$$\forall\, n \geq 1 \quad 2^n \leq \frac{(2n)!}{n!^2}.$$

$n=1$

$$\cancel{2^1 = 2 \quad \frac{2!}{2\cdot 1!} = 2}$$

$$2^1 = 2 \leq \frac{(2)!}{1!^2} = 2$$

Assume $\displaystyle 2^k \leq \frac{(2k)!}{k!\,k!}$

Trying for the upper bound.

$$\frac{(2k+2)!}{(k+1)!\,(k+1)!}$$

$$\boxed{2^{k+1}} = 2\cdot 2^k$$

$$\leq 2\cdot \frac{(2k)!}{k!\,k!}, \text{ by assumption.}$$

$$= 2\cdot \frac{(k+1)(k+1)\,(2k)!}{(k+1)(k+1)\,k!\,k!}$$

$$= \frac{(2k+2)(k+1)\,(2k)!}{(k+1)!\,(k+1)!}$$

$$< \frac{(2k+2)(2k+1)\,(2k)!}{(k+1)!\,(k+1)!} = \boxed{\frac{(2k+2)!}{(k+1)!^2}}.$$

So we can conclude.

$$2^{k+1} \leq \frac{(2k+2)!}{(k+1)!\,(k+1)!}$$

Def 2.1 Let $a, b \in \mathbb{Z}$.
We say "b divides a" iff $\exists\, c \in \mathbb{Z}$.

$$a = b \cdot c.$$

Notation: $b \mid a$.

or can write $b \nmid a$ to mean $\nexists$ such a complementary factor c.

e.g. $2 \mid 10 \qquad 10 = 2 \cdot 5$

$4 \mid 12 \qquad 12 = 4 \cdot 3$

and $3 \nmid 10 \qquad 10 = 3 \cdot \_\_$ no integer will work here

---

$a \mid b$ is a binary relation on the integers.

Theorem 2.1 Basic properties of divisibility.

1. $\forall\, a \in \mathbb{Z}$ $a \mid a$, i.e. divisibility is reflexive

Proof $a = a \cdot \underline{1}$.

2. Transitivity.

$\forall a, b, c \in \mathbb{Z}$. If ($a|b$ and $b|c$) then $a|c$.

Proof Assume $a|b$ and $b|c$.

$\Rightarrow \exists \underline{\beta, \gamma \in \mathbb{Z}}$ $b = \beta a$, $c = \gamma b$.

$c = \gamma b = \gamma(\beta a)$

$\Rightarrow c = a \underline{\gamma \beta}$, clearly $\beta\gamma \in \mathbb{Z}$.

$\Rightarrow a|c$.

3. Div. of linear combinations.

$\forall a, b, c \in \mathbb{Z}$. If ($a|b$ and $a|c$)

then $\forall m, n \in \mathbb{Z}$ $a | nb + mc$

Proof Assume $a|b$ and $a|c$.

$\Rightarrow \exists \beta, \gamma \in \mathbb{Z}$ $b = \beta a$, $c = \gamma a$

$\Rightarrow nb + mc = a\underline{(n\beta + m\gamma)}$, and $(\quad) \in \mathbb{Z}$.

$\Rightarrow a | nb + mc$

Q4. $\forall a \in \mathbb{Z}$ $1|a$. Proof $a = \underline{a}\, 1$.

Q5 $\forall a \in \mathbb{Z}$ $a|0$. Proof $0 = \underline{0}\, a$

Q6. $\forall\, a \in \mathbb{Z} \quad 0 \mid a \Rightarrow a = 0$

Proof Assume $0 \mid a$, i.e. $a = \_\_\_ . 0 = 0$

7. $\forall\, a, b, c \in \mathbb{Z} \quad c \neq 0$

$$a \mid b \iff ac \mid bc$$

Proof $a \mid b$

$\iff \exists\, \beta \quad b = \beta a.$

$\iff \exists\, \beta \quad bc = \beta ac.$, since $c \neq 0$.

$\iff ac \mid bc.$

2.3 Common divisors.

Def 2.3 c is a common divisor of a and b means $c \mid a$ & $c \mid b$.

Def 2.4 $\gcd(a, b)$ is the greatest common divisor.

eg. $\gcd(2, 4) = 2$

$\gcd(30, 42) = 6$

Def 2.5 The pair (a, b) is called a co-prime pair iff $\gcd(a, b) = 1$.

eg. $10, 21$ are co-prime

There is an efficient algorithm, Euclidean Algorithm, for calculating gcd(a,b)

Built from the process of integer division with remainder.

eg. divide 20 by 6.

"20 divided by 6 goes in 3 times with remainder 2"

Theorem 2.2 formalises this.

For any $a, b \in \mathbb{Z}$, $b \neq 0$ there exists a unique pair $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad , \qquad 0 \leq r < |b|$$

Proof Read in your own time.

Theorem 2.3 If $a, b \in \mathbb{Z}$, not both zero. and if $d = \gcd(a,b)$ then $\exists$ $n, m \in \mathbb{Z}$ such that

$$d = ma + nb.$$

and any common divisor of a,b, divides d.

Proof. Consider set S.

$$S = \{ \alpha a + \beta b : \alpha, \beta \in \mathbb{Z}, \; \alpha a + \beta b > 0 \}$$

S is a non-empty subset of $\mathbb{Z}^+$

So by the <u>well-ordered axiom</u> it has a smallest element, called

$$d = ma + nb > 0 \quad , \quad m, n \in \mathbb{Z}.$$

<u>Claim</u> $d \mid a$ and $d \mid b$.

<u>Proof</u> (by contradiction)

Let's assume $d \nmid a$. and consider dividing a by d with remainder

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

$$\Rightarrow \quad r = a - qd$$
$$= a - q(ma + nb)$$
$$= (1 - qm)a - qnb \; > 0$$

So $r \in S$ and smaller than d, ie $r < d$.

this is a contradiction that came from the assumption $d \nmid a$.

So therefore $d \mid a$. And similarly $d \mid b$.

So d is a common divisor of a, b.

$$d = ma + nb \quad , \quad m, n \in \mathbb{Z}.$$

if $c > 0$ is any common divisor of a, b

then $c \mid d$ by part 3 of Th. 2.1.

Therefore $d \geq c$.

Therefore $d = \gcd(a, b)$.

Euclidean Algorithm.

<u>Lemma</u> 2.4.

If $a = qb + r$ for $a, b, q, r \in \mathbb{Z}$.

then $\gcd(a, b) = \gcd(b, r)$.

<u>Proof</u> Assume $a = qb + r$

if $c \mid a$ and $c \mid b$.

then $c \mid r$, since $r = a - qb$
a linear comb. of a, b.

So c is also a common divisor of b, r.

Converseley. If $c \mid b$ and $c \mid r$

then $c \mid a$, since $a = qb + r$
a lin, comb. of b, r

So c is a common divisor of a, b.

Hence, common divisors of (a,b) are exactly the common divisors of (b,r)

$$\Rightarrow \quad \gcd(a,b) = \gcd(b,r). \quad \blacksquare$$

Can now show Euclidean Algorithm via some examples.

$$\gcd(525, \cancel{}\ 90) = ?$$

$$525 = \underline{\ \ 5\ \ }\ \cancel{}\ 90 + \underline{\ \ 75\ \ }$$

$$\gcd(525, 90) = \gcd(90, 75) = ?$$

, by Lemma

$$90 = \underline{\ \ 1\ \ }\ 75 + \underline{\ \ 15\ \ }$$

$$\gcd(90, 75) = \gcd(75, 15) = ?$$

, by Lemma.

$$75 = \underline{\ \ 5\ \ }\ 15 + \underline{\ \ 0\ \ }$$

$$\gcd(75, 15) = \gcd(15, 0) = 15$$

So $\gcd(525, 90) = 15$

The Extended Euclidean algorithm works backwards through the integer divisions to find Bezout's identity, i.e. the expression for $\gcd(a,b)$ as a lin. comb. of a,b.

e.g. $15 = 90 - 75$

$= 90 - (525 - 5\times 90)$

$= 6\times 90 - 525$

<u>Ex 2.5</u> Finding a Bezout's identity for $6 = \gcd(\underline{12378}, \underline{3054})$

$6 = 24 - 18$

$= 24 - (138 - 5\times 24)$

$= 6\times 24 - 138$

$= 6\times(162 - 138) - 138$

$= 6\times 162 - 7\times 138$

$= 6\times 162 - 7(3054 - 18\times 162)$

$= -7\times 3054 + 132\times 162.$

$$= -7\times 3054 + 132(12378 - 4\times 3054)$$

$$\boxed{= 132\times \underline{12{,}378} - 535\times \underline{3054}}$$

Complete reading chaps 1, 2.

Look at exercises. 2.1, 2.2, 2.3.