А. Г. ШКОЛЬНИК

ЗАДАЧА ДЕЛЕНИЯ КРУГА

А. Г. ШКОЛЬНИК

ЗАДАЧА ДЕЛЕНИЯ КРУГА

ИЗДАНИЕ ТРЕТЬЕ

ПОСОБИЕ ДЛЯ УЧИТЕЛЕЙ

ГОСУДАРСТВЕННОЕ
УЧЕБНО-ПЕДАГОГИЧЕСКОЕ ИЗДАТЕЛЬСТВО
МИНИСТЕРСТВА ПРОСВЕЩЕНИЯ РСФСР
МОСКВА * 1961

Книга А. Г. Школьника, посвящённая вопросу о двучленных уравнениях и делении круга циркулем и линейкой, представляет собой написанную очень доступно и вместе с тем на безукоризненном научном уровне монографию по одному из вопросов, наиболее интересных и поучительных во всей истории математики. Издание этой монографии имеет поэтому значительную ценность прежде всего для библиотеки учителя, а затем и для студенчества и всех интересующихся математикой и развитием её идей.

Действительный член АПН проф. *А. Хинчин.*

9/X-1947 г.

ИЗ ПРЕДИСЛОВИЯ К ПЕРВОМУ ИЗДАНИЮ

Вопрос о возможности деления окружности циркулем и линейкой на равные части (или о возможности построения правильных многоугольников), с которым мы встречаемся в курсе элементарной геометрии, не получает там своего разрешения, так как требует более глубоких средств исследования. Полное решение этой задачи давалось до сих пор на основе теории Галуа и потому оставалось в значительной мере недоступным преподавателям средней школы, не владеющим этой теорией. Настоящая работа ставит своей целью дать вполне строгое изложение названного выше вопроса более элементарными средствами, без применения теории групп.

§ 1. ВВЕДЕНИЕ

1. Решение уравнений вида $x^n - a = 0$, называемых двучленными, находится в тесной связи с геометрической задачей построения правильных многоугольников, или, что то же, с задачей деления окружности на равные части. Из элементарной геометрии известно, как, пользуясь циркулем и линейкой, построить вписанные в окружность квадрат и правильные шестиугольник, треугольник, десятиугольник, пятиугольник и пятнадцатиугольник. Известно, далее, как удвоить число сторон правильного многоугольника, пользуясь теми же средствами построения. Таким образом, оказывается возможным делить окружность на 2^k, $3 \cdot 2^k$, $5 \cdot 2^k$, $15 \cdot 2^k$ частей. Возникает вопрос, на сколько же равных частей вообще возможно разделить окружность при помощи циркуля и линейки. Можно ли, например, разделить окружность на 7, 9 и т. д. частей?

Задача деления окружности, известная ещё в древности, получила своё полное разрешение, однако, лишь в новое время. Решение её выпало на долю юного Гаусса, выяснившего условия, от которых зависит возможность построения правильных многоугольников циркулем и линейкой, доказавшего (1796 г.) возможность построения *правильного семнадцатиугольника* и давшего общий метод и почти исчерпывающее решение всей проблемы.

2. Решение двучленного уравнения $x^n - a = 0\ (a \neq 0)$ равносильно извлечению корня n-й степени из числа a: $x = \sqrt[n]{a}$. Последняя задача допускает, как известно, следующее решение.

Пусть

$$a = r(\cos\varphi + i \sin\varphi),$$

где r — модуль и φ — аргумент комплексного числа a. Кор-

нем n-й степени из a называется такое число $b = \sqrt[n]{a}$, что $b^n = a$.

Пусть $b = \rho(\cos\theta + i\sin\theta)$. Тогда, возводя b в n-ю степень по формуле Муавра, получаем:

$$\rho^n(\cos n\theta + i\sin n\theta) = r(\cos\varphi + i\sin\varphi)$$

и, следовательно,

$$\rho^n = r,\ n\theta = \varphi + 2k\pi \quad (k = 0, 1, 2,\ldots),$$

откуда

$$\rho = \sqrt[n]{r}, \qquad \theta = \frac{\varphi+2k\pi}{n}$$

и, следовательно,

$$b = \sqrt[n]{r}\left(\cos\frac{\varphi+2k\pi}{n} + i\sin\frac{\varphi+2k\pi}{n}\right) \qquad (k = 0, 1, 2,\ldots). \quad (1)$$

Под $\sqrt[n]{r}$ мы здесь понимаем положительное число — арифметический корень из положительного числа[1].

Давая k последовательно значения 0, 1, 2,..., мы получим для b n различных значений при $k = 0, 1, 2,\ldots, n-1$:

$$\left.\begin{aligned}
&b_0 = \sqrt[n]{r}\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right),\\
&b_1 = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi}{n} + i\sin\frac{\varphi+2\pi}{n}\right),\\
&b_2 = \sqrt[n]{r}\left(\cos\frac{\varphi+4\pi}{n} + i\sin\frac{\varphi+4\pi}{n}\right),\\
&\cdots\cdots\cdots\cdots\cdots\\
&b_{n-1} = \sqrt[n]{r}\left(\cos\frac{\varphi+2(n-1)\pi}{n} + i\sin\frac{\varphi+2(n-1)\pi}{n}\right).
\end{aligned}\right\} \quad (2)$$

При дальнейшем увеличении k корни будут повторяться. Например, при $k = n$ $\frac{\varphi+2n\pi}{n} = \frac{\varphi}{n} + 2\pi$ и так как 2π есть период для синуса и косинуса, то $b_n = b_0$. Таким образом, корень n-й степени имеет n различных значений.

В частности, при $a = 1$ ($r = 1$; $\varphi = 0$) мы получаем особенно важный случай *корней n-й степени из единицы*:

$$\varepsilon = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \qquad (k = 0, 1, 2,\ldots, n-1). \quad (3)$$

---

[1] В теории иррациональных чисел доказывается, что для всякого положительного действительного числа α всегда существует единственный положительный корень n-й степени $\beta = \sqrt[n]{\alpha}$.

Или подробно:

$$\left.\begin{aligned}
&\varepsilon_0 = 1,\\
&\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},\\
&\varepsilon_2 = \cos\frac{4\pi}{n} + i\sin\frac{4\pi}{n},\\
&\qquad\cdots\cdots\cdots\cdots\cdots\\
&\varepsilon_{n-1} = \cos\frac{2(n-1)\pi}{n} + i\sin\frac{2(n-1)\pi}{n}.
\end{aligned}\right\} \qquad (4)$$

Так как

$$b_k = \sqrt[n]{r}\left[\cos\left(\frac{\varphi}{n} + \frac{2k\pi}{n}\right) + i\sin\left(\frac{\varphi}{n} + \frac{2k\pi}{n}\right)\right] =$$

$$= \sqrt[n]{r}\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right)\cdot\left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right),$$

то

$$b_k = b\cdot\varepsilon_k. \qquad (5)$$

Таким образом, *зная b_0 — значение одного корня n-й степени из числа a, мы можем получить все остальные корни умножением на все значения корня n-й степени из единицы.*

Формулы (1) и (3) могут быть записаны в более компактной форме, если прибегнуть к показательной форме комплексного числа

$$a = r\cdot e^{i\varphi}$$

(такую форму для комплексного числа мы получим, использовав известную формулу Эйлера[1], связывающую показательную функцию с тригонометрическими: $\cos\varphi + i\sin\varphi = e^{i\varphi}$).

Тогда

$$b = \sqrt[n]{r}\cdot e^{\frac{\varphi+2k\pi}{n}i}, \qquad (6)$$

$$\varepsilon = e^{\frac{2k\pi i}{n}}. \qquad (7)$$

---

[1] Выводится из рассмотрения рядов:

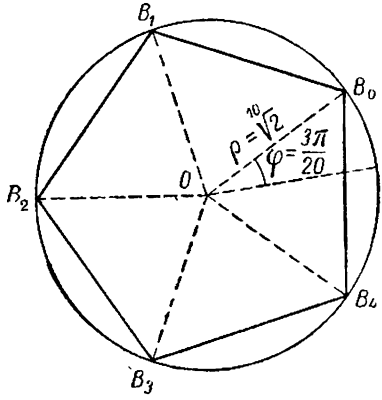
$$e^z = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \ldots,$$

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \ldots,$$

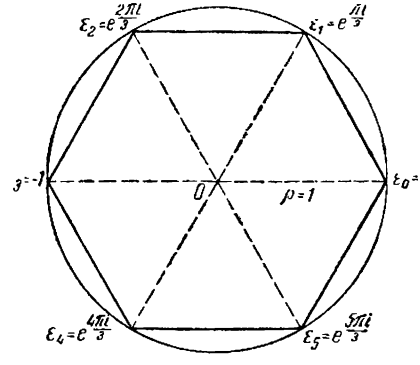
$$\sin z = 1 - \frac{z^3}{3!} + \frac{z^5}{5!} - \ldots.$$

Если воспользоваться геометрическим изображением комплексных чисел как точек плоскости, то сразу становится ясной тесная зависимость, существующая между извлечением корня n-й степени и, следовательно, решением двучленного уравнения, с одной стороны, и делением окружности на n частей, или построением правильного многоугольника, — с другой.

В самом деле, формулы (2) показывают, что все n корней имеют одинаковый модуль $\rho = \sqrt[n]{r}$ и, следовательно, располагаются на окружности с центром в начале координат и радиусом, равным ρ.



Черт. 1.



Черт. 2.

$n = 5$; $a = -1 + i =$
$= \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)$;
$b_k = \sqrt[5]{a} = \sqrt[5]{-1+i} =$
$= \sqrt[10]{2}\left[\cos\left(\frac{3\pi}{20} + \frac{2k\pi}{5}\right) +\right.$
$\left. + i\sin\left(\frac{3\pi}{20} + \frac{2k\pi}{5}\right)\right]$
$(k = 0, 1, 2, 3, 4)$

$n = 6$; $a = 1 = \cos 0 + i\sin 0$;
$\varepsilon_k = \sqrt[6]{1} = \cos\frac{2k\pi}{6} + i\sin\frac{2k\pi}{6} =$
$= e^{\frac{2k\pi i}{6}}$
$(k = 0, 1, 2, 3, 4, 5)$

Из рассмотрения же аргументов видно, что каждый из них отличается от следующего на $\frac{2\pi}{n}$; это и показывает, что точки, изображающие корни n-й степени, делят окружность на n равных частей, что они располагаются в вершинах правильного n-угольника (см. черт. 1 и 2).

3. Итак, извлечение корня, или решение двучленного уравнения, эквивалентно геометрической задаче деления окружности, или построения правильного многоугольника. Нашей целью является исследование условий, при которых эта задача на построение разрешима с помощью циркуля и линейки. Иными словами, нужно установить, в каких случаях корни двучленного уравнения могут быть построены при помощи циркуля и линейки. Но как решается вопрос о возможности построения циркулем и линейкой корней любого уравнения вообще?

Из элементарной геометрии известно, как (с помощью циркуля и линейки) строить сумму или разность данных отрезков $a + b$ или $a - b$, произведение отрезка на целое число $m \cdot a$, четвёртую пропорциональную $\frac{ab}{c}$ и среднее геометрическое $\sqrt{ab}$. Следовательно (полагая в выражении $\frac{ab}{c}$ $b = 1$ и $c = b$, а в выражении $\sqrt{ab}$ $b = 1$), мы видим, что можем построить отрезки:

$$a \pm b, \quad ab, \quad \frac{a}{b}, \quad \sqrt{a}. \tag{8}$$

Отсюда вытекает, что *при помощи циркуля и линейки можно построить любую функцию данных величин (отрезков), если для её получения приходится совершать конечное число раз следующие пять операций: сложение, вычитание, умножение, деление и извлечение квадратного корня.*

В частности, следовательно, можно построить корни квадратного уравнения $ax^2 + bx + c = 0$:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

так как для получения их из данных величин a, b, c над ними не приходится производить никаких иных действий, кроме указанных выше операций: уравнение $ax^2 + bx + c = 0$ разрешимо в квадратных радикалах.

Предположим обратно, что некоторая величина (отрезок) — пусть это будет корень какого-либо уравнения — может быть построена с помощью циркуля и линейки. Всякое построение циркулем и линейкой разбивается на ряд элементарных построений, которые заключаются в нахождении точек пересечения либо двух прямых, либо прямой и окружности, либо двух окружностей. Аналитически для нахождения координат искомых точек приходится решать си-

стему двух уравнений: в случае двух прямых—это два уравнения I степени; в случае прямой и окружности — одно уравнение I степени и одно уравнение II степени; в случае двух окружностей — два уравнения II степени. Во всех случаях системы разрешимы в квадратных радикалах (или даже без их помощи). Это очевидно в первом и во втором случаях. В последнем случае приходится решать систему уравнений:

$$\begin{cases} (x-a)^2 + (y-b)^2 = r^2, \\ (x-a_1)^2 + (y-b_1)^2 = r_1^2. \end{cases}$$

Открывая скобки и вычитая одно уравнение из другого, мы получим уравнение I степени:

$$2(a_1-a)x + 2(b_1-b)\,y + (a^2+b^2 - r^2 - a_1^2-b_1^2+r_1^2) = 0.$$

Определяем из него x или y, подставляем в одно из исходных уравнений, и дальнейшее сводится к решению квадратного уравнения. Итак, координаты искомых точек будут выражаться при помощи квадратных радикалов. Искомая величина (отрезок) найдётся как расстояние между этими точками. Но формула аналитической геометрии $d = \sqrt{(x_2-x_1)^2 + (y_2-y_1)^2}$, дающая расстояние между двумя точками по их координатам, не содержит никаких других иррациональностей, кроме квадратного радикала; поэтому не будет их содержать и искомое выражение для данной величины. Таким образом, если некоторая величина может быть построена циркулем и линейкой, то она выражается (через данные величины) в квадратных радикалах. Итак, окончательно мы можем сделать следующее заключение:

Для того чтобы корни уравнения $f(x) = 0$ *могли быть построены с помощью циркуля и линейки, необходимо и достаточно, чтобы уравнение это разрешалось в квадратных радикалах* [1].

Мы видим, таким образом, что поставленная нами задача деления окружности, или построения правильного многоугольника, циркулем и линейкой сводится к вопросу о разрешении двучленного уравнения в квадратных радикалах.

4. Возможность разрешения двучленного уравнения в квадратных радикалах будет зависеть, как мы увидим,

[1] Подробнее о разрешимости уравнений в радикалах см. ниже (§ 3).

от свойств целого числа n — степени двучленного уравнения. При установлении этой зависимости нам придётся опираться как на некоторые свойства целых чисел, так и на некоторые свойства целых рациональных функций (многочленов, или полиномов). Простейшие из них, чтобы к этому в дальнейшем не возвращаться, мы здесь напомним. Причём, так как многочлены (целые рациональные функции) ведут себя во многих отношениях как целые числа, то мы, чтобы проследить эту аналогию, изложим свойства тех и других параллельно. На доказательстве в большинстве случаев останавливаться не будем.

Для двух (целых и положительных) чисел a и b ($a > b$) всегда можно найти два числа q (частное) и r (остаток) таких, что:

$$a = bq + r \quad (0 \leqslant r < b)$$

(«делимое равно делителю, умноженному на частное, плюс остаток»). Если $r = 0$ и, следовательно, $a = bq$, то a *делится* на b, или кратно b; b является *делителем* a.

Для двух многочленов $f(x)$ и $g(x)$ всегда можно найти два многочлена $q(x)$ (частное) и $r(x)$ (остаток) таких, что (тождественно):

$$f(x) = g(x) \cdot q(x) + r(x),$$

причём степень $r(x)$ меньше степени $g(x)$.

Если $r(x) = 0$ и, следовательно, $f(x) = g(x) \cdot q(x)$, то $f(x)$ *делится* на $g(x)$; $g(x)$ есть *делитель* функции $f(x)$.

I. Имеют место следующие простые предложения (теоремы о делимости):

1. Если a делится на b, а b делится на c, то и a делится на c.
2. Если a и b делятся на c, то и их сумма или разность $a \pm b$ разделится на c [1].
3. Если a делится на c, то и ab делится на c.

1. Если $f(x)$ делится на $g(x)$, а $g(x)$ делится на $h(x)$, то и $f(x)$ делится на $h(x)$.
2. Если $f(x)$ и $g(x)$ делятся на $h(x)$, то и их сумма или разность $f(x) \pm g(x)$ разделится на $h(x)$.
3. Если $f(x)$ делится на $h(x)$, то и $f(x)\,g(x)$ делится на $h(x)$.

[1] Если же a делится на c, а b не делится на c, то и сумма $a + b$ не разделится на c (то же относится и к функциям).

II. Наибольший общий делитель

Число c, являющееся одновременно делителем двух (или более) данных чисел a и b, есть их общий делитель. Наибольший из этих делителей, который делится на все остальные общие делители чисел a и b, есть их *наибольший общий делитель*. В символах:

$$(a, b) = d.$$

Числа, не имеющие общих делителей (кроме единицы, являющейся делителем всякого числа), называются *взаимно простыми*. Для них наибольшим общим делителем служит единица:

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

Если $d = (a, b)$, то

$$a = d \cdot a_1, \quad b = d \cdot b_1,$$

где a_1 и b_1 — взаимно простые числа.

Нахождение наибольшего общего делителя производится методом последовательного деления с помощью *алгорифма Евклида*:

a делится на b, затем b делится на первый остаток r_1, далее первый остаток r_1—на второй остаток r_2 и т. д. Так как остатки убывают, то неизбежно придём к остатку $r_{m+1} = 0$.

$$\left.\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\cdots\cdots\cdots \\ r_{m-3} &= r_{m-2}q_{m-1} + r_{m-1} \\ r_{m-2} &= r_{m-1}q_m + r_m \\ r_{m-1} &= r_m \cdot q_{m+1} \end{aligned}\right\}$$

Если многочлены $f(x)$ и $g(x)$ делятся на $h(x)$, то $h(x)$ есть их общий делитель. Делитель наивысшей степени (определяемый с точностью до постоянного множителя), который делится на всякий другой общий делитель функций $f(x)$ и $g(x)$, есть их *наибольший общий делитель*. Обозначаем его так:

$$(f(x), g(x)) = D(x).$$

Многочлены, не имеющие общих делителей (кроме постоянного, на которое делится всякий многочлен), называются *взаимно простыми*. За их наибольший общий делитель можно принять единицу

$$(f(x), g(x)) = 1.$$

Если $D(x) = (f(x) \cdot g(x))$, то

$$f(x) = D(x) \cdot f_1(x)$$
$$g(x) = D(x) \cdot g_1(x),$$

причём многочлены $f_1(x)$ и $g_1(x)$ взаимно простые.

Нахождение наибольшего общего делителя многочленов производится, как и для чисел, с помощью *алгорифма Евклида*:

$f(x)$ делится на $g(x)$, $g(x)$ делится на первый остаток $r_1(x)$, затем первый остаток $r_1(x)$ — на второй остаток $r_2(x)$ и т. д. Так как степени остатков убывают, то некоторый остаток должен стать равным нулю; пусть $r_{m+1}(x) = 0$.

Последний, не равный нулю, остаток r_m и есть наибольший общий делитель. Докажем это. В том, что r_m есть общий делитель чисел a и b, убеждаемся, рассматривая написанные равенства снизу: из последнего следует, что r_{m-1} делится на r_m, из предпоследнего, — что на r_m делится r_{m-2} и т. д., пока не дойдём до b и a. Чтобы убедиться, что r_m делится на всякий общий делитель a и b, поступим так.

Из предпоследнего равенства:

$$r_m = r_{m-2} - r_{m-1} \cdot q_m, \quad (*)$$

из предшествующих равенств:

$$r_{m-1} = r_{m-3} - r_{m-2} \cdot q_{m-1},$$
$$r_{m-2} = r_{m-4} - r_{m-3} \cdot q_{m-2},$$
$$\cdots\cdots\cdots\cdots$$
$$r_1 = a - bq_1.$$

Подставляя последовательно значения r_{m-1}, r_{m-2}, ..., r_1 в (*), выразим r_m через a и b:

$$r_m = a\alpha + b\beta,$$

где α и β — целые (но не обязательно положительные) числа. Это равенство и показывает, что r_m делится на всякий общий делитель a и b, т. е. что $r_m = d$. Это можно формулировать так: если d есть наибольший общий делитель натуральных чисел a и b, то всегда можно

Тогда

$$\left.\begin{aligned} f(x) &= g(x) \cdot q_1(x) + r_1(x), \\ g(x) &= r_1(x) \cdot q_2(x) + r_2(x), \\ r_1(x) &= r_2(x) \cdot q_3(x) + r_3(x), \\ &\cdots\cdots\cdots\cdots \\ r_{m-3}(x) &= r_{m-2}(x) q_{m-1}(x) + \\ &\quad + r_{m-1}(x), \\ r_{m-2}(x) &= r_{m-1}(x) q_m(x) + \\ &\quad + r_m(x), \\ r_{m-1}(x) &= r_m(x)\, q_{m+1}(x). \end{aligned}\right\}$$

Последний, не равный тождественно нулю, остаток $r_m(x)$ и есть наибольший общий делитель. В том, что $r_m(x)$ есть делитель $f(x)$ и $g(x)$, убеждаемся так же, как и для целых чисел, рассматривая равенства снизу вверх.

Далее из предпоследнего равенства находим $r_m(x)$:

$$r_m(x) = r_{m-2}(x) - r_{m-1}(x) q_m(x). \quad (*)$$

Затем, идя снизу вверх, определяем из остальных равенств остатки $r_{m-1}(x)$, $r_{m-2}(x)$ и т. д.:

$$r_{m-1}(x) = r_{m-3}(x) - r_{m-2}(x)\, q_{m-1}(x),$$
$$r_{m-2}(x) = r_{m-4}(x) - r_{m-3}(x) q_{m-2}(x),$$
$$\cdots\cdots\cdots$$
$$r_1(x) = f(x) - g(x) \cdot q_1(x).$$

Подставляя последовательно найденные значения $r_{m-1}(x)$, $r_{m-2}(x)$,..., $r_1(x)$ в (*), выразим $r_m(x)$ через $f(x)$ и $g(x)$:

$$r_m(x) = f(x) \cdot \varphi(x) + g(x) \cdot \psi(x),$$

но подобрать два целых числа α и β так, что:

$$a \cdot \alpha + b \cdot \beta = d.$$

В частности, если a и b взаимно простые, то можно подобрать α и β так, чтобы

$$a \cdot \alpha + b \cdot \beta = 1.$$

где $\varphi(x)$ и $\psi(x)$ — некоторые многочлены. Это равенство и показывает, что $r_m(x)$ делится на всякий общий делитель функций $f(x)$ и $g(x)$, т. е., что

$$r_m(x) = D(x).$$

Полученное соотношение можно выразить так:

если $D(x)$ есть наибольший общий делитель многочленов $f(x)$ и $g(x)$, то всегда можно найти два многочлена $\varphi(x)$ и $\psi(x)$ таких, что

$$f(x) \cdot \varphi(x) + g(x) \cdot \psi(x) = D(x).$$

В частности, если функции $f(x)$ и $g(x)$ взаимно простые, то можно подобрать $\varphi(x)$ и $\psi(x)$ так, чтобы

$$f(x)\ \varphi(x) + g(x)\ \psi(x) = 1.$$

III. Для взаимно простых чисел (многочленов) имеют место следующие теоремы:

1. Если произведение $a \cdot b$ делится на c, а a взаимно просто с c, то b делится на c.

2. Если a взаимно простое с c и b взаимно простое с c, то и их произведение $a \cdot b$ взаимно простое с c.

3. Если a делится на каждое из двух взаимно простых чисел b и c, то оно делится и на их произведение $b \cdot c$.

1. Если произведение многочленов $f(x) \cdot g(x)$ делится на $h(x)$, а $f(x)$ и $h(x)$ взаимно простые, то $g(x)$ делится на $h(x)$.

2. Если $f(x)$ взаимно простое с $h(x)$ и $g(x)$ взаимно простое с $h(x)$, то их произведение $f(x)\ g(x)$ взаимно простое с $h(x)$.

3. Если $f(x)$ делится на каждый из двух взаимно простых многочленов $g(x)$ и $h(x)$, то он делится и на их произведение $g(x) \cdot h(x)$.

Доказательство этих предложений без труда проводится, если воспользоваться соотношениями $a\alpha + b\beta = 1$ и $f(x)\,\varphi(x) + g(x)\psi(x) = 1$.

Число, которое делится только на 1 и на самого себя, называется *простым*. Простому числу в теории многочленов соответствует понятие неприводимого, не разлагающегося на множители многочлена. На понятии *неприводимости* мы остановимся ниже (§ 3, 1).

Если p — простое число, то всякое число или делится на p или взаимно простое с p.

Если произведение $a \cdot b$ делится на простое число p, то по крайней мере один из сомножителей делится на p.

Всякое (натуральное) число n может быть единственным образом разложено на произведение простых чисел. Если при этом делитель p_1 встречается α_1 раз, делитель p_2—α_2 раз и т. д., то *разложение числа n на простые множители имеет следующий вид*:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}.$$

В теории чисел вообще, и в частности в нашем вопросе, важную роль играет *число чисел взаимно простых с n и не превышающих n*; эта величина носит название числовой *функции Эйлера* и обозначается символом $\varphi(n)$. Если p—простое число, то, очевидно, $\varphi(p) = p - 1$. В общем же случае выражение для функции $\varphi(n)$ более сложное; оно может быть получено элементарными методами теории чисел. Мы выведем выражение для $\varphi(n)$ ниже (§ 2, 3), попутно с рассмотрением свойств двучленных уравнений.

§ 2. ДВУЧЛЕННЫЕ УРАВНЕНИЯ

1. Решение уравнения $x^n - a = 0$ сводится, как мы видели выше, к извлечению корня n-й степени из числа a. Задача эта была решена нами в предшествующем параграфе (§ 1, 2) с помощью тригонометрических или показательных функций. Это трансцендентное решение является, однако, недостаточным для наших дальнейших целей, ибо нас интересует возможность разрешения двучленного уравнения в квадратных радикалах; полученное же решение ответа на этот вопрос не даёт. Поэтому мы займёмся выяснением возможности решения двучленного уравнения алгебраическими средствами.

Как мы видели выше, все n корней уравнения $x^n - a = 0$ $(a \neq 0)$ различны. В том, что это уравнение не имеет кратных корней, можно было бы убедиться ещё и так. Каждый кратный корень функции является, как известно, корнем её производной. Производная же $f'(x) = nx^{n-1}$ не имеет других корней, кроме $x = 0$, не являющегося корнем функции $f(x) = x^n - a$.

Покажем, что решение уравнения $x^n - a = 0$ можно свести к нахождению одного какого-нибудь корня этого уравнения и решению уравнения $x^n - 1 = 0$.

Пусть α — какой-нибудь корень уравнения $x^n - a = 0$, а ε — любой корень уравнения $x^n - 1 = 0$, т. е. какой-нибудь корень n-й степени из единицы. Тогда $\alpha \cdot \varepsilon$ является также корнем уравнения $x^n - a = 0$. В самом деле:

$$(\alpha \cdot \varepsilon)^n = \alpha^n \cdot \varepsilon^n = a \cdot 1 = a.$$

Пусть α и β — два каких-нибудь корня уравнения $x^n - a = 0$.

Тогда $$\left(\frac{\beta}{\alpha}\right)^n = \frac{\beta^n}{a^n} = \frac{a}{a} = 1,$$

но соотношение $\left(\frac{\beta}{\alpha}\right)^n = 1$ указывает, что $\frac{\beta}{\alpha}$ есть корень из единицы:

$$\frac{\beta}{\alpha} = \varepsilon: \quad \beta = \alpha\varepsilon.$$

Если, следовательно, α есть корень двучленного уравнения $x^n - a = 0$, то любой другой его корень β мы получим умножением α на корень n-й степени из единицы; мы получим, таким образом, все корни уравнения $x^n - a = 0$ умножением одного его корня на все корни n-й степени из единицы, т. е. на все корни уравнения $x^n - 1 = 0$. Таким образом, *решение уравнения $x^n - a = 0$ сводится к нахождению одного какого-нибудь корня этого уравнения и к решению уравнения $x^n - 1 = 0$*[1]. Этим уравнением мы в дальнейшем и будем заниматься.

2. Обратимся теперь к рассмотрению свойств корней уравнения

$$x^n - 1 = 0, \tag{1}$$

[1] Это предложение может быть доказано ещё так. Полагаем $x = \alpha \cdot y$ и подставляем в данное уравнение:

$$a^n y^n - a = 0; \; ay^n - a = 0; \; a(y^n - 1) = 0; \; y^n - 1 = 0.$$

или, что то же, свойств корней n-й степени из единицы. Для наглядности будем иллюстрировать получаемые соотношения, прибегая к геометрическому истолкованию корней n-й степени из единицы как вершин правильного n-угольника, вписанного в круг единичного радиуса.

Как мы видели выше, все n корней уравнения (1) ε_0, ε_1, ε_2,..., ε_{n-1} получаются по формуле:

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = e^{\frac{2\pi ik}{n}} \quad (k = 0, 1, 2, \ldots, n-1). \qquad (2)$$

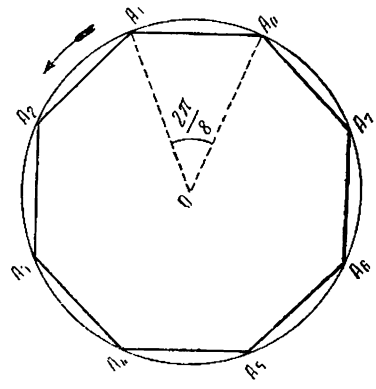
Отсюда легко видеть, что при любом k

$$\varepsilon_k = (\varepsilon_1)^k. \qquad (3)$$

Таким образом, все корни n-й степени из единицы могут быть получены как последовательные степени *первого* корня $\varepsilon_1 = e^{\frac{2\pi i}{n}}$ (корень $\varepsilon_0 = 1$, общий для всех уравнений $x^n - 1 = 0$, представляет тривиальное решение):

ε_1, ε_1^2, ε_1^3,..., $\varepsilon_1^n = 1$,

причём, заметим, в этом случае сохраняется расположение корней в порядке возрастания их аргументов; это расположение будем называть натуральным.



Черт 3.

В геометрическом истолковании умножение на $e^{\frac{2\pi i}{n}}$ есть поворот [1] на угол $\frac{2\pi}{n}$. Соотношение (3) допускает, таким образом, следующую совершенно очевидную геометрическую интерпретацию: все вершины правильного n-угольника могут быть получены из первой его вершины (A_1) путём последовательных поворотов на угол $\frac{2\pi}{n}$ (черт. 3; $n = 8$).

[1] Умножение на комплексное число $z = \rho(\cos\varphi + i\sin\varphi) = \rho e^{\varphi i}$ равносильно, как известно, растяжению модуля в ρ раз и повороту на угол φ.

Покажем следующее свойство корней уравнения (1). Если ε и ε'—корни n-й степени из единицы, то их произведение $\varepsilon \cdot \varepsilon'$, частное $\frac{\varepsilon}{\varepsilon'}$, а также любая целая степень ε^k представляют собой тоже корни n-й степени из единицы.

В самом деле, по условию $\varepsilon^n = 1$ и $\varepsilon'^n = 1$; тогда:

$$(\varepsilon \cdot \varepsilon')^n = \varepsilon^n \cdot \varepsilon'^n = 1 \cdot 1 = 1$$

$$\left(\frac{\varepsilon}{\varepsilon'}\right)^n = \frac{\varepsilon^n}{\varepsilon'^n} = \frac{1}{1} = 1$$

$$(\varepsilon^k)^n = \varepsilon^{kn} = (\varepsilon^n)^k = 1^k = 1.$$

Таким образом, предложение доказано. Геометрически оно иллюстрируется так: при повороте какой-нибудь вершины правильного n-угольника (в положительном или отрицательном направлении) на угол, соответствующий другой (или той же самой) вершине этого n-угольника, мы получим опять некоторую вершину этого же многоугольника.

Пусть ε — какой-нибудь корень n-й степени из единицы. По доказанному, в бесконечной последовательности

$$\varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^k \ldots$$

каждый член является корнем n-й степени из единицы. В этой последовательности содержится, в частности, и член, равный 1. Таким будет во всяком случае ε^n, но может оказаться равным единице и какой-нибудь из предшествующих членов. Пусть m — наименьший показатель, при котором

$$\varepsilon^m = 1.$$

Мы скажем тогда, что корень ε *принадлежит показателю* m.

Показатель m, *к которому принадлежит какой-нибудь корень* n-*й степени из единицы, должен быть делителем числа* n.

Докажем это. Пусть ε — принадлежащий показателю m корень n-й степени из единицы.

Допустим, что $n = mq + r$ $(0 \leqslant r < m)$.

Тогда $$\varepsilon^n = \varepsilon^{mq+r} = (\varepsilon^m)^q \varepsilon^r = \varepsilon^r,$$

т. е. $\varepsilon^r = 1$. И так как $r < m$, то, если бы r было отлично от нуля, это противоречило бы тому условию, что ε принадлежит показателю m. Итак, $r = 0$ и, следовательно, $n = m \cdot q$, т. е. m есть делитель n.

Если корень ε уравнения $x^n - 1 = 0$ принадлежит показателю n, т. е. является корнем данного уравнения, но не удовлетворяет никакому уравнению $x^m - 1 = 0$,

степени, меньшей, чем n, то такой корень называется *первообразным* корнем уравнения $x^n - 1 = 0$, или, просто, первообразным корнем n-й степени. Таким корнем наверно является первый корень

$$\varepsilon_1 = e^{\frac{2\pi i}{n}},$$

так как $\varepsilon_1^n = 1$, но $\varepsilon_1^k = e^{\frac{2\pi ik}{n}} \neq 1$ (при $k < n$). Но, кроме ε_1, существуют ещё другие первообразные корни.

Вершину n-угольника, соответствующую первообразному корню, мы назовём *собственной* вершиной. Собственная вершина n-угольника не принадлежит никакому многоугольнику с меньшим, чем n, числом вершин. Такой вершиной наверно является первая (после начальной) вершина n-угольника.

Основным свойством первообразных корней является следующее:

если r есть какой-либо первообразный корень уравнения $x^n - 1 = 0$, то ряд из n последовательных его степеней

$$r, r^2, \ldots, r^{n-1}, r^n = 1 \qquad (4)$$

представляет все n корней n-й степени из единицы (в отличном, вообще говоря, от натурального расположения порядке).

Мы видели, что этим свойством обладал первый корень $\varepsilon_1 = e^{\frac{2\pi i}{n}}$. Покажем справедливость этого для всякого первообразного корня. В самом деле, каждый член написанного ряда есть корень данного уравнения, и все они между собой различны. Действительно, если предположить, что при $k > l$ $r^k = r^l$, то $r^{k-l} = 1$, а так как $k - l < n$, то r не был бы первообразным корнем, что противоречит условию.

Отмеченное свойство первообразных корней показывает, что для решения двучленного уравнения $x^n - 1 = 0$ достаточно найти только один его первообразный корень; все остальные корни будут получены из найденного первообразного корня путём последовательного возвышения его в степень.

Если корень не является первообразным для уравнения $x^n - 1 = 0$, то он принадлежит к некоторому показателю m (m — делитель n) и, следовательно, будет первообразным для уравнения $x^m - 1 = 0$ низшей степени.

Как узнать, является ли данный корень первообразным и если нет, то к какому показателю он принадлежит (первообразным корнем какой степени он является).

Ответ даёт следующая теорема.

Пусть r — какой-либо первообразный корень уравнения $x^n - 1 = 0$; тогда, как мы видели, ряд (4) представляет все корни этого уравнения. Теорема утверждает, что *корень* r^k *принадлежит к показателю* $\frac{n}{d}$, *где* d *— есть наибольший общий делитель чисел* k и n. Докажем это.

Пусть r^k принадлежит показателю m. Это значит, что

$$(r^k)^m = r^{km} = 1,$$

причём m должно быть наименьшим числом, при котором это соотношение имеет место.

Так как r есть первообразный корень n-й степени, то из равенства $r^{km} = 1$ следует, что km должно быть кратно n:

$$km = nq.$$

Если d есть наибольший общий делитель k и n, то

$$k = k_1 d \text{ и } n = n_1 d,$$

где k_1 и n_1 взаимно простые. Подставляя k и n в написанное соотношение и сокращая на d, получим:

$$k_1 m = n_1 q.$$

Отсюда следует, что $k_1 m$ должно делиться на n_1 и так как k_1 и n_1 взаимно простые, то m должно делиться на n_1. Наименьшее возможное для этого значение m есть $m = n_1$. Покажем, что $(r^k)^{n_1}$ действительно равно единице. В самом деле:

$$(r^k)^{n_1} = r^{kn_1} = r^{k_1 dn_1} = r^{k_1 n} = (r^n)^{k_1} = 1.$$

И так как, по доказанному, n_1 есть наименьшее значение для m, то r^k принадлежит показателю n_1, но

$$n_1 = \frac{n}{d}.$$

Таким образом, теорема доказана.

Отсюда вытекает такое следствие.

Для того чтобы r^k *было первообразным корнем* n*-й степени, необходимо и достаточно, чтобы* k *было взаимно простым с* n.

Действительно, если $(k, n) = 1$, то $d = 1$ и r^k принадлежит показателю n, т. е. является первообразным корнем. Если же $(k, n) = d \neq 1$, то $\frac{n}{d} < n$ и r^k принадлежит

показателю, меньшему, чем n, и первообразным корнем уже не является.

Замечание. Доказанная теорема и следствие из неё не зависят от того, какой первообразный корень принят за основание ряда (4); данный корень может принадлежать только к одному какому-нибудь показателю, независимо от того первообразного корня, при помощи которого он выражен. Показать это можно так. Пусть ρ — какой-нибудь другой первообразный корень данного уравнения; тогда

$$\rho,\ \rho^2,\ldots,\ \rho^{n-1},\ \rho^n$$

также представляют собой все корни нашего уравнения. Как выразится в этом ряду корень r^k?

Так как r есть первообразный корень, $r = \rho^s$, где s взаимно простое с n. Отсюда

$$r^k = (\rho^s)^k = \rho^{sk}.$$

По доказанной теореме корень ρ^{sk} должен принадлежать показателю $\frac{n}{d_1}$, где $d_1 = (sk, n)$. Но наибольший общий делитель чисел sk и n и k и n один и тот же, так как s взаимно простое с n. Поэтому $d_1 = d$. Получаем, следовательно, тот же самый показатель.

В частности, если за первообразный корень принят «первый» корень n-й степени $\varepsilon_1 = e^{\frac{2\pi i}{n}}$ и все корни

$$\varepsilon_0 = 1,\ \varepsilon_1,\ \varepsilon_2,\ldots,\ \varepsilon_k,\ldots,\ \varepsilon_{n-1}\ \left(\varepsilon_\kappa = \varepsilon_1^k = e^{\frac{2\pi i k}{n}}\right)$$

расположены, следовательно, в натуральном порядке, то можно сказать, что k-й по порядку корень ε_k принадлежит к показателю $\frac{n}{d}$, где $d = (n, k)$; ε_k является первообразным в том случае, если индекс k взаимно простой с n.

Из сказанного следует, что первообразных корней уравнения $x^n - 1 = 0$ существует столько, сколько есть чисел взаимно простых с n (и не превосходящих n). И в частности, если n — простое, то первообразных корней будет $n - 1$.

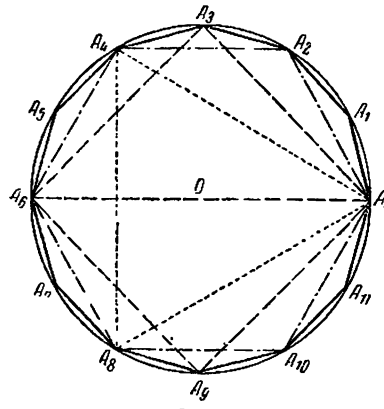
Пример. $x^{12} - 1 = 0$. Из 12 корней этого уравнения $\varepsilon_0 = 1,\ \varepsilon_1,\ \varepsilon_2,\ \varepsilon_3,\ \varepsilon_4,\ \varepsilon_5,\ \varepsilon_6,\ \varepsilon_7,\ \varepsilon_8,\ \varepsilon_9,\ \varepsilon_{10},\ \varepsilon_{11}$ первообразными будут корни, индексы которых взаимно простые с 12:

$$\varepsilon_1,\ \varepsilon_5,\ \varepsilon_7,\ \varepsilon_{11}.$$

Делители 12 следующие: 6, 4, 3, 2, 1.

Показателю 6 будут принадлежать (т. е. будут первообразными для уравнения $x^6 - 1 = 0$) корни с индексами, имеющими с 12 наибольший общий делитель, определяемый из соотношения $\frac{12}{d} = 6$, т. е. имеющими с 12 наибольший общий делитель $d = 2$; таковы корни

$$\varepsilon_2, \ \varepsilon_{10}.$$



Черт. 4.

Далее так же устанавливаем, что показателю 4 принадлежат корни ε_3 и ε_9, показателю 3 — корни ε_4 и ε_8 и показателю 2 — корень ε_6. Корень $\varepsilon_0 = 1$, общий для всех уравнений $x^n - 1 = 0$, можно считать первообразным для уравнения $x - 1 = 0$ и, следовательно, принадлежащим показателю 1.

Геометрически разобранный пример интерпретируется так. В правильном двенадцатиугольнике (см. чертеж 4) вершины:

A_1, A_5, A_7, A_{11} — собственные для двенадцатиугольника;
A_2, A_{10} — принадлежат шестиугольнику;
A_3, A_9 — принадлежат четырёхугольнику;
A_4, A_8 — принадлежат треугольнику;
A_6 — есть точка деления окружности пополам и
A_0 — начальная точка всех рассматриваемых многоугольников.

3. Мы видели, что число первообразных корней n-й степени равно числу чисел, меньших n и взаимно простых с n. Величина эта, как мы указывали выше (§ 1, 4), носит название *функции Эйлера* и обозначается символом $\varphi(n)$.

Итак, число первообразных корней уравнения $x^n - 1 = 0$ равно $\varphi(n)$. Мы ставим сейчас своей задачей вывести выражение для этой числовой функции.

Заметим прежде всего следующее: если r и s — числа взаимно простые, то уравнения $x^r - 1 = 0$ и $x^s - 1 = 0$ не имеют общих корней, кроме $x = 1$. В самом деле, пусть α — общий корень этих уравнений, тогда

$$\alpha^r = 1 \text{ и } \alpha^s = 1.$$

Так как $(r, s) = 1$, то можно подобрать такие целые числа ρ и σ, чтобы

$$r \cdot \rho + s \cdot \sigma = 1,$$

а тогда

$$\alpha = \alpha^{r \cdot \rho + s \cdot \sigma} = (\alpha^r)^\rho \cdot (\alpha^s)^\sigma = 1,$$

т. е. α необходимо равно единице.

Возвращаясь к функции $\varphi(n)$, мы в первую очередь покажем следующее её свойство: если r и s взаимно простые, то

$$\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s). \tag{5}$$

Чтобы вывести это соотношение, рассмотрим соответствующие двучленные уравнения:

$$x^{rs} - 1 = 0, \; x^r - 1 = 0, \; x^s - 1 = 0.$$

Последние два из них, как мы видели, не имеют общих корней (кроме $x = 1$).

Пусть α — первообразный корень уравнения $x^r - 1 = 0$, а β — первообразный корень уравнения $x^s - 1 = 0$. Покажем, что их произведение $\alpha \cdot \beta$ является первообразным для уравнения $x^{rs} - 1 = 0$. Прежде всего убеждаемся, что $\alpha\beta$ есть корень этого уравнения:

$$(\alpha\beta)^{rs} = \alpha^{rs} \cdot \beta^{rs} = (\alpha^r)^s \cdot (\beta^s)^r = 1.$$

Пусть $\alpha\beta$ принадлежит показателю m:

$$(\alpha\beta)^m = 1.$$

Отсюда

$$\alpha^m = \beta^{-m}.$$

α^m есть корень уравнения $x^r - 1 = 0$, β^{-m} — корень уравнения $x^s - 1 = 0$, и так как эти уравнения не имеют общих корней, кроме единицы, то

$$\alpha^m = \beta^{-m} = 1.$$

Так как α есть первообразный корень уравнения $x^r - 1 = 0$, то из $\alpha^m = 1$ следует, что m должно быть кратно r, точно так же из равенства $\beta^{-m} = 1$ следует, что m должно делиться на s, и так как r и s взаимно простые, то m должно делиться на их произведение $r \cdot s$. Поэтому наименьшее значение для m есть $r \cdot s$. Корень $\alpha\beta$ принадлежит, таким образом, показателю rs, он есть первообразный корень уравнения $x^{rs} - 1 = 0$. Так как уравнение $x^r - 1 = 0$ имеет $\varphi(r)$ первообразных корней, а уравнение $x^s - 1 = 0$ $\varphi(s)$ первообразных корней и все эти корни между собой различны, то отсюда следует, что все

$\varphi(r) \cdot \varphi(s)$ произведений вида $\alpha\beta$ являются первообразными корнями уравнения $x^{rs} - 1 = 0$. Покажем, что никаких других первообразных корней это уравнение не имеет.

Пусть γ — первообразный корень уравнения $x^{rs} - 1 = 0$. Так как $(r, s) = 1$, то можно подобрать два таких целых числа ρ и σ, что

$$r \cdot \rho + s \cdot \sigma = 1$$

(заметим при этом, что ρ и σ, а также r и σ должны быть тоже взаимно простыми; в противном случае единица должна была бы делиться на их общий делитель, что невозможно). Тогда

$$\gamma = \gamma^{r\rho+s\sigma} = \gamma^{r\rho} \cdot \gamma^{s\sigma}.$$

$\gamma^{s\sigma}$ есть корень уравнения $x^r - 1 = 0$, так как $(\gamma^{s\sigma})^r = \gamma^{s\sigma r} = (\gamma^{sr})^\sigma = 1$; покажем, что $\gamma^{s\sigma}$ есть первообразный корень этого уравнения. Пусть $\gamma^{s\sigma}$ принадлежит показателю m:

$$(\gamma^{s\sigma})^m = \gamma^{s\sigma m} = 1.$$

Так как γ принадлежит показателю rs, то $s\sigma m$ должно быть кратно rs, а, следовательно, σm должно быть кратно r; а так как σ и r взаимно простые, то m должно делиться на r. Наименьшее значение для m при этом условии $m = r$; таким образом, $\gamma^{s\sigma}$ есть первообразный корень уравнения $x^r - 1 = 0$. Совершенно аналогично доказывается, что $\gamma^{r\rho}$ есть первообразный корень уравнения $x^s - 1 = 0$. Итак, всякий первообразный корень уравнения $x^{rs} - 1 = 0$ есть произведение первообразных корней уравнений $x^r - 1 = 0$ и $x^s - 1 = 0$.

Так как, с одной стороны, число первообразных корней уравнения $x^{rs} - 1 = 0$ равно числу чисел взаимно простых с rs и не превосходящих rs, т. е. равно $\varphi(rs)$, и так как, с другой стороны, все первообразные корни этого уравнения представятся в виде $\varphi(r) \cdot \varphi(s)$ произведений вида $\alpha \cdot \beta$ (где α и β — первообразные корни уравнений $x^r - 1 = 0$ и $x^s - 1 = 0$), то отсюда и вытекает, что

$$\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s).$$

Теорема эта индуктивно распространяется на любое число сомножителей. Пусть теорема верна для $n - 1$ попарно взаимно простых сомножителей:

$$\varphi(q_1 \cdot q_2 \dots q_{n-1}) = \varphi(q_1) \cdot \varphi(q_2) \dots \varphi(q_{n-1}).$$

Докажем, что в таком случае она имеет место и для n сомножителей. Так как $q_1 \cdot q_2 \dots q_{n-1}$ и q_n взаимно простые, то

$$\varphi(q_1 q_2 \dots q_{n-1} q_n) = \varphi(q_1 q_2 \dots q_{n-1}) \cdot \varphi(q_n),$$

откуда. принимая во внимание допущение, получаем:

$$\varphi(q_1 q_2 \dots q_n) = \varphi(q_1) \cdot \varphi(q_2) \dots \varphi(q_n). \qquad (6)$$

Теорема доказана.

Для p простого $\varphi(p) = p - 1$. Найдём функцию Эйлера для того случая, когда n есть степень простого числа: $n = p^\alpha$.

В ряду чисел от 1 до p^α:

$$1, 2, 3, \dots, p^\alpha$$

общие делители с p^α имеют числа, кратные p:

$$p, 2p, 3p, \dots, p^{\alpha-1} \cdot p;$$

таких чисел имеется $p^{\alpha-1}$. Остальные же числа взаимно простые с p^α. Их будет $p^\alpha - p^{\alpha-1}$. Таким образом,

$$\varphi(p^\alpha) = p^{\alpha-1}(p - 1). \qquad (7)$$

А теперь нетрудно получить выражение для функции $\varphi(n)$ в общем случае. Пусть $n = p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$.

Так как все сомножители $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$ — числа попарно взаимно простые, то, применяя доказанную выше теорему, получаем:

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k}) =$$
$$= p_1^{\alpha_1-1}(p_1 - 1) \cdot p_2^{\alpha_2-1}(p_2 - 1) \dots p_k^{\alpha_k-1}(p_k - 1).$$

Итак, функция Эйлера $\varphi(n)$, дающая число чисел, взаимно простых с n и не превосходящих n, или число первообразных корней уравнения $x^n - 1 = 0$, выражается следующим образом:

$$\varphi(n) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1}(p_1 - 1)(p_2 - 1) \dots (p_k - 1). \qquad (8)$$

Например: 1) $n = 12 = 2^2 \cdot 3$; $\varphi(12) = 2 \cdot (2-1)(3-1) = 4$

2) $n = 54 = 2 \cdot 3^3$; $\varphi(54) = 3^2 \cdot (2-1)(3-1) = 18$.

Заметим ещё следующее свойство функции $\varphi(n)$. Если взять все делители числа n (включая само n и единицу):

$$1, d_1, d_2, \dots, d_k, n$$

и принять $\varphi(1) = 1$, то сумма

$$\varphi(1) + \varphi(d_1) + \varphi(d_2) + \dots + \varphi(d_k) + \varphi(n) = n.$$

Это следует из того, что

1) каждый из n корней уравнения $x^n - 1 = 0$ является перво-

образным для одного (и только одного) из уравнений $x^d - 1 = 0$ (где $d = 1, d_1, d_2, \ldots, d_k, n$);

2) что каждый корень уравнения $x^d - 1 = 0$ есть также корень уравнения $x^{d'} - 1 = 0$ и что

3) число первообразных корней уравнения $x^d - 1 = 0$ равно $\varphi(d)$.

Так, например, для $n = 12$ имеет место соотношение:

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12,$$

в чем мы убедились непосредственно, разбивая в рассмотренном выше примере уравнения $x^{12} - 1 = 0$ 12 его корней на группы по их «первообразной» принадлежности.

§ 3. О РАЗРЕШИМОСТИ УРАВНЕНИЙ В КВАДРАТНЫХ РАДИКАЛАХ

1. Поставленная нами задача о возможности построения циркулем и линейкой правильных многоугольников равносильна, как мы видели (§ 1, 3), вопросу о разрешимости двучленного уравнения в квадратных радикалах. Оставляя на время двучленные уравнения в стороне, мы поставим вопрос в более общей форме — о возможности решения в квадратных радикалах любого алгебраического уравнения. При исследовании этого вопроса (и более общего — о разрешимости уравнения в радикалах вообще, не только в квадратных) существенную роль играют понятия числового поля и неприводимого многочлена.

Полем в алгебре называется множество чисел, обладающих тем свойством, что результат рациональной операции (за исключением деления на нуль) над числами (элементами) этого множества есть опять элемент того же множества. Таким образом, действия сложения, вычитания, умножения и деления (за исключением деления на нуль) над элементами поля, как говорят, не выводят за пределы этого поля. Множество R всех рациональных чисел есть поле. Полем будет также, например, множество всех чисел вида $a + b\sqrt{2}$, где a и b — рациональные числа, так как результат сложения, вычитания, умножения и деления над числами этого вида есть число того же вида:

$$(a + b\sqrt{2}) \pm (a_1 + b_1\sqrt{2}) = (a \pm a_1) + (b \pm b_1)\sqrt{2};$$

$$(a + b\sqrt{2}) \cdot (a_1 + b_1\sqrt{2}) = (aa_1 + 2bb_1) + (ab_1 + a_1b)\sqrt{2};$$

$$\frac{a + b\sqrt{2}}{a_1 + b_1\sqrt{2}} = \frac{(a + b\sqrt{2})(a_1 - b_1\sqrt{2})}{(a_1 + b_1\sqrt{2})(a_1 - b_1\sqrt{2})} = \frac{aa_1 - 2bb_1}{a_1^2 - 2b_1^2} + \frac{a_1b - ab_1}{a_1^2 - 2b_1^2}\sqrt{2}.$$

Нуль сам по себе образует поле. Всякое иное числовое поле P содержит в себе поле R как часть, так как, содержа какой-нибудь элемент α ($\neq 0$), оно должно содержать и $\frac{\alpha}{\alpha} = 1$, $1 + 1 = 2$ и т. д.

Если наряду с полем P мы рассматриваем новое поле P_1, такое, что все элементы P принадлежат полю P_1, но которое, кроме них, содержит еще и другие элементы, то поле P_1 называется *расширением* поля P.

Если к полю P присоединён новый элемент α, то для того чтобы новая область продолжала оставаться полем, необходимо наряду с числом α присоединить и все те числа, которые получаются в результате рациональных действий над элементами P и числом α. При этих обстоятельствах мы скажем, что новое поле (расширение) P_1 получено путём *приобщения* элемента α к полю P, что записывается так:

$$P_1 = P(\alpha).$$

Так, например, если к полю R рациональных чисел приобщить иррациональное число $\sqrt{2}$, то расширение $R\ (\sqrt{2})$ будет состоять из всех чисел вида $a + b\sqrt{2}$, где a и b — рациональные числа.

При изучении свойств целых рациональных функций (многочленов) существенное значение имеет вопрос о той числовой области, к которой принадлежат коэффициенты данных функций. Если коэффициенты многочлена принадлежат полю P, то говорят, что многочлен принадлежит полю P, или дан над полем P.

Нетрудно видеть, что наибольший общий делитель $D(x)$ многочленов $f(x)$ и $g(x)$, принадлежащих полю P, сам тоже принадлежит полю P, ибо коэффициенты его находятся путём рациональных действий над коэффициентами $f(x)$ и $g(x)$.

Выше (§ 1, 4) мы проследили аналогию, существующую между многочленами и целыми числами, и тогда же отметили, что понятию простого, не разлагающегося на сомножители числа соответствует понятие *неприводимой* функции.

Если целая рациональная функция $f(x)$ может быть представлена в виде произведения двух каких-либо многочленов $g(x)$ и $h(x)$:

$$f(x) = g(x) \cdot h(x),$$

из которых ни один не сводится к постоянному, то мы говорим, что $f(x)$ разлагается на множители, или что она приводима; в противном случае функция называется неприво-

димой. Но при этом понятие приводимости или неприводимости не будет иметь определённого содержания, если не указать той числовой области, к которой должны принадлежать коэффициенты функций $g(x)$ и $h(x)$. Так, функция $f(x) = x^2 - 2$ неприводима во множестве рациональных чисел, но разлагается на множители $[x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})]$ в поле действительных чисел и даже в поле $R[\sqrt{2}]$.

Если целая рациональная функция $f(x)$ может быть разложена на множители (не сводящиеся к постоянному), коэффициенты которых принадлежат полю P, то функция называется *приводимой в поле* P; в противном случае — *неприводимой в поле* P.

Неприводимые (в поле P) функции обладают рядом важных свойств. Пусть $f(x)$ и $\varphi(x)$ — целые рациональные функции (многочлены) в поле P.

1) Если $f(x)$ — неприводима, а $\varphi(x)$ — любая функция, то либо $\varphi(x)$ делится на $f(x)$, либо $\varphi(x)$ и $f(x)$ взаимно простые.

Это следует из того, что $f(x)$ и $\varphi(x)$ не могут иметь наибольшего общего делителя, отличного от постоянной или от $f(x)$ (так как $f(x)$ неприводима).

2) Если уравнение $\varphi(x) = 0$ имеет общий корень с неприводимым уравнением $f(x) = 0$[1], то все корни уравнения $f(x) = 0$ удовлетворяют уравнению $\varphi(x) = 0$ и $\varphi(x)$ делится на $f(x)$.

В самом деле, общий корень функций $f(x)$ и $\varphi(x)$ является корнем их наибольшего общего делителя, который поэтому наверно отличен от постоянной, а потому функции $f(x)$ и $\varphi(x)$ не могут быть взаимно простыми, и, следовательно, по 1) $\varphi(x)$ делится на $f(x)$; откуда и следует, что все корни уравнения $f(x)=0$ удовлетворяют уравнению $\varphi(x)=0$.

Поэтому, если какой-либо корень α неприводимого уравнения $f(x) = 0$ не является корнем уравнения $\varphi(x)= 0$, то функции $f(x)$ и $\varphi(x)$ взаимно простые.

3) Неприводимое уравнение $f(x) = 0$ не может иметь общих корней с уравнением $\varphi(x) = 0$ низшей степени [2].

[1] Речь идёт, конечно, о корне, не принадлежащем полю P, ибо неприводимая в поле P функция не может иметь в нем корней.

[2] Отсюда вытекает, что неприводимое уравнение не может иметь кратных корней, так как каждый кратный корень функции $f(x)$ является вместе с тем корнем её производной $f'(x)$; уравнение же $f'(x) = 0$ — низшей степени, чем $f(x) = 0$.

Это вытекает из 1), так как в рассматриваемом случае $\varphi(x)$ не может делиться на $f(x)$.

4) Два различных неприводимых уравнения $f(x) = 0$ и $\varphi(x) = 0$ не могут иметь общих корней.

В самом деле, если бы $f(x)$ и $\varphi(x)$ имели общий корень, то $f(x)$ должна была бы делиться на $\varphi(x)$ [или, наоборот, $\varphi(x)$ на $f(x)$], но это невозможно, так как $f(x)$ неприводима.

2. Нас будет интересовать вопрос о разрешимости алгебраического уравнения $f(x) = 0$ в радикалах и, в частности, радикалах квадратных. Решить уравнение в радикалах — это значит выразить при помощи элементарных алгебраических действий (сложения, вычитания, умножения, деления, возведения в степень и извлечения корня) корни данного уравнения через его коэффициенты. Однако эта задача далеко не всегда разрешима (уравнения выше 4-й степени в общем виде не решаются в радикалах). Поэтому при исследовании алгебраического решения уравнений мы становимся на несколько иную, более общую точку зрения: *мы рассматриваем решение уравнения как расширение первоначального поля* P (к которому принадлежат коэффициенты данного уравнения) *путём приобщения к нему* новых элементов — *корней этого уравнения* (или же других величин, через которые корни данного уравнения выражаются рационально).

С этой точки зрения решение, например, квадратного уравнения $x^2 + px + q = 0$ с рациональными коэффициентами есть расширение поля рациональных чисел R путем приобщения к R одного из корней $x_{1,2} = -\frac{p}{2} \pm \pm \sqrt{\frac{p^2}{4} - q}$ данного уравнения, что равносильно построению поля $R\left[\sqrt{\frac{p^2}{4} - q}\right]$.

Указанная точка зрения на решение алгебраических уравнений имеет следующее преимущество. Хотя построить новое поле (расширение) в явном виде, подобно тому как это мы только что сделали для квадратного уравнения, вообще говоря, нельзя (в случае уравнений 5-й и высших степеней), тем не менее оказывается возможным установить свойства, которые должно иметь расширение, и отсюда уже сделать те или иные заключения о характере корней уравнения. К рассмотрению расширений поля мы сейчас и переходим.

Мы будем исходить из поля R рациональных чисел Пусть α — корень неприводимого в R алгебраического уравнения n-й степени:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \qquad (1)$$

с рациональными коэффициентами: $f(\alpha) = 0$. Число (элемент) α называется в этом случае *алгебраическим* [1]; n — есть *степень* α относительно поля R. Неприводимое уравнение, которому удовлетворяет данный алгебраический элемент, определяется однозначно, так как не может в данном поле существовать двух неприводимых в нем функций, имеющих общий корень.

Построим поле R_1 — расширение поля R путём приобщения к нему алгебраического элемента α:

$$R_1 = R[\alpha]. \qquad (2)$$

Элемент α назовём *образующим* или *примитивным* элементом поля R_1.

Поле R_1 наряду с рациональными числами содержит также все те числа, которые получаются путём применения рациональных операций к элементам поля R и числу α; таким образом, элементы поля R_1 представляют собой всевозможные рациональные функции (с рациональными коэффициентами) от α. Общий вид любого элемента γ поля R_1 следующий:

$$\gamma = \frac{\varphi(\alpha)}{\psi(\alpha)}, \qquad (3)$$

где $\varphi(x)$ и $\psi(x)$ — целые рациональные функции в поле R (т. е. многочлены с рациональными коэффициентами). Итак, мы видели, что любой элемент γ алгебраического расширения R_1 (расширение поля при помощи алгебраического элемента мы называем *алгебраическим* расширением) есть рациональная функция его примитивного элемента γ. Мы докажем следующее свойство этого расширения.

Если образующий элемент α расширения $R[\alpha]$ — n-й степени (относительно R), то всякий элемент этого поля представляет собой *целую* рациональную функцию от α (с рациональными коэффициентами) и притом не выше $(n-1)$-й *степени*.

[1] Число, не являющееся корнем никакого алгебраического уравнения вида (1), называется *трансцендентным*. Таковыми, как доказывается, являются числа e и π. Число i есть алгебраическое, так как служит корнем уравнения $x^2 + 1 = 0$.

Прежде всего заметим, что в равенстве (3) знаменатель $\psi(\alpha) \neq 0$. С другой стороны, по условию $f(\alpha) = 0$. Так как корень α неприводимой функции $f(x)$ не является корнем функции $\psi(x)$, то эти функции взаимно простые. А потому в поле R можно найти два многочлена $F(x)$ и $\Psi(x)$ таких, что

$$f(x) \cdot F(x) + \psi(x) \cdot \Psi(x) = 1. \qquad (4)$$

Полагая в этом равенстве $x = \alpha$, найдём, что

$$\psi(\alpha) \cdot \Psi(\alpha) = 1.$$

Умножая в (3) числитель и знаменатель на $\Psi(\alpha)$, получим:

$$\gamma = \frac{\varphi(\alpha)}{\psi(\alpha)} = \frac{\varphi(\alpha)\cdot\Psi(\alpha)}{\psi(\alpha)\cdot\Psi(\alpha)} = \varphi(\alpha) \cdot \Psi(\alpha) = g(\alpha). \qquad (5)$$

Итак, показано, что γ — целая рациональная функция от α (в поле R). Если бы степень $g(x)$ оказалась выше $(n-1)$-й, то, деля $g(x)$ на $f(x)$, мы получили бы:

$$g(x) = f(x) \cdot q(x) + r(x) \qquad (6)$$

и, полагая здесь $x = \alpha$, имели бы

$$g(\alpha) = r(\alpha),$$

где степень $r(x)$ не выше $(n-1)$-й.

Предложение, таким образом, доказано полностью. Всякий элемент поля $R[\alpha]$ может быть, следовательно, представлен в виде целой рациональной функции $(n-1)$-й степени образующего элемента α:

$$\gamma = b_1\alpha^{n-1} + b_2\alpha^{n-2} + \ldots + b_{n-1}\alpha + b_n \ , \qquad (7)$$

где b_i принадлежат полю R[1]. Этому факту, характеризующему строение расширения $R(\alpha)$, мы дадим несколько иную формулировку.

Если некоторое множество элементов Z обладает тем свойством, что в нём можно указать m *линейно-независимых* (относительно поля P) элементов[2]:

$$z_1, z_2, \ldots, z_m$$

---

[1] Нетрудно показать, что такое представление является единственным.

[2] m элементов $z_1, z_2, \ldots, z_m$ называются *линейно-независимыми* (относительно P), если (в P) нельзя подобрать m чисел k_i, из которых не все равны нулю и таких, чтобы выполнялось соотношение

$$k_1z_1 + k_2z_2 + \ldots + k_nz_n = 0.$$

В противном случае эти элементы называются линейно-зависимыми.

таких, что любой элемент z из Z может быть представлен в виде их линейной однородной функции (с коэффициентами из P):

$$z = c_1 z_1 + c_2 z_2 + \ldots + c_m z_m,$$

то такое множество элементов называется *линейным многообразием* порядка m (относительно P); числа z_i образуют *базис* этого линейного многообразия.

Возвращаясь к алгебраическому расширению $R[\alpha]$, мы видим из (7), что элементы

$$\alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha, \alpha^0 = 1 \qquad (8)$$

играют в нём роль базиса: каждый элемент γ поля $R[\alpha]$ представляет линейную однородную функцию (с рациональными коэффициентами) элементов (8). Кроме того, элементы (8) — линейно-независимы в R, так как в случае существования между ними линейной зависимости

$$C_1\alpha^{n-1} + C_2\alpha^{n-2} + \ldots + C_{n-1}\alpha + C_n = 0$$

α удовлетворяло бы уравнению $(n-1)$-й степени, чего быть не может, так как α есть корень неприводимого в R уравнения n-й степени.

Таким образом, алгебраическое расширение $R_1 = R[\alpha]$ полученное путём приобщения к полю R алгебраического элемента n-й степени, представляет собой (относительно R) линейное многообразие n-го порядка[1].

---

[1] Не следует думать, что примитивный элемент α, при помощи которого построено поле $R_1 = R[\alpha]$, является в нём исключительным элементом. Можно показать, что такую же роль может играть любой элемент β из этого поля, если только он степени n относительно поля R, т. е. если он удовлетворяет неприводимому в R уравнению n-й степени (иначе: если $1, \beta, \beta^2, \ldots, \beta^n$ линейно-зависимы, а $1, \beta, \beta^2, \ldots, \beta^{n-1}$ линейно-независимы в R). Построенное путём приобщения элемента β поле $R[\beta]$ будет совпадать с $R[\alpha]$. Поясним это на примере.

Пусть $\alpha = \sqrt[3]{2}$ — корень неприводимого в R уравнения 3-й степени $x^3 - 2 = 0$. Поле $R[\sqrt[3]{2}]$ представляет собой линейное многообразие 3-го порядка, базисом которого служат элементы $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$, и, следовательно, есть совокупность чисел вида:

$$p + q\sqrt[3]{2} + r\sqrt[3]{4},$$

где p, q и r — рациональные числа. Возьмем в поле $R[\sqrt[3]{2}]$ элемент $\beta = 1 + \sqrt[3]{4}$. Степень этого элемента относительно R равна 3, так как он служит корнем неприводимого в R уравнения $(x-1)^3 - 4 = 0$.

Мы скажем, что степень построенного нами расширения R_1 относительно R есть n, и запишем это так:

$$\{R_1 : R\} = n. \tag{9}$$

Процесс алгебраического расширения поля можно продолжать далее. Рассматриваем в поле $R_1 = R[\alpha]$ неприводимую в нём целую рациональную функцию $g(x)$ степени, положим, m. Пусть β есть корень этой функции:

$$g(\beta) = 0.$$

Элемент β приобщаем к полю R_1. Строим, следовательно, новое поле

$$R_2 = R_1[\beta] = R[\alpha, \beta],$$

элементы которого будут всевозможные рациональные функции от β (с коэффициентами из R_1). По доказанному выше, расширение $R_2 = R_1[\beta]$ представляет собой линейное многообразие m-го порядка относительно R_1; его базисом являются m чисел:

$$\beta^{m-1},\ \beta^{m-2},\ \ldots,\ \beta,\ 1.$$

Степень расширения R_2 относительно R_1 есть, следовательно, m:

$$\{R_2 : R_1\} = m.$$

Основная теорема, которую мы хотим доказать, заключается в том, что поле $R_2 = R_1[\beta] = R[\alpha, \beta]$ является линейным многообразием также относительно R и что порядок его относительно R равен произведению $m \cdot n$; нужно доказать, следовательно, что

$$\{R_2 : R\} = m \cdot n.$$

Возьмём произвольный элемент δ поля R_2. Он выразится, по доказанному выше, в виде целой рациональной функции $(m-1)$-й степени от образующего элемента β:

$$\delta = d_1\beta^{m-1} + d_2\beta^{m-2} + \ldots + d_{m-1}\cdot\beta + d_m \tag{10}$$

с коэффициентами d_i, принадлежащими полю R_1.

Поле $R[1+\sqrt[3]{4}]$ будет представлять собой совокупность чисел вида:

$$p_1 + q_1(1+\sqrt[3]{4}) + r_1(1+\sqrt[3]{4})^2 = p_1 + q_1 + q_1\sqrt[3]{4} + r_1 + 2r_1\sqrt[3]{4} + 2r_1\sqrt[3]{2} = (p_1 + q_1 + r_1) + 2r_1\sqrt[3]{2} + (q_1 + 2r_1)\sqrt[3]{4} = s + t\sqrt[3]{2} + u\sqrt[3]{4},$$

где s, t и u — рациональные числа. Таким образом,

$$R[1+\sqrt[3]{4}] = R[\sqrt[3]{2}].$$

Так как все d_i принадлежат R_1, то все они представляют собой целые рациональные функции от α $(n-1)$-й степени (или ниже):

$$d_i = a_{1i}\alpha^{n-1} + a_{2i}\alpha^{n-2} + \ldots + a_{n-1,i}\alpha + a_{ni} \quad (i = 1,2, \ldots, m), \tag{11}$$

где все a_{ki} принадлежат R.

Подставляя в (10) вместо d_i их значения из (11), получаем:

$$\begin{aligned}\delta = {} & (a_{11}\alpha^{n-1} + a_{21}\alpha^{n-2} + \ldots + a_{n-1,1}\alpha + a_{n1})\beta^{m-1} + \\ & + (a_{12}\alpha^{n-1} + a_{22}\alpha^{n-2} + \ldots + a_{n2})\beta^{m-2} + \ldots + \\ & + (a_{1m}\alpha^{n-1} + a_{2m}\alpha^{n-2} + \ldots + a_{nm}) = a_{11}\alpha^{n-1}\beta^{m-1} + \\ & + a_{21}\alpha^{n-2}\beta^{m-1} + \ldots + a_{n1}\beta^{m-1} + \\ & + a_{12}\alpha^{n-1}\beta^{m-2} + \ldots + a_{nm}.\end{aligned} \tag{12}$$

Из (12) мы видим, что любой элемент δ поля R представляет (относительно R) линейную однородную функцию от $n \cdot m$ элементов:

$$\alpha^{n-1}\cdot\beta^{m-1},\ \alpha^{n-2}\cdot\beta^{m-1},\ \ldots,\ \beta^{m-1},\ \alpha^{n-1}\cdot\beta^{m-2},\ \ldots,\ 1, \tag{13}$$

каждый из которых есть, как нетрудно видеть, элемент R_2. Остаётся только доказать, что элементы (13) линейно-независимы. Допустим, что между ними существует линейная зависимость:

$$\begin{aligned}& C_{11}\alpha^{n-1}\beta^{m-1} + C_{21}\alpha^{n-2}\beta^{m-1} + \ldots + C_{n1}\beta^{m-1} + \\ & + C_{12}\alpha^{n-1}\beta^{m-2} + C_{22}\alpha^{n-2}\beta^{m-2} + \ldots + C_{n2}\beta^{m-2} + \ldots + \\ & + C_{1m}\alpha^{n-1} + C_{2m}\alpha^{n-2} + \ldots + C_{mn} = 0,\end{aligned} \tag{14}$$

где C_{ik} принадлежит R.

Тогда, собирая все члены, содержащие одинаковую степень β, и, вынося её за скобки, имеем:

$$\begin{aligned}& (C_{11}\alpha^{n-1} + C_{21}\alpha^{n-2} + \ldots + C_{n1})\beta^{m-1} + \\ & + (C_{12}\alpha^{n-1} + C_{22}\alpha^{n-2} + \ldots + C_{n2})\beta^{m-2} + \ldots + \\ & + (C_{1m}\alpha^{n-1} + C_{2m}\alpha^{n-2} + \ldots + C_{mn}) = 0.\end{aligned} \tag{15}$$

Но так как β есть корень неприводимого в R_1 уравнения m-й степени, то этот элемент не может удовлетворять никакому уравнению низшей степени. Поэтому все m коэффициентов (15), представляющие собой числа из R_1, должны обратиться в нуль:

$$C_{1k}\alpha^{n-1} + C_{2k}\alpha^{n-2} + \ldots + C_{nk} = 0, (k = 1, 2, \ldots, m). \tag{16}$$

А так как элемент α, со своей стороны, есть корень неприводимого в R уравнения n-й степени, то он не может служить корнем никакого уравнения $(n-1)$-й степени с рациональными коэффициентами. Поэтому во всех m равенствах (16) все коэффициенты C_{ik} должны быть равны нулю.

Этим доказана линейная независимость в R $m \cdot n$ элементов (13), которые, таким образом, образуют базис многообразия R_2 относительно R. Следовательно, степень расширения R_2 относительно R есть mn:

$$\{R_2 : R\} = mn. \tag{17}$$

Теорема доказана. Путём повторного применения результаты её распространяются на любое число последовательных расширений.

Если, следовательно, мы берём поле рациональных чисел R и к нему последовательно приобщаем алгебраические числа $\alpha_1, \alpha_2, \ldots, \alpha_h$, причём:
α_1 есть корень неприводимой в R функции степени n_1,
α_2 — корень неприводимой в $R_1 = R[\alpha_1]$ функции степени n_2,

. . . . . .

α_h — корень неприводимой в $R_{h-1} = R[\alpha_1, \alpha_2, \ldots, \alpha_{h-1}]$ функции степени n_h, то полученное алгебраическое расширение

$$R_h = R[\alpha_1, \alpha_2, \ldots, \alpha_h]$$

является относительно R линейным многообразием $n_1 n_2 \ldots n_h$-го порядка. Иными словами, степень расширения R_h относительно R есть произведение $n_1 n_2 \ldots n_h$:

$$\{R_h : R\} = n_1 \cdot n_2 \ldots n_h. \tag{18}$$

3. Применим полученные результаты к исследованию вопроса о разрешимости уравнения в радикалах. Так как всякий радикал $\sqrt[m]{a}$ есть корень двучленного уравнения $x^m - a = 0$, то решить уравнение в радикалах — это значит выразить рационально его корни через корни двучленных уравнений.

Пусть дано уравнение n-й степени с рациональными коэффициентами

$$f(x) = 0. \tag{19}$$

Если уравнение (19) разрешимо в радикалах, то это значит, что решение его сводится к решению цепи двучленных уравнений:

$$\begin{aligned} x^{n_1} - a_1 &= 0, \\ x^{n_2} - a_2 &= 0, \\ x^{n_3} - a_3 &= 0, \\ &\cdots\cdots\cdots \\ x^{n_h} - a_h &= 0, \end{aligned} \tag{20}$$

где a_1 — рациональное число, a_2 — рациональная функция от корней первого уравнения, a_3 — рациональная функция от корней первого и второго уравнений и т. д.

Если $\alpha_1, \alpha_2, \ldots, \alpha_h$—корни уравнений (20), то некоторый корень x_1 данного уравнения (19) будет, в случае разрешимости этого уравнения в радикалах, рациональной в R функцией от корней двучленных уравнений[1]

$$x_1 = F(\alpha_1, \alpha_2, \ldots, \alpha_h).$$

Построим поле, к которому принадлежали бы все иррациональности α_i. Для этого будем расширять поле R, приобщая к нему последовательно $\alpha_1, \alpha_2, \ldots, \alpha_h$. Получим:

$$R_h = R[\alpha_1, \alpha_2, \ldots, \alpha_h]. \tag{21}$$

Какова степень этого расширения? α_1 есть корень уравнения $x^{n_1} - a_1 = 0$, но это уравнение может оказаться приводимым в поле R. Пусть $K_1(x)$ — та неприводимая в R функция, корнем которой служит α_1, и пусть степень её k_1. Точно так же двучленное уравнение $x^{n_2} - a_2 = 0$, доставляющее корень α_2, может оказаться приводимым в поле $R_1 = R[\alpha_1]$; пусть $K_2(x)$ будет неприводимая в R_1

[1] Так, например, если уравнение разрешимо в радикалах и корень его x_1 выражается следующим образом:

$$x_1 = \frac{\sqrt[3]{2+\sqrt{3}} - 2\sqrt[3]{4}}{6+\sqrt[4]{5-3\sqrt{3}}},$$

то этот корень является рациональной функцией от корней следующей цепи двучленных уравнений:

$x^2 - a_1 = 0$, где $a_1 = 3$; $\quad a_1 = \sqrt{3}$,
$x^3 - a_2 = 0$, где $a_2 = 2 + a_1$; $\quad a_2 = \sqrt[3]{a_2} = \sqrt[3]{2+\sqrt{3}}$,
$x^5 - a_3 = 0$, где $a_3 = 4$; $\quad a_3 = \sqrt[3]{4}$.
$x^4 - a_4 = 0$, где $a_4 = 5 - 3a_1$; $a_4 = \sqrt[4]{5-3\sqrt{3}}$.

Через корни a_1, a_2, a_3, a_4 этих уравнений x_1 выразится так:

$$x_1 = \frac{a_2 - 2a_3}{6 + a_4}.$$

функция степени k_2, корнем которой служит α_2, и т. д., пусть, наконец, α_h будет корнем неприводимой в поле R_{h-1} функции $K_h(x)$ степени k_h.

Ряд функций

$$K_1(x),\ K_2(x),\ldots,\ K_h(x) \tag{22}$$

образует *разрешающую цепочку* функций для уравнения (19).

Согласно доказанной выше теореме, степень расширения R_h относительно R равна произведению степеней функций (22), т. е.

$$\{R_h : R\} = k_1 \cdot k_2,\ \ldots,\ k_h. \tag{23}$$

Мы будем предполагать далее, что уравнение (19) является *неприводимым* в поле R.

Пусть x_1 есть корень этого уравнения; следовательно, $f(x_1) = 0$. Приобщая его к полю R, мы получим алгебраическое расширение $R[x_1]$, степень которого есть

$$\{R[x_1] : R\} = n. \tag{24}$$

С другой стороны, корень $x_1 = F(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_h)$ как рациональная функция от α_i является элементом поля R_h; к этому же полю принадлежит и всякая рациональная функция от x_1, т. е. принадлежат все элементы поля $R[x_1]$, которое, таким образом, представляет собой часть поля R_h; следовательно, R_h есть расширение поля $R[x_1]$. Пусть q есть степень этого расширения[1]:

$$\{R_h : R[x_1]\} = q.$$

Итак, поле R_h можно рассматривать как полученное из R путём двух последовательных расширений от R до $R[x_1]$ — степени n и от $R[x_1]$ до R_h — степени q. По доказанной выше теореме степень расширения R_h относительно R есть произведение этих степеней:

$$\{R_h : R\} = \{R_h : R[x_1]\} \cdot \{R[x_1] : R\}, \tag{25}$$

---

[1] Поле R_s, являющееся алгебраическим расширением поля R и представляющее линейное многообразие некоторого порядка s относительно R, является также линейным многообразием (низшего порядка) относительно всякого поля R^*, заключённого между R_s и R

$$R_s \subset R^* \subset R.$$

В самом деле, все элементы R_s выражаются линейно через элементы некоторого базиса $\sigma_1, \sigma_2, \ldots, \sigma_s$ и коэффициентами из R. Но так как каждый коэффициент из R принадлежит также R^*, то R_s представляет собой линейное многообразие относительно R^*. Число линейно-независимых среди $\sigma_1, \sigma_2, \ldots, \sigma_s$ относительно поля R^* и есть степень расширения R_s относительно R^*.

или

$$k_1 \cdot k_2 \ldots k_h = q \cdot n. \qquad (26)$$

Таким образом, степень неприводимой функции $f(x)$ должна быть делителем произведения степеней разрешающей цепочки функций.

Пусть теперь неприводимое уравнение $f(x) = 0$ разрешимо в *квадратных* радикалах. Тогда разрешающая цепочка состоит из функций второй степени

$$k_1 = k_2 = \ldots = k_h = 2. \qquad (27)$$

Из (26) мы видим, что в этом случае число n, являясь делителем числа 2^h, само должно быть степенью двойки:

$$n = 2^m . \qquad (28)$$

Итак, *для того чтобы неприводимое в R уравнение $f(x) = 0$ было разрешимо в квадратных радикалах, необходимо, чтобы степень его была степенью двойки*[1].

Выведенное нами условие разрешимости является необходимым, но, вообще говоря, ещё недостаточным.

§ 4. ПОЛИНОМЫ ДЕЛЕНИЯ ОКРУЖНОСТИ. НЕОБХОДИМОЕ УСЛОВИЕ РАЗРЕШИМОСТИ В КВАДРАТНЫХ РАДИКАЛАХ УРАВНЕНИЯ $x^n - 1 = 0$

1. Установленное выше необходимое условие разрешимости неприводимого алгебраического уравнения в квадратных радикалах применить непосредственно к интересующему нас случаю двучленных уравнений не представляется возможным, потому что двучленные уравнения $x^n - 1 = 0$, имея корнем $x = 1$, всегда являются приводимыми.

Мы видели выше (§ 2, 2), что для решения двучленного уравнения n-й степени $x^n - 1 = 0$ достаточно найти хотя бы один из его $\varphi(n)$ первообразных корней, все остальные корни получатся путём последовательного возвышения в степень этого корня r:

$$r, r^2, \ldots, r^{n-1}, r^n = 1.$$

Ввиду этого вопрос о решении двучленного уравнения можно свести к решению такого уравнения $\Phi_n(x) = 0$

---

[1] Отсюда, между прочим, вытекает, что известные задачи об *удвоении куба* и о *трисекции угла* невыполнимы с помощью циркуля и линейки, так как степень соответствующих уравнений, к которым приводятся эти задачи: $x^3 - 2 = 0$ и $x^3 - 3x - b = 0$ (неприводимость их в R доказывается без труда), не является степенью двойки.

(уже не двучленного), которое своими корнями имело бы первообразные корни данного двучленного уравнения и только эти корни; тогда любой корень уравнения $\Phi_n(x) = 0$ давал бы решение двучленного уравнения.

Такое уравнение $\Phi_n(x) = 0$, ввиду связи двучленных уравнений с задачей деления окружности, называется *уравнением деления окружности*. Левую часть этого уравнения будем называть полиномом деления окружности (на n частей). Итак, полиномом деления окружности называется такой многочлен $\Phi_n(x)$, корнями которого служат все первообразные корни n-й степени из единицы (и только они). Очевидно, степень такого полинома должна быть $\varphi(n)$. Мы покажем, что для всякого значения n (для всякого уравнения $x^n - 1 = 0$) такой многочлен с рациональными (и даже целыми) коэффициентами всегда существует.

В случае, когда степень двучленного уравнения есть простое число p, то все корни такого уравнения, кроме $x = 1$, первообразные. Поэтому полином деления окружности в этом случае мы получим просто делением $x^p - 1$ на $x - 1$:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1. \qquad (1)$$

Рассмотрим теперь случай, когда степень двучленного уравнения есть степень простого числа: $n = p^\alpha$.

Так как $p^{\alpha-1}$ есть делитель числа p^α, то всякий корень уравнения $x^{p^{\alpha-1}} - 1 = 0$, очевидно, будет являться корнем уравнения $x^{p^\alpha} - 1 = 0$. С другой стороны, мы покажем, что всякий непервообразный корень уравнения $x^{p^\alpha} - 1 = 0$ должен быть корнем уравнения $x^{p^{\alpha-1}} - 1 = 0$.

Все делители p^α суть числа

$$1,\ p,\ p^2,\ \ldots,\ p^{\alpha-1}.$$

Если ε — непервообразный корень уравнения $x^{p^\alpha} - 1 = 0$, то он принадлежит как к показателю к одному из написанного выше ряда чисел. Пусть ε принадлежит к показателю p^β ($\beta \leqslant \alpha - 1$) и, следовательно, является корнем (первообразным) уравнения $x^{p^\beta} - 1 = 0$. Но так как p^β есть делитель числа $p^{\alpha-1}$, то ε будет являться также корнем уравнения $x^{p^{\alpha-1}} - 1 = 0$. Таким образом, корнями уравнения $x^{p^{\alpha-1}} - 1 = 0$ служат все непервообразные корни уравнения $x^{p^\alpha} - 1 = 0$. Поэтому полином

деления окружности на p^α частей мы найдём, разделив $x^{p^\alpha} - 1$ на $x^{p^{\alpha-1}} - 1$. Выполняя это деление, получаем:

$$\Phi_{p^\alpha}(x) = \frac{x^{p^\alpha} - 1}{x^{p^{\alpha-1}} - 1} = x^{p^{\alpha-1}(p-1)} + x^{p^{\alpha-1}(p-2)} + \\ + \ldots + x^{p^{\alpha-1}} + 1. \qquad (2)$$

В общем случае, при произвольном n, выражение для $\Phi_n(x)$ будет более сложным. Именно мы покажем, что если

$$n = p^\alpha \cdot q^\beta \cdot r^\gamma \cdot s^\delta \ldots,$$

то полином деления окружности найдётся по следующей формуле:

$$\Phi_n(x) = \frac{(x^n - 1)(x^{\frac{n}{pq}} - 1)(x^{\frac{n}{pr}} - 1)(x^{\frac{n}{qr}} - 1)\ldots(x^{\frac{n}{pqrs}} - 1)\ldots}{(x^{\frac{n}{p}} - 1)(x^{\frac{n}{q}} - 1)(x^{\frac{n}{r}} - 1)\ldots(x^{\frac{n}{pqr}} - 1)(x^{\frac{n}{pq^2}} - 1)\ldots} = \\ = \frac{\prod (x^{d_1} - 1)}{\prod (x^{d_2} - 1)}. \qquad (3)$$

В этом выражении числитель состоит из произведения двучленов вида $x^{d_1} - 1$, где d_1 принимает значения, равные n и всем делителям числа n, получающимся от деления n на *чётное* число простых чисел, входящих в состав n. Знаменатель же есть произведение всевозможных двучленов $x^{d_2} - 1$, где d_2 принимает значения, получающиеся от деления n на *нечётное* число его простых делителей[1]. Покажем справедливость формулы (3).

Так как каждый двучлен $x^{d_1} - 1$ или $x^{d_2} - 1$ имеет своими корнями корни n-й степени из единицы (каждый корень уравнения $x^{\frac{n}{pqr\ldots}} - 1 = 0$ является также корнем уравнения $x^n - 1 = 0$), то и числитель и знаменатель дроби (3) представляют собой произведения двучленов вида $x - \varepsilon$, где ε — различные значения корня n-й степени из единицы. Пусть ε — какой-нибудь из этих корней n-й степени и притом непервообразный. Он является тогда первообразным для уравнения $x^d - 1 = 0$, где d есть некоторый делитель числа n. Если d есть делитель n, то некоторые из простых сомножителей числа n входят в состав d в степени меньшей, чем они входят в n. Пусть все такие сомножители суть:

$$p_1, p_2, \ldots, p_m. \qquad (4)$$

[1] При $n = p^\alpha$ формула (3) переходит в (2).

Среди показателей степеней двучленов, входящих в состав числителя выражения (3), на d делятся: во-первых, само n, затем показатели вида $\frac{n}{p_i p_k}$, где p_i, p_k — числа ряда (4), таких показателей будет $C_m^2 = \frac{m(m-1)}{1 \cdot 2}$; далее, на d делятся показатели вида $\frac{n}{p_i p_k p_j p_l}$, где p_i, p_k, p_j, p_l — числа ряда (4), этих показателей C_m^4 и т. д.

Всего в числителе дроби выражения (3) двучленов с показателями степени, делящимися на d, будет:

$$\alpha = 1 + C_m^2 + C_m^4 + \dots . \qquad (5)$$

Так как на $x - \varepsilon$ (где ε — первообразный корень d-й степени) будут делиться только такие двучлены $x^{d_1} - 1$, в которых показатели d_1 делятся на d, и так как ни один из этих двучленов кратных корней иметь не может, то отсюда можно заключить, что $x - \varepsilon$ войдёт в состав числителя выражения (3) ровно α раз.

Рассуждая подобным же образом, мы убедимся, что в состав знаменателя (3) тот же множитель $x - \varepsilon$ войдёт β раз, где

$$\beta = C_m^1 + C_m^3 + C_m^5 + \dots . \qquad (6)$$

Но, как известно, в разложении бинома Ньютона сумма биномиальных коэффициентов, стоящих на чётных местах, равна сумме коэффициентов, стоящих на нечётных местах[1]. Поэтому $\beta = \alpha$.

Таким образом, множитель $x - \varepsilon$ войдёт в состав числителя и знаменателя выражения (3) одинаковое число раз и, следовательно, сократится. То же будет с каждым непервообразным корнем. В составе выражения (3) остаются только двучлены вида $x - \varepsilon$, в которых ε — первообразные корни n-й степени. Таких двучленов имеется $\varphi(n)$; они находятся только в числителе в разложении двучлена $x^n - 1$, и каждый из них войдёт один раз. Поэтому определяемое по формуле (3) выражение для $\Phi_n(x)$ и есть

[1] Полагая по формуле

$$(x-y)^m = x^m - C_m^1 x^{m-1} y + C_m^2 x^{m-2} y^2 - C_m^3 x^{m-3} y^3 + C_m^4 x^{m-4} y^4 \dots$$

$x = y = 1$, получаем

$$0 = 1 - C_m^1 + C_m^2 - C_m^3 + C_m^4 - C_m^5 + \dots ,$$

откуда

$$1 + C_m^2 + C_m^4 + \dots = C_m^1 + C_m^3 + C_m^5 + \dots$$

многочлен степени $\varphi(n)$, имеющий своими корнями первообразные корни n-й степени, т. е. это и есть полином деления окружности.

Примеры: 1) Найдём $\Phi_{30}(x)$.

$n = 30 = 2 \cdot 3 \cdot 5$

$d_1 \mid 30,\ \frac{30}{2\cdot 3},\ \frac{30}{2\cdot 5},\ \frac{30}{3\cdot 5}$

$d_2 \mid \frac{30}{2},\ \frac{30}{3},\ \frac{30}{5},\ \frac{30}{2\cdot 3\cdot 5}$

$$\Phi_{30}(x) = \frac{(x^{30}-1)(x^5-1)(x^3-1)(x^2-1)}{(x^{15}-1)(x^{10}-1)(x^6-1)(x-1)} = \frac{(x^{15}+1)(x+1)}{(x^5+1)(x^3+1)} =$$

$$= \frac{x^{10}-x^5+1}{x^2-x+1} = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$$

2) Составим таблицу $\Phi_n(x)$ от $n = 2$ до $n = 12$.

$\Phi_2(x) = x + 1,$

$\Phi_3(x) = x^2 + x + 1,$

$\Phi_4(x) = x^2 + 1,$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$

$\Phi_6(x) = x^2 - x + 1,$

$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$

$\Phi_8(x) = x^4 + 1,$

$\Phi_9(x) = x^6 + x^3 + 1,$

$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1,$

$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$

$\Phi_{12}(x) = x^4 - x^2 + 1.$

Полиномы Φ_2, Φ_3, Φ_5, Φ_7, Φ_{11} найдены по формуле (1),

Φ_4, Φ_8, Φ_9 » по формуле (2) и

Φ_6, Φ_{10}, Φ_{12} » по общей формуле (3).

2. Весьма важным свойством полиномов деления окружности является их *неприводимость* в области рациональных чисел (в дальнейшем под неприводимостью мы будем понимать неприводимость в R).

При доказательстве неприводимости полинома $\Phi_n(x)$ нам понадобятся следующие ниже вспомогательные предложения, принадлежащие Гауссу.

Пусть $f(x)$ — многочлен с *целыми* коэффициентами и пусть δ — общий наибольший делитель всех коэффициентов $f(x)$.

Тогда:

$$f(x) = \delta \cdot \varphi(x),$$

где коэффициенты многочлена $\varphi(x)$ уже не имеют общего делителя; такой многочлен назовём *первообразным*. До-

кажем, что произведение двух первообразных многочленов есть тоже первообразный многочлен.

Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

и

$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$$

— два первообразных многочлена и

$$F(x) = f(x) \cdot g(x) = c_0x^{n+m} + c_1x^{n+m-1} + \ldots + c_{n+m-1}x + c_{n+m}$$

— их произведение. Возьмём любое простое число p. Пусть a_k — первый из коэффициентов $f(x)$, который не делится на p, так что a_0, a_1, ..., a_{k-1} делятся на p (все a_i на p делиться не могут, так как $f(x)$ — первообразный многочлен). Точно так же пусть b_l — первый из коэффициентов $g(x)$, не делящийся на p. Рассмотрим коэффициент с индексом $k + l$ функции $F(x)$:

$$c_{k+l} = a_kb_l + a_{k+1}b_{l-1} + a_{k+2}b_{l-2} + \ldots + a_{k-1}b_{l+1} + a_{k-2}b_{l+2} + \ldots . \qquad (7)$$

В правой части равенства (7) все слагаемые, кроме первого, делятся на p, поэтому c_{k+l} не может делиться на p. Следовательно, p не может быть общим делителем всех коэффициентов функции $F(x)$, и так как p взято произвольно, то отсюда следует, что $F(x)$ — первообразный многочлен.

Теперь докажем следующую теорему:

Если многочлен с целыми коэффициентами приводим, то его можно разложить на произведение многочленов с целыми коэффициентами.

Пусть

$$f(x) = \varphi(x) \cdot \psi(x), \qquad (8)$$

где $\varphi(x)$ и $\psi(x)$ имеют рациональные коэффициенты.

В многочлене $\varphi(x)$ приведём коэффициенты к общему знаменателю s и затем вынесем за скобки наибольший общий делитель d числителей коэффициентов; то же сделаем и с многочленом $\psi(x)$. Тогда

$$\varphi(x) = \frac{d}{s} \cdot \varphi_1(x),$$

$$\psi(x) = \frac{\delta}{l} \cdot \psi_1(x), \qquad (9)$$

где $\varphi_1(x)$ и $\psi_1(x)$ — первообразные многочлены.

Подставляя значения $\varphi(x)$ и $\psi(x)$ в (8), получаем:

$$f(x) = \frac{d \cdot \delta}{s \cdot t} \varphi_1(x) \cdot \psi_1(x). \qquad (10)$$

Покажем, что $\frac{d \cdot \delta}{s \cdot t}$ есть целое число. Пусть $\frac{d \cdot \delta}{s \cdot t} = \frac{p}{q}$ (p и q—взаимно простые). Так как многочлен $\frac{p}{q} \cdot \varphi_1(x) \cdot \psi_1(x)$ должен иметь целые коэффициенты [ибо таков многочлен $f(x)$] и так как p и q взаимно простые, то все коэффициенты многочлена $\varphi_1(x) \cdot \psi_1(x)$ должны делиться на q. Но $\varphi_1(x) \cdot \psi_1(x)$, как произведение первообразных многочленов, само должно быть первообразным; поэтому $q = 1$.

Итак, $$f(x) = p \cdot \varphi_1(x) \cdot \psi_1(x). \qquad (11)$$

Таким образом, $f(x)$ разложен на произведение двух многочленов с целыми коэффициентами —$p\varphi_1(x)$ и $\psi_1(x)$. Теорема доказана.

Отсюда вытекает, что для того чтобы доказать неприводимость многочлена с целыми коэффициентами, достаточно показать, что он не может быть представлен в виде произведения многочленов с *целыми* коэффициентами.

Далее заметим ещё следующее. Пусть многочлен с целыми коэффициентами $f(x)$ имеет коэффициент при старшем члене, равный единице (такой многочлен назовём приведённым). Тогда, если

$$f(x) = g(x) \cdot h(x) \qquad (12)$$

есть разложение $f(x)$ на многочлены с целыми коэффициентами, то очевидно, что старшие коэффициенты функций $g(x)$ и $h(x)$ тоже равны единице. Но верно и обратное предложение: если в разложении (12) приведённого многочлена $f(x)$ с целыми коэффициентами на множители $g(x)$ и $h(x)$ с рациональными коэффициентами старший коэффициент функции $g(x)$ (а следовательно, и функции $h(x)$) равен единице, то разложение (12) есть разложение на множители с целыми коэффициентами.

В самом деле, если бы один из множителей, например $g(x)$, имел бы дробные коэффициенты, то, приводя их к общему наименьшему знаменателю p, мы имели бы

$$g(x) = x^m + \frac{\beta_1 x^{m-1} + \beta_2 x^{m-2} + \ldots + \beta_m}{p} = \frac{1}{p} g_1(x), \qquad (13)$$

где $g_1(x) = px^m + \beta_1 x^{m-1} + \ldots + \beta_m$ — первообразный многочлен (все β_i не могут иметь общего делителя с p,

так как p — наименьший знаменатель) Точно так же мы поступим с многочленом $h(x)$, если он имеет дробные коэффициенты (если же у $h(x)$ коэффициенты целые, то он сам первообразный, так как его старший коэффициент равен единице):

$$h(x) = \frac{1}{q} \cdot h_1(x), \tag{14}$$

где $h_1(x)$ — первообразный многочлен.

Подставляя значение $g(x)$ и $h(x)$ в (12), получаем:

$$f(x) = \frac{1}{p \cdot q} \cdot g_1(x) \cdot h_1(x). \tag{15}$$

Так как $f(x)$ — многочлен с целыми коэффициентами, то коэффициенты произведения $g_1(x)h_1(x)$ должны все делиться на pq; но $g_1(x) \cdot h_1(x)$ есть первообразный многочлен, следовательно, $pq = 1$ и $p = q = 1$.

Этим доказано, что коэффициенты $g(x)$ и $h(x)$ целые.

Отсюда можно сделать ещё такой вывод. Определяя $h(x)$ из равенства (12)

$$h(x) = \frac{f(x)}{g(x)}, \tag{16}$$

мы можем сформулировать следующее предложение: если приведённый многочлен с целыми коэффициентами $f(x)$ делится на другой приведённый многочлен, то частное есть приведённый многочлен с *целыми* коэффициентами. Отсюда, в частности, вытекает, что полином деления круга $\Phi_n(x)$, определяемый по формуле (3) [§ 4, 1], должен иметь целые коэффициенты.

Переходим к доказательству неприводимости полиномов деления окружности. Дадим доказательство для $n = p^\alpha$. В этом случае, как мы видели,

$$\Phi(x) = x^{p^{\alpha-1}(p-1)} + x^{p^{\alpha-1}(p-2)} + \ldots + x^{p^{\alpha-1}} + 1.$$

Допустим, что $\Phi(x)$ разлагается на произведение многочленов с целыми коэффициентами:

$$\Phi(x) = f(x) \cdot g(x). \tag{17}$$

Так как старший коэффициент многочлена $\Phi(x)$ равен единице, то таковыми же должны быть старшие коэффициенты функций $f(x)$ и $g(x)$.

Полагая в равенстве (17) $x = 1$ и замечая, что $\Phi(1) = p$, получаем:

$$p = f(1) \cdot g(1). \tag{18}$$

Так как p — простое, то один из сомножителей $f(1)$ или $g(1)$ равен ± 1, а другой $\pm p$. Не нарушая общности, положим, что

$$f(1) = \pm 1. \tag{19}$$

Пусть r есть тот корень уравнения $\Phi(x) = 0$, который является корнем $f(x)$, так что $f(r) = 0$.

Пусть ε — любой корень уравнения $\Phi(x) = 0$, т. е. любой первообразный корень p^α-й степени из единицы; тогда ряд

$$\varepsilon,\ \varepsilon^2,\ \ldots,\ \varepsilon^{p^\alpha} = 1$$

представляет собой все p^α корней уравнения $x^{p^\alpha} - 1 = 0$.

Из них:

$$\varepsilon,\ \varepsilon^a,\ \varepsilon^b,\ \ldots,\ \varepsilon^k,$$

где $a, b, \ldots, k$ не делятся на p (и, следовательно, взаимно простые с p^α), являются первообразными корнями уравнения $x^{p^\alpha} - 1 = 0$. Рассмотрим произведение

$$f(\varepsilon) \cdot f(\varepsilon^a) \cdot f(\varepsilon^b) \ldots f(\varepsilon^k). \tag{20}$$

Нетрудно видеть, что выражение это равно нулю, так как среди чисел $\varepsilon, \varepsilon^a, \ldots, \varepsilon^k$, представляющих все корни уравнения $\Phi(x) = 0$, найдётся равное r, а $f(r) = 0$.

Отсюда следует, что функция

$$F(x) = f(x) \cdot f(x^a) \cdot f(x^b) \ldots f(x^k) \tag{21}$$

имеет своим корнем $x = \varepsilon$, где ε — любой корень уравнения $\Phi(x) = 0$. Таким образом, функция $F(x)$ имеет своими корнями все корни функции $\Phi(x)$, а потому $F(x)$ делится на $\Phi(x)$:

$$F(x) = \Phi(x) \cdot \varphi(x), \tag{22}$$

причём функция $\varphi(x)$ должна иметь *целые* коэффициенты, так как старшие коэффициенты функций $F(x)$ и $\Phi(x)$ равны единице (что старший коэффициент $F(x)$ равен 1, это видно из формулы (21), так как старший коэффициент $f(x)$ равен 1).

Полагая в равенстве (21) $x = 1$ и замечая, имея в виду (19), что $F(1) = f(1)f(1)\ldots f(1) = \pm 1$, а $\Phi(1) = p$, получаем, что

$$\pm 1 = p \cdot \varphi(1). \tag{23}$$

Но произведение двух целых чисел p и $\varphi(1)$ не может равняться ± 1. Это противоречие и доказывает неправильность допущения о том, что $\Phi(x)$ разлагается на произ-

ведение функций с целыми коэффициентами. А отсюда вытекает неприводимость $\Phi(x)$.

Вопросом о неприводимости полиномов деления окружности занимались многие математики, начиная с середины прошлого столетия и вплоть до настоящего времени. Приведённое выше доказательство (для случая $n = p^\alpha$), использующее свойства первообразных корней, принадлежит Кронекеру. Существуют (для этого же случая) и другие доказательства, из которых наиболее просто доказательство Эйзенштейна, использующее свойства коэффициентов уравнения $\Phi_{p^\alpha}(x) = 0$ и опирающееся на критерий неприводимости Эйзенштейна.

Доказательство неприводимости полинома $\Phi_n(x)$ в общем случае, для любого n, более сложно. Для него предложено было несколько методов. Мы изложим одно из последних доказательств (идея которого принадлежит И. Шуру) примерно в том виде, как оно даётся Н. Г. Чеботарёвым (см. монографию Чеботарёва «Теория Галуа», М., 1936, гл. I; там же приведена и литература по этому вопросу[1]).

Для доказательства нам понадобится вспомогательное предложение, известное под названием *формулы Шенемана*. Возьмём многочлен $f(x)$ с целыми коэффициентами:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \qquad (24)$$

и возведём его в p-ю степень, где p — простое число.

p-я степень этого многочлена содержит, кроме p-х степеней отдельных членов, только такие члены, коэффициенты которых делятся на p. Действительно, коэффициенты всех членов, не являющихся p-ми степенями, будут вида[2]:

$$\frac{p!}{k_0!k_1!k_2!\ldots k_n!}\ (k_0 + k_1 + \ldots + k_n = p). \qquad (25)$$

И так как все k_i при членах, не являющихся p-ми степенями, меньше, чем простое число p, то p сохранится в выражении (25) и, следовательно, все указанные коэффициенты разделятся на p.

Соединяя все эти члены вместе и вынося p за скобки, получим:

$$[f(x)]^p = a_0^px^{np} + a_1^px^{(n-1)p} + \ldots + a_{n-1}^px^p + a_n^p + p\ .\ \psi(x), \qquad (26)$$

где $\psi(x)$ — некоторая функция с целыми коэффициентами.

Замечаем далее, что по теореме Ферма[3] $a^p - a$ делится на p и, следовательно:

$$\left.\begin{aligned} a_0^p &= a_0 + p\ .\ q_0,\\ a_1^p &= a_1 + p\ .\ q_1,\\ &\ldots\ldots\ldots\ldots\\ a_n^p &= a_n + p\ .\ q_n. \end{aligned}\right\} \qquad (27)$$

---

[1] Последнее по времени (1937 г.) доказательство принадлежит Ван дер Вардену.

[2] Это есть обобщение на многочлен обычной формулы для степени бинома, где коэффициенты

$$C_p^k = \frac{p(p-1)\ldots(p-k)}{1\cdot 2\ldots k} = \frac{p!}{k!\,(p-k)!}\ .$$

[3] $a^p \equiv a \pmod p$. Это доказывается нами ниже в § 5, 1.

Подставляя значения a_0^p, a_1^p ... из (27) в (26) и вновь соединяя вместе члены, содержащие p, имеем

$$[f(x)]^p = a_0x^{pn} + a_1x^{p(n-1)} + \ldots + a_{n-1}x^p + a_n + p \cdot \varphi(x),$$

где $\varphi(x)$ — функция с целыми коэффициентами. Но первые $n+1$ слагаемых в правой части — это результат подстановки в функцию $f(x)$ вместо xx^p. Поэтому окончательно получаем:

$$[f(x)]^p = f(x^p) + p \cdot \varphi(x). \tag{28}$$

Это и есть формула Шенемана.

Далее нам придётся воспользоваться некоторыми свойствами результантов и дискриминантов. Если заданы два приведённых многочлена $f(x)$ и $g(x)$, имеющие корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ и $\beta_1, \beta_2, \ldots, \beta_m$ соответственно, то *результантом* их, как известно, будут выражения:

$$\left.\begin{aligned} R(f, g) &= g(\alpha_1)g(\alpha_2) \ldots g(\alpha_n) = \prod_{i=1}^{n} g(\alpha_i), \text{ или} \\ R(g, f) &= f(\beta_1)f(\beta_2) \ldots f(\beta_m) = \prod_{k=1}^{m} f(\beta_k), \end{aligned}\right\} \tag{29}$$

могущие отличаться только знаками:

$$R(g, f) = (-1)^{m+n}R(f, g).$$

Равенство нулю результанта есть условие, необходимое и достаточное для того, чтобы многочлены имели общий корень. Результант есть симметрическая функция от корней каждого из многочленов, а симметрическая функция от корней многочлена, согласно основной теореме теории симметрических функций, рационально выражается через коэффициенты многочлена; в случае же если эта симметрическая функция имеет целочисленные коэффициенты, то её рациональное выражение через коэффициенты многочленов имеет также целые коэффициенты. Если сверх того окажется, что и данный многочлен имеет целые коэффициенты, то результант является *целым числом*. С этим случаем нам и придётся иметь дело.

Дискриминантом называется (взятый с определённым знаком) результант многочлена и его производной:

$$D(f) = R(f, f') = \pm f'(\alpha_1)f'(\alpha_2)\ldots f'(\alpha_n) = \pm \prod_{i=1}^{n} f'(\alpha_i). \tag{30}$$

Составим выражение для дискриминанта произведения двух многочленов:

$$\pm D(f \cdot g) = R(f \cdot g, f' \cdot g + f \cdot g') = \prod_{x=\alpha_i \cdot \beta_k} [f'(x)g(x) + f(x)g'(x)] =$$

$$= \prod_{i=1}^{n} [f'(\alpha_i)g(\alpha_i) + f(\alpha_i)\, g'(\alpha_i)] \cdot \prod_{k=1}^{m} [f'(\beta_k)g(\beta_k) + f(\beta_k)g'(\beta_k)],$$

но $$f(\alpha_i) = 0 \text{ и } g(\beta_k) = 0.$$

Поэтому

$$\pm D(f\cdot g) = \prod_{i=1}^{n} f'(\alpha_i)g(\alpha_i)\cdot\prod_{k=1}^{m} f(\beta_k)g'(\beta_k) =$$

$$= \prod_{i=1}^{n} f'(\alpha_i)\cdot\prod_{k=1}^{m} g'(\beta_k)\cdot\prod_{i=1}^{n} g(\alpha_i)\cdot\prod_{k=1}^{m} f(\beta_k) =$$

$$= \pm D(f)\cdot D(g)\cdot R(f, g)\cdot R(g, f). \qquad (31)$$

Окончательно имеем: $D(f\cdot g) = \pm D(f)\cdot D(g)\cdot R^2(f, g)$.

Эта формула может быть обобщена на случай произведения нескольких многочленов. Так, для произведения трёх многочленов f, g, h выводится:

$$D(f\cdot g\cdot h) = \pm D(f)\cdot D(g)\cdot D(h)\cdot R^2(f, g)\cdot R^2(f, h)\cdot R^2(g, h). \qquad (32)$$

Из этого мы сделаем следующее заключение. Пусть некоторый многочлен $F(x)$ с целыми коэффициентами делится на произведение двух других многочленов $f(x)$ и $g(x)$, т. е. $F(x) = f(x)\cdot g(x)\cdot\varphi(x)$; коэффициенты всех функций f, g и φ мы можем считать целыми; в этом случае дискриминанты и результанты являются целыми числами; формула (32) показывает, в частности, что дискриминант функции $F(x)$ разделится нацело на результант $R(f, g)$ функций $f(x)$ и $g(x)$.

Переходим к доказательству неприводимости $\Phi_n(x)$. Пусть ε — какой-нибудь корень полинома $\Phi_n(x)$, т. е. какой-нибудь первообразный корень n-й степени из единицы. Допустим, что полином $\Phi_n(x)$ приводим. Тогда он разлагается на произведение неприводимых сомножителей, коэффициенты которых мы, не нарушая общности, будем считать целыми числами. Пусть $f(x)$ — тот неприводимый сомножитель, который имеет корнем ε, так что $f(\varepsilon) = 0$. Возьмём простое число p, меньшее, чем n, и взаимно простое с n. Тогда ε^p является также первообразным корнем n-й степени и, следовательно, корнем полинома $\Phi_n(x)$. Мы покажем, что ε^p должно быть корнем функции $f(x)$. Если бы это было не так, то ε^p должно было бы быть корнем какого-нибудь другого неприводимого полинома $g(x)$, коэффициенты которого можно считать целыми. Многочлен $F(x) = x^n - 1$, имея с неприводимыми функциями $f(x)$ и $g(x)$ общие корни, должен делиться на каждую из них, а так как они взаимно простые [по свойству неприводимых функций — потому что корень ε^p, будучи корнем $g(x)$, не является, по предположению, корнем $f(x)$], то он должен делиться и на их произведение. А тогда, согласно вышесказанному, дискриминант $D(x^n - 1)$ должен разделиться на результант $R(f, g)$. Найдём сначала $D(x^n - 1)$, взяв корни многочлена $x^n - 1$ в виде ε, ε^2, ..., ε^{n-1}, $\varepsilon^n = 1$:

$$D(x^n - 1) = R(x^n - 1, nx^{n-1}) = \pm n\varepsilon^{n-1}n\varepsilon^{2(n-1)}\ldots n\varepsilon^{n(n-1)} =$$

$$= \pm n^n\varepsilon^{\frac{n(n+1)(n-1)}{2}} = \pm n^n, \qquad (33)$$

так как $\varepsilon^{\frac{n(n+1)(n-1)}{2}} = \pm 1$ как $(n-1)$-я степень произведения всех корней уравнения $x^n - 1 = 0$.

Вычислим теперь $R(f, g)$:

$$R(f, g) = \pm f(y_1) \cdot f(y_2) \ldots f(y_k),$$

где $y_1, y_2, \ldots, y_k$—корни полинома $g(x)$; среди них должен быть равный ε^p. Не нарушая общности, можем считать, что $y_1 = \varepsilon^p$.

Полагая в выведенной выше формуле Шенемана (28) $x = \varepsilon$ и замечая, что $f(\varepsilon) = 0$, получаем

$$f(\varepsilon^p) = -p \cdot \varphi(\varepsilon). \tag{34}$$

Так как $y_1 = \varepsilon^p$ есть тоже первообразный корень, то ε можно выразить как некоторую степень y_1:

$$\varepsilon = y_1^s.$$

Подставляя в (34), получаем

$$f(y_1) = p\psi(y_1), \tag{35}$$

где $\psi(y_1)$ — некоторая функция с целыми коэффициентами. Функция $f(x) - p\psi(x)$, имеющая корнем y_1, должна иметь своими корнями и все остальные корни $y_2, \ldots, y_k$ неприводимой функции $g(x)$. Поэтому соотношение (35) имеет место для всех корней y_i:

$$f(y_i) = p\psi(y_i) \quad (i = 1, 2, \ldots, k), \tag{36}$$

а потому

$$R(f, g) = \pm p^k \psi(y_1) \cdot \psi(y_2) \ldots \psi(y_k). \tag{37}$$

Произведение $\psi(y_1) \cdot \psi(y_2) \ldots \psi(y_k)$ есть симметрическая функция с целочисленными коэффициентами от корней полинома $g(x)$, имеющего целые коэффициенты, и потому должно быть целым числом. Соотношение (37), таким образом, показывает, что результант $R(f, g)$ делится на p^k. С другой стороны, дискриминант $D(x^n - 1)$ должен делиться на $R(f, g)$. Следовательно, как показывает (34), n^n должно делиться на p^k. Но этого быть не может, так как p взаимно простое с n.

Это противоречие и доказывает, что ε^p не может быть корнем никакого другого полинома $g(x)$, а должно быть корнем функции $f(x)$, т. е.

$$f(\varepsilon^p) = 0. \tag{38}$$

Теперь нетрудно показать, что любой корень полинома $\Phi_n(x)$ является корнем $f(x)$. В самом деле, такой корень всегда имеет вид ε^u, где u взаимно простое с n. Пусть.

$$u = p \cdot p' \cdot p'' \ldots .$$

Тогда $\varepsilon^{p \cdot p'} = (\varepsilon^p)^{p'}$. И так как $f(\varepsilon^p) = 0$, а p'— простое число, меньшее n, и взаимно простое с n, то по доказанному $f[(\varepsilon^p)^{p'}] = f(\varepsilon^{pp'}) = 0$. Точно так же покажем, что $\varepsilon^{pp'p''}$ есть корень, так как $\varepsilon^{pp'p''} = (\varepsilon^{pp'})^{p''}$, а p'' — простое число, меньшее n, и взаимно простое с n и т. д. Следовательно,

$$f(\varepsilon^u) = 0.$$

Итак показано, что любой корень полинома $\Phi_n(x)$ является корнем его неприводимого сомножителя $f(x)$. Поэтому

$$\Phi_n(x) = f(x).$$

Этим и доказана неприводимость[1] $\Phi_n(x)$.

3. Как мы уже указывали, решение двучленного уравнения $x^n - 1 = 0$ можно свести к решению соответствующего уравнения деления окружности $\Phi_n(x) = 0$, корни которого являются первообразными корнями двучленного уравнения. И если уравнение деления окружности окажется разрешимым в квадратных радикалах, то то же можно будет сказать и о двучленном уравнении. Наоборот, если уравнение деления окружности в квадратных радикалах не разрешается, то не решается в квадратных радикалах и двучленное уравнение (так как его первообразные корни не будут выражаться в квадратных радикалах).

Но уравнение деления окружности, как только что было установлено, неприводимо. А поэтому к нему можно применить установленный выше (§ 3,3) критерий разрешимости. А именно, мы видели, что для того, чтобы неприводимое уравнение было разрешимо в квадратных радикалах, необходимо, чтобы степень его была степенью двойки. Но степень уравнения $\Phi_n(x) = 0$ равна $\varphi(n)$. Когда же $\varphi(n)$ будет степенью двойки?

Пусть $n = 2^{\alpha} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ есть разложение n на простые множители, так что $p_1, p_2, \ldots, p_k$ — различные нечётные простые числа.

Тогда, как известно (§ 2, 3):

$$\varphi(n) =$$

$$= 2^{\alpha-1} \cdot p_1^{\alpha_1-1} p_2^{\alpha_2-1} \ldots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\ldots(p_k-1). \quad (39)$$

Для того чтобы $\varphi(n)$ было степенью двойки, необходимо, во-первых, чтобы все множители $p_i^{\alpha_i-1}$ были равны единице, т. е. чтобы

$$\alpha_1 = \alpha_2 = \ldots = \alpha_k = 1$$

и чтобы, во-вторых, множители $p_i - 1$ были степенями двойки, т. е. чтобы каждое простое число p_i имело вид

---

[1] А так как, кроме того, все корни уравнения $\Phi_n(x) = 0$ являются степенями одного из них, то уравнение деления окружности *нормально* в области R. (Нормальным называется неприводимое уравнение, обладающее тем свойством, что все его корни рационально выражаются через один из них.)

$2^m + 1$. Простые числа этого вида называются *гауссовыми* простыми числами или простыми числами *Ферма*[1].

Таково необходимое условие разрешимости в квадратных радикалах уравнения деления окружности, а следовательно, и двучленного уравнения.

Итак, *для того чтобы двучленное уравнение* $x^n - 1 = 0$ *было разрешимо в квадратных радикалах, необходимо, чтобы число* n *имело следующий вид*:

$$n = 2^\alpha \cdot p_1 \cdot p_2 \dots p_k, \qquad (40)$$

где α — целое положительное число или нуль, а p_i—*различные* простые числа вида $2^m + 1$.

Установленное нами необходимое условие оказывается, в чём мы убедимся в дальнейшем, вместе с тем и достаточным.

Из доказанного, в частности, следует, что, например, уравнения $x^7 - 1 = 0$ и $x^9 - 1 = 0$ неразрешимы в квадратных радикалах, так как числа 7 и 9 не удовлетворяют условию (39). Таким образом, оказывается невозможным разделить циркулем и линейкой окружность на 7 и на 9 частей, или, что то же, построить правильный семиугольник или девятиугольник[2].

§ 5. УСЛОВИЕ ВОЗМОЖНОСТИ ПОСТРОЕНИЯ ПРАВИЛЬНОГО МНОГОУГОЛЬНИКА ЦИРКУЛЕМ И ЛИНЕЙКОЙ

1. Выше нами было установлено необходимое условие разрешимости двучленного уравнения в квадратных радикалах. Имея в виду доказать и *достаточность* этого условия, мы первоначально покажем возможность разрешения в квадратных радикалах уравнения $x^p - 1 = 0$, где p — простое число вида $2^m + 1$. Метод, при помощи которого мы проведём решение в квадратных радикалах указанного двучленного уравнения, требует некоторых дополнительных сведений из теории чисел, а именно — знакомства со свойствами так называемых «первообразных

[1] Об этих числах см. ниже, § 5, 3.

[2] Следует подчеркнуть, что *невозможность* построения относится к употребляемым здесь средствам построения — циркулю и линейке. С помощью других средств та же задача может быть решена. Например, правильный семиугольник может быть построен с помощью двух прямых углов (см. *Адлер*, Теория геометрических построений, гл. VIII).

корней числа p», или иначе — первообразных корней *сравнения* $x^{p-1} - 1 \equiv 0 \pmod{p}$.

Если два (целых) числа a и b при делении на целое положительное число m дают одинаковые остатки:

$$a = mp + r$$
$$b = mq + r,$$

то такие числа называются *равноостаточными* или *сравнимыми* по *модулю* m, что записывается в таком виде:

$$a \equiv b \pmod{m}. \qquad (1)$$

Очевидно, что для того чтобы a было сравнимо с b, необходимо и достаточно, чтобы разность $a - b$ делилась на m.

Числа, дающие при делении на m один и тот же остаток, или, как говорят, *вычет*, т. е. сравнимые между собой (mod m), мы отнесём к одному и тому же классу. Так как различных вычетов по модулю m всего есть m : 0, 1, 2, ..., $m - 1$, то все числа разобьются на m *классов сравнений*, каждый из которых характеризуется своим вычетом. Совокупность m чисел, из которых каждое принадлежит к разному классу, образует так называемую *полную систему вычетов*.

Сравнения обладают многими свойствами обыкновенных равенств. Сравнения можно почленно складывать, вычитать, умножать, возводить в целую положительную степень. Доказательство этих предложений не представляет труда. Пусть

$$a \equiv b \pmod{m},$$
$$c \equiv d \pmod{m}. \qquad (2)$$

Следовательно, $a - b = mp$ и $c - d = mq$. Отсюда выводим:

$$(a - b) \pm (c - d) = m(p \pm q),$$
$$(a \pm c) - (b \pm d) = m(p \pm q),$$
$$a \pm c \equiv b \pm d \pmod{m}.$$

Путём умножения получаем

$$ac = bd + (dp + bq + mpq)m, \text{ или}$$
$$ac \equiv bd \pmod{m}.$$

Это свойство распространяется на любое число сравнений, и отсюда вытекает возможность возвышения обеих частей сравнения в степень. Так как каждое число сравнимо с самим собой, то из этого следует, что к обеим частям

сравнения можно прибавить (или отнять) одно и то же число, что обе части сравнения можно умножить на одно и то же число.

Что же касается деления, то соответствующая теорема формулируется так:

Обе части сравнения, имеющие общий делитель q, *взаимно простой* с модулем, можно разделить на q.

Покажем это. Пусть $a \equiv b \pmod m$, $a = q \cdot a_1$, $b = q \cdot b_1$ и q и m взаимно простые. Тогда, по условию, $qa_1 \equiv qb_1 \pmod m$; т. е. $q(a_1 - b_1)$ делится на m, а так как q и m взаимно простые, то $a_1 - b_1$ должно разделиться на m, т. е.

$$a_1 \equiv b_1 \pmod m.$$

Отсюда можно вывести следующую теорему о почленном делении сравнений. Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, a делится на c, а b делится на d и c (а следовательно, и d) взаимно простое с m, то сравнения можно почленно разделить одно на другое.

Пусть $a = ca_1$ и $b = db_1$. Умножая сравнение $ca_1 \equiv db_1 \pmod m$ почленно на сравнение $d \equiv c \pmod m$, получаем $cda_1 \equiv cdb_1 \pmod m$. Так как c и d взаимно простые с m, то и их произведение $c \cdot d$ взаимно простое с m. Сокращая последнее сравнение на $c \cdot d$, получаем $a_1 \equiv b_1 \pmod m$, что и требовалось доказать.

Докажем теперь следующее предложение. Пусть p — простое число. Покажем, что при любом a

$$a^p - a \equiv 0 \pmod p. \tag{3}$$

Доказательство проведём методом индукции. Сравнение, очевидно, верно при $a = 1$. Допустим, что оно имеет место при $a = m$:

$$m^p - m \equiv 0 \pmod p,$$

и покажем, что тогда оно будет справедливо и при $a = m + 1$.

В самом деле,

$$(m+1)^p - (m+1) = m^p - m + \frac{p}{1} m^{p-1} + \\ + \frac{p(p-1)}{1 \cdot 2} m^{p-2} + \ldots + pm.$$

Так как каждый из биномиальных коэффициентов делится на p (потому что p — простое, а в знаменателях

числа, меньшие p) и так как, по предположению, то же можно сказать и о $m^p - m$, то и всё выражение в правой части разделится на p, т. е.

$$(m+1)^p - (m+1) \equiv 0 \pmod{p}.$$

Теорема доказана.

Положим теперь, что a не делится на p (взаимно простое с p), тогда обе части сравнения (3) можно разделить на a. Получаем:

$$a^{p-1} - 1 \equiv 0 \pmod{p}. \tag{4}$$

Этим доказана так называемая *малая теорема Ферма.*

От тождественных сравнений переходим к сравнениям-уравнениям.

Если $f(x)$ — многочлен с целыми коэффициентами:

$$f(x) = c_0 x^n + c_1 x^{n-1} + \ldots + c_{n-1} x + c_n$$

и если a есть корень сравнения

$$f(x) \equiv 0 \pmod{p}, \tag{5}$$

т. е. если $f(a) \equiv 0 \pmod{p}$, то всякое число $b \equiv a \pmod{p}$ является тоже корнем сравнения (5).

В самом деле, из $a \equiv b \pmod{p}$ вытекает, что

$$a^n \equiv b^n, \quad a^{n-1} \equiv b^{n-1}, \quad \ldots \quad a \equiv b \pmod{p}.$$

Умножая эти сравнения на c_0, c_1, ..., c_{n-1} и почленно складывая, получаем:

$$c_0 a^n \equiv c_0 b^n, \quad c_1 a^{n-1} \equiv c_1 b^{n-1}, \quad \ldots, \quad c_{n-1} a \equiv c_{n-1} b, \quad c_n \equiv c_n \pmod{p},$$

$$c_0 a^n + c_1 a^{n-1} + \ldots + c_{n-1} a + c_n \equiv c_0 b^n + c_1 b^{n-1} + \ldots + c_{n-1} b + c_n \pmod{p},$$

т. е.

$$f(a) \equiv f(b) \pmod{p}$$

и, следовательно,

$$f(b) \equiv 0 \pmod{p}. \tag{6}$$

Два корня, принадлежащие к одному классу сравнений, мы не будем считать существенно отличными и скажем, что сравнение имеет корень:

$$x \equiv a \pmod{p}.$$

Рассмотрим двучленное сравнение

$$x^{p-1} - 1 \equiv 0 \pmod{p}. \tag{7}$$

По теореме Ферма все числа, взаимно простые с p, являются корнями этого сравнения. Следовательно, так как p — простое число, это сравнение имеет $p-1$ существенно различных корней:

$$x \equiv 1,\ x \equiv 2,\ \ldots,\ x \equiv p-1 \pmod{p}. \tag{8}$$

Других корней, очевидно, быть не может [$x \equiv 0 \pmod{p}$ корнем не является].

Корни двучленного сравнения (7) обладают свойствами, аналогичными свойствам корней двучленного уравнения $x^p - 1 = 0$. Пусть m — какой-либо коре сравнения (7), тогда числа

$$m,\ m^2,\ m^3,\ \ldots$$

являются также корнями этого сравнения; это следует из того, что обе части сравнения $m^{p-1} \equiv 1 \pmod{p}$ можно возвести в любую степень. Среди них есть сравнимые с $1 \pmod{p}$; таким во всяком случае будет m^{p-1}.

Если d наименьший показатель, при котором

$$m^d \equiv 1 \pmod{p},$$

то говорят, что число m принадлежит (по модулю p) к показателю d. Те числа, которые принадлежат к показателю $p-1$, т. е. те, которые удовлетворяют сравнению (7), но не удовлетворяют никакому двучленному сравнению $\pmod{p}$ низшей степени, назовём *первообразными корнями* сравнения (7) или просто *первообразными корнями числа* p.

Докажем следующее основное свойство первообразных корней. Пусть g — какой-либо первообразный корень числа p. Тогда ряд чисел

$$g,\ g^2,\ \ldots,\ g^{p-2},\ g^{p-1}\ [\equiv 1] \pmod{p} \tag{9}$$

представляет собой все корни сравнения (7). В самом деле, каждое из чисел (9) есть корень этого сравнения, и все они между собой не сравнимы, так как если допустить, что

$$g^k \equiv g^l \pmod{p}\ (k, l < p-1, \text{ и пусть } k > l),$$

то, деля обе части на g^l (взаимно простое с p), мы имели бы

$$g^{k-l} \equiv 1 \pmod{p},$$

и так как $k - l < p - 1$, то g не было бы первообразным корнем.

Таким образом, числа (9) представляют собой все корни (8) уравнения (7), а потому они сравнимы с числами 1, 2, ..., $p-1$ (взятыми, вообще говоря, в ином порядке) и составляют, следовательно, полную систему вычетов.

Примеры: 1) Для $p=5$ одним из первообразных корней будет $g=2$, так как 2 является корнем сравнения $x^4-1\equiv 0 \pmod 5$, но не удовлетворяет сравнениям низшей степени $x-1\equiv 0$, $x^2-1\equiv 0$, $x^3-1\equiv 0 \pmod 5$. Поэтому ряд чисел: $2, 2^2, 2^3, 2^4$ должен представлять все корни сравнения $x^4-1\equiv 0 \pmod 5$. Нетрудно видеть, что эти числа сравнимы (mod 5) с 2, 4, 3, 1.

2) Для $p=17$ за первообразный корень g можно взять 3. Тогда числа ряда
$g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}, g^{13}, g^{14}, g^{15}\ g^{16}\equiv 1$
будут сравнимы (mod 17) с числами от 1 до 16 (взятыми в следующем порядке):

3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1.

Выведем, наконец, ещё одно соотношение. Пусть g — первообразный корень простого числа $p(>2)$.

Следовательно,

$$g^{p-1}-1\equiv 0 \pmod p. \tag{10}$$

Разлагая левую часть на множители, имеем

$$\left(g^{\frac{p-1}{2}}-1\right)\left(g^{\frac{p-1}{2}}+2\right)\equiv 0 \pmod p,$$

$g^{\frac{p-1}{2}}-1$ не может делиться на p, так как тогда g принадлежало бы показателю $\frac{p-1}{2}$ и не было бы первообразным корнем. Следовательно, на p должно делиться $g^{\frac{p-1}{2}}+1$, а потому

$$g^{\frac{p-1}{2}}+1\equiv 0 \pmod p, \tag{11}$$

или

$$g^{\frac{p-1}{2}}\equiv -1 \pmod p.$$

Выведенными соотношениями мы впоследствии воспользуемся.

При этом заметим, что сравнение $g^k + 1 \equiv 0 \pmod{p}$, имеющее место, как показывает (11), при $k = \frac{p-1}{2}$, не удовлетворяется ни при каком другом значении k в пределах от 1 до p. В самом деле, из сравнений $g^k \equiv -1 \pmod{p}$ и $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, деля почленно одно на другое (делить можно, так как все корни сравнения (7), а следовательно, g и его любая степень взаимно простые с p), получаем: $g^{k-\frac{p-1}{2}} \equiv 1 \pmod{p}$ — в случае, когда $k > \frac{p-1}{2}$, либо $g^{\frac{p-1}{2}-k} \equiv 1 \pmod{p}$ — в случае, когда $k < \frac{p-1}{2}$. Но ни первое сравнение при $k \leqslant p$, ни второе сравнение не могут иметь места, так как g есть первообразный корень числа p.

2. Перейдём теперь к доказательству разрешимости в квадратных радикалах уравнения $x^p - 1 = 0$ в случае, когда p — простое число вида $2^m + 1$.

Когда p — простое число, то, как мы знаем, кроме $x = 1$, все остальные $p - 1$ корней двучленного уравнения $x^p - 1 = 0$ являются первообразными и совпадают с корнями полинома

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0. \qquad (12)$$

Если ε один из корней уравнения $\Phi_p(x) = 0$, то все корни могут быть представлены в виде

$$\varepsilon,\ \varepsilon^2,\ \varepsilon^3, \ldots, \varepsilon^{p-1}. \qquad (13)$$

Отсюда, между прочим, ясно, что если один из корней выражается в квадратных радикалах, то то же будет иметь место и в отношении всех остальных корней.

Метод Гаусса, которым мы воспользуемся, основывается на своеобразном порядке расположения корней (13). Пусть g — первообразный корень числа p. Тогда, как было выяснено, числа $1, g, g^2, \ldots, g^{p-2}$ образуют полную систему вычетов по модулю p, т. е. сравнимы с числами $1, 2, 3, \ldots, p-1$ (взятыми, вообще говоря, в другом порядке). С другой стороны, если два числа k и l сравнимы (mod p), то $\varepsilon^k = \varepsilon^l$; в самом деле, из $k \equiv l \pmod{p}$ следует, что $k = l + pt$, а потому $\varepsilon^k = \varepsilon^{l+pt} \equiv \varepsilon^l(\varepsilon^p)^t = \varepsilon^l$, так как $\varepsilon^p = 1$. Поэтому числа

$$\varepsilon,\ \varepsilon^g,\ \varepsilon^{g^2}, \ldots, \varepsilon^{g^{p-2}} \qquad (14)$$

представляют собой те же корни (13), но расположенные в ином порядке, именно в таком, что каждый последующий

корень представляет собой g-ю степень предшествующего (первый — ε_1 представляет собой g-ю степень последнего: $(\varepsilon^{g^{p-2}})^g = \varepsilon^{g^{p-1}} = \varepsilon$).

Из $p-1$ чисел (14) составим две следующие суммы по $\frac{p-1}{2}$ $\left(\frac{p-1}{2}\right.$ — число целое, так как $\left.p = 2^m + 1\right)$ слагаемых в каждой — два $\frac{p-1}{2}$ — *членных периода* (по терминологии Гаусса):

$$\begin{aligned}\eta_0 &= \varepsilon + \varepsilon^{g^2} + \varepsilon^{g^4} + \ldots + \varepsilon^{g^{p-3}}\\ \eta_1 &= \varepsilon^g + \varepsilon^{g^3} + \varepsilon^{g^5} + \ldots + \varepsilon^{g^{p-2}}.\end{aligned} \tag{15}$$

В этих суммах каждый член представляет g^2-ю степень от предшествующего.

Докажем следующее свойство этих периодов. Если в них произвести подстановку, взяв вместо ε какой-нибудь корень, входящий в состав η_0, то от такой подстановки оба периода η_0 и η_1 не изменятся; если же вместо ε подставить корень, входящий в период η_1, то η_0 превратится в η_1, а η_1 в η_0. Убедимся в этом. Подставим в η_0, а затем в η_1 вместо ε, например, ε^{g^2}. Тогда

$$\begin{aligned}\varepsilon^{g^2} + (\varepsilon^{g^2})^{g^2} + (\varepsilon^{g^2})^{g^4} + \ldots + (\varepsilon^{g^2})^{g^{p-3}} &= \varepsilon^{g^2} + \\ + \varepsilon^{g^4} + \varepsilon^{g^6} + \ldots + \varepsilon^{g^{p-1}} (= \varepsilon) &= \eta_0,\\ (\varepsilon^{g^2})^g + (\varepsilon^{g^2})^{g^3} + \ldots + (\varepsilon^{g^2})^{g^{p-2}} &=\\ = \varepsilon^{g^3} + \varepsilon^{g^5} + \ldots + \varepsilon^{g^p} (= \varepsilon^g) &= \eta_1.\end{aligned}$$

Оба периода остались без изменения; изменился только порядок слагаемых. То же будет, если подставить любой другой корень $\varepsilon^{g^{2s}}$, принадлежащий η_0.

Подставим теперь вместо ε какой-нибудь корень, входящий в η_1, например ε^{g^3}. Получим:

$$\begin{aligned}\varepsilon^{g^3} + (\varepsilon^{g^3})^{g^2} + \ldots + (\varepsilon^{g^3})^{g^{p-3}} &= \varepsilon^{g^3} + \varepsilon^{g^5} + \ldots + \varepsilon^{g^p} = \eta_1\\ (\varepsilon^{g^3})^g + (\varepsilon^{g^3})^{g^3} + \ldots + (\varepsilon^{g^3})^{g^{p-2}} &=\\ = \varepsilon^{g^4} + \varepsilon^{g^6} + \ldots + \varepsilon + \varepsilon^{g^2} &= \eta_0.\end{aligned}$$

Мы видим, что η_0 перешло в η_1, а η_1 — в η_0. То же произойдёт при всякой подстановке $\varepsilon \to \varepsilon^{g^{2s+1}}$.

Заметим, что периоды η_0 и η_1 различны по своей величине. Если предположить, что $\eta_0 = \eta_1$, т. е. что

$$\varepsilon + \varepsilon^{g^2} + \ldots + \varepsilon^{g^{p-3}} = \varepsilon^g + \varepsilon^{g^3} + \ldots + \varepsilon^{g^{p-2}},$$

то, заменяя в этом равенстве степени g их вычетами и сократив на ε, мы получим уравнение $(p-2)$-й степени, которому удовлетворяет ε; этого, однако, быть не может, так как ε является корнем неприводимого уравнения (12) $(p-1)$-й степени. Следовательно, $\eta_0 \neq \eta_1$.

Мы постараемся теперь показать, что *периоды* η_0 и η_1 *являются корнями квадратного уравнения с целыми коэффициентами.*

Прежде всего замечаем, что

$$\eta_0 + \eta_1 = -1, \tag{16}$$

так как сумма $\eta_0 + \eta_1$ есть сумма всех корней полинома (12), у которого коэффициент при x^{p-1} равен единице[1].

Далее составим произведение $\eta_0 \cdot \eta_1$:

$$\eta_0 \cdot \eta_1 = (\varepsilon + \varepsilon^{g^2} + \varepsilon^{g^4} + \ldots + \varepsilon^{g^{p-3}}) \times \\ \times (\varepsilon^{g} + \varepsilon^{g^3} + \varepsilon^{g^5} + \ldots + \varepsilon^{g^{p-2}}).$$

Умножение будем выполнять следующим образом: все члены первой строки сначала умножим на находящиеся непосредственно под ними члены второй строки, затем на находящиеся на один член правее, на два члена правее и т. д., дополняя недостающие с противоположного конца (пользуясь при этом соотношениями: $\varepsilon^g = \varepsilon^{g^p}$, $\varepsilon^{g^3} = \varepsilon^{g^{p+2}}$ и т. д.).

Получим следующее выражение:

$$\begin{aligned}
\eta_0 \cdot \eta_1 = {} & \varepsilon^{1+g} + \varepsilon^{(1+g)g^2} + \varepsilon^{(1+g)g^4} + \ldots + \varepsilon^{(1+g)g^{p-3}} + \\
& + \varepsilon^{1+g^3} + \varepsilon^{(1+g^3)g^2} + \varepsilon^{(1+g^3)g^4} + \ldots + \varepsilon^{(1+g^3)g^{p-3}} + \\
& + \varepsilon^{1+g^5} + \varepsilon^{(1+g^5)g^2} + \ldots + \varepsilon^{(1+g^5)g^{p-3}} + \\
& \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
& + \varepsilon^{1+g^{p-2}} + \varepsilon^{(1+g^{p-2})g^2} + \ldots + \varepsilon^{(1+g^{p-2})g^{p-3}}.
\end{aligned} \tag{17}$$

В каждой из $\frac{p-1}{2}$ горизонтальных строк находится сумма, представляющая собой результат подстановки в период η_0 вместо ε одного из $\frac{p-1}{2}$ чисел:

---

[1] Или так: корни (14) это те же корни (13): но ε есть корень полинома (12), а потому

$$\varepsilon^{p-1} + \varepsilon^{p-2} + \ldots + \varepsilon + 1 = 0,$$

или

$$\varepsilon^{p-1} + \varepsilon^{p-2} + \ldots + \varepsilon = -1.$$

$$\varepsilon^{1+g},\quad \varepsilon^{1+g^3},\quad \varepsilon^{1+g^5},\ \ldots,\ \varepsilon^{1+g^{p-2}}. \tag{18}$$

Каждое из чисел (18), представляя собой степень ε, является корнем полинома (12); исключение могло бы представиться лишь в том случае, если бы некоторые числа обратились в 1. Это могло бы иметь место при условии

$$1 + g^{2t+1} \equiv 0 \pmod{p}.$$

Но это сравнение не может иметь места, потому что, как мы видели, сравнение $1 + g^k \equiv 0 \pmod{p}$ может иметь место лишь при $k = \frac{p-1}{2}$; но $2t + 1$ не может равняться $\frac{p-1}{2}$, так как $\frac{p-1}{2}$ есть число чётное. Поэтому ни одно из чисел (18) не равно единице и, следовательно, все они являются корнями полинома (12), а потому входят либо в состав периода η_0, либо η_1. В первом случае результат подстановки даёт η_0 и, следовательно, соответствующая строка в (17) равна η_0, во втором случае она будет равна η_1. Если m_0 чисел из ряда (18) принадлежат η_0, а остальные m_1 периоду η_1, то наше произведение $\eta_0 \cdot \eta_1$ примет следующий вид:

$$\eta_0 \cdot \eta_1 = m_0\eta_0 + m_1\eta_1, \tag{19}$$

причём $m_0 + m_1 = \frac{p-1}{2}$. Произведение η_0 на η_1 представляет, таким образом, их линейную однородную функцию с целыми коэффициентами. Мы покажем, более того, что $m_0 = m_1$.

Для этого составим то же произведение периодов η_0 и η_1, но будем множить η_1 на η_0 (умножение будем производить тем же методом, что и выше, но только при получении первой горизонтальной строки вместо чисел ε, ε^{g^2}, ..., $\varepsilon^{g^{p-2}}$ возьмём равные им $\varepsilon^{g^{p-1}}$, $\varepsilon^{g^{p+1}}$, ..., $\varepsilon^{g^{2p-3}}$).

$$\eta_1 \cdot \eta_0 = (\varepsilon^g + \varepsilon^{g^3} + \varepsilon^{g^5} + \ldots + \varepsilon^{g^{p-2}}) \times$$
$$\times (\varepsilon + \varepsilon^{g^2} + \varepsilon^{g^4} + \ldots + \varepsilon^{g^{p-3}}) =$$
$$= \varepsilon^{(1+g^{p-2})g} + \varepsilon^{(1+g^{p-2})g^3} + \ldots + \varepsilon^{(1+g^{p-2})g^{p-2}} +$$
$$+ \varepsilon^{(1+g)g^2} + \varepsilon^{(1+g)g^3} + \ldots + \varepsilon^{(1+g)g^{p-2}} +$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$+ \varepsilon^{(1+g^{p-4})g} + \varepsilon^{(1+g^{p-4})g^3} + \ldots + \varepsilon^{(1+g^{p-4})g^{p-2}}.$$

Полученное произведение представляет собой результат подстановки тех же чисел (18), но уже в период η_1.

Так как по предположению m_0 из чисел (18) принадлежат периоду η_0, а m_1 — периоду η_1, то

$$\eta_1 \cdot \eta_0 = m_0 \cdot \eta_1 + m_1 \cdot \eta_0. \qquad (20)$$

Сравнивая (19) и (20), находим

$$m_0\eta_0 + m_1\eta_1 = m_0\eta_1 + m_1\eta_0,$$

или

$$(m_0 - m_1)(\eta_0 - \eta_1) = 0. \qquad (21)$$

И так как $\eta_0 \neq \eta_1$, то $m_0 - m_1 = 0$, т. е. $m_0 = m_1$.

И так как сумма их $m_0 + m_1 = \frac{p-1}{2}$, то $m_0 = m_1 = \frac{p-1}{4}$.

Следовательно,

$$\eta_0 \cdot \eta_1 = m_0(\eta_0 + \eta_1) = \frac{p-1}{4}(-1) = -\frac{p-1}{4}.$$

Итак,

$$\eta_0 \cdot \eta_1 = -\frac{p-1}{4}. \qquad (22)$$

Отсюда и из (16) следует, что η_0 и η_1 служат корнями квадратного уравнения

$$z^2 + z - \frac{p-1}{4} = 0. \qquad (23)$$

Откуда

$$z = \frac{-1 \pm \sqrt{p}}{2}$$

и, следовательно[1],

$$\eta_0 = \frac{-1+\sqrt{p}}{2}, \qquad \eta_1 = \frac{-1-\sqrt{p}}{2} \qquad (24)$$

Таким образом, мы не только показали, что η_0 и η_1 являются корнями квадратного уравнения с целыми коэффициентами, но и вычислили их значения.

Теперь возьмём $\frac{p-1}{2}$-членные периоды η_0 и η_1 и каждый из них разобьём на два периода с вдвое меньшим числом членов:

$$\begin{aligned}
\eta_0' &= \varepsilon + \varepsilon^{g^4} + \varepsilon^{g^8} + \ldots + \varepsilon^{g^{p-5}},\\
\eta_2' &= \varepsilon^{g^2} + \varepsilon^{g^6} + \varepsilon^{g^{10}} + \ldots + \varepsilon^{g^{p-3}},\\
\eta_1' &= \varepsilon^{g} + \varepsilon^{g^5} + \varepsilon^{g^9} + \ldots + \varepsilon^{g^{p-4}},\\
\eta_3' &= \varepsilon^{g^3} + \varepsilon^{g^7} + \varepsilon^{g^{11}} + \ldots + \varepsilon^{g^{p-2}}. \qquad (25)
\end{aligned}$$

[1] От нас зависит, какой корень уравнения (23) принять за η_0 и какой за η_1. Это связано лишь с выбором первообразного корня ε, который был взят произвольно. Мы примем $\eta_0 > 0$ и $\eta_1 < 0$.

Все корни данного уравнения, таким образом, распределены между четырьмя $\frac{p-1}{4}$-членными периодами, причём

$$\eta'_0 + \eta'_2 = \eta_0 \text{ и } \eta'_1 + \eta'_3 = \eta_1. \quad (26)$$

В каждом из периодов (25) последующий член представляет g^4-ю степень предшествующего. Периоды (25) аналогично $\frac{p-1}{2}$-членным периодам обладают свойством: при подстановке в них вместо ε какого-нибудь корня, входящего в состав периода η'_0, все 4 периода не изменяются; при подстановке вместо ε корня, принадлежащего периоду η'_1, η'_0 переходит в η'_1, η'_1 в η'_2, η'_2 в η'_3 и η'_3 в η'_0; при подстановке корня, принадлежащего периоду η'_2, η'_0 переходит в η'_2, η'_1 — в η'_3 и т. д. в циклическом порядке. В правильности этого можно убедиться непосредственной подстановкой. Докажем теперь следующее свойство этих периодов: *каждая пара периодов* η'_0 *и* η'_2 *и* η'_1, η'_3 *удовлетворяет квадратному уравнению, коэффициентами которого служат рациональные функции от периодов* η_0 и η_1.

Возьмём, положим, пару η'_0 и η'_2. Относительно них нам известно (26), что сумма их равна η_0. Составим теперь произведение $\eta'_0 \cdot \eta'_2$. Умножение будем производить указанным выше способом.

$$\begin{aligned}
\eta'_0\eta'_2 &= (\varepsilon + \varepsilon^{g^4} + \varepsilon^{g^8} + \ldots + \varepsilon^{g^{p-5}}) \times \\
&\times (\varepsilon^{g^2} + \varepsilon^{g} + \varepsilon^{g^{10}} + \ldots + \varepsilon^{g^{p-3}}) = \\
&= \varepsilon^{1+g^2} + \varepsilon^{(1+g^2)g^4} + \varepsilon^{(1+g^2)g^8} + \ldots + \varepsilon^{(1+g^2)g^{p-5}} + \\
&+ \varepsilon^{1+g^6} + \varepsilon^{(1+g^6)g^4} + \ldots + \varepsilon^{(1+g^6)g^{p-5}} + \ldots + \\
&+ \varepsilon^{1+g^{p-3}} + \varepsilon^{(1+g^{p-3})g^4} + \ldots + \varepsilon^{(1+g^{p-3})g^{p-5}}. \quad (27)
\end{aligned}$$

В полученном выражении каждая из $\frac{p-1}{4}$ горизонтальных строк представляет собой результат подстановки в период η'_0 вместо ε одного из чисел

$$\varepsilon^{1+g^2}, \quad \varepsilon^{1+g^6}, \quad \ldots, \quad \varepsilon^{1+g^{p-3}}, \quad (28)$$

являющихся, как степени ε, корнями уравнения (12) и потому входящих в состав того или другого периодов (14). [Ни одно из чисел (27) не обращается в 1, так как для этого было бы необходимо, чтобы $1 + g^{2(2l+1)} \equiv 0 \pmod{p}$,

а это сравнение удовлетворяется лишь при показателе степени, равном $\frac{p-1}{2}$, но $\frac{p-1}{2}$ делится на 4, а $2(2t+1)$ ни при каком t на 4 не делится.] Поэтому каждая из горизонтальных строк в равенстве (27) оказывается равной некоторому η'.

Если предположить, что среди $\frac{p-1}{4}$ чисел (28) m'_0 принадлежат периоду η'_0, m'_1 — периоду η'_1, m'_2 — периоду η'_2 и m'_3 — периоду η'_3, то равенство (27) примет вид

$$\eta'_0 \cdot \eta'_2 = m'_0 \cdot \eta'_0 + m'_1 \cdot \eta'_1 + m'_2 \cdot \eta'_2 + m'_3 \cdot \eta'_3. \quad (29)$$

Покажем, что $m'_0 = m'_2$ и $m'_1 = m'_3$.

Для этого составим произведение тех же периодов η'_0 и η'_2, умножая η'_2 на η'_0, при этом получим $\frac{p-1}{4}$ горизонтальных строк, каждая из которых будет представлять собой результат подстановки тех же чисел (28) в период η'_2. Тогда, согласно отмеченному выше свойству этих периодов, от подстановки m'_0 корней, принадлежащих периоду η'_0, мы получим m'_0 строк, равных каждая η'_2; от подстановки m'_1 корней, входящих в состав периода η'_1, получим m'_1 строк, равных η'_3, и т. д. в циклическом порядке. Окончательно получим:

$$\eta'_2 \cdot \eta'_0 = m'_0 \cdot \eta'_2 + m'_1 \eta'_3 + m'_2 \cdot \eta'_0 + m'_3 \cdot \eta'_1. \quad (30)$$

Сравнивая (29) и (30), получаем:

$$m'_0 \eta'_0 + m'_1 \eta'_1 + m'_2 \eta'_2 + m'_3 \eta'_3 = m'_0 \eta'_2 + m'_1 \eta'_3 + m'_2 \eta'_0 + m'_3 \eta'_1,$$

или

$$(m'_0 - m'_2)\eta'_0 + (m'_1 - m'_3)\eta'_1 = (m'_0 - m'_2)\eta'_2 + (m'_1 - m'_3)\eta'_3,$$

откуда

$$(m'_0 - m'_2)(\eta'_0 - \eta'_2) + (m'_1 - m'_3)(\eta'_1 - \eta'_3) = 0. \quad (31)$$

Если предположить, что какой-нибудь из коэффициентов $m'_0 - m'_2$ либо $m'_1 - m'_3$ в равенстве (31) отличен от нуля, то мы бы имели, подставляя вместо η' их значения и упрощая, соотношение (с рациональными коэффициентами) не выше $(p-2)$-й степени, которому удовлетворяло бы ε. А этого быть не может в силу неприводимости многочлена (12). Итак,

$m'_0 - m'_2 = 0$ и $m'_1 - m'_3 = 0$, т. е. $m'_0 = m'_2$ и $m'_1 = m'_3$.

Поэтому из (29) получаем

$$\eta'_0\eta'_2 = m'_0(\eta'_0 + \eta'_2) + m'_1(\eta'_1 + \eta'_3)$$

и, принимая во внимание (26), окончательно имеем

$$\eta'_0\eta_2' = m'_0\eta'_0 + m'_1\eta_1. \tag{32}$$

А отсюда и из (26) следует, что η'_0 и η'_2 являются корнями квадратного уравнения

$$z^2 - \eta_0 z + (m'_0\eta_0 + m'_1\eta_1) = 0 \tag{33}$$

с коэффициентами, рационально зависящими от η_0 и η_1.

Совершенно то же можно было бы показать и для другой пары периодов η'_1 и η'_3.

Процесс образования периодов со вдвое меньшим числом членов продолжаем дальше. Составляем $\frac{p-1}{8}$-членные периоды и так же, как выше, показываем, что они являются корнями квадратного уравнения, коэффициенты которого рациональным образом зависят от $\frac{p-1}{4}$-членных периодов, и т. д. В результате, так как $p - 1 = 2^m$, после $(m - 1)$-го деления мы получим двучленные периоды, каждый из которых будет являться корнем квадратного уравнения с коэффициентами, рационально зависящими от предшествующих (четырёхчленных) периодов. Таков будет, в частности, первый из двучленных периодов:

$$\eta_0^{(m-1)} = \varepsilon + \varepsilon^{g^{\frac{p-1}{2}}}. \tag{34}$$

Замечая, что $g^{\frac{p-1}{2}} \equiv -1 \pmod p$ и обозначая для краткости $\eta_0^{(m-1)}$ через ξ, получаем

$$\varepsilon + \varepsilon^{-1} = \xi$$

или, окончательно,

$$\varepsilon^2 - \xi\varepsilon + 1 = 0. \tag{35}$$

ε, следовательно, определится как корень этого последнего квадратного уравнения.

Таким образом, доказано, что ε находится путём последовательного решения цепи квадратных уравнений.

Первообразный корень ε двучленного уравнения $x^p - 1 = 0$ (в случае, когда простое $p = 2^m + 1$), а следовательно, и все корни этого уравнения выражаются, как

мы видим, *в квадратных радикалах и могут поэтому быть построены циркулем и линейкой.*

3. Сделаем теперь несколько замечаний по поводу простых чисел вида

$$p = 2^m + 1.$$

Прежде всего заметим, что число $2^m + 1$ может быть простым лишь в том случае, если показатель m сам есть степень двойки. Если бы это было не так, то m делилось бы на *нечётное* число q (< 1):

$$m = q \cdot s.$$

Но тогда

$$p = 2^m + 1 = 2^{qs} + 1 = (2^s)^q + 1,$$

и так как q — нечётное, то (сумма нечётных степеней делится на сумму оснований):

$$p = (2^s)^q + 1 = (2^s + 1)(2^{s(q-1)} - 2^{s(q-2)} + \ldots \pm 1).$$

p, следовательно, не было бы простым числом.

Поэтому $m = 2^k$ и, следовательно,

$$p = 2^{2^k} + 1. \qquad (36)$$

Однако не всякое число вида (36) является простым. Простые числа получим при $k = 0, 1, 2, 3, 4$:

$$3, 5, 17, 257, 65\,537$$

Простые числа (36) для $k > 4$ неизвестны. Уже при $k = 5$ формула (36) даёт, как показал Эйлер, составное число;

$$p = 2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,267$$

делится на 641. Число $2^{2^6} + 1 = 2^{64} + 1$ тоже составное (делится на 274 177).

Исследованиями, ведшимися до настоящего времени, установлено, что составные числа получаются также при $k = 7, 8, 9, 11, 12, 15, 18, 23, 36, 38, 73$. Для каждого из них (кроме случаев $k = 7,8$) найден один делитель; так, $2^{2^{73}} + 1$ делится на простое число $5 \cdot 2^{75} + 1$[1].

4. Рассмотрим теперь в качестве примера сначала уравнение $x^5 - 1 = 0$.

$$p = 5 = 2^2 + 1; \quad \Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

Один из первообразных корней 5 есть, как мы видели выше, $g = 2$ и потому

$$g, g^2, g^3, g^4$$

[1] См. Э. Трост, Простые числа, М., 1959, стр. 46—48.

сравнимы (mod 5) с

$$2,\ 4,\ 3,\ 1.$$

Поэтому

$$\eta_0 = \varepsilon + \varepsilon^4 \text{ и } \eta_1 = \varepsilon^2 + \varepsilon^3.$$

Периоды η_0 и η_1 найдутся сразу по формулам

$$\eta_0 = \frac{-1+\sqrt{5}}{2}, \quad \eta_1 = \frac{-1-\sqrt{5}}{2}.$$

Замечая, что $\varepsilon^4 = \varepsilon^{-1}$, пишем

$$\varepsilon + \varepsilon^{-1} = \frac{-1+\sqrt{5}}{2},$$

или

$$2\varepsilon^2 + (1-\sqrt{5})\varepsilon + 2 = 0.$$

Откуда (взяв, например, положительное значение корня)

$$\varepsilon = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

Остальные корни уравнения $x^5 - 1 = 0$ будут ε^2, ε^3, ε^4, $(\varepsilon^5 = 1)$.

Для деления окружности на 5 равных частей (построения правильного пятиугольника) можно поступить так. Возьмём решение уравнения $x^5 - 1 = 0$ в тригонометрической форме:

$$\varepsilon(=\varepsilon_1) = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5},$$

$$\varepsilon^2 = \cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5},$$

$$\varepsilon^3 = \cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5} = \cos\frac{4\pi}{5} - i\sin\frac{4\pi}{5},$$

$$\varepsilon^4 = \cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5} = \cos\frac{2\pi}{5} - i\sin\frac{2\pi}{5}.$$

Отсюда

$$\eta_0 = \varepsilon + \varepsilon^4 = 2\cos\frac{2\pi}{5}, \ \eta_1 = \varepsilon^2 + \varepsilon^3 = 2\cos\frac{4\pi}{5}.$$

И. следовательно, в частности,

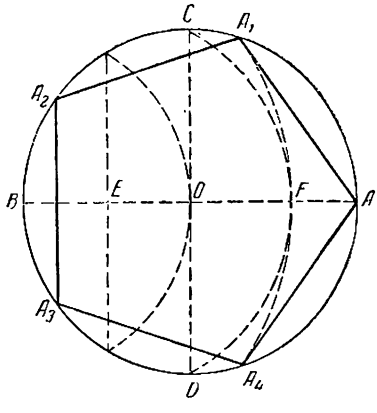
$$\cos\frac{4\pi}{5} = \frac{\eta_1}{2} = \frac{-1-\sqrt{5}}{4}.$$

Тогда

$$\cos\frac{\pi}{5} = \cos\left(\pi - \frac{4\pi}{5}\right) = -\cos\frac{4\pi}{5} = \frac{1+\sqrt{5}}{4}.$$

Из последнего равенства вытекает следующий способ построения правильного пятиугольника (черт. 5).

Берём окружность и проводим два взаимно перпендикулярных диаметра AB и CD. Радиус OB делим в точке E пополам. Проводим дугу с центром в точке E радиусом EC, пересекающую диаметр в точке F. Затем радиусом, равным BF, с центром в точке B делаем засечку A_1 на окружности.



Черт. 5.

Дуга AA_1 есть $\frac{1}{5}$ часть окружности $-\frac{2\pi}{5}$.

Действительно,

$$OE = \frac{1}{2};$$

$$EC = \sqrt{\frac{1}{4} + 1} = \frac{\sqrt{5}}{2};$$

$$EF = EC;$$

$$BA_1 = BF = BE + EF = \frac{1 + \sqrt{5}}{2}.$$

Из треугольника ABA_1

$$\cos \angle ABA_1 = \frac{BA_1}{BA} = \frac{\frac{1+\sqrt{5}}{2}}{2} = \frac{1+\sqrt{5}}{4} = \cos\frac{\pi}{5};$$

таким образом, $\angle ABA_1 = \frac{\pi}{5}$, а потому центральный

$$\angle AOA_1 = \frac{2\pi}{5}.$$

Откладывая по окружности дугу AA_1, строим искомый пятиугольник $AA_1A_2A_3A_4$.

Кроме изложенного, существуют, как известно, и другие способы построения правильного пятиугольника.

Рассмотрим в качестве второго примера уравнение $x^{17} - 1 = 0$. Для $p = 17$ одним из первообразных корней служит $g = 3$.

Числа:

$1, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}, g^{13}, g^{14}, g^{15}$

сравнимы, как мы видели, с числами:

1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6.

Составляем два $\frac{p-1}{2} = 8$-членных периода.

$$\eta_0 = \varepsilon + \varepsilon^9 + \varepsilon^{13} + \varepsilon^{15} + \varepsilon^{16} + \varepsilon^8 + \varepsilon^4 + \varepsilon^2,$$
$$\eta_1 = \varepsilon^3 + \varepsilon^{10} + \varepsilon^5 + \varepsilon^{11} + \varepsilon^{14} + \varepsilon^7 + \varepsilon^{12} + \varepsilon^6.$$

η_0 и η_1 могут быть определены по формуле (23) как корни уравнения[1]:

$$x^2 - x - 4 = 0.$$

Какой корень этого уравнения принять за η_0 и какой за η_1? Это зависит от выбора ε. Если за ε принять первый корень, т. е. $\varepsilon = \varepsilon_1 = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$, то нетрудно видеть, что $\eta_0 > 0$, а $\eta_1 < 0$. В самом деле, заменяя ε^{17-k} через ε^{-k} и замечая, что $\varepsilon^k + \varepsilon^{-k} = 2\cos\frac{2k\pi}{17}$, видим, что $\eta_1 = 2\cos\frac{6\pi}{17} + 2\cos\frac{10\pi}{17} + 2\cos\frac{12\pi}{17} + 2\cos\frac{14\pi}{17} < 0$, так как здесь 3 слагаемых отрицательны и лишь одно $2\cos\frac{6\pi}{17} > 0$, но уже $2\cos\frac{14\pi}{17} = -2\cos\frac{3\pi}{17}$ по своей абсолютной величине больше, чем $2\cos\frac{6\pi}{17}$.

Поэтому $\eta_0 = \frac{-1+\sqrt{17}}{2}$, $\eta_1 = \frac{-1-\sqrt{17}}{2}$.

Далее составляем четырёхчленные периоды:

$$y_0 = \varepsilon + \varepsilon^{13} + \varepsilon^{16} + \varepsilon^4,$$
$$y_1 = \varepsilon^9 + \varepsilon^{15} + \varepsilon^8 + \varepsilon^2,$$
$$y_2 = \varepsilon^3 + \varepsilon^5 + \varepsilon^{14} + \varepsilon^{12},$$
$$y_3 = \varepsilon^{10} + \varepsilon^{11} + \varepsilon^7 + \varepsilon^6.$$

При этом

$$y_0 + y_1 = \eta_0, \text{ а } y_2 + y_3 = \eta_1.$$

---

[1] Если готовой формулой не пользоваться, то сразу видим, что $\eta_0 + \eta_1 = -1$, и непосредственным вычислением убеждаемся, что $\eta_0 \cdot \eta_1 = -4$.

Составляем произведение y_0 на y_1.

$$y_0 \cdot y_1 = \varepsilon^{10} + \varepsilon^{11} + \varepsilon^7 + \varepsilon^6 + \varepsilon^{16} + \varepsilon^4 + \varepsilon + \varepsilon^{13} + \varepsilon^9 + \varepsilon^{15} + \varepsilon^8 + \varepsilon^2 + \varepsilon^3 + \varepsilon^5 + \varepsilon^{14} + \varepsilon^{12} = y_3 + y_0 + y_1 + y_2 = -1.$$

Поэтому y_0 и y_1 — корни квадратного уравнения

$$y^2 - \eta_0 y - 1 = 0.$$

Корни этого уравнения разных знаков. За y_0 нужно взять положительный корень, потому что $y_0 = \varepsilon + \varepsilon^{-1} + \varepsilon^4 + \varepsilon^{-4} = 2\cos\frac{2\pi}{17} + 2\cos\frac{8\pi}{17} > 0$. Следовательно,

$$y_0 = \frac{\eta_0 + \sqrt{\eta_0^2 + 4}}{2}.$$

Составляя произведение y_2 на y_3, убеждаемся, что и $y_2 \cdot y_3 = -1$. А так как $y_2 + y_3 = \eta_1$, то y_2 и y_3 удовлетворяют квадратному уравнению

$$y^2 - \eta_1 y - 1 = 0.$$

За y_2 нужно принять положительный корень этого уравнения, так как

$$y_2 = \varepsilon^3 + \varepsilon^{-3} + \varepsilon^5 + \varepsilon^{-5} = 2\cos\frac{6\pi}{17} + 2\cos\frac{10\pi}{17} = 2\cos\frac{6\pi}{17} - 2\cos\frac{7\pi}{17} > 0.$$

Следовательно, $$y_2 = \frac{\eta_1 + \sqrt{\eta_1^2 + 4}}{2}.$$

Составляем, наконец, двучленные периоды:

$$z_0 = \varepsilon + \varepsilon^{16};\ z_1 = \varepsilon^{13} + \varepsilon^4;\ z_2 = \varepsilon^9 + \varepsilon^8;\ z_3 = \varepsilon^{15} + \varepsilon^2;$$
$$z_4 = \varepsilon^3 + \varepsilon^{14};\ z_5 = \varepsilon^5 + \varepsilon^{12};\ z_6 = \varepsilon^{10} + \varepsilon^7;\ z_7 = \varepsilon^{11} + \varepsilon^6.$$

Нам достаточно взять два первых периода z_0 и z_1.

Сумма их

$$z_0 + z_1 = y_0.$$

Составляем произведение z_0 на z_1:

$$z_0 \cdot z_1 = \varepsilon^{14} + \varepsilon^5 + \varepsilon^{12} + \varepsilon^3 = y_2.$$

Следовательно, z_0 и z_1 — корни квадратного уравнения

$$z^2 - y_0 z + y_2 = 0.$$

Корни этого уравнения одного знака, но легко видеть, что

$$z_0 > z_1,$$

так как

$$z_0 = 2\cos\frac{2\pi}{17}, \quad \text{а } z_1 = 2\cos\frac{8\pi}{17}.$$

Поэтому

$$z_0 = \frac{y_0 + \sqrt{y_0^2 - 4y_2}}{2}.$$

И, наконец, чтобы найти ε, составляем уравнение

$$\varepsilon + \varepsilon^{-1} = z_0,$$

или

$$\varepsilon^2 - z_0\varepsilon + 1 = 0.$$

ε найдётся как корень этого уравнения: $\varepsilon = \frac{z_0 + \sqrt{z_0^2 - 4}}{2}$; перед корнем берём знак $+$, потому что $z_0 = 2\cos\frac{2\pi}{17}$ и, следовательно, $\varepsilon = \frac{z_0}{2} + \sqrt{\left(\frac{z_0}{2}\right)^2 - 1} = \frac{z_0}{2} +$

$$+ i\sqrt{1 - \left(\frac{z_0}{2}\right)^2} = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}.$$

Переходим теперь к самому построению правильного семнадцатиугольника. Нам, следовательно, придётся построить следующие пять отрезков:

$$\eta_0 = \frac{\sqrt{17}}{2} - \frac{1}{2}; \quad \eta_1 = -\frac{\sqrt{17}}{2} - \frac{1}{2},$$

$$y_0 = \frac{\eta_0}{2} + \sqrt{\left(\frac{\eta_0}{2}\right)^2 + 1},$$

$$y_2 = \frac{\eta_1}{2} + \sqrt{\left(\frac{\eta_1}{2}\right)^2 + 1}$$

$$\text{и } z_0 = \frac{y_0}{2} + \sqrt{\left(\frac{y_0}{2}\right)^2 - y_2}$$

($\frac{z_0}{2} = \cos\frac{2\pi}{17}$; поэтому самое ε для построения не потребуется).

Построение производим следующим образом (черт. 6). Берём окружность радиуса, равного 1, и проводим два вза-

имно перпендикулярных диаметра AB и CD. За положительное направление по горизонтальной оси примем от A к B, так что вправо от O будем откладывать отрицательные отрезки. Радиус OA делим на четыре части и строим

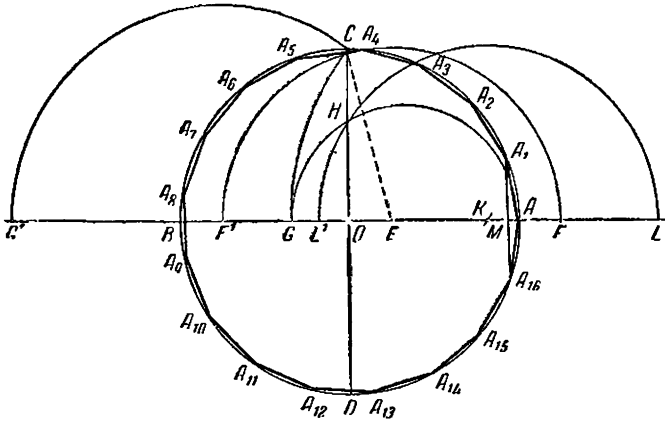
$$OE = -\frac{1}{4};$$

тогда

$$EC = \sqrt{OC^2 + OE^2} = \sqrt{1 + \frac{1}{16}} = \frac{\sqrt{17}}{4}.$$

Из E как из центра радиусом, равным EC, делаем на горизонтальной прямой засечки F и F', так что

$$EF = -\frac{\sqrt{17}}{4} \text{ и } EF' = \frac{\sqrt{17}}{4}.$$



Черт. 6.

Затем из точек F и F' соответственно радиусам и FC и $F'C$ делаем засечки G и G'.

Тогда

$$OF = OE + EF = -\frac{1}{4} - \frac{\sqrt{17}}{4} = \frac{\eta_1}{2},$$

$$OF' = OE + EF' = -\frac{1}{4} + \frac{\sqrt{17}}{4} = \frac{\eta_0}{2},$$

$$OG = OF + FG = OF + FC = \frac{\eta_1}{2} + \sqrt{\left(\frac{\eta_1}{2}\right)^2 + 1} = y_2,$$

$$OG' = OF' + F'G' = OF' + F'C = \frac{\eta_0}{2} + \sqrt{\left(\frac{\eta_0}{2}\right)^2 + 1} = y_0.$$

Далее на AG как на диаметре строим полуокружность, которая пересекает радиус OC в точке H, и из точки H

делаем засечку K радиусом $HK = \frac{OG'}{2}$. Затем из точки K радиусом HK делаем засечки L и L'.
Тогда

$$LO + OL' = LL' = 2KH = OG' = y_0,$$
$$LO \cdot OL' = OH^2 = AO \cdot OG = OG = y_2. \quad .$$

Следовательно, LO и OL' — корни уравнения (24) и потому совпадают с z_0 и z_1, и так как $LO > OL'$, то

$$LO = z_0.$$

Деля LO пополам, получаем

$$MO = \frac{LO}{2} = \frac{z_0}{2} = \cos\frac{2\pi}{17}.$$

Восставляем в точке M перпендикуляр, который пересекает окружность в искомой точке A_1 (и A_{16}). Дуга $AA_1 = \frac{2\pi}{17}$.

Откладывая эту дугу по окружности, строим правильный семнадцатиугольник.

5. Выше мы убедились в том, что при помощи циркуля и линейки можно разделить окружность на p частей, где p — гауссово простое число.

Мы покажем теперь, что задача деления окружности на n частей выполнима для всякого n, имеющего вид

$$n = 2^\alpha \cdot p_1 p_2 \cdot \ldots \cdot p_k,$$

где p_i — различные простые числа вида $2^m + 1$.

Для этого докажем сначала следующее предложение.

Если окружность может быть разделена (циркулем и линейкой) на α и на β частей и если α и β — числа взаимно простые, то окружность можно разделить и на $\alpha \cdot \beta$ частей. В самом деле, так как $(\alpha, \beta) = 1$, то можно подобрать два таких целых числа a и b, что

$$\alpha \cdot a + \beta \cdot b = 1.$$

Деля на $n = \alpha \cdot \beta$, получаем

$$\frac{1}{n} = \frac{a}{\beta} + \frac{b}{\alpha}.$$

Чтобы построить $\frac{1}{n}$-ю часть окружности, нужно, следовательно, a раз взять $\frac{1}{\beta}$-ю часть и b раз $\frac{1}{\alpha}$-ю часть

и сложить (вычесть); всё это выполнимо циркулем и линейкой.

Например, чтобы разделить окружность на 15 равных частей ($n = 15 = 3 \cdot 5$), замечаем, что

$$(-3) \cdot 3 + 2 \cdot 5 = 1$$

и

$$\frac{1}{15} = \frac{2}{3} - \frac{3}{5}.$$

Таким образом, мы получим $\frac{1}{15}$ часть окружности, если из $\frac{2}{3}$ вычтем $\frac{3}{5}$ её части.

Точно так же для деления на 170 частей замечаем, что $170 = 17 \cdot 10$, где $(17, 10) = 1$.

Далее находим, что

$$3 \cdot 17 - 5 \cdot 10 = 1$$

и

$$\frac{1}{170} = \frac{3}{10} - \frac{5}{17}.$$

$\frac{1}{170}$ часть окружности получим, вычитая из $\frac{3}{10}$ её $\frac{5}{17}$ её частей.

Установленная выше теорема индуктивно обобщается на любое число m попарно взаимно простых чисел α_1, $\alpha_2, \ldots, \alpha_m$.

Допустим, что, умея разделить (циркулем и линейкой) окружность на α_1, на α_2, ..., α_{m-1} частей, мы можем делить окружность на $d = \alpha_1 \cdot \alpha_2, \ldots, \alpha_{m-1}$ частей. Тогда, так как d и α_m взаимно простые, а на d частей (по допущению) и на α_m частей (по условию) мы делить окружность умеем, то по доказанной выше теореме сумеем разделить и на $n = d \cdot \alpha_m = \alpha_1 \cdot \alpha_2 \ldots \alpha_{m-1} \cdot \alpha_m$ частей. Этим теорема доказана.

Пусть

$$n = 2^{\alpha} \cdot p_1 \cdot p_2 \ldots p_k.$$

Мы умеем делить циркулем и линейкой на 2, на 4 и вообще на любое число 2^{α} частей. По доказанному ранее мы умеем разделить окружность и на p_1, на p_2, ..., p_k частей, ибо всё это гауссовы простые числа. И так как все эти

числа взаимно простые, то мы сумеем разделить окружность и на число частей, равное произведению этих чисел, т. е. на n частей. Этим и доказана достаточность условия, необходимость которого была установлена нами выше (§ 4, 3).

Итак, нами полностью доказано следующее предложение.

Разделить окружность циркулем и линейкой на n равных частей (построить правильный n-угольник) возможно в том и только в том случае, когда n число вида

$$n = 2^{\alpha} \cdot p_1 \cdot p_2 \ldots p_k,$$

где α — произвольное целое положительное число или нуль, а $p_1, p_2, \ldots, p_k$ — различные между собой простые числа вида $2^m + 1$.

ОГЛАВЛЕНИЕ

Адольф Григорьевич Школьник

ЗАДАЧА ДЕЛЕНИЯ КРУГА

Редактор *Н. И. Лепешкина.* Художник *А. М. Гельфер.*
Художественный редактор *В. И. Бельский*
Технический редактор *В. Л. Коваленко*
Корректор *Н. И. Котельникова*

Сдано в набор 26/I 1961 г. Подписано к печати 30/V 1961 г. 84×108¹/₃₂.
Печ. л. 4,75 (3,90). Уч.-изд. л. 3,49. Тираж 34 тыс. экз.

Учпедгиз. Москва, 3-й проезд Марьиной рощи, 41.
Полиграфкомбинат Саратовского совнархоза,
г. Саратов, ул. Чернышевского, 59. Заказ № 2146.
Цена 9 коп.