THEORY OF NUMBERS
GAUSSIAN INTEGERS

$\alpha = a + ib,\ a\ b$ are rational integers.
Conjugate of $\alpha : \alpha' = a - ib$
Norm of $\alpha = N(\alpha) = \alpha\alpha'$

(i) $N(\alpha)$ is a rational integer.

(ii) $N(\alpha) \geq 0$ equality$\Leftrightarrow \alpha = 0$.

(iii) $N(\alpha\beta) = N(\alpha)N(\beta)$ so $\mu|\nu \Rightarrow N(\mu)|N(\nu)$

Unit: ε such that $\varepsilon,\ \varepsilon^{-1}$ are both gaussian integers, $\varepsilon|\alpha$ for all α.
There are exactly 4 units $\pm 1\ \ \pm i$
If $\alpha_1 = \varepsilon\alpha$ we say α_1 is associated to α.
Gaussian Prime: $\pi\ N(\pi) > 1$, which has no divisors other than units or associates. If $N(\alpha) = p$ then α is G-prime, but the converse is not necessarily true.

Theorem (Euclidean Algorithm) Suppose $\alpha,\ \beta$ are G-integers, $\beta \neq 0$

$\exists \mu,\ \lambda$ such that $\alpha = \mu\beta + \lambda\ N(\lambda < N(\beta)$

Proof $\frac{\alpha}{\beta} = x + iy\ x, y$ rational. $\exists$ rational integers $u,\ v$ such that $|x - v| \leq \frac{1}{2}\ |y - v| \leq \frac{1}{2}$

Write $\mu = u + iv\ \lambda = \alpha - \mu\beta$

$$\begin{aligned}
N(\lambda) &= N(\alpha - \mu\beta) \\
&= |\alpha - \mu\beta|^2 \\
&= |\beta|^2 \left| \frac{\alpha}{\beta} - \mu \right|^2 \\
&= |\beta|^2 \left\{ (x-u)^2 + (y-v)^2 \right\} \\
&\leq \frac{1}{2}|\beta|^2 < N(\beta)
\end{aligned}$$

Theorem (Greatest common denominator) $\alpha,\ \beta$ not both zero. $\exists\delta$such that

(i) $\delta|\alpha;\ \delta|\beta$

(ii) $\eta|\alpha;\ \eta|\beta \Rightarrow \eta|\delta$

(iii) $\exists\lambda\mu$ such that $\delta = \lambda\alpha + \mu\beta$

Proof Consider the set S of all G-integers δ of the form $\lambda\alpha + \mu\beta$.

Let δ be such that $N(\delta)$ is minimal and positive. The proof follows as in the classical case.

Theorem $\pi|\alpha\beta \Rightarrow \pi|\alpha$ or $\pi|\beta$.

Proof Suppose π does not divide α then $(\pi, \alpha) = \varepsilon$. $\exists\lambda,\ \mu$ such that $\varepsilon = \lambda\pi + \mu\alpha\ \beta = \lambda\pi\beta + \mu\alpha\beta$ therefore $\pi|\beta$

Theorem (Unique factorisation) Proof analogous to classical case.

Another proof of Fermat's theorem Suppose $p \equiv 1 \bmod 4$. $\exists x$ such that $x^2 + 1 \equiv 0 \bmod p$. $\exists\pi$ such that $\pi|p$. π is not associated to p.

For $\pi|x^2 - 1$ and so $\pi|(x + i)(x - i)$ therefore $\pi|x + i$ or $\pi|x - i$.

π associated to $p \Rightarrow p|x + i$ or $p|x - i$ which are not so therefore $N(\pi)|N(p) = p^2$ So $N(\pi) = 1, p, p^2$

$N(\pi \neq 1$ π is prime $N(\pi \neq p^2$ π is not associated to p therefore $N(\pi) = p$.

If $\pi = a + ib,\ p = a^2 + b^2$.

Theorem The G-primes are

(i) $1 + i$

(ii) $q \equiv -1\ (4)$

(iii) $a + ib\ a > -\ b > 0\ a^2 + b^2 = p\ p \equiv 1\ (4)$

and their associates.

Proof $\pi|N(\pi) = p_1 \dots p_\nu$ therefore every G-prime divides a rational prime.

(i) $N(1 + i) = 2$

(ii) $q \equiv -1\ (4)\ \pi|q \Rightarrow N(\pi)|N(q) = q^2$ therefore $N(\pi) = 1, q$ or q^2.
$N(\pi \neq 1$ π is prime $N(\pi) \neq q$ by Fermats theorem therefore $N(\pi) = q^2$ therefore π is associated to q.

(iii) $p \equiv 1\ (4)$
$p = (a + ib)(a - ib)$ (Fermat) $= -i(a + ib)(b + ia)$
$a + ib,\ b + ia$ are both g-prime as their norms are equal to p.

Theorem Suppose $n > 1$ and suppose $n = 2^r p_1^{s_1} \dots p_\mu^{s_\mu} q_1^{t_1} \dots q_\nu^{t_\nu}$ where $p_i \equiv 1 \bmod 4$ $q_i \equiv -1 \bmod 4$.

If $r(n)$ is the number of representations of n as a sum of two squares then

$$r(n) = \begin{cases} 0 & \text{if the } t\text{'s are not all even} \\ 4(s_1 + 1 \dots (s_\mu + 1) & \text{is the } t\text{'s are all even} \end{cases}$$

Note If $X(d) = \begin{cases} = 1 & d \equiv 1 \quad (4) \\ -1 & d \equiv -1 \quad (4) \\ 0 & d \equiv 0 \quad (2) \end{cases}$ then $r(n) = 4 \sum_{d|n} X(d)$ so

$r(n) \leq 4d(n)$

Proof We look for the number of G-integers for which $N(\alpha) = n$

Now $n = \varepsilon(1+i)^{2r} \pi_1^{s_1} \pi'^{s_1}_1 \dots \pi_\mu^{s_\mu} \pi'^{s_\mu}_\mu q_1^{t_1} \dots q_\nu^{t_\nu}$

Since $2 = -i(1+i)^2$ and $p \equiv 1 \ (4) \Rightarrow p = \pi\pi'$.

Now suppose $N(\alpha) = n$. Then $\alpha | n$ since $\alpha | N(\alpha$ therefore α is of the form

$$\alpha = \epsilon_1 (1+i)^R \pi_1^{S_1} \pi_1'^{S_1'} \dots q_1^{T_1} \dots \tag{1}$$

where $0 \leq R \leq 2r$ $0 \leq S_1 \leq s_1$ $0 \leq S_1' \leq s_1 \dots) \leq T_1 \leq t_1 \dots$ $(1')$

A number α of the form (1) satisfies

$$N(\alpha) = n \text{ i.e. } \alpha\alpha' = n \Leftrightarrow 2R = 2r \ \ S_1 + S_1' = s_1 \dots \ \ 2T_1 = t_1 \dots \tag{2}$$

Thus the number of α satisfying $\alpha\alpha' = n$ is 4 times the number of α satisfying (2) subject to $(1')$ (4 choices of ϵ_1)

There are no solutions unless the t_i are all even.

If the t_i are all even then the T's are unique and R is unique.

For S_1 we have $s_1 + 1$ choices and then S_1' is uniquely determined. Therefore the number of choices is $(s_1+1)(s_2+1)\dots(s_\mu+1)$ therefore $r(n) = 4(s_1+1)(s_2+1)\dots(s_\mu+1)$.