Why do we only check until $\sqrt{N}$ when finding factors of N?

January 17, 2004

Originally I came to checking up to $\sqrt{N}$ using calculus, but it appears that there is a much simpler way.

Factors of a number come in pairs, for example if the number to be factorised (N) is 12, then a factor pair (n_1 and n_2), is 3 and 4 ($3 \times 4 = 12$), another is 6 and 2, ($2 \times 6 = 12$). If you have one half of the pair the other half is easily obtained using N/n.

Now, lets look at all the factor pairs of $N = 120$,

n_1	n_2
2	60
3	40
4	30
5	24
6	20
8	15
10	12
12	10
15	8
20	6
30	5
40	3
60	2

Notice that the pairs in the top half of the table are the same as the bottom half just flipped around. This means that once you have the factors in the top half, we no longer need to calculate the rest. The cross-over point (the double lines in the table) is the 'halfway' point at which $n_1 = n_2$ i.e. $\sqrt{N}$.

So once we have the factors up to $\sqrt{N}$, we use N/n to calculate their factors pairs which make up the rest of the factors.