Primes

Let's step through the "whole" numbers, what math peeps call the integers, from 2 to 9, one at a time.

4 is the first one to have any factor other than itself (and 1), since $2 \cdot 2 = 4$. The next one is 6, since $2 \cdot 3 = 6$. And then 8, since $2 \cdot 2 \cdot 2 = 8$. And finally 9, since $3 \cdot 3 = 9$.

So the first thing is, we can separate the integers into those numbers that have factors (other than themselves and 1), and those that don't. The latter are called primes. We have the first four primes

```
2 3 5 7
```

The other kind, that do have factors, are called composite

```
4 6 8 9
```

There's a method for finding primes, it's called the Sieve of Eratosthenes. Write out the first 25 integers:

```
  1  2  3  4  5  6  7  8  9 10
 11 12 13 14 15 16 17 18 19 20
 21 22 23 24 25
```

1 is special, so we don't think about it for now

```
  .  2  3  4  5  6  7  8  9 10
 11 12 13 14 15 16 17 18 19 20
```

```
21 22 23 24 25
```

Now, strike out every number that is a multiple of 2, which means every even number after 2. (Anything that ends in $2, 4, 6, 8, 0$).

```
 .  2  3  .  5  .  7  .  9 ..
11 .. 13 .. 15 .. 17 .. 19 ..
21 .. 23 .. 25
```

Next, strike out every number that is a multiple of 3. Notice that the first number to get clobbered is $3 \cdot 3 = 9$:

```
 .  2  3  .  5  .  7  .  . ..
11 .. 13 .. .. .. 17 .. 19 ..
.. .. 23 .. 25
```

What remains (except for the last one) are the primes. The prime numbers smaller than 25 are

```
2 3 5 7 11 13 17 19 23
```

If we were to do another round, the next number to be xx'd out would be $5 \cdot 5 = 25$

A couple of points:

◦ to find primes $< N$, we check candidates up to $\sqrt{N}$

◦ this makes it efficient. We checked only 2 and 3 and obtained 9 different primes.

round of 5

If we run the same algorithm up to 49 we get

```
 .  2  3  .  5  .  7  .  9 ..
11 .. 13 .. .. .. 17 .. 19 ..
21 .. 23 .. .. .. .. .. 29 ..
31 .. .. .. .. .. 37 .. .. ..
41 .. 43 .. .. .. 47 .. 49
```

Now, 49 is not prime, it's still there because we haven't checked $7 \cdot 7 = 49$ yet.

We only got 5 new primes. The density of primes is smaller going to larger numbers.

Once again, the first number knocked out by checking multiples of n is n^2. What that means is that, if we are factoring numbers up to say, 120, we only need to check $2, 3, 5, 7$ as possibles. That makes life a lot easier. Similarly up to $17^2 = 289$, we need only add 11 and 13.

All primes going forward end in $1, 3, 7, 9$.

One more thing, every number that is not prime has a *unique* prime factorization. Let's look at all the non-primes from our sieve

```
 4 = 2.2
 6 = 2.3
 8 = 2.2.2
 9 = 3.3
10 = 2.5
12 = 2.2.3
14 = 2.7
15 = 3.5
16 = 2.2.2.2
18 = 2.3.3
20 = 2.2.5
21 = 3.7
```

```
22 = 2.11
24 = 2.2.2.3
25 = 5.5
26 = 2.13
27 = 3.3.3
28 = 2.2.7
30 = 2.3.5
32 = 2.2.2.2.2
33 = 3.11
34 = 2.17
35 = 5.7
36 = 2.2.3.3
38 = 2.19
39 = 3.13
40 = 2.2.2.2.5
42 = 2.3.7
44 = 2.2.11
45 = 3.3.5
46 = 2.23
48 = 2.2.2.2.3.
49 = 7.7
```

It seems to be quite amazing how the gears mesh together so that the patterns from $2 \cdot 13$, $2 \cdot 19$, $3 \cdot 13$, etc. don't clash with the ones from smaller numbers.