Day 15

Proposition: A polynomial $f(x) \in F[x]$ has a root $r \in F$ if and only if $(x - r)$ divides f.

Corollary: A polynomial of degree n over a field F has at most n roots.

Proposition: A finite subgroup of the multiplicative group of a field is cyclic.

Proof: Let U be such a subgroup. By the fundamental, theorem of abelian groups, U is the product of its Sylow p-subgroups. Let $U(p)$ be such a subgroup. If $U(p)$ were not cyclic, then $U(p)$ and hence U would have more than p elements that are solutions to the equation $x^p = 1$. But $x^p - 1$ has at most p roots. Since $U(p)$ is cyclic for each p dividing the order of U, U itself is cyclic.

Corollary: The group of units $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Generators of this group are called *primitive roots mod p*.

Back to the Gaussian integers

The irreducibles in $\mathbb{Z}[i]$ are: - $(1 + i)$ - $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$ - $a \pm bi$ where $a^2 + b^2 = p$ for $p \in Z$ and $p \equiv 1 \pmod 4$.

A positive integer is a sum of two squares if and only if it factors

$$n = 2^k p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_r^{f_r}$$

where the $p_i \equiv 1 \pmod 4$ and the $q_i \equiv 3 \pmod 4$ and all the f_i are even.

The proof follows from the question of when is $n = N(x)$ for some $x \in \mathbb{Z}[i]$.

Algorithm for Fermat's theorem

Suppose $p \equiv 1 \pmod 4$. To write $p = a^2 + b^2$, find a solution u to the congruence $u^2 \equiv -1 \pmod p$. Then use the Gaussian Euclidean algorithm to find a generator π for the ideal $(p, u + i)$ in $\mathbb{Z}[i]$. This generator divides p so its norm is a divisor of p^2. If its norm *were* p^2, then π would be an associate of p and this would mean p divides $u + i$, which it visibly does not. If its norm were 1, then the ideal $(p, u + i)$ would be all of $\mathbb{Z}[i]$ and so we would have $px + (u + i)y = 1$ in $\mathbb{Z}[i]$.

But in that case, multiplying by $(u-i)$ would be $px(u-i)+(u^2+1)y=(u-i)$ and since p divides the left side we'd have p dividing $u-i$, which is not true. So therefore $N(\pi)=p$ and so if $\pi=a+bi$ we have $a^2+b^2=p$.