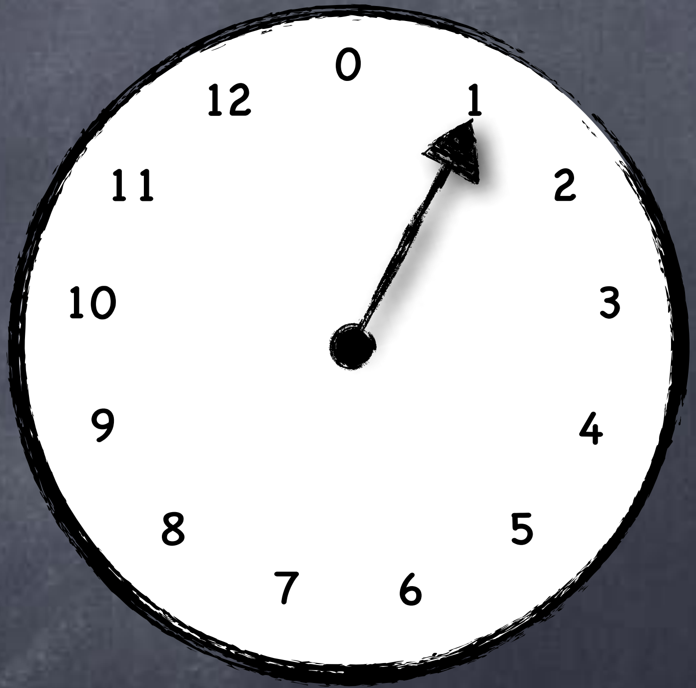
Numb3rs

Prime Factorisation



Primes

- Definition: $p \in \mathbb{Z}$ is said to be a prime number if $p \geq 2$ and the only positive factors of p are 1 and p itself
  - 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, ...

Unique Factorisation

(Fundamental Theorem of Arithmetic):

$\forall a \in \mathbb{Z}$, if $a \geq 2$ then $\exists! \,(p_1,\ldots,p_t, d_1,\ldots,d_t)$ s.t.

$p_1 < \ldots < p_t$ primes, $d_1,\ldots,d_t \in \mathbb{Z}^+$, and $a = p_1^{d_1} p_2^{d_2} \ldots p_t^{d_t}$

- Recall: We already saw that prime factorisation exists (using strong induction)
- Will prove uniqueness now

Primes

- Definition: $p \in \mathbb{Z}$ is said to be a prime number if $p \geq 2$ and the only positive factors of p are 1 and p itself

- **Euclid's Lemma**

  $\forall a,b,p \in \mathbb{Z}$ s.t. p is prime $(p \mid ab) \rightarrow (p|a \vee p|b)$

- Since the only positive factors of p are 1, p, we have two cases: $\gcd(a,p) = 1$ or $\gcd(a,p) = p$.

- If $\gcd(a,p) = p$, then $p|a$ ✓

- If $\gcd(a,p) = 1$, then $\exists u,v$ s.t. $1 = ua+vp \Rightarrow b = uab + vpb$

  $\Rightarrow \exists k$ s.t. $b = ukp+vbp$ (since $p|ab$) $\Rightarrow p|b$

Primes

- Definition: $p \in \mathbb{Z}$ is said to be a prime number if $p \geq 2$ and the only positive factors of p are 1 and p itself

- **Euclid's Lemma**

  $\forall a, b, p \in \mathbb{Z}$ s.t. p is prime $(p \mid ab) \rightarrow (p \mid a \vee p \mid b)$

- Generalisation of Euclid's Lemma (Prove by induction):
  $\forall a_1, \ldots, a_n, p \in \mathbb{Z}$ s.t. p is prime, $(p \mid a_1 \cdots a_n) \rightarrow \exists\, i,\ p \mid a_i$

- Uniqueness of prime factorisation: Suppose z is the smallest positive integer with two distinct prime factorisations as $z = p_1 \cdots p_m = q_1 \cdots q_n$. $\max\{p_1, \ldots, p_m\} \neq \max\{q_1, \ldots, q_n\}$ (Why?). So w.l.o.g., $p_m > q_i$, $i=1$ to n $\Rightarrow$ $p_m \nmid q_i$, $i=1$ to n. But, $p_m \mid q_1 \cdots q_n \Rightarrow p_m \mid q_i$ for some i (by Lemma). Contradiction!

Divisors, Again

- Suppose $a = \Pi_{p \text{ prime}}\ p^{\alpha_p}$ and $b = \Pi_{p \text{ prime}}\ p^{\beta_p}$ (only finitely many primes p have $\alpha_p > 0$ or $\beta_p > 0$)
- $a|b$ iff for every p, $\alpha_p \leq \beta_p$
  - $a|b \Rightarrow b = aq$ where say, $q = \Pi_{p \text{ prime}}\ p^{\gamma_p}$

    $\Rightarrow$ for every p, $\beta_p = \alpha_p + \gamma_p \geq \alpha_p$
  - For every p, $\alpha_p \leq \beta_p$

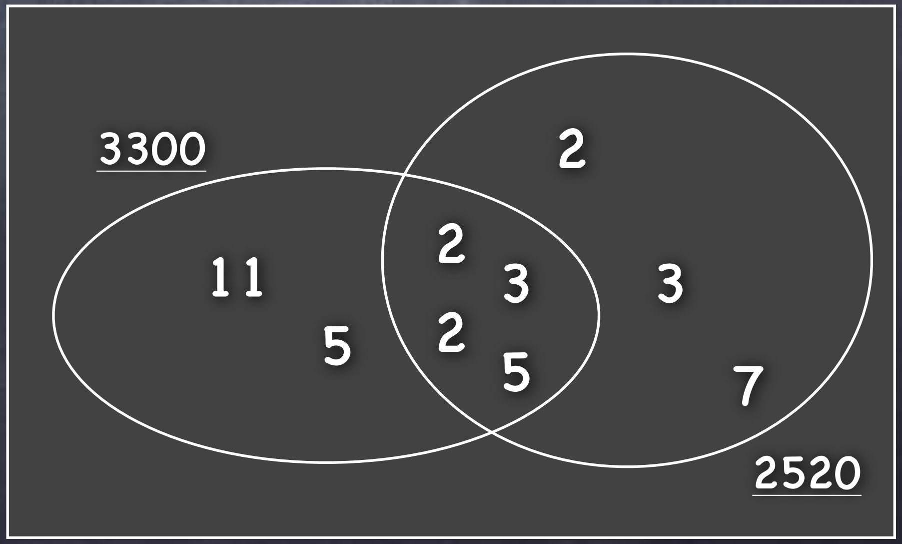
    $\Rightarrow$ for every p, $\gamma_p := \beta_p - \alpha_p \geq 0$

    $\Rightarrow b = aq$ where $q = \Pi_{p \text{ prime}}\ p^{\gamma_p}$

    $\Rightarrow a|b$

GCD, Again

- An alternate algorithm for gcd(a,b): Given the prime factorisation of a,b, construct that of gcd(a,b)
  - For each prime number p let α_p and β_p be its exponents in the factorisations of a and b resp. (Ignore p s.t. $\alpha_p=\beta_p=0$)
  - Then $\gamma_p = \min(\alpha_p, \beta_p)$ is p's exponent in the prime factorisation of gcd(a,b)
- $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$
  $3300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11$
  $\gcd(2520, 3300) = 2^2 \cdot 3 \cdot 5$



- Not very practical compared to Euclid's algorithm, as prime factorisation is not easy

Common Multiples

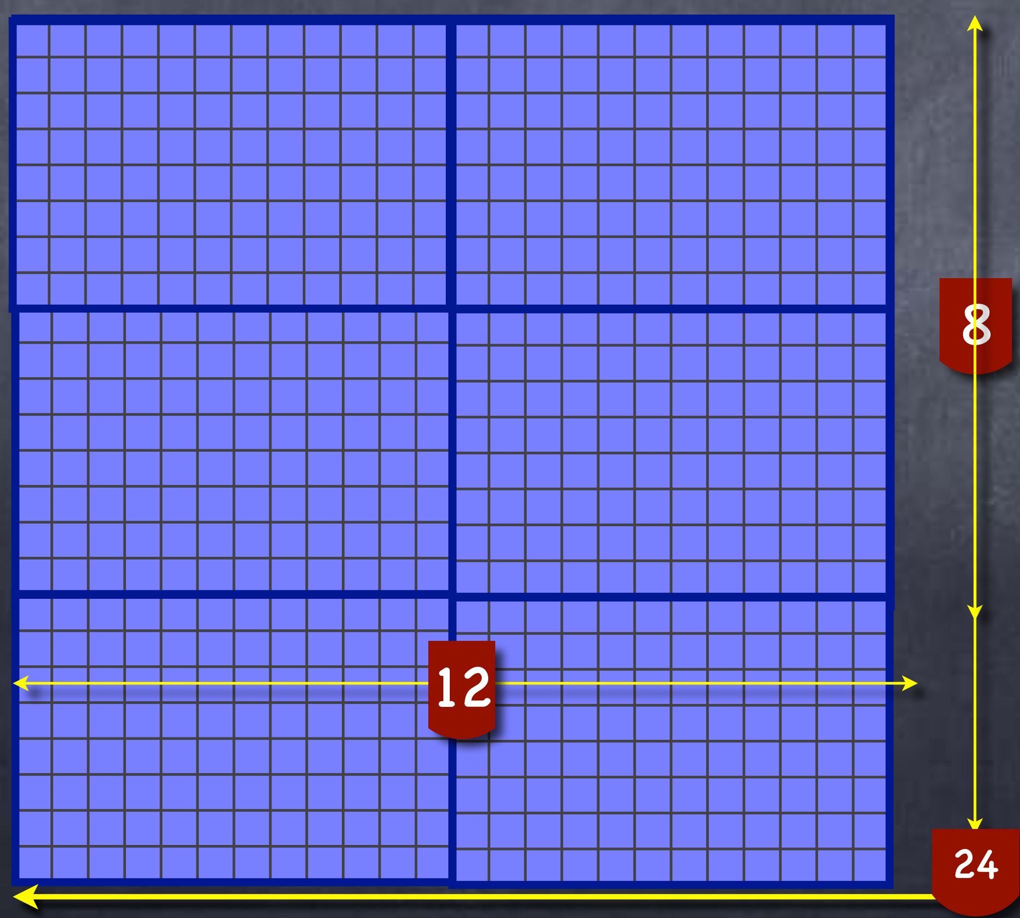
- Common Multiple: c is a common multiple of a and b if $a|c$ and $b|c$.
- Least Common Multiple (for $a \neq 0$ and $b \neq 0$)
  lcm(a,b) = smallest positive integer among the common multiples of a and b
  - Well-defined: $a \cdot b$ is a positive common multiple of (a,b) (unless a=0 or b=0) and we restrict to positive multiples. So an integer in the range $[1, a \cdot b]$.
  - e.g. $36 = 2^2 \cdot 3^2$, $30 = 2 \cdot 3 \cdot 5$. $\mathrm{lcm}(36,30) = 2^2 \cdot 3^2 \cdot 5 = 180$

LCM as Tiling

[Here all numbers are positive integers]

- n is a common multiple of a & b, iff an a x b tile can be used to perfectly tile an n x n square

LCM: smallest such square



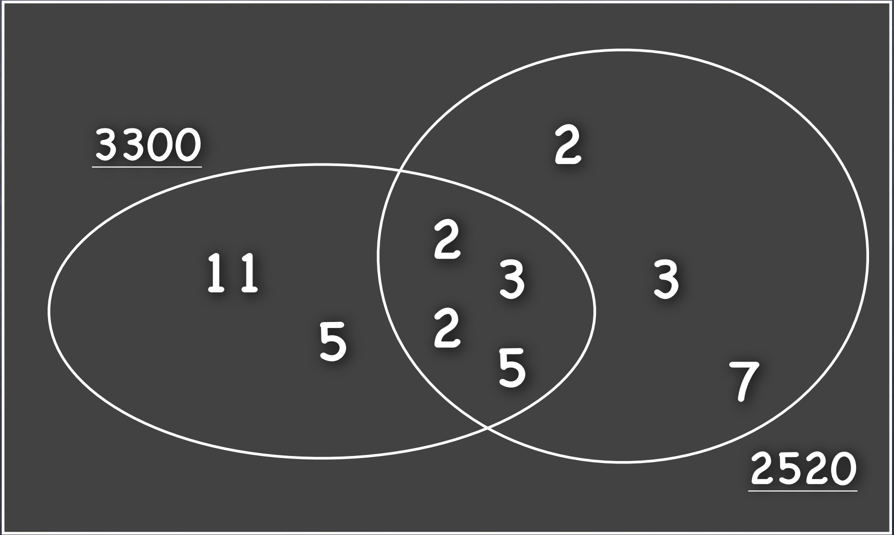
LCM from Factorisation

- For each prime number p let α_p and β_p be its exponents in the factorisations of a and b resp. (Ignore p s.t. $\alpha_p=\beta_p=0$)
- Then $\lambda_p = \max(\alpha_p, \beta_p)$ is p's exponent in the prime factorisation of lcm(a,b)
- $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$

  $3300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11$

  lcm (2520, 3300)

  $= 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11$



- gcd(a,b) · lcm (a,b) = |a·b| [Why?]