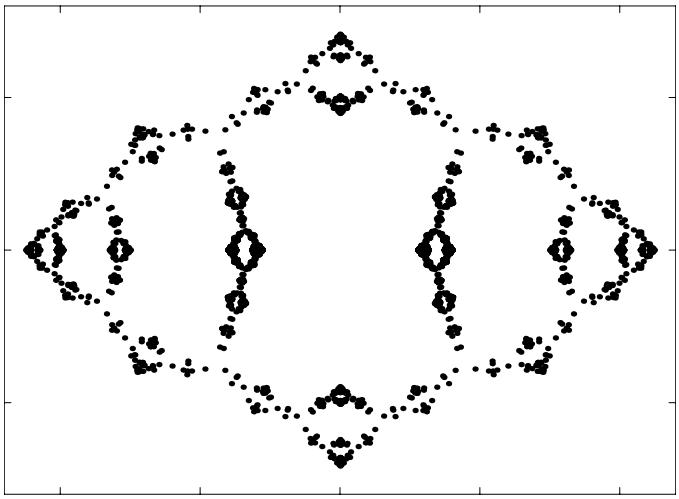
Fractalized Cyclotomic Polynomials

David P. Roberts
University of Minnesota, Morris

1. **Cyclotomic polynomials**
2. **FCPs: basic properties extended**
3. **FCPs: greater complexity**



The 4096 roots of $\Phi_{2;1,0,\infty,1,0,\infty,1,0,\infty,1,0,\infty,1}(x)$, one of the 3^{13} analogs of $\Phi_{2^{13}}(x)$. 466 of these roots are real.

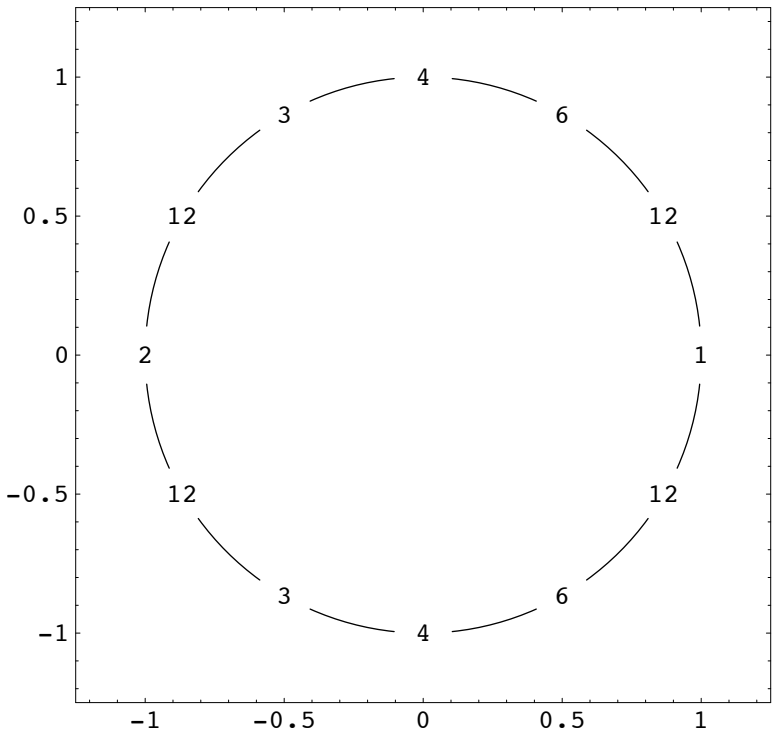
Corresponding paper to appear in *Proceedings of the AMS*.

1. Cyclotomic Polynomials. For n a positive integer, the n^{th} cyclotomic polynomial is

$$\Phi_n(x) = \prod_r (x - e^{2\pi i r})$$

where the product is over rational numbers in $[0, 1)$ with denominator n.

For $n = 1$, 2, 3, 4, 6, and 12, the indexing sets are $\{0\}$, $\{1/2\}$, $\{1/3, 2/3\}$, $\{1/4, 3/4\}$, $\{1/6, 5/6\}$, and $\{1/12, 5/12, 7/12, 11/12\}$. The corresponding roots $e^{2\pi i r}$ are as drawn:



In general, one has

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \qquad (1)$$

Cyclotomic polynomials can be computed inductively from (1) without any reference to complex roots. E.g., one has

$$\begin{aligned}
x - 1 &= \Phi_1(x) \\
x^2 - 1 &= \Phi_1(x)\Phi_2(x) \\
x^3 - 1 &= \Phi_1(x)\Phi_3(x) \\
x^4 - 1 &= \Phi_1(x)\Phi_2(x)\Phi_4(x) \\
x^6 - 1 &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) \\
x^{12} - 1 &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)
\end{aligned}$$

Inverting, one gets

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_{12}(x) &= x^4 - x^2 + 1
\end{aligned}$$

The degree of $\Phi_n(x)$ is "Euler's totient" $\phi(n)$, the number of rational numbers in $[0,1)$ with denominator n.

The case when n is a prime power, $n = p^m > 1$, is the main case. Then, very simply

$$\begin{aligned}\Phi_{p^m}(x) &= \frac{x^{p^m}-1}{x^{p^{m-1}}-1} \\ &= \sum_{j=0}^{p-1} x^{jp^{m-1}}.\end{aligned}$$

The degree of $\Phi_{p^m}(x)$ is $\phi(p^m) = (p-1)p^{m-1}$.

As another example, $\phi(105) = \phi(3)\phi(5)\phi(7) = 2 \cdot 4 \cdot 6 = 48$ and $\Phi_{105}(x) =$

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

Cyclotomic polynomials are irreducible.

(Proof in the case $n = p$:

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^n + px^{n-1} + \cdots + px + 1 - 1}{x} \\ &= x^{n-1} + px^{n-2} + \cdots + p,\end{aligned}$$

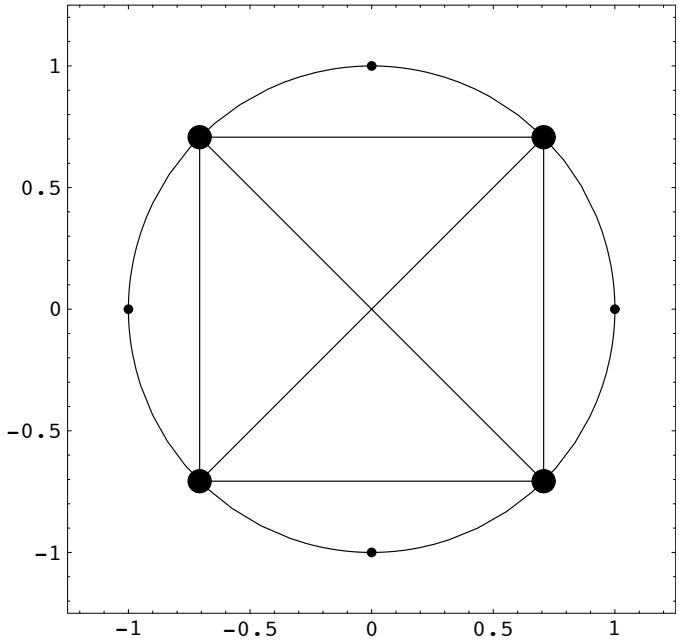
an Eisenstein polynomial.)

The Galois group of $\Phi_n(x)$ is the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$. In fact, for $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ the corresponding permutation of the roots of $\Phi_n(x)$ is

$$e^{2\pi ir} \mapsto e^{2\pi iar}.$$

(This fact, and the fact that $\phi(17) = 16$ is a power of 2, underlies Gauss' construction of the 17-gon by ruler and compass.)

The primes dividing the discriminant $D(\Phi_n)$ of $\Phi_n(x)$ all divide n. *Proof in the case $n = 8$:*



$$\begin{aligned} |D(\Phi_8)| &= \left(\prod_{r_1<r_2} |e^{2\pi i r_1} - e^{2\pi i r_2}| \right)^2 \\ &= \left(\sqrt{2} \cdot \sqrt{2} \cdot \sqrt{2} \cdot \sqrt{2} \cdot 2 \cdot 2 \right)^2 = 2^8 \end{aligned}$$

The ring $\mathbf{Z}[e^{2\pi i/n}]$ is the full ring of integers in the cyclotomic field $\mathbf{Q}(e^{2\pi i/n})$, and so the field discriminant $d(\Phi_n)$ agrees with the polynomial discriminant $D(\Phi_n)$.

2. Fractalized Cyclotomic Polynomials: basic properties extended. Consider the following linear operators from polynomials of degree $\leq n$ polynomials of degree $\leq pn$.

$$\begin{aligned} F^*_{n,p;0}f(x) &= f(1-(1-x)^p) \\ F^*_{n,p;1}f(x) &= f(x^p) \\ F^*_{n,p;\infty}f(x) &= (x^p-(x-1)^p)^n f(\frac{x^p}{x^p-(x-1)^p}) \end{aligned}$$

The complicated $F^*_{n,p,0}$ and $F^*_{n,p,\infty}$ are conjugates of the simple $F^*_{n,p,1}$ by fractional linear transformations of the x-line stabilizing $\{0,1,\infty\}$.

Define

$$\begin{aligned} \Psi_0(x) &= x \\ \Psi_1(x) &= x-1 \\ \Psi_\infty(x) &= 1 \end{aligned}$$

Define $\Phi_{p;\tau}(x) = \frac{F_{1,p;1}(\Psi_\tau)}{\Psi_\tau}$. For $m \geq 2$, define

$$\Phi_{p;\tau_1,\ldots,\tau_m} = F^*_{(p-1)p^{m-2},p;\tau}\Phi_{p;\tau_1,\ldots,\tau_{m-1}}.$$

The special case $\Phi_{p;1,\ldots,1}$ is just the classical cyclotomic polynomial Φ_{p^m}.

Properties of the operators $F_{n,p;\tau} : V_n \to V_{pn}$.

Preservation of cuspidal values. For $f(x) = a_0x^n + \cdots + a_{n-1}x + a_n$ one has $f(0) = a_n$, $f(1)$, and also $f(\infty) = a_0$. Direct computation shows

$$(F^*_{n,p;\tau}f)(\sigma) = f(\sigma) \tag{2}$$

for $\sigma \in \{0, 1, \infty\}$.

Transformation of discriminant. For $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$, its discriminant is $D(f) = a_0^{2n-2}\prod_{i<j}(\alpha_i - \alpha_j)^2$. One has

$$D(F^*_{n,p;\tau}f) = \tag{3}$$
$$(-1)^{p^{np(p-1)/2}}p^{np}f(\tau')^{p-1}f(\tau'')^{p-1}D(f)^p$$

where $\{\tau, \tau', \tau''\} = \{0, 1, \infty\}$. This formula and (4) below are proved by reduction to the simple case of $F_{n,p;1}(x) = x^p$.

Reduction modulo p. If $f(x) \in \mathbf{Z}[x]$ then

$$(F^*_{n,p;\tau}f)(x) \equiv f(x)^p \pmod{p}. \tag{4}$$

Consequences of the general properties for the particular polynomials $\Phi_{p;\tau_1,\ldots,\tau_m}$.

1. Cuspidal values. One checks directly that

$$\Phi_{p;\tau_1}(\sigma) = \begin{cases} \pm p & \text{If } \sigma = \tau_1 \\ \pm 1 & \text{If } \sigma \neq \tau_1 \end{cases} \tag{5}$$

for $\sigma \in \{0, 1, \infty\}$. By (2), the same formulas hold with $\Phi_{p;\tau_1}$ replaced by $\Phi_{p;\tau_1,\ldots,\tau_m}$.

2. Polynomial discriminant. From (3) one gets that

$$D(\Phi_{p;\tau_1,\ldots,\tau_m}) = \pm p^{c(p;\tau_1,\ldots,\tau_m)}$$

with

$$\begin{aligned} c(p;\tau_1,\ldots,\tau_m) = \\ p - 2 + \sum_{j=2}^{m} (p-1)^2 p^{j-2} j + \\ \sum_{j=2}^{m} \delta(\tau_1 \neq \tau_j)(p-1)p^{m-j}. \end{aligned}$$

3. Irreducibility. Equation (4) says

$$\Phi_{p;\tau_1,\ldots,\tau_m}(x) \equiv \Psi_{\tau_1}(x)^{\phi(p^m)} \pmod{p}.$$

This fact, together with (5), says that $\Phi_{p;\tau_1,\ldots,\tau_m}$ is an Eisenstein polynomial if $\tau_1 = 0$. By the Eisenstein criterion, which applies directly if $\tau_1 = 0$, one gets that $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ is irreducible.

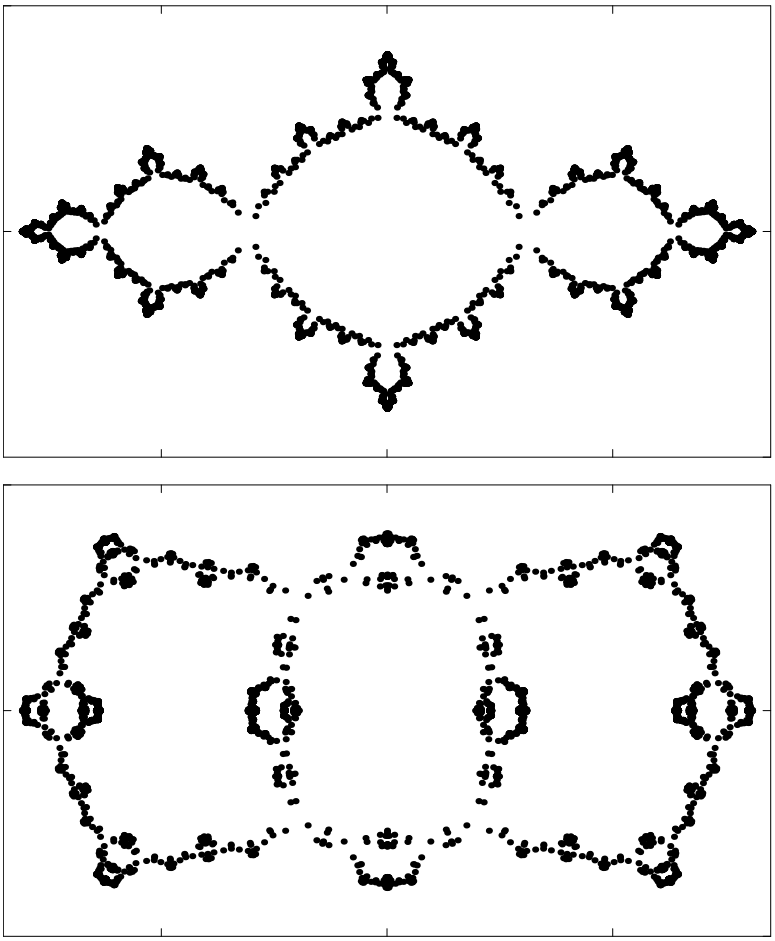
4. Field discriminant. In general, polynomial discriminants $D(f)$ and field discriminants $d(f) = d(\mathbf{Q}[x]/f(x))$ are integers related by

$$d(f) = \frac{D(f)}{i(f)^2}.$$

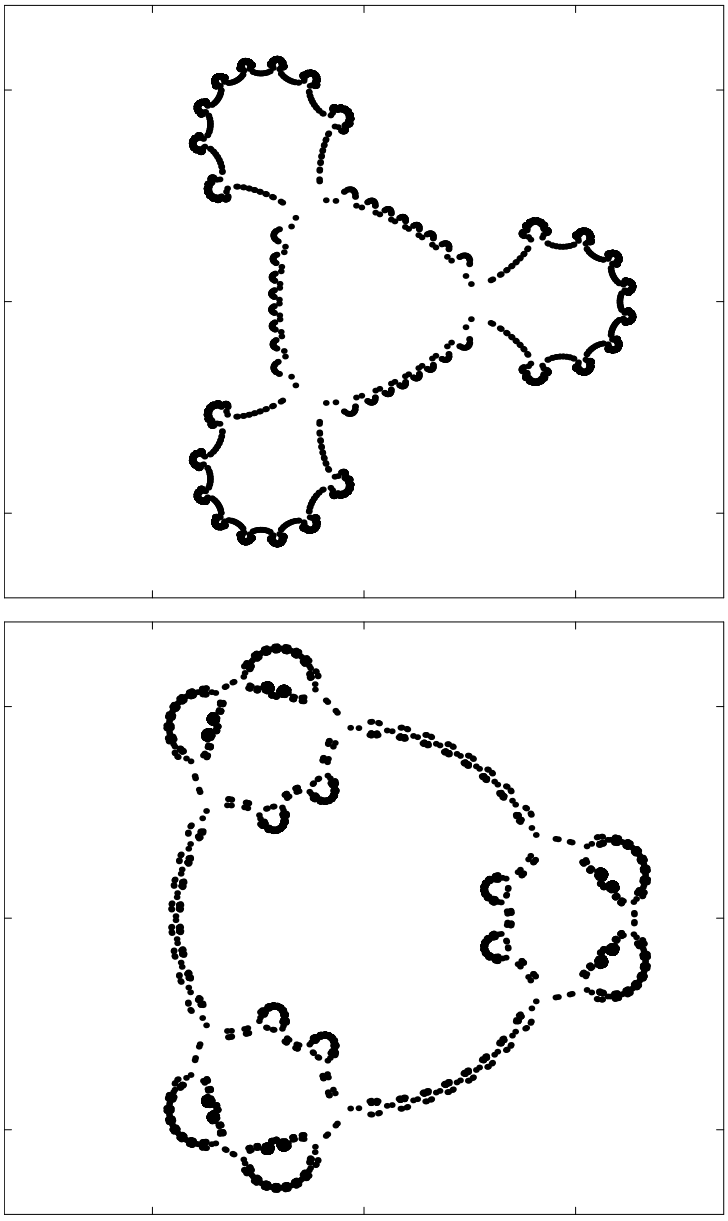
Since $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ is essentially Eisenstein at p, the prime p does not divide $i(\Phi_{p;\tau_1,\ldots,\tau_m})$. Since $D(\Phi_{p;\tau_1,\ldots,\tau_m})$ has the form $\pm p^a$, the only possibility is

$$d(\Phi_{p;\tau_1,\ldots,\tau_m}) = D(\Phi_{p;\tau_1,\ldots,\tau_m}).$$

3. FCPs: greater complexity. Root plots are much more complicated:



The 4096 roots of $\Phi_{2;1,0,1,0,1,0,1,0,1,0,1,0,1}(x)$ on the top (two real) and the 4096 roots of $\Phi_{2;1,0,\infty,0,1,0,\infty,0,1,0,\infty,0,1}(x)$ below (338 real). The maximum possible number of real roots for analogs of $\Phi_{2^m}(x)$ is 2 Fibonacci(m), as represented by the cover slide.



Roots of $\Phi_{3;1,0,0,1,1,0,0,1}(x)$ on the top and $\Phi_{3;1,0,\infty,1,1,\infty,0,1}(x)$ on the bottom. Both polynomials have $\phi(3^8) = 2 \cdot 3^7 = 4374$ roots. When $p \neq 2$, all roots of analogs of $\Phi_{p^m}(x)$ are non-real.

Galois groups still have order of the general form $(p-1)p^c$. However, except in the classical case, the order is always larger than the degree $(p-1)p^{m-1}$ and so the group is non-abelian.

The table considers the case $p = 2$ and $m = 4$, thus octic polynomials $\Phi_{2;\tau_1,\ldots,\tau_4}(x)$ generalizing the octic polynomial $\Phi_{16}(x) = x^8 + 1$. On the table, a, b, and c represent distinct elements of $\{0, 1, \infty\}$.

$\tau_1\tau_2\tau_3\tau_4$	$\lvert G\rvert$	G	$\tau_1\tau_2\tau_3\tau_4$	$\lvert G\rvert$	G
$aaaa$	8	$T2$	$abac$	64	$T28$
$aaab$	32	$T21$	$abba$	64	$T30$
$aaba$	32	$T19$	$abbb$	16	$T8$
$aabb$	32	$T17$	$abbc$	64	$T28$
$aabc$	16	$T6$	$abca$	64	$T27$
$abaa$	16	$T8$	$abcb$	64	$T27$
$abab$	64	$T30$	$abcc$	32	$T16$

Concluding problem. Let K be the union of all Galois extensions of $\mathbf{Q}$ of degree a power of 2 and with absolute discriminant a power of 2. Remarkably, the infinite Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$ is known; it is the pro-p completion of the free product of $Z/2\mathbf{Z}$ and $\mathbf{Z}$.

From general ramification theory one knows that G is filtered by ramification subgroups G^s with all minimal subquotients G^s/G^{s+} of order two, indexed by positive rational numbers s called "slopes."

The problem is to find the slopes s that appear. Our discriminant formulas for FCPs already give some infinite families of slopes. A closer study of low degree cases gives more slopes. Can one somehow use FCPs to get infinitely more slopes? Do FCPs get all the slopes?

One has analogous results and questions for $p > 2$ as well.