Summary, March 15

Gauss Primes.

We have seen that the ring $\mathbb{Z}[i]$of Gauss integers is a principal ideal domain and therefore a unique factorization domain. Here we describe the irreducible (or prime) elements of $\mathbb{Z}[i]$. They are called the *Gauss primes*.

A prime integer may be an irreducible element of $\mathbb{Z}[x]$, a Gauss prime, or not. The prime 3 is irreducible, as is seen by looking for a proper divisor. The only Gauss integers α with absolute value < 3 are associates of $1+i$. They don't divide 3. Instead, $(i+i)(i-i) = 2$. So 2 is not a Gauss prime. Similarly, $5 = (2+i)(2-i)$. The factors $1 \pm i$ and $2 \pm i$ are Gauss primes.

Lemma 1. Let p be a prime different from 2, and let M be the multiplicative group of nonzero elements of the field $\mathbb{F}_p$ of integers modulo p.

(i) M contains an element of order 4 if and only if $p \equiv 1$ modulo 4.

(ii) The residue $\overline{a}$ of an integer a in M is an element of order 4 if and only if $a^2 \equiv -1$ modulo p. If so, then $\overline{a}^2 = -1$.

proof (i) We inspect the homomorphism $M \xrightarrow{\varphi} M$ defined by $varphi(\overline{a}) = \overline{a}^2$. Its kernel is $\{\pm 1\}$ and its image H has order $(p-1)/2$. This subgroup contains 1 and an element $\overline{a}$ distinct from ± 1 can be paired with its inverse. So H contains -1 if and only if its order $(p-1)/2$ is even. If so, say $(p-1)/2 = 2n$, then $p - 1 = 4n$ and $p \equiv 1$ modulo 4. □

Lemma 2. An integer prime p is either a Gauss prime or a product a product $\overline{\pi}\pi$ of a Gauss prime and its conjugate.

proof Of course, if $\alpha = a + bi$ is a Gauss integer ($a, b \in \mathbb{Z}$), then $\overline{\alpha}\alpha = a^2 + b^2$ is an integer.

We factor p into Gauss primes in the ring $\mathbb{Z}[i]$, say $p = \pi_1 \cdots \pi_k$. Then $p^2 = \overline{p}p$ is the product of the integers $(\overline{\pi}_1\pi_1), ..., (\overline{\pi}_k\pi_k)$. Since $\mathbb{Z}$ is a unique factorization domain, $k \leq 2$. If $k = 2$, then $p = \overline{\pi}_1\overline{\pi}_1$, and if $k = 1$, then p is an associate of π. □

The next theorem describes the Gauss primes.

Theorem. Let p be an odd prime integer. The following are equvalent:

1. There is a Gauss prime π such that $p = \overline{\pi}\pi$.

2. p is the sum of two integer squares: $p = a^2 + b^2$.

3. p is congruent 1 modulo 4: $p = 5, 13, 17, ...$

4. The residue of -1 modulo p is a square.

proof 1. $\Leftrightarrow$ **2.**This is rather trivial. If $p = \overline{\pi}\pi$ and $\pi = a + bi$ then $\overline{\pi}\pi = (a - bi)(a + bi) = a^2 + b^2$.

1. $\Leftrightarrow$ **4.** This is the most interesting part of the theorem because, a priori, these assertions don't seem related.

We show that a prime integer p is a Gauss prime if and only if the residue of -1 isn't a square in the field $\mathbb{F}_p$ of integers modulo p. The ring $\mathbb{Z}[i]$ of Gauss integers can be obtained from the ring of integers $\mathbb{Z}$ by adjoining an element i with the relation $i^2 + 1 = 0$. So as explained last time, $\mathbb{Z}[i]$ is isomorphic to the quotient ring $\mathbb{Z}[x]/Q$ of the integer polynomial ring, where Q is the principal ideal of $\mathbb{Z}[x]$ generated by $x^2 + 1$.

Next, p is a Gauss prime if and only if it generates a prime, and therefore maximal, ideal of the ring $\mathbb{Z}[i]$ of Gauss integers. Let $\overline{R}$ denote the quotient ring $\mathbb{Z}[i]/p\mathbb{Z}[i]$.

(The ring $\overline{R}$ has finite order, in fact, its order is p^2. Its elements are the residues of the cosets n and ni with $n = 0, ., ..., p - 1$. If p geenrate a prime idela, then $\overline{R}$ is a domain. A finite domain is a field.)

So $\overline{R}$ is obtained from the integer polynomial ring $\mathbb{Z}[x]$ by killing $x^2 + 1$, and then killing p. It is the quotient $\mathbb{Z}[x]/I$, where I is the ideal generated by the two elements $x^2 + 1$ and p. Moreover, we can just as well start by killing p in $\mathbb{Z}[x]$ first, then killing the residue of $x^2 + 1$. The two procedures are summed up in this diagram:

$$\begin{array}{ccc} \mathbb{Z}[x] & \xrightarrow{a} & \mathbb{Z}[i] \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle c} \\ \mathbb{F}_p[x] & \xrightarrow{d} & \overline{R} \end{array}$$

where b and c stad for for killing p, a stands for killing x^2+1 in $\mathbb{Z}[x]$, and d for killing x^2+1 in $\mathbb{F}_p[x]$.

Therefore $\overline{R}$ is a domain field if and only if p is an irreducible element of $\mathbb{Z}[i]$, and also if and only if x^2+1 is an irreducible element of $\mathbb{F}_p[x]$. And, x^2+1 is irreducible in $\mathbb{F}_p$ if and only if it has no root, which means that -1 is not a square in $\mathbb{F}_p$. This shows that **1.** and **4.** are equivalent.

3. $\Leftrightarrow$ **4.**: Let G be the group of nonzero elements in $\mathbb{F}_p$. Its order is $p-1$. We consider the homomorphism $G \xrightarrow{sq} G$ that sends an element α to α^2. Its kernel is $\{\pm 1\}$, so its image H has order $(p-1)/2$. In H we can pair the elements that aren't equal to ± 1 with their inverses. So the number of such elements is even. We also have the identity element 1. So, if the order $|H|$ of H is odd, -1 cannot be in H, and if $|H|$ is even, -1 must be in H. And, if -1 is in H, there is an element α in G whose square is -1. Then -1 is a square in $\mathbb{F}_p$. Since the order of H is $(p-1)/2$, this happens if and only if $p \equiv 1$ modulo 4. Therefore **3.** and **4.** are equivalent. This completes the proof of the theorem. $\square$