LECTURE 2: taken from Chapter 2 of Stillwell's Elements of Number Theory.

§2.1 The gcd by subtraction

If natural #'s a & b have common divisor d then this indicates $\exists\, a', b' \in \mathbb{N}$ s.t.

$$a = a'd \quad \text{and} \quad b = b'd$$

Hence,

$$a - b = a'd - b'd = (a' - b')d$$

$$\left[\, d \mid a \text{ and } d \mid b \Rightarrow d \mid (a-b) \,\right]$$

Since $d > 0$ and $a, b < \infty$ there must exist a largest (greatest) common divisor, the $\gcd(a,b)$

<u>Algorithm</u>: § $a > b$ and let

$$a_1 = a, \quad b_1 = b$$

Define $a_{i+1} = \max(b_i, a_i - b_i)$, $b_{i+1} = \min(b_i, a_i - b_i)$
these #'s decrease ... eventually must reach n for which $a_n = b_n$ and $\gcd(a,b) = a_n = b_n$.
In fact, $\gcd(a_1, b_1) = \gcd(a_2, b_2) \cdots = \gcd(a_n, b_n)$

<u>Example</u>: $a = 17$, $b = 6$

$(a_1, b_1) = (17, 6)$ $\quad 17 - 6 = 11$
$(a_2, b_2) = (11, 6)$ $\quad 11 - 6 = 5$
$(a_3, b_3) = (6, 5)$ $\quad 6 - 5 = 1$
$(a_4, b_4) = (5, 1)$ $\quad 5 - 1 = 4$
$(a_5, b_6) = (4, 1)$ $\quad 4 - 1 = 3$
$(a_6, b_6) = (3, 1)$ $\quad 3 - 1 = 2$
$(a_7, b_7) = (2, 1)$ $\quad 2 - 1 = 1$
$(a_8, b_8) = (1, 1)$ $\quad \rightarrow \underbrace{\gcd(17, 6) = 1}$

17 and 6 are <u>coprime</u> or <u>relatively prime</u>.

§2.2: THE GCD BY DIVISION WITH REMAINDER:

This version of Euclid's Algorithm is <u>faster</u>.

Given pair (a_i, b_i) with $a_i > b_i$ the next pair is:

$$a_{i+1} = b_i \,, \quad b_{i+1} = \text{remainder of } \frac{a_i}{b_i}$$

This eliminates some steps where $a_i = a_{i+1}$ in §2.1 method.
However, $\gcd(a_1, b_1) = \gcd(a_2, b_2) = \cdots$ so same result holds.
(see my typed notes for some proof of these assertions)

HALT when $b_k \mid a_k$ and conclude $\gcd(a_1, b_1) = b_k$

Example: $a = 17$, $b = 6$ (again.)

$$(a_1, b_1) = (17, 6)$$
$$(a_2, b_2) = (6, 5)$$
$$(a_3, b_3) = (5, 1)$$
$$(a_4, b_4) = (1, 1) \hookrightarrow \underline{\gcd(17, 6) = 1}.$$

Comment: in $\mathbb{N}$ it is true that division is repeated subtraction, however, in $\mathbb{Z}[i]$ Stillwell argues that the division algorithm here still works whereas $17 = (4+i)(4-i) \hookrightarrow \frac{17}{4-i} = 4+i$ does this still ~~mean "(4-i) subtractions" 4+i to times gives~~ ... mean repeated subtraction?

Example: $a = 24$, $b = 4$

$$(a_1, b_1) = (24, 4) \hookrightarrow \gcd(24, 4) = 4$$
$$\cancel{= (4, 0)}$$

as $4/24$.

Consider the algebra below,

$$\frac{a}{b} = \frac{bq + r}{b} = q + \frac{r}{b} = q + \frac{1}{b/r}$$

$$\frac{b}{r} = \frac{r q_2 + r_2}{r} = q_2 + \frac{r_2}{r} = q_2 + \frac{1}{r/r_2}$$

$$\frac{r}{r_2} = \frac{r_2 q_3 + r_3}{r_2} = q_3 + \frac{1}{r_2/r_3}$$

$$\frac{r_2}{r_3} = \frac{r_3 q_4 + r_4}{r_3} = q_4 + \frac{1}{r_3/r_4}$$

Compare with

$$(a, b) \longrightarrow (b, r) \longrightarrow (r, r_2) \longrightarrow (r_2, r_3) \longrightarrow (r_3, r_4) \rightarrow \vdots$$

Therefore, we find a close connection between the continued fractions and Euclid's Algorithm,

$$\frac{a}{b} = q + \frac{1}{\frac{b}{r}} = q + \frac{1}{q_2 + \frac{1}{\frac{r}{r_2}}}$$

$$= q + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\frac{r_2}{r_3}}}} \cdots$$

Example:

$(34, 19)$
$(19, 15)$
$(15, 4)$
$(4, 3)$
$(3, 1)$

$$\frac{34}{19} = 1 + \frac{1}{19/15}$$

$$= 1 + \frac{1}{1 + 4/15}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{3}{4}}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{3}}}}.$$

§2.3 LINEAR REPRESENTATION OF THE GCD

Proposition: $\gcd(a,b) = ma + nb$ for some $m, n \in \mathbb{Z}$. Moreover, all #'s a_i, b_i in Euclid's algorithm appear as $\mathbb{Z}$-linear combinations of a & b.

Proof: Suppose $a > b$ and set $a_1 = a$, $b_1 = b$. Observe,

$$a_1 = 1\cdot a + 0\cdot b \quad \& \quad b_1 = 0\cdot a + 1\cdot b.$$

Next assume inductively $a_i = m_a a + n_a b$ and $b_i = m_b a + m_b b$ observe,

$$a_i - b_i = (m_a - m_b)a + (n_a - n_b)b$$

page 23 of Stillwell in case you forgot.

and as $a_{i+1} = \max(b_i, a_i - b_i)$ and $b_{i+1} = \min(b_i, a_i - b_i)$ it follows a_{i+1} and b_{i+1} are $\mathbb{Z}$-linear comb. of a & b. //

Example:

$$(a_1, b_1) = (17, 6) = (a, b)$$

$$\Rightarrow (6, 5) = (b, a - 2b)$$

$$\Rightarrow (5, 1) = (a - 2b, b - (a - 2b)) = (a-2b, \underbrace{3b-a})$$

$$\Rightarrow (1, 1) = (3b - a, a - 2b - 4(3b - a))$$

$$= (3b - a, 5a - 14b)$$

could stop here really, this already shows $\gcd(17,6) = 1$ and

$$\boxed{-17 + 3(6) = 1} \qquad \boxed{5(17) - 14(6) = 1}$$

- See pg. 36 for more about the purple bit. Not important for §2.3.

$$\Rightarrow (1, 0) = (3b - a, \underbrace{(5a - 14b) - (3b - a)}_{\boxed{6a - 17b = 0}})$$

§ 2.4 PRIMES AND FACTORIZATION

Th^m/ Each natural number n can be written as a product of primes; $n = p_1 p_2 \cdots p_k$

Proof: If $n = ab$ and both a, b prime then done. Otherwise, if a prime (wlog) then $a = a'b'$ and if a', b' prime then $n = a'b'b$ and we're done. Otherwise, (wlog) $a' = a''b''$ and again either a'', b'' both prime or we continue breaking into factors. However

$$a > a' > a'' \quad \text{etc..}$$

Hence by descent this terminates and we find the desired result //

Existence of $p_1, p_2, .., p_n$ for which $n = p_1 p_2 \cdots p_n$ is interesting, but, uniqueness is even better. We work towards proof of uniqueness upto reordering.

Th^m/ PRIME DIVISOR PROPERTY: (Euclid 300 BC)
If a prime $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: Suppose $p \mid ab$ but $p \nmid a$ then it remains to show $p \mid b$. Notice $p \nmid a \Rightarrow \gcd(a, p) = 1 \Rightarrow \exists m, n \in \mathbb{Z}$, $ma + np = 1$. Multiply by $b \Rightarrow b = mab + npb$. By assumption $\exists j \in \mathbb{Z}$ for which $ab = jp$ $\therefore$ $b = mjp + npb = (mj + nb)p$ which shows $p \mid b$ as desired. //

Th^m/ UNIQUE PRIME FACTORIZATION: (Gauss 1801)
The prime factorization of each $n \in \mathbb{N}$ is unique up to reordering

Proof: Suppose towards $\rightarrow\leftarrow$ $\boxed{p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_\ell}$ * ← all primes.
where $p_i \neq q_j$ $\forall i,j$. (no loss of generality as common factors could be cancelled before this argument)

Note $* \Rightarrow p_1 \mid q_1(q_2 \cdots q_\ell)$ $\therefore$ $p_1 \mid q_1$ or $p_1 \mid (q_2 \cdots q_\ell)$

continuing we deduce

$p_1 \mid q_1$ or $p_1 \mid q_2$ or $\ldots$ or $p_1 \mid q_\ell$

Hence,

$p_1 = q_1$ or $p_1 = q_2$ $\cdots$ or $p_1 = q_\ell$ which contradicts $p_i \neq q_j$ $\forall i,j$. //

§2.5 CONSEQUENCES OF UNIQUE PRIME FACTORIZATION:

If $c = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ then $c^2 = p_1^{2m_1} p_2^{2m_2} \cdots p_n^{2m_n}$

Also if $d = p_1^{2m_1} p_2^{2m_2} \cdots p_n^{2m_n}$ then $d = c^2$.

Th^m/ A natural number n is a square iff each prime in n is an even power.

Further, if $d = ab$ and $\gcd(a,b) = 1$ then $d = c^2 \Rightarrow a = c_1^2$ and $b = c_2^2$ by the Th^m above.

Th^m/ If a, b are relatively prime and ab is a square then both a and b are squares.

Similar results hold for cubes.

Thm/ If N is a nonsquare natural number then $\sqrt{N}$ is irrational

Proof: Suppose $N \in \mathbb{N}$ and $\sqrt{N} \in \mathbb{Q}$ then $\exists a, b \in \mathbb{N}$ for which $\sqrt{N} = a/b$. Squaring both sides,

$$N = a^2/b^2 = \underbrace{p_1^{2m_1} p_2^{2m_2} \cdots p_n^{2m_n}}_{\text{formed by cancelling appropriate powers in the prime factorization of } b^2}$$

Thus N is a square. Consequently, if N is a nonsquare then $\sqrt{N} \notin \mathbb{Q}$ which shows $\sqrt{N}$ is irrational. //

Prime factorization, gcd, and lcm

Unique prime factorization $\Rightarrow$ $p/n \iff n = p\, p_2^{m_2} \cdots p_n^{m_n}$ primes divide n only when they appear in the factorization. So, $\gcd(a,b) | a$ and $\gcd(a,b) | b$ means whatever prime in $\gcd(a,b)$ must appear in prime factorization of <u>both</u> a & b.

Example: $500 = 4 \times 125 = 4 \times 5 \times 25 = \underline{2}^2 \times \underline{\underline{5}}^3$

$300 = 3 \times 100 = 3 \times 4 \times 25 = \underline{2}^2 \times 3 \times \underline{\underline{5}}^2$

$$\gcd(300, 500) = 2^2 \cdot 5^2 = 4 \cdot 25 = \underline{100}.$$

wins. $\left\{ \begin{array}{l} (500, 300) \\ (300, 200) \\ (200, 100) \longrightarrow \underline{\gcd(500, 300) = 100}. \end{array} \right.$

Example: $4444 = 4 \times 1111 = 4 \times 11 \times 101 = 2^2 \times 11 \times 101$
$9090 = 9 \times 1010 = 9 \times 10 \times 101 = 3^2 \times 2 \times 5 \times 101$

$$\gcd(4444, 9090) = 2 \cdot 101 = 202.$$

$(9090, 4444)$

$(4444, 202) \longrightarrow \gcd(4444, 9090) = 202.$

~~(102, 78)~~

~~(78,~~

for comparison to Euclid's method.

$$\begin{array}{r} 9090 \\ -\,8888 \\ \hline 202 \end{array}$$

$$\begin{array}{r} 22 \\ 202 \overline{)\,4444} \\ 404 \\ \hline 404 \\ 404 \\ \hline \boxed{0} \end{array}$$

$\therefore 202 \mid 4444.$

- least common multiple: product of maximum prime powers appearing in their prime factorizations

Example: $4444 = 2^2 \times 11 \times 101$
$9090 = 2 \times 3^2 \times 5 \times 101$

$$\text{lcm}(4444, 9090) = 2^2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 101 = 199{,}980.$$

FUN FACT (Ex. 2.5.5 pg. 33) $\gcd(a,b)\,\text{lcm}(a,b) = ab$

Hence $\text{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)} = \dfrac{(4444)(9090)}{202} = 199{,}980.$

§2.6 Linear Diophantine Equations

Consider the following

$$\boxed{ax + by = c}$$

where $a, b, c \in \mathbb{Z}$ and we seek $x, y \in \mathbb{Z}$ which solve this linear Diophantine Eq^{n} in 2-variables.

Example: $6x + 15y = 0$

Has sol^{n} $x = 15t$, $y = -6t$ $\forall t \in \mathbb{Z}$.

Example: $ax + by = 0$

Has sol^{n} $x = bt$, $y = -at$ $\forall t \in \mathbb{Z}$.

But, sometimes, $\nexists$ any sol^{n}'s.

Example: $6x + 15y = 1$ has no sol^{n} since the l.h.s. would be divisible by 3 yet the r.h.s. is not divisible by 3.

Example: $6x + 15y = 3 \longleftrightarrow 2x + 5y = 1$ Sorry messy. Anyway, better.

$\gcd(6, 15) = 3.$

$(15, 6) = (a, b)$

$(6, 3) = (b, a - 2b)$

$\cancel{(3, 0)}$

$3 = a - 2b$

$\Rightarrow x = 1, \; y = -2$

~~Check: 2·6(1) + 15(-2) = 24.~~

$1 \cdot 15 - 2 \cdot 6 \overset{\checkmark}{=} 3$

general sol^{n}: $x = 1 + t(6)$, $y = -2 - t(15)$.

$15(1 + 6t) + 6(-2 - 15t) = 15 - 12 \overset{\checkmark}{=} 3$

CRITERION FOR SOLVABILITY OF LINEAR DIOPHANTINE EQ$^{\underline{n}}$S

When $a, b, c \in \mathbb{Z}$ the eq$^{\underline{n}}$ $ax + by = c$ has an integer sol$^{\underline{n}}$ iff $\gcd(a,b)$ divides c.

<u>Proof</u>: since $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b \Rightarrow$ $\gcd(a,b) \mid (ax+by)$ $\forall x, y \in \mathbb{Z}$. Therefore, if $\exists x, y$ s.t. $ax + by = c$ then $\gcd(a,b) \mid c$.
Conversely, if $\gcd(a,b) \mid c$ then $[\gcd(a,b)]j = c$ for some $j \in \mathbb{Z}$ and we also know $\exists m, n \in \mathbb{Z}$ s.t. $am + bn = \gcd(a,b)$ hence

$$c = \gcd(a,b)\, j = (am+bn)j = a(mj) + b(nj)$$

thus $x = mj$, $y = nj$ gives integer sol$^{\underline{n}}$ to $ax+by=c$. //

Algorithm to solve $ax+by=c$

1.) Check if $c \mid \gcd(a,b)$. If $c = d \cdot \gcd(a,b)$ then continue, else stop since no sol$^{\underline{n}}$ exists when $c \nmid \gcd(a,b)$.

2.) Find m, n for which $am + bn = \gcd(a,b)$

3.) Set $x_0 = md$ and $y_0 = nd$, this solves $ax+by=c$.

4.) To form the <u>general</u> <u>sol$^{\underline{n}}$</u> write:

$$x = x_0 + \frac{bt}{\gcd(a,b)}$$

$$y = y_0 - \frac{at}{\gcd(a,b)}$$

return 0 as $0 = a\left(\frac{bt}{\gcd(a,b)}\right) + b\left(\frac{-at}{\gcd(a,b)}\right)$

produce c as $ax_0 + by_0 = c$.

Proof of Algorithm to find sol$^{\text{n}}$ of $ax+by=c$

Observe if $c \mid \gcd(a,b)$ then $\exists\, m,n \in \mathbb{Z}$ s.t. $am+bn = \gcd(a,b)$ and $c = d\cdot\gcd(a,b)$ for some $d \in \mathbb{Z}$. Hence $a(md)+b(nd) = d\gcd(a,b) = c$ which proves $ax_0+by_0 = c$ for $x_0 = md$, $y_0 = nd$.

Moreover, $x = \dfrac{bt}{\gcd(a,b)}$, $y = \dfrac{-at}{\gcd(a,b)}$ clearly has

$$ax+by = a\left(\frac{bt}{\gcd(a,b)}\right) + b\left(\frac{-at}{\gcd(a,b)}\right) = 0$$

where $b/\gcd(a,b)$, $\dfrac{a}{\gcd(a,b)} \in \mathbb{Z}$ since the $\gcd(a,b)$ divides both a and b. Finally,

$$a(x+x_0)+b(y+y_0) = \underbrace{ax+by}_{0} + \underbrace{ax_0+by_0}_{c} = c.$$

Conversely, if x,y is any sol$^{\text{n}}$ of $ax+by=c$ then $x' = x-x_0$ and $y' = y-y_0$ gives

$$ax'+by' = ax-ax_0+by-by_0 = c-c = 0.$$

Hence, x',y' solve $a'x' = -b'y'$ where

$a' = \dfrac{a}{\gcd(a,b)}$ and $b' = \dfrac{b}{\gcd(a,b)}$ have $\underline{\gcd(a',b') = 1.}$ *

Thus a',b' have no common divisor $\Rightarrow$ by prime divisor property, $a'x' = -b'y' \Rightarrow b' \mid x' \Rightarrow \underline{x' = b't}$. for some $t \in \mathbb{Z}$, $\therefore a'b't = -b'y' \Rightarrow \underline{y' = -a't}$.

We found $x' = b't$ and $y' = -a't$ hence,

$$x' = x - x_0 = \frac{bt}{\gcd(a,b)}$$

$$y' = y - y_0 = \frac{-at}{\gcd(a,b)}$$

Therefore, $x = x_0 + \dfrac{bt}{\gcd(a,b)}$ & $y = y_0 + \dfrac{(-at)}{\gcd(a,b)}$.

* **Claim**: $\gcd(a', b') = 1$ where $a' = \dfrac{a}{\gcd(a,b)}$ and $b' = \dfrac{b}{\gcd(a,b)}$.

Proof: ~~$a = a'\gcd(a,b)$ and $b = b'\gcd(a,b)$ thus $a' \mid a$ and $b' \mid b$. If $a' \mid b'$ then we'd have $a' \mid a$ and a'~~

$$ma + nb = \gcd(a,b)$$

Divide by $\gcd(a,b)$,

$$m\underbrace{\left[\frac{a}{\gcd(a,b)}\right]}_{a'} + n\underbrace{\left[\frac{b}{\gcd(a,b)}\right]}_{b'} = \frac{\gcd(a,b)}{\gcd(a,b)} = 1.$$

$\therefore ma' + nb' = 1$

$\Rightarrow \gcd(a', b') = 1.$ //

Example: find general sol$^{\underline{n}}$ of $6x + 15y = 3$

$(15, 6) = (a, b)$

$(6, 3) = (b, a - 2b)$

Halt as $3 \mid 6$ we find $3 = a - 2b = \gcd(6, 15)$.

That is, $6(-2) + 15(1) = 3$

We find particular sol$^{\underline{n}}$ $\underline{x_0 = -2,\ y_0 = 1}$

Following 4.) we write,

$$x = -2 + \frac{6t}{3} = -2 + 2t$$
$$y = 1 - \frac{15t}{3} = 1 - 5t$$

Then $\boxed{\{(-2 + 2t, 1 - 5t) \mid t \in \mathbb{Z}\}}$ forms the sol$^{\underline{n}}$ set of $6x + 15y = 3$ in $\mathbb{Z}$.

§27 THE VECTOR EUCLIDEAN ALGORITHM

Assume $a > 0$ and $b < 0$ ⋯> Euclid. Alg. runs by addition

Numbers	Symbolic Pairs	Vector Pairs
$(12, -5)$	(a, b)	$((1,0), (0,1))$
$(7, -5)$	$(a+b, b)$	$((1,1), (0,1))$
$(2, -5)$	$((a+b)+b, b) = (a+2b, b)$	$((1,2), (0,1))$
$(2, -3)$	$(a+2b, b+(a+2b)) = (a+2b, a+3b)$	$((1,2), (1,3))$
$(2, -1)$	$(a+2b, 2a+5b)$	$((1,2), (2,5))$
$(1, -1)$	$(3a+7b, 2a+5b)$	$((3,7), (2,5))$
$(1, 0)$	$(3a+7b, \cancel{2a+5b}\ 5a+12b)$	$((3,7), (5,12))$

(this is interesting because ↴)

Relative Primality in vector Euclidean Algorithm

1.) every vector produced from $(1,0)$ and $(0,1)$ is a relatively prime pair of natural numbers (such a vector is called <u>primitive</u>)

2.) every relatively prime pair (a,b) of natural numbers can be produced (by starting the ordinary Euclidean Algorithm on b and $-a$)

1.) <u>Proof</u>: If $((m_1,n_1),(m_2,n_2))$ is vector pair at some step then $m_1n_2 - n_1m_2 = 1$. Observe true for $((1,0),(0,1))$. Moreover inductively, if it is true for $((m_1,n_1),(m_2,n_2))$ then the next pair is either

$$\underline{((m_1+m_2,\, n_1+n_2),\, (m_2,n_2))} \text{ or } \underline{((m_1,n_1),\, (m_1+m_2,\, n_1+n_2))}$$

for which we have

$$(m_1+m_2)n_2 - (n_1+n_2)m_2 = \underline{\underline{m_1n_2}} + \cancel{m_2n_2} - \underline{\underline{n_1m_2}} - \cancel{n_2m_2}$$

$$= 1 \text{ by induction step.}$$

$$m_1(n_1+n_2) - n_1(m_1+m_2) = \cancel{m_1n_1} + \underline{\underline{m_1n_2}} - \cancel{n_1m_1} - \underline{\underline{m_2n_1}}$$

$$= 1.$$

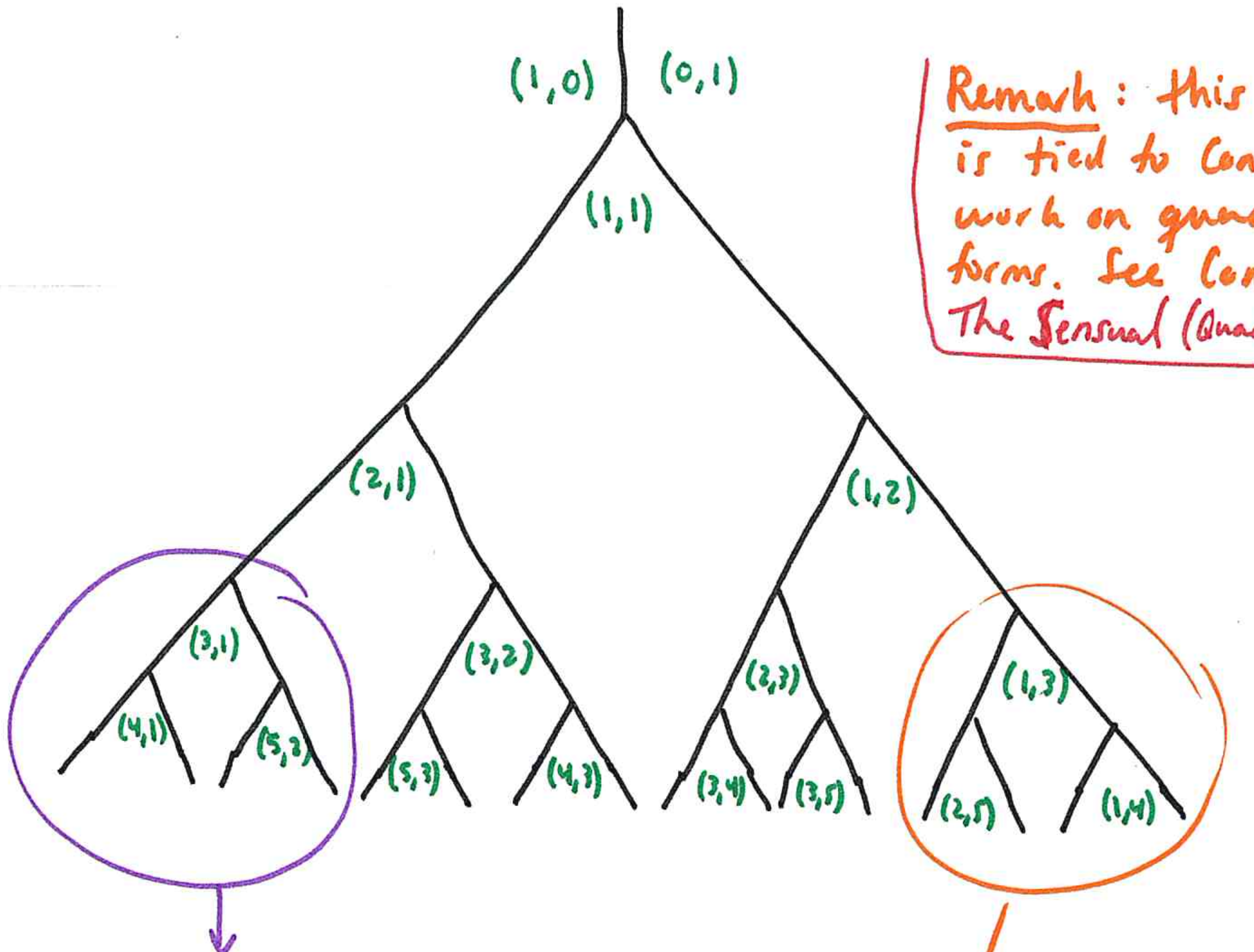
Hence $\gcd(m_1,n_1) = 1$.
Likewise $\gcd(m_2,n_2) = 1$.

(notice $n_2m_1 - n_1m_2 = 1$ $\hookrightarrow \gcd(m_1,n_1) = 1$)

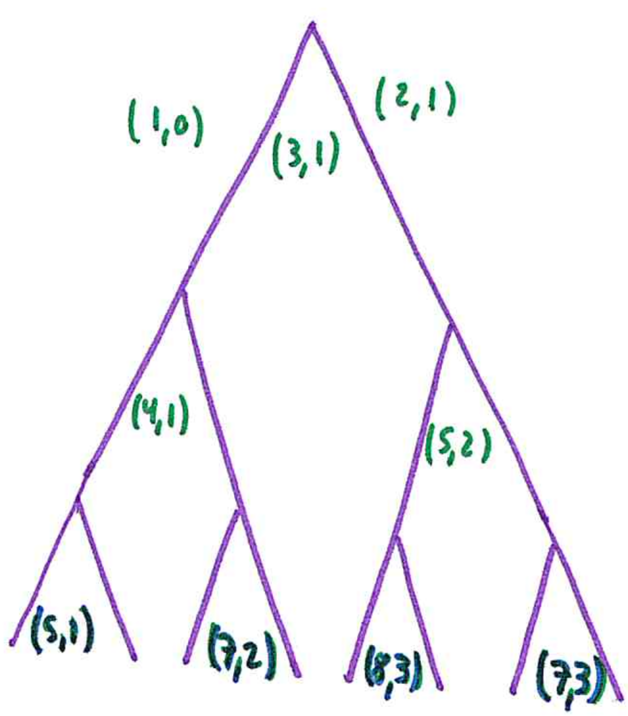
2.) If $\gcd(a,b) = 1$ for some $a,b \in \mathbb{N}$, then the vector Euclidean algorithm on $b,-a$ produces vector (m,n) s.t. $mb - na = 0$ with $\gcd(m,n) = 1$
But, $mb = na$ for relatively prime a,b & m,n $\Rightarrow m = a$ and $n = b$ $\Rightarrow$ can get (a,b) from the vect. algorithm.

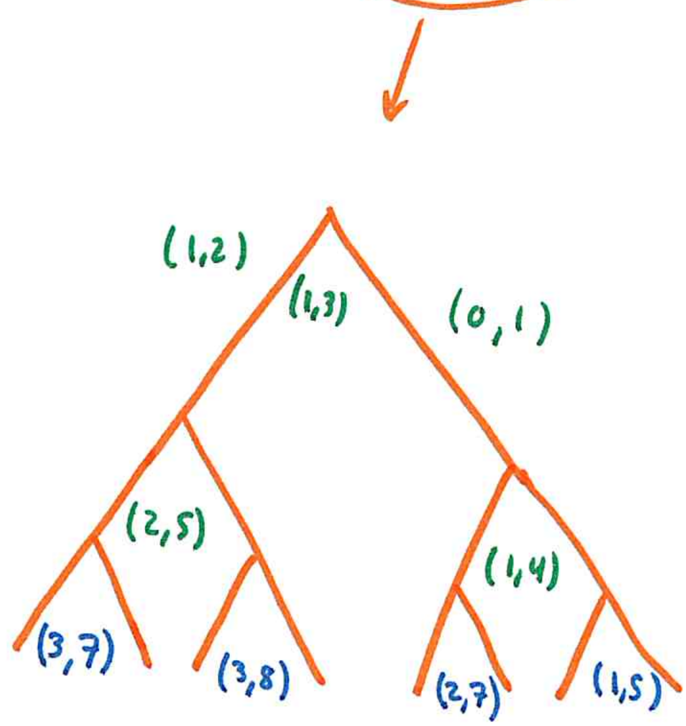
(this explains the role of tree to follow)

§2.8 The map of relatively prime pairs



Remark: this game is tied to Conway's work on quadratic forms. See Conway's The Sensual (Quadratic) Form





(the blue row may be part of the answer to a hwk I assigned ☺

§2.9 DISCUSSION

We've seen the main things that make $\mathbb{Z}$ what it is

- Ring (+ and ×)
- Has Primes (known to Euclid, mastered by Gauss)
- Unique Factorization (1801 Gauss appreciated)

However, as usual, Euler comes into the story.

In 1748 Euler presented the product formula:

$$\underbrace{\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{primes } p} \left(\frac{1}{1-p^{-s}} \right)}_{\text{the equality above} \approx \text{prime factorization of } n.}$$

Geometric series,

$$\frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \dots$$

$$\prod_{\text{primes } p} \left(\frac{1}{1-p^{-s}} \right) = \prod_{\text{primes } p} \left(1 + p^{-s} + p^{-2s} + \dots \right)$$

... get sum of 1 and $\frac{1}{2^s}, \frac{1}{3^s}, \dots$

$\Rightarrow$ product of $p_1^{-m_1 s} p_2^{-m_2 s} \cdots p_n^{-m_n s} = \dfrac{1}{(p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n})^s} = \dfrac{1}{n^s}$

Also, when $s = 1$ harmonic series diverges

$\Rightarrow$ ∞-ly many primes. (If finite # then $\prod_{\text{primes}}$ not diverge)

(BIRTH OF ANALYTIC # THEORY)

$\zeta(s)$ the zeta-function. We don't go into this as Math 331 is needed prereq. here.