TTM4135 - Lecture Notes
Lecture 2

Page 1

Title slide.

This lecture relates to book chapters 2 and 5

Page 2

Disrete maths AND algebra

No examples here

mention i'll do examples on the blackbord

Page 3

Overview

Page 4

Overview, what now?

Page 5 - Factorisation

$\mathbb{Z}$ is ring (don't need to mention)

Write $a|b$, ex: $5|25$

$\exists k \in \mathbb{Z}$ st. $ak = b$, so for

~~$a=10$~~ $a=11$, $b=44$, ~~$k=4$~~

we have $k=4$ and since $4 \cdot 11 = 44$ we have $a|b$

Trial division

Want to find out if a number a is prime: (not the most efficien)

Lets say ~~a = 123~~ $a = 63$

We have ~~$\sqrt{a} = 11.09 \approx 12$~~ $\sqrt{63} = 7.94 \approx 8$

round up for safety

$63/2 = 31.5$

$63/3 = 21 \Rightarrow 21 \mid 63 \Rightarrow$ not prime

Now $63 = 127$, $\sqrt{63} \approx 12$

~~$127/2 = 63.5$~~

$127/3 = 42.3\ldots$

$127/5 = 25.4$

$127/7 = 18.14$

$127/11 = 11.55$

Why not more than $\sqrt{63}$?

If $p \mid n$ then $n = p \cdot q$

If $q < p$ then we would find some $q \mid n$ before reaching p

eg. p is the smallest number that divides n.

Also see a pattern here, it is only worth testing other primes, if not it would be discovered earlier. that p|n.

So for finding a testing bound β :

Suppose p_i is the i-th prime

The last prime worth testing is

$\beta = p_i$, i s.t $p_{i+1}^2 > n$

Also, if $\sqrt{n} \in \mathbb{Z}$ than n is not prime.

Page 6

(1.) $a \mid b$ and $a \mid c$, we have

$ak = b$ and $az = c$; $k, z \in \mathbb{Z}$

$a \mid b + c$

$b + c = ak + az = a(k + z)$

$a(k+z) / a = k + z \in \mathbb{Z}$

$a \mid b + c$

(2) p prime, $p \mid ab$

$pk = ab$ assume $pz = a$

$pk = (pz)b \neq pzb$

(2) Doesn't hold for non-primes.
f. ex. $p = 8$, $a = 2$, $b = 12$

$8 \mid 24$ but $8 \nmid 2$ and $8 \nmid 12$

(2) Euclids Lemma

If p prime and $p \mid ab$, $ab \in \mathbb{Z}^+$

Then $p \mid a$ or $p \mid b$.

Proof

~~Let t be the smallest integer~~ ~~Positive~~

~~s.t. p ∤ at~~ $\boxed{\text{FTA} \Rightarrow a = q_1^{m_1} \cdot q_2^{m_2} \cdots q_\alpha^{m_\alpha} \quad b = r_1^{n_1} \cdot r_2^{n_2} \cdots r_\beta^{n_\beta}}$

Assume p is the smallest prime where this assertion fails.
And let $a, b \in \mathbb{Z}^+$ s.t. $p \mid ab$ and $p \nmid a$ and $p \nmid b$.

$\Rightarrow p \neq q_i \ \forall i \in [\alpha] \quad p \neq r_j \ \forall j \in [\beta]$

$$ab = q_1^{m_1} q_2^{m_2} \cdots q_\alpha^{m_\alpha} r_1^{n_1} r_2^{n_2} \cdots r_\beta^{n_\beta} \Big\} \text{FTA}$$

Therefore $p \nmid ab$ $\square$

Euclidian Division

$\left(\frac{a}{b} = q + \frac{r}{b}\right)$

For $a, b \in \mathbb{Z}$, $a > b$

q = quotient

r = remainder

$\exists = 1$ $q, r \in \mathbb{Z}$ s.t.

$$a = bq + r \quad , \quad 0 \leq r < b$$

Assume $b > 0$. If $b < 0$ rewrite as $a = (-b)(-q) + r$

~~Be given $b > 0$ and a there are integers q and $r \geq 0$ s.t.~~

~~Basic Representation Theorem:~~

Existence

Fix b, let $P(a)$ ~~be~~ : $\exists q, r \in \mathbb{Z}$ s.t. $a = bq + r$

$P(0)$: $q = r = 0$ ok.

$P(a+1)$: Assume $P(a)$.

Then $\exists$ some q', $r' < b$ with $a = bq' + r'$!

Since $r' < b$, either $r' = b-1$ or $r' < b-1$.

We want to show that in either case there exists q and r $a+1 = bq + r$.

Case $r' = b-1$:

We have:

$a = bq' + b - 1$, therefore

$a+1 = bq' + b = b(q'+1) + 0$

Let $q = q'+1$ and $r = 0$ ok (satisfied)

Case $r' < b-1$:

Let $q = q'$ and $r = r'+1$

Since $0 \leq r' < b-1$ we see $0 \leq r < b$

Since ~~$a = q$~~ $a = bq' + r'$

we see $a+1 = bq + r$

ok

Uniqueness

Assume q_1, r_1 and q_2, r_2

with ~~$a = q \cdot b$~~ $a = bq_1 + r_1 = bq_2 + r_2$

and $0 \leq r_i < b$.

We want to show that

$q_1 = q_2$ and $r_1 = r_2$.

Rearranging:

$$bq_1 + r_1 = bq_2 + r_2$$

$$b(q_1 - q_2) = r_2 - r_1$$

We know $0 \leq r_2 < b$, $0 \leq r_1 < b$

negating the last yields $-b < -r_1 \leq 0$

Then we see $\boxed{-b < r_2 - r_1 < b}$

The only multiple of b between $-b$ and b is 0, so

$r_2 - r_1 = 0 \Rightarrow r_2 = r_1$

Since $b(q_1 - q_2) = r_2 - r_1 = 0$ and $b \neq 0$

we get $q_1 - q_2 = 0 \rightarrow q_1 = q_2$. □

Page 8 (T)

Theorem Bezouts identity

For $a, b \in \mathbb{Z}$ not both 0, the smallest linear combination of a and b equals gcd(a,b)

Proof

Suppose d is the smallest Positive lin. comb. of a and b we claim its the gcd

$d = \alpha a + \beta b$, by div. algo. we have:

$$a = qd + r \;, \quad 0 \leq r < d$$

$$\Rightarrow r = a - qd = a - q(\alpha a + \beta b)$$

$$= a - q\alpha a - q\beta b = (1 - q\alpha)a - (q\beta)b$$

Therefore r is also a lin. comb of a and b but $0 \leq r < d$

So $r = 0$ ~~is smallest~~ since d is smallest.

Page 8 (2)

~~Page 11/12 Extended gcd~~

Therefore $a = qd \Rightarrow d|a$

Similarly for $b \Rightarrow d|b$

Suppose $c|a$ and $c|b$

~~Then $c|(\alpha a + \beta b)$ so $c|d$ so $c \leq d$~~

$a = z_1 c$, $b = z_2 c$

$d = \alpha a + \beta b$

$= \alpha z_1 c + \beta z_2 c$

$= (\alpha z_1 + \beta z_2) c \Rightarrow c|d$

Which implies $c \leq d$.

Page 8 (3)

~~Watch video~~ Assume $d = \gcd(a,b)$

We know $d|a$, $d|b$ ofc. d is a divisor ok

~~Assume And $c|a$, $c|b$~~

Suppose $c|a$, $c|b$

Since $d = \alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$ we have $c|d$. ok.

Since $d|a$ and $d|b$ its obvi. a common divisor.

Since $c|a$ and $c|b$ we know $c|d$

and $c \leq d$, if not c would be gcd.

Page 18 - Residue Classes

Page 9

$r_{-2} = a$, $r_{-1} = b$, $a > b$

Do division algo until

$r_{k-1} = r_k q_{k+1} + r_{k+1}$, $r_{k+1} = 0$

$r_{-2} = r_{-1} q_0 + r_1$

$r_{-1} = r_1 q_2 + r_2$

Example

$r_{-2} = 1071$, $r_{-1} = 462$

$1071 = q_0 \cdot 462 + r_0 = 2 \cdot 462 + 147$

$462 = q_1 \cdot 147 + r_1 = 3 \cdot 147 + 21$

$147 = q_2 \cdot 21 + r_2 = 7 \cdot 21 + 0$

Last remainder is 21, and

$\gcd(1071, 462) = 21$

Factoring a and b we get

$1071 = 3^2 \cdot 7 \cdot 17$

$462 = 2 \cdot 3 \cdot 7 \cdot 11$

The common factors, 3, 7 yields

$3 \cdot 7 = 21 = \gcd(1071, 462)$.

Page 10, just explain algorithm.

Page 11/12

Calculates gcd(a,b) and the coefficients in Bezouts Identity

Example

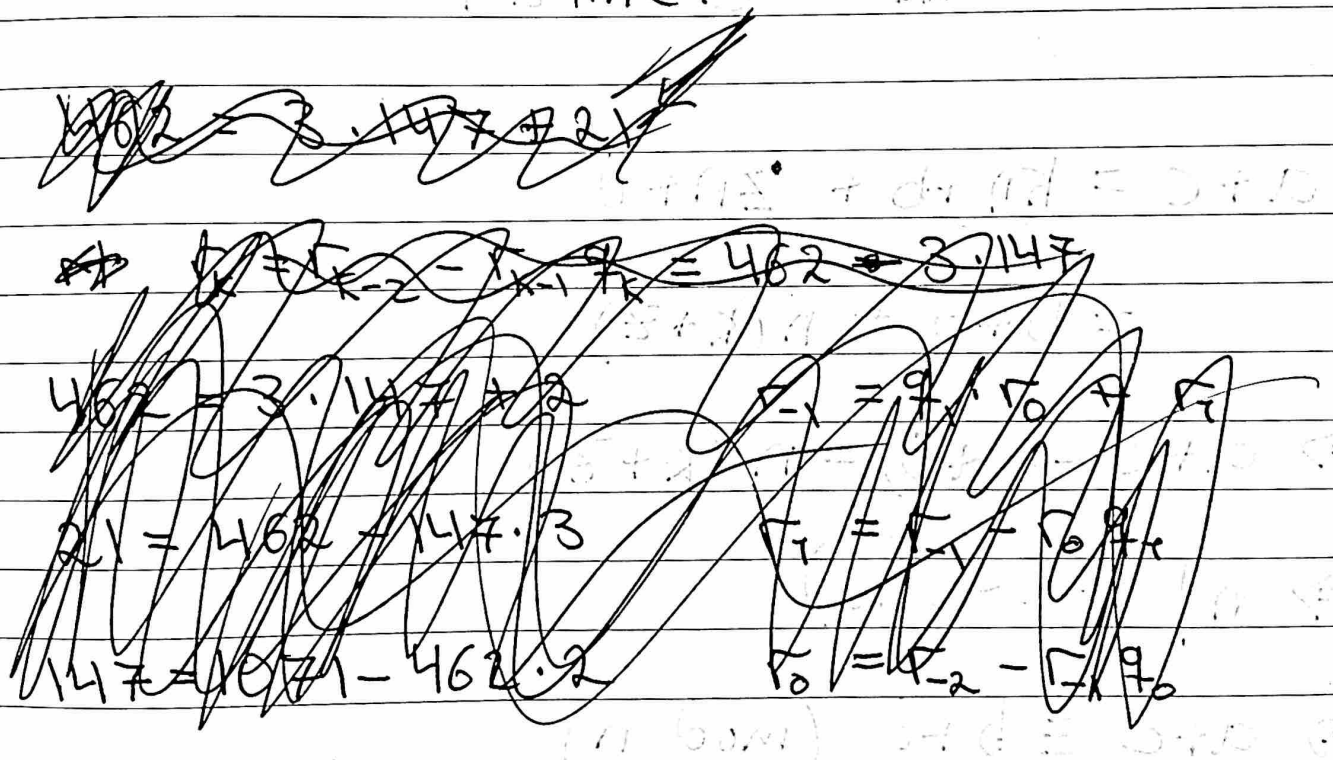
$d = 21$

$a = 1071$

$b = 462$

Continuing our euclids example from earlier

Starting with penultimate line:



$$21 = 462 - 3 \cdot 147$$
$$= 462 - 3(1071 - 2 \cdot 462)$$
$$= 462 - 3 \cdot 1071 + 6 \cdot 462$$
$$= 7 \cdot 462 - 3 \cdot 1071$$

$\Rightarrow \alpha = -3, \beta = 7, (-3)1071 + 7 \cdot 462 = 21$

Page 14

a and b are congruent mod n

If n is a divisor of their difference, e.g.

$$n \mid a-b$$

$$\Rightarrow a-b = kn \iff a \equiv b \pmod{n}$$

(1) $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$

$a - b = kn$ $\quad c - d = zn$

$$a+c = kn + b + zn + d$$

$$= b+d + n(k+z)$$

$$\Rightarrow a+c-(b+d) = n(k+z)$$

$$\Rightarrow n \mid a+c-(b+d)$$

$$\iff a+c \equiv b+d \pmod{n}$$

(2) and (3) similar

Do it yourself. !!

Page 15

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ → least residue system

$0 \bmod 5 = 0$
$1 \bmod 5 = 1$
$2 \bmod 5 = 2$
$3 \bmod 5 = 3$
$4 \bmod 5 = 4$
$5 \bmod 5 = 0$ because $5 = 1 \cdot 5 + 0$
$6 \bmod 5 = 1$

and so on.

larger modulus n gives larger

For example

~~$\{13, 14, 15, 16, 17\}$~~

$\{15, 16, 17, 18, 19\}$ is a complete ~~set of~~ residue system of modulo 5

Page 16

$5 \mod 5 \equiv 0$ ← remainder after dividing a by n. as previously in the lecture.

Warning

You might see people write

~~$\mod 5$~~

$a \mod n \equiv b$

as

$a\ (n) \equiv b$ sometimes.

That confused me once.