From Previous Lecture

Euclidean algorithm:
$a, b \in \mathbb{Z}$, $b > 0$. We do successive divisions

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\cdots$$
$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

until $r_{n+1} = 0$. Then $\gcd(a,b) = r_n$.

Proof.

a) We show that algorithm finishes in finite time.

$$b > r_1 > r_2 > r_3 > \ldots r_n \geq 0$$

Sooner ore later we should have $r_{n+1} = 0$.

b) $\gcd(a,b) = \gcd(b,a) \overset{\text{Lemma}}{=\!=} \gcd(b, a - q_1 b)$
$= \gcd(b, r_1) \overset{\text{Lemma}}{=\!=} \gcd(r_1, b - q_2 r_1)$
$= \gcd(r_1, r_2) = \ldots = \gcd(r_n, r_{n+1})$

$= r_n.$ $\boxtimes$

Theorem. Let $a, b \in \mathbb{Z}$, $d = \gcd(a, b)$. Then there exist integers s, t such that

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

Proof. We only consider the case $a \geq b > 0$.

We will prove that for any subscript i, r_i can be written as

$$r_i = (-1)^{i+1} k_i \times a + (-1)^i h_i \times b \quad , \quad k_i, h_i \in \mathbb{Z}.$$

Then theorem applies for $i = n$.

Prove by induction.

Base: $r_{-1} = a = 1 \cdot a + 0 \cdot b$, $k_{-1} = 1$, $h_{-1} = 0$

$r_0 = b = 0 \cdot a + 1 \cdot b$, $k_0 = 0$, $h_0 = 1$

Inductional step. Assume we have the formula for $i-1$, i. Then we prove it for $i+1$.

$$r_{i-1} = (-1)^i k_{i-1} a + (-1)^{i-1} h_{i-1} b$$

$$r_i = (-1)^{i+1} k_i a + (-1)^i h_i b$$

Then $r_{i-1} = q_{i+1} r_i + r_{i+1}$ (from Euclidean algorithm)

$$r_{i+1} = r_{i-1} - q_{i+1} r_i$$

$$= \underset{\substack{\parallel \\ (-1)^{i+2}}}{(-1)^i}(k_{i-1} + q_{i+1} k_i) a + \underset{\substack{\parallel \\ (-1)^{i+1}}}{(-1)^{i-1}}(h_{i-1} + q_{i+1} h_i) b$$

Finally we take

$$k_{i+1} = k_{i-1} + q_{i+1} k_i$$

$$h_{i+1} = h_{i-1} + q_{i+1} h_i \qquad \boxtimes$$

From the proof we have a nice algorithm which constructs values d, s, t from a and b. (Extended Euclidean Algorithm, EEA).

Sumarise in a table:

$\overset{a}{\overset{\parallel}{r_{-1}}}$	$\overset{b}{\overset{\parallel}{r_0}}$	r_1	r_2	$\dots$	r_n	$r_{n+1} = 0$ ← we stop here.
		q_1	q_2	$\dots$	q_n	
$\overset{0}{\overset{\parallel}{h_{-1}}}$	$\overset{1}{\overset{\parallel}{h_0}}$	h_1	h_2	$\dots$	h_n	
$\underset{1}{\underset{\parallel}{k_{-1}}}$	$\underset{0}{\underset{\parallel}{k_0}}$	k_1	k_2	$\dots$	k_n	

The rule for the table:

A	B	R
...	...	Q
K	L	$K+L\cdot Q$
M	N	$M+N\cdot Q$

$A = QB + R$.

Example. $a = 63$, $b = 57$

63	57	6	3	0
...	...	1	9	
0	1	1^{-}	10	
1	0	1	9^{-}	

gcd(63, 57)

~~s~~ t

~~t~~ s

$$63 = 1\cdot 57 + 6$$
$$57 = 9\cdot 6 + 3$$
$$6 = 2\cdot 3 + 0$$

Finally $\gcd(63,57) = 3 = \cancel{10\cdot 63 - 9\cdot 57}$

$10\cdot 57 - 9\cdot 63$

§2 Prime and composite numbers, Factorisation.

§2.1 Primes and composites.

Q: Which numbers do we need to represent every positive integer as their product.

Definition. Let $n \in \mathbb{Z}$, $n > 1$. n is called <u>prime</u> if all its divisors are 1 and n. Otherwise it is called composite.

Remark: $0, 1$ are neither prime nor composite.

We call the set of prime numbers by $\mathbb{P}$.

Important property of primes.

Proposition. Let $a, b \in \mathbb{Z}$, p be prime. Then if $p | ab$ then either $p | a$ or $p | b$.

Proof. Assume $p | ab$

Consider $\gcd(p, a)$

(I) $\gcd(p, a) = p \Rightarrow p | a$ ✓

(II) $\gcd(p, a) = 1$

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

$$b = \underbrace{s \cdot p \cdot b}_{\text{p divides this}} + \underbrace{t \cdot a \cdot b}_{\text{p divides this}}$$

$\Longrightarrow p \mid b.$ ✓ $\boxtimes$

Remark. Sometimes this property is used as the definition of primes.

Corollary: Let $a_1, a_2, \dots, a_n \in \mathbb{Z}$, p be prime. If $p \mid a_1 a_2 \cdots a_n$ then p divides one of a_i's $(1 \leq i \leq n)$.

Proof - Ex.

First primes:

$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$