Lesson 18

division th

gcd / Euclidean algorithm

diophantine equations

Recall division Th: $\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ \ b>0 \Rightarrow$
$\exists! q \in \mathbb{Z}\ \exists! r \in \mathbb{Z}\ (0 \le r < b \wedge a = bq + r)$

Note : b divides a $\Leftrightarrow r = 0$

Th: 3 div a $\Leftrightarrow$ 3 div a^2

Proof: first we shall prove 3 div a $\Rightarrow$ 3 div a^2 :
assume 3 div a, then $a = 3k$ for some $k \in \mathbb{Z}$,
therefore $a^2 = 9k^2 = 3(3k^2)$ so 3 div k^2
Now let's prove 3 div $a^2 \Rightarrow$ 3 div a :
by contraposition assume 3 does not divide a,
then $a = 3q+1$ or $a = 3q+2$ for some $q \in \mathbb{Z}$
so $a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2+2q) + 1$
or $a^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 =$
$= 3(3q^2 + 4q + 1) + 1$
In any case, 3 does not divide a^2

In hw use this to prove $\sqrt{3}$ is not rational

Questions is $\forall n \in \mathbb{Z}^+\ \forall a \in \mathbb{Z}^+$ n div a $\Leftrightarrow$ n div a^2 true ?
Is $\sqrt{n}$ irrational for every $n \in \mathbb{Z}^+$ that is not a perfect square ?

Note: If $n \in \mathbb{Z}^+$ is a perfect square, i.e $n = a^2$ for some $a \in \mathbb{Z}^+$, then the remainder of n divided by 3 cannot be 2

3333335 is not a perfect square

why? $3333335 = 3 \times 1111111 + 2$

Def: Given $a, b \in \mathbb{Z}$, not both equal to 0, the greatest common divisor of a and b, (a, b) or $(\gcd(a,b))$ is the unique integer d s.t

1) $d > 0$
2) $d \text{ div } a$ and $d \text{ div } b$
3) $\forall c \in \mathbb{Z}^+ \ (c \text{ div } a \wedge c \text{ div } b) \Rightarrow c \leq d$

How do I know there is one and only one integer d with these properties?

Let $A = \{ n \in \mathbb{Z}^+ \mid n \text{ div } a \text{ and } n \text{ div } b \}$

then $1 \in A$ so A is not empty

any element of A is $\leq |a|$ and $|b|$ if $a \neq 0$ $b \neq 0$

so A is finite and therefore it has max

Ex : $(12, 0) = 12$

Ex : $(45, 25) = 5$, why ?

$25 = 5 \cdot 5 = 5^2$

$45 = 3 \cdot 3 \cdot 5 = 3^2 \cdot 5^1$

$(25, 45) = 5$

Take common divisors, with lowest exponent

Factoring is hard.

Euclidean algorithm to compute $(45, 25)$

$45 = 25 \cdot 1 + 20$

$25 = 20 \cdot 1 + 5$

$20 = 5 \cdot 4 + 0$

$5 = 25 \cdot 2 - 45$

$5 = 25 - (45 - 25)$

$5 = 25 - 20 \cdot 1$

We should:

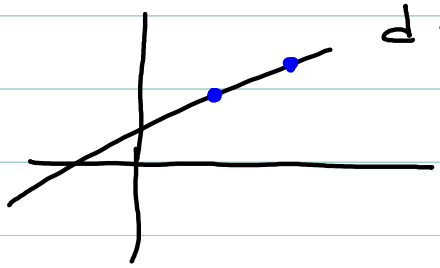
1) Describe a general algorithm
2) Prove it terminates
3) Prove it is correct i.e outputs gcd
4) How long does it take? How many divisions?
   $\leq 5 \cdot$ #digits of smaller of a and b

Th Let $a = bq + r$ then $(a, b) = (b, r)$

Proof: Let $d_1 = (a, b)$ and $d_2 = (b, r)$
since d_2 div b and d_2 div r, then
d_2 div a so $d_2 \leq d_1$
since d_1 div a and d_1 div b and $r = a - bq$
then d_1 div r so $d_1 \leq d_2$. Then $d_1 = d_2$

Th: If $d = (a, b)$ Then there are x_0 y_0 s.t $d = ax_0 + by_0$

i.e the linear diophantine equation $d = ax + by$ has solution $x = x_0$ $y = y_0$



Th the linear diophantine equation $c = ax + by$ has no solutions if $(a\ b)$ does not divide c

Ex $2x + 4y = 3$ has no (integer solutions), and has infinitely many solutions if (a, b) divides c

Ex $2x + 4y = 6$

Solve $2x + 4y = 6$

① write $2 = x_0 \cdot 2 + y_0 \cdot 4$

$4 = 2 \cdot 2 + 0$ $\qquad a = qb + r$

$2 = 4 \cdot 1 - 2 \cdot 1$ $\qquad b = a - (q-1)b$

② Multiply by 3

$3 \cdot 2 : 2(-1) \cdot 3 + 4 \cdot 1 \cdot 3$

one solution is $x_1 = -3 \quad y_2 = 3$

③ If $x = x_1$, $y = x_1$ is a solution to $ax + by = c$ and $d = (a, b)$

$a_1 d x_1 + b_1 d y_1 = c_1 d$

then $x_1 + \frac{b}{d} n \qquad y_1 - \frac{a}{d} n \qquad n \in \mathbb{Z}$

is also a solution

$a\left(x_1 + \frac{b}{d} n\right) + b\left(y_1 - \frac{a}{d} n\right) = ax_1 + by_1$

Def: If $a, b \in \mathbb{Z}$ a, b are called coprime if $(a, b) = 1$

Th If a divides bc and $(a, b) = 1$ then a divides c.

Proof: We can write $1 = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$. So $c = cax_0 + bcy_0$ so $c = cax_0 + aky_0$ for some k so a divides c

Corollary: if p is prime and p div ab then p divides a or p divides b

Corollary: if p is prime and p div $a_1 \cdots a_n$ then p divides a_i for some i.

Corollary: prime factorization is unique:

by contradiction assume there is $n \in \mathbb{Z}^+$ which has 2 distinct prime factorizations that is $n = p_1^{k_1} \cdots p_n^{k_n} = q_1^{h_1} \cdots q_m^{h_m}$, with p_i is and q_j $1 < j < m$ all prime and $i \leq n$ either no p is equal to q_1, which is impossible because q_1 must divide p_i for some i so $q_1 = p_i$ or $p_1 = q_1$ but $h_1 > k_1$ which after dividing both sides by $q_1^{k_1}$ becomes the previous case.