Lecture 22

Instructor's Comments: One thing I noticed that I want to spend a bit of time going over at the beginning was how to write a factorization of a number n

Recall: Fundamental Theorem of Arithmetic. Suppose that $n > 1$ is an integer. Then n can be factored uniquely as a product of prime numbers up to reordering of prime numbers.

Note: For a natural number n we can write down this factorization in a number of ways:

(i) $n = \prod_{i=1}^{k} p_i$ where each p_i is prime. ($n > 1$ required)

(ii) $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where each $\alpha_i \geq 1$ is an integer and each p_i is distinct. ($n > 1$ required)

(iii) $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where each $\alpha_i \geq 0$ is an integer and each p_i is distinct. This is useful if you have two numbers and want to write them using the same primes p_i. They might not have the same prime factors, but allowing for the exponent to be 0 allows you to write them using the same prime factors. For example, $30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0$ and $14 = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^1$.

Instructor's Comments: This is the 5 minute mark.

Theorem: Divisors From Prime Factorization (DFPF). Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where each $\alpha_i \geq 1$ is an integer. Then d is a positive divisor of n if and only if a prime factorization of d can be given by

$$d = \prod_{i=1}^{k} p_i^{\delta_i} \qquad \text{where } \delta_i \in \mathbb{Z}, 0 \leq \delta_i \leq \alpha_i \text{ for } 1 \leq i \leq k$$

Proof: Extra reading. ■

Example: Positive divisors of $63 = 3^2 \cdot 7$ are given by

$$3^0 \cdot 7^0, 3^0 \cdot 7^1, 3^1 \cdot 7^0, 3^1 \cdot 7^1, 3^2 \cdot 7^0, 3^2 \cdot 7^1$$

or

$$1, 7, 3, 21, 9, 63$$

Instructor's Comments: This is the 15 minute mark

Handout or Document Camera or Class Exercise

How many multiples of 12 are positive divisors of 2940? What are they?

Solution: Notice that $2940 = 12(245)$ (say by long division). Then, to find the number of divisors of 2940 that are multiples of 12, you just need to take the divisors of 245 (and then multiply them all by 12). Since $245 = 5 \cdot 7^2$, the total number of divisors is $(1+1)(2+1) = 6$.

Instructor's Comments: Explain to students this is like taking 0 or 1 five and then 0, 1, or 2 sevens.

Hence the multiples are:

$$12, 12 \cdot 5, 12 \cdot 7, 12 \cdot 5 \cdot 7, 12 \cdot 7^2, 12 \cdot 5 \cdot 7^2$$

Instructor's Comments: This is the 25 minute mark

Example: Prove that $a^2 \mid b^2$ if and only if $a \mid b$.

Proof: Assume that $a \mid b$. Then there exists a $k \in \mathbb{Z}$ such that $ak = b$. Now $a^2k^2 = b^2$ and hence $a^2 \mid b^2$ by definition.

Now, assume that $a^2 \mid b^2$. For convenience, assume that $a, b > 0$. Now, write

$$a = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{k} p_i^{\beta_i}.$$

where $0 \leq \alpha_i$ and $0 \leq \beta_i$ are integers and the p_i are distinct primes. Since $a^2 \mid b^2$, we have that

$$\prod_{i=1}^{k} p_i^{2\alpha_i} \;\Bigg|\; \prod_{i=1}^{k} p_i^{2\beta_i}$$

Now, Divisors From Prime Factorization implies that $2\alpha_i \leq 2\beta_i$ and so $\alpha_i \leq \beta_i$ true for $1 \leq i \leq k$. Divisors From Prime Factorization again implies that

$$a = \prod_{i=1}^{k} p_i^{\alpha_i} \;\Bigg|\; \prod_{i=1}^{k} p_i^{\beta_i} = b$$

as required. ■

Instructor's Comments: One more theorem. This is the 35 minute mark

Example:

$$\begin{aligned} \gcd(2^5 \cdot 3^0 \cdot 5^4, 2^4 \cdot 3^1 \cdot 5^4) &= 2^{\min\{4,5\}} \cdot 3^{\min\{0,1\}} \cdot 5^{\min\{4,4\}} \\ &= 2^4 \cdot 5^4 \\ &= 10000 \end{aligned}$$

Instructor's Comments: Mention that factoring is very complicated.

Theorem: (GCD From Prime Factors (GCDPF)) If

$$a = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{k} p_i^{\beta_i}.$$

where $0 \leq \alpha_i$ and $0 \leq \beta_i$ are integers and the p_i are distinct primes, then

$$\gcd(a, b) = \prod_{i=1}^{k} p_i^{m_i}$$

where $m_i = \min\{\alpha_i, \beta_i\}$ for $1 \leq i \leq k$.

Proof: More extra reading. ■

Instructor's Comments: The next topic is completely optional on least common multiples. Do it if you have time

Let $\text{lcm}(a, b)$ represent the least common multiple of a and b.

Example:

(i) Write out a formal definition of $\text{lcm}(a, b)$.

(ii) Show that $\text{lcm}(a, b) = \prod_{i=1}^{k} p_i^{e_i}$ where $e_i = \max\{\alpha_i, \beta_i\}$.

(iii) Prove that $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.

Instructor's Comments: Lastly, I give tips for solving GCD problems. The analogy is going to Toronto: Taking the 401 (might be hard but is ideal). Walking (Slow but will get you there). Flying (Theoretically fastest but takes longer to set up) These are continued on the lecture if you run out of time.

When solving GCD problems, the following gives a rough order of how and when you should try a technique

(i) Bézout's Theorem (EEA) [Good when gcd is in hypothesis]

(ii) GCDWR [Good when terms in gcd depend on each other; good for computations]

(iii) GCDCT [Good when gcd is in conclusion]

(iv) Definition [Good when nothing else seems to work]

(v) GCDPF [Good when you're desperate]