Recap :

1. Def. of "a divides b"

2. Using WOP / PMI, it follows that
   - every natural number can be expressed as prod. of primes (i)
   - for every n, n_0, $\exists q \in \mathbb{Z}$, $r \in \{0, \dots, n_0 - 1\}$ s.t. $n = q \cdot n_0 + r$ (ii)
   - prime p divides $a \cdot b \Rightarrow$ p divides a or p divides b (iii)
     (uses WOP + (ii))
   - every natural number $n > 1$ has a unique prime factorization (iv)
     (uses WOP + (iii))

LECTURE 07

GREATEST COMMON DIVISOR

Def.: 7.1 : The greatest common divisor of two natural numbers n, m, denoted by $\gcd(n,m)$, is the largest number $d \geq 1$ s.t. d divides n and d divides m.

Some properties of gcd that were proposed in class:

1. $\forall\ n \in \mathbb{N}$, $\gcd(n, n+1) = 1$
2. $\forall$ primes $p_1 \neq p_2$, $\gcd(p_1, p_2) = 1$
3. $\forall\ n, m$ $n \leq m$, $\gcd(n,m) = \gcd(m \dot{-} n, n)$
4. $\forall\ n, m$, if n div m, then $\gcd(n,m) = n$.
5. $\big((d \text{ divides } a) \wedge (d \text{ divides } b)\big) \iff d$ divides $\gcd(a,b)$

The first four properties follow from the def.: of gcd (and the def.: of primes). What about property 5? We can use the fundamental thm. of arithmetic, but is there a more direct proof? We will come back to this question in the second half of this lecture.

How to compute gcd(n, m):

1. Iterate over the set $\{1, 2, \ldots, \min(n, m)\}$

   Time required : $O(\min(n, m))$.

   Algorithm's correctness is obvious. Poor running time.

2. Euclid's Algorithm

```
EuclidGCD (n, m) :

    if m < n
        swap (n, m)
        // at this point, n ≤ m

    if n divides m
        return n
    else
        return EuclidGCD (m % n, n)
```

remainder when n divides m

Is this algorithm correct? Running time?

Correctness of EuclidGCD: Relies on following claim (which is same as one of the properties discussed at start of lec.)

Claim 7.1 : $\forall n, \forall m \geq n, \gcd(n, m) = \gcd(m \% n, n)$

Proof: Let $m = qn + r$ for $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, n-1\}$

If a number divides n, m, then it also divides $r = m - qn$.

Therefore $\gcd(n, m) \leq \gcd(m \,\%\, n, n)$.

Similarly, if a number divides both r and n, then it also divides $m = q \cdot n + r$.

Therefore $\gcd(m \,\%\, n, n) \leq \gcd(n, m)$.

Hence $\gcd(n, m) = \gcd(m \,\%\, n, n)$.

∎

Lemma 7.1: For all natural numbers n, m,

$\text{EuclidGCD}(n, m) = \gcd(n, m)$.

Proof: PROOF USING STRONG INDUCTION.

Predicate $P(n)$: $\forall\, m \geq n$, $\text{EuclidGCD}(n, m) = \gcd(n, m)$

Base case: $n = 1$. $\text{EuclidGCD}(n, m)$ outputs 1.

Inductive Step: Suppose $P(k)$ holds for all $k < n$.

We need to prove $P(n)$.

Take any $m \geq n$.

If n divides m, then EuclidGCD(n, m) outputs n, which is $\gcd(n, m)$.

If n does not divide m, then EuclidGCD(n, m) outputs EuclidGCD$(m \% n, n)$.

Since $m \% n < n$, we can use $P(m \% n)$ to conclude

EuclidGCD(n, m)
$=$ EuclidGCD$(m \% n, n)$
$= \gcd(m \% n, n)$.

Finally, using Claim 7.1, we conclude that EuclidGCD(n, m) outputs $\gcd(n, m)$

Therefore, the inductive step holds.

Using Strong PMI, we conclude that for all n, $P(n)$ holds. ▨

Let us pause here and check what would happen if we took a different predicate.

Suppose we define the predicate $Q : \mathbb{N} \to \{T, F\}$:

$$Q(m) := \forall\, n \leq m,\ \text{EuclidGCD}(n, m) = \gcd(n, m)$$

We want to prove that $\forall m \in \mathbb{N}$, $Q(m)$ holds, using regular / strong induction.

Base case : $m = 1$ is easy since we only need to check for $n = m = 1$

Induction step : How to derive $Q(m)$ from $Q(k)$, $k < m$? Not clear!

Euclid's algorithm can be extended to derive a useful identity, which shows that the gcd of two numbers can be expressed as "integer linear combination" of the two numbers.

Lemma 7.2 [Bézout's Lemma]:

$\forall\, n, m \in \mathbb{N}$, $\exists\, s, t \in \mathbb{Z}$ s.t. $sn + tm = \gcd(n, m)$.

We will prove this by extending Euclid's algorithm → Extended Euclid (n, m). This algorithm outputs three integers (r, s, t) s.t. $r = \gcd(n, m)$ and $sn + tm = r$.

Extended Euclid GCD (n, m) :

```
if m < n
    swap (n, m)
    // at this point, n ≤ m

if n divides m
    return (n, 1, 0)
else
    (r', s', t') = Extended Euclid GCD (m % n, n)
    // r' = gcd(n, m) = s' · (m % n) + t'n
                      = s' (m - ⌊m/n⌋ n) + t'n
                      = s'm + (t' - ⌊m/n⌋ s') n
    return (r', t' - ⌊m/n⌋ s', s')
```

An easy extension of Lemma 7.1 gives the following:

Lemma 7.3 : For all natural numbers n, m, Extended Euclid GCD (n, m) outputs (r, s, t) s.t. $r = \gcd(n, m)$ and $r = sn + tm$.

Proof using strong induction.

$P(n)$: $\forall\, m \geq n$, $\exists$ integers s, t s.t. $\gcd(n, m) = sn + tm$.

Base case : $n = 1$. $\forall\, m \geq 1$, $1 = \gcd(1, m) = 1 \times 1 + 0 \cdot m$

Induction step : Suppose $P(1) \wedge \dots \wedge P(n)$ holds.

To prove : $\forall\, m \geq n$, $\exists$ integers s, t s.t.

$\gcd(n, m) = s \cdot n + t \cdot m$.

If n divides m, then $\gcd(n, m) = 1 \cdot n + 0 \cdot m$

Else, let $m = q \cdot n + r$.

Using $P(r)$, we get that $\exists\, s', t'$ s.t.

$$\begin{aligned} \gcd(n, m) = \gcd(r, n) &= s'r + t'n \\ &= s'\left(m - \lfloor m/n \rfloor n\right) + t'n \\ &= s'm + \left(t' - \lfloor m/n \rfloor s'\right)n \end{aligned}$$

∎

Proof using WOP: Let $S = \{ s \cdot n + t \cdot m : s, t \in \mathbb{Z}, \; s \cdot n + t \cdot m > 0 \}$

$S \subseteq \mathbb{N}$. S is nonempty since $n, m \in S$.

By WOP, S has a minimal element, say d_0.

The following claim is very similar to what we used for Euclid's lemma in Lecture 06.

Claim: d_0 divides every element in S.

Pf: Proof by contradiction. Suppose there exists some $d \in S$ s.t. d_0 does not divide d. Then, as discuseed in last class, there exists $q \in \mathbb{N} \cup \{0\}$ and $r \in \{1, \dots, d_0 - 1\}$ s.t. $d = q \cdot d_0 + r$.

Since $d_0 \in S$, $\exists \, s_0, t_0 \in \mathbb{Z}$ s.t. $d_0 = s_0 \cdot n + t_0 \cdot m$

Since $d \in S$, $\exists \, s, t \in \mathbb{Z}$ s.t. $d = s \cdot n + t \cdot m$

$$r = d - q \cdot d_0 = (s - q \cdot s_0) n + (t - q \cdot t_0) m$$

$\Rightarrow r \in S$. But this is a contradiction, since $r < n_0$.

∎

In particular, d_0 divides n and m.

Claim: d_0 is the largest natural number dividing both n and m.

Proof: Proof by contradiction.

Suppose $\exists\ d > d_0$ s.t. d divides n and m.

Since $d_0 \in S$, $\exists\ s, t \in \mathbb{Z}$ s.t. $d_0 = s \cdot n + t \cdot m$

d divides $n, m \Rightarrow d$ divides $s \cdot n + t \cdot m = d_0$.

Contradiction.

Summary of Bezout's Lemma: $\exists\ s, t \in \mathbb{Z}$ s.t. $\gcd(n, m) = s \cdot n + t \cdot m$

(1)- Look at the set S of all nat. numbers that can be expressed as $s \cdot n + t \cdot m$, $n \in S$, $m \in S$

(2)- Let d_0 be the smallest in this set.

(3)- d_0 divides all numbers in $S \Rightarrow d_0$ div. n and m

(4)- If d divides n and m, then $d \leq d_0$.

(3) + (4) $\Rightarrow$ d_0 is the greatest common div. of n, m.

Bézout's identity / lemma has several applications:

1. If d div. n and m, then d div. $\gcd(n, m)$.

$\exists\, s, t \in \mathbb{Z}$ s.t. $\gcd(n, m) = s \cdot n + t \cdot m$. If d divides both n, m, then it also divides $s \cdot n + t \cdot m$.

2. Euclid's Lemma: if p divides $a \cdot b$, then p divides a or p divides b.

Suppose p divides $a \cdot b$, but p does not divide a. We need to show that p must divide b.

Since p does not divide a, and since p is prime, $\gcd(p, a) = 1$. Therefore, $\exists\, s, t \in \mathbb{Z}$ s.t. $1 = s \cdot p + t \cdot a$

$$b = 1 \cdot b = s \cdot p \cdot b + t \cdot a \cdot b$$

p divides $s \cdot p \cdot b$. p divides $t \cdot a \cdot b$.

Hence p divides $s \cdot p \cdot b + t \cdot a \cdot b = b$.