Obvious (but Important!) Fact: If $a$ and $b$ are positive integers, then there are non-negative integers, $q$ and $r$ called the quotient and remainder, respectively, with $0 \leq r < b$ such that

$$a = qb + r.$$

To emphasize that $q$ and $r$ depend on $a,b$, we write $q(a,b),r(a,b)$.

Problem 7.1:

(i) Find $q(101,17)$ and $r(101,17)$.

(ii) Find $q(100,20)$ and $r(100,20)$.

(iii) Find $q(7,9)$ and $r(7,9)$.

Solution to 7.1:

(i) $17 \cdot 5$ is strictly less than 101 but $17 \cdot 6$ is $\geq 101$ hence $q = 5$, and $r = 101 - 17 \cdot 5 = 101 - 85 = 16$. So $q(101,17) = 5$, $r(101,17) = 16$.

(ii) $20 \cdot 4$ is strictly less than 100 but $20 \cdot 5$ is $\geq 100$ (in fact it is equal to 100), hence $q = 5$, and $r = 100 - 20 \cdot 5 = 100 - 100 = 0$. So $q(100,20) = 5$, $r(100,20) = 0$.

(i) $9 \cdot 0$ is strictly less than 7 but $9 \cdot 1$ is $\geq 7$, hence $q = 0$ and $r = 7 - 9 \cdot 0 = 7$. So $q(7,9) = 0$, $r(7,9) = 7$.

Ans. to 7.1: (i) $q(101,17) = 5$, $r(101,17) = 16$. (ii) $q(100,20) = 5$, $r(100,20) = 0$. (iii) $q(7,9) = 0$, $r(7,9) = 7$.

Definition: an integer $m$ is a divisor of an integer $n$ if $r(n,m) = 0$, in other words if $n/m = q(n,m)$, in other words if $n/m$ is an integer.

Definition: The set of divisors of an integer $n$, $\text{Div}(n)$, is the set of all integers $m$ such that $m$ is a divisor of $n$.

$$\text{Div}(n) = \{m; n/m \text{ is an integer}\}.$$

How to find the set of divisors of an integer $n$ (the stupid way!)

If $m \in \text{Div}(n)$ then $m \leq n$, so we can test every integer $m$, between 1 and $n$, and include those for which $r(n,m) = 0$. 

1
Problem 7.2: Use the stupid way to find $\text{Div}(10)$.

$10/1 = 10$ is an integer so $1 \in \text{Div}(10)$, $10/2 = 5$ is an integer, so $2 \in \text{Div}(10)$, $10/3$ and $10/4$ are not integers, so they do not belong. $10/5 = 2$ is an integer, so $5 \in \text{Div}(10)$. $10/6$, $10/7$, $10/8$, and $10/9$ are not integers, so they do not belong. $10/10 = 1$ is an integer, so $10 \in \text{Div}(10)$.

So we have Ans. to 7.2:

$$\text{Div}(10) = \{1, 2, 5, 10\} .$$

Note: $\text{Div}(n)$ has at least two elements, 1, and $n$. If $n$ is prime, then these are the only ones, otherwise it has more elements.

How to find the set of divisors of an integer $n$ (the clever way)

Step 1: Use the algorithm of Lecture 6 to find the product-of-prime-powers representation of $n$.

$$n = \prod_{i=1}^{k} p_i^{a_i} .$$

Then

$$\text{Div}(n) = \prod_{i=1}^{k} p_i^{a_i} ; \ 0 \leq a_i \leq a_i \} .$$

Interesting consequence: The number of divisors of $n$ is $(1 + a_1) \cdots (1 + a_k) \ (= \prod_{i=1}^{k} (1 + a_i) ).$

Problem 7.3: Use the clever way to find $\text{Div}(10)$.

Solution to 7.3: $10 = 2^1 \cdot 5^1$, so $k = 2$, $p_1 = 2$, $p_2 = 5$ and $a_1 = 1$, $a_2 = 1$. Hence there are $(1 + 1) \cdot (1 + 1) = 4$ divisors.

$$\text{Div}(10) = \{2^0 \cdot 5^0 , \ 2^1 \cdot 5^0 , \ 2^0 \cdot 5^1 , \ 2^1 \cdot 5^1 \}$$

$$= \{1, 2, 5, 10\}$$

Ans. to 7.3: $\text{Div}(10) = \{1, 2, 5, 10\}$.

Problem 7.4: Use the clever way to find $\text{Div}(300)$.

Solution to 7.3: $300 = 2^2 \cdot 3^1 \cdot 5^2$, so $k = 3$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ and $a_1 = 2$, $a_2 = 1$, $a_3 = 2$. Hence there are $(1 + 2) \cdot (1 + 1) \cdot (1 + 2) = 18$ divisors of 300.

$$\text{Div}(300) = \{2^0 \cdot 3^0 \cdot 5^0 , \ 2^0 \cdot 3^0 \cdot 5^1 , \ 2^0 \cdot 3^1 \cdot 5^0 , \ 2^0 \cdot 3^1 \cdot 5^1 , \ 2^0 \cdot 3^1 \cdot 5^2 ,$$

$$2^1 \cdot 3^0 \cdot 5^0 , \ 2^1 \cdot 3^0 \cdot 5^1 , \ 2^1 \cdot 3^0 \cdot 5^2 , \ 2^1 \cdot 3^1 \cdot 5^0 , \ 2^1 \cdot 3^1 \cdot 5^1 , \ 2^1 \cdot 3^1 \cdot 5^2 , \ 2^1 \cdot 3^1 \cdot 5^2 ,$$

$$2^2 \cdot 3^0 \cdot 5^0 , \ 2^2 \cdot 3^0 \cdot 5^1 , \ 2^2 \cdot 3^0 \cdot 5^2 , \ 2^2 \cdot 3^1 \cdot 5^0 , \ 2^2 \cdot 3^1 \cdot 5^1 , \ 2^2 \cdot 3^1 \cdot 5^2 ,$$

$$2^2 \cdot 3^1 \cdot 5^2 \} .$$
\[2^2 \cdot 3^0 \cdot 5^0 \ , \ 2^2 \cdot 3^0 \cdot 5^1 \ , \ 2^2 \cdot 3^0 \cdot 5^2 \ , \ 2^2 \cdot 3^1 \cdot 5^0 \ , \ 2^2 \cdot 3^1 \cdot 5^1 \ , \ 2^2 \cdot 3^1 \cdot 5^2 \} \ .

So
\[
\text{Div}(300) = \{1 \ , \ 5 \ , \ 25 \ , \ 3 \ , \ 15 \ , \ 75 \ , \\
2 \ , \ 10 \ , \ 50 \ , \ 6 \ , \ 30 \ , \ 150 \ , \\
4 \ , \ 20 \ , \ 100 \ , \ 12 \ , \ 60 \ , \ 300 \} \ .
\]

It is convenient to put the members in increasing order (but being a set it does not really matter). So \textbf{Ans. to 7.4}:
\[
\text{Div}(300) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60, 75, 100, 150, 300\} \ .
\]

**Definition of Greatest Common Divisor**

The \textbf{greatest common divisor} of integers \(m\) and \(n\) is the \textbf{largest} element of 
\[
\text{Div}(m) \cap \text{Div}(n) \ .
\]

**How to find the Greatest Common Divisor** (The VERY stupid way).

\textbf{Input}: positive integers \(m\) and \(n\).

\textbf{Output}: \textit{gcd}(m, n) \ (\textit{often written, for short, (m, n) but it is a confusing and stupid abbreviation!}), the greatest common divisor of \(m\) and \(n\).

\textbf{Step 1}: Find \textit{explicitly} both \textit{Div}(m) and \textit{Div}(n).

\textbf{Step 2}: Find their intersection, \textit{Div}(m) \cap \textit{Div}(n).

\textbf{Step 3}: Find the largest element of \textit{Div}(m) \cap \textit{Div}(n).

\textbf{Problem 7.5}: Find \textit{gcd}(20, 30) using the VERY stupid way.

\textbf{Solution to 7.5}: \(20 = 2^2 \cdot 5\) and \(30 = 2 \cdot 3 \cdot 5\).

\textbf{Step 1}:
\[
\text{Div}(20) = \{1, 2, 4, 5, 10, 20\} \ , \ \text{Div}(30) = \{1, 2, 3, 5, 6, 10, 15, 30\} \ .
\]

(You do it!)

\textbf{Step 2}:
\[
\text{Div}(20) \cap \text{Div}(30) = \{1, 2, 5, 10\} \ .
\]

The \textbf{largest} member is 10.
Ans. to 7.5: $\gcd(20, 30) = 10$.

**How to find the Greatest Common Divisor** (The neither-stupid-nor-clever way).

**Step 1:** Use the algorithm of Lecture 6 to find the product-of-prime representations of $m$ and $n$

\[ m = \prod_{i=1}^{k_1} p_i^{a_i}, \]
\[ n = \prod_{i=1}^{k_2} q_i^{b_i}, \]

with $a_i \geq 1$, $b_i \geq 1$.

**Step 2:** Let \( \{r_1, \ldots, r_k\} \) be the union of \( \{p_1, \ldots, p_{k_1}\} \) and \( \{q_1, \ldots, q_{k_2}\} \), and rewrite

\[ m = \prod_{i=1}^{k} r_i^{c_i}, \]
\[ n = \prod_{i=1}^{k} r_i^{d_i}, \]

where now $c_i \geq 0$, $d_i \geq 0$. In other words, we pad the representations of $m$ and $n$ with a product of “primes to the power 0”, in order to make them compatible.

**Step 3:**

\[ \gcd(m, n) = \prod_{i=1}^{k} r_i^{\min(c_i, d_i)}. \]

**Problem 7.6:** Find $\gcd(140, 30)$ using the neither-stupid-nor-clever way.

**Solution to 7.6:**

**Step 1:**

\[ 140 = 2^2 \cdot 5^1 \cdot 7^1, \quad 30 = 2^1 \cdot 3^1 \cdot 5^1, \]

**Step 2:** \( \{2, 5, 7\} \cup \{2, 3, 5\} = \{2, 3, 5, 7\} \), so let’s rewrite

\[ 140 = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^1, \quad 30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0. \]

**Step 3:**

\[ \gcd(140, 30) = 2^{\min(2, 1)} \cdot 3^{\min(0, 1)} \cdot 5^{\min(1, 1)} \cdot 7^{\min(1, 0)} = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 10. \]

**Ans. to 7.6:** $\gcd(140, 30) = 10.$