Math 122 Friday, December 2

3 classes of integral domains R (we'll define more precisely a bit later)

1) R has a Euclidean algorithm (R is a <u>Euclidean domain</u>)

⇓

2) Every $I \subset R$ is principal, $I=(a)$, $a \in R$ (R is a <u>principal ideal domain</u> or a <u>PID</u>)

⇓

3) Every element $r \in R$ can be written as a product of irreducible elements $r = p_1 \cdots p_n$ in an essentially unique way (R is a <u>unique factorization domain</u> or <u>UFD</u>)

Book V of Euclid: Every integer is uniquely expressed as a product of primes ($\mathbb{Z}$ is a UFD)

1) Euclidean algorithm for $\mathbb{Z}$: for $a \neq b$, $b = ma + r$ with $0 \leq r < a$ ($\mathbb{Z}$ is Euclidean)

2) [not in Euclid] Any ideal $I \subset \mathbb{Z}$ is principle, generated by $a \geq 1$, the smallest positive integer in $I=(a)$. If $b > a$ in I write $b = ma + r \Rightarrow r = b - ma \in I \to r = 0 \to b = ma \Rightarrow I = (a)$. ($\mathbb{Z}$ is a PID)

3) [this is in Euclid] For any two integers a, b $\exists$ $\gcd(a,b) = d = xa + yb$
Pf: Consider the ideal $I = a\mathbb{Z} + b\mathbb{Z} = (d)$ by part 2. $(d) \supset (a)$, $(d) \supset (b) \Rightarrow d$ divides both a and b.

4) If p is a prime and p divides $a \cdot b$ it divides either a or b. If p does not divide a then $\gcd(p,a) = 1 = xa + yp$. Multiply by b: $b = xab + ypb$. $p \mid$ RHS $\Rightarrow p \mid b$.

5) Unicity of prime factorization $n = p_1 \cdots p_k = q_1 \cdots q_\ell$. Then $k = \ell$ and $p_i = q_i$ after reordering.
Pf: p_1 divides n so $p_1 \mid q_1 \cdot (q_2 \cdots q_\ell) \Rightarrow p_1 \mid q_1$ or $p_1 \mid q_2 \cdots q_\ell$. If $p_1 \mid q_1$ then $p_1 = q_1$ as both are prime. If $p_2 \mid q_2 \cdots q_\ell$ then $p_1 = q_2$ or $p_1 \mid q_3 \cdots q_\ell$ etc. Relabel: then $n/p_1 = p_2 \cdots p_k = q_2 \cdots q_\ell$. Finish with induction on n. ($\mathbb{Z}$ is a UFD)

Note: it's remarkable that the Greeks knew enough math to distinguish theorems like this from obvious statements.

Ring theoretic formulation) p is prime means that (p) is maximal for principal ideals for if $(p) \subset (n) \subset \mathbb{Z}$ then $p = x \cdot n$. As every ideal in $\mathbb{Z}$ is principal, (p) is maximal $\Rightarrow \mathbb{Z}/(p)$ is a field. p divides ab means $ab = 0$ in $\mathbb{Z}/(p) \Rightarrow$ either $a = 0$ or $b = 0$ as any field is an integral domain.

General defn of a Euclidean ring. A ring R is Euclidean wrt a size function δ if $\exists$ a map $\delta : R - \{0\} \to \{0, 1, 2, 3, \ldots\}$ such that $\forall$ $a, b \in R$, $a \neq 0$, $b = ma + r$ for some $m, r \in R$ with $r = 0$ or $\delta(r) < \delta(a)$.

ex. For $R = \mathbb{Z}$, $\delta(n) = |n|$
For $R = F[x]$, $\delta(f(x)) = \deg(f)$
For $R = \mathbb{Z}[i]$, $\delta(a+bi) = a^2 + b^2$
For $R = F$, can take $\delta = 0$ for you can always divide by $a \neq 0$ so r is always 0.

Prop If R is a Euclidean domain then R is a PID.

Pf: Let $I \subset R$. If $I=(0)$ done. If not take $a \neq 0$ in I with smallest value $\delta(a)$ (can do b/c $\mathbb{N}$ is well-ordered; a is not unique, which is fine). Clearly $(a) \subset I$. If $b \in I$ write $b = ma + r$ with $\delta(r) < \delta(a)$ or $r = 0$. But $b - ma = r \in I$ so can't have $\delta(r) < \delta(a) \Rightarrow r = 0 \Rightarrow b = ma \Rightarrow b \in (a) \Rightarrow I = (a)$.

defn We say $p \in R$ is <u>irreducible</u> if the principal ideal (p) is <u>maximal for principal ideals</u>. If $(p) \subsetneq (q) \subsetneq R$ then $p = q \cdot r$ is a non-trivial factorization.

Note in our PID, (p) is a maximal ideal so $R/(p)$ is a field $\Rightarrow$ integral domain. Hence if $p \mid a \cdot b$ in R then either $p \mid a$ or $p \mid b$ by the previous argument $\Rightarrow$ p is what is called prime.

defn We say $p \in R$ is <u>prime</u> if whenever $p \mid ab$ $a, b \in R$ then $p \mid a$ or $p \mid b$.

Prop $\mathbb{Z}[i]$ is a Euclidean domain with respect to $\delta(a+bi) = a^2 + b^2$.

Pf: $a, b \in \mathbb{Z}[i] \subset \mathbb{C}$ $a \neq 0$. Then $b = aw$ in $\mathbb{C}$, $w = \frac{b}{a} = \frac{b\bar{a}}{a \cdot \bar{a}}$ $a = x + iy$, $a\bar{a} = x^2 + y^2 \geq 1$ an integer. Write $w = \alpha + \beta i$. Then α, β are both in $\mathbb{Q}$. Write $\alpha = q_0 + r_0$, $\beta = b_0 + s_0$ with $a_0, b_0 \in \mathbb{Z}$; $|r_0|, |s_0| \leq \frac{1}{2}$. $b = a \cdot w = a((a_0 + r_0) + (b_0 + s_0)i) = a(a_0 + b_0 i) + a(r_0 + s_0 i)$. $m = a_0 + b_0 i \in \mathbb{Z}[i] \Rightarrow b - am = r = a(r_0 + s_0 i) \in \mathbb{Z}[i]$. Calculate $\delta(r) = |r|^2$. Note $\delta(w \cdot z) = \delta(w) \cdot \delta(z)$. So $\delta(r) = \delta(a) \cdot \delta(r_0 + s_0 i)$ where $\delta(r_0 + s_0 i) = r_0^2 + s_0^2 \leq \frac{1}{4} \Rightarrow \delta(r) < \delta(a)$. ∎

From before breaks when $p \equiv 1 \pmod 4$ there is a surjective homomorphism $\mathbb{Z}[i] \to \mathbb{Z}/p\mathbb{Z}$. Kernel $= I = (a+bi)$ is principal $\Rightarrow$ $p = a^2 + b^2$.

Note: the method in the Prop does not work for all rings $\mathbb{Z}[\sqrt{-n}] = \mathbb{Z} + \mathbb{Z}(\sqrt{-n})$ Here $\delta(r_0 + s_0\sqrt{-n}) = |r_0 + s_0\sqrt{-n}|^2 = r_0^2 + n s_0^2 \leq \frac{n+1}{4}$ which may be greater than 1. In fact, all but a finite number of such rings will not be principal ideal domains and their class number (see ch II, this is a measure of how non-principal the ideals are) is $\sim \sqrt{n}$.

Finally (proof next time)

Prop Every PID is a UFD.