

## Some Uses of Prime Numbers

I will continue adding to this list as I have time and I discover more. Reader feedback may illicit some new and exciting uses as well.

- (1) Using prime factoring to find out how many divisors a number has. This is a little gem from the world of number theory. Write your number in its prime factored form, showing all exponents, even "1". So if we had the number 60, we would write it like this:  $60 = 2^2 \times 3^1 \times 5^1$ . Now add 1 onto each exponent and multiply the results. So  $(2 + 1) \times (1 + 1) \times (1 + 1) = 3 \times 2 \times 2 = 12$ . Therefore there are twelve divisors of the number 60. They are: {1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60}. I always use this little trick when I have to work out divisors, just to check that I haven't left out one.
- (2) One of the great uses of Prime Numbers in today's age is in Cryptography, in working out codes and internet security. A wonderful book on this, called *InCode*, is from a young 16 year old Irish girl named Sarah Flannery. I just Googled her name and came up with 10 400 hits. She won the Irish science fair with her work on primes and internet security when she was 16. It is a good read and I recommend it highly. It does a really good job on how prime numbers, very large ones, are at the centre of internet security and high level codes. The general idea is to encrypt your message with a one-way "trap-door", method. Every person publishes a public key that can be thought of as a telephone number. This public key allows you to encrypt your message, but only the person you are sending it to has the proper key to decrypt the message. The solution to all of this comes from prime numbers. If you take two very large prime numbers, each of over 100 digits in length. Multiply these (assuming you have the right math software to do this). The resulting product will have some 200 digits. With the right math software, this is not hard to do. However, the message can only be decoded if someone, given the product, can break down (or factor) the 200 digit number into the two unique primes that were multiplied to produce it. If this interests you at all, I urge you to read Sarah Flannery's book mentioned above.
- (3) Another use of primes is in working out Greatest Common Divisors (GCD) and Lowest Common Multiples (LCM). Here is an example: Let's find the HCD and LCM of 48 and 60.

First, write each in its prime factored (exponential) form:

$$48 = 2^4 \times 3^1 \times 5^0$$

$$60 = 2^2 \times 3^1 \times 5^1$$

GCD pick out least of each  $2^2 \times 3^1 \times 5^0 = 4 \times 3 \times 1 = 12$ ,

LCM pick out largest of each  $2^4 \times 3^1 \times 5^1 = 16 \times 3 \times 5 = 240$

12 is the greatest of all the divisors that are common to each 48 and 60

Divisors of 48 (1, 2, 3, 4, 6, 8, 12, 16, 24, 48)

Divisors of 60 (1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60)

240 is the Lowest multiple that is common to both 48 and 60.

Multiples of 48 (48, 96, 144, 192, 240, 288, ...)

Multiples of 60 (60, 120, 180, 240, 300, 360, ...)

More to be added later...