MAST-332/COMP-367
Techniques in Symbolic Computation
Lecture 2 Notes:

Bezout's Identity, Diophantine Equations (Ch.3)

Bezout's Identity & Extended Euclid's Algorithm (Ch. 3D)

Let a and b be (positive) integers. Then the following Theorem is true:

Theorem ('*Bezout's Identity*') : If $(a, b) = d$ **then** $d = a \cdot t + b \cdot s$ for some integers t and s.

The Bezout's Identity can be proven by the method of reversing the standard Euclid's algorithm:

$$b = a \cdot q_1 + r_1$$
$$a = r_1 \cdot q_2 + r_2 :$$
$$r_1 = r_2 \cdot q_3 + r_3 :$$
....
$$r_{k-2} = r_{k-1} \cdot q_k + r_k :$$

The key is that each of the residuals r_k can be presented in the form of linear combination of initial numbers a and $b \geq a$ using back-substitution of previous residuals. Say, for r_2 we can write

$$r_1 = -q_1 \cdot a + b :$$
$$r_2 = a - q_2 r_1 = a - q_2 \left(b - q_1 \cdot a \right)$$
$$= \left(1 + q_2 q_1 \right) \cdot a - q_2 \cdot b :$$
....
$$r_k = r_{k-2} - r_{k-1} \cdot q_k = \ldots.$$
$$= \left(x_k \cdot a + y_k \cdot b \right) :$$
with some integers x_k **and** y_k. To make this procedure more clear it is convenient to start with the

numbers b $\left(denoted\ as\ r_{-1}\right)$ and a $\left(denoted\ as\ r_{0}\right)$ themselves (note that we assumed $b > a$):

$$eq1 := \ b \equiv r_{-1} = 0 \cdot a + 1 \cdot b :$$

$$eq2 := \ a \equiv r_{0} = 1 \cdot a + 0 \cdot b :$$

$$eq3 := \ r_{1} = -q_{1} \cdot a + b :$$

Thus, $x_1 = -q_1$ represents the integer quotient of division $\frac{b}{a}$, and $y_1 = 1$.
The next residual is found again by the operation

$$r_{2} = -q_{2} \cdot r_{1} + a = \left(1 + q_{1} \cdot q_{2}\right) \cdot a - q_{2} \cdot b = \ x_{2} \cdot a + y_{2} \cdot b :$$

where $x_2 = \left(1 + q_1 \cdot q_2\right)$ **and** $y_2 = -q_2$
This can be continued untill we get $r_k = d$ on the left:

$$d = t \cdot a + s \cdot b :$$

It is easy to see that all these operations actually represent a sequence of elementary row operations starting with the first two rows of the matrix

$EEA := Matrix\left(4, 3, \left[b, 0, 1, a, 1, 0, r_1, x_1, y_1, r_2, x_2, y_2\right]\right);$

$$\begin{bmatrix} b & 0 & 1 \\ a & 1 & 0 \\ r_1 & x_1 & y_1 \\ r_2 & x_2 & y_2 \end{bmatrix} \quad \textbf{(1.1.1)}$$

etc., where the new row is written below the row of the last calculated remainder.
In this matrix the 3d row is
$row3 \ = \ row1 - \ iquo(b, a) \cdot row2 :$

where $iquo(b, a)$ stands for the integer quotient of (*b/a*) . The next row is
$row4 = row2 - \ iquo\left(a, r_1\right) \cdot row[3] :$ etc.

The matrix *EEA* produced by this algorithm corresponds to the ***Extended Euclid's Algorithm***.
Note that the scaling factors in these row operation (corresponding formally to *replacement operations*) are the quatients of the leftmost elements of the previous two rows.

Question: When does the EEA end?
Answer : When $r_{k+1} = 0$. The previous row gives the values of the coefficients x_k, y_k :

Exercise 1: Construct EEA matrix to find the GCD (*a,b*) and the solution to the Bezout's Identity $d = t \cdot a + s \cdot b :$ for the following numbers a and b:

(**A**) b=270 and a=114;

Solution:

We start EEA algorithm $r_k = \left(x_k \cdot a + y_k \cdot b \right)$: with the first two highest 'remaiders' corresponding to the first two equations
$270 = 0 \cdot 114 + 1 \cdot 270$:
$114 = 1 \cdot 114 + 0 \cdot 270$:

Step 1: write the first two rows as a list:
$row1 := [270, 0, 1]$;

$$[270, 0, 1] \tag{1.1.2}$$

$row2 := [114, 1, 0]$;

$$[114, 1, 0] \tag{1.1.3}$$

Step 2: find the 3d row
$row3 := row1 - iquo(270, 114) \cdot row2$;

$$[42, -2, 1] \tag{1.1.4}$$

Note that the equation corresponding to row3 is
$42 = -2 \cdot 114 + 1 \cdot 270$;

$$42 = 42 \tag{1.1.5}$$

Step 3: continue, until the remainder (the first entry in the new row) is 0
$row4 := row2 - iquo(114, 42) \cdot row3$;

$$[30, 5, -2] \tag{1.1.6}$$

$row5 := row3 - iquo(42, 30) \cdot row4$;

$$[12, -7, 3]$$

$row6 := row4 - iquo(30, 12) \cdot row5$;

$$[6, 19, -8]$$

$row7 := row5 - iquo(12, 6) \cdot row6$;

$$[0, -45, 19]$$

This means the row 6 gives the solution for the Bezout's identity:
$6 = 19 \cdot 114 - 8 \cdot 270$;

$$6 = 6 \tag{1.1.10}$$

So, in the Bezout's Identity $t = 19$ **and** $s = -8$, and (114,270)=6. The matrix resulting from the Extended Euiclid's Algorithm is

$EEAmatrix := Matrix(7, 3, [row1, row2, row3, row4, row5, row6, row7])$;

$$\begin{bmatrix} 270 & 0 & 1 \\ 114 & 1 & 0 \\ 42 & -2 & 1 \\ 30 & 5 & -2 \\ 12 & -7 & 3 \\ 6 & 19 & -8 \\ 0 & -45 & 19 \end{bmatrix} \quad (1.1.11)$$

(**B**) a=600 and b=11312 .
(*Class work*):

Corollary 6: Two numbers a and b are coprime iff there are integers r and s such that $a \cdot r + b \cdot s = 1$:

Proof:
1. Let a and b be coprime, $(a, b) = 1$. Then by the Bezout's Identity, $a \cdot r + b \cdot s = 1$ has a solution $\{r, s\}$.

2. Let $a \cdot r + b \cdot s = 1$ has a solution $\{r, s\}$. Assume $(a, b) = d > 1$. Then $a = d \cdot a_1$ **and** $b = d \cdot b_1 \Rightarrow d \cdot (a_1 r + b_1 s) = 1$. This is impossible because d cannot divide 1. Thus, d=1 and a and b must be coprime.

Corollary 7: If c divides a and c divides b, then c divides $(a, b) = d$:

Proof:
If $a = c \cdot f$ **and** $b = c \cdot g$ then from the Bezout's Identity follows
$$d = a \cdot r + b \cdot s = c \cdot (f \cdot r + g \cdot s) \Rightarrow c | d.$$

Note that this corollary basically states that *any* common divisor of a and b is a factor of their greatest common divosor.

Example: The number c=3 divides $a = 45$ **and** $b = 75$. And 3 also divides $(45, 75) = 15 \quad (= 3 \cdot 5)$

The following corollary is of the great importance for the ***Fundamental Theorem of Arithmethics***:

Corollary 8: If a divides bc and $(a, b) = 1$ then a divides c.

Proof:
The Bezout's Identity follows that $a \cdot r + b \cdot s = 1$ for some integers r **and** s. Mutiplying this equation by c, we can write $a \cdot r \cdot c + b \cdot s \cdot c = c \Rightarrow a \cdot r \cdot c + (b \cdot c) \cdot s = c$.

However, if a divides $(bc) \Rightarrow bc = a \cdot t$ for some integer t. Therefore $a \cdot (rc + t \cdot s) = c$, which means that a divides c.

Diophantine Equations (Ch. 3E)

Using the Bezout's Identity Theorem, one can prove the following important proposition:

Proposition (#10, p.44): Given integers a, b, c (>0), there are integers x and y such that $a \cdot x + b \cdot y = c$ if and only if $(a, b) = d$ divides c.

Proof:

1. Let d divides c, i.e. $c = d \cdot m$, $m \geq 1$. Then $a \cdot r + b \cdot s = d$ for some $r, s \in \mathbb{Z}$. Hence, $a \cdot r \cdot m + b \cdot s \cdot m = d \cdot m = c$, so $x = r \cdot m$ **and** $y = s \cdot m$ solve $a \cdot x + b \cdot y = c$.

2. Let $a \cdot x + b \cdot y = c$ for some x and y, and $(a, b) = d$. Then $d \cdot \left(a_1 x + b_1 y\right) = c$ so d divides c.

NOTE: Equation $a \cdot x + b \cdot y = c$ is called ***Linear Diophantine Equation***.

***Example* 1:**
Find a solution to the equation $365\, x + 1876\, y = 24$.

***Solution* 1:**
Check first the GCD: $gcd(365, 1876)$;

$$1 \tag{1.2.1}$$

These numbers are coprime. Since 1 divides 24, the equation must be consistent.
Solve first the Bezout's Identity. Using the Extenden Euclead's algorithm, we find

$row1 := [1876, 0, 1]$;
$row2 := [365, 1, 0]$;

$$[1876, 0, 1]$$

$$[365, 1, 0] \tag{1.2.2}$$

Find the 3d, 4th, etc rows by elementary row operations

$row3 := row1 - iquo(row1[1], row2[1]) \cdot row2$;

$$[51, -5, 1] \tag{1.2.3}$$

$row4 := row2 - iquo(row2[1], row3[1]) \cdot row3$;

$$[8, 36, -7] \tag{1.2.4}$$

$row5 := row3 - iquo(row3[1], row4[1]) \cdot row4$;

$$[3, -221, 43] \tag{1.2.5}$$

$row6 := row4 - iquo(row4[1], row5[1]) \cdot row5$;

$$[2, 478, -93]$$

$row7 := row5 - iquo(row5[1], row6[1]) \cdot row6;$

$$[1, -699, 136] \quad (1.2.7)$$

Obviously, the next step will produce 0 in the first position, so we can stop here.
The equation coresponding to row7 is:

$1 = -699 \cdot 365 + 136 \cdot 1876;$

$$1 = 1$$

Multiplying the equation by 24, we find a solution for the initial Diophantine equation
$(-699 \cdot 24) \cdot 365 + (136 \cdot 24) \cdot 1876 = 24$

$$24 = 24 \quad (1.2.9)$$

Thus, the numbers solving LDE are $x = -16776$ **and** $y = 255136$.

Solution **2:**

A more efficient method for solving the LDE would imply stopping the EEA as soon as the remainder r_k of the algorithm would divide c. By inspection, we see that the *row4* of the EEA matrix corresponds to $8 = 36 \cdot 365 - 7 \cdot 1876;$

$$8 = 8$$

Then, multiplying this equation by 3, we find $24 = 108 \cdot 365 - 21 \cdot 1876;$

$$24 = 24 \quad (1.2.11)$$

Thus, we found another solution for the given Diophantine Equation with much smaller coefficients:
$x = 108$ **and** $y = -21$.
This raises the quation: how many solutions are possible, and what is the general solution for the LDE?

Proposition (#11, p,45): Let x_0 and y_0 be a solution of $a \cdot x + b \cdot y = c$. Then the general solution of
$a \cdot x + b \cdot y = c$ is of the form $x = x_0 + z,\ y = y_0 + w$ where z, w is any solution of $a \cdot z + b \cdot w = 0:$

Proof: Let $\{x, y\}$ **and** $\{x_0, y_0\}$ be two solutions of the given equation, i.e.
$a \cdot x + b \cdot y = c:$
$a \cdot x_0 + b \cdot y_0 = c:$
Subtracting the second equation from the first results in
$a \cdot (x - x_0) + b \cdot (y - y_0) = 0$
Thus, denoting $z = x - x_0$ **and** $w = y - y_0$, we find $a \cdot z + b \cdot w = 0$, so the general solution should be in the form $x = x_0 + z,\ y = y_0 + w$

NOTE: this proposition is similar to solution of a system of linear equations $A\boldsymbol{x}=\boldsymbol{b}$:
the general solution $\boldsymbol{x}=\boldsymbol{u}+\boldsymbol{v}$, where $\boldsymbol{u}$ is some solution of the system $A\boldsymbol{x}=\boldsymbol{b}$, and $\boldsymbol{v}$ is any vector in the kernel of A: $A\boldsymbol{v}=\boldsymbol{0}$.

Proposition (#12, p,45): The general solution of $a \cdot x + b \cdot y = 0$ is
$x = \frac{b}{d} n,\ y = -\frac{a}{d} n:$ where $d=(a,b)$ and $n \in \mathbb{Z}$.

Proof:
If d=(a,b) , then $a=d\cdot a_1$ **and** $b=d\cdot b_1$, where $\left(a_1, b_1\right)=1$.
From $a\cdot x+b\cdot y=0$ follows $a_1\cdot x=-b_1\cdot y$. Because a_1 **and** b_1 are coprime, the latter equation is consistent only if x is a multiple of b_1 and y is a multiple of a_1 , namely, if $x=nb_1=\frac{b}{d}n$ and $y=-na_1=-\frac{a}{d}n$.

***Corollary*:** If x_0, y_0 is a solution of $a\cdot x+b\cdot y=c$, then all solutions of this equation are
$x=x_0+\frac{b}{d}\cdot k$:
$y=y_0-\frac{a}{d}\cdot k$:
for any $k\in\mathbb{Z}$, where $d=(a, b)$:

***Example* 2:**
(A) Find all solutions of the equation $114\,x+270\,y=0$:
(B) Find all solutions of the equation $114\,x+270\,y=24$:

***Solution*:**
(A) Recall from the Exercise 1 above that GCD of 114 and 270 is 6. Thus, the given homogeneous equation is reduced to $19\,x+45\,y=0$:
The general solution of this equation is
$x_0:=45\cdot k$:
$y_0:=-19\cdot k$:
where k is any integer.

(B)
The EEA matrix constructed earlier in Ex.1 above is

$$\begin{bmatrix} 270 & 0 & 1 \\ 114 & 1 & 0 \\ 42 & -2 & 1 \\ 30 & 5 & -2 \\ 12 & -7 & 3 \\ 6 & 19 & -8 \\ 0 & -45 & 19 \end{bmatrix}$$

The 5-th row of it implies the equation $12=-7\cdot 114+3\cdot 270$;

$$12=12 \qquad \textbf{(1.2.12)}$$

By multiplying it by 2 we find $24=-14\cdot 114+6\cdot 270$;

$$24=24 \qquad \textbf{(1.2.13)}$$

So the general solution is $x=-14+45\cdot k,\ y=6-19\cdot k$.

***Exercise* 2** (*class*):
Find all solutions of the equation $49\,x + 35\,y = 42$:

***Solution*:**

Factorization (Ch. 4)

Induction

Induction Theorem : Let P(n) be a statement that is defined for any integer $n \geq n_0$.
P(n) is true for all integers $n \geq n_0$ if the following two statements are (or *could be shown to be*) true:
1. $P(n_0)$ is true.
2. If $P(n)$ is true for some $n \geq n_0$, then $P(n+1)$ is also true.

***Example*:** *Prove* that the number 8 divides $P(n) = 3^{2n} - 1$ for all $n \geq 0$:

***Proof*:**
1. $P(0) = 3^0 - 1 = 0$, therefore 8 divides P(0).
2. Assume 8 divides $P(k) = 3^{2k} - 1$: Then
 $P(k+1) = 3^{2k+2} - 1 = 3^{2k} \cdot 3^2 - 3^2 + 3^2 - 1$
 $= (3^{2k} - 1) \cdot 3^2 + 8 = 9 \cdot P(k) + 8$:
Because 8 divides P(k) and 8 divides 8, follows that 8 divides P(k+1).

A modification of the I*nduction Theorem* is the ***Complete Induction Theorem***, where he second statement is replaced by the following:
2. If P(k) is true for any $n_0 \leq k < n$, **then** it is true also for $k = n$.
This is simlar to the Induction Theorem because the statement "if P(k) is true for any $k < n$ " means that it is true for $k = (k-1)$, so the counting logic of the I*nduction Theorem* can be applied for P(k).

Recall that by definition, a number p is called prime if it is divisible only by itself and 1, i.e. $p = p \cdot 1$ is the only possible factorization of p. We take convention that ***product of primes*** may consist of only one factor, say, $17 = 17 \cdot 1 = 17$.

***Lemma* 1:** If p is prime and p divides $b \cdot c$, then p divides b or p divides c (*or both b and c* !).

In other words, this Lemma says that p must be a factor either in b or in c. Intuitively, proof is based on the fact that p cannot be factored to a product of two integers, so it must be in full a factor in at least one of these numbers b or c.

Proof: If p divides b, the statement is true.
If p does not divide b then $(p, b) = 1$ because p is prime. But then by the ***Corollary 8*** of the previous section,
p divides c because it divides $b \cdot c$.

Theorem: Every natural number factors into a product of primes.

Proof: If n>1 is prime then factorization is obvious because $n = n$, and n is prime (by convention, product may include just one factor.)
Otherwise $n = a \cdot b$ with $1 < a, b < n$: But then by *complete induction*, both a and b can be factored,

$a = a_1 \cdot \ldots a_k;$
$b = b_1 \cdot \ldots b_q$:
so then $n = a_1 \ldots \cdot a_k \cdot b_1 \cdot \ldots \cdot b_q$: i.e n is factored.

Fundamental Theorem of Arithmetic: Any natuaral number $n > 1$ factors **uniquely** into a product of primes.

By the previous Theorem, every natural number can be factored.
Proof of uniqueness of factorization is done by a method of *complete induction*, using the Lemma 1 above.

Proof:
1 The statement is obviously true for n=2 (which is prime).

2. Let the statement be true for any $2 \le k < n$. Conider factorization of n.
If n is prime the statement is true (the only factoriazation is n*1).
If n is not prime then $n = p \cdot k$ for some prime p. Because $p > 1 \Rightarrow k < n$.
Assume another factorization of n. Because p divides n, by the Lemma 1, p must be equal to a factor, call it q_1, in that second factorization $n = p \cdot q_2 \cdot \ldots \cdot q_s = p \cdot k \cdot$. But then
$k = q_2 \cdot \ldots \cdot q_s$, and this factorization is unique because $k < n$.

Example:
ifactor(45);

$$(3)^2 (5) \tag{2.1}$$

ifactor(30723);

$$(3)\ (7)^2\ (11)\ (19) \tag{2.2}$$

Exercise:

Show that if n is not prime it has a prime divisor $\leq \sqrt{n}$.

Solution: (*class*)

Least Common Multiple:

Definition: A number c is said to be a ***common multiple*** of a and b if both a and b divide c.

Example:
Let $a = 12$ **and** $b = 8$. The number $c = 48$ is divisible by both 12 and 8: $48 = 12 \cdot 4$, **and** $48 = 8 \cdot 6$, so it is a common multiple of a and b. Also the numbers $\{24, 72, 96, ...\}$ all are common multiples of 12 and 8.

The smallest of all common multiples of a and b is the ***least common multiple*** (LCM) and is denoted LCM, or $[a, b]$. For example, [12,8]=24, [6,10]=30.

Proposition : The least common multiple of a and b is the product divided by the greatest common divisor, $[a, b] = \dfrac{a \cdot b}{(a, b)}$:

Proof: (Euclid).
Let $(a, b) = 1$. The product $s = a \cdot b = \dfrac{a \cdot b}{(a, b)}$ is obviously a common multiple of a and b.
Show that s divides any other common multiple c of a and b. Because a divides c, $\Rightarrow c = a \cdot q$.
But because b also divides c, and a **and** b are coprime, b must divide q, $\Rightarrow q = b \cdot t$, *with* $t \geq 1$.
Hence, $c = a \cdot b \cdot t = s \cdot t$. But then the smallest common multiple of a and b is s.

Consider now the general case $(a, b) = d$:
We can write $a = a_1 d$ **and** $b = b_1 d$, so that $(a_1, b_1) = 1$.

Then $s = \dfrac{a \cdot b}{d} = a_1 b_1 d = a_1 b = a \cdot b_1$.

So both a and b divide s, which says that s is a common multiple of a and b.
Suppose now that m is another common multiple of a and b. Then d divides m because d is a factor in a and *in* b.
So $m = m_1 \cdot d$ for some m_1.
Because $a = a_1 d$ divides $m = m_1 \cdot d$, then a_1 divides m_1. Therefore
$m_1 = a_1 \cdot q \Rightarrow m = a_1 \cdot \boldsymbol{q} \cdot d$.
Because also $b = b_1 d$ divides $\boldsymbol{m}$, and b_1 and a_1 are coprime, b_1 must divide $\boldsymbol{q}$. So $q = b_1 \cdot t$, **and**
$m = \boldsymbol{d \cdot a_1 \cdot b_1} \cdot t = \boldsymbol{s} \cdot t$ for $t \geq 1$.
This means that indeed $[a, b] = s$.

Example:
Find LCM of 210 and 126:

Solution:
$d := gcd(210, 126);$

$$42 \qquad \textbf{(2.3)}$$

$LCM := \dfrac{210 \cdot 126}{d};$

$$630 \qquad \textbf{(2.4)}$$

Check: $lcm(210, 126);$

$$630 \qquad \textbf{(2.5)}$$

Primes:

Theorem 9: There are infinitely many primes.

Proof:
Suppose the set of primes is finite, $P = \{p_1, p_2, ..., p_k\}$. Construct a number $m = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$.
(*Class:* continue....)