# Session 16 – Prime Factorization

## *Computer Security*

> *As mentioned in Session 14, prime numbers are important in computer security such as with Public Key Cryptography. A concern in computer security is the ability to factor large numbers. One of the reasons that computers can maintain security is that many large numbers are difficult to factor into products of primes. Should someone find a method to easily factor any large number or to test if it is prime, computer security would no longer be secure. At one time, RSA Laboratories offered significant monetary awards for challenge problems involving factoring large numbers.*
>
> *http://en.wikipedia.org/wiki/Integer_factorization*
> *http://www.rsa.com/rsalabs/node.asp?id=2094*

## *Can prime numbers be thought of as the building blocks of natural numbers?*

*We know that* 42 = 2 × 3 × 7. *Is there another way to represent 42 as a product of primes?*

### *Prime Factorization*

The only way to write 42 as the product of primes (except to change the order of the factors) is 2 × 3 × 7. We call 2 × 3 × 7 the prime factorization of 42. It turns out that every counting number (natural number) has a *unique* prime factorization, different from any other counting number. This fact is called the *Fundamental Theorem of Arithmetic*.

In order to maintain this property of unique prime factorizations, it is necessary that the number one, 1, be categorized as neither prime nor composite. Otherwise a prime factorization could have any number of factors of 1, and the factorization would no longer be unique.

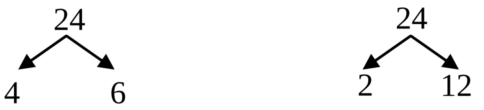
Prime factorizations can help us with divisibility, simplifying fractions, and finding common denominators for fractions.

### *Factor Trees*

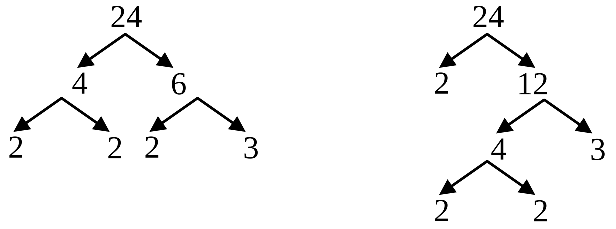
One method for producing the prime factorization of a natural number is to use what is called a factor tree.

The first step in making a factor tree is to find a pair of factors whose product is the number that we are factoring. These two factors are the first branching in the factor tree. There are often several different pairs of factors that we could choose to begin the process. The choice does not matter; we may begin with any two factors. We repeat the process with each factor until each branch of the tree ends in a prime. Then the prime factorization is complete. The Fundamental Theorem of Arithmetic guarantees that all prime factorizations of the same number will result in the same, unique prime factorization for the number.

Example: We show two of the ways of constructing a factor tree for 24.



Continue factoring each tree until complete.

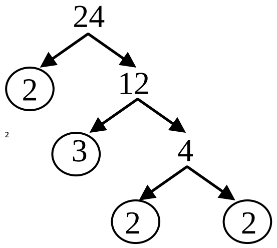


Note that each tree ends with the unique prime factorization of

$$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3.$$

There are two different styles for writing down the factor tree of a natural number. In the first style, as soon as we obtain a prime number in one of the branches, we circle it and then do not work on that branch any more. If a number at the end of a branch is still not prime (a composite), we find two factors for that value. Continue this process until the value at the end of each branch is a circled prime number. The prime factorization is the product of the circled primes.

Example:



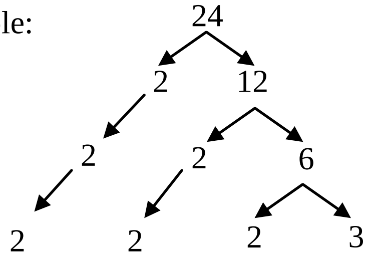
So the prime factorization of 24 is

$$\begin{aligned} 24 &= 2 \times 2 \times 2 \times 3 \\ &= 2^3 \cdot 3 \end{aligned}$$

A good way to check the result is to multiply it out and make sure the product is 24.

For the other style of factor tree, we maintain the product of the original value at each level of the factor tree by extending the branch (“bringing down”) for any prime obtained on the way to getting all of the branches to end in prime numbers. The following example shows this style and also how we may start with a different pair of factors and still come out with the same prime factorization for the natural number.

Example:



Some people prefer this method because each level still multiplies to be the original number, and by bringing down the primes, we are less likely to miss them and leave them out of our prime factorization.

Notice that the prime factorization is still $24 = 2 \times 2 \times 2 \times 3 = 2^3 \cdot 3$ even though we started with $2 \times 12$ instead of $6 \times 4$.

## *Standard Form of a Prime Factorization*

For this class, the standard form of a prime factorization is to write the factors in ascending order (least to greatest) and to use the exponent form when a factor is repeated with a dot to symbolize multiplication.

Examples: $24 = 2^3 \cdot 3$
$600 = 2^3 \cdot 3 \cdot 5^2$

## *Factorial*

***Problem from Session 1.***

> *Cary, Dana, and Pat are elected to be president, secretary, and treasurer of a club. How many different election results are possible?*

We solved this problem by drawing all the possible 1-1 correspondences between the people and the offices. We were able to make six different 1-1 correspondences. Later, in Session 9, we had the Fundamental Counting Principle, which gave us a method for finding the number of possibilities by multiplication: 3 choices for president, then 2 choices for secretary, and finally only 1 choice for treasurer. So, the number of possibilities was $3 \cdot 2 \cdot 1 = 6$.

Problems of this type where we multiply descending natural numbers turn up quite often in mathematics, especially in probability and statistics. This motivates a *factorial*, which is an operation for this type of multiplication.

***Factorial:*** The symbol for factorial is an exclamation mark (!) where $n!$, read $n$ factorial, is defined as the product $n \cdot (n - 1) \cdot (n - 2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1$.

To evaluate *four factorial*, we multiply 4 times each successively smaller natural number, all the way down to 1. So *four factorial* is $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$.

Example: $8! = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 40{,}320$.

Notice that the value becomes large quite quickly.

We can find the prime factorization of a factorial by finding the prime factorization of each of its factors.

Example:
$$\begin{aligned} 8! &= 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= (2 \cdot 2 \cdot 2) \cdot 7 \cdot (2 \cdot 3) \cdot 5 \cdot (2 \cdot 2) \cdot 3 \cdot 2 \\ &= (2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2) \cdot (3 \cdot 3) \cdot 5 \cdot 7 \\ &= 2^7 \cdot 3^2 \cdot 5 \cdot 7 \end{aligned}$$

We may use this prime factorization to determine whether 8! has certain numbers as factors. If we can form a number by multiplying only numbers from the prime factorization, and only in a quantity available in the prime factorization, then the product is a factor of the original number.

Example: $2^7 = 128$ must be a factor of 8! since $2^7$ is part of the prime factorization of 8!.

Example: 10 must be a factor of 8! since both 2 and 5 are prime factors of 8!.

Example: 100 is NOT a factor of 8! since $100 = 2^2 \cdot 5^2$, so we need two factors of 5 to get 100, and 8! only has one factor of 5.

Example: $2^2 \cdot 3^2$ must be a factor of 8! since the prime factorization of 8! contains both two 2's and two 3's.

Here are some other possible questions that may be discussed before going on to the lab:

1. Is 8! divisible

   (a) by 12?

   Since $12 = 2^2 \cdot 3$ and they are prime factors of $8! = 2^7 \cdot 3^2 \cdot 5 \cdot 7$, 8! is divisible by 12.

   (b) by $12^2$?

   Since $12^2 = (2^2 \cdot 3)^2 = 2^4 \cdot 3^2$ and they are prime factors of $8! = 2^7 \cdot 3^2 \cdot 5 \cdot 7$, 8! is divisible by $12^2$.

   (c) by $12^3$?

   Since $12^3 = (2^2 \cdot 3)^3 = 2^6 \cdot 3^3$ and 8! only has $3^2$ as a factor, 8! is *not* divisible by $12^3$.

2. Find the prime factorization of 12! and write it in standard form.

$$\begin{aligned} 12! &= 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= (2 \cdot 2 \cdot 3) \cdot 11 \cdot (2 \cdot 5) \cdot (3 \cdot 3) \cdot (2 \cdot 2 \cdot 2) \cdot 7 \cdot (2 \cdot 3) \cdot 5 \cdot (2 \cdot 2) \cdot 3 \cdot 2 \\ &= 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \end{aligned}$$

   (a) How many zeros will be at the end of the numeral form of 12! ?

   Since $2^2 \cdot 5^2$ is a factor of 12!, 100 is a factor of 12!. So, there are two zeros at the end of the numeral form of 12!.

   (b) What is the largest value that is a power of 2 that is a factor of 12! ?

   The largest value that is a power of 2 that is a factor of 12! is $2^{10} = 1{,}024$.

   (c) What is the largest value that is a power of 6 that is a factor of 12! ?

   Since $2^5 \cdot 3^5 = (2 \cdot 3)^5 = 6^5$, the largest value that is a power of 6 that is a factor of 12! is $6^5$.