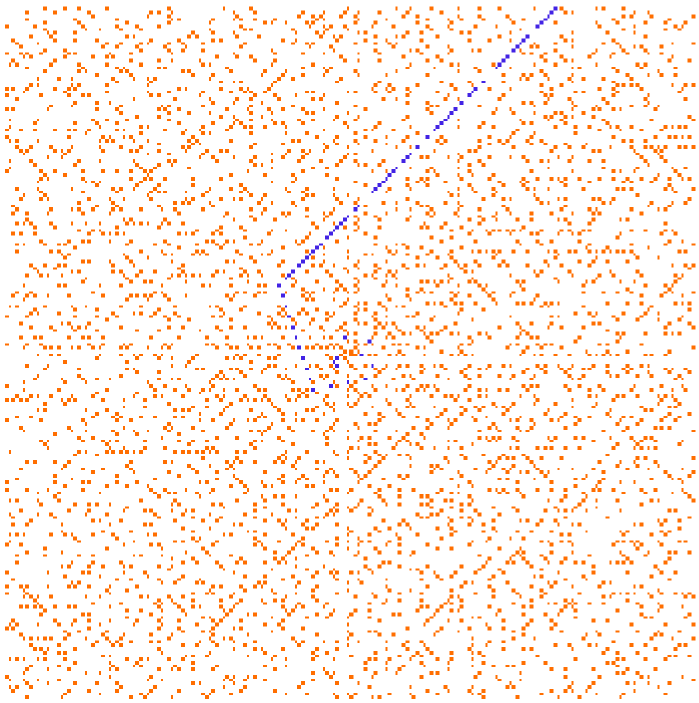
What is Euler's Prime Generating Polynomial?

talk by Isaac Smith



"Ulam's Spiral" with the primes of the form x^2+x+41 highlighted.

Euler noted the remarkable fact that the equation:

$$n^2 + n + 41$$

assumes prime values $n = 0, 1, \ldots, 39$ for

Main Theorem:

Let **q** be prime and $f_q(x) = x^2 + x + q$

The following three statements are equivalent:

$$(1)\ q = 2, 3, 5, 11, 17, 41.$$

$$(2)\ f_q(n) \texttt{ is prime for } n = 0, 1, \ldots, q-2.$$

$$(3)\ \mathbb{Q}(\sqrt{1-4q}) \texttt{ has class number 1.}$$

(1) implies (2) follows by inspection.

The equivalence of (1) and (3) was conjectured by Gauss and proved by Heegner in 1952.

The equivalence of (2) and (3) was first shown by Rabinovitch in 1912 and again by Lehmer in (1936), and will be the main item of my talk.

Important Definitions and concepts:

1. The Algebraic integers, **A**, of $\mathbb{Q}(\sqrt{d})$ are defined as:

$$a \in A \subseteq \mathbb{Q}(\sqrt{d})\ s.t.\ a^2+ma+n=0 \text{ for some integers } m, n$$

2. An ideal **P**≠0 is Prime if the residue ring **A / P** has no zero-divisor.

3. The Prime Ideal **P** containing the rational integer prime **p** divides the ideal **Ap**.
(that is, **Ap** = **P · I**, where I is another Ideal)

4.The Norm of an Ideal, **I,** of **A** is defined as #(**A** / **I**). If **I** divides **J**, then N(**I**) divides N(**J**).

5. We call a prime **p** inert with respect to $\mathbb{Q}(\sqrt{d})$ if **Ap** is a prime ideal.
Theorem: a prime **p**≠2 is inert if and only if **d** is not a quadratic residue modulo **p** and furthermore, **2** is inert if and only if **d** ≡ 5 (mod 8).

Theorem (Method for calculating class number)**:**

$$\text{let } \theta = \begin{cases} \frac{1}{2}\sqrt{d} & if \ \ d > 0, \\ \frac{2}{\pi}\sqrt{-d} & if \ \ d < 0. \end{cases}$$

Then $\mathbb{Q}(\sqrt{d})$ has class number 1 (i.e. is a Principal Ideal Domain) if
$p \leq \lfloor \theta \rfloor \ \Rightarrow \ p$ is inert.

Now we are ready to begin proving the equivalence of (2) and (3) from the Main Theorem. (proof taken from *My Numbers, My Friends* by Ribenboim pp. 91-1110).

References:

(2000) Ribenboim, Paulo. *My Numbers, My Friends: Popular Lectures on Number Theory*. New York: Springer. pp 91-110
(1936) D. H. Lehmer. On the Function $x^2 + x + A$. Sphinx, 6: pp 212-214..