The Synapse: Intercollegiate science magazine

Volume 9 | Issue 1 Article 12

2016

# Promiscuous Primes: Is There a Pattern?

Oliver Meldrum

# Promiscuous Primes

*Is There a Pattern?*

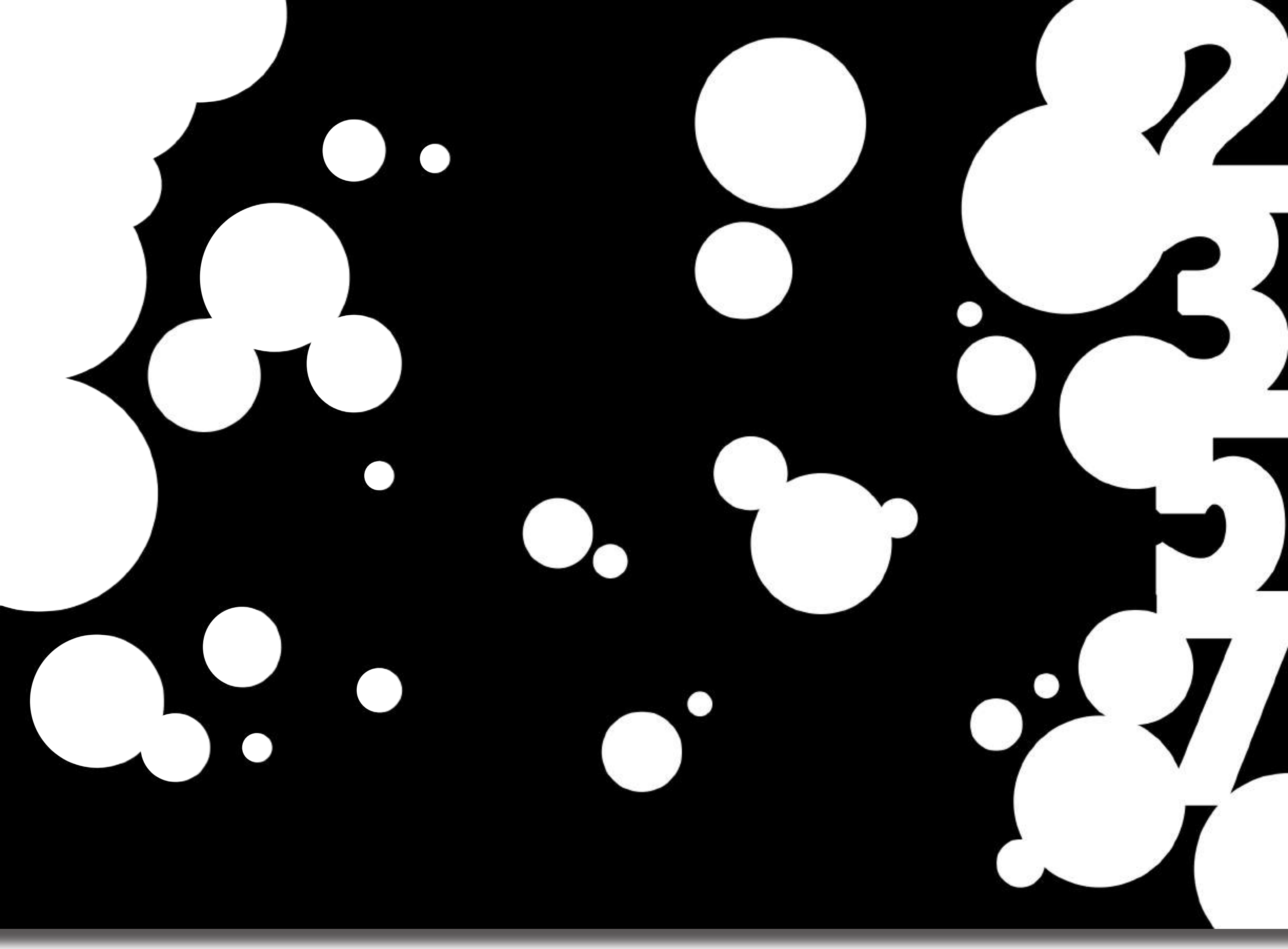
**By Oliver Meldrum**
**Artwork by Jane Sedlak**

2, 3, 5, 7, 11, 13, 17, 19, 23, 29… You may recognize this sequence from a distant math class or perhaps this is what you fall asleep every night thinking about.However, regardless of your familiarity with it, this list of numbers is the beginning to one of the most famous sequences in all of mathematics: the prime numbers. The prime numbers are one of the simplest and yet most fascinating objects in all of mathematics. They are defined quite simply as having only themselves and the number 1 as divisors. For example, 7 is prime because there are no numbers other than 1 and 7 that can be multiplied by another integer to get 7. However, 27 is not prime because 27 = 3 x 9. Although this definition is relatively simple, we very quickly run into problems that are very difficult, or perhaps impossible, to answer.

Let's start with one of the most elegant and well known proofs. Euclid's proof from around 400 B.C. stating that there are an infinite number of primes goes like this: Suppose there is a finite number of primes. We can therefore define a collection of all of the prime numbers and this collection has a finite number of elements. Multiply all of the numbers in this collection together and add 1 to achieve a number; call it *n*. Now, there are to possibilities. Firstly, *n* could be prime. In which case, we're done since *n* is a prime that is bigger and therefore different to every other prime in our initial collection of "all" the primes so by repeating the process above, we know that there are an infinite number of primes since we can always find a new one. If *n* is not prime, it must have a prime factor that wasn't in the original collection. This is because every number in the collection divides *n* by definition and no number can divide 2 numbers only one apart from each other. For example, 14 is divisible by 7 but 15 is not. Similarly, 8 is divisible by 2 but 9 is not. This happens because the gap between successive multiples of a number are the size of the number itself so because we're not allowing 1, the gaps between multiples of any number are bigger than or equal to 2. So, we've found another prime number not in the initial collection, again, showing that there has to be an infinite number of primes.

This is one of the many nice results about prime numbers that are relatively easy to understand and prove. However, we very quickly run into unanswerable questions. For example, it is not known if there are an infinite number of twin primes. Twin primes are two primes that are separated by 2. These include (3,5), (11,13), and many more. Again, this seems like a relatively simple question, but despite much work on this question, we still don't know for sure. Recently, Yitang Zhang showed that there are an infinitely-many number of pairs of primes differing by 70 million or less. While 70 million is a very big number, it's exciting to know that that number exists at all!

One aspect of primes that we know, or at least thought we knew, a fair amount about is their distribution and the probability of finding a prime number in a given interval. As the prime number theorem states and shows in detail, it turns out that as numbers get bigger and bigger, it becomes less and less likely that a number will be prime. This makes sense



because for bigger numbers, there are more numbers less than them that could divide the big number.

We have thought for a long time that primes are essentially randomly distributed beyond the obvious patterns. For example, we know that no even numbers are prime and that numbers that end in a 0 or a 5 are not prime. But, beyond patterns similar to these, we don't have a good way of predicting whether a given number will be prime without doing some serious calculations. This seemingly random distribution can be seen through the fact that there are roughly the same number of primes ending with the digits 1, 3, 7, and 9. These are the only digits that a prime can end in since numbers ending in 0, 2, 4, 6 and 8 are even and those ending in 5 are a multiple of 5 and hence not prime.

There are many applications of prime numbers in areas such as cryptography that, to a certain extent, rely on this pseudo-randomization. Despite the lack of predictability, we do know some things about the distribution of primes. For example, we can very accurately predict the probability that a given number will be prime based on how big it is.

Within the last month, an article was published that suggests there may be more patterns to the primes than we previously thought.

On March 11, Robert J. Lemke Oliver and Kannan Soundarajan, two mathematicians at Stanford University, published a paper that has confused many mathematicians and posed many new questions. It uses a lot of very complicated number theory but it has its basis in, and tries to give an explanation for, a relatively simple observation. It can be seen through an example using the very way we write numbers in base 10. If we look at the first million primes, if a prime ends with a 1, then we would expect the next prime to have about a 25% chance of ending in a 1. This would be expected because primes can only end in 1, 3, 7, or 9 and those are equally distributed amongst all the primes. However, what this paper shows, is that the actual probability of the second prime ending in a 1 is much lower than 25%. This also applies to 3, 7, and 9 in the same way that it applies to 1. This finding is very strange as it seems like gaps of multiples of 10 between primes are much less likely than gaps of other sizes. However, the paper shows that this pattern appears in any other numbering system. In other words, the above example uses base 10 but it also applies if you use base 6 or any other base. This seems to suggest that gaps of all sizes between primes are less likely which doesn't make sense. Clearly, there is something strange going on here that we, including the authors of the paper, don't understand.

The prime numbers are one of the most intriguing ideas in mathematics. You can explain them, and questions about them to elementary school students, yet even modern day mathematicians can't answer some of these questions. In addition, almost all of modern day electronic security which relies on public key encryption is based on essentially a lack of understanding about prime numbers. If someone had an efficient way of factoring large non prime numbers that are as long as you want, you could have access to pretty much anything on the World Wide Web.