Lecture 2: Prime Factorization and More on Factors

Fundamental theorem of arithmetics

Every positive integer n has a unique prime factorization.

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

Proof First we prove the existence. If n is a prime, then $n = n$. If n is a composite number, then $n = n_1 n_2$. We can continue the process on n_1 and n_2 until we get a prime fractorization.

Second, we prove the uniqueness. If there are two factorizations,

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = q_1^{m_1} q_2^{m_2} \cdots q_l^{m_l}$$

Since p_1 is a factor of the right hand side, p_1 must equal to some q_i. Now dividing both sides on p_1 to get a smaller product. So it reduces to prove uniqueness for smaller n. Now we may repeat such argument to prove the uniquenss. QED.

Example

- $420 = 10 \cdot 42 = (2 \cdot 5) \cdot (2 \cdot 3 \cdot 7) = 2^2 \cdot 3 \cdot 5 \cdot 7$
- $729 = 9^3$
- $181 = ?$ not trivial, so it may be a prime. suffices to divide prime numbers up to 13.

Perfect squares

Perfect squares are of the form n^2. Its prime factorization has all even powers.

Example

- $2^{10} \cdot 3^6 \cdot 7^{30} = (2^5)^2 (3^3)^2 (7^{15})^2$

It is useful to memorize them checking a number is prime of not. Below is the list of squares of numbers from 1 to 30, split into three columns:

1 to 10 Squares	11 to 20 Squares	21 to 30 Squares
$1^2 = 1$	$11^2 = 121$	$21^2 = 441$
$2^2 = 4$	$12^2 = 144$	$22^2 = 484$

1 to 10 Squares	11 to 20 Squares	21 to 30 Squares
$3^2 = 9$	$13^2 = 169$	$23^2 = 529$
$4^2 = 16$	$14^2 = 196$	$24^2 = 576$
$5^2 = 25$	$15^2 = 225$	$25^2 = 625$
$6^2 = 36$	$16^2 = 256$	$26^2 = 676$
$7^2 = 49$	$17^2 = 289$	$27^2 = 729$
$8^2 = 64$	$18^2 = 324$	$28^2 = 784$
$9^2 = 81$	$19^2 = 361$	$29^2 = 841$
$10^2 = 100$	$20^2 = 400$	$30^2 = 900$

Factor counting formula

If $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, then the number of factors are

$$(n_1 + 1)(n_2 + 1) \cdots (n_k + 1).$$

Example

- $n = p^a$ has $a + 1$ factors: $1 = p^0, p = p^1, p^2, ..., p^a$
- $n = p_1^a p_2^b$ has $(a+1)(b+1)$ factors.

Product of factors

Factors usually come in pairs, $n = a \cdot (n/a)$. For example,

- $42 = 1 * 42 = 2 * 21 = 3 * 14 = 7 * 6$
- $169 = 1 * 169 = 13^2$.

So the product of all factors of n is $n^{\frac{\#\text{factors}}{2}}$. The number of factors is even if and only if n is a perfect square.

Sum of factors

The factors of $20 = 2^2 \cdot 7$ are

- $1 = 2^0, 2 = 2^1, 4 = 2^2$
- $7 = 2^0 \cdot 7, 14 = 2^1 \cdot 7, 28 = 2^2 \cdot 7$

Their sum equals $(1+2+4)(1+7)=56$. This generalizes to all cases. If $n=p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$, then the sum of factors are

$$(1+p_1+p_1^2+\cdots+p_1^{n_1})\cdots(1+p_k+p_k^2+\cdots+p_k^{n_k})$$

If the sum of factors equals the number itself, we call it a **perfect number**. The first two are 6 and 28.

Homework Use ChatGPT to understand the relation between perfect numbers and Mersenne primes.

Class activity

Any prime number is either 2 or an odd prime number.
Theorem Any odd prime number of the form $4k+1$ is a sum of two squares.

- very difficult, need college math

Theorem Any odd prime number of the form $4k+3$ is not a sum of two squares.

- relatively easy, proved in later lectures

Prime table up to 300:

$$\begin{array}{cccccc}
2 & 3 & 5 & 7 & 11 & 13 \\
17 & 19 & 23 & 29 & 31 & 37 \\
41 & 43 & 47 & 53 & 59 & 61 \\
67 & 71 & 73 & 79 & 83 & 89 \\
97 & 101 & 103 & 107 & 109 & 113 \\
127 & 131 & 137 & 139 & 149 & 151 \\
157 & 163 & 167 & 173 & 179 & 181 \\
191 & 193 & 197 & 199 & 211 & 223 \\
227 & 229 & 233 & 239 & 241 & 251 \\
257 & 263 & 269 & 271 & 277 & 281 \\
283 & 293 & & & &
\end{array}$$