**Parabola Volume 36, Issue 1 (2000)**

# THE CIRCLE DIVIDERS

**Peter Brown**[1]

Fairly early in your study of algebra, you meet one of the most useful of algebraic techniques, the *difference of two squares* which enables you to write, for example $x^2-1 = (x-1)(x+1)$. Somewhat later you come across the so called *sum and difference of two cubes* so you can write $x^3+1 = (x+1)(x^2-x+1)$ and $x^3-1 = (x-1)(x^2+x+1)$. The polynomials $x-1, x+1, x^2+x+1, x^2-x+1$ are examples of what are known as *cyclotomic polynomials* or *circle dividing* polynomials (from the Greek $\kappa\acute{\upsilon}\kappa\lambda o\varsigma$- a circle and $\tau\acute{\epsilon}\mu\nu\omega$ - I cut.) The cyclotomic polynomials arise from factoring the polynomial $x^n-1$, where $n$ is a positive integer. I will give the exact definition of what we mean by a cyclotomic polynomial a bit later, but the name arises from the fact that if we solve $x^n-1$ using complex numbers, then all the solutions lie on a circle of radius 1 and are equally spaced on that circle, so they cut the circle up into $n$ equal pieces.

Cyclotomic polynomials have many interesting properties and are a favourite source of questions for the 'harder 3-unit' section of the Four Unit HSC exam.

For example, suppose now we look at the equation $x^5-1=0$. Clearly the only real root is $x=1$, but in the complex plane there are 5 distinct solutions, given by

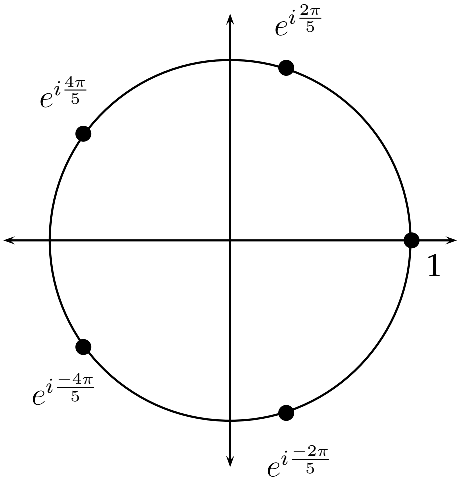
$x = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5},\ \cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5},\ 1,\ \cos\frac{2\pi}{5} - i\sin\frac{2\pi}{5},\ \cos\frac{4\pi}{5} - i\sin\frac{4\pi}{5}.$

I dislike the notation cis $\theta$ and so I will define

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

(It can be shown that this at least makes sense, since $[\text{cis}(\theta)]^n = \text{cis}(n\theta)$, but one usually takes this as the definition of $e^{i\theta}$.)

We can then write the roots as $e^{\pm i\frac{2\pi}{5}}, e^{\pm i\frac{4\pi}{5}}, 1$ and plot these in the complex plane:



[1] Peter Brown is an associate lecturer at UNSW, and is on the editorial board of Parabola.

Now we can in fact factor the polynomial as

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$$

and so if we discard the real root, we find that the four complex numbers are the roots of $x^4 + x^3 + x^2 + x + 1 = 0$. Does this polynomial factor over the rationals? Well, the answer is no, and I will show you why later on, but over the real numbers it certainly does factor. There are a number of ways to do this but I will do it as follows. Call the four complex roots, $\alpha, \beta, \overline{\alpha}, \overline{\beta}$ (notice that the complex roots occur in pairs, i.e. if $\alpha = a + ib$ is a root then so is $\overline{\alpha} = a - ib$) then we have

$$(x^4 + x^3 + x^2 + x + 1) = (x - \alpha)(x - \overline{\alpha})(x - \beta)(x - \overline{\beta}).$$

Now if we expand the brackets in pairs, using the facts that $\alpha + \overline{\alpha} = a + ib + a - ib = 2a$ and $\alpha\overline{\alpha} = (a+ib)(a-ib) = a^2 + b^2 = |\alpha|^2 = 1$, we have

$$(x^4 + x^3 + x^2 + x + 1) = (x^2 - 2x\cos\frac{2\pi}{5} + 1)(x^2 - 2x\cos\frac{4\pi}{5} + 1) \qquad (1)$$

which gives the factorisation over the real numbers.
Moreover, we can use (1) to find an explicit formula for $\cos\frac{2\pi}{5}$ as follows. Divide the polynomial equation $x^4 + x^3 + x^2 + x + 1 = 0$ by $x^2$ to get $x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0$. Now complete the square, and we get

$$\left(x + \frac{1}{x}\right)^2 + \left(x + \frac{1}{x}\right) - 1 = 0.$$

If we let $y = x + \frac{1}{x}$, then we get the quadratic $y^2 + y - 1 = 0$ which has roots $\frac{-1\pm\sqrt{5}}{2}$. Now since the modulus of $x$ is 1, $\frac{1}{x} = \overline{x}$ and so $x + \frac{1}{x} = 2\cos\frac{2\pi}{5}$ or $2\cos\frac{4\pi}{5}$. Thus we can equate the real terms to obtain

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4} \quad \text{and} \quad \cos\frac{4\pi}{5} = \frac{-1-\sqrt{5}}{4}.$$

As part of this problem, we had to factorise $x^4 + x^3 + x^2 + x + 1$ over the reals, and we could see from the answer, that this polynomial could not be factored over the rationals. Thus when we think about factoring a polynomial we have to state where the roots (and hence the co-efficients in the factors) are allowed to come from. If we allow complex numbers then every polynomial factors into a product of linear factors (at least in theory, although this is very difficult to do in practice). If we only allow real numbers then every polynomial with integer co-efficients factors as a product of linear and/or quadratic factors. These two cases are then, in a sense, not very interesting algebraically. If we only allow **rational** numbers then the problem is much more interesting. For example the polynomial $x^4+1$ factors as $(x-e^{i\pi/4})(x-e^{-i\pi/4})(x-e^{3i\pi/4})(x-e^{-3i\pi/4})$ if we allow complex numbers; it factors as $(x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$ if we allow real numbers and it cannot be factored at all if we only allow rational numbers. We will say that a polynomial which cannot be factored over the rational numbers is

*irreducible*. On the other hand, the polynomial $x^4 + 4$ is reducible over the rationals since it factors as $(x^2 - 2x + 2)(x^2 + 2x + 2)$ using only rational numbers.
We now return to the cyclotomic polynomials. These arise when we try to factor $x^n - 1$, so we need to spend a little time looking at the factorisation of such polynomials. For example $x^5 - 1$ factors, as we have seen, as $(x-1)(x^4+x^3+x^2+x+1)$ while $x^6 - 1$ factors as $(x-1)(x+1)(x^2-x+1)(x^2+x+1)$ over the rationals. You can easily check (by expanding) that $x^n - 1$ always has a factorisation $(x-1)(x^{n-1}+x^{n-2}+...+x+1)$. So when factoring such a polynomial we really are interested in whether $x^{n-1}+x^{n-2}+...+x+1$ can be factored or not.

A little experimentation suggests that if $n$ is **prime** then $x^{n-1} + x^{n-2} + ... + x + 1$ is irreducible over the rationals. To prove this result we need the following test.

**Eisenstein's Test:** Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, where the co-efficients $a_i$ are all integers. If there is a prime $p$ such that $p$ does not divide $a_n$, but $p$ does divide all the other co-efficients, and $p^2$ does not divide $a_0$, then $f(x)$ is irreducible over the set $\mathbb{Q}$ of rationals.

**Proof:** Suppose we have

$$a_n x^n + a_{n-1}x^{n-1} + ... + a_0 = (b_k x^k + b_{k-1}x^{k-1} + ... + b_0) \times (c_l x^l + c_{l-1}x^{l-1} + ... + c_0),$$

where the $b_i$'s and $c_i$'s are all integers. You will recall that if a prime $p$ divides the product $ab$ of two integers then it must divide either $a$ or $b$ (or both). (This of course is not true in general of a composite number, for example 6 is a factor of 12, but not of the numbers 3 and 4 whose product is 12.) We use the symbol | to mean 'is a factor of'. So 6 | 12 means 6 is a factor of 12.

Now $p \mid a_0 = b_0 c_0$ and so $p \mid b_0$ or $p \mid c_0$. But the condition $p^2 \not| a_0$ means that $p$ cannot divide both. Without loss of generality, suppose $p \not| c_0$ (and so $p \mid b_0$). Then $p \mid a_1 = b_1 c_0 + b_0 c_1$ and so $p \mid b_1$. Also $p \mid a_2 = b_2 c_0 + b_1 c_1 + b_0 c_2$ and so $p \mid b_2$. Continuing thus, we have $p \mid b_k$ for all $b_k$: but then $p \mid a_n$ contrary to our assumption.
**Example:** $f(x) = x^7 + 2x^3 + 4x + 6$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$.

Also $f(x) = x^n + a$ (where $a$ is not a square) is irreducible over the rationals.

**Example:** $f(x) = 1 + x + x^2 + x^3 + x^4$.
It does not appear that Eisenstein is applicable here, but, clearly $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible, and $f(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5$ which is irreducible by Eisenstein with $p = 5$. Thus $f(x)$ is irreducible over $\mathbb{Q}$.

In fact if $p$ is a prime then the polynomial $x^{p-1} + x^{p-2} + ... + x^2 + x + 1$ is always irreducible over the rationals. It is an example of a cyclotomic polynomial.

To see this, recall that we can write $p(x)$ as $\frac{x^p-1}{x-1}$ and also that $p(x)$ can be factorised if and only if $p(x+1)$ can be.
Now $p(x+1) = \frac{(x+1)^p-1}{x}$ and so we have

$$p(x+1) = x^{p-1} + \begin{pmatrix} p \\ 1 \end{pmatrix} x^{p-2} + \begin{pmatrix} p \\ 2 \end{pmatrix} x^{p-3} + ... + \begin{pmatrix} p \\ p-k \end{pmatrix} x^{p-k-1} + .... + p.$$

Now the general co-efficient can be written as $p\frac{(p-1)!}{k!(p-k)!}$ with $1 \leq j \leq p-1$ and so this number is divisible by $p$ since $p$ is prime.
Thus **all** the non-leading co-efficients are divisible by $p$ but $p^2$ does not divide the constant term $p$ and so the polynomial is irreducible by Eisenstein's test.

We can now finally give a definition of what we mean by a cyclotomic polynomial. We will define the cyclotomic polynomials to be the polynomials $\Phi_n(x)$ which we calculate as follows. Firstly, we take $\Phi_1(x) = x - 1$ and then

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}$$

for $n > 1$. This formula looks horrendous, so let me explain what it means. The notation $\prod$ means we take a product of the cyclotomic polynomials $\Phi_d(x)$, where $d$ is a factor of $n$ excluding $n$ itself. So to compute $\Phi_2(x)$ we take $x^2 - 1$ and divide by $\Phi_1(x)$ to obtain $x + 1$. Similarly, $\Phi_3(x) = x^2 + x + 1$ and

$$\Phi_4(x) = \frac{x^4 - 1}{\Phi_1(x)\Phi_2(x)} = x^2 + 1.$$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ (since 5 is prime) and

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = x^2 - x + 1 \qquad \text{etc.}$$

We have seen that if $p$ is prime, then $\quad \Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1$.

It is not obvious that the definition of $\Phi_n(x)$ will in fact produce a polynomial, since how do we know that all the factors in the denominator will divide the numerator $x^n - 1$? I will not go through the proof of it here since it is slightly harder.
Here is a list of the next few cyclotomic polynomials

$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_8(x) = x^4 + 1$
$\Phi_9(x) = x^6 + x^3 + 1$
$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$
$\Phi_{11}(x) = x^{10} + x^9 + ... + x + 1$
$\Phi_{12}(x) = x^4 - x^2 + 1$
$\Phi_{13}(x) = x^{12} + x^{11} + ... + x + 1$
$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
$\Phi_{16}(x) = x^8 + 1$
$\Phi_{17}(x) = x^{16} + x^{15} + ... + x + 1$
$\Phi_{18}(x) = x^6 - x^3 + 1$
$\Phi_{19}(x) = x^{18} + x^{17} + ... + x + 1$
$\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$

If you compute the first hundred cyclotomic polynomials you will find that all the co-efficients are $0, 1$ or $-1$. For example, the fiftieth cyclotomic polynomial is

$$\Phi_{50}(x) = x^{20} - x^{15} + x^{10} - x^{5} + 1.$$

This phenomenon is however a nice example of the 'lore of small numbers', in other words, a happy accident that depends only on the fact that $n$ is 'small'. If we look at the 105th cyclotomic polynomial

$$\begin{aligned}\Phi_{105}(x) \quad = \quad & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2\,x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} \\ & + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} \\ & + x^{12} - x^{9} - x^{8} - 2\,x^{7} - x^{6} - x^{5} + x^{2} + x + 1,\end{aligned}$$

we see that it contains terms whose co-efficients are $-2$. Furthermore, it was shown (in about 1931) that the co-efficients in any cyclotomic polynomial can be as large as we please, provided we take $n$ large enough.

Here are some problems for you to think about.
(1) Can you find a way to predict the degree of a cyclotomic polynomial?
(2) Can you show that if $n$ is odd, then $\Phi_{2n}(x) = \Phi_{n}(-x)$?

As well as being fun to play with, cyclotomic polynomials are an important theoretical tool in modern abstract algebra. More recently they have been used in developing algorithms to factorise very large numbers and so they have a very important practical use as well.