The application of prime numbers

Vocabulary:

prime (number)	*to rely on*
to uncover	*factorisation*
ongoing	*encryption*
to aim to discover	*to decipher*
endeavour	*eavesdropping*

Why do we need to know about prime numbers with millions of digits?

Prime numbers are more than just numbers that can only be divided by themselves and one. They are a mathematical mystery, the secrets of which mathematicians have been trying to uncover ever since Euclid proved that they have no end.

An ongoing project – the Great Internet Mersenne Prime Search – which aims to discover more and more primes of a particularly rare kind, has recently resulted in the discovery of the largest prime number known to date. Stretching to 23,249,425 digits, it is so large that it would easily fill 9,000 book pages. By comparison, the number of atoms in the entire observable universe is estimated to have no more than 100 digits.

The number, simply written as $2^{77\,232\,917} - 1$ (two to the power of 77 232 917 minus one) was found by a volunteer who had dedicated 14 years of computing time to the endeavour.

You may be wondering, if the number stretches to more than 23m digits, why we need to know about it? Surely the most important numbers are the ones that we can use to quantify our world? That's not the case. We need to know about the properties of different numbers so that we can not only keep developing the technology we rely on, but also keep it secure.

Secrecy with prime numbers

One of the most widely used applications of prime numbers in computing is the RSA encryption system. In 1978, Ron Rivest, Adi Shamir and Leonard Adleman combined some simple, known facts about numbers to create RSA. The system they developed allows for the secure transmission of information – such as credit card numbers – online.

The first ingredient required for the algorithm are two large prime numbers. The larger the numbers, the safer the encryption. The counting numbers one, two, three, four, and so on – also called the natural numbers – are, obviously, extremely useful here. But the prime numbers are the building blocks of all natural numbers and so even more important.

Take the number 70 for example. Division shows that it is the product of two and 35. Further, 35 is the product of five and seven. So 70 is the product of three smaller numbers: two, five, and

seven. This is the end of the road for 70, since none of these can be further broken down. We have found the primal components that make up 70, giving its prime factorisation.

Multiplying two numbers, even if very large, is perhaps tedious but a straightforward task. Finding prime factorisation, on the other hand, is extremely hard, and that is precisely what the RSA system takes advantage of.

Suppose that Alice and Bob wish to communicate secretly over the internet. They require an encryption system. If they first meet in person, they can devise a method for encryption and decryption that only they will know, but if the initial communication is online, they need to first openly communicate the encryption system itself – a risky business.

However, if Alice chooses two large prime numbers, computes their product, and communicates this openly, finding out what her original prime numbers were will be a very difficult task, as only she knows the factors.

So Alice communicates her product to Bob, keeping her factors secret. Bob uses the product to encrypt his message to Alice, which can only be decrypted using the factors that she knows. If Eve is eavesdropping, she cannot decipher Bob's message unless she acquires Alice's factors, which were never communicated. If Eve tries to break the product down into its prime factors – even using the fastest supercomputer – no known algorithm exists that can accomplish that before the sun will explode.

The primal quest

Large prime numbers are used prominently in other cryptosystems too. The faster computers get, the larger the numbers they can crack. For modern applications, prime numbers measuring hundreds of digits suffice. These numbers are minuscule in comparison to the giant recently discovered. In fact, the new prime is so large that – at present – no conceivable technological advancement in computing speed could lead to a need to use it for cryptographic safety. It is even likely that the risks posed by the looming quantum computers wouldn't need such monster numbers to be made safe.

It is neither safer cryptosystems nor improving computers that drove the latest Mersenne discovery, however. It is mathematicians' need to uncover the jewels inside the chest labelled "prime numbers" that fuels the ongoing quest. This is a primal desire that starts with counting one, two, three, and drives us to the frontiers of research. The fact that online commerce has been revolutionised is almost an accident.

The celebrated British mathematician Godfrey Harold Hardy said: "Pure mathematics is on the whole distinctly more useful than applied. For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics". Whether or not huge prime numbers, such as the 50th known Mersenne prime with its millions of digits, will ever be found useful is, at least to Hardy, an irrelevant question. The merit of knowing these numbers lies in quenching the human race's intellectual thirst that started with Euclid's proof of the infinitude of primes and still goes on today.

Ittay Weissz
Teaching Fellow
Department of Mathematics
University of Portsmouth