Los fundamentos de la aritmética elemental establecidos por medio del modo recursivo del pensamiento, sin el uso de variables aparentes que se extienden sobre dominios infinitos.

Por
Thoralf Skolem

Traducción de
Emilio Méndez Pinto

Los fundamentos de la aritmética elemental establecidos por medio del modo recursivo del pensamiento, sin el uso de variables aparentes que se extienden sobre dominios infinitos

Por

Thoralf Skolem

Traducción de

Emilio Méndez Pinto

Edición digital para la Biblioteca Digital del ILCE

Título original: The foundations of elementary arithmetic established by means of the recursive mode of thought, without the use of apparent variables ranging over infinite domains

Publicado originalmente en Det Norske Videnskaps-Akademi i Oslo (1923). La Academia Noruega de Ciencias y Letras otorgó los permisos de traducción y publicación digital de esta obra para esta colección.

Las nociones fundamentales de la lógica que suelen considerarse como necesarias para los fundamentos de las matemáticas (véase, por ejemplo, *Whitehead y Russell 1910, 1912, y 1913*) son, en primer lugar, las siguientes: las nociones *proposición* y *función proposicional* de una, dos, o más variables; las tres operaciones de (1) *conjunción* (expresada en el lenguaje ordinario por medio de la palabra "y" o de las palabras "— así como —"), (2) *disyunción* (comúnmente expresada por medio de las palabras "o bien — o —"), y (3) *negación* (indicada con la palabra "no"); y finalmente las nociones de Russell y Whitehead de "siempre" y "a veces". Estas dos últimas nociones expresan la idea de que una proposición vale *en todos los casos* o en *al menos un caso*, respectivamente. Decir que una proposición vale en al menos un caso es establecer una proposición existencial, y eso suele hacerse por medio de la palabra "existe". A lo largo de este trabajo utilizaré letras mayúsculas como símbolos para funciones proposicionales, de modo que $A(x)$, $B(x)$, … denotan funciones proposicionales de una variable, $A(x, y)$, $B(x, y)$, … denotan funciones proposicionales de dos variables, y así sucesivamente. Además, empleo los signos de Schröder (*1890*) para la conjunción, la disyunción, y la negación, de modo que, si A y B son proposiciones, AB significa la proposición "tanto A como B", $A + B$ la proposición "o bien A o B", y finalmente $\overline{A}$ la negación de A. No obstante, Russell y Whitehead también introducen la noción de "función descriptiva". Una función descriptiva es una expresión que tiene un significado inequívocamente determinado; es un tipo de nombre propio funcional. Finalmente, de acuerdo con Russell y Whitehead, es necesario introducir, como un tipo de *afirmaciones funcionales*, proposiciones que valen de manera general. Decimos que tenemos una afirmación funcional cuando se afirma que una proposición vale para el caso indeterminado.

Ahora bien, lo que quiero mostrar en este trabajo es lo siguiente: *Si consideramos los teoremas generales de la aritmética como afirmaciones funcionales y tomamos como base al modo recursivo del pensamiento, entonces dicha ciencia puede fundarse, rigurosamente, sin el uso de las nociones de "siempre" y "a veces" de Russell y Whitehead*. Esto puede igualmente expresarse como sigue: puede suministrarse un fundamento lógico para la aritmética sin el uso de variables lógicas aparentes. Para estar seguros, a menudo será ventajoso introducir variables aparentes; pero requeriremos que estas variables se extiendan sólo sobre dominios finitos, y entonces, por medio de

definiciones recursivas, siempre podremos evitar el uso de tales variables. Y esto se aclarará en lo que sigue.

Incidentalmente, me gustaría remarcar que en realidad considero a todas las funciones como descriptivas; las funciones proposicionales están únicamente caracterizadas por el hecho de que sólo pueden tener los dos valores "verdadero" y "falso", que, desde luego, también están entre las nociones lógicas fundamentales.

Considero las funciones descriptivas como nombres propios funcionales, esto es, nombres propios cuyo significado depende de lo que elijamos para una o más variables. Por ejemplo, considero a "n + 1", "el número que sigue a n", como siendo el nombre de un número, pero uno que, dependiendo de lo que elijamos para n, denota números distintos.

De acuerdo con Russell y Whitehead, funciones descriptivas como "el autor de *Waverley*" realmente no significan nada, y son símbolos meramente incompletos. No me parece que esta concepción esté más allá de toda duda; pero incluso si fuera correcta para las funciones descriptivas del lenguaje ordinario, no necesitaríamos adoptarla para las funciones descriptivas de la aritmética.

Russell y Whitehead razonan como sigue: "El autor de *Waverley*" no puede significar Scott; porque entonces la proposición "Scott es el autor de *Waverley*" significaría "Scott es Scott", y ésta es una proposición completamente vacía. Por el otro lado, "el autor de *Waverley*" no puede significar ninguna otra persona; porque entonces la proposición "Scott es el autor de *Waverley*" sería falsa, lo que, como es bien sabido, no es el caso. Consecuentemente, "el autor de *Waverley*" no significa nada; es un símbolo incompleto.

Esta prueba, que tiene un carácter más bien filosófico, no me parece del todo convincente. ¿Qué nos impide considerar "el autor de X" – abreviemos esto con $V(X)$ – como un tipo de nombre propio variable? Entonces seguramente "el autor de *Waverley*" nombra a la misma persona que nombra "Scott". Pero los dos nombres son distintos, y es por eso por lo que la proposición "Scott es el autor de *Waverley*" no puede reemplazarse por la proposición "Scott es Scott". La última proposición es vacía, pero no la primera, y la razón de esto es que uno ya sabe algo, de antemano, acerca de la persona llamada $V(X)$, ya que, después de todo, suele aceptarse que una persona ha de llamarse $V(X)$ si y sólo si ella y

nadie más escribió *X*. La información transmitida es, en mi opinión, del mismo tipo que en el siguiente caso: un hombre tiene dos nombres propios, *A* y *B*. En un momento hemos escuchado algo acerca de *A*, por ejemplo, que tiene cinco hijos. En otra ocasión nos presentan al señor *B*, y se nos dice que *B* es el señor *A*. Esta proposición, entonces, contiene información acerca de *B*, a saber, que *B* tiene cinco hijos, porque teníamos algún conocimiento previo acerca de *A*. La proposición "*B* es *A*" es por tanto completamente distinta de las proposiciones "*A* es *A*" y "*B* es *B*"; las últimas son completamente vacías, pero la primera no lo es, si ya se sabe algo de antemano acerca de *A* pero no acerca de *B*, o acerca de *B* pero no de *A*.

En lo que sigue, el signo de igualdad siempre ha de entenderse en el sentido de que dos nombres o expresiones significan o designan la misma cosa. Esto también da cuenta de por qué considero como obvio que siempre pueda remplazar iguales por iguales, y hago esto por todas partes.

Se toman como base las nociones de "número natural" y de "el número $n + 1$ que sigue al número n" (así, la función descriptiva $n + 1$), así como el modo recursivo del pensamiento.[1]

§ 1. ADICIÓN

Deseo introducir una función descriptiva de dos variables, a y b, que llamaré la *suma* de a y b; la denoto con $a + b$ porque, para $b = 1$, ha de significar precisamente al número que sigue a a, a saber, $a + 1$. Esta función, por tanto, ha de considerarse como ya definida para $b = 1$ para una a arbitraria. Para definirla generalmente, sólo necesito definirla para $b + 1$ para una a arbitraria, si ya se asume que está definida para b para una a arbitraria. Esto se consigue mediante la siguiente definición:

Definición 1. $a + (b + 1) = (a + b) + 1$.

[1] En lo que sigue, el frecuentemente incómodo formalismo de las funciones proposicionales se debe al hecho de que este trabajo fue escrito como una especie de secuela [in Anschluss] al trabajo de Russell y Whitehead.

Así, la suma de a y $b + 1$ se establece igual al número que sigue a $a + b$. Si, por lo tanto, la adición ya está definida para valores arbitrarios de a para un cierto número b, entonces, por la Definición 1, la adición está definida para arbitrarias a para $b + 1$ y de este modo definida de manera general. Este es un ejemplo típico de una definición recursiva.

Teorema 1. (La ley asociativa.) $a + (b + c) = (a + b) + c$.

Prueba. La proposición vale para $c = 1$ en virtud de la Definición 1. Asumo que vale para un cierto c para valores arbitrarios de a y b. Necesariamente, entonces, para valores arbitrarios de a y b,

(α) $a + (b + (c + 1)) = a + ((b + c) + 1)$,

ya que, de acuerdo con la Definición 1, $b + (c + 1) = (b + c) + 1$. Pero de acuerdo con la Definición 1 necesariamente también

(β) $a + ((b + c) + 1) = (a + (b + c)) + 1$.

Ahora, de acuerdo con la asunción, $a + (b + c) = (a + b) + c$, por lo cual

(γ) $(a + (b + c)) + 1 = ((a + b) + c) + 1$.

De acuerdo con la Definición 1, finalmente tenemos también que

(δ) $((a + b) + c) + 1 = (a + b) + (c + 1)$.

De (α), (β), (γ), y (δ) se sigue que

$a + (b + (c + 1)) = (a + b) + (c + 1)$,

lo que prueba la proposición para $c + 1$ para a y b no especificados. Así, la proposición vale de manera general. Este es un ejemplo típico de una prueba recursiva (prueba por inducción matemática).

Lema. $a + 1 = 1 + a$.

Prueba. La proposición vale para $a = 1$. Pruebo que vale para $a + 1$, asumiendo que vale para a. De hecho, obtenemos

$(a + 1) + 1 = (1 + a) + 1 = 1 + (a + 1)$

en virtud de la asunción hecha y de la Definición 1. Así, la proposición vale de manera general.

Teorema 2. (La ley conmutativa.) $a + b = b + a$.

Prueba. Como consecuencia del lema, la proposición vale para $b = 1$. Asumo que es verdadera para a arbitraria para un cierto b y después pruebo que es verdadera para $b + 1$ para a arbitraria. Esto se hace como sigue:

$a + (b + 1) = (a + b) + 1 = (b + a) + 1 = b + (a + 1) = b + (1 + a) = (b + 1) + a$,

por el uso del Teorema 1 y del lema. La aserción proposicional $a + b = b + a$ es, por lo tanto, verdadera.

§ 2. LAS RELACIONES < (MENOR QUE) Y > (MAYOR QUE)

Estrechamente conectadas con la adición están las relaciones “menor que” y “mayor que”, denotadas con < y >, respectivamente. Ya que la última relación es sólo la inversa de la primera, únicamente necesita definirse la relación <. Esto suele hacerse por medio de una variable lógica aparente, con el uso de la noción lógica de existencia, o el “a veces” de Russell y Whitehead. La definición usual, de hecho, tiene la forma

$$(a < b) = \sum_{x} (a + x = b),$$

donde el signo de Schröder se utiliza para expresar que una proposición vale en al menos un caso (Schröder habla después de sumación proposicional [Aussagensummation] y la denota con Σ). En palabras, la definición es como sigue: “se dice que a es menor que b si y sólo si *existe un número* x tal que $a + x = b$”. Por lo tanto, esta definición involucra el uso de la noción lógica de existencia, o, en otras palabras, el uso de una variable aparente. Pero fácilmente podemos evitar el uso de esta noción al definir la relación “menor que” recursivamente. De hecho, esto puede hacerse así:

Definición 2. $a < 1$ es falso. $(a < b + 1) = (a < b) + (a = b)$.

Fácilmente se ve que esta es una definición recursiva perfectamente legítima; pues, primero, especifica bajo qué condiciones $a < b$ si $b = 1$, a saber, ninguna; y, segundo, especifica bajo qué condiciones ha de obtenerse la relación $<$ entre una a arbitraria y un cierto $b + 1$ si ya está definida para b para a arbitraria. Como vemos, *no ocurre ningún signo-Σ lógico en esta definición*.

Definición 2.1. $(a > b) = (b < a)$.

Teorema 3. $\overline{(a < b)(b < c)} + (a < c)$, o, $\overline{(a < b)} + \overline{(b < c)} + (a < c)$. En palabras, este teorema dice: si tanto $a < b$ como $b < c$ valen, entonces $a < c$.

Prueba. La proposición vale para a y b arbitrarias cuando $c = 1$; pues, de acuerdo con la Definición 2, $b < 1$ es falso, esto es, $\overline{(b < 1)}$ es verdadero. Quiero por tanto probar que la proposición es verdadera para $c + 1$ siempre que sea verdadera para c (con los valores de a y b sin especificar). Desde $(a < b)(b < c + 1)$ se sigue, de acuerdo con la Definición 2, o bien que $(a < b)(b < c)$ o bien que $(a < b)(b = c)$. Pero, de acuerdo con la asunción, desde $(a < b)(b < c)$ se sigue que $a < c$, por lo cual, por la Definición 2, $a < c + 1$. Desde luego, de $(a < b)(b = c)$ se sigue también que $a < c$, por lo cual, nuevamente, $a < c + 1$. En cualquier caso, por tanto, $a < c + 1$ si tanto $a < b$ como $b < c + 1$ valen, de modo que la proposición también debe ser verdadera para a y b arbitrarias para $c + 1$. Esto prueba el Teorema 3.

Definición 3. $(a \leq b) = (a < b) + (a = b)$.

Definición 3.1. $(a \geq b) = (a > b) + (a = b)$.

Estas definiciones, como la Definición 2.1, meramente introducen variantes de notación; son, por tanto, teóricamente superfluas, lo que no es el caso para las definiciones recursivas.

Lema 1 (para el Teorema 4). $\overline{(a < b)} + (a + 1 \leq b)$.

En palabras: o bien a no es menor que b, o bien $a + 1$ es menor que o igual a b. Pero es mejor establecerlo así: de $a < b$ se sigue que $a + 1 \leq b$.

Prueba. Para un a no especificado, la proposición vale para $b = 1$. Asumo que es verdadera para a arbitrario para un cierto b y después pruebo que es verdadera para a arbitrario para $b + 1$. De $a < b + 1$ se sigue (Definición 2) o bien que $a < b$, por lo cual, como consecuencia de la asunción, $a+1 \le b,$ que a su vez produce (Definición 2) $a+1 \le b+1,$ o bien que $a = b$, por lo cual claramente $a + 1 = b + 1$, lo que produce (Definición 3) $a+1 \le b+1.$ La proposición vale entonces para valores arbitrarios de a, también para $b + 1$, y por lo tanto vale en general.

Lema 2 (para el Teorema 4). $1 \le a.$

Prueba. La proposición vale para $a = 1$. De la asunción de que vale para a, esto es, que $1 \le a,$ se sigue (Definiciones 2 y 3) que $1 < a + 1$, lo que produce (Definición 3) $1 \le a+1;$ esto es, la proposición también vale para $a + 1$.

Teorema 4. $(a < b) + (a = b) + (a > b)$.

Prueba. La proposición vale para $b = 1$, porque de acuerdo con el Lema 2 necesariamente $a = 1$ o $a > 1$. Asumo que la proposición es verdadera para b con a no especificado y pruebo que es verdadera para $b + 1$ para a arbitrario. Pues, si no es el caso que $a < b + 1$, ni $a < b$ ni $a = b$ es posible (Definición 2); pero entonces, como consecuencia de la asunción, $a > b$, por lo cual (Lema 1) $a \ge b+1$.

Lema. $(a < b)(a+1 < b+1) + \overline{(a < b)}\,\overline{(a+1 < b+1)}.$

Esta proposición puede expresarse en palabras así: De $a < b$ se sigue que $a + 1 < b + 1$, y a la inversa.

Prueba. De $a < b$ se sigue (Lema 1 para el Teorema 4) que $a+1 \le b$, por lo cual (Definición 2) $a + 1 < b + 1$. De $a + 1 < b + 1$ se sigue (Definición 2) o bien que $a + 1 < b$ o que $a + 1 = b$. Por lo tanto, en cualquier caso $a < b$.

Teorema 5. $\overline{a < a};$ esto es, ningún número es menor que sí mismo.

Prueba. Esto es verdadero para $a = 1$ (Definición 2). Asumo que es verdadero para un cierto a. De $a + 1 < a + 1$ se seguiría, de acuerdo con el último lema, que $a < a$, lo que entra en conflicto con la asunción hecha.

Corolario a los Teoremas 3 y 5. [Para a y b distintos] $(a < b)\overline{(a > b)} + \overline{(a < b)}(a > b)$.

En palabras: Si $a < b$, entonces no $a > b$, y a la inversa.

Pues, si tuviésemos $a < b$ y al mismo tiempo $a > b$, se seguiría (Teorema 3) que $a < a$.

Corolario. $\overline{(a < b)} + (a \neq b)$;[2] esto es, si $a < b$, entonces a no es igual a b. Pues de $(a < b)(a = b)$ se seguiría que $a < a$.

Las tres relaciones $a < b$, $a = b$, $a > b$ son entonces mutuamente excluyentes, mientras que, debido al Teorema 4, en cada caso debe satisfacerse una de ellas.

Teorema 6. $(a < b)(a + c < b + c) + \overline{(a < b)}\,\overline{(a + c < b + c)}$.

Prueba. De acuerdo con el lema para el Teorema 5, esto es ciertamente verdadero cuando $c = 1$. Asumimos que ya ha sido probado como verdadero para a y b arbitrarios para un cierto c. De $a < b$ se sigue entonces que $a + c < b + c$, por lo que, en virtud del Teorema 1 y del mismo lema, $a + (c + 1) < b + (c + 1)$. A la inversa, se sigue de $a + (c + 1) < b + (c + 1)$, en virtud del Teorema 1 y del mismo lema, que $a + c < b + c$, por lo cual, de acuerdo con la asunción, $a < b$.

Teorema 7. $\overline{(a < b)(c < d)} + (a + c < b + d)$.

Esto es, si valen tanto $a < b$ como $c < d$, $a + c < b + d$.

Prueba. De $a < b$ se sigue (Teorema 6) que $a + c < b + d$. De $c < d$ se sigue (Teoremas 2 y 6) que $b + c < b + d$. De la asunción de que tanto $a + c < b + c$ como $b + c < b + d$ valen se sigue (Teorema 3) que $a + c < b + d$.

[2] Escribo $a \neq b$, como se hace habitualmente, para expresar el hecho de que a no es igual a b, es decir, que $\overline{(a = b)}$ vale.

Este es un ejemplo típico de una prueba no recursiva, una que consiste meramente en una combinación finita de teoremas anteriores, mientras que una prueba por inducción matemática representa un proceso infinito. Incidentalmente, ya hemos tenido otros varios ejemplos de pruebas no recursivas (a saber, aquellas del lema para el Teorema 5 y de los corolarios a los Teoremas 3 y 5).

Teorema 8. $(a + c \neq b + c) + (a = b)$.

Esto es, de $a + c = b + c$ se sigue que $a = b$. Claramente, lo inverso también es verdadero.

Prueba. Si $a \neq b$, entonces necesariamente (Teorema 4) o bien $a < b$ o $a > b$. Sin embargo, de $a < b$ se sigue (Teorema 6) que $a + c < b + c$ y de $a > b$, del mismo modo, que $a + c > b + c$, y ambas contradicen (corolario al Teorema 5) la ecuación $a + c = b + c$.

El caso especial $c = 1$ de este teorema afirma que puede existir a lo mucho un número teniendo un cierto sucesor, o, en otras palabras, cada número puede tener *un* predecesor a lo mucho.

Teorema 9. $a < a + b$.

Prueba. Verdadero para $b = 1$ para a no especificado (Definición 2). Asumimos que la proposición es verdadera para a arbitrario para un cierto b. Pero de $a < a + b$ obtenemos además (Definición 2) $a < (a + b) + 1$, esto es (Definición 1), $a < a + (b + 1)$.

§ 3. MULTIPLICACIÓN

Definición 4. $a \cdot 1 = a$. $a(b + 1) = ab + a$.

Esta es una definición recursiva de una función descriptiva ab de dos variables, a y b, llamada el *producto* de a y b.

Teorema 10. (Primera ley distributiva.) $a(b + c) = ab + ac$.

Prueba. La proposición vale (Definición 4) para $c = 1$. Por tanto, asumimos que vale para a y b arbitrarios para un cierto c. Entonces obtenemos

$$a(b + (c + 1)) = a((b + c) + 1) = a(b + c) + a$$

$$= (ab + ac) + a = ab + (ac + a) = ab + a(c + 1),$$

haciendo uso del Teorema 1, Definición 4, y de la asunción hecha.

Teorema 11. (La ley asociativa.) $a(bc) = (ab)c$.

Prueba. La proposición vale (Definición 4) para $c = 1$. Asumimos por lo tanto que es verdadera para a y b arbitrarios para un cierto c. Entonces obtenemos

$$a(b(c + 1)) = a(bc + b) = a(bc) + ab = (ab)c + ab = (ab)(c + 1),$$

aplicando la Definición 4, Teorema 10, y la asunción hecha.

Teorema 12. (Segunda ley distributiva.) $(a + b)c = ac + bc$.

Prueba. Cuando $c = 1$, la proposición es verdadera (Definición 4). Asumimos que es verdadera para a y b arbitrarios para un cierto c. Entonces, al aplicar la Definición 4 y los Teoremas 1 y 2, obtenemos

$$(a + b)(c + 1) = (a + b)c + (a + b) = (ac + bc) + (a + b) = ((ac + bc) + a) + b$$

$$= (ac + (bc + a)) + b = (ac + (a + bc)) + b = ((ac + a) + bc) + b$$

$$= (a(c + 1) + bc) + b = a\,(c + 1) + (bc + b) = a\,(c + 1) + b(c + 1).$$

Lema. $1 \cdot a = a$.

Prueba. Verdadero para $a = 1$ (Definición 4). Si la proposición es verdadera para a, entonces $1 \cdot (a + 1) = (1 \cdot a) + 1 = a + 1$; esto es, también es verdadera para $a + 1$.

Teorema 13. (La ley conmutativa.) $ab = ba$.

Prueba. Esta proposición vale (por el lema) para a arbitrario cuando $b = 1$. Desde la asunción de que es verdadera para b para a arbitrario se sigue (Teorema 12 y el lema) que

$a(b + 1) = ab + a = ba + a = (b + 1)a$.

Teorema 14. $(a < b)(ac < bc) + \overline{(a < b)}(\overline{ac < bc})$.

En palabras: De $a < b$ se sigue que $ac < bc$, y a la inversa.

Prueba. Claramente, la proposición es verdadera para a y b arbitrarios cuando $c = 1$. Por tanto, ahora asumimos que vale para a y b arbitrarios para un cierto c. Entonces, de $a < b$ se sigue que $ac < bc$, por lo cual (Teorema 7) $ac + a < bc + b$, esto es (Definición 4), $a(c + 1) < b(c + 1)$. Lo inverso también debe ser verdadero; pues desde $a = b$ se seguiría que $ac = bc$, y desde $a > b$, de acuerdo con lo que ha sido probado, que $ac > bc$.

Corolario. $(ac \neq bc) + (a = b)$; esto es, de $ac = bc$ se sigue que $a = b$.

Teorema 15. $a \leq ab$.

Prueba. Verdadero para $b = 1$ (Definición 4). A partir de la asunción de que la proposición es verdadera para b se sigue, por el Teorema 3, [y] ya que (Teorema 9) $ab < ab + a$, que $a < a(b + 1)$; esto es, la proposición también es verdadera para $b + 1$.

Corolario. De $ab \leq c$ se sigue que $a \leq c$, o, alternativamente, $(ab > c) + (a \leq c)$.

§ 4. LA RELACIÓN DE DIVISIBILIDAD

Íntimamente relacionada con la multiplicación está la noción de divisibilidad, que generalmente se define por medio de una variable aparente. Pues decimos que a es divisible por b si existe un número x tal que $a = bx$. Si utilizamos los símbolos de Schröder y permitimos que $D(a, b)$ signifique la función proposicional "a es divisible por b", esta definición toma la siguiente forma:

$$D(a,b) = \sum_x (a = bx).$$

Tal definición involucra una tarea infinita – es decir, una que no puede completarse – porque el criterio de divisibilidad es si, *mediante sucesivos ensayos a lo largo de toda la secuencia de números*, podemos encontrar un número *x* tal que *a* = *bx*.

Aquí, no obstante, es fácil liberarnos de la infinitud que se adhiere a esta definición. Pues es claro que un número *x* teniendo la propiedad requerida, si tal número existe en absoluto, debe ocurrir entre los números 1, 2, …, *a*; pues de *bx* = *a* se sigue, por el Teorema 15, que $x \leq a$. Por lo tanto, la relación de divisibilidad puede definirse igualmente bien como sigue:

$$D(a,b) = \sum_{1}^{a} (a = bx) = ((a = b) + (a = 2b) + (a = 3b) + ... + (a = ab)).$$

Para estar seguros, aquí sigue ocurriendo una variable aparente *x*; *pero se extiende sobre un dominio finito solamente*, a saber, sólo los valores de 1 a *a*. Por tanto, esta definición nos proporciona un criterio de divisibilidad finito; en cada caso podemos, al completar una tarea finita, esto es, al realizar un número finito de operaciones, cerciorarnos de si la proposición *D*(*a*, *b*) vale o no. Ya que, ahora, la suma proposicional de Schröder en esta definición es finita, a su vez puede definirse por recursión, y entonces, ultimadamente, puede evitarse del todo el uso de una variable aparente. Para conseguir esto sólo necesitamos definir, como un primer paso, una relación ternaria $\Delta(a,b,c)$ que ha de significar que *a* es igual a *b* multiplicado por un número entre 1 y *c* (ambos inclusivos). La definición precisa de $\Delta(a,b,c)$ se lee como sigue:

Definición 5. $\Delta(a,b,1) = (a = b)$. $\Delta(a,b,c+1) = \Delta(a,b,c) + (a = b(c+1))$.

Por medio de la función proposicional Δ, la relación de divisibilidad *D* se define así:

Definición 6. $D(a,b) = \Delta(a,b,a)$.

Es muy fácil ver que se obtiene la equivalencia proposicional

$$\Delta(a,b,c) = \sum_{1}^{c}{}_{x} (a = bx),$$

de modo que la Definición 6 coincide completamente con la definición finita de divisibilidad mencionada arriba. De hecho, esta equivalencia vale para c = 1, porque la suma proposicional a la derecha se reduce entonces al único término $a = b$, y a partir de la asunción de que es verdadera para c se sigue que es verdadera para c + 1; pues $\sum_{1}^{c+1}{}_{x}(a = bx)$, después de todo, significa lo mismo que $\sum_{1}^{c}{}_{x}(a = bx) + (a = b(c+1))$.

Teorema 16. $(a \neq bc) + \Delta(a,b,c)$; esto es, de $a = bc$ se sigue que $\Delta(a,b,c)$.

Esto se sigue inmediatamente de la Definición 5.

Teorema 17. $\overline{\Delta(a,b,c)} + (c > c') + \Delta(a,b,c')$.

Esto también puede expresarse así: De $\Delta(a,b,c)(c \leq c')$ se sigue que $\Delta(a,b,c')$.

Prueba. Claramente, la proposición es verdadera para c' = 1. Asumimos que es verdadera para un cierto c' para valores arbitrarios de a, b, y c. De $c \leq c'+1$ se sigue, o bien que $c \leq c'$, que, junto con $\Delta(a,b,c)$ produce, de acuerdo con la asunción, $\Delta(a,b,c')$ y consecuentemente (Definición 5) también $\Delta(a,b,c'+1)$, o que $c = c' + 1$, que, junto con $\Delta(a,b,c)$, produce desde luego $\Delta(a,b,c'+1)$. Por lo tanto, la proposición también es verdadera para $c' + 1$ para valores arbitrarios de a, b, y c y entonces vale con completa generalidad.

Teorema 18. $\overline{\Delta(a,b,c)} + D(a,b)$; esto es, de $\Delta(a,b,c)$ se sigue que $D(a, b)$.

Prueba. De $\Delta(a,b,1)$, esto es, $a = b$, se sigue, por el Teorema 17, ya que (Lema 2 para el Teorema 4) $1 \leq a$, que $\Delta(a,b,a)$, esto es, $D(a, b)$. Asumamos ahora que la proposición vale para c. De $\Delta(a,b,c+1)$ se sigue (Definición 5) o bien que $\Delta(a,b,c)$, por lo cual, como consecuencia de la asunción, $D(a, b)$, o que $a = b(c + 1)$, por lo cual (Teorema 15) $c+1 \leq a$; pero de $\Delta(a,b,c+1)(c+1 \leq a)$ se sigue (Teorema 17) que $\Delta(a,b,a)$, es decir, $D(a, b)$.

Corolario a los Teoremas 16 y 18. $(a \neq bc) + D(a,b)$; esto es, de $a = bc$ se sigue que $D(a, b)$.

Teorema 19. $(a \neq bd) + \overline{\Delta(b,c,e)} + \Delta(a,c,de)$; esto es, de $(a = bd)\Delta(b,c,e)$ se sigue que $\Delta(a,c,de)$.

Prueba. Si $e = 1$, entonces $\Delta(b,c,e) = (b = c)$; de $(a = bd)\Delta(b,c,1)$ se sigue entonces que $a = cd$, por lo que (Teorema 16) $\Delta(a,c,d)$. Asumimos por tanto que la proposición es verdadera para e (con a, b, c, y d arbitrarios). De $(a = bd)\Delta(b,c,e+1)$ obtenemos (Definición 5) o bien que $(a = bd)\Delta(b,c,e)$, por lo cual $\Delta(a,c,de)$, por lo cual, a su vez, por el Teorema 17, $\Delta(a,c,d(e+1))$, ya que ($de < de + d$ por el Teorema 9) $de < d(e + 1)$, o $(a = bd)(b = c(e + 1))$, por lo cual $a = cd(e + 1)$, lo que nuevamente produce (Teorema 16) $\Delta(a,c,d(e+1))$.

Corolario a los Teoremas 18 y 19. $(a \neq bd) + \overline{D(b,c)} + D(a,c)$; esto es, de $(a = bd)D(b, c)$ se sigue que $D(a, c)$.

Pues de $(a = bd)\Delta(b,c,b)$ se sigue (Teorema 19) que $\Delta(a,c,bd)$, por lo cual (Teorema 18) $D(a, c)$.

Teorema 20. $\overline{\Delta(a,b,d)} + \overline{D(b,c)} + D(a,c)$.

Prueba. De $\Delta(a,b,1)D(b,c)$ se sigue, desde luego, que $D(a, c)$, ya que $\Delta(a,b,1) = (a = b)$. Asumimos que la proposición es verdadera para a, b, y c arbitrarios para un cierto d. De $\Delta(a,b,d+1)D(b,c)$ obtenemos (Definición 5) o bien que $\Delta(a,b,d)D(b,c)$, por lo cual, como consecuencia de la asunción, $D(a, c)$, o $(a = b(d + 1))D(b, c)$, por lo que, de acuerdo con el corolario a los Teoremas 18 y 19, se sigue que $D(a, c)$. Esto prueba que la proposición es verdadera para $c + 1$.

Corolario. $\overline{D(a,b)D(b,c)} + D(a,c)$; esto es, de $D(a, b)D(b, c)$ se sigue que $D(a, c)$.

De hecho, éste es justo el caso especial que obtenemos a partir del Teorema 20 si ponemos $d = a$.

Esta última proposición, que $D(a, c)$ se sigue de $D(a, b)D(b, c)$, está íntimamente relacionada con la proposición que establece que $a = cde$ se sigue de $(a = bd)(b = ce)$, pero

tiene un significado muy distinto. Incluso de acuerdo con la concepción ordinaria que hace uso de variables aparentes extendiéndose sobre un dominio infinito, las dos proposiciones son muy diferentes en contenido, como se vuelve claro una vez que las dos se formulan de manera precisa. Una de las proposiciones es, en símbolos de Schröder,

$$(\alpha)\quad \prod_a \prod_b \prod_c (\overline{\sum_x (a = bx)} + \overline{\sum_y (b = cy)} + \sum_z (a = cz)).$$

La otra proposición es

$$(\beta)\quad \prod_a \prod_b \prod_c \prod_d \prod_e ((a \neq bd) + (b \neq ce) + (a = cde)).$$

Cuando, no obstante, uno prueba que la proposición $\overline{D(a,b)} + \overline{D(b,c)} + D(a,c)$, o ($\alpha$), es verdadera probando la proposición (β), como usualmente se hace, lo hace sobre la base de ciertos esquemas lógicos concernientes al uso de los signos $\prod$ y $\sum$; sin embargo, en el pensamiento matemático ordinario estos esquemas son pasados por alto.

Teorema 21. $\overline{\Delta(a,c,d)} + (b \neq ce) + \Delta(a+b, d+e)$.

Prueba. De $\Delta(a,c,1)(b = ce)$, o, en otras palabras, (a = c)(b = ce), se sigue que $a + b = c(1 + e)$ y por tanto (Teorema 16) que $\Delta(a+b, c, 1+e)$. La proposición es entonces verdadera para d = 1. Asumimos que es verdadera para un cierto d y probamos, como sigue, que es verdadera para d + 1. De $\Delta(a,c,d+1)(b = ce)$ se sigue o bien que $\Delta(a,c,d)(b = ce)$, por lo que, como consecuencia de la asunción, $\Delta(a+b, c, d+e)$, que a su vez implica (Teoremas 1 y 2, y Definición 5) $\Delta(a+b, c, (d+1)+e)$, o que (a = c(d + 1))(b = ce), por lo cual $a + b = c((d + 1) + e)$, lo que nuevamente implica (Teorema 16) $\Delta(a+b, c, (d+1)+e)$.

Corolario. $\overline{\Delta(a,c,d)} + \overline{\Delta(b,c,1)} + \Delta(a+b, c, d+1)$.

Teorema 22. $\overline{\Delta(a,c,d)} + \overline{\Delta(b,c,e)} + \Delta(a+b, c, d+e)$.

Prueba. De acuerdo con el corolario al Teorema 21, esto vale para e = 1. Asumimos por tanto que la proposición es verdadera para un cierto e y probamos, como sigue, que es

verdadera para *e* + 1. De $\Delta(a,c,d)\Delta(b,c,e+1)$ obtenemos o bien $\Delta(a,c,d)\Delta(b,c,e)$ y por lo tanto, como consecuencia de la asunción, $\Delta(a+b,c,d+e)$, que a su vez implica $\Delta(a+b,c,d+(e+1))$, o $\Delta(a,c,d)(b=c(e+1))$, por lo que (Teorema 21) $\Delta(a+b,c,d+(e+1))$.

Corolario. $\overline{D(a,c)D(b,c)}+D(a+b,c)$.

En palabras: Si tanto *a* como *b* son divisibles por *c*, entonces *a* + *b* también es divisible por *c*. Pues desde $\Delta(a,c,a)\Delta(b,c,b)$ obtenemos, por el Teorema 22, $\Delta(a+b,c,a+b)$.

Lema. $\overline{\Delta(a+b,b,c+1)}+\Delta(a,b,c)$.

Prueba. De $\Delta(a+b,b,2)$ se sigue (Definición 5) o bien que *a* + *b* = *b*, lo que es imposible, ya que necesariamente (Teorema 9) *a* + *b* > *b* y ya que (Teorema 5) las relaciones > y = son mutuamente excluyentes, o que $a+b=b\cdot 2$, por lo cual *b* = *a* (ya que de *a* + *b* = *b* + *b* se debe seguir, de acuerdo con el Teorema 8, que *a* = *b*). Así, nuestro lema es verdadero para *c* = 1. Asumimos que vale para *c* y después lo probamos para *c* + 1. De $\Delta(a+b,b,c+2)$ se sigue, de hecho, o bien que $\Delta(a+b,b,c+1)$, por lo cual, como consecuencia de la asunción, $\Delta(a,b,c)$ y por lo tanto también $\Delta(a,b,c+1)$, o que *a* + *b* = *b*(*c* + 2), por lo que (Teorema 8) *a* = *b*(*c* + 1), que nuevamente implica $\Delta(a,b,c+1)$.

Al hacer uso de la sustracción, incluso antes de que sea introducida (véase § 5), también podemos establecer este lema de la siguiente manera: De $\Delta(a+b,b,c)(c>1)$ se sigue que $\Delta(a,b,c-1)$. Pues esto es verdadero cuando *c* = 1, porque la hipótesis es entonces falsa. Siempre que la proposición valga para *c*, también vale para *c* + 1; pues de $\Delta(a+b,b,c+1)$ obtenemos, de acuerdo con lo que se acaba de probar, $\Delta(a,b,c)$, y *c* = (*c* + 1) – 1 (véase la Definición 7, más abajo).

Teorema 23. $\overline{\Delta(a+bd,b,c+d)}+\Delta(a,b,c)$.

Prueba. En caso de que *d* = 1, estamos de vuelta en el lema. Asumimos por tanto que la proposición es verdadera para *d* y probamos que es verdadera para *d* + 1. De

$\Delta(a+bd+b,b,c+d+1)$ se sigue (Definición 5) o bien que $a + bd + b = b(c + d + 1)$ o que $\Delta(a+bd+b,b,c+d)$. En el primer caso, ya que (Teorema 10) $b(c + d + 1) = bc + b(d + 1)$, obtenemos (Teorema 8) $a = bc$, por lo cual (Teorema 16) $\Delta(a,b,c)$. En el segundo caso, ya que necesariamente (Lema 2 para el Teorema 4, y Teorema 9) $c + d > 1$, obtenemos, por el lema, $\Delta(a+bd,b,c+d-1)$, por lo que $\Delta(a+bd,b,c+d)$, que, de acuerdo con la asunción, implica $\Delta(a,b,c)$.

Teorema 24. $\overline{\Delta(a+b,c,d+e)} + \overline{\Delta(b,c,e)} + \Delta(a,c,d+e)$.

Prueba. Esto es verdadero para $e = 1$; pues de $\Delta(a+b,c,d+1)(b=c)$ obtenemos, de acuerdo con el lema para el Teorema 23, $\Delta(a,c,d)$, y por tanto también $\Delta(a,c,d+1)$. Asumiremos entonces que la proposición es verdadera para e (con a, b, c, y d arbitrarios) y después probaremos que es verdadera para $e + 1$ (para valores arbitrarios de a, b, c, y d). De $\Delta(a+b,c,d+(e+1))\Delta(b,c,e+1)$ obtenemos o bien que $\Delta(a+b,c,(d+1)+e)\Delta(b,c,e)$, que, de acuerdo con la asunción, implica $\Delta(a,c,(d+1)+e)$, en otras palabras $\Delta(a,c,d+(e+1))$, o $\Delta(a+b,c,d+(e+1))(b=c(e+1))$, por lo cual (Teorema 23) $\Delta(a,c,d)$, que de nuevo implica (Teorema 17) $\Delta(a,c,d+(e+1))$.

Corolario. $\overline{D(a+b,c)D(a,c)} + D(b,c)$.

Pues, primero, $\Delta(b,c,a+b)$ debe seguirse (Teorema 24) de $\Delta(a+b,c,a+b)\Delta(a,c,a)$ y, segundo, $D(b, c)$ es una consecuencia (Teorema 18) de $\Delta(b,c,a+b)$.

Después de la introducción de la sustracción, podremos escribir este teorema también como sigue: $\overline{(a>b)} + \overline{D(a,c)} + \overline{D(b,c)} + D(a-b,c)$.

Esto es, si tanto a como b son divisibles por c y si a es mayor que b (de modo que existe la diferencia $a - b$), entonces $a - b$ es divisible por c.

Teorema 25. $\overline{\Delta(a,b,c)} + (a \geq b)$.

Prueba. Claramente, la proposición vale para $c = 1$. Si asumimos que vale para c, de $\Delta(a,b,c+1)$ obtenemos o bien que $\Delta(a,b,c)$, que produce entonces $a \geq b$, o $a = b(c + 1)$, de donde (Teorema 15) $a \geq b$ también se sigue.

Corolario 1. $\overline{D(a,b)} + (a \geq b)$.

Corolario 2. $\overline{D(a,b)} + \overline{D(b,a)} + (a = b)$.

Pues de $(a \geq b)(b \geq a)$ debe seguirse (Teorema 5) que $a = b$.

Teorema 26. $\Delta(a,b,d)\Delta(ac,bc,d) + \overline{\Delta(a,b,d)\Delta(ac,bc,d)}$.

En palabras: De $\Delta(a,b,d)$ se sigue que $\Delta(ac,bc,d)$, y a la inversa.

Prueba. La proposición es verdadera para $d = 1$; pues de $ac = bc$ se sigue, de acuerdo con el corolario al Teorema 14, que $a = b$, y a la inversa, de $a = b$ se sigue desde luego que $ac = bc$. Asumimos que la proposición es verdadera para d y probamos que es verdadera para $d + 1$. De $\Delta(a,b,d+1)$ obtenemos o bien que $\Delta(a,b,d)$, que de acuerdo con la asunción implica $\Delta(ac,bc,d)$ y por lo tanto también $\Delta(ac,bc,d+1)$, o $a = b(d + 1)$, por lo cual (Teoremas 11 y 13) $ac = (b(d + 1))c = b((d + 1)c) = b(c(d + 1)) = (bc)(d + 1)$, y de $ac = bc(d + 1)$ se sigue de nuevo (Teorema 16) que $\Delta(ac,bc,d+1)$. Igualmente, de $\Delta(ac,bc,d+1)$ obtenemos o bien que $\Delta(ac,bc,d)$, por lo que $\Delta(a,b,d)$ y por lo tanto también $\Delta(a,b,d+1)$, o $ac = bc(d + 1) = b(d + 1)c$, por lo que, como consecuencia del corolario al Teorema 14, $a = b(d + 1)$, por lo que (Teorema 16) $\Delta(a,b,d+1)$.

Corolario. $D(a,b)D(ac,bc) + \overline{D(a,b)}\,\overline{D(ac,bc)}$.

Teorema 27. $(a \neq bd) + \overline{\Delta(d,c,e)} + \Delta(a,bc,e)$.

Prueba. Verdadero para $e = 1$. Asumimos entonces que la proposición es verdadera para e y probamos que es verdadera para $e + 1$. De $\Delta(d,c,e+1)$ obtenemos o bien que $\Delta(d,c,e)$, que junto con $a = bd$ produce, de acuerdo con la asunción, $\Delta(a,bc,e)$ y por tanto

también $\Delta(a, bc, e+1)$, o $d = c(e + 1)$, que junto con $a = bd$ produce (Teorema 11) $a = (bc)(e + 1)$, por lo que (Teorema 16) $\Delta(a, bc, e+1)$.

§ 5. SUSTRACCIÓN Y DIVISIÓN. FUNCIONES DESCRIPTIVAS CON UN DOMINIO RESTRINGIDO DE EXISTENCIA

La sustracción, como es consabido, puede definirse de la siguiente manera:

Definición 7. $(c - b = a) = (c = a + b)$.

Es claro que de esta manera es definida una función descriptiva $c - b$, llamada la *diferencia*; pues, por medio de la ecuación $a + b = c$, a está determinado de forma única por b y c. Ésta, no obstante, es una función descriptiva con un dominio restringido de existencia; pues, si $c \leq b$, no puede obtenerse ninguna ecuación de la forma $c = a + b$, y entonces, de acuerdo con la Definición 7, se obtiene la desigualdad $c - b \neq a$ para cada número a; es decir, $c - b$ no es igual a ningún número. Por otro lado, puede probarse que $c - b$ ciertamente tendrá un valor cuando $c > b$. Uno estaría inclinado a formular esta proposición así:

$$\overline{(c > b)} + \sum_{x} (x + b = c),$$

donde la sumación proposicional sobre x tendría que extenderse sobre "todos" los números desde 1 hasta ∞. Pero aquí tampoco es necesario aducir un infinito real tal; de hecho, podemos probar la siguiente proposición:

$$\overline{(c > b)} + \sum_{1}^{c}{}_{x} (x + b = c),$$

que, después de todo, servirá más fácilmente para asegurar la existencia de un valor para $c - b$. Pero la función proposicional

$$\sum_{1}^{z}{}_{u} (u + y = x) = L(x, y, z)$$

de las tres variables *x*, *y*, y *z* de nuevo puede definirse recursivamente, de modo que podemos evitar del todo la variable aparente *u*. El teorema que ha de probarse es entonces, obviamente, el siguiente:

Teorema 28. $\overline{c > b} + L(c, b, c)$.

En palabras, este teorema se lee como sigue: Si $c > b$, entre los números desde 1 hasta *c* existe un número *x* tal que $x + b = c$, o, en otras palabras, $x = c - b$.

Necesitamos la definición recursiva de la función *L* y unos pocos teoremas sencillos acerca de ella.

Definición 8. $L(x, y, 1) = (x = 1 + y)$. $L(x, y, z + 1) = L(x, y, z) + (x = (z + 1) + y)$.

Teorema 29. $\overline{L(x, y, z)(z \leq z')} + L(x, y, z')$.

Prueba. Verdadero para $z' = 1$. Asumo que es verdadero para z' y a partir de ahí pruebo que es verdadero para $z' + 1$. En realidad, de $z \leq z'+1$ se sigue, o bien que $z \leq z'$, que junto con $L(x, y, z)$, de acuerdo con la asunción, produce $L(x, y, z')$ y por lo tanto (Definición 8) también $L(x, y, z' + 1)$, o que $z = z' + 1$, que con $L(x, y, z)$ obviamente produce $L(x, y, z' + 1)$.

Teorema 30. $\overline{L(x, y, z)} + L(x+1, y, z+1)$.

Prueba. Verdadero cuando $z = 1$; pues de $x = 1 + y$ se sigue (Teoremas 1 y 2) que $x + 1 = (1 + y) + 1 = 1 + (y + 1) = 1 + (1 + y) = (1 + 1) + y$. Asumo que la proposición es verdadera para *z* y pruebo que es verdadera para $z + 1$. De $L(x, y, z + 1)$ se sigue (Definición 8), o bien que $L(x, y, z)$, por lo cual, de acuerdo con la asunción hecha, $L(x + 1, y, z + 1)$ y por tanto también $L(x + 1, y, z + 2)$, o que $x = (z + 1) + y$, por lo que (Teoremas 1 y 2) $x + 1 = ((z + 1) + y) + 1 = (z + 1) + (y + 1) = (z + 1) + (1 + y) = (z + 2) + y$, por lo que (Definición 8) $L(x + 1, y, z + 2)$.

Ahora puede llevarse a cabo la prueba del Teorema 28.

La proposición declarada como Teorema 28 es ciertamente verdadera para $c = 1$; pues, en ese caso, $\overline{1 > b}$ ya es verdadero. Asumo por tanto que es verdadera para *c* y pruebo

que es verdadera para $c + 1$. De $c + 1 > b$ obtenemos (véase el Lema 1 para el Teorema 4, el Lema para el Teorema 5, y el Teorema 8), o bien que $c > b$, que, de acuerdo con la asunción hecha, nos da $L(c, b, c)$, de donde se sigue además (Teorema 30) que $L(c + 1, b, c + 1)$, o $c = b$, por lo que (Teorema 2) $c + 1 = b + 1 = 1 + b$; por lo tanto (Definición 8) $L(c + 1, b, 1)$, y por lo tanto (Teorema 29) nuevamente $L(c + 1, b, c + 1)$.

La división se introduce de una manera análoga a la sustracción.

Definición 9. $(c/b = a) = (c = ab)$.

La expresión c/b, llamada el *cociente*, es claramente, una vez más, una función con un dominio restringido de definición; pues de $c = ab$ se sigue (corolario a los Teoremas 16 y 18) que $D(c, b)$, de modo que c/b tiene un valor sólo si $D(c, b)$ es verdadero. A la inversa, esto también es suficiente; pues la proposición $D(c, b)$ o, en otras palabras (véase la Definición 6), $\Delta(c, b, c)$, es equivalente a la suma proposicional

$$\sum_{1}^{c}{}_{x}(c = bx)$$

(véase la p. 15), y $(c = bx) = (c = xb)$, de modo que esta suma proposicional puede formularse, en palabras, así: Entre los números de 1 hasta c [inclusivos] existe un número x tal que $c = xb$, o, en otras palabras, $c/b = x$.

La función proposicional $D(c, b)$ es por tanto completamente equivalente a la afirmación de que entre 1 y c existe un valor para c/b.

Ofrezco ahora algunos teoremas simples acerca de las diferencias y los cocientes. Presumiblemente, no tengo que ofrecer las pruebas, que son triviales; estos teoremas son, después de todo, meras transformaciones de los más simples teoremas acerca de las sumas y los productos.

Teorema 31_{+}. $(a - b) + b = a$.

$31_{\times}$. $(a/b)b = a$.

32_{+}. $(a - b) + c = (a + c) - b$.

$32_{\times}$. $(a/b)c = ac/b$.

33_{+}. $(a - b) - c = a - (b + c)$.

$33_{\times}$. $(a/b)/c = a/bc$.

34_{+}. $a - (b - c) = (a - b) + c$.

$34_{\times}$. $a/(b/c) = (a/b)c$.

35. $(a - b)c = ac - bc$.

36a. $(a/c) + (b/c) = (a + b)/c$.

36b. $(a/c) - (b/c) = (a - b)/c$.

§6. MÁXIMO COMÚN DIVISOR Y MÍNIMO COMÚN MÚLTIPLO

Las definiciones habituales del máximo común divisor y del mínimo común múltiplo de dos números hacen uso de variables aparentes que se extienden sobre un dominio infinito. En símbolos de Schröder, estas definiciones tienen la siguiente forma:

(c es el máximo común divisor de a y b)

$$= D(a,c)D(b,c)\prod_{x}(\overline{D(a,x)} + \overline{D(b,x)} + D(c,x)),$$

(c es el mínimo común múltiplo de a y b)

$$= D(c,a)D(c,b)\prod_{x}(\overline{D(x,a)} + \overline{D(x,b)} + D(x,c)).$$

Ya que, no obstante, $x \leq a$ se sigue (Corolario 1 al Teorema 25) de $D(a, x)$, el dominio infinito sobre el que se extiende la variable en la definición del máximo común divisor puede inmediatamente reducirse a un [dominio] finito, y también podemos escribir

(c es el máximo común divisor de a y b)

$$= D(a,c)D(b,c)\prod_{1}^{a}{}_{x}(\overline{D(a,x)} + \overline{D(b,x)} + D(c,x)).$$

Sin embargo, una desventaja de esta definición es que es asimétrica con respecto a *a* y *b*. Pero esto también puede remediarse fácilmente, porque sobre el signo $\prod$ podemos escribir *a* + *b* en lugar del límite superior *a*, o incluso mejor Min(*a*, *b*), donde Min(*a*, *b*) es el mínimo de los números *a* y *b*. Para la definición del mínimo común múltiplo, una reducción tal del rango de la variable a un dominio finito no puede llevarse a cabo tan fácilmente.

En lo que sigue introduciré estas nociones de un modo distinto, uno que evita por completo las variables aparentes. Empero, al hacer esto, debo hacer uso del método de definición recursivo de un modo distinto al de antes (aunque, como mostraré en breve, la diferencia es puramente superficial). Hasta ahora, siempre hemos ofrecido definiciones recursivas estrictamente como sigue: definimos una noción para el número 1 y después, sobre la asunción de que la definición para un número arbitrariamente dado *n* ya está completa, definimos la noción para *n* + 1. Además, aquí utilizaremos un principio lógico formal, a saber, que podemos ofrecer definiciones separadas para cada uno de los casos mutuamente excluyentes. Introduzco dos funciones descriptivas de dos variables *a* y *b*, a saber, $a \wedge b$ y $a \vee b$, que más tarde mostraré que son idénticas al máximo común divisor y al mínimo común múltiplo, respectivamente.

Definición 10. $\begin{array}{l}((a \neq b) + (a \wedge b = a))(\overline{(a > b)} + (a \wedge b = (a - b) \wedge b))(\overline{a < b}) \\ +(a \wedge b) = a \wedge (b - a))).\end{array}$

Esta es una definición recursiva perfectamente legítima de la función descriptiva $a \wedge b$; si asumimos que ya está definida para aquellos valores de *a* y *b* para los que *a* + *b* < *n*, entonces, por la Definición 10, está definida para *a* + *b* = *n*. Pues, si *a* y *b* son dos números tales que *a* + *b* = *n*, entonces *a* = *b* o *a* > *b* o *a* < *b*, y estos tres casos son mutuamente excluyentes, mientras que la Definición 10 especifica, para cada caso, qué ha de significar $a \wedge b$. Más aún, la Definición 10 nos da el valor de $a \wedge b$ cuando *a* + *b* = 2, en cuyo caso necesariamente *a* = *b* = 1.

En las pruebas de algunos de los teoremas que siguen también haré uso de la inducción matemática de un modo distinto al de antes (aunque, como mostraré en breve, la diferencia es puramente superficial). Hasta ahora, esta inferencia inductiva siempre se ha hecho así: probamos una proposición para el número 1 y después la probamos para $n + 1$ sobre la asunción de que vale para n. Ahora, probaré también inductivamente como sigue: pruebo una proposición para 1, y después, asumiendo que vale para un número arbitrario < n, la pruebo para n.

Lema. $a \wedge 1 = 1$.

Prueba. Verdadero para $a = 1$ como consecuencia de la Definición 10. Si asumimos que la proposición es verdadera para a, obtenemos, de acuerdo con la Definición 10, ya que (Teorema 9) $a+1>1, (a+1)\wedge 1 = a \wedge 1$, y por lo tanto también $(a+1)\wedge 1 = 1$.

Igualmente puede probarse que $1 \wedge a = 1$. En general, desde luego, $a \wedge b = b \wedge a$.

Teorema 37. $D(a, a \wedge b)D(b, a \wedge b)$.

Prueba. Esta proposición es verdadera para b arbitrario para $a = 1$ y para a arbitrario para $b = 1$; pues, de acuerdo con el lema, $a \wedge 1 = 1 \wedge b = 1$. Asumo que la proposición es verdadera para $a + b < n$ y después pruebo que es verdadera para $a + b = n$. Pues si, primero, $a = b$, entonces, de acuerdo con la Definición 10, $a \wedge b = a$, y consecuentemente, la proposición vale. Si, segundo, $a > b$, entonces $(a - b) + b < n$, y entonces, como consecuencia de la asunción, $D(a-b,(a-b)\wedge b)D(b,(a-b)\wedge b)$ vale. Pero, de acuerdo con la Definición 10, $(a-b)\wedge b = a \wedge b$, y por lo tanto obtenemos $D(a-b, a\wedge b)D(b, a\wedge b)$, desde donde, por el corolario al Teorema 22 y por el Teorema 31_+, también se sigue $D(a, a\wedge b)$. Por tanto, la proposición también es verdadera en este caso. Si, tercero, $a < b$, podemos proceder de un modo exactamente análogo.

Teorema 38. $\overline{D(a,c)D(b,c)} + D(a \wedge b, c)$.

Prueba. La proposición vale para b arbitrario cuando $a = 1$ y para a arbitrario cuando $b = 1$; porque entonces se sigue, de $D(a, c)$ o $D(b, c)$, respectivamente, que $c = 1$. Asumo que la proposición vale para a y b tales que harán que $a + b < n$, y desde esa

asunción pruebo que vale para *a* y *b* tales que harán que *a* + *b* = *n*. Por lo tanto, sean *a* y *b* números tales que *a* + *b* = *n*. Primero, entonces, puede ser que *a* = *b*; en este caso, de acuerdo con la Definición 10, $a \wedge b = a,$ y la definición es por lo tanto verdadera. Segundo, puede ser que *a* > *b*. Ya que $(a - b) + b < n, D((a-b) \wedge b, c)$ debe seguirse, por la asunción, de *D*(*a* – *b*, *c*)*D*(*b*, *c*); pero *D*(*a* – *b*, *c*) es, a su vez, una consecuencia de *D*(*a*, *c*)*D*(*b*, *c*) (corolario al Teorema 24), y finalmente (Definición 10) en este caso $(a-b) \wedge b = a \wedge b.$ Así, $D(a \wedge b, c)$ se sigue de *D*(*a*, *c*)*D*(*b*, *c*). En el tercer caso, *a* < *b*, procedemos exactamente de la misma manera.

Los teoremas 37 y 38 expresan juntos las propiedades características del máximo común divisor.

Teorema 39. $\overline{D(a,b)} + (a \wedge b = b).$

Prueba. Como consecuencia del Teorema 37 tenemos $D(b, a \wedge b)$. Por el otro lado, $D(a \wedge b, b)$ se sigue (Teorema 38) de *D*(*a*, *b*)*D*(*b*, *b*). De $D(b, a \wedge b)D(a \wedge b, b),$ no obstante, se sigue (Corolario 2 al Teorema 25) que $a \wedge b = b.$

Corolario. $ab \wedge a = a.$

Teorema 40. $ac \wedge bc = (a \wedge b)c.$

Prueba. La proposición es verdadera para *a* arbitrario para *b* = 1 y para *b* arbitrario para *a* = 1, como se sigue inmediatamente del lema para el Teorema 37 y del corolario al Teorema 39. Asumimos, por tanto, que ya hemos probado que la proposición vale para *a* + *b* < *n*, y sobre esta base probamos que vale para *a* y *b* tales que *a* + *b* = *n*. Es posible, primero, que *a* = *b*. Entonces también *ac* = *bc*, y, de acuerdo con la Definición 10, tenemos $ac \wedge bc = ac$ y $a \wedge b = a$, que producen $ac \wedge bc = (a \wedge b)c$. El segundo caso es *a* > *b*. Ya que (*a* – *b*) + *b* < *n*, tenemos, de acuerdo con la asunción hecha, $(a-b)c \wedge bc = ((a-b) \wedge b)c.$ Pero además $a \wedge b = (a-b) \wedge b$, y como, entonces, también (Teorema 14) *ac* > *bc*, necesariamente tenemos, de acuerdo con la Definición 10, $(ac-bc) \wedge bc = ac \wedge bc.$ Finalmente (Teorema 35), (*a* – *b*)*c* = *ac* – *bc*. Así, se sostiene la

ecuación $ac \wedge bc = (a \wedge b)c$. En el tercer caso, cuando $a < b$, procedemos desde luego de la misma manera.

Definición. Decimos que dos números *a* y *b* son *relativamente primos* si $a \wedge b = 1$. No introduzco un símbolo especial para esto, porque siempre podemos utilizar la ecuación corta $a \wedge b = 1$ como una expresión de ello.

Teorema 41. $\overline{D(ac, b)(a \wedge b = 1)} + D(c, b)$.

Este es el consabido teorema de que un número *b* que divide un producto *ac* mientras que es relativamente primo al factor *a*, debe dividir el otro factor, *c*.

Prueba. De $D(ac, b)D(bc, b)$ se sigue (Teorema 38) que $D(ac \wedge bc, b)$. Pero de $a \wedge b = 1$ se sigue (Teorema 40) que $ac \wedge bc = c$, de modo que $D(c, b)$ debe ser verdadero.

Teorema 42. $\overline{(a \wedge b = 1)D(a, a')} + (a' \wedge b = 1)$.

Prueba. Como consecuencia del Teorema 37, se sostiene que $D(a', a' \wedge b)D(b, a' \wedge b)$; pero de $D(a, a')D(a', a' \wedge b)$ se sigue (corolario al Teorema 20) que $D(a, a' \wedge b)$, que junto con $D(b, a' \wedge b)$ produce (Teorema 38) $D(a \wedge b, a' \wedge b)$. Entonces, de $(a \wedge b = 1)D(a, a')$ debe por lo tanto seguramente seguirse que $a' \wedge b = 1$; pues de $D(1, \alpha)$ se sigue (Corolario 1 al Teorema 25) que $\alpha = 1$.

Teorema 43. $(a \wedge b \neq 1) + (a \wedge c \neq 1) + (a \wedge bc = 1)$.

Prueba. Si un número *d* divide a *a* así como a *bc*, entonces necesariamente (Teorema 42) $d \wedge b = 1$ así como $d \wedge c = 1$, siempre que se obtenga $(a \wedge b = 1)(a \wedge c = 1)$. Además, de acuerdo con el Teorema 41, debe seguirse de $D(bc, d)(c \wedge d = 1)$ que $D(b, d)$. Pero de $D(b, d)$ se sigue (Teorema 39) que $b \wedge d = d$; por el otro lado, teníamos que $b \wedge d = 1$; por lo tanto, $d = 1$. Pero ahora (Teorema 37) $a \wedge bc$ divide a *a* así como a *bc*; por lo tanto, $a \wedge bc = 1$.

Teorema 44. (Generalización del Teorema 41.) $\overline{D(ac, b)} + D(c, b / (a \wedge b))$.

Prueba. En primer lugar, es claro que necesariamente $(a/(a \wedge b)) \wedge (b/a \wedge b)) = 1$; pues, por el Teorema 40, tenemos [que] $((a/(a \wedge b)) \wedge (b/a \wedge b)))(a \wedge b) = a \wedge b$. De $D(ac, b)$ se sigue (corolario al Teorema 26) que $D(ac/(a \wedge b),\ b/(a \wedge b))$, por lo que, de acuerdo con el Teorema 41, $D(c, b/(a \wedge b))$, ya que $a/(a \wedge b)$ y $b/(a \wedge b)$ son relativamente primos.

Definición 11. $a \vee b = ab/(a \wedge b)$.

Teorema 45. $\Delta(a,b,d)D(a,c) + \Delta(a,b \vee c,d)$.

Prueba. Verdadero cuando $d = 1$; pues de $(a = b)D(a, c)$ se sigue que $D(b, c)$, por lo que (Teorema 39) $b \wedge c = c$ y consecuentemente, por la Definición 11, $b \vee c = b$. Asumo que la proposición es verdadera para d y pruebo que es verdadera para $d + 1$. De $\Delta(a,b,d+1)$ se sigue, o bien que $\Delta(a,b,d)$, que junto con $D(a, c)$ produce, de acuerdo con la asunción, $\Delta(a,b \vee c,d)$ y por tanto también $\Delta(a,b \vee c,d+1)$, o que $a = b(d + 1)$, que junto con $D(a, c)$ produce (Teorema 44) $D(d+1, c/(b \wedge c))$. Pero desde $(a = b(d+1))D(d+1, c/(b \wedge c))$ obtenemos nuevamente $\Delta(a,b \vee c,d+1)$, por el Teorema 27.

Teorema 46. $D(a \vee b, a)D(a \vee b, b)$.

Prueba. De acuerdo con el Teorema 37, se sostiene que $D(a, a \wedge b)$, por lo que (corolario al Teorema 26) $D(ab/(a \wedge b), b)$, esto es, $D(a \vee b, b)$. Igualmente, $D(b, a \wedge b)$ implica que $D(a \vee b, a)$ es verdadero.

Teorema 47. $\overline{D(c,a)D(c,b)} + D(c, a \vee b)$.

Este es meramente un caso especial del Teorema 45, que resulta cuando se igualan d y a.

Juntos, los Teoremas 46 y 47 expresan las propiedades características del mínimo común múltiplo de dos números a y b. Así, $a \vee b$ denota al mínimo común múltiplo de a y b.

Un caso especial importante del Teorema 47 es aquel en el que $a \wedge b = 1$. De $D(c,a)D(c,b)(a \wedge b = 1)$ se sigue que $D(c, ab)$.

Tenemos, correspondiente al Teorema 39,

Teorema 48. $\overline{D(a,b)} + (a \vee b = a)$.

Que esta proposición es verdadera se sigue inmediatamente del Teorema 39 y de la Definición 11.

Tenemos, correspondiente al Teorema 40,

Teorema 49. $ac \vee bc = (a \vee b)c$.

Prueba. $ac \vee bc = (ac \cdot bc) / (ac \wedge bc) = (ac \cdot bc) / (a \wedge b)c = (ab \cdot c) / (a \wedge b) = (a \vee b)c$; aquí, se hace uso de los Teoremas 11, 13, 32, y 40.

Quiero concluir esta sección ofreciendo una prueba de que los tipos más supuestos de definición recursiva y de prueba recursiva utilizados antes difieren sólo formalmente, no realmente, de la prueba recursiva simple ordinaria que va de *n* a *n* + 1. La forma estándar de una definición recursiva, después de todo, es como sigue: una función proposicional $U(x)$ se define primero para $x = 1$ y después, si ya se ha definido $U(n)$, para $x = n + 1$. Pero antes también consideramos definiciones recursivas del siguiente tipo: primero definimos $U(1)$ y después, asumiendo haber definido $U(m)$ para $m < n$ arbitraria, $U(n)$. Es claro que el valor de la función proposicional $U(y)(y \leq x)$ para *x* e *y* arbitrariamente elegidas será conocido si $U(y)$ está definida para la *y* en cuestión; pero, a la inversa, también será conocido si $U(y)$ es verdadera o falsa para una $y \leq x$ si $U(y)(y \leq x)$ está definida para la *x* y la *y* en cuestión. Para definir $U(x)$, por lo tanto, será suficiente con definir $U(y)(y \leq x)$ para *x* e *y* arbitrarias; aquí podemos observar que, para cada par de valores (x, y) para los que $y > x$, $U(y)(y \leq x)$ debe necesariamente ser falsa. Para especificar el valor de $U(y)(y \leq x)$ de manera general, podemos ahora aplicar el procedimiento recursivo estándar. Para $x = 1$, $U(y)(y \leq x)$ es necesariamente falsa, de acuerdo con la definición de la relación "menor que", siempre que $y > 1$; así, meramente necesitamos especificar $U(1)$ para tener el valor de $U(y)(y \leq 1)$ para *y* arbitraria. Además, especificamos el valor de $U(y)(y \leq x)$ para $x + 1$ para *y* arbitraria cuando ya ha sido especificado para *x* para *y* arbitraria. Siempre que $y > x + 1$, $U(y)(y \leq x+1)$ es falsa. Cuando $y \leq x$, ya conocemos el valor de la función

proposicional; esto es, meramente debemos especificar $U(x + 1)$. Por lo tanto, *especificar el valor de* $U(x + 1)$ *cuando esta función se considera como conocida para* $y < x + 1$ *arbitraria equivale precisamente a especificar el valor de la función proposicional* $U(x)(y \leq x)$ *para* $x = n + 1$ *para y arbitraria cuando esta función proposicional ya es conocida para* $x = n$ *para y arbitraria*. Así, el tipo aparentemente divergente de definición recursiva ha sido reducido a la forma estándar.

Es igualmente fácil ver que la más complicada forma de inferencia inductiva, que consiste en probar una proposición para *n* cuando se asume que es verdadera para $m < n$ arbitraria, difiere sólo formalmente, pero no realmente, de la forma estándar de inferencia inductiva, la inferencia de *n* a $n + 1$. Decir que $U(y)$ ha sido probada para $y < x$ arbitraria es, después de todo, equivalente a decir que $(y \geq x) + U(y)$ ha sido probado para esta *x* para *y* arbitraria, y entonces no es difícil ver que *probar* $U(x)$, *asumiendo que* $U(y)$ *es verdadera para* $y < x$ *arbitraria, es equivalente a probar* $(y \geq x + 1) + U(y)$ *para y arbitraria cuando ya se ha probado* $(y \geq x) + U(y)$ *para y arbitraria*.

§ 7. LA NOCIÓN DE NÚMERO PRIMO

Definición 12. $P(x, 1)$ es verdadero. $P(x, y + 1) = P(x, y)((x = y + 1) + \overline{D(x, y + 1)})$.

Definición 13. $P(x) = P(x, x)(x \neq 1)$.

La función proposicional $P(x)$ significa "*x* es un número primo".

Definición 14. $De(x, 1)$ es falso. $De(x, y + 1) = De(x, y) + D(x, y + 1)(y + 1 < x)$.

Definición 15. $Dp(x, 1)$ es falso. $Dp(x, y + 1) = Dp(x, y) + D(x, y + 1)P(y + 1)$.

Definición 16. $T(1)$ es verdadero. $T(x + 1) = T(x)Dp(x + 1, x + 1)$.

En la definición habitual de la noción de número primo se utiliza una variable aparente. Si se considera como ya definida la relación de divisibilidad, puede darse como sigue la definición de número primo:

$$P(x) = (x \neq 1)\prod_{y} \overline{(D(x, y)} + (y = 1) + (y = x)).$$

Aquí ocurre un producto proposicional infinito (o, en otras palabras, el "siempre" de Russell y Whitehead). Pero en las Definiciones 12 y 13 de arriba no ocurre ninguna variable aparente. Puede evitarse el producto proposicional infinito, porque inmediatamente puede ser remplazado por uno finito. Pues, de acuerdo con el corolario al Teorema 25, necesariamente tenemos que $y \leq x$ si $D(x, y)$ es verdadero, y de allí se sigue que en el producto infinito todos los factores para los que vale que $y > x$ se vuelven inoperantes. Consecuentemente, podemos definir igual de bien a $P(x)$ así:

$$P(x) = (x \neq 1)\prod_{1}^{x} {}_{y} \overline{(D(x, y)} + (y = 1) + (y = x)).$$

El producto proposicional finito que ocurre aquí no es sino el factor $P(x, x)$ del lado derecho de la Definición 13; $P(x, y)$ está recursivamente definida por la Definición 12 y es equivalente al producto

$$\prod_{1}^{y} {}_{z} \overline{(D(x, z)} + (z = x)).$$

Precisamente porque estos productos proposicionales son finitos, pueden definirse recursivamente, y por tanto las variables aparentes se evitan por completo.

Las restantes funciones proposicionales introducidas arriba, *De*, *Dp*, y *T*, tienen, como puede verse fácilmente, los siguientes significados en palabras:

De(x, y) significa "x es divisible por un número > 1, $\leq y$, y $< x$".

Dp(x, y) significa "x es divisible por un primo $\leq y$".

T(x) significa que todos los números de 2 a x son divisibles por al menos un primo $\leq x$.

Teorema 50. $\overline{P(x, y)D(x, z)(z \leq y)} + (z = 1) + (z = x).$

Prueba. Cuando y = 1, la proposición es claramente verdadera. Pruebo la proposición para y + 1, asumiendo que vale para y. De $z \leq y+1$ se sigue o bien que $z \leq y$ o que $z = y + 1$. De $z \leq y$, junto con $P(x, y)$ (que se sigue de $P(x, y + 1)$) y $D(x, z)$, obtenemos, de acuerdo con la asunción, o bien que $z = 1$ o [que] $z = x$. De $z = y + 1$, junto con $(x = y+1) + \overline{D(x, y+1)}$ (que también se sigue de $P(x, y + 1)$) y $D(x, z)$, obtenemos $z = x$.

Corolario. $\overline{P(x)D(x, y)} + (y = 1) + (y = x)$.

Pues de $P(x, x)(x \neq 1)D(x, y)$ se sigue (Teorema 25) que $P(x, x)D(x, y)(y \leq x)$, por lo que, de acuerdo con el teorema recién probado, $(y = 1) + (y = x)$.

Teorema 51. $\overline{P(y)} + D(x, y) + (x \wedge y = 1)$.

Prueba. Ya que $D(y, x \wedge y)$ es verdadero (Teorema 37), necesariamente tenemos, siempre que valga que $P(y)$, o bien que $x \wedge y = 1$ o que $x \wedge y = y$, de acuerdo con el corolario al Teorema 50; pero de $x \wedge y = y$ se sigue (Teorema 37) que $D(x, y)$.

Teorema 52. $\overline{D(xy, z)P(z)} + D(x, z) + D(y, z)$.

Prueba. De acuerdo con el teorema precedente, si $P(z)$ es verdadera, o bien vale $D(x, z)$ o $x \wedge z = 1$. De $D(xy, z)P(z)$, por lo tanto, debe seguirse que $D(x, z)$ o que $D(xy, z)(x \wedge z = 1)$; pero de $D(xy, z)(x \wedge z = 1)$ se sigue a su vez (Teorema 41) que $D(y, z)$.

Teorema 53. $P(x, y) + De(x, y)$.

Prueba. Verdadero para y = 1, porque (Definición 12) $P(x, 1)$ ya es verdadera. Asumo que la proposición es verdadera para y, y sobre esta base pruebo que es verdadera para y + 1. De $\overline{P(x, y+1)}$ se sigue (Definición 12) o bien que $\overline{P(x, y)}$, por lo que tenemos $De(x, y)$ y consecuentemente (Definición 14) también $De(x, y + 1)$, o que $(x \neq y+1)D(x, y+1)$, por lo que (Corolario 1 al Teorema 25) $D(x, y + 1)(y + 1 < x)$, que, habida cuenta de la Definición 14, produce $De(x, y + 1)$.

Teorema 54. $\overline{(y \leq y')Dp(x, y)} + Dp(x, y')$.

Prueba. Claramente verdadero cuando $y' = 1$. Asumo que la proposición es verdadera para y' y después pruebo que es verdadera para $y' + 1$. De $y \leq y'+1$ se sigue o bien que $y \leq y'$, que junto con $Dp(x, y)$, de acuerdo con la asunción, implica $Dp(x, y')$ y por lo tanto (Definición 15) también $Dp(x, y' + 1)$, o que $y = y' + 1$, que junto con $Dp(x, y)$ implica desde luego que $Dp(x, y' + 1)$.

Teorema 55. $\overline{D(x, y)Dp(y, z)} + Dp(x, z)$.

Prueba. Para $z = 1$, esta proposición es verdadera, ya que (Definición 15) $Dp(y, 1)$ es falso. Asumo por tanto que la proposición vale para z y después pruebo que vale para $z + 1$. De $Dp(y, z + 1)$ obtenemos (Definición 15) o bien que $Dp(y, z)$, que junto con $D(x, y)$ implica $Dp(x, z)$ y consecuentemente también $Dp(x, z + 1)$, o [que] $D(y, z + 1)P(z + 1)$, que junto con $D(x, y)$, de acuerdo con el corolario al Teorema 20, hace verdadero a $D(x, z + 1)$, por lo que, de acuerdo con la Definición 15, $Dp(x, z + 1)$.

Teorema 56. $\overline{Dp(x, y)} + Dp(x, x)$.

Prueba. De acuerdo con la Definición 15, esto debe ser verdadero para $y = 1$. Asumo que es verdadero para y, y pruebo que es verdadero para $y + 1$. De $Dp(x, y + 1)$ se sigue, o bien que $Dp(x, y)$, por lo que tenemos $Dp(x, x)$, o que $D(x, y + 1)P(y +1)$, por lo que, de acuerdo con el Corolario 1 al Teorema 25, $y+1 \leq x$; pero de $Dp(x, y+1)(y+1 \leq x)$ se sigue (Teorema 54) que $Dp(x, x)$.

Teorema 57. $\overline{De(x, y)T(y)} + Dp(x, x)$.

Prueba. La proposición vale para $y = 1$; para $De(x, 1)$ es falsa. Asumo que la proposición vale para y, y la pruebo para $y + 1$. De $De(x, y + 1)T(y + 1)$ se sigue o bien que $De(x, y)T(y + 1)$, por lo que (Definición 16) $De(x, y)T(y)$, por lo que, como consecuencia de la asunción, $Dp(x, x)$, o que $D(x, y + 1)(y + 1 < x)T(y + 1)$, por lo que (Definición 16) $D(x, y + 1)(y + 1 < x)Dp(y + 1, y + 1)$, por lo que a la vez, de acuerdo con el Teorema 55, $Dp(x, y + 1)(y + 1 < x)$, lo que implica (Teorema 54) que se sostiene que $Dp(x, x)$.

Teorema 58. $T(x)$.

Prueba. Verdadero para $x = 1$ (Definición 16). Pruebo que $T(x + 1)$ se sostiene sobre la asunción de que $T(x)$ lo hace. De acuerdo con la Definición 16, sólo necesito probar que $Dp(x + 1, x + 1)$ para conseguir esto. De acuerdo con la Definición 13, tenemos que $P(x + 1)$ o que $\overline{P(x+1, x+1)}$. De $P(x + 1)D(x + 1, x + 1)$ se sigue, de acuerdo con la Definición 15, que $Dp(x + 1, x + 1)$. De $\overline{P(x+1, x+1)}$ se sigue, de acuerdo con el Teorema 53, que $De(x + 1, x + 1)$, que debe (véase la Definición 14) tener a $De(x + 1, x)$ como una consecuencia; pero de $De(x + 1, x)T(x)$ se sigue, de acuerdo con el Teorema 57, que $Dp(x + 1, x + 1)$.

Corolario. $Dp(x + 1, x + 1)$.

Pues de $T(x + 1)$ se sigue (Definición 16) que $Dp(x + 1, x + 1)$.

Este es el teorema al efecto de que cada número > 1 es divisible por al menos un primo. $Dp(x + 1, x + 1)$ realmente significa que $x + 1$ es divisible por al menos un primo $\leq x+1$.

Ahora, para poder formular y probar el teorema de que cada número > 1 es un producto de primos, introduzco una relación ternaria $P(x, y, z)$ que ha de significar "x es el producto de y primos que son todos $\leq z$".

Definición 17. Es falso que

$$P(x, y, z) = P(x, y, z-1) + P(x / z, y-1, z)P(z)D(x, z).P(x,1, z) = (x \leq z)P(x).P(x, y,1).$$

Esta es una definición doblemente recursiva, pues es recursiva con respecto a y así como con respecto a z. $P(x, 1, x)$ está definida para z arbitraria (y x) y, si se asume que $P(x, y - 1, z)$ ya está definida para z arbitraria (y x), entonces, por medio de la primera ecuación de la Definición 17 y la estipulación de que $P(x, y, 1)$ ha de ser falsa, tenemos una definición recursiva de la función proposicional $P(x, y, z)$, esto es, recursiva con respecto a z. Mediante la última estipulación de la Definición 17, $P(x, y, 1)$ está determinada y, mediante la primera ecuación, $P(x, y, z)$ está determinada sobre la base de la asunción de que $P(x, y - 1, z)$ ya es conocida.

Quiero introducir tres funciones proposicionales más.

Definición 18. $P'(x, 1, z) = P(x, 1, z)$. $P'(x, y + 1, z) = P'(x, y, z) + P(x, y + 1, z)$.

Definición 19. $\prod(x) = P'(x, x, x)$.

Definición 20. $\prod'(1)$ es verdadero. $\prod'(x+1) = \prod'(x)\prod(x+1)$.

La proposición $P'(x, y, z)$ obviamente significa que x es un producto de a lo mucho y primos, cada uno $\leq z$. La proposición $\prod(x)$ significa que x es un producto de a lo mucho x primos, cada uno $\leq x$. $\prod'(x)$ significa que cada número y desde 1 hasta x o bien es igual a 1 o es un producto de a lo mucho y primos $\leq y$, o, en otras palabras, que cada número y desde 2 hasta x es un producto de a lo mucho y primos $\leq y$. El propósito real de las consideraciones que siguen es probar que $\prod(x+1)$ se sostiene.

Teorema 59. $\overline{P(x, y, z)(z \leq z')} + P(x, y, z')$.

Prueba. Claramente, la proposición es verdadera cuando $z' = 1$. La pruebo para $z' + 1$ sobre la asunción de que vale para z'. De $z \leq z'+1$ se sigue o bien que $z \leq z'$, que junto con $P(x, y, z)$ tiene a $P(x, y, z')$ y por lo tanto también (Definición 17) a $P(x, y, z' + 1)$ como consecuencias, o que $z = z' + 1$, y de $(z = z' + 1)P(x, y, z)$ claramente se sigue de nuevo que $P(x, y, z' + 1)$.

Lema 1 (para el Teorema 60). $\overline{P(x_1, 1, z)P(x_2, 1, z)} + P(x_1x_2, 2, z)$.

Prueba. Verdadero para $z = 1$; pues (Definiciones 17 y 13) $P(x, 1, 1)$ ya es falsa. Pruebo la proposición para $z + 1$ sobre la asunción de que vale para z. De $P(x_1, 1, z + 1)P(x_2, 1, z + 1)$ se sigue, de acuerdo con la Definición 17, que $P(x_1, 1, z)P(x_2, 1, z)$, por lo que tenemos [que] $P(x_1x_2, 2, z)$, que a su vez tiene a $P(x_1x_2, 2, z + 1)$ como una consecuencia, o que $(x_1 = z + 1)P(x_1)P(x_2, 1, z + 1)$, o que $(x_2 = z + 1)P(x_2)P(x_1, 1, z + 1)$. Pero de $P(z + 1)P(x_1x_2/(z + 1), 1, z + 1)$ se sigue (Definición 17) que $P(x_1x_2, 2, z + 1)$. Procedemos de manera análoga en el tercer caso.

Lema 2 (para el Teorema 60). $\overline{P(x_1, y, z)P(x_2, 1, z)} + P(x_1x_2, y+1, z)$.

Prueba. De acuerdo con el Lema 1, esto es verdadero para $y = 1$. Pruebo que la proposición es verdadera para $y + 1$ sobre la asunción de que vale para y. Ahora, en caso de que $z = 1$, de hecho obtenemos que $P(x_1x_2, y + 2, z)$ desde $P(x_1, y + 1, z)P(x_2, 1, z)$, pues $P(x_2, 1, 1)$ es falsa. Por lo tanto, sobre la asunción de que el paso inductivo de y a $y + 1$ vale para z, pruebo que vale para $z + 1$. Desde $P(x_1, y + 1, z + 1)P(x_2, 1, z + 1)$ obtenemos (Definición 17) tres posibilidades: (1) $P(x_1, y + 1, z)P(x_2, 1, z)$ ya se sostiene; entonces, de acuerdo con la asunción tenemos [que] $P(x_1x_2, y + 2, z)$, por lo que (Definición 17) $P(x_1x_2, y + 2, z + 1)$. (2) Tenemos [que] $P(x_1/(z + 1), y, z + 1)P(z + 1)P(x_2, 1, z + 1)$; pero de $P(x_1/(z + 1), y, z + 1)P(x_2, 1, z + 1)$ se sigue, ya que asumimos que nuestra proposición era verdadera para y para z arbitraria, que $P(x_1x_2/(z + 1), y + 1, z + 1)$, que junto con $P(z + 1)$, en virtud de la Definición 17, implica $P(x_1x_2, y + 2, z + 1)$. (3) Tenemos [que] $P(x_1, y + 1, z + 1)(x_2 = z + 1)P(x_2)$; pero de esto obtenemos (Definición 17) $P(x_1x_2, y + 2, z + 1)$.

Teorema 60. $\overline{P(x_1, y_1, z)P(x_2, y_2, u)(u \le z)} + P(x_1x_2, y_1 + y_2, z)$.

Prueba. Habida cuenta del Lema 2, cuando $y_1 = 1$ o $y_2 = 1$, esta proposición es ciertamente verdadera para valores arbitrarios de las variables restantes. Así, seguramente vale para el menor valor posible de la suma $y_1 + y_2 + z + u$, a saber, 4, para el que necesariamente $y_1 = y_2 = z = u = 1$. Ahora pruebo que la proposición es verdadera para valores de y_1, y_2, z, y u tales que $y_1 + y_2 + z + u = n$, asumiendo que es verdadera para aquellos casos en los que $y_1 + y_2 + z + u = n - 1$. $P(x_1, y_1, z)$ es equivalente o bien a $P(x_1, y_1, z - 1)$ o bien a $P(x_1/z, y_1 - 1, z)P(z)D(x, z)$. Además, tenemos o bien que $u \le z - 1$ o que $u = z$. La primera posibilidad es por tanto $P(x_1, y_1, z - 1)P(x_2, y_2, u)(u \le z - 1)$. Pero, ya que $y_1 + y_2 + (z - 1) + u = n - 1$, se sigue, de acuerdo con la asunción hecha, que $P(x_1x_2, y_1 + y_2, z - 1)$ y de aquí, a la vez (Definición 17) que $P(x_1x_2, y_1 + y_2, z)$. La segunda posibilidad es $P(x_1, y_1, z - 1)P(x_2, y_2, z)$. Pero, como aquí también necesariamente $y_1 + y_2 + (z - 1) + u = n - 1$, se sigue que $P(x_1x_2, y_1 + y_2, z)$. La tercera posibilidad es $P(x_1 / z, y_1 - 1, z)P(z)P(x_2, y_2, u)(u \le z)$. Pero de allí se sigue, ya que $(y_1 - 1) + y_2 + z + u = n - 1$, que $P(x_1x_2/z, y_1 + y_2 - 1, z)P(z)$, y de allí (Definición 17) nuevamente que $P(x_1x_2, y_1 + y_2, z)$.

Corolario. $\overline{P(x_1, y_1, z)P(x_2, y_2, z)} + P(x_1x_2, y_1 + y_2, z)$.

Lema. $\overline{P'(x_1, y_1, z)P(x_2, y_2, z)} + P'(x_1x_2, y_1 + y_2, z)$.

Prueba. Verdadero para $y_1 = 1$ (Definición 18 y Lema 2 para el Teorema 60). Pruebo que la proposición es verdadera para $y_1 + 1$ sobre la asunción de que vale para y_1. De $P'(x_1, y_1 + 1, z)$ se sigue, o bien que $P'(x_1, y_1, z)$, que junto con $P(x_2, y_2, z)$ tiene, de acuerdo con la asunción, a $P'(x_1x_2, y_1 + y_2, z)$ y por tanto también a $P'(x_1x_2, y_1 + y_2 + 1, z)$ como consecuencias, o que $P(x_1, y_1 + 1, z)$, por lo que, junto con $P(x_2, y_2, z)$, se sigue, de acuerdo con el corolario al Teorema 60, que $P(x_1x_2, y_1 + 1 + y_2, z)$, por lo que (Definición 18) nuevamente $P'(x_1x_2, y_1 + 1 + y_2, z)$.

Teorema 61. $\overline{P'(x_1, y_1, z)P'(x_2, y_2, z)} + P'(x_1x_2, y_1 + y_2, z)$.

Prueba. De acuerdo con el lema, esto es verdadero para $y_2 = 1$. Pruebo que la proposición es verdadera para $y_2 + 1$ bajo la asunción de que es verdadera para y_2. De $P'(x_2, y_2 + 1, z)$ se sigue (Definición 18) o bien que $P'(x_2, y_2, z)$, por lo que junto con $P'(x_1, y_1, z)$, de acuerdo con la asunción hecha, $P'(x_1x_2, y_1 + y_2, z)$, y por tanto también $P'(x_1x_2, y_1 + y_2 + 1, z)$, o que $P(x_2, y_2 + 1, z)$, que junto con $P'(x_1, y_1, z)$, de acuerdo con el lema, implica $P'(x_1x_2, y_1 + y_2 + 1, z)$.

Lema. $\overline{P'(x, y, z)} + P'(x, y, z + 1)$.

Prueba. En virtud de las Definiciones 17 y 18, esto es verdadero para $y = 1$. Pruebo la proposición para $y + 1$ sobre la asunción de que vale para y. De $P'(x, y + 1, z)$ se sigue o bien que $P'(x, y, z)$, de donde obtenemos [que] $P'(x, y, z + 1)$, y por lo tanto (Definición 18) a la vez $P'(x, y + 1, z + 1)$, o que $P(x, y + 1, z)$, por lo que (Definición 17) $P(x, y + 1, z + 1)$, y por tanto (Definición 18) $P'(x, y + 1, z + 1)$.

Teorema 62. $\overline{P'(x, y, z)(z \leq z')} + P'(x, y, z')$.

Prueba. Claramente verdadero cuando $z' = 1$. Asumo que la proposición es verdadera para z' y después la pruebo para $z' + 1$. De $z \leq z'+1$ se sigue, o bien que $z \leq z'$, y entonces de $P'(x, y, z)(z \leq z')$ se sigue, de acuerdo con la asunción hecha, que $P'(x, y, z')$, y

de allí, de acuerdo con el lema, que $P'(x, y, z' + 1)$, o se sigue que $z = z' + 1$, y de allí, junto con $P'(x, y, z)$, claramente se sigue que $P'(x, y, z' + 1)$.

Teorema 63. $\overline{P'(x, y, z)(y \leq y')} + P'(x, y', z)$.

Prueba. Claramente verdadero cuando $y' = 1$. Asumo que la proposición es verdadera para y'. De $y \leq y'+1$ se sigue, o bien que $y \leq y'$, o que $y = y' + 1$. Ahora bien, de acuerdo con la asunción, de $P'(x, y, z)(y \leq y')$ se sigue que $P'(x, y', z)$ y por lo tanto (Definición 18) también que $P'(x, y' + 1, z)$. De $P'(x, y, z)(y = y' + 1)$ se sigue, desde luego, que $P'(x, y' + 1, z)$. Así, la proposición también es válida para $y' + 1$.

Teorema 64. $(x = 1) + (y = 1) + \overline{\prod(x)} + \overline{\prod(y)} + \prod(xy)$.

Prueba. Ya que, de acuerdo con el Teorema 15, necesariamente $x \leq xy$ e igualmente $y \leq xy$, de $P'(x, x, x)P'(y, y, y)$, esto es, de $\prod(x)\prod(y)$, se sigue, de acuerdo con el Teorema 62, que $P'(x, x, xy)P'(y, y, xy)$. Pero, de acuerdo con el Teorema 61, de $P'(x, x, xy)P'(y, y, xy)$ se sigue a su vez que $P'(xy, x + y, xy)$. Si, ahora, [tenemos] además [que] $(x > 1)(y > 1)$, entonces $x + y \leq xy$, de modo que, empleando el Teorema 63, obtenemos $P'(xy, xy, xy)$, esto es, $\prod(xy)$. Así, de $(x > 1)(y > 1)\prod(x)\prod(y)$ se sigue que $\prod(xy)$, que es lo que había que probar.

Lema 1 (para el Teorema 65). $\overline{\prod'(x)(y \leq x)} + \prod'(y)$.

Prueba. Claramente verdadero para $x = 1$. Asumo que la proposición es verdadera para x. De $y \leq x + 1$ se sigue, o bien que $y \leq x$, o que $y = x + 1$. De $\prod'(x+1)$ se sigue (Definición 20) que $\prod'(x)$, y por lo tanto de $\prod'(x+1)(y \leq x)$ se sigue, primero, que $\prod'(x)(y \leq x)$, y de allí entonces que $\prod'(y)$. De $\prod'(x+1)(y = x+1)$ se sigue, desde luego, que $\prod'(y)$.

Lema 2 (para el Teorema 65). $\overline{\Delta(x, y, z)\prod(y)\prod'(z)(y > 1)} + \prod(x)$.

Prueba. Esto es verdadero cuando $z = 1$. Asumo que la proposición es verdadera para z. De $\Delta(x, y, x+1)$ se sigue (Definición 5) o bien que $\Delta(x, y, z)$ o que $x = y(z + 1)$. De $\Delta(x, y, z)\prod(y)\prod'(z+1)(y>1)$ obtenemos, de acuerdo con la Definición 20, $\Delta(x, y, z)\prod(y)\prod'(z)(y>1)$ y de aquí, de acuerdo con la asunción hecha, $\prod(x)$. De $(x = y(z+1))\prod(y)\prod'(z+1)(y>1)$ se sigue (Definición 20) que $(x = y(z+1))\prod(y)\prod(z+1)(y>1)$ y de aquí, de acuerdo con el Teorema 64, que $\prod(x)$. Así, la proposición también es válida para $z + 1$.

Lema 3 (para el Teorema 65). $\overline{De(x, y)\prod'(x-1)} + \prod(x)$.

Prueba. Esto vale para $y = 1$, como puede verse por la Definición 14. Asumo que la proposición vale para y. Desde $De(x, y + 1)$ se sigue (Definición 14) o bien que $De(x, y)$ o que $D(x, y + 1)(y + 1 < x)$. Desde $De(x, y)\prod'(x-1)$ debe seguirse, de acuerdo con la asunción, que $\prod(x)$. De acuerdo con la Definición 2, $D(x, y + 1)(y + 1 < x)$ debe ser equivalente a $D(x, y+1)(y+1 \le x-1)$; pero de $\prod'(x-1)(y+1 \le x-1)$ se sigue (Lema 1) que $\prod'(y+1)$, de donde (Definición 20) $\prod(y+1)$, y como además, como se ve fácilmente, necesariamente (véanse las Definiciones 5 y 6) tenemos [que] $D(x, y+1) = \Delta(x, y+1, x-1)$, de $D(x, y+1)\prod(y+1)\prod'(x-1)$ se sigue, de acuerdo con el Lema 2, que $\prod(x)$.

Teorema 65. $\prod'(x)$.

Prueba. Verdadero para $x = 1$ (Definición 20). Asumo que $\prod'(x-1)$ es verdadero y después pruebo $\prod(x)$, que también prueba (Definición 20) [que] $\prod'(x)$. O bien se sostiene que $P(x)$, o bien que $\overline{P(x)}$. De $P(x)$ se sigue (Definición 17) que $P(x, 1, x)$, esto eso (Definición 18), que $P'(x, 1, x)$, desde donde, de acuerdo con el Teorema 63, $P'(x, x, x)$, esto es, $\prod(x)$. De $\overline{P(x)}(x>1)$ se sigue (Definición 13) que $\overline{P(x, x)}$, por lo cual (Teorema 53) $De(x, x)$. Pero, de acuerdo con el Lema 3, $De(x, x)\prod'(x-1)$ implica $\prod(x)$.

Corolario. $\prod(x+1)$.

Pues, de acuerdo con la Definición 20, $\prod(x+1)$ se sigue de $\prod'(x+1)$. Esto, empero, es el importante teorema de que cada número > 1 es un producto de números primos.

§ 8. ALGUNOS USOS EXPLÍCITOS DE SUMAS Y PRODUCTOS LÓGICOS FINITOS

Si nos interesa evitar únicamente el uso de variables lógicas que se extienden sobre dominios infinitos, aún podemos, desde luego, hacer libre uso de variables que se extienden sobre dominios *finitos*; no necesitan preocuparnos ni las maneras por las que estas [variables lógicas] podrían evitarse por medio de definiciones recursivas ni las maneras por las que las conclusiones que nos permiten alcanzar podrían derivarse, por inducción matemática, de aquellas [conclusiones] que valen para proposiciones que no contienen variables aparentes.

Si adoptamos este enfoque, entonces la teoría de la factorización de primos, por ejemplo, puede presentarse de forma más sencilla, como muestro abajo. Uso la definición de números primos ofrecida antes:

Definición. $P(x) = (x \neq 1)\prod_{y=1}^{x}(\overline{D(x,y)} + (y=1) + (y=x))$.

Teorema 66. $\sum_{p=1}^{n} D(n,p)P(p) + (n=1)$.

Prueba. Vale para $n = 1$. Asúmase que la proposición vale para $v < n$, con $n > 1$. Entonces o bien la proposición $\sum_{v=1}^{n} D(n,v)(v<n)(n>1)$ o su negación $\prod_{v=1}^{n}(\overline{D(n,v)} + (v=n) + (v=1))$ vale (porque aquí $v \geq n$ es equivalente a $v = n$, y $v \leq 1$ a $v = 1$). En el último caso tenemos $D(n, n)P(n)$. En el primer caso, de acuerdo con la asunción,

$\sum_{p=1}^{n} D(v, p)P(p)$ vale; consecuentemente $\sum_{v=1}^{n} \sum_{p=1}^{v} D(n,v)D(v, p)P(p)$, por lo que $\sum_{p=1}^{n} D(n, p)P(p)$.

Ya que $D(n, p)$ es equivalente a la suma proposicional $\sum_{v=1}^{n}(n = vp)$, tenemos el

Corolario. $(n = 1) + \sum_{v=1}^{n} \sum_{p=1}^{n}(n = vp)P(p)$.

Defino ahora, recursivamente, una función proposicional que en palabras es "n es igual a un producto de μ factores primos, todos los cuales son $\leq n$".

Definición 21. $P(n,1) = P(n); P(n, \mu+1) = \sum_{v=1}^{n} \sum_{p=1}^{n}(n = vp)P(v, \mu)P(p)$.

El teorema sobre la factorización de cualquier número > 1 en un producto de primos puede entonces formularse como sigue:

Teorema 67. $(n = 1) + \sum_{\mu=1}^{n} P(n, \mu)$.

Prueba. Vale para $n = 1$. Asúmase que la proposición vale para $v < n$ cuando $n > 1$. Entonces, de acuerdo con el corolario al Teorema 66, $\sum_{v=1}^{n} \sum_{p=1}^{n}(n = vp)P(p)$ vale. Sin embargo, de $(n = vp)P(p)$ se sigue (Teorema 15) que $v < n$ y entonces, de acuerdo con la asunción, $\sum_{\mu=1}^{v} P(v, \mu)$. Por lo tanto, $\sum_{\mu=1}^{n-1} P(v, \mu)$ y además $\sum_{v=1}^{n} \sum_{p=1}^{n} \sum_{\mu=1}^{n-1}(n = vp)P(v, \mu)P(p)$, que es $= \sum_{\mu=1}^{n-1} P(n, \mu+1)$, por lo que $\sum_{\mu=1}^{n} P(n, \mu)$.

Quiero probar, además, el teorema sobre la existencia de infinitos primos. Primero defino la función $n!$ como

Definición 22. $1! = 1$; $(n + 1)! = n!(n + 1)$.

Lema. $(m > n) + D(n!, m)$.

Prueba. Claramente verdadero para $n = 1$. Asúmase que es verdadero para un cierto n. Si no [es el caso que] $m > n + 1$, entonces o bien $m = n + 1$ o $m < n + 1$ (esto es, $m \leq n$). De acuerdo con la Definición 22 y el Teorema 18 tenemos $D((n + 1)!, n + 1)$. Si $m \leq n$ tenemos, de acuerdo con la asunción, $D(n!, m)$, y, ya que (Teoremas 16 y 18) $D((n + 1)!, n!)$ también vale, obtenemos (corolario al Teorema 20) $D((n + 1)!, m)$.

Teorema 68. $\sum_{p=1}^{n!+1} P(p)(p > n)$. (En palabras: Para n arbitrario hay un primo $p > n$ y $\leq n!+1$.)

Prueba. De acuerdo con el Teorema 66, se sostiene la proposición $\sum_{p=1}^{n!+1} D(n!+1, p)P(p)$. Pero de $D(n! + 1, p)P(p)$ se sigue que $p > n$. Pues, si tuviésemos que $p \leq n$, se seguiría, de acuerdo con el lema, que $D(n!, p)$, y esto, junto con $D(n! + 1, p)$, implicaría (corolario al Teorema 24) [que] $D(1, p)$ y por lo tanto que $p = 1$, lo que es imposible habida cuenta de $P(p)$.

Para probar la unicidad [uniqueness] de la factorización de un número en un producto de factores primos debo primero anticipar algunas consideraciones sobre sumas y productos de arbitrariamente muchos términos o factores, así como definir una función $I(a, b; m, n)$.

Sea $f(r)$ una función descriptiva arbitraria. Defino las expresiones $\sum_{r=1}^{n} f(r)$ y $\prod_{r=1}^{n} f(r)$ recursivamente como sigue:

Definición 23.

$$\sum_{r=1}^{1} f(r) = f(1); \sum_{r=1}^{n+1} f(r); \sum_{r=1}^{n} f(r) + f(n+1). \prod_{r=1}^{1} f(r) = f(1); \prod_{r=1}^{n+1} f(r) = \prod_{r=1}^{n} f(r) \cdot f(n+1).$$

En lugar de $f(r)$ a menudo escribimos a_r, b_r, y así sucesivamente. Para una función descriptiva arbitraria a_r establezco que

Definición 24. $a_r^{(v)} = a_r$ si $r < v$, y $a_r^{(v)} = a_{r+1}$ si $r \geq v$.

Teorema 69. $(n = 1) + (v > n) + \left(\sum_{r=1}^{n} a_r = a_v + \sum_{r=1}^{n-1} a_r^{(v)} \right) \left(\prod_{r=1}^{n} a_r = a_v \cdot \prod_{r=1}^{n-1} a_r^{(v)} \right)$.

Prueba. Solamente necesito considerar la suma. La proposición vale cuando $n = 1$. Asúmase que vale para n. Para mostrar que entonces también vale para $n + 1$, sea primero que $v \leq n$. Entonces

$$\sum_{r=1}^{n+1} a_r = \sum_{r=1}^{n} a_r + a_{n+1} = a_v + \sum_{r=1}^{n-1} a_r^{(v)} + a_{n+1}$$

y además $a_n^{(v)} = a_{n+1}$. Consecuentemente (de acuerdo con la Definición 24)

$$\sum_{r=1}^{n-1} a_r^{(v)} + a_{n+1} = \sum_{r=1}^{n-1} a_r^{(v)} + a_n^{(v)} = \sum_{r=1}^{n} a_r^{(v)}$$

y por lo tanto

$$\sum_{r=1}^{n+1} a_r = a_v + \sum_{r=1}^{n} a_r^{(v)}.$$

Por otro lado, sea $v = n + 1$. Entonces $a_r^{(v)} = a_r$ para $r \leq n$. Consecuentemente

$$\sum_{r=1}^{n+1} a_r = \sum_{r=1}^{n} a_r + a_{n+1} = a_{n+1} + \sum_{r=1}^{n} a_r^{(v)}.$$

En muchas derivaciones hacemos uso del argumento de que tal suma (o producto) permanece sin cambios cuando los términos (o factores) *a* son remplazados por números *b*, siempre que éstos estén en algún orden secuencial idéntico al de los [términos (o factores)] *a*. Para poder formular esto convenientemente, introduzco una función proposicional $I(a, b; m, n)$, donde *a* y *b* son signos para dos funciones descriptivas arbitrarias.

Definición 25. $I(a, b; 1, 1) = (a_1 = b_1)$. $I(a, b; 1, n)(n > 1)$ es falso. $I(a, b; m, 1)(m > 1)$ es falso. $I(a,b;m+1,n) = \sum_{v=1}^{n} (a_{m+1} = b_v) I(a,b^{(v)};m,n-1)$ ($b^{(v)}$ fue definido en la Definición 24).

$I(a, b; m, n)$ significa entonces, en palabras: "Los números $a_1, \ldots, a_m$ son en algún ordenamiento idénticos a los números $b_1, \ldots, b_n$".

Teorema 70. $\overline{I(a,b;m,n)} + (m = n)$.

Prueba. Verdadero cuando $m = 1$, por la Definición 25. Asúmase que es verdadero para m. De $I(a, b; m + 1, n)$ se sigue que $\sum_{v=1}^{n} (a_{m+1} = b_v) I(a,b^{(v)};m,n-1)$. Pero $I(a,b^{(v)};m,n-1)$ implica que $m = n - 1$. Por lo tanto, $m + 1 = n$.

Teorema 71. $\overline{I(a,b;m,n)} + \left(\sum_{r=1}^{m} a_r = \sum_{r=1}^{n} b_r \right) \left(\prod_{r=1}^{m} a_r = \prod_{r=1}^{n} b_r \right)$.

Prueba. Considero solamente la suma. Primero, cuando $n = 1$, se sigue que $m = n$ y la proposición claramente vale. Asúmase que vale para $n - 1$. De $I(a, b; m, n)$ se sigue que $\sum_{\rho=1}^{n} (a_n = b_p) I(a,b^{(\rho)};n-1,n-1)$. Pero, de acuerdo con la asunción, $I(a,b^{(\rho)};n-1,n-1)$ produce $\sum_{r=1}^{n-1} a_r = \sum_{r=1}^{n-1} b_r^{(\rho)}$, y además tenemos (Teorema 69) $b_\rho + \sum_{r=1}^{n-1} b_r^{(\rho)} = \sum_{r=1}^{n} b_r$. De $a_n = b_\rho$ y $\sum_{r=1}^{n-1} a_r = \sum_{r=1}^{n-1} b_r^{(\rho)}$ se sigue por lo tanto que $\sum_{r=1}^{n} a_r = \sum_{r=1}^{n} b_r$.

Teorema 72. $\overline{D\left(\prod_{r=1}^{n} a_r, p \right) P(p)} + \sum_{r=1}^{n} D(a_r, p)$.

Prueba. La proposición vale para $n = 1$; asúmase que vale para un cierto n. De $D\left(a_{n+1} \cdot \prod_{r=1}^{n} a_r, p \right)$ se sigue (Teorema 52) que $D(a_{n+1}, p) + D\left(\prod_{r=1}^{n} a_r, p \right) P(p)$. De

$D\left(\prod_{r=1}^{n} a_r, p\right) P(p)$ se sigue, de acuerdo con la asunción, que $\sum_{r=1}^{n} D(a_r, p)$. Así, en cualquier caso, $D(a_{n+1}, p) + \sum_{r=1}^{n} D(a_r, p)$, que es $= \sum_{r=1}^{n+1} D(a_r, p)$, vale.

Teorema 73. $\overline{D\left(\prod_{r=1}^{n} p_r, q\right) \prod_{r=1}^{n} P(p_r) P(q)} + \sum_{r=1}^{n} (p_r = q)$.

Prueba. Por el Teorema 72, desde $D\left(\prod_{r=1}^{n} p_r, q\right)$ derivamos $\sum_{r=1}^{n} D(p_r, q)$. De $D(p_r, q)P(p_r)P(q)$, sin embargo, se sigue que $((p_r = q) + (q = 1))P(q)$; por lo que $p_r = q$. Por lo tanto, $\sum_{r=1}^{n} (p_r = q)$.

El teorema sobre la unicidad de la factorización de primos se lee ahora como sigue:

Teorema 74. $\left(\prod_{r=1}^{\mu} p_r \neq \prod_{s=1}^{\nu} q_s\right) + \sum_{r=1}^{\mu} \overline{P(p_r)} + \sum_{s=1}^{\nu} \overline{P(q_s)} + I(p, q; \mu, \nu)$.

Prueba. Pruebo primero la proposición para $\mu = 1$. Si $\left(p_1 = \prod_{s=1}^{\nu} q_s\right) P(p_1) \prod_{s=1}^{\nu} P(q_s)$, entonces se sigue, de acuerdo con el Teorema 73, que $\sum_{\sigma=1}^{\nu} (p_1 = q_\sigma)$. Además, de $p_1 = q_\sigma$ y de $p_1 = p_\sigma \prod_{s=1}^{\nu-1} q_s^{(\sigma)}$ se sigue la ecuación $1 = \prod_{r=1}^{\nu-1} q_s^{(\sigma)}$, que es imposible si $\nu > 1$.

Asúmase que la proposición es verdadera para un cierto μ. Entonces, de la proposición $\left(\prod_{r=1}^{\mu+1} p_r = \prod_{s=1}^{\nu} q_s\right) \prod_{r=1}^{\mu+1} P(p_r) \prod_{s=1}^{\nu} P(q_s)$ se sigue que $D\left(\prod_{s=1}^{\nu} q_s, p_{\mu+1}\right) \prod_{s=1}^{\nu} P(q_s) P(p_{\mu+1})$, por lo que a la vez, de acuerdo con el Teorema 73, $\sum_{\rho=1}^{\nu} (p_{\mu+1} = q_\rho)$. Además, $\prod_{s=1}^{\nu} q_s = q_\rho \prod_{s=1}^{\nu-1} q_s^{(\rho)}$, y por lo tanto obtenemos

$\sum_{\rho=1}^{\nu}\left(\prod_{r=1}^{\mu} p_r = \prod_{s=1}^{\nu-1} p_s^{(\rho)}\right)$, y por consiguiente, de acuerdo con la asunción, $\sum_{\rho=1}^{\nu} I(p, q^{(\rho)}; \mu, \nu-1)(p_{\mu+1} = q_\rho)$, que es = $I(p, q; \mu + 1, \nu)$.

Finalmente, quiero abordar algunas reflexiones de un tipo más general. Tenemos el siguiente

Teorema 75a. $\overline{U(n)} + \sum_{\nu=1}^{n} \prod_{\mu=1}^{\nu} U(\nu)(\overline{U(\mu)} + (\mu = \nu))$, donde U denota una función proposicional arbitraria.[3]

En palabras: Si conocemos un número n para el que la proposición U es verdadera, existe un menor número para el que U es verdadera. Aquí, debe notarse que las proposiciones con las que estamos ahora ocupados siempre se consideran como dadas sin variables aparentes que se extienden sobre dominios infinitos, de modo que siempre es finitamente decidible si $U(x)$ es verdadera o no para una x arbitraria.

Prueba. Para $n = 1$ la proposición es claramente verdadera. Asúmase que es verdadera para toda $x \leq$ un cierto n. Entonces, si $U(n + 1)$ es verdadera, también lo es $\prod_{x=1}^{n} \overline{U(x)}$ o $\sum_{x=1}^{n} U(x)$. En el primer caso, por lo tanto, se sostiene que $U(n+1)\prod_{\nu=1}^{n+1}(\overline{U(\nu)} + (\nu = n+1))$. En el último caso, de acuerdo con la asunción, de $U(x)(x \leq n)$ se sigue que $\sum_{y=1}^{x}\prod_{z=1}^{y} U(x)(\overline{U(z)} + (z = y))$ y por tanto, *a fortiori*, que $\sum_{\nu=1}^{n+1}\prod_{\mu=1}^{\nu} U(\nu)(\overline{U(\mu)} + (\mu = \nu))$.

[3] Desde luego, también podemos escribir, por ejemplo, $\overline{U(n)} + \sum_{\nu=1}^{n} \prod_{\mu=1}^{n} U(\nu)(\overline{U(\mu)} + (\mu \geq \nu))$.

Teorema 75b. De $U(a)\prod_{x=1}^{a}(\overline{U(x)}+(x=a))U(b)\prod_{y=1}^{b}(\overline{U(y)}+(y=b))$ se sigue que *a* = *b*.

Este teorema expresa la unicidad del menor número.

Prueba. Si tuviésemos que $a \neq b$, tendríamos que (*a* < *b*) + (*a* > *b*). Pero de *a* < *b* se sigue de inmediato que $\overline{U(a)}$, e igualmente, de *b* < *a*, que $\overline{U(b)}$.

Debido a esta unicidad podemos introducir una muy importante función descriptiva de la función proposicional general *U*, que denota al menor número para el que *U* es verdadera. Concedido, esta función descriptiva tiene un restringido dominio de definición, porque no tiene ningún valor si la proposición *U* no es verdadera de ningún número. Pero debe enfatizarse que nos estamos ocupando sólo de los números naturales hasta cierto límite superior, que, no obstante, puede ser arbitrariamente grande. La función descriptiva, por lo tanto, puede denotarse con Min(*U, n*). Esto significa el menor número entre los números 1 a *n* para el que *U* es verdadera, y no tiene ningún significado si *U* es falsa para todos estos números. Así, no estamos tratando con una función Min(*U*), o Min(*U*, ∞), que significaría el menor número satisfaciendo la proposición *U* y no tendría ningún significado si *U* es falsa para cada número; pues todo esto requeriría del "infinito real", por tanto, del uso de variables lógicas aparentes extendiéndose sobre dominios infinitos. Pero la restricción que aquí debemos imponer sobre el significado de esta función mínima no hace ningún daño en la práctica; pues, siempre que utilicemos el teorema que afirma que en una clase de enteros positivos existe uno menor, en cualquier caso debemos primero llegar a conocer un número *n* de esta clase, y después podemos trabajar con esta mismísima función Min(*U*, *n*).

Finalmente, deseo hacer algunas observaciones sobre la *noción de cardinalidad* [zum *Anzahl-begriffe*]. Si ciertos objetos (números, pares de números, triples de números, y así sucesivamente, o quizá funciones descriptivas) son mapeados uno-a-uno sobre todos los números ≤ un cierto número *n*, entonces yo digo que *su cardinalidad es n*.

Con el fin de mostrar que este número *n* es invariante con respecto a los diferentes mapeos, debemos probar el siguiente

Teorema 76. De $\prod_{x=1}^{m}\prod_{y=1}^{m}((x=y)+(f(x)\neq f(y)))\prod_{x=1}^{m}(f(x)\leq n)\prod_{y=1}^{n}\sum_{z=1}^{m}(y=f(z))$, donde f es una función descriptiva arbitraria, se sigue que $m = n$.

En palabras: Asúmase que los números que son $\leq m$ son mapeados uno-a-uno sobre todos los números $\leq n$; entonces $m = n$.

Prueba. Tomo primero el caso en el que $m = 1$. De $\prod_{y=1}^{n}\sum_{z=1}^{1}(y=f(z))=\prod_{y=1}^{n}(y=f(1))$ se sigue, habida cuenta de la unicidad de $f(1)$, que necesariamente $n = 1$.

Asúmase que la proposición vale para un cierto m. Entonces, si tomo el valor $m + 1$, en cualquier caso necesariamente $n > 1$. Si no, de $\prod_{x=1}^{m+1}(f(x)\leq 1)$ obtendríamos $f(1) = 1$ así como $f(2) = 1$, mientras que se suponía que teníamos $f(1)\neq f(2)$. Consecuentemente, podemos escribir $n + 1$ en lugar de n, y ahora debemos probar que $m = n$.

Considérese primero la asunción $f(m + 1) = n + 1$. Entonces $\prod_{x=1}^{m}(f(x)\neq f(m+1))$, o $\prod_{x=1}^{m}(f(x)\neq n+1)$. Ya que, además, $\prod_{x=1}^{m}(f(x)\leq n+1)$, se sigue que $\prod_{x=1}^{m}(f(x)\leq n)$. De $\prod_{y=1}^{n+1}\sum_{z=1}^{m+1}(y=f(z))$ se sigue que $\prod_{y=1}^{n}\sum_{z=1}^{m+1}(y=f(z))(y\leq n)$, esto es,

$$\prod_{y=1}^{n}\sum_{z=1}^{m}((y=f(z))+(y=f(m+1))(y<f(m+1))),$$

que es $=\prod_{y=1}^{n}\sum_{z=1}^{m}(y=f(z))$. En virtud de la asunción hecha, por tanto, necesariamente $m = n$.

Considérese después la asunción $f(m + 1) = v < n + 1$. De acuerdo con la asunción de que $\prod_{y=1}^{n+1}\sum_{z=1}^{m+1}(y=f(z))$ tenemos $\sum_{z=1}^{m+1}(n+1=f(z))$, es decir,

$$\sum_{\mu=1}^{m}(n+1=f(\mu))+(n+1=f(m+1)),$$

[y] por consiguiente $\sum_{\mu=1}^{m}(n+1=f(\mu))$. Aquí, el número μ está determinado de manera única. Introduzco ahora una nueva función descriptiva f', que está definida así: $f'(x) = f(x)$ si $x \neq \mu$ y $\leq m$. Además, $f'(\mu) = f(m + 1) = v$; $f'(m + 1) = f(\mu) = n + 1$. Debemos entonces mostrar meramente que f' satisface las mismas condiciones que f.

De $(f(x) \leq n+1)(x \neq \mu)(x \leq m)$ se sigue que $f'(x) \leq n+1$, ya que, en este caso, $f'(x) = f(x)$. Además, claramente tanto $f'(\mu)$ como $f'(m)$ son $\leq n+1$. Así, $\prod_{x=1}^{m+1}(f'(x) \leq n+1)$.

De $\sum_{y=1}^{m+1}(x = f(y))$ se sigue que

$$\sum_{y=1}^{m+1}(x=f(y))(y \neq \mu)(y<m)+\sum_{y=1}^{m+1}(x=f(y))((y=\mu)+(y=m+1)),$$

por lo que $\sum_{y=1}^{m+1}(x=f'(y))+(x=f'(m+1))+(x=f'(\mu))$, que es $=\sum_{v=1}^{m+1}(x=f'(y))$. Así, de $\prod_{x=1}^{n+1}\sum_{y=1}^{m+1}(x=f(y))$ se sigue también que $\prod_{x=1}^{n+1}\sum_{y=1}^{m+1}(x=f'(y))$.

De acuerdo con la asunción, $\prod_{x=1}^{m+1}\sum_{y=1}^{m+1}((x=y)+(f(x)\neq f(y)))$ vale. Si tenemos

$$(f(x)\neq f(y))(x\neq\mu)(x\leq m)(y\neq\mu)(y\leq m),$$

entonces inmediatamente se sigue que $f'(x) \neq f'(y)$. Si tenemos

$$(f(x)\neq f(y))((x=\mu)+(x=m+1))(y\neq\mu)(y\leq m),$$

entonces

$$((f(x) = f(\mu)) + (f(x) = f(m+1)))(f(y) = f'(y))(f(y) \neq f(\mu))(f(y) \neq f(m+1))$$

vale, y consecuentemente $f'(x) \neq f'(y)$. Similarmente si

$$(f(x) \neq f(y))(x = \mu)(x \leq m)((y = \mu) + (y = m)).$$

Finalmente,

$$(f(x) \neq f(y))((x = \mu) + (x = m+1))((y = \mu) + (y = m+1))$$

produce

$$(x = \mu)(y = m+1) + (x = m+1)(y = \mu),$$

y por lo tanto también

$$(f'(x) = f(m+1))(f'(y) = f(\mu)) + (f'(x) = f(\mu))(f'(y) = f(m+1)),$$

y consecuentemente $f'(x) \neq f'(y)$. Así, la proposición $\prod_{x=1}^{n+1} \prod_{y=1}^{m+1} ((x = y) + (f'(x) \neq f'(y)))$ es verdadera.

Observación. Cuando está dada una cierta clase de objetos, uno estará tentado a decir: que estos objetos sean *n* en número, *n* siendo finito, significa que *existe* un mapeo uno-a-uno de estos objetos sobre los primeros *n* números. Pero en esta definición ocurre una variable lógica aparente (el mapeo), y no hay ninguna razón *a priori* para esperar que el dominio sobre el que se extiende esta variable sea finito, a menos que uno tenga, de antemano, un teorema que afirme que *el número de posibles mapeos es finito*. Por lo tanto, desde el punto de vista estrictamente finitista aquí adoptado, tal teorema primero tendría que ser probado si ha de ser definible la noción de cardinalidad para los objetos en cuestión. Esto parece ser un círculo vicioso, pero no lo es: no necesitamos la definición general de la noción de cardinalidad, ofrecida arriba, para establecer un teorema especial que afirme que ciertos objetos son *n* en número, porque podemos establecer tal teorema *ofreciendo realmente* un mapeo; de este modo, evitamos tratar el mapeo como una variable lógica. Así, incluso en los casos mencionados podemos establecer primero un teorema especial a efecto

de que el número de mapeos que son posibles en absoluto sea finito, y después de eso ofrecer la definición general de la noción de cardinalidad para clases de objetos.

Para cualquier clase, puede ofrecerse de manera general el número de enteros positivos que son $\leq n$ y que pertenecen a esa clase mediante una función definible como sigue.

Sea *U* una función proposicional arbitraria; establezco la[4]

Definición 26. $(NU(1) =)U(1) + (NU(1) = 0)\overline{U(1)}$ y

$$(NU(n+1) = NU(n)+1)U(n+1) + (NU(n+1) = NU(n))\overline{U(n+1)}.$$

En palabras: La función descriptiva *NU*(*x*) tendrá el valor 1 o 0 para *x* = 1 dependiendo de si *U*(1) es verdadera o no. Además, *NU*(*n* + 1) será igual a *NU*(*n*) + 1 o a *NU*(*n*) dependiendo de si *U*(*n* + 1) es verdadera o no.

Es fácil mostrar entonces que *NU*(*n*) da, de hecho, el número de números $x \leq n$ para el que *U*(*x*) es verdadera. No profundizaré en esto aquí.

Frecuentemente es el caso que ciertos objetos son numerados por medio de enteros, pero de un modo tal que varios números son asignados como subíndices para cada objeto. Puede entonces ofrecerse el número de *distintos* objetos entre ellos por medio de una función *T*(*x*) que paso a definir ahora.

Sean $a_1, \ldots, a_n$ los objetos; establecemos la

$$\text{Definición 27. } T(1) = 1; (T(r+1) = T(r))\left(\sum_{s=1}^{r}(a_{r+1} = a_s)\right) + (T(r+1) = T(r)+1)\prod_{s=1}^{r}(a_{r+1} \neq a_s).$$

Por otra parte, por medio de la función Min(*U*, *n*) definida antes, puede ofrecerse una elección, determinada de manera única, de un sistema completo de representantes de distintos objetos *a*. Además, es posible definir las frecuencias asociadas [Häufigkeits-

[4] Estrictamente hablando, el número 0 no ha sido introducido; pero podemos hacer la convención de que la cardinalidad 0 ha de significar que no hay "objetos".

zahlen] que indican qué tan a menudo ocurre cada objeto distinto en la secuencia $a_1, \ldots, a_n$; y así sucesivamente. No quiero elaborar más este punto.

OBSERVACIÓN FINAL

Este artículo fue escrito durante el otoño de 1919, después de haber estudiado el trabajo de Russell y Whitehead. Se me ocurrió que ya el uso de las variables lógicas que ellos llaman "reales" ciertamente bastaría para suministrar un fundamento para grandes partes de las matemáticas. (Relacionado con esto, pues, debe observarse que, por medio de definiciones recursivas, pueden eliminarse variables aparentes que se extienden sobre dominios finitos.) La justificación para introducir variables aparentes que se extienden sobre dominios infinitos parece ser, por tanto, muy problemática; es decir, uno puede dudar de que haya cualquier justificación para el infinito real o el transfinito.

Por otro lado, ya no estoy satisfecho con la manera en la que procede aquí la elaboración lógica, porque al haber seguido el patrón del trabajo de Russell y Whitehead la hice demasiado pesada desde el punto de vista puramente formal. Empero, incluso al suministrar un fundamento para las matemáticas es la sustancia lo que es importante, no la notación. Pronto publicaré otro trabajo sobre los fundamentos lógicos de las matemáticas que esté libre de esta torpeza formal.[5] Pero ese trabajo también es consistentemente finitista; está construido sobre el principio de Kronecker de que una definición matemática [Bestimmung] es una definición genuina si y sólo si conduce a la meta por medio de un número *finito* de intentos.

[5] Desafortunadamente, Skolem nunca publicó este trabajo. Nota del Traductor.