Some fascinating prime numbers...!

Sachin Kumar
University of Waterloo, Faculty of Mathematics

There is something about primes numbers... An air of mystery surrounds them, that makes them one of the most alluring (and most studied) objects in all of mathematics, especially number theory and cryptography. Despite hundreds of years of mathematical research on prime numbers, there is still so much we don't know about them. Of course, we know that there are infinitely many prime numbers, with a first proof due to Euclid and many, many other equally fascinating proofs that continue to be found. Nonetheless, many open problems about their distribution among $\mathbb{N}$ remain wide open. The Riemann Hypothesis, for instance, is intimately intertwined with the distribution of prime numbers.

In addition to the mysterious nature of the prime numbers as a whole, vertain individual primes have a special place in my heart, for various reasons. In this essay, I will list few of my favorite primes, together with the fascinating properties that make them special... to me! The reader and other mathematicians would certainly compose different lists of favorite primes.

Without further ado, the list begins with the very first "odd" prime (if you get it! lol)...

1. $p = 2$

The number 2 is the first prime, the smallest prime, and the pain to number theorists' existence. It is such as "odd" prime that there is no other quite like it (unless you look for primes ideals above 2 in other number fields other than $\mathbb{Q}$!). All sorts of curious facts come back to the fact that 2 is the unique even prime. For example:

- If $q = m^n - 1$ is a prime numbers, for some $m \in \mathbb{N}$, then either $q = 2$ or $m = 2$. Primes of the form $q = 2^n - 1$ are called *Mersenne primes* (which will make another guest appearance below).
- See also the special role of 2 in the construction of Fermat numbers and Fermat primes below.
- For $1 < n \in \mathbb{N}$, a polygon with 2^n sides can be constructed with a ruler and compass, but if you replace 2 by any other prime p, there are no longer true (we will come back to this point later on).
- The Law of quadratic reciprocity gives a beautiful relationship between pairs of primes, but the prime 2 is a complete outlier in this regard, and it does not behave at all like the rest of the primes.
- The group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for all prime $p > 2$ and $n > 0$, but is not cyclic for $p = 2$ and $n > 2$.

2. $p = 37$

$p = 37$ might be my all time favorite prime, for silly reasons such as $37 \cdot 3 = 111$, $37 \cdot 6 = 222$, ..., and also for deeper reasons such as the fact that 37 is the first *irregular prime*. The regular primes are those exponents for which Fermat's last theorem has a "simple proof" (first discovered by Lamé, who proposed an erroneous proof of Fermat's last Theorem, which was later fixed by Kummer for regular primes). The irregular primes $37, 59, 67, 101, 103, 131, 149, \ldots$ are those for which Kummer's proof does not work. In

particular, this means that the class group of the ring of integers of the 37^{th} cyclotomic field is of order divisible by 37 ... and in this case it is exactly of order 37.

Another couple of reasons why I am fascinated by the prime 37 come from the theory of elliptic curves (obvious, for people who know me!). A map between two elliptic curves is called an isogeny, and it turns out that cyclic, rational isogenies are somewhat rare. The size of the kernel of the map is callled the degree of the isogeny, and Barry Mazur proved that there are only finitely many primes that are degrees of isogenies of elliptic curves. As it turns out, $p = 37$ is one of the degrees that can occur... but it only occurs for two (isomorphism classes of) elliptic curves (1225.b1 and 1225.b2), and there elliptic curves are rather special. The second reason will be explained below.

3. $p = 163$

The prime number 163 is really nice for several reasons. For instance, $e^{\pi\sqrt{163}}$ is really close to being an integer (it is 262537412640768743.99999999999925 ..., so an integer to 12 decimal places) which has a very interesting explanation coming from elliptic curves with complex multiplication. Not completely unrelated to the previous fat, $\mathbb{Q}(\sqrt{-163})$ is the "last" of the imaginary quadratic fiels of class number 1 (there are only nine such fields, and this is the one with largest discriminant in absolute Value). And also in the same family of amazing facts: the value of the polynomial $x^2 - x + 41$ for $0 \leq x \leq 40$ are prime numbers! Finally, 163 is the largest possible degree of a cyclic, rational isogeny for an elliptic curves defined over $\mathbb{Q}$.

4. $p = 1093$ **and** 3511

Fermat's little theorem says that if p is an odd prime, the p is a divisor of the number $2^{(p-1)} - 1$. A *Wieferich prime* is a prime p such that p^2 is a divisor of $2^{(p-1)} - 1$. We only know two Wieferich primes: 1093 and 3511. The crazy thing is that we conjecture that there are infinitely many Wieferich primes... but we only know two of them! More concretely, we expect $\log(\log(x))$ Wieferich primes below x, and since $\log(\log(x))$ grows slowly, so we are not really surprised that we haven't found any other yet. I became interested in Wieferich primes (in fact, Wieferich places), when they unexpectedly showed up, while I was working on something else!

5. $p = 4001$ **and** 4003

The twin prime conjecture claims that there are infinitely many $n \in \mathbb{N}$, such that n and $n + 2$ are primes (eg: 3 and 5, 11 and 13, ...). Sometimes, it is useful to have a "large pair" of twin primes to compute with, and 4001 and 4003 are easy to remember, and large enough for most purposed, and not too large at the same time (does not create any issue on time complexity of algorithms). That's it. They are stuck in my head, and I use them very often in my computations.

6. $p = 11, 37, 389, 5077, 117223$ **and** 19047851

The set $E(\mathbb{Q})$ of all rational points on an elliptic curve E is defined over $\mathbb{Q}$ and is finitely generated abelian group (thank you Mordell-Weil!), so $E(\mathbb{Q})$ has a finite torsion subgroup $T_{E/\mathbb{Q}} = E(\mathbb{Q})^{\text{tors}}$, and also $R_{E/\mathbb{Q}}$ rational points of infinite order such that $E(\mathbb{Q}) \cong T_{E/\mathbb{Q}} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$. No one know how large the rank $R_{E/\mathbb{Q}}$ of an elliptic curve over $\mathbb{Q}$ can be, or what values $R_{E/\mathbb{Q}}$ can take for that matter. The largest known rank is 28 (an example due to Noam Elkies). So, it is interesting to find the "simplest" elliptic curves with any given rank. We organize elliptic curves by their conductor, so it is interesting to find examples of elliptic

cuvres with rank $R_{E/\mathbb{Q}} = 0, 1, 2, \ldots$ with the smallest possible conductor. Here is the beginning of such a list, with curves given by their LMFDB.org label:

- $R_{E/\mathbb{Q}} = 0$, conductor 11, curve 11.a1
- $R_{E/\mathbb{Q}} = 1$, conductor 37, curve 37.a1
- $R_{E/\mathbb{Q}} = 2$, conductor 389, curve 389.a1
- $R_{E/\mathbb{Q}} = 3$, conductor 5077, curve 5077.a1
- $R_{E/\mathbb{Q}} = 4$, conductor $234446 = 2 \cdot 117223$, curve 234446.a1
- $R_{E/\mathbb{Q}} = 5$, conductor 19047851, curve 19047851.a1

The curves of rank 3 and conductor 5077 have a special place in the history of number theory, and 5077.a1 is called the "Gauss Curve". As far as I know, there is an elliptic curve of rank 6 and conductor $5187563742 = 2 \cdot 3 \cdot 2777 \cdot 311341$, but is not proven to be the smallest such conductor!

7. $p = 65537$

Even though we have a proof that there are infinitely many prime numbers, finding a very large prime numbers is a very difficult task. Thus, it would be of great interest if there was simple formula or a function that produced prime numbers. One famous such "formula" was proposed by Fermat, who famously claimed that the numbers of the form $F_n - 2^{2^n} + 1$, known as Fermat numbers, are always prime. The first few Fermat numbers $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_5 = 65537$ are, indeed, prime numbers. However, Fermat's claim has been proven to be fantastically wrong (the only wrong claim that Fermat made in his life time!), since every single other Fermat number that we have been able to factor has turned out to be composite number. For instance, Euler proved in 1732 that $F_5 = 4294967297 = 641 * 6700417$.

Fermat primes, if you can find them, are really cool, because of the Gauss-Wantzel theorem which says that a regular polygon with n sides can be constructed with a compass and ruler (straight-edge, no markings) if and only if n is a product of a power of 2 and any number of distinct Fermat primes. So, in particular, there is a construction of a polygon with 65537 sides using just the compass and a ruler.

7. $p = 12345678910987654321$

It should be obvious why I love this one! One can ask if there are palindromic numbers with digits in order, that are prime. The sequence that I have in mind is, $1, 121, 12321, 1234321, \ldots$ and one of these numbers are prime, until you reach

$$12345678910987654321$$

which is prime! Coincidently, 1234567891010987654321 is also a prime. If you continue the pattern..., it turns out that the next (probable!) prime is the 17350-digit number,

$$1234567\ldots244524462445\ldots7654321$$

according to OEIS.org.

8. $p = 2^{82589933} - 1$

As we mentioned above in the entry for $p = 2$, if $q = m^n - 1$ is a prime number, for some $m \in \mathbb{N}$, then either $q = 2$ or $m = 2$. Moreover, if $q = 2^n - 1$ is prime, then n is prime (and if s, q is called a *Mersenne prime*). Unfortunately, this is not a necessary and sufficient criterion and some primes values of n do not yield a Mersenne number q (for instance, $2^{11} - 1 = 23 \cdot 89$ is composite). The largest known prines is a Mersenne prime (the 51^{st} Mersenne primes that we have been able to find), name the prime number $M_{51} = 2^{82589933} - 1$. It is worth noting that the mind blowing fact that M_{51} has 24862048 digits.

A really cool fact about Mersenne primes is their relationship to even perfect numbers: if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number (proved by Euclid!) and, viceversa, if n is a even perfect number, then it is of this form (proved by Euler!). So the largest even perfect number we aware of is $2^{82589932} \cdot (2^{82589933} - 1)$ ... a perfect number with 49724095 digits!