

Gaussian Integers: NumThy

Jonathan L.F. King
 University of Florida, Gainesville FL 32611-2082, USA
 squash@ufl.edu
 Webpage <http://www.math.ufl.edu/~squash/>
 1 June, 2014 (at 01:27)

(A natnum N is a **SOTS**, Sum Of Two Squares, if there are integers for which $\ell^2 + k^2 = N$. If there exists such a pair with $\ell \perp k$, then N is **coprime-SOTS**. (E.g, 25 has a non-coprime rep as $5^2 + 0^2$; nonetheless, 25 is coprime-SOTS, since $25 = 3^2 + 4^2$. OTOHand, both $4 = 0^2 + 2^2$ and $40 = 2^2 + 6^2$ have these unique SOTS reps, so neither is **coprime-SOTS**.) An odd integer L is **4Neg** if $L \equiv_4 -1$ and is **4Pos** if $L \equiv_4 +1$. Fermat's Prime-SOTS Thm says: *Oddprime p is SOTS iff p is 4Pos.*

Mod N , a **rono** is a (square-)Root Of Negative One; an integer I such that $I^2 \equiv_N -1$.

Use **CRT** for the Chinese Remainder Thm.)

The ring. Let $\mathbb{G} := \{b + ci \mid b, c \in \mathbb{Z}\}$ be the set of **Gaussian integers**, a subring of \mathbb{C} . The **norm** of a gaussint $B := b + ci$ is

$$N(B) := B \cdot \bar{B} = b^2 + c^2.$$

To set notation, I will henceforth use

$$B := b + ci, \quad E := e + fi, \quad \text{and} \quad S := s + ti$$

for gaussints. I will use

$$\beta := N(B), \quad \varepsilon := N(E), \quad \text{and} \quad \sigma := N(S)$$

for their norms.

A number in \mathbb{G} or \mathbb{Z} which is neither zero nor a unit will be called **non-trivial**. A gaussint $S = s+ti$ lying on the real or imaginary axis is said to be **axial**, i.e either $s = 0$ or $t = 0$. Lastly, use **0** for the complex number $0 + 0i$.

1: Lemma. *The \mathbb{G} -norm is totally multiplicative: $\forall B, E: N(B \cdot E) = N(B) \cdot N(E)$. Furthermore,*

$$S = \mathbf{0} \iff N(S) = 0 \quad ;$$

$$S \text{ is a } \mathbb{G}\text{-unit} \iff N(S) = 1 \quad .$$

Thus there are four \mathbb{G} -units, comprising the set $\{\pm 1, \pm i\}$. (Proof: Exercise.) ♦

Evidently each axial non-zero S can be decomposed uniquely as $(*)$, below.

The *raison d'être* of this note is $(??)$.

2: Irreducibility Theorem. *Fix a non-trivial gaussint S .*

When S is axial, written as

$$*: \quad S = n \cdot E, \quad \text{with } E \text{ a } \mathbb{G}\text{-unit and } n \in \mathbb{Z}_+,$$

then

$$??:1: \quad S \text{ is } \mathbb{G}\text{-irred} \iff n \text{ is a 4NEG prime.}$$

When S is non-axial then

$$??:2: \quad S \text{ is } \mathbb{G}\text{-irred} \iff \sigma \stackrel{\text{def}}{=} N(S) \text{ is } \mathbb{Z}\text{-irred.}$$

Remark. A norm value, σ , is automatically a SOTS-number. So a \mathbb{Z} -irreducible norm is necessarily a SOTS-prime.

Consequently, parts $(??)$ and $(??)$ together say that a gaussint S is \mathbb{G} -irreducible iff: *The norm $N(S)$ is either a SOTS-prime or is the square of a 4NEG prime.* □

Proof of $(??)$ (\Rightarrow). A non-trivial \mathbb{Z} -factorization $n = k \cdot \ell$ yields a non-trivial \mathbb{G} -factorization $S = k \cdot \ell E$. Nope; so n is prime.

Were n a SOTS-prime then take integers b and c with $b^2 + c^2 = n$. Automatically $b \neq 0$ and $c \neq 0$, so

$$S = [b + ci] \cdot [b - ci]E$$

is a non-trivial \mathbb{G} -factorization. In consequence, the Prime-SOTS Thm implies that n must be 4NEG. ♦

Proof of $(??)$ (\Leftarrow). A \mathbb{G} -factorization $S = B \cdot E$ yields a \mathbb{Z} -factorization $n^2 \stackrel{\text{note}}{=} \sigma = \beta \cdot \varepsilon$. Each of β and ε is a norm, so each is 4negprime-even. But n is a 4NEG prime. So WLOG $\beta = n^2$ and $\varepsilon = 1$. Thus the \mathbb{G} -factorization of S was trivial after all. ♦

Reverse-melding and all that jazz

We now come to the most interesting part, implication (??). The (\Rightarrow) direction is immediate: Consider a non-trivial \mathbb{G} -factorization $S = B \cdot E$. Then Lemma ?? assures that $\sigma = \beta\varepsilon$ is a non-trivial \mathbb{Z} -factorization of σ .

As for the (\Leftarrow) direction, first let $g := \text{Gcd}(s, t)$. Then

$$E := \frac{s}{g} + \frac{t}{g}i$$

is not a \mathbb{G} -unit, since S is not axial. Were $g \neq 1$, then $g \cdot E$ would be a non-trivial \mathbb{G} -factorization of S . The upshot is that we may WLOG assume that $s \perp t$.

Proof of (??) (\Leftarrow). Together, $t \perp s$ and $s^2 + t^2 = \sigma$ yield that $t \perp \sigma$. Since $s^2 + t^2 \equiv_{\sigma} 0$, necessarily

3: $I := \left\langle \frac{s}{t} \right\rangle_{\sigma}$ is a σ -rono. Thus σ has no 4NEG-prime factors.

Strategy. Let's now assume that σ factors non-trivially over \mathbb{Z} , say $\sigma = \beta \cdot \varepsilon$, and then endeavor to show that S factors over \mathbb{G} .

Certainly we want to define a gaussint $B := b + ci$ by somehow having chosen numbers b and c with

4: $b^2 + c^2 = \beta$ and $b, c \in \mathbb{Z}$.

Automatically this gives $S = B \cdot E$, a factorization over the *Gaussian rationals*, where

$$E := \frac{S}{B} = \frac{S\bar{B}}{B\bar{B}} = \frac{1}{\beta} \cdot S\bar{B}.$$

Now $\bar{B} = b - ci$, so

$$S\bar{B} = [sb + tc] + [tb - sc]i.$$

The upshot is that the real and imaginary coefficients of E will be *integers* iff

5: $sb \equiv_{\beta} -tc$, and
 $tb \equiv_{\beta} sc$.

Thus our goal is to pick b and c so as to fulfill (??) and (??) simultaneously.

Reverse-Melding. (This clever term is due to Stephen Hicks.) Observation (??) together with $\beta \bullet \sigma$ tell us that β is a SOTS-number and I is a β -rono.

Courtesy of our proof of Prime-SOTS Theorem we can use I to construct integers b and c with $b^2 + c^2 = \beta$ and

6: $b \equiv_{\beta} I \cdot c$.

OTOHand, (??) gives $s \equiv_{\sigma} I \cdot t$. So we certainly have

7: $s \equiv_{\beta} I \cdot t$,

since β divides σ .

We are now happy campers. Firstly

$$sb = \text{LhS}(??)\text{LhS}(??) \equiv_{\beta} I^2tc = -tc$$

as (?? upper) wanted. Secondly

$$Itb = \text{RhS}(??)\text{LhS}(??) \equiv_{\beta} sIc.$$

Dividing by I yields (?? lower), as desired. *Neat!* ♦

Happy conclusion. We have an algorithm for computing SOTS pairs, given an algorithm that factors over \mathbb{Z} . So the above now gives us an effective *algorithm* for factoring a Gaussian integer.

In particular, since there are fast algorithms for determining if an integer is irreducible (prime), we now have a fast algorithm for telling if a gaussint is \mathbb{G} -irreducible. □

Filename: Problems/NumberTheory/gaussints.tex
As of: Monday 17Apr2006. Typeset: 1Jun2014 at 01:27.