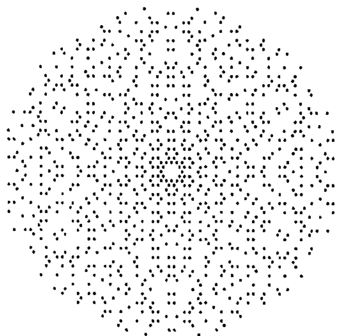
Macros

Harnessing TEX to Compute Third Root of Unity Primes

Klaus Thull*
mahīlatā samāja



This image, showing the primes of $\mathbb{Z}(\sqrt{-3})$, up to norm 1000, was done by another "useless" macro set inspired by the `\primes` and the `\point` examples out of *The TEXbook*.

Mathematics: $\mathbb{Z}(\sqrt{-3})$ consists of all numbers of the form $(x + y\sqrt{-3})/2$ where x and y are rational integers, and $x + y$ is even. These numbers may also be expressed as $a + b(1 + \sqrt{-3})/2$ where a and b are rational integers. We need this later.

In $\mathbb{Z}(\sqrt{-3})$, there exists a Euclidean Algorithm. Thus, even as with the rational integers, there is a divisor theory, and prime numbers. The primes, instead of listing them as numbers, are mapped onto points of a Euclidean plane and plotted.

Any pair of numbers $q + r\sqrt{-3}$ and $q - r\sqrt{-3}$ is said to be conjugate. Their product is rational and is called their norm. The norm of a $\mathbb{Z}(\sqrt{-3})$ integer is a rational integer.

Two numbers of $\mathbb{Z}(\sqrt{-3})$ are associated if their quotient is a unit. The units are the powers of $(1+\sqrt{-3})/2$. There are six different units, arranged in a regular hexagon. Hence for each number there are six associates. The set of associates of a number may be equal to their conjugate, or disjunct. Yet in any case, their union obeys the D_6 (snow crystal) symmetry.

Each natural prime gives rise to a set of primes in $\mathbb{Z}(\sqrt{-3})$ which so obeys the D_6 symmetry. There are three cases:

- The *inert* case: The natural prime $2+3k$ is also prime in $\mathbb{Z}(\sqrt{-3})$. There is one self-conjugate set of six associates.
- The *split* case: The natural prime $1+3k$ is a product of two $\mathbb{Z}(\sqrt{-3})$ primes conjugate but not associate. There are two disjunct conjugate sets of six associates each.
- The *ramified* case: The natural prime 3 is an associate of a square of a $\mathbb{Z}(\sqrt{-3})$ prime. There is one self-conjugate set of six associates.

Macros: This describes how the image is done in TEX. The macros listed are clarified somewhat. All the `\new`... and the space gobblers are omitted as well as a few of the lowest level functions.

The outer main call: Note how the three different cases are handled.

```
\def\primes#1{\plot\@ne\@ne %  ramified
   \ri=7\rid=6\ru=#1 %            split
   \let\primeaction=\splitprimeaction
   \primesexecute
   \plot\tw@\z@ %                 inert
   \isqrt\ru\ru=\csqrt\ri=5
   \let\primeaction=\inertprimeaction
   \primesexecute}
```

Natural Primes: We compute the natural primes of the residue class given by `\ri` mod `\rid` in a range of numbers:

```
\def\primesexecute
   {\ifnum\ri>\ru\let\next=\relax
   \else\isitprime\ri\advance\ri by\rid
   \let\next=\primesexecute
   \fi\next}
```

Here is the primality test for one number. It is very simple: try division by 2, 3, and the residue classes 1 and 5 mod 6 until $\sqrt{\#1}$ or residue 0. Note that `\z@`, `\@ne`, `\tw@` etc. are TEX's constants for $0, 1, 2 \ldots$

```
\def\isitprime#1{\pc=#1\isqrt\pc
   \pl=\csqrt
   {\global\primetrue}
   \pt=\tw@ \tryprime \pt=\thr@@
   \tryprime \pt=\fiv@ \trynext
   \ifprime\primeaction\fi}

\def\trynext{\let\next=\relax
   \ifnum\pl<\pt\else
   \ifprime \let\next=\trynext
   \tryround\fi\fi\next}

\def\tryround
   {\tryprime \advance\pt by \tw@
   \tryprime \advance\pt by \f@ur}

\def\stateprimefalse
   {{\global\primefalse}}
```

* c/o Dittrich, Zeughofstraße 23,
D-1 Berlin 36, Germany

```
\def\tryprime{\rem\pc\pt
   \ifnum\wa=\z@\stateprimefalse\fi}
```

```
\def\splitprimeaction{\starter\pc}
\def\inertprimeaction{\plot\pc\z@}
```

Third Root of Unity Prime: For each split prime p in $\mathbb{Z}$, there is exactly one prime in $\mathbb{Z}(\sqrt{-3})$

$$a + b\frac{1+\sqrt{-3}}{2}$$

with a, b rational integer, $0 < b < a$ whose norm is p. To find this prime, we solve the diophantine equation

$$n = a^2 + ab + b^2 - p = 0.$$

The algorithm used here is $O(p^{1/2})$ yet cheap as such, and fast* for numbers $< 10^{15}$: Choose a fitting octant of the conic and start traveling at the concave side: $(a \leftarrow \lfloor\sqrt{p}\rfloor;\rangle b \leftarrow 0;\rangle n \leftarrow a^2 - p)$

```
\def\starter#1{\cn=#1
   \isqrt\cn\ca=\csqrt\cb=\z@
   \cn=\ca\multiply\cn by\ca
   \advance\cn by-\cx
   \onestep}
```

```
\def\onestep{\isit\ifnum\ca>\cb
   \oneadvance\let\next=\onestep
   \else\let\next=\relax\fi\next}
```

```
\def\oneadvance{\ifnum\cn<\z@\bp
   \else\bpam\fi}
```

weave out ... $(n \leftarrow n + a + 2b + 1;\rangle b \leftarrow b + 1)$

```
\def\bp{\advance\cn by\cb
   \advance\cb by \@ne \advance\cn by\cb
   \advance\cn by \ca}
```

and in: $(n \leftarrow n - a + b + 1;\rangle a \leftarrow a - 1;\rangle b \leftarrow b + 1)$

```
\def\bpam{\advance\cb by \@ne
   \advance\cn by\cb \advance\cn by -\ca
   \advance\ca by -\@ne}\relax
```

on solution ...

```
\def\isit{\ifnum\cn=\z@\ifnum\ca<\cb
   \else\action\fi\fi}
```

do something about it:

```
\def\action{\plot\ca\cb}
```

Plotting the primes: On obtaining one solution, we now compute all the associates and conjugates, thereby unskewing the coordinates such that the numbers in question are expressed as

$$\frac{x + y\sqrt{-3}}{2}$$

and `\point` the dots. This way, we retain integral coordinates. Yet, scaling y-unit by $1.7 \approx \sqrt{3}$ while `\pointing` yields a surprisingly close approximation to a true Euclidean mapping.

```
\def\plot#1#2{\ifnum#2=\z@\xa=#1
```

The inert case:

```
   \point{\xa}{\xa}\point{-\xa}{\xa}
   \point{\xa}{-\xa}\point{-\xa}{-\xa}
   \multiply\xa by \tw@
   \point{\xa}{\z@}\point{-\xa}{\z@}
\else\ifnum#2=#1\xa=#1
```

The ramified case:

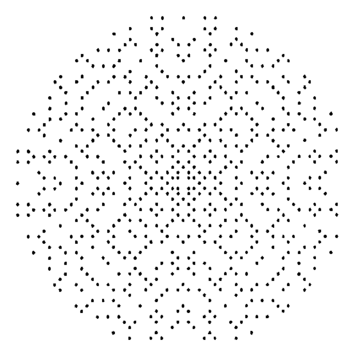
```
   \advance\xa by \xa
   \point{\z@}{\xa}\point{-\z@}{-\xa}
   \advance\xa by #1
   \point{\xa}{#1}\point{-\xa}{-#1}
   \point{-\xa}{#1}\point{\xa}{-#1}
\else
```

The split case:

```
   \xa=#1\ya=#2\yb=\ya\advance\yb by-\xa
   \xb=\xa\advance\xb by \ya
   \xc=\xa\advance\xc by\xb
   \xd=\ya\advance\xd by\xb
   \point{\xc}{\ya}\point{-\xc}{-\ya}
   \point{-\xc}{\ya}\point{\xc}{-\ya}
   \point{\yb}{\xb}\point{-\yb}{-\xb}
   \point{-\yb}{\xb}\point{\yb}{-\xb}
   \point{\xd}{\xa}\point{-\xd}{-\xa}
   \point{-\xd}{\xa}\point{\xd}{-\xa}
   \fi\fi}
```

What else: Since no more $\mathbb{Z}(\sqrt{-3})$ mathematics are to be reported (and to keep this short) I left out the `\point` macro which follows the one recorded in the "Dirties" section except the y-unit scaling. Likeso the `\rem` macro, and the `\isqrt` (integral square root) which uses the Newton algorithm.

Exercise: Devise a set of TeX macros plotting this image:



* I might have exited the algorithm upon the first solution found, speeding it up even more. This is left as an exercise.