. Se dan las siguientes propiedades:

1. $a=0+(m)\Leftrightarrow m|a$
2. $b=c+(m)\Leftrightarrow ab=ac+(am)$ si $a\geq 0$
3. Si $a=b+(m)$ y $a=b+(n)$ entonces $a=b+([m,n])$. En particular, si $(m,n)=1$ entonces $a=b+(mn)$.
4. Si $a=b+(mn)$ entonces $a=b+(m)$ y $a=b+(n)$.

Demostración: Es muy sencilla para los cuatro enunciados y se deja como ejercicio al lector. Para el tercero, se recomienda revisar el ejercicio 4 del primer capítulo.

2.2. Reglas de divisibilidad.

En esta sección se describirán y demostrarán las reglas de divisibilidad que habitualmente se estudian en la educación obligatoria, y se añadirán otras; todo ello como una aplicación de las congruencias. Antes definiremos y justificaremos la representación decimal de los naturales. Con muy poco esfuerzo adicional se podría haber hecho lo mismo para sistemas de numeración en otras bases, pero no considero que este punto tenga demasiada relación con el contenido del libro y lo he pasado por alto. Denotaremos por 9 al número 1+1+1+1+1+1+1+1+1 y 10 será 9+1.

Teorema 2.2.1: Sea $a\in\mathbb{N}$. Entonces existen $n\geq 0$, y enteros $a_0,\ldots,a_n$ que cumplen:

- $a=\sum_{k=0}^{n} 10^k a_k$
- $0 \le a_k \le 9 \; \forall \, k \in \{0,\ldots,n\}$
- $a_n \neq 0$

Demostración: Razonemos por inducción. El resultado es obvio si $a \le 9$. Si no, podemos escribir $a = 10\,q + a_0$, con $1 \le q < a$ y $0 \le a_0 \le 9$. Así, por la hipótesis de inducción, podemos escribir que $q=\sum_{k=1}^{n} 10^{k-1} a_k$ y por tanto $a=\sum_{k=0}^{n} 10^k a_k$.

Definición 2.2.2: Dado $a \in \mathbb{N}$, la (n+1)-upla de enteros cuya existencia se asegura en el teorema anterior se llama representación decimal de a. Los enteros de la $(n+1)$-upla son las cifras de a. Se considera generalmente que a_0 es la última cifra y a_n la primera.

Proposición 2.2.3: Si el natural a tiene una representación decimal con n cifras, entonces $10^{n-1} \le a < 10^n$. En consecuencia, todas las representaciones de a tienen el mismo número de cifras.

Demostración: Sea $a=\sum_{k=0}^{n-1} 10^k a_k$. Como $a_{n-1} \neq 0$, tenemos que $a \ge 10^{n-1}$. Por otra parte, $\sum_{k=0}^{n-1} 10^k a_k \le \sum_{k=0}^{n-1} 9 \cdot 10^k = (10-1)\sum_{k=0}^{n-1} 10^k = 10^n - 1$.

Teorema 2.2.4: La representación decimal de un número natural es única.

Demostración: Ya hemos visto que si hay dos, tendrán el mismo número de cifras. Supongamos entonces que $\sum_{k=0}^{n-1} 10^k a_k = \sum_{k=0}^{n-1} 10^k b_k$. Sea $j \in \{0,\ldots,n-1\}$ el mayor posible, con tal que $a_j \neq b_j$. Entonces se cancelan todos los sumandos de n-1 a j+1 y queda $\sum_{k=0}^{j} 10^k a_k = \sum_{k=0}^{j} 10^k b_k$. Podemos suponer por simetría que $b_j > a_j$ (lo que a su vez implica que $1 \le b_j - a_j < 10$) y escribir $\sum_{k=0}^{j-1} 10^k a_k = 10^j (b_j - a_j) + \sum_{k=0}^{j-1} 10^k b_k$. El primer miembro es una representación decimal con j cifras y el segundo otra con $j+1$, lo que contradice la proposición anterior.

Notación: En esta sección la expresión $a_n a_{n-1} \cdots a_0$ no será el producto de los números $a_n, a_{n-1}, \ldots, a_0$, sino el número $\sum_{k=0}^{n} 10^k a_k$.

Reglas de divisibilidad:

1. $a_n a_{n-1} \cdots a_0 = a_{k-1} a_{k-2} \cdots a_0 + (10^k)$
2. $a_n a_{n-1} \cdots a_0 = a_{k-1} a_{k-2} \cdots a_0 + (2^k)$
3. $a_n a_{n-1} \cdots a_0 = a_{k-1} a_{k-2} \cdots a_0 + (5^k)$
4. $a_n a_{n-1} \cdots a_0 = \sum_{k=0}^{n} a_k + (9)$
5. $a_n a_{n-1} \cdots a_0 = \sum_{k=0}^{n} a_k + (3)$
6. $a_n a_{n-1} \cdots a_0 = \sum_{k=0}^{n} (-1)^k a_k + (11)$
7. $a_n a_{n-1} \cdots a_0 = a_2 a_1 a_0 + a_5 a_4 a_3 + \ldots + (999)$
8. $a_n a_{n-1} \cdots a_0 = a_2 a_1 a_0 + a_5 a_4 a_3 + \ldots + (37)$
9. $a_n a_{n-1} \cdots a_0 = a_2 a_1 a_0 + a_5 a_4 a_3 + \ldots + (27)$
10. $a_n a_{n-1} \cdots a_0 = a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - a_{11} a_{10} a_9 + \ldots + (1001)$
11. $a_n a_{n-1} \cdots a_0 = a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - a_{11} a_{10} a_9 + \ldots + (13)$
12. $a_n a_{n-1} \cdots a_0 = a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - a_{11} a_{10} a_9 + \ldots + (7)$

Demostración: La reglas 1, 4, 6, 7 y 10 se obtienen tomando módulo 10^k, 9, 11, 999 y 1001 respectivamente. Las reglas 2 y 3 son consecuencia de la 1, la 5 de la 4, la 8 y la 9 de la 7 y la 11 y la 12 de la 10.

Seguro que el lector puede obtener muchas más reglas de divisibilidad.

Ejemplo: Encontrar las cifras x, y para que el número $N = 5xy6$ sea divisible por 117.
En primer lugar factorizamos el 117: $117 = 3^2 \cdot 13$. Así, $5 + x + y + 6 = 0 + (9)$, es decir, $x + y = 7 + (9)$. Por otro lado, $xy6 - 5 = xy1$ debe ser múltiplo de 13. Los múltiplos de 13 con tres cifras que terminan en 1 son: 91, 221, 351, 481, 611, 741 y 871. El único que cumple la otra condición es el 611, así que la solución es 5616.

2.3. Anillos de restos.

Los resultados de la sección 2.1 nos permiten definir ciertos conjuntos y dotarles de una

estructura algebraica. No es intención de este libro profundizar en el estudio de los anillos, pero dar unas nociones mínimas puede agilizar enormemente el tratamiento de las congruencias.

El corolario del teorema 2.1.2 nos dice que para cada $m \geq 1$ podemos dar una partición de $\mathbb{Z}$ en m subconjuntos. Pues bien, al conjunto de esos subconjuntos se le llama $\mathbb{Z}_m$. Un elemento de $\mathbb{Z}_m$ viene dado por la expresión $\bar{a}$, donde $a \in \mathbb{Z}$; $\bar{a}$ denotará el conjunto de todos los enteros congruentes con a módulo m.

El teorema 2.1.3 nos garantiza la posibilidad de definir una suma y una multiplicación en $\mathbb{Z}_m$ del siguiente modo: $\bar{a}+\bar{b}=\overline{a+b}$, $\bar{a}\,\bar{b}=\overline{ab}$, ya que la clase resultante de la operación no depende de los representantes elegidos para efectuarla. Consideremos, para aclarar esto con un ejemplo, $m=14$, $a=5$, $b=11$. Tenemos así, $\bar{5}+\bar{11}=\bar{16}$. Si elegimos otros representante de $\bar{5}$ y $\bar{11}$, es decir, números congruentes con 5 y con 11 módulo 14, debería darnos el mismo resultado. Tenemos que 33=5+(14), -3=11+(14), y al sumar, $\bar{33}+\overline{-3}=\bar{30}$, pero $\bar{30}=\bar{16}$, ya que $30=16+(14)$. Compruebe el lector lo mismo con el producto. Es importante darse cuenta de que todo esto está garantizado por el teorema 2.1.3.

Es inmediato deducir que $\mathbb{Z}_p$ tiene, con las operaciones así definidas, estructura de anillo.

Definición 2.3.1: Sea A un conjunto no vacío en el que se han definido dos operaciones $+,\cdot$, que tienen las siguientes propiedades:

- $a+(b+c)=(a+b)+c \;\forall\, a,b,c \in A$ (asociativa de la suma)
- $a+b=b+a \;\forall\, a,b \in A$ (conmutativa de la suma)
- $\exists 0 \in A : a+0=0+a=a \;\forall\, a \in A$ (elemento neutro para la suma)
- $\forall\, a \in A \exists -a \in A : a+(-a)=(-a)+a=0$ (elemento simétrico para la suma)
- $(ab)c=a(bc) \;\forall\, a,b,c \in A$ (asociativa del producto)
- $a(b+c)=ab+ac \;\forall\, a,b,c \in A$ (distributiva por la izquierda)
- $(a+b)c=ac+bc \;\forall\, a,b,c \in A$ (distributiva por la derecha)

A la terna $(A,+,\cdot)$ se le llama anillo. Si se cumple esta propiedad:

- $\exists 1 \in A : 1\,a=a\,1=a$

se llama anillo unitario, y si se cumple esta otra

- $ab=ba \;\forall\, a,b \in A$

anillo conmutativo. Los anillos conmutativos y unitarios en los que $1 \neq 0$ se llaman dominios.

Proposición 2.3.2: En todo anillo A se tiene que $0\,a=a\,0=0 \;\forall\, a \in A$.

Demostración: $0\,a=(0+0)\,a=0\,a+0\,a$, y por tanto $0\,a=0$. De modo análogo se prueba que $a\,0=0$.

Proposición 2.3.3: Si un anillo unitario A tiene al menos dos elementos distintos, entonces $1 \neq 0$.
Demostración: Supongamos que $1=0$ y que $a \in A$. Entonces $a=1a=0a=0$. Entonces resulta que el único elemento de A es 0.

Teorema 2.3.4: Dado un entero $m \geq 2$, el conjunto $\mathbb{Z}_m$ es un dominio.

El conjunto $\mathbb{Z}$ de los números enteros es otro dominio, por supuesto, lo que nos asegura que hay ciertas similitudes entre $\mathbb{Z}$ y $\mathbb{Z}_m$, pero también hay diferencias esenciales:

- $\mathbb{Z}$ es infinito y $\mathbb{Z}_m$ tiene m elementos.
- En $\mathbb{Z}$ las expresiones 1, 1+1, 1+1+1,... son todas distintas de 0, mientras que en $\mathbb{Z}_m$, al sumar 1 m veces se obtiene 0.
- En $\mathbb{Z}$ se puede definir los números positivos y negativos, y con ello un orden coherente con las operaciones, y en $\mathbb{Z}_m$ no (por ejemplo en $\mathbb{Z}_7$, -3=4).
- Los dominios donde el producto de dos elementos no nulos nunca da 0 se llaman dominios de integridad. $\mathbb{Z}$ es por tanto un dominio de integridad, sin embargo:

Teorema 2.3.5: $\mathbb{Z}_m$ es dominio de integridad si y sólo si m es primo.
Demostración: Si $m=1$, $\mathbb{Z}_1$ se reduce a $\{0\}$, y si m es compuesto tendrá algún divisor d con $1<d<m$. Entonces $\bar{d} \cdot \overline{m/d}=\bar{0}$. En cambio, si m es primo y $a, b \in \mathbb{Z}$ son tales que $\bar{a}\,\bar{b}=\bar{0}$, esto quiere decir que $m|ab$, y por el teorema 1.3.5, $m|a$ ó $m|b$, es decir, $\bar{a}=\bar{0}$ ó $\bar{b}=\bar{0}$.

Definición 2.3.6: Sea D un dominio. Se dice que $d \in D$ es un divisor de cero si $d \neq 0$ y existe $d' \neq 0$ tal que $dd'=0$ (en cuyo caso d' también es divisor de cero). Se dice que $u \in D$ es una unidad si existe $u' \in D$ tal que $uu'=1$ (en cuyo caso u' también es unidad). El conjunto de las unidades de D se denota $U(D)$. Si $U(D) \cup \{0\}=D$, se dice que D es un cuerpo.

Proposición 2.3.7: Sea D un dominio, $a, b, c \in D$ con $ab=ac$. Si a no es cero ni divisor de cero entonces $b=c$.
Demostración: $ab=ac \Rightarrow ab-ac=0 \Rightarrow a(b-c)=0 \Rightarrow b-c=0$. En la última implicación se ha hecho uso de que a no es cero ni divisor de cero.

Teorema 2.3.8: En un dominio finito, los elementos no nulos son unidades o divisores de cero.
Demostración: Sea F un dominio finito, y $a \in F \setminus \{0\}$. Consideramos el conjunto $G=\{a^n, n \in \mathbb{N}\}$. Es obvio que $G \subseteq F$, y como F es finito existirán $m, n \in \mathbb{N}$ con $m>n$ tales que $a^m=a^n$. Si a es

divisor de cero, el teorema está probado. Si no, por la proposición anterior, cancelamos n veces el término a y queda $a^{m-n}=1$, es decir $a\cdot a^{m-n-1}=1$, por lo que $a\in U(F)$.

Nota: Deberíamos haber dado sentido a la expresión a^n para $a\in D$ y $n\geq 0$, pero esto hubiera alargado excesivamente esta sección y creemos que el lector podrá imaginarse sin problemas su significado. En cualquier caso, se puede encontrar en cualquier libro de álgebra de anillos.

Todo lo anterior se puede resumir así:

Teorema 2.3.9: Sea $D=\mathbb{Z}_m$.

- Si $m=1$, $D=\{0\}$.
- Si m es primo, D es un cuerpo.
- Si m es compuesto, D es un dominio con divisores de cero.

Teorema 2.3.10: Sea $m\geq 2$. Si $a\in\mathbb{Z}$, $\bar{a}\in U(\mathbb{Z}_m)\Leftrightarrow(a,m)=1$.
Demostración: Si $\bar{a}\in U(\mathbb{Z}_m)$ existe $b\in\mathbb{Z}$ tal que $\bar{a}\,\bar{b}=\bar{1}$, es decir, $m|(ab-1)$, es decir, existe $c\in\mathbb{Z}$ tal que $ab-1=cm$, o sea, $ab-cm=1$, por lo que $(a,m)=1$. Para el recíproco, véase la proposición 2.1.4.

Definición 2.3.11: Sea D un dominio y $u\in U(D)$. Denotaremos u^{-1} al elemento de $U(D)$ que cumple $uu^{-1}=1$.

Teorema 2.3.12: Sea D un dominio y $u,v\in U(D)$. Entonces $uv\in U(D)$.
Demostración: $uvv^{-1}u^{-1}=1$.

2.4. Teoremas de Euler, Fermat, Lagrange, Wilson y Wolstenholme.

La siguiente función se estudiará con mucho más detalle en el capítulo siguiente, pero la introducimos aquí para formular el teorema de Euler.

Definición 2.4.1: Sea $n\in\mathbb{N}$. Se define: $\varphi(n)=\#\{m\in\mathbb{N}, m\leq n, (m,n)=1\}$, donde el símbolo $\#$ denota el cardinal del conjunto que aparece a continuación.

Teorema de Euler: Sea $m\geq 2$ y $a\in\mathbb{Z}$. Si a es primo con m entonces $a^{\varphi(m)}=1+(m)$.

Demostración: En virtud del teorema 2.3.10, $U(\mathbb{Z}_m)$ tiene $\varphi(m)$ elementos. Pongamos $U(\mathbb{Z}_m)=\{\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_{\varphi(m)}\}$. Ahora bien, el conjunto $\{\bar{a}\,\bar{a}_1,\bar{a}\,\bar{a}_2,\ldots,\bar{a}\,\bar{a}_{\varphi(m)}\}$ está contenido en $U(\mathbb{Z}_m)$ por el teorema 2.3.12, ya que $\bar{a}\in U(\mathbb{Z}_m)$, y tiene el mismo número de elementos (compruebe el lector que no tiene elementos repetidos), así que en definitiva es también $U(\mathbb{Z}_m)$. Multiplicando sobre cada conjunto tenemos la igualdad

$$\prod_{k=1}^{\varphi(m)}\bar{a}_k=\bar{a}^{\varphi(m)}\prod_{k=1}^{\varphi(m)}\bar{a}_k$$

y cancelando los productorios nos queda el teorema.

Teorema de Fermat: Sea $p\in P$ y $a\in\mathbb{Z}$. Entonces $a^p=a+(p)$.

Demostración: Si a no es primo con p entonces $a=0+(p)$ y el teorema es obvio. En otro caso estamos en las condiciones del Teorema de Euler, por lo que podemos afirmar que $a^{\varphi(p)}=1+(p)$. Pero $\varphi(p)=p-1$ por ser p primo, así que $a^{p-1}=1+(p)$. Multiplicando en $\mathbb{Z}_p$ por $\bar{a}$ nos queda el teorema.

Teorema de Lagrange: Sea f un polinomio de grado n con coeficientes enteros y $p\in P$. Supongamos que $f(\bar{a})=\bar{0}$ para más de n elementos distintos $\bar{a}$ de $\mathbb{Z}_p$. Entonces todos los coeficientes de f son múltiplos de p.

Demostración: Sea $f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0$. Razonamos por inducción sobre n.

Si $n=1$, $f(x)=a_1x+a_0$. Sean $\bar{x}_1,\bar{x}_2$ tales que $\overline{a_1x_1+a_0}=\overline{a_1x_2+a_0}=\bar{0}$. Como $\bar{x}_1\neq\bar{x}_2$, debe ser $\bar{a}_1=0$ y por tanto $\bar{a}_0=0$.

Supongamos el teorema probado para polinomios de grado menor que n. Sean $\bar{x}_k$, $1\leq k\leq n+1$ elementos distintos de $\mathbb{Z}_p$ tales que $f(\bar{x}_k)=\bar{0}$. El polinomio $h(x)=f(x)-f(x_0)$ tiene al menos una raíz entera, a saber, x_0, por lo que podemos escribir $f(x)-f(x_0)=g(x)(x-x_0)$. Entonces

$$\bar{0}=f(\bar{x}_k)-f(\bar{x}_0)=(\bar{x}_k-\bar{x}_0)\,g(\bar{x}_k)$$

donde g es un polinomio de grado $n-1$ con coeficientes enteros. Como $\bar{x}_k\neq\bar{x}_0$ para $k\neq0$, g se anula en $\mathbb{Z}_p$ para más de $n-1$ elementos, y por la hipótesis de inducción, p divide a todos sus coeficientes. Pero $f(x)=(x-x_0)g(x)+f(x_0)$, y como $p|f(x_0)$, p divide a todos los coeficientes de f.

Proposición 2.4.2: Sea $p\in P$ y $f(x)=\prod_{j=1}^{p-1}(x-j)-x^{p-1}+1$. Todos los coeficientes de f son múltiplos de p.

Demostración: El grado de f es $p-2$, luego, en virtud del Teorema de Lagrange, bastará probar que $p|f(k)$ para $1\le k\le p-1$. Para estos valores de k el productorio se anula y tenemos $f(k)=1-k^{p-1}$, pero por el teorema de Euler $k^{p-1}=1+(p)$.

Teorema de Wilson: Sea $p\in P$. Entonces $(p-1)!=-1+(p)$.

Demostración: En el polinomio de la propsición anterior hacemos $f(0)=(p-1)!+1$, que al ser el término independiente de f, debe ser múltiplo de p.

Teorema 2.4.3: Sea $m\ge 2$. Si $m=4$, $(m-1)!+1=2+(m)$, y si m es cualquier otro número compuesto, $(m-1)!=0+(m)$.

Demostración: Para $m=4$ es una comprobación directa. Supongamos que m es otro número compuesto y $p=\min S(m)$. Entonces $p^2\le m$. Tenemos dos posibilidades:

- Si $p^2=m$, al ser $m\neq 4$, será $p\neq 2$. Entonces $2p<m$ y $2p^2|(m-1)!$, por lo que $m|(m-1)!$
- Si $p^2<m$, $\frac{m}{p}>p$ y $p\cdot\frac{m}{p}|(m-1)!$, luego $m|(m-1)!$

Teorema de Wolstenholme: Si $p\in P$ y $p\ge 5$, entonces $\sum_{j=1}^{p-1}\frac{(p-1)!}{j}=0+(p^2)$.

Demostración: Sea f el polinomio de la proposición 2.4.2. Desarrollándolo queda:

$$f(x)=1+(p-1)!-S_{p-1}x+S_{p-2}x^2-\cdots-S_1x^{p-2}$$

Evaluando en $x=p$,

$$f(p)=1+(p-1)!-S_{p-1}p+S_{p-2}p^2-\cdots-S_1p^{p-2}$$

Pero sustituyendo en la expresión sin desarrollar nos da $f(p)=1+(p-1)!-p^{p-1}$, de donde

$$S_{p-1}=S_{p-2}p-\cdots-S_1p^{p-3}+p^{p-2}$$

Como $p\ge 5$ y $p|S_{p-2}$, resulta que $p^2|S_{p-1}$, pero $S_{p-1}=\sum_{j=1}^{p-1}\frac{(p-1)!}{j}$.