Pero $p < n$ y $q < n$; luego $p - q < n$: con lo cual resulta demostrado el teorema.

TEOREMA 3.º En el caso anterior a es raíz de una ecuación

$$x^m - 1 = 0$$

cuyo exponente m no sólo es inferior á n, sino divisor exacto de n.

DEMOSTRACIÓN. Puesto que a es raíz de $x^n - 1 = 0$, tendremos,

$$a^n = 1$$

Y, puesto que a es raíz impropia, según el teorema anterior será raíz de una ecuación $a^{n'} - 1 = 0$, siendo $n' < n$: es decir

$$a^{n'} = 1.$$

Dividamos n por n': si la división es exacta, el teorema queda demostrado; y si no lo fuere resultaría

$$n = ln' + n'',$$

siendo l el cociente y n'' el resto, que será $< n'$.

En este último caso podremos escribir

$$a^n = 1 \text{ y } a^{n'} = 1$$

bajo esta forma:

$$a^{ln' + n''} = 1 \text{ y } a^{ln'} = 1,$$

sustituyendo para ello por n su valor en la primera, y elevando á l la segunda. Y, por la división de una por otra, se concluye que

$$\frac{a^{ln' + n''}}{a^{ln'}} = 1, \text{ ó bien } a^{n''} = 1.$$

Siguiendo el mismo método, podremos dividir n' por n''; y, suponiendo que la división da l' por cociente y n''' por resto, llegaremos á $a^{n'''} = 1$; y así sucesivamente.

Ahora bien: hemos dividido n por n'

n' por el resto anterior n''

n'' por el resto n'''

. . . .

y, una de dos: ó n y n' tienen un máximo común divisor, m, ó son primos. Si lo primero, tendremos $a^m = 1$: donde se ve que a' es raíz de $x^m = 1$, siendo m divisor de n, puesto que es máximo común divisor de n y n', y el teorema queda demostrado.

Si lo segundo, el último resto será 1 y tendremos $a^1 = 1$, que también está comprendido como caso particular en el teorema, puesto que 1 divide á n.

Consecuencia de los teoremas anteriores para las raíces impropias, en el caso de $n = p^\pi$.—Puesto que toda raíz impropia, a, es raíz de una ecuación $x^m = 1$, siendo m divisor de p^π, habrá de ser m de la forma $p^{\pi'}$, $(\pi' < \pi)$, y tendremos:

$$a^{p^{\pi'}} = 1;$$

y, elevando á $p^{\pi - \pi' - 1}$,

$$\left(a^{p^{\pi'}}\right)^{p^{\pi - \pi' - 1}} = 1;$$

ó bien

$$a^{p^{\pi'} \cdot p^{\pi - \pi' - 1}} = 1;$$

y por último

$$a^{p^{\pi - 1}} - 1 = 0:$$

luego todas las raíces impropias son raíces de

$$a^{p^{\pi - 1}} - 1 = 0,$$

Pero ¿habrá alguna otra raíz en la ecuación precedente?

Para averiguarlo veamos cuál es el número de raíces impropias de $x^{p^\pi} - 1 = 0$.

El número total de raíces en este caso es p^π.

El de raíces propias es

$$\varphi(p^\pi) = p^{\pi - 1}(p - 1) = p^\pi - p^{\pi - 1}$$

Luego el de raíces impropias será

$$p^{\pi}-(p^{\pi}-p^{\pi-1})=p^{\pi-1}:$$

precisamente el grado de la ecuación

$$x^{p^{\pi-1}}-1=0.$$

Resumiendo: todas las raíces impropias están en $x^{p^{\pi-1}}-1=0$; su número es $p^{\pi-1}$; y son desiguales, pues desiguales son las raíces de $x^n-1=0$: luego precisamente $x^{p^{\pi-1}}-1=0$ es el factor correspondiente á las raíces impropias, las contiene todas, y no contiene ninguna más.

De aquí resulta como consecuencia final que, dividiendo $x^{p^{\pi}}-1$ por $x^{p^{\pi-1}}-1$, se tendrá el factor de las raíces propias: es decir que en el caso $n=p^{\pi}$

$$f_n(x)=\frac{x^{p^{\pi}}-1}{x^{p^{\pi-1}}-1}:$$

resultado idéntico al que obtuvimos por el método de la inversión, pero con mucha más rapidez ahora.

Sólo hemos expuesto de estas diversas teorías lo puramente preciso para la cabal inteligencia de la nota de Wantzel: quien desee profundizarlas puede, repetimos, consultar los tratados clásicos de Gauss, el Algebra superior de Serret, y la obra citada de Dedekin: ó la de D. Eulogio Jiménez, en la cual con gran acierto, aunque con excesiva concisión á veces, se hallan condensados los fundamentos de la Teoría de los Números.

DIVISIÓN DE LA CIRCUNFERENCIA EN PARTES IGUALES.

Supongamos que se pretende dividir una circunferencia en n partes iguales.

Desde luego puede simplificarse el teorema si n es un número compuesto.

Supongamos que n se descompone en dos factores primos entre sí, N y N', de modo que

$$n = N \times N'.$$

El problema de dividir la circunferencia en n partes quedará resuelto si se sabe dividir en N y N' partes respectivamente.

Supongamos en efecto que por la recta y el círculo sabemos buscar dos arcos (siendo el radio 1)

$$\frac{2\pi}{N} \quad y \quad \frac{2\pi}{N'}.$$

Repitamos el primer arco m veces y m' veces el segundo, siendo m y m' números enteros que ya determinaremos: resultarán dos arcos

$$m\,\frac{2\pi}{N} \quad y \quad m'\,\frac{2\pi}{N'};$$

y, restándolos uno de otro, tendremos un arco

$$x = m\,\frac{2\pi}{N} - m'\,\frac{2\pi}{N'} = 2\pi\,\frac{mN' - m'N}{NN'} = \frac{2\pi}{n}\,(mN' - m'N).$$

Siendo N y N' primos entre sí, se sabe, por la teoría de las ecuaciones indeterminadas de primer grado, que siempre pueden determinarse dos enteros, m' y m, tales que

$$mN' - m'N = 1$$

Luego

$$x = \frac{2\pi}{n}:$$

con lo cual queda la circunferencia dividida en n partes iguales, porque sumar arcos y restarlos es operación que se efectúa con la recta y el círculo.

El problema general se reduce, pues, á otro más sencillo; y podrá dividirse 2π en n partes, siendo

$$n = a^{\alpha}\, b^{\beta}\, c^{r} \ldots,$$

si sabemos y podemos dividir 2π en

$$a^{\alpha},\ b^{\beta},\ c^{r} \ldots$$

partes iguales.

Tratemos, pues, de este problema: dividir la circunferencia en n partes iguales, siendo

$$n = p^{\pi}.$$

Aplicación de la ecuación binomia. Dada en general la ecuación

$$x^n - 1 = 0,$$

(siendo n cualquiera) hemos visto que es raíz de dicha ecuación

$$x = \cos\frac{2\pi}{n} + \sqrt{-1}\,\mathrm{sen}\frac{2\pi}{n}.$$

Pues bien, si por la recta y el círculo pudiésemos construir esta raíz, el problema quedaba resuelto, porque

$$\cos\frac{2\pi}{n} \text{ y } \mathrm{sen}\frac{2\pi}{n}$$

son el coseno y el seno de la n^{ma}. parte de 2π.

Más aun: si se quiere evitar el empleo de imaginarias, puede determinarse una ecuación cuyas raíces den los valores de

$$\cos\frac{2\pi}{n},\ \cos\frac{4\pi}{n};\ \cos\frac{6\pi}{n}\ \ldots$$

En efecto: si suponemos n impar y dividimos $x^n - 1$ por $x - 1$, para suprimir la raíz 1, la ecuación

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + x^{n-3} + \ldots + x + 1 = 0$$

es de la forma de las ecuaciones recíprocas; y sustituyendo en ella $x + \frac{1}{x} = z$, puede obtenerse una ecuación del grado $\frac{n-1}{2}$ en z, cuyas raíces serán

$$\cos\frac{2k\pi}{n} + \sqrt{-1}\,\mathrm{sen}\frac{2k\pi}{n} + \frac{1}{\cos\frac{2k\pi}{n} + \sqrt{-1}\,\mathrm{sen}\frac{2k\pi}{n}};$$

ó bien

$$\cos\frac{2k\pi}{n} + \sqrt{-1}\,\mathrm{sen}\frac{2k\pi}{n} + \frac{\cos\frac{2k\pi}{n} - \sqrt{-1}\,\mathrm{sen}\frac{2k\pi}{n}}{\cos^2\frac{2k\pi}{n} + \mathrm{sen}^2\frac{2k\pi}{n}},$$

que es igual á

$$\cos\frac{2k\pi}{n}+\sqrt{-1}\,\text{sen}\frac{2k\pi}{n}+\cos\frac{2k\pi}{n}-\sqrt{-1}\,\text{sen}\frac{2k\pi}{n}=2\cos\frac{2k\pi}{n}$$

Si n fuese par, podria fácilmente reducirse este caso al anterior por los métodos generales del Algebra; pero es inútil insistir sobre este punto, porque para dividir 2π en

$$n = 2^s a^\alpha b^\beta \ldots$$

basta dividir la circunferencia en 2^s partes, y después en a^α, en b^β etc., según poco antes hemos visto.

La división de dos en dos partes no ofrece dificultad, y sólo queda la división en p^π, siendo p un número impar: de suerte que nos basta examinar este caso.

Supongamos, pues, según hemos dicho, que $n=p^\pi$, representando por p un entero impar.

La ecuación del problema, la $F(x) = 0$ del método general de Wantzel, será en este caso

$$x^{p^\pi} - 1 = 0;$$

y el primer problema que debemos resolver es el de averiguar si esta ecuación es ó no irreducible. Desde luego no lo es porque tiene el factor $x-1$; pero aun tiene otro factor de mayor grado, que es precisamente el que contiene todos los binomios $x - a$ de las raíces propias.

Hemos visto, en efecto, que

$$x^{p^\pi} - 1 = \left[x^{p^{\pi-1}(p-1)} + x^{p^{\pi-1}(p-2)} + x^{p^{\pi-2}(p-3)} \ldots + \right.$$
$$\left. + x^{p^{\pi-1}} + 1\right]\left[x^{p^{\pi-1}} - 1\right].$$

El primer factor contiene la raíz propia

$$x = \cos\frac{2\pi}{n} + \sqrt{-1}\,\text{sen}\,\frac{2\pi}{n},\ (\text{siendo } n = p^\pi)$$

que es la del problema, porque $\cos\frac{2\pi}{n}$ es el coseno del arco que buscamos: luego la verdadera ecuación del problema será:

$$x^{p^{\pi-1}(p-1)}+x^{p^{\pi-1}(p-2)}+x^{p^{\pi-1}(p-3)}+\ldots+x^{p^{\pi-1}}+1=0,$$

y se presenta la siguiente cuestión fundamental para que podamos aplicar el método de Wantzel : ¿esta ecuación es irreducible?

Resolución. La ecuación propuesta, que para abreviar llamaremos X, es decir

$$X=x^{p^{\pi-1}\cdot(p-1)}+x^{p^{\pi-1}(p-2)}+\ldots+x^{p^{\pi-1}}+1=0,$$

es en efecto irreducible, y he aquí la sencillísima demostración que da Kronecker y que ha reproducido D. Eulogio Jiménez en su obra citada.

Si X no es irreducible, podrá descomponerse en dos factores ó polinomios, de coeficientes enteros, que llamaremos $\varphi(x)$ y $\Psi(x)$, porque esta es la definición de las ecuaciones reducibles, y tendremos:

$$X=\varphi(x)\ \Psi(x);$$

ó bien

$$x^{p^{\pi-1}(p-1)}+x^{p^{\pi-1}(p-2)}+x^{p^{\pi-1}(p-3)}\ldots+x^{p^{\pi-1}}+1$$
$$=\varphi(x)\ \Psi(x).$$

Haciendo $x=1$ en la *identidad anterior*, resultará:

$$1+1+1+\ldots+1+1=\varphi(1)\ \Psi(1).$$

El número de unidades del primer miembro es el de términos de X, igual á p: luego

$$p=\varphi(1)\ \Psi(1)$$

Mas como p es un número primo, que no puede, por lo tanto, descomponerse en dos factores enteros, una de las dos cantidades, $\varphi(1)$ ó $\Psi(1)$, será necesariamente igual á ± 1, para que desaparezca el absurdo indicado. Supongamos para fijar las ideas que $\varphi(1)$ sea la que se reduce á la unidad, y tendremos

$$\varphi(1)=\pm 1.$$

Ahora bien: si a es una raíz propia de $x^{p^\pi}-1=0$, las potencias

$$a,\ a^\alpha,\ a^\beta,\ a^\gamma \ldots$$

representando α, β, γ... los números primos con p^π, é inferiores al mismo, serán precisamente la totalidad de las raíces de $X=0$ (que es la ecuación que contiene todas las raíces propias); y para que X se reduzca á cero será preciso que uno de sus factores, φ ó Ψ, se reduzca á cero. Resulta, pues, que algunas de estas raíces anularán á $\varphi(x)$; y, sustituyéndolas todas en $\varphi(x)$, en el producto

$$\varphi(a)\,.\,\varphi(a^\alpha)\,.\,\varphi(a^\beta)\,.\,\varphi(a^\gamma)\ldots$$

uno ó varios factores serán nulos de modo que tendremos

$$\varphi(a)\,.\,\varphi(a^\alpha)\,.\,\varphi(a^\beta)\,.\,\varphi(a^\gamma)\ldots=0.$$

Lo que hemos dicho para la raíz propia a puede repetirse para todas las demás raíces a', a'' ...: luego la ecuación

$$\varphi(x)\,.\,\varphi(x^\alpha)\,\varphi(x^\beta)\,\varphi(x^\gamma)\ldots=0$$

se anula por a, a', a'' ..., es decir por todas las raíces de $X=0$: lo cual significa que dicha ecuación contiene á X como factor. Tendremos, pues,

$$\varphi(x)\,\varphi(x^\alpha)\,\varphi(x^\beta)\,\varphi(x^\gamma)\ldots=X\,.\,C(x)$$

representando por $C(x)$ el polinomio entero que resulta de dividir $\varphi(x)\,\varphi(x^\alpha)\,\varphi(x^\beta)\ldots$ por X

Haciendo en esta identidad $x=1$, tendremos:

$$[\varphi(1)]^{\varphi(p^\pi)}=p\,.\,C(1),\quad \text{ó bien}\quad 1=p\,C(1):$$

puesto que el número de factores $\varphi(1)$ es el de números primos con p^π inferiores á él, aunque esto nada importa, porque $\varphi(1)=\pm1$, y porque X, para $x=1$, se reduce como hemos visto á p: además $C(1)$ es número entero que no puede ser *cero*, pues entonces tendríamos $1=0$.

Pero la ecuación $1 = pC$ (1) es absurda, puesto que 1 no puede ser igual á un entero p, distinto de la unidad, ni á un múltiplo suyo.

Este resultado absurdo nos prueba que la ecuación $X = 0$ no es reducible, toda vez que dicho resultado es consecuencia lógica de suponerla reducible.

Casos de posibilidad. Puesto que

$$x^{p^{\pi-1}(p-1)} + x^{p^{\pi-1}(p-2)} + \ldots\ldots + x^{p^{\pi-1}} + 1 = 0$$

es la ecuación del problema y es irreducible, para que la división del círculo en partes ó arcos iguales *sea posible*, será preciso, según la teoría general de Wantzel, que $p^{\pi-1}(p-1)$, que expresa el grado de la ecuación, sea de la forma 2^n: condición *necesaria* aunque no *suficiente*.

Mas para que $p^{\pi-1}(p-1)$ sea igual á 2^n, será preciso también que solo contenga factores primos iguales á 2.

Examinemos con dicho criterio los dos factores $p^{\pi-1}$ y $p-1$.

1.° Siendo p impar, como hemos supuesto, para que $p-1$ sólo contenga el factor primo 2, ó se verifique que

$$p-1 = 2^{n'}$$

p ha de ser de la forma

$$p = 2^{n'} + 1.$$

Pero en este caso

$$p^{\pi-1} = (2^{n'} + 1)^{\pi-1},$$

que es el otro factor, no puede ser de la forma $2^{n''}$, porque es esencialmente impar: luego es preciso que se reduzca á la unidad ya que no puede ser una potencia de 2; y así tendremos

$$\pi - 1 = 0 \text{ ó } \pi = 1.$$

Luego la primera *condición de posibilidad* de la división de la circunferencia en partes iguales por la recta y el círculo, cuando el número n en que ha de dividirse la circunferencia es primo p y está elevado á 1, es que dicho número primo sea de la forma $2^{n'} + 1$. Condición de *posibilidad* quiere decir condición *necesaria*, pero no *suficiente*.

2.º El factor $p^{\pi-1}$, si $\pi-1$ no es igual á *cero*, tiene que ser igualmente de la forma $2^{n''}$: luego $p=2$; en cuyo caso $p-1=1$.

Es, pues, segunda *condición de posibilidad* cuando el número primo p entra elevado á una potencia que p sea igual á 2.

Ahora bien: cuando estas condiciones se verifican, para apurar la cuestión y ver si realmente es posible la división propuesta, será preciso aplicar ó el método de Wantzel, ó el de Gauss, ó el general de las ecuaciones abelianas.

Ejemplos. Sabemos dividir 2π en 2, 3 y 4 partes iguales por los métodos elementales de la Geometría, y todos estos casos están comprendidos en los dos de posibilidad indicados.

Porque $2=2^1$;

$3=2^1+1$

y $4=2^2$.

También es posible dividir 2π en 5 partes iguales, porque $5=2^2+1$.

Para dividir 2π en 6 partes se dividirá en 3 y 2.

Para dividirlo en 7 partes, hay que aplicar la fórmula general; y, como la mayor potencia de 2 contenida en 7 es 4, y queda un resto igual á 3, el problema no es posible.

La división en 8 partes es posible, y en efecto $8=2^3$.

No lo es la división en 9 partes, porque $9=3^2$.

Es posible la división en 10 partes, por la división en 5 y 2.

No lo es la división en 11 partes, porque $11=8+3=2^3+3$.

Es posible la división en 12 partes, porque $12=2^2 \,.\, 3$.

No lo es la división en 13, porque $13=2^3+5$.

No lo es la división en 14, porque $14=2 \,.\, 7$

Es posible la división en 15, atendiendo á que $15=3 \,.\, 5$

También es posible la división en 16, porque $16=2^4$

Y hay posibilidad (preventiva al menos, que luego se ve que es real) de dividir 2π en 17 partes, porque

$$17=16+1=2^4+1$$

Y así sucesivamente.

El estudio del caso $n = 17$, en el cual la aplicación del método general de Wantzel trae consigo cálculos pesadísimos, nos ha inducido á introducir algunas simplificaciones en dicho método, y entre otras las que resultan de resolver el siguiente problema.

Problema. Dado un sistema de varias ecuaciones con varias incógnitas x, y, z, etc., determinar las raíces enteras, sin necesidad de obtener la ecuación final de cada incógnita.

Como la idea es en extremo sencilla y no la hemos visto tomada en cuenta por ningún autor, la expondremos sumariamente.

Resolución. Para ello es preciso ante todo demostrar un

Lema. Si una de las ecuaciones del sistema, ordenada por relación á una incógnita, x por ejemplo, es de la forma

$$x^m + Ax^{m-1} + Bx^{m-1} + \ldots\ldots + Tx + N = 0,$$

siendo A, B, C ..... polinomios enteros de las demás incógnitas, y la cantidad independiente de x es un número entero N, los valores enteros de x, si los hay en combinación con valores enteros también de y, z, ..., serán divisores de N, y entre los divisores de N deberán buscarse, por lo tanto, dichas raíces como en el caso sencillísimo de una ecuación con una incógnita.

En efecto, si $x = a$, $y = b$, $z = c$ ..... es un sistema entero que satisface á todas las ecuaciones, y por lo tanto á

$$x^m + A x^{m-1} + Bx^{m-1} + \ldots\ldots + T x + N = 0,$$

tendremos, efectuando dicha sustitución,

$$a^m + A(b, c, \ldots) a^{m-1} + B(b, c \ldots) a^{m-1} + \ldots T(d, c \ldots) a + N = 0$$

ó, dividiendo por a,

$$a^{m-1} + A(b, c \ldots) a^{m-2} + B(b, c \ldots) a^{m-3} + \ldots T(d, c \ldots) = -\frac{N}{a}$$

Pero el primer miembro es entero: luego $\frac{N}{a}$ también lo es: y a es un divisor de N, como queríamos demostrar.

La dificultad consiste en que este caso es al parecer particularísimo; pues en general tendremos

$$x^m + A(y,z....)x^{m-1} + B(y,z....)x^{m-2} + ... + T(y,z....)x + U(y,z....) + N = 0,$$

siendo $U(y, z.....)$ un polinomio entero de todas las incógnitas, menos x.

El teorema se aplica entonces á $U(y,z.....)+N$ como antes á N; pero de nada sirve esta observación, porque y, $z.....$ son incógnitas cuyos valores no conocemos todavía.

Y, sin embargo, este caso general puede reducirse al del lema, eliminando sucesivamente todos los términos de $U(y, z.....)$ como vamos á indicar.

Para más claridad en las ideas consideremos por de pronto un caso particular, y aun éste aclarémoslo con un ejemplo.

Propongámonos resolver con números enteros las dos ecuaciones

$$x^2 - 2xy + y^2 - y + 2 = 0$$
$$x^2 + xy - y^2 + 2y - 7 = 0$$

Toda la dificultad consiste en hacer que desaparezcan los términos con y, quedando únicamente términos con x y cantidades constantes.

Para ello vamos á eliminar el término $+y^2$ y el $-y$ de la primera; y el $-y^2$ y el $+2y$ de la segunda; y como importa poco lo que pueda resultar de los términos en x, con tal que todos contengan x, los representaremos invariablemente por (x), prescindiendo de las alteraciones de sus coeficientes.

Las dos ecuaciones propuestas tomarán la forma

$$\left.\begin{array}{l}(x) + y^2 - y + 2 = 0 \\ (x) - y^2 + 2y - 7 = 0\end{array}\right\} (1)$$

Sumando para eliminar y^2 tendremos

$$(x) + y - 5 = 0:$$

advirtiendo que esta (x) no será la misma que antes, lo cual importa poco.

A las dos ecuaciones propuestas podemos sustituir estas dos:

$$\left.\begin{array}{l}(x) - y^2 + 2y - 7 = 0 \\ (x) + y - 5 = 0.\end{array}\right\} (2)$$

Ó, multiplicando la última por y, estas otras dos:

$$\left.\begin{array}{l}(x) - y^2 + 2y - 7 = 0 \\ (x) + y^2 - 5y = 0.\end{array}\right\} (3).$$

Sumándolas tendremos

$$(x) - 3y - 7 = 0.$$

Y al sistema (3) podremos sustituir el siguiente:

$$\left.\begin{array}{l}(x) - 3y - 7 = 0 \\ (x) + y - 5 = 0.\end{array}\right\}$$

Multiplicando la segunda por 3 se convierte en

$$(x) + 3y - 15 = 0:$$

y, sumando este resultado con la anterior, en

$$(x) - 22 = 0$$

En la cual (x) es un polinomio en x sin término constante, cuyos coeficientes son funciones de y. Dicha ecuación está comprendida en el *Lema*: luego, si hay soluciones enteras para x, y, los valores de x serán, con el signo $\pm$,

1, 2, 11 ó 22.

Ensayemos todos estos valores.

Sustituyendo $x = 1$ en la primera, por ejemplo, de las dos ecuaciones propuestas tendremos:

$$1 - 2y + y^2 - y + 2 = 0$$

ó bien

$$y^2 - 3y + 3 = 0,$$

que no tiene raíces enteras: luego debemos desechar $x = 1$.

Sustituyendo $x = 2$ en la misma, resultará

$$4 - 4y + y^2 - y + 2 = 0,$$

ó bien

$$y^2 - 5y + 6 = 0,$$

que tiene las dos raíces $y = 2$, $y = 3$

Pero, sustituyendo en la 2.ª de las propuestas, resulta

$$4+2\,y-y^2+2\,y-7=0,$$

ó bien

$$y^2-4\,y+3=0,$$

que solo admite la raíz 3.

Tenemos, pues, el sistema

$$x=2\ ;\ y=3.$$

Del mismo modo ensayaríamos la solución $x=11$,

Podríamos haber empezado por determinar la y, poniendo las ecuaciones propuestas bajo esta forma

$$y^2\begin{array}{r|l} -2x & y+x^2+2=0 \\ -\ 1 & \end{array}$$

$$y^2\begin{array}{r|l} -x & y-x^2+7=0 \\ -2 & \end{array}$$

ó bien

$$(y)+x^2+2=0$$
$$(y)-x^2+7=0$$

Y, sumándolos, habríamos deducido esta otra finalmente:

$$(y)+9=0,$$

que nos induciría á ensayar como valores de y los números 1, 3 (ya determinado), y el 9.

Observaciones.—1.ª En vez de las eliminaciones sucesivas de las potencias de una de las incógnitas, y, por ejemplo, pudiera aplicarse el método de las determinantes, multiplicando cuantas veces fuere preciso ambas ecuaciones por y, y buscando la determinante final en que resultasen eliminadas las potencias de y, como en el conocido método de Sylvester.

2.ª Si se observan atentamente las operaciones efectuadas, se verá que equivalen á la aplicación de las divisiones sucesivas de los polinomios finales hasta llegar á un resto independiente de la incógnita.

Caso general.—Puede generalizarse este procedimiento para el caso de m ecuaciones con m incógnitas.

Basta elegir una de ellas y ordenar por relación á sus potencias: sea x dicha incógnita.

El término independiente de x en cada ecuación será un polinomio con m—1 incógnitas, y, z, t..., Eliminando las potencias de y por los métodos indicados, obtendremos m — 1 ecuaciones, cuyos últimos polinomios solo contendrán las m—2 incógnitas z, t...; y, siguiendo el mismo procedimiento, llegaremos á una ecuación en la que el término independiente de x será un número entero. Entre sus divisores estarán los únicos valores enteros y posibles de x.

Aclaremos esta idea general por un ejemplo.

Sean las tres ecuaciones con tres incógnitas.

$$
\begin{aligned}
(y^2-1)z+x^2+xy+y-7&=0\\
z^2+yz+xy^2+4&=0\\
(-y+1)z^2+(-y+1)z+x-2&=0
\end{aligned}
$$

que pueden ponerse bajo esta forma:

$$
\left.\begin{aligned}
&(z)+x^2+xy+y-7=0,\\
&(z)+xy^2+4=0,\\
&(z)+x-2=0.
\end{aligned}\right\}\ldots \qquad (1)
$$

Eliminemos de las dos últimas la x, multiplicando la última por y^2 y restando; y así tendremos

$$
\begin{aligned}
&(z)+xy^2+4=0\\
&(z)+xy^2-2y^2=0
\end{aligned}
$$

y, por fin,

$$(z)+2y^2+4=0 \ldots \qquad (2)$$

Eliminemos entre la primera y la tercera de (1) las potencias sucesivas de x. Tendremos:

$$
\begin{aligned}
&(z)+x^2+xy+y-7=0,\\
&(z)+x-2=0,\\
&(z)+x^2-2x=0\\
&(z)+(2+y)x+y-7=0.
\end{aligned}
$$

Esta ecuación y la segunda forman un grupo

$$
\begin{aligned}
&(z)+(2+y)x+y-7=0\\
&(z)+x-2=0
\end{aligned}
$$

que solo contiene x, la cual podremos eliminar, resultando por consiguiente:

$$(z)+(2+y)x+y-7=0$$
$$(z)+(2+y)x-2(2+y)=0$$

de donde $$(z)+2(2+y)+y-7=0$$

ó bien

$$(z)+3y-3=0 \ldots \qquad (3)$$

La (2) y (3) forman el siguiente grupo, que solo contiene y:

$$(z)+2y^2+4=0$$
$$(z)+3y-3=0.$$

Multiplicando la segunda por 2 y y la primera por 3, y restando, resulta

$$(z)+6y+12=0$$

Y ésta y la segunda forman el grupo

$$(z)+3y-3=0$$
$$(z)+6y+12=0$$

de donde, eliminando y, obtendremos:

$$(z)+18=0 \ldots \qquad (4)$$

En suma: para el caso que nos ocupa, al sistema propuesto de tres ecuaciones podremos sustituir el siguiente:

$$z^2+yz+xy^2+4=0$$
$$(z)+3y-3=0$$
$$(z)+18=0:$$

la primera de las cuales sólo contiene x, y, en el polinomio final; solamente y la segunda; y el número 18 la tercera.

Si hay valores enteros para z serán 1, 2, 3, 9, 6, ó 18, tanto con signos positivos como negativos.

Suprimiendo pormenores sencillísimos y simplificaciones que desde luego ocurren, ensayemos $z=3$.

Las dos primeras ecuaciones fundamentales se convierten en

$$(y^2-1)3+x^2+xy+y-7=0$$
$$9+3y+xy^2+4=0$$

ó bien

$$x^2+xy+3y^2+y-10=0$$
$$xy^2+3y+13=0$$

ó, en forma más sencilla:

$$(x)+3y^2+y-10=0$$
$$(x)+3y+18=0$$

Aplicando á estas dos ecuaciones uno de los métodos generales, el del m. c. d por ejemplo, tendremos

$$(x)+42=0.$$

Los valores de x deben buscarse entre los divisores de 42: para abreviar tomemos sólo el 2, y tendremos el sistema $z=3$, $x=2$, que, sustituído en una de las primeras ecuaciones, da

$$4+2\,y+3\,y^2+y-10=0$$

ó bien

$$y^2+y-2=0;$$

ecuación satisfecha por $y=1$.

Así, pues, el sistema propuesto admite los valores $z=3$, $x=2$, $y=1$.

A pesar de lo expedito del método, los cálculos que su aplicación exige son pesados, como se advierte en ejemplos tan sencillos como los que preceden; pero en cambio pueden emplearse multitud de *simplificaciones* y *exclusiones de valores* que den rapidez al procedimiento.

Nueva generalización.—Todo lo dicho para las soluciones enteras puede aplicarse en general á las soluciones enteras y racionales de varias ecuaciones con varias incógnitas en que los datos sean algebráicos.

El problema anterior es el *primero* de los que deben resolverse para hallar la solución del problema principal, referente á la división por 17 de la circunferencia.

El segundo consiste en determinar las *soluciones fraccionarias* de un sistema de ecuaciones sin pasar por la ecuación final: cuestión mucho más difícil, y en la cual por falta de tiempo no podemos detenernos ya, pues el presente trabajo va tomando excesiva extensión: mucha más de la que en un principio imaginamos que alcanzaría.

Ambas cuestiones se completan con esta otra: determinación *de límites* para las raíces reales en un sistema de ecuaciones, lo cual quizá pueda conseguirse por un artificio particular y aplicando la teoría de las desigualdades.

Pero aún resueltas estas diferentes cuestiones preliminares, el método de Wantzel conduce, en el caso concreto que nos ocupa, á cálculos sumamente pesados, porque la ecuación final es de octavo grado; y á fin de simplificar su aplicación hemos dividido el problema en dos partes: tomando por de pronto una ecuación de 4.º grado y otra de 2.º; y después, ya determinados los coeficientes numéricos de la primera, reemplazándola por dos de 2.º grado.

Todo esto es en extremo enojoso, si no difícil; y por las razones expuestas y por falta de tiempo, daremos fin por ahora á nuestra tarea, aplazando para ocasión más desahogada la terminación y análisis minuciosa de todas las cuestiones que hemos indicado ligeramente.
