MATH 417 9/10/2018
Mo

Last time: division algorithm in $\mathbb{Z}$, divisibility of integers. 6.1
$\gcd(m,n)$.

Started proving: existence of $\gcd(m,n)$ if m, n not both zero.

We showed: $S = \{an+bm \mid a,b \in \mathbb{Z},\ an+bm > 0\}$ is nonempty

By well-ordering $\exists\ d = \min(S)$.

Since $d \in S$, $d = xn + ym$ for some $x, y \in \mathbb{Z}$.

Hence $\forall \beta \in \mathbb{Z}$ with $\beta \mid n$ and $\beta \mid m$, $\beta \mid d$.

We need to show: $d \mid n$ and $d \mid m$.

By the devision algorithm $\exists q, r \in \mathbb{Z}$ s.t.

1) $n = q \cdot d + r$

2) $0 \leq r < d$

if $r > 0$, then

$$0 < r = n - q \cdot d = n - q \cdot (xn + ym)$$
$$= (1 - qx)n + ((-q)y)m$$

$\Rightarrow r \in S$.

But $d = \min S$ and $r < d$. Contradiction.

Hence $r = 0$, i.e., $n = q \cdot d$ for some $q \in \mathbb{Z}$, i.e., $d \mid n$.

Similarly $d \mid m$.

Conclusion: $d = \min\{an+bm \mid a,b \in \mathbb{Z},\ an+bm > 0\}$

is a gcd of m and n.

In particular $\gcd(m,n)$ exists. $\square$

Q. How do we compute $\gcd(m,n)$?

Remember: we don't have factorization into primes yet

(Key) Lemma 6.1 For all n, m (not both zero), for all $k \in \mathbb{Z}$

$$\gcd(n,m) = \gcd(n - km, m)$$

Proof Let $d = \gcd(n,m)$, $f = \gcd(n-km, m)$.

<u>We argue:</u> $d \mid f$ and $f \mid d$

(Recall this implies: $d = \pm f$. Since $d, f > 0$, this actually implies $d = f$)

Since $d \mid m$ and $d \mid n$, $d \mid (m - kn)$ for any $k \in \mathbb{Z}$.

Since $d \mid (m-kn)$ and $d \mid n$, $d \mid f = \gcd(m-kn, n)$.

Conversely, since $f \mid (m-kn)$ and $f \mid n$,

$f \mid (m-kn) + k \cdot n = m$. And since $f \mid m$ and $f \mid n$, $f \mid d$. $\square$

<u>Note</u> $\forall m, n \in \mathbb{Z}$ $\gcd(m,n) = \gcd(-m,n) = \gcd(m,-n)$.

So it's enough to figure out how to compute $\gcd(m,n)$ when $m, n > 0$. [What's $\gcd(m, 0)$?]

<u>Key fact</u> if $n > m > 0$, $\exists\, q, r \in \mathbb{Z}$ s.t. $n = qm + r$ and $0 \le r < m$.

$\gcd(n,m) = \gcd(n - qm, m) = \gcd(r, m)$

$\uparrow$ Lemma 6.1

if $r = 0$, $\gcd(r, m) = m$

if $r > 0$, repeat: $m = q'r + r'$, $0 \le r' < r$ ...)

<u>Ex</u> Find $\gcd(154, 35)$ and $x, y \in \mathbb{Z}$ s.t.

$$\gcd(154, 35) = x \cdot 154 + y \cdot 35.$$

<u>Solution</u>

$$154 = 4 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7 + 0$$

$\Rightarrow \gcd(154, 35) = \gcd(35, 14) = \gcd(14, 7) = 7$

Also, $7 = 35 - 2 \cdot 14 = 35 - 2 \cdot (154 - 4 \cdot 35)$

$= (-2) \cdot 154 + (1 + 8) \cdot 35$

<u>Definition</u> Two integers m, n are <u>relatively prime</u> if $\gcd(m, n) = 1$

Proposition 1.6.15 (of Goodman) $m, n \in \mathbb{Z}$ are relatively prime $\Leftrightarrow$ $\exists\, x, y \in \mathbb{Z}$ so that $1 = x \cdot m + y \cdot n$.

Proof ($\Rightarrow$) $\exists\, x, y \in \mathbb{Z}$ st $xm + yn = \gcd(m,n)$

$\gcd(m,n) = 1 \Rightarrow \exists\, x, y \in \mathbb{Z}$ st $xm + yn = 1$.

($\Leftarrow$) Suppose $\exists\, x, y \in \mathbb{Z}$ st $xm + yn = 1$, $d = \gcd(m,n)$.

Since $d \mid (xm + yn)$, $d \mid 1$. $1 \mid d$ for any d.

$\Rightarrow$ $d = \pm 1$. But $d > 0$. $\Rightarrow d = 1$. $\square$

Prop 1.6.18 (Goodman) Suppose $a \in \mathbb{Z}$ and p is prime Then either $p \mid a$ or $\gcd(p, a) = 1$.

Proof Let $d = \gcd(p,a)$. Then $d \mid p$. Since p is prime either $d = 1$ or $d = p$. If $d = 1$ we're done.

If $d = p$, $p \mid a$ since $d = \gcd(p,a) \mid a$. $\square$

Proposition 1.6.19 Let $p \in \mathbb{Z}$ be prime, $a, b \in \mathbb{Z}$ $a, b \neq 0$.
If $p \mid (ab)$ then either $p \mid a$ or $p \mid b$.

Remark There are "numbers" for which 1.6.19 is false:
Consider $\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$

$$4 = 2 \cdot 2 = (\sqrt{5} - 1)(\sqrt{5} + 1)$$

But one can show that $2 \nmid (\sqrt{5} \pm 1)$.

Proof of 1.6.19 Suppose $p \nmid a$. Want to show: $p \mid b$.
By 1.6.18, $\gcd(p,a) = 1$ (since $p \nmid a$).
By 1.6.15 $\exists\, x, y \in \mathbb{Z}$ s.t $1 = xp + ya$. $\Rightarrow$

$b = b \cdot 1 = bxp + bya = bxp + y(ab)$

Now $p \mid bxp$ and $p \mid y(ab)$ (since $p \mid ab$).

$\Rightarrow$ $p \mid bxp + yab = b$. $\square$

Corollary (problem 1.6.9 in Goodman) Suppose $a_1, \dots a_r \in \mathbb{Z}$, $a_i \neq 0$, p is a prime and $p \mid (a_1 \cdots a_r)$.
Then $\exists i$ s.t. $p \mid a_i$.

Proof (exercise). $\square$

Thm (Compare Goodman 1.6.4, 1.6.21) Any natural number $n \geq 2$ can be written uniquely (up to order) as a product of primes:
$\exists k \in \mathbb{N}$, $p_1, \dots p_k$ primes s.t. $n = p_1 \cdot \dots \cdot p_k$
($k=1$ is allowed)

Proof (existence) Let $S = \{ m \in \mathbb{N} \mid m \geq 2,$ m is not a prime or a product of primes$\}$.

Suppose $S \neq \emptyset$. By well-ordering S has the smallest element, call it n. Since n is not a prime, n is a product of two smaller positive integers. Call them m_1, m_2: $n = m_1 \cdot m_2$, $m_1, m_2 < n$

Since $m_1, m_2 < n = \min S$, $m_1, m_2 \notin S$.
$\Rightarrow m_1, m_2$ are products of primes $\Rightarrow n = m_1 \cdot m_2$ is a product of primes. Contradiction.
$\Rightarrow S = \emptyset \Rightarrow$ every integer $n \geq 2$ is a product of primes (or a prime). $\square$

Next time: Uniqueness.