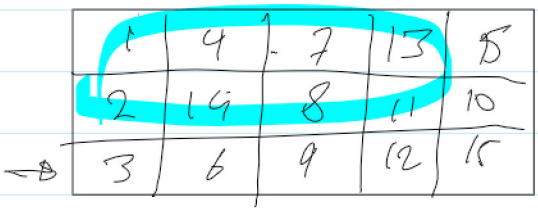
Division

Wednesday, January 19, 2022 12:52 PM

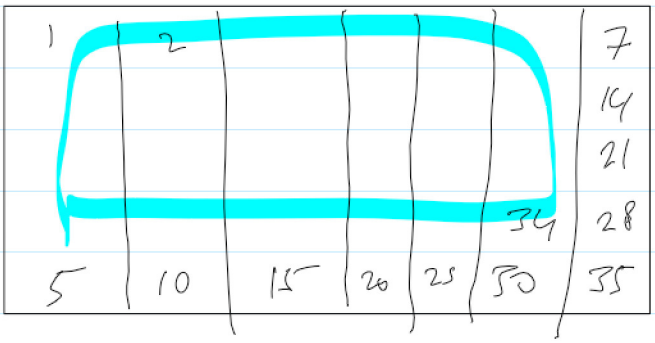
15



$n = 35$

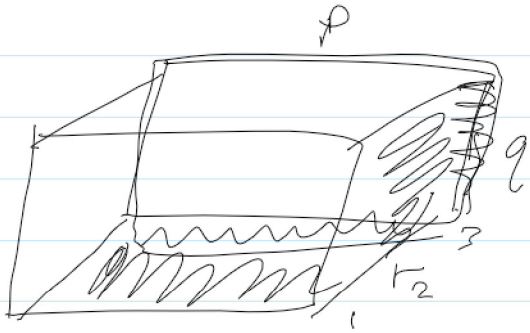
$n = p \cdot q$

$(p-1)(q-1)$



$n = p \cdot q \cdot r$

$(p-1)(q-1)(r-1)$



$n = p^2$ how?

---

1) Division: Given two integers a and b, with $a \neq 0$, we say a divides b if

$\exists c, \quad b = ac$

notation: $a \mid b$ denotes a divides b

e.g. $3 \mid 12$ yes, for $c = 4$

$3 \nmid 7$

2] Thm 1 : let $a, b, c \in \mathbb{Z}$

① if $a \mid b$ and $a \mid c$ then $a \mid (b \pm c)$

② if $a \mid b$ then $a \mid bc$ $\forall c$

③ if $a \mid b$ and $b \mid c$ then $a \mid c$

④ from ①, ②,

if $a \mid b$ and $a \mid c$ then $\forall m, n$

$a \mid (m \cdot b \pm n \cdot c)$

Proof: ① $a \mid b \Rightarrow \exists c_1, \; b = a c_1$

$a \mid c \Rightarrow \exists c_2, \; c = a c_2$

$\therefore b + c = a c_1 + a c_2$

$\Rightarrow b + c = a (c_1 + c_2)$

$\therefore a \mid b + c$ by defn.

3] Note: $0 = 0 \cdot 2$

$2 \mid 0$ for $c = 0 \Rightarrow 0 = 2 \cdot 0$

$0 \mid 0$ for $c = 2 \Rightarrow 0 = 0 \cdot c$ ✗

but $a \neq 0$

e.g. $14 \mid 2$ No

$2 \mid 14$ yes, for $c = 7$, $14 = 2 \cdot 7$

$-2 \mid 14$ yes for $c = -7$

$2 \mid -14$ yes for $c = -7$

$-2 \mid -14$ yes for $c = 7$

4] Primes

Def^n. $p > 1$ is prime if the only positive divisors of p are 1 and p.
$n > 1$ is called composite if it is not prime.

e.g. 5

$5 \mid 5$
$1 \mid 5$

5] The Fundamental Theorem of Arithmetic (FTA)

every $n > 1$ can be written uniquely as a prime or the product of primes.

e.g. $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
$105 = 3 \cdot 5 \cdot 7$
$97 = 97$
$1024 = 2^{10}$

6] Thrm: a composite integer n has a prime divisor $p \mid n$ s.t. $p \leq \sqrt{n}$

e.g. Show that 101 is prime.
it not divisible by 2, 3, 5, 7, $\leq \sqrt{101}$