Lecture 2

Recall $d := GCD(a,b)$ $\qquad a, b \in \mathbb{Z}$

d such that $\qquad d \mid a \;\&\; d \mid b$

if $e \mid a \;\&\; e \mid b \implies e \le d$

Proposition 2 $\qquad$ Benzout's identity

Let $a, b \in \mathbb{Z}$ then there exist $r, s \in \mathbb{Z}$ such that

$$ar + bs = GCD(a,b)$$

Example

1) $GCD(6,5) = 1$ $\qquad 6 = 5 \cdot (1) + 1$

$$\implies \underset{a}{6}(\underset{r}{1}) + \underset{b}{5}(\underset{s}{-1}) = \underset{GCD(a,b)}{1}$$

2) $GCD(12, 20) =$
$= GCD(12, 8) =$
$= GCD(4, 8) = 4$

$20 = 12 \cdot (1) + 8$
$12 = 8 \cdot (1) + 4$

$$\underset{GCD(a,b)}{4} = 12 - 8 = 12 - (20 - 12) = \underset{a}{12} \cdot \underset{r}{2} + \underset{b}{20}(\underset{s}{-1})$$

Bezout's identity

Let $a, b \in \mathbb{Z}$ There exist $r, s \in \mathbb{Z}$ so that

$$ar + bs = GCD(a,b)$$

The proof is a bit similar to the proof of Euclid's algorithm

Let $S = \{ \cancel{ar+bs}\ av + bw \mid v, w \in \mathbb{Z} \text{ s.t. } av + bw > 0 \}$

S is non-empty, it has at least one element.

a or $-a$ i.e. $v = \pm 1$ $w = 0$

Since S is non empty and it is a set of positive integers by the well-ordering theorem S has a minimum element.

Let h = minimum element of S.

Our goal is to show that $h = GCD(a,b)$

A) $h \mid a$ & $h \mid b$

B) If $e \mid a$ & $e \mid b$ $\Rightarrow$ $e \leq h$

A) By Euclid $a = qh + r$ $0 \leq r < h$, $q \in \mathbb{Z}$

But then $0 \leq r = a - qh = a - q(av + bw) = a(1-qv) + b(-qw)$

$r \in S \cup \{0\}$

Since h is the minimum element of S, $0 \leq r < h$

$\Rightarrow r = 0$

So by minimality of h we must have

$r = 0 \quad \Rightarrow \quad h \mid a$

A similar argument shows that $h \mid b$

$h \mid a$ & $h \mid b$ h is a ~~comon divo~~ common divisor, a and b.

B) Now $e \mid a$ & $e \mid b$

$a = es$ & $b = et$ $s, t \in \mathbb{Z}$

$$h = av + bw = \underbrace{es}_{a} v + \underbrace{et}_{b} w = e(sv + tw)$$

$\Rightarrow e \mid h$ Since $h > 0$ this implies

$e \leq h$

$\Rightarrow h = GCD(a, b)$

Proposition

Let $a, b \in \mathbb{Z}$ & $d \in \mathbb{N}$ Then the following are equivalent

1) The equation $ax + by = d$ has solⁿ $(x, y) \in \mathbb{Z}^2$

2) $GCD(a, b) \mid d$.

Examples

1) $2x + 4y = 3$ has No solution $(x, y) \in \mathbb{Z}^2$

$2(x + 2y) = 3$

the LHS is even
the RHS is odd.

Also $GCD(2,4) = 2$ does not divide 3.

2) $5x + 15y = 25$ has a solution

$5 \cdot 5 + 15 \cdot 0 = 25$

$GCD(5, 15) = 5 \mid 25$ Yes!

Proof : "$\Rightarrow$" Let $g = GCD(a,b) \Rightarrow g|a$ & $g|b$

$$g \mid ax+by = d$$

"$\Leftarrow$" By Bezout's ~~theo~~ identity

$\exists\, u,v \in \mathbb{Z}$ s.t. $au + bv = g = GCD(a,b)$

As $g|d$ $\exists\, q \in \mathbb{Z}$ such that $d = gq$

But then

$$d = gq = q\underbrace{(au+bv)}_{=g} = a(qu) + b(qv)$$

So (uq, vq) is a solution of $ax+by=d$.

Thus very easily we can say whether $ax+by=d$ is solvable in $\mathbb{Z}^2$ or not: Just check $GCD(a,b)|d$ or not. [Find $GCD(a,b)$ via Euclid]

Primes & Factorization

You probably recall what a prime is

Def A natural number $p > 1$ is called prime if the following is true

$$d \mid p \implies d \in \{\pm 1, \pm p\}$$

that is the only integers that divide p are $+1, -1, +p, -p$.

The goal of this section is to show that every integer >1 can be factorized into primes and that the factorization is unique up to re-orderings of the primes (permute the primes)

e.g. $30 = 2 \times 3 \times 5 = 5 \times 3 \times 2 = 3 \times 5 \times 2$

$12 = 2 \times 2 \times 3 = 3 \times 2 \times 2 = 2 \times 3 \times 2$

Lemma Let $a, b \in \mathbb{Z}$ and p be a prime

$$p \mid ab \iff p \mid a \text{ or } p \mid b$$

Proof " $\Leftarrow$ " is obvious (convince yourself)

" $\Rightarrow$ " Let $p \nmid a$ so we need to show $p \mid b$

Claim: $GCD(p, a) = 1$

Indeed if $d \mid p$ $d > 0$ then by definition of prime

$d = 1$ or $d = p$, but $p \nmid a$ $\Rightarrow GCD(p, a) = 1$

Thus by Bezout's we have

$x, y \in \mathbb{Z}$ s.t. $ax + py = 1$

Multiply by b $abx + bpy = b$

$p \mid ab$ (by assumption) and $p \mid bpy$

$\Rightarrow p \mid b$ $\square$

The above lemma can be understood as a equivalent definition of a prime.

Lemma Let $n \in \mathbb{N}$ $n > 1$ have the property

$n \mid ab \implies n \mid a$ or $n \mid b$

then n is prime.

Proof Let $n = ab$ $\quad n \mid ab \implies n \mid a$ or $n \mid b$

Assumption

Let $n \mid a$ $\quad a = qn$ for some $q \in \mathbb{Z}$

$$n = ab = \underbrace{q \cdot n}_{= a} \cdot b = (qb)\, n \implies qb = 1$$

But $qb = 1$ has only two possible sol^n in (q, b)

namely $(1,1)$ or $(-1,-1)$

In any case $\quad a = n \quad \& \quad b = 1$

or $\quad a = -n \quad \& \quad b = -1$

In other words if $n = ab$ and $n \mid a$ we can have only

$a = n$, $b = 1$

$a = -n$ $\quad b = -1$

In other words only possible divisor of n lie in

$\{\pm 1, \pm n\} \implies n$ is a prime.

<u>Exercise</u> Let $a_1, a_2 \ldots a_n \in \mathbb{Z}$ and p be prime

If $p \mid a_1 a_2 a_3 \ldots a_n$ then

$p \mid a_1$ or $p \mid a_2$ or $\ldots$ $p \mid a_n$

[left as an exercise]

Fundamental theorem of arithmetics

This is the goal theorem. Namely:

Theorem (FTA)

Every $\mathbb{N} \ni n > 1$ can be written as a product of primes.
Moreover this factorization is unique up to re-orderings of the primes.

Proof Existence of prime factors

By induction.

If $n = 2$ n is prime (base step)

Let the statement hold for $\forall\ n \leq N-1$ (induction step)

If N is prime there is nothing to do.

If N is not prime, then by definition of prime

$$\exists\, a, b \in \mathbb{N} \quad a, b > 1 \quad \text{s.t.} \quad N = ab$$

$$a, b > 1 \implies a, b \leq N-1$$

By inductive hypothesis both a, b are product of primes.

Hence $N = ab$ is the same.

<u>Uniqueness</u> Let $n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_\ell$

p_i, q_j are prime.

As $p_1 \mid q_1 q_2 \cdots q_\ell$ by the previous exercise

$p_1 \mid q_j$ for some $1 \leq j \leq \ell$

By reordering (which is allowed) we may assume

$p_1 \mid q_1$ But q_1 is a prime $p_1 > 1 \Rightarrow p_1 = q_1$

$p_2 \, p_3 \cdots p_k = q_2 \cdot q_3 \cdots q_\ell$ (cancel $p_1 = q_1$)

Repeat the above process!

This proves that the factorization is unique. $\square$

We end the lecture remarking that finding prime divisors of a very large number is extremely hard!

Even by a computer (basics of cybesecurity)