Math 122 Monday, December 5

Last time: R integral domain Euclidean wrt $\delta: R-\{0\} \to \{0,1,2,\dots\}$
Principal Ideal Domain every $I=(a)$
Unique Factorization Domain $n=up_1\cdots p_r$ uniquely factorizable into irreducibles
$u\in R$, p_i irreducible elements

Lemma $(p)=(q) \iff p=u\cdot q$ with $u\in R^*$ a unit.
Pf: If $p=uq$ then $(p)\subset(q)$ but also $q=u^{-1}p$ so $(q)\subset(p)$. If $(p)=(q)$ then $p=mq$ and $q=m'p \Rightarrow p=mm'p \Rightarrow p(1-mm')=0 \Rightarrow (1-mm')=0$ as R is a domain $\Rightarrow mm'=1$ are units.

Note however that if $(p_i)\subsetneq(q)\subsetneq R$ then $p_i=q\cdot m$ where m is not a unit so this gives a non-trivial factorization.

Know 3 examples of Euclidean rings:

$\mathbb{Z}$	$\longrightarrow$	$I=(n)$ $n\geq 1$ is the unique positive generator	$\mathbb{Z}^*=\langle\pm 1\rangle$
$F[x]$	$\longrightarrow$	$I=(f(x))$ $f(x)$ unique monic generator	$F[x]^*=F^*$
$\mathbb{Z}[i]$	$\longrightarrow$	$I=(a+bi)$ but no natural generator	$\mathbb{Z}[i]^*=\langle\pm 1,\pm i\rangle$

e.g. $I=(2+i)$. Possible generators: $2+i, -2-i, 2i-1, -2i+1$
$5=(2+i)(2-i)=(2i-1)(-2i-1)=(-1)(2i-1)(2i+1)$ etc.

Prop Any principal ideal domain R is a unique factorization domain.

Lemma If $p\in R$ is irreducible (R a PID) then p divides ab (i.e., $ab\in(p)$) $\Rightarrow$ p divides either a or b.
Pf: Recall $p\in R$ is irreducible iff there is no principal ideal $(p)\subsetneq(q)\subsetneq R$. As R is a PID this says that (p) is maximal so $R/(p)$ is a field. In particular $R/(p)$ is a domain. Consider $\varphi: R\to R/(p)$, where $\varphi(a)=a+(p)$. If p divides ab then $\varphi(ab)=ab+(p)=(p)$ as $ab\in(p)$. So $\varphi(a)\cdot\varphi(b)=\varphi(ab)=0$ in $R/(p) \Rightarrow \varphi(a)$ or $\varphi(b)$ is $0 \Rightarrow a$ or b is $(p) \Rightarrow p$ divides a or b.

Pf of Prop) The same argument we used for $\mathbb{Z}$ works. $n=up_1\cdots p_r=u^*p_1^*\cdots p_t^*$. p_1 divides $n \Rightarrow$ p_1 divides p_1^* or $u^*p_2^*\cdots p_t^* \Rightarrow (p_1^*)\subset(p_1) \Rightarrow (p_1)=(p_1^*)$ as p_1^* is irreducible $\Rightarrow p_1=$ unit$\cdot p_1^*$. Divide and relabel and continue.

Claim The ring $\mathbb{Z}[x]$ has unique factorization (though it is not Euclidean or even a PID).

Note: More generally Gauss' methods will show that if R has unique factorization so does $R[x]$.

First we'll show that $\mathbb{Z}[x]$ is not a PID. Consider φ the composition of
$\mathbb{Z}[x]\to\mathbb{Z}\to\mathbb{Z}/2\mathbb{Z}$
$f(x)\longmapsto f(0)\longmapsto f(0) \bmod 2$.
$\ker\varphi=(x,2)=I$. Say $I=(a)$. Then $x=f(x)\cdot a$, $2=g(x)a \Rightarrow a=\pm 1$. But $(\pm 1)=R\neq I$. So $I\neq(a)$.

Pf of Claim: We'll relate factorization in $\mathbb{Z}[x]$ to factorization in $\mathbb{Q}[x]$, which is a PID and hence also a UFD. We will use the following definition.

Def: Say $f_0(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ is primitive iff $\gcd(a_n, \ldots, a_0) = 1$.

Note any monic f is primitive but things like $2x+3$ are also. Can write any $f(x) \in \mathbb{Z}[x]$ as a product $c \cdot f_0(x)$ where $f_0(x)$ is primitive and $c \geq 1$ is an integer (specifically the gcd of the coefficients). We'll call c the content of f. E.g. $2x^2+6x+14 = 2(x^2+3x+7)$ so 2 is the content.

If $f(x) \in \mathbb{Q}[x]$ can do the same thing: $f(x) = c \cdot f_0(x)$ where $f_0(x) \in \mathbb{Z}[x]$ is primitive and $c \in \mathbb{Q}_{>0}$ is the content. Process: $\exists f(x) \in \mathbb{Z}[x]$ by clearing denominators $\Rightarrow f(x) = \frac{c}{d} f_0(x)$.

Lemma: c is an integer $\iff f(x) \in \mathbb{Z}[x]$. [Hence $c = \prod p_i^{a_i}$ as $\mathbb{Z}$ a UFD and $c=1$ iff no $p \mid c$.]
Pf: Obvious.

To talk about factorization we need a non-obvious fact due to Gauss called Gauss' lemma:

Gauss' Lemma: Assume $f_0(x), g_0(x) \in \mathbb{Z}[x]$ are primitive. Then $f_0(x) g_0(x)$ is primitive.
Pf: Suffices to show that no prime p divides all of the coefficients of $f_0 g_0$. We know that no p divides all of the coefficients of f_0 and similarly for g_0. But the map $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ given by $f(x) \mapsto f(x) \bmod p$ is a ring homomorphism. If p divides all coefficients of $f_0 g_0$ then $f_0 g_0 \equiv 0 \bmod p$. On the other hand $f_0 \not\equiv 0 \bmod p$ and $g_0 \not\equiv 0 \bmod p$. But $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain (consider the leading coefficients) $\Rightarrow\Leftarrow$.

Cor: The content of $f \cdot g$ is the product of the contents of f and g.
Pf: $f = c f_0$, $g = d g_0 \Rightarrow fg = (cd) f_0 g_0$ and $f_0 g_0$ is primitive.

Prop: Let $f \in \mathbb{Z}[x]$ be primitive and $g \in \mathbb{Z}[x]$ be arbitrary. Then f divides g in $\mathbb{Z}[x]$ iff f divides g in $\mathbb{Q}[x]$.
Pf: $\Rightarrow$ is obvious. Say $g = fh$, $h \in \mathbb{Q}[x]$. Then $h = c \cdot h_0$, $h_0 \in \mathbb{Z}[x]$ primitive.
$g = c \cdot f h_0 \Rightarrow c$ is content of $g \Rightarrow c \in \mathbb{Z}[x] \Rightarrow h \in \mathbb{Z}[x]$.

So for any $f \in \mathbb{Z}[x]$, f factors uniquely up to units in $\mathbb{Q}[x]$, which gives a factorization in $\mathbb{Z}[x]$ (by redistributing the units if necessary), which must therefore be unique.