Math 122 Wednesday, November 23

Beginning of modern number theory was when Fermat obtained a translated copy of Diophantos' classic text (translated to Latin by Bachet ~1636) for he worked to prove the results it contained and developed many techniques.

One result: every prime $p \equiv 1 \pmod 4$ is the sum of two squares (essentially uniquely) $p = a^2 + b^2$ e.g. $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, etc.

Gauss in some sense found the right proof of this by considering the ring $R = \mathbb{Z} + \mathbb{Z}i$ of Gaussian integers.

Say p a prime. Then the ideal $(p) = \{pa + pbi\} \subset R$. $R/(p)$ is a finite ring with p^2 elements. (as an abelian group $R/(p) = \mathbb{Z}/p\mathbb{Z} + \mathbb{Z}/p\mathbb{Z}$ by $a+bi \longmapsto (a \bmod p, b \bmod p)$). Cosets can be represented by $a+bi$, a and b reduced mod p.

Claim This is a field $\iff$ $p \equiv 3 \pmod 4$

Cor For $p \equiv 1 \pmod 4$ there is an ideal $R \supsetneq I \supsetneq (p)$. Hence $I/(p)$ gives a non-trivial ideal of $R/(p)$.

PF: By Claim $R/(p)$ is not a field so $\exists$ a non-trivial ideal. As an ideal is a subgroup under $+$ it must have order p. But this implies that there is an ideal of R containing (p) of index p.

Lemma (to prove the claim) If $p \equiv 3 \pmod 4$ there is no element $a \pmod p$ with $a^2 \equiv -1 \pmod p$.
If $p \equiv 1 \pmod 4$ the element $a = \left(\frac{p-1}{2}\right)! \pmod p$ satisfies $a^2 \equiv -1 \pmod p$.

Pf: The group $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $p-1$. If $p \equiv 3 \pmod 4$ then this order is not divisible by 4 so no element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order 4 (as a would of $a^2 \equiv -1$).
Now say $p \equiv 1 \pmod 4$, $a = 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)$. Then $(-1)^{\frac{p-1}{2}} a = (-1)\cdot(-2)\cdots\left(-\frac{p-1}{2}\right) = a$, as $(p-1)/2$ is even. So $a^2 = (-1)^{\frac{p-1}{2}} a \cdot a = (1)(2)(3)\cdots\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1) \pmod p$.
So $a^2 \equiv (p-1)! \pmod p$. But $(p-1)! \equiv 1 \pmod p$ for all odd p by Wilson's Thm.
[$(p-1)! = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} a = \prod_{b=b^{-1}} b$ (can cancel a and a^{-1} if not equal) $= \prod b = 1 \cdot (-1) = -1$. Note $b^2 = 1 \pmod 4 \iff p \mid b^2 - 1 = (b-1)(b+1) \overset{b \neq 1}{\Longrightarrow}$ either $b \equiv 1 \pmod p$ or $b \equiv -1 \pmod p$]
This is what we wanted.

Constructive Pf of Cor) I = kernel of the homomorphism $R = \mathbb{Z} + \mathbb{Z}i \longrightarrow \mathbb{Z}/p\mathbb{Z}$ ← (the only finite ring of order p, so the only thing that will give the index we want) by $1 \longmapsto 1$, $a \longmapsto a \pmod p$, $i \longmapsto \left(\frac{p-1}{2}\right)! \pmod p$. So $a+bi \longmapsto a + b\left(\frac{p-1}{2}\right)! \pmod p$. Note $f(i)^2 = f(i^2) = f(-1) \equiv 1 \pmod p$.

e.g. $p = 5 \Rightarrow \left(\frac{5-1}{2}\right)! = 2$ so $3 + 7i \longmapsto 3 + 14 \equiv 17 \equiv 2 \pmod 5$

Note there is another I of index p which is the kernel of the homomorphism $\phi: R \to \mathbb{Z}/p\mathbb{Z}$
$a+bi \mapsto a-\left(\frac{p-1}{2}\right)!\, b$. $\left(-\left(\frac{p-1}{2}\right)!\right)^2 = \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1$

Big question Is every ideal $I \subset R = \mathbb{Z}+\mathbb{Z}i$ generated by a single element? Yes

If so then I constructed above has the form $(a+bi)$ ← some generator.

Gauss If $I = (a+bi)$ is principal then $p^2 = a^2+b^2$.
Pf) We know $p \in I$. So $p = (a+bi)(c+di)$ is a multiple of the generator $(a+bi)$ then $(c+di) = (a-bi)\cdot m \Rightarrow p = (a^2+b^2)m$. But $a^2+b^2 = 1 \Rightarrow a+bi = \pm 1$ or $\pm i$ is a unit in $R \Rightarrow I = R$. So $m=1 \Rightarrow p = a^2+b^2$. QED

Note: this innocuous problem in number theory leads to some deep problems in algebra

Are all ideals in $\mathbb{Z}+\mathbb{Z}i$ principal? Yes In any ring? No

Can we construct a field of order p^2 for each p? Yes Of order p^r? Yes