

Prime Numbers II for Helpers

A. Think of a number bigger than 1 and smaller than 23 (23 is a prime number). Call it n . Can you find another number m , also bigger than 1 and smaller than 23, such that $nm - 1$ is divisible by 23? Can you do this for another choice of n ? Replace 23 by 41 and try again. What if you replace 23 by 39 and take $n = 13$?

This may need a bit of explanation, and they will probably have to use trial and error. The point is that 23 and 41 are prime so we can always find an inverse for $n \pmod{23}$ or $\pmod{41}$ (though it won't always be obvious what it is), but $3 \times 13 = 39$ so $13m$ is 0, 13 or 26 $\pmod{39}$.

B. Let's say that p is a Left prime if $p + 1$ is a multiple of 4, and a Right prime if it isn't. Do you think there are likely to be infinitely many Left primes and infinitely many Right primes, or will we run out of one kind if we go high enough?

There are infinitely many of both, because of Dirichlet's theorem on primes in arithmetic progressions: but there is a quick argument for this one. I should be amazed if any of them found it, and all I'm really asking them to do is make an intelligent guess that about half the primes are like that. The quick argument is to modify Euclid's proof: if p_1, \dots, p_n are all the primes which are congruent to $-1 \pmod{4}$ (the Left primes), then either $p_1 p_2 \dots p_n + 2$ (if n is even) or $p_1 p_2 \dots p_n + 4$ (if n is odd) must have a prime factor which is $-1 \pmod{4}$ and is not one of the ones we've seen already. The argument for Right primes is similar but slightly trickier.

C. Choose an odd number between 50 and 100. Can you find three prime numbers which give you the number you have chosen when you add them together? Try it with some more odd numbers, including some bigger ones.

Yes, they can. Here is a useful list of all primes less than 100:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.