Notes for 14 Feb (Thursday)

1 The road so far...

1. Proved Fermat's and Euler's theorems.
2. Wrote a formula for $\phi(m)$.

2 Rings and Fields

Here is a beautiful characterisation of primes (called Wilson's theorem).

Theorem 1. $[(n-1)!]_n = [-1]_n$ *iff* n *is a prime.*

Proof. If n is composite, then n is divisible by a prime $2 \leq q \leq n-2$. But $(n-1)! \equiv_n -1$ and hence $(n-1)! \equiv_q -1$ but $(n-1)! \equiv_q 0$.
If $n = p$ is a prime, the result is trivial for $p = 2$. So assume that p is an odd prime. Every non-zero $[a]_p$ has a multiplicative inverse. Note that $x^2 \equiv_p 1$ has exactly two solutions $x \equiv \pm 1$ in the integral domain $\mathbb{Z}_p$. Hence, other than $[\pm 1]_p$, the factors of $(p-1)!$ can be arranged in unequal pairs whose product is $[1]_p$. This proves Wilson's theorem. □

Wilson's theorem in turns proves another important result.

Theorem 2. *For any prime* $p \equiv_4 1$, $[-1]_p = [q^2]_p$ *for some integer* q.

Proof. Let $p = 2m+1$. Then note that $[-1]_p = [(p-1)!]_p = [1.(p-1)]_p.[2.(p-2)]_p \ldots [m.(p-m)]_p = [1].[-1].[2].[-2] \ldots = [m!]_p^2(-1)^m$. Thus if m is even, we are done. □

Now we prove the following theorem in number theory.

Theorem 3. *A prime* p *can be written as* $a^2 + b^2$ *for two integers* a, b *iff* $p \equiv_4 1$.

It is easy to see that if $p = a^2 + b^2$, then $p \equiv_4 1$. The converse is much harder. To prove it, we need to introduce a new construction, in fact, a new ring - The ring of Gaussian integers $\mathbb{Z}[\sqrt{-1}] \subset \mathbb{C}$ consisting of $a + b\sqrt{-1}$ where $a, b \in \mathbb{Z}$. It is easy to see that this subset is a subring of the field $\mathbb{C}$.

While it is not relevant for our present purposes, here are a couple of definitions :
An element p in a commutative ring R is called an irreducible if it is not a product of two non-units.
An element p in a commutative ring R is called a prime, if whenever ab is divisible by p, either a or b is divisible by p.

In an integral domain (one with no zero divisors, i.e., the cancellation rule holds), primes are irreducibles. (Part of your HW.) However, the converse need not be true. It turns out to be true for certain kinds of rings where "unique factorisation into irreducibles" (the fundamental theorem of arithmetic) holds. It turns out that $\mathbb{Z}[\sqrt{-1}]$ is such a ring anyway.
Two elements $a, b \in R$ where R is a commutative ring are called associate to each other if $a = bc$ where c is a unit. For instance, $\pm a$ are associate in $\mathbb{Z}$ for any $a > 0$.

Returning to $\mathbb{Z}[\sqrt{-1}]$, note that 2 is not an irreducible because $2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$ and these factors are not units. Clearly, $\pm 1, \pm\sqrt{-1}$ are units in the ring but are there others ?
Def : $N : \mathbb{Z}[\sqrt{-1}] \to \mathbb{Z}$ given by $N(a + b\sqrt{-1}) = a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1})$ is called the norm. (So the theorem we want is : Is $p = N(\alpha)$ for some $\alpha \in \mathbb{Z}$?) Here are its properties (easy to prove).

1. $N(\alpha) = 0$ iff $\alpha = 0$
2. $N(\alpha\beta) = N(\alpha)N(\beta)$.
3. $N(\alpha) = 1$ iff α is a unit.
4. The complete set of units in $\mathbb{Z}[\sqrt{-1}]$ is $\{\pm 1, \pm\sqrt{-1}\}$.

The deepest property of $\mathbb{Z}[\sqrt{-1}]$ is the following Euclidean division algorithm.

Theorem 4. *Given $\alpha, \beta \neq 0 \in \mathbb{Z}[\sqrt{-1}]$, there exists $\kappa, \rho \in \mathbb{Z}[\sqrt{-1}]$ such that $\alpha = \kappa\beta + \rho$ where $N(\rho) < N(\beta)$.*

Proof. Divide the plane into boxes formed out of $\beta, \sqrt{-1}\beta$, i.e., consider the vertices $\beta\mathbb{Z}[\sqrt{-1}]$. α will lie in one of these boxes. Let $\kappa.\beta$ be a closest corner to α in that box. Let $\rho = \alpha - \kappa\beta$. Clearly the length of ρ is less than half of the diagonal, i.e., $\sqrt{N(\rho)} \leq \frac{\sqrt{2}}{2}\sqrt{N(\beta)} < \sqrt{N(\beta)}$. □

Def : An element $\delta \in \mathbb{Z}[\sqrt{-1}]$ is called the gcd of α, β if δ is an element of maximal norm that divides both.

It is not hard to see that the gcd can be calculated using the Euclidean algorithm and that the Bezout identity holds. (HW)

Theorem 5. *Let $0 \neq \pi \in \mathbb{Z}[\sqrt{-1}]$. Then π is a prime element iff it is irreducible.*

The proof of this theorem is quite similar to that for integers. It will be given as a HW. Here is an interesting lemma.

Lemma 2.1. *If $\pi \in \mathbb{Z}[\sqrt{-1}]$ is such that $N(\pi)$ is a prime integer, then π is a Gaussian irreducible and hence a Gaussian prime.*

Proof. If $\pi = \alpha\beta$, then $N(\alpha)N(\beta) = N(\pi)$. Thus $N(\alpha) = 1$ or $N(\beta) = 1$ which means that one of them is a unit. So π is irreducible and hence a prime. □

Now we prove the number theoretic result on sum of squares.

Proof. If $p \equiv_4 1$, then there exists a $c \in \mathbb{Z}$ satisfying $[c]_p^2 = [-1]_p$. Hence, p divides $(c - \sqrt{-1})(c + \sqrt{-1})$ in $\mathbb{Z}[\sqrt{-1}]$. But p does not divide $c \pm \sqrt{-1}$. Therefore, p is not a Gaussian prime and hence reducible. This means that $p = \alpha\beta$ where $N(\alpha), N(\beta) \neq 1$. Thus $p^2 = N(p) = N(\alpha)N(\beta)$ which means that $N(\alpha) = p = N(\beta)$. Hence $p = \alpha\bar{\alpha}$ where α is a Gaussian prime. $\square$