# PrimeGrid: Searching for a New World Record Prime Number

**PrimeGrid** [1] is a volunteer computing project which has two main aims; firstly to find large prime numbers, and secondly to educate members of the project and the wider public about the mathematics of primes. This means engaging people from all walks of life in computational mathematics is essential to the success of the project.

In the first regard we have been very successful – as of November 2013, over 70% of the primes on the Top 5000 list [2] of largest known primes were discovered by PrimeGrid. The project also holds various records including the discoveries of the largest known Cullen and Woodall Primes (with a little over 2 million and 1 million decimal digits, respectively), the largest known Twin Primes and Sophie Germain Prime Pairs, and the longest sequence of primes in arithmetic progression (26 of them, with a difference of over 23 million between each). Our educational aim has been partly met by the lively and ongoing discussions between members of the PrimeGrid Community, but until now we have had only limited outreach to the general public. In September 2013 I gave a lecture to an audience of over 100 people at the British Science Festival in Newcastle, to spread the word about PrimeGrid as well as inspire and educate them about our new world record prime search.

We began with the reasons why searching for large prime numbers is worthwhile. As the building blocks of arithmetic, primes are of central importance in mathematics generally and crop up in a wide range of areas. For example: the breeding cycle of the North American Cicada which emerge from dormancy once every 13 or 17 years – since 13 and 17 are prime, this means broods of Cicada on different cycles will only compete for food once every 221 years; The difficulty of finding the factors of large composite (non-prime) numbers underpins the security of the Internet, although even the largest number used by the RSA algorithm has only 617 digits, much smaller than the numbers we are searching for. In the words of Professor Curtis Cooper, discoverer of the current largest known prime number, $2^{57885161}-1$, which has 17.4 million digits, 'I don't know of any practical application of the fact that this number is prime'. Instead, our real motive for searching for extremely large primes is pure mathematical curiosity. While it is easy to define a prime number as an integer with no factors other than itself and one, proving a given integer prime or composite is a difficult task, and while we can say approximately how many primes we should expect in a given range of integers thanks to Gauss' Prime Number Theorem, we know of no method of predicting exactly which integers will turn out to be prime, or of the exact pattern of gaps between them. Such questions have fascinated such great minds as Fermat, Euler, Mersenne, Legendre, Riemann, Lucas and many others, and one of the great attractions of a volunteer computing project like PrimeGrid is that participants are in some way becoming part of this great tradition of mathematics. Of course there is also a competitive aspect of being the discoverer of a new, larger than ever before prime, not to mention the offer of a cash prize from the Electronic Frontier Foundation of $150,000 for the discoverer of the first 100 million digit prime. As we will see, that target is still some way off!

Next we reviewed the history of prime searching, beginning with the study of Mersenne primes ($2^p-1$, where $p$ is a prime). In 1588 Pietro Cataldi proved that $2^{19}-1$ (524287, 6 digits) was prime, although it is worth noting he also incorrectly stated that $p=23,\ 29,\ 31$ and 37 also give Mersenne primes! Until the mid-19th century the only known method of primality proving was to exhaustively trial divide the candidate integer by all primes up to its square root. With some small improvements due to Euler, this method was used by Fortuné Llandry in 1867 to prove the primality of 3203431780337 (13 digits long). Only 9 years later a breakthrough was to come when Édouard Lucas developed a new method based on Group Theory, and proved $2^{127}-1$ (39 digits) to be prime. Modified slightly by Lehmer in the 1930s, Lucas Sequences are still in use today!

The next important breakthrough in primality testing was the development of electronic computers in the latter half of the 20th century. In 1951 the largest known prime (proved with the aid of a mechanical calculator), was $(2^{148}+1)/17$ at 49 digits long, but this was swiftly beaten by several successive discoveries by Jeffrey Miller and David Wheeler with the EDSAC-2 computer at Cambridge, then Raphael Robinson using the SWAC computer at Berkeley. By the end of 1952, the record had been increased to the 687-digit Mersenne Prime $2^{2281}-1$. From then until 1996, the record grew steadily through the use of ever-improving computer technology (see Figure 1). Many records were held by David Slowinski, an engineer at the Cray Research, who ran primality testing programs on customers' supercomputers while they were idle!

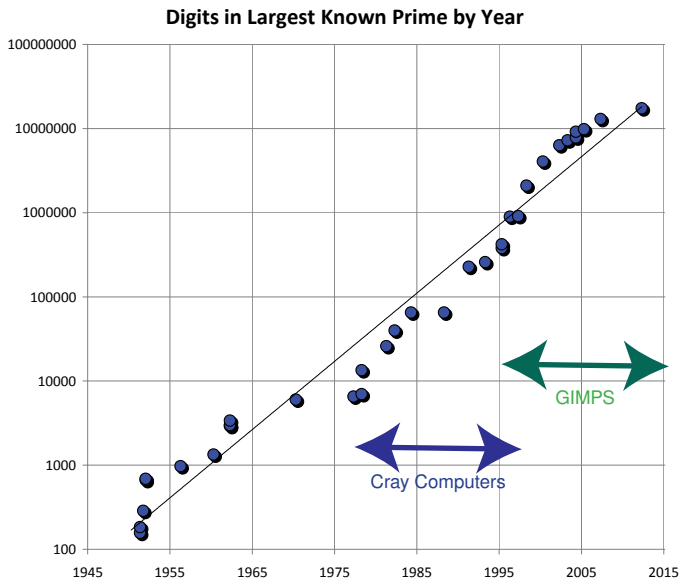


Figure 1: Historical data of the size of the largest known prime during the computer era (1951–present), from [1].

Another paradigm shift occurred in 1996, when the Mersenne Prime $2^{1398269}-1$ was discovered using a computer with a Pentium 90 Mhz processor – 80 times less powerful than the Cray T94 (Figure 2) which held the previous record! This discovery was facilitated by the Great Internet Mersenne Prime Search (GIMPS) [3], a project set up by George Woltman, which used his Prime95 program running on thousands of home computers to search or 'crunch' through new Mersenne candidates much more rapidly than using a single Cray supercomputer. GIMPS is the first known 'Volunteer Computing' project, predating the more widely known SETI@Home and ClimatePrediction.net, both set up in 1999. Since its original find in 1996, GIMPS has increased its own record 11 times, culminating with the current world record prime $2^{57885161}-1$, which has 17425170 digits!

PrimeGrid was first set up in 2005 by Rytis Slatkevičius in an attempt to factorise the 640-digit RSA number, but was beaten to it by a team from the German Federal Office for Information Security. Since then the project has been devoted to prime search projects, has now grown to over 50,000 users, and is run by a team of volunteer administrators, software developers and researchers. In contrast to GIMPS, PrimeGrid is interested in finding primes of many different kinds, including Proth ($k\times 2^n+1,\ k<2^n$), Riesel ($k\times 2^n-1,\ k<2^n$), Cullen and Woodall ($n\times 2^n+/-1$, respectively), and rarer classes such as Twin primes (primes separated by 2), and Sophie Germain primes (when $p$ and $2p+1$ are both prime). In addition, PrimeGrid is working towards computational proofs of the Sierpiński and Riesel (and other related) conjectures.

In 1960 Sierpiński [4] proved that there are infinitely many odd integers $k$ such that $k\times 2^n+1$ is composite for all $n>1$ – quite a surprising result! Two years later, John Selfridge proved that $k=78557$ fulfils this criteria and so it is called a Sierpiński number. The conjecture is that this is the smallest Sierpiński number, and so the proof requires discovery of a Proth prime for each $k<78557$. To date, only 6 $k$ remain without a known prime and PrimeGrid is currently testing 3 of these (the other 3 being tested by the 'Seventeen or Bust' project – started in 2002 when 17 $k$ remained). To date, all values of $n$ up to 21 million have been tested for each remaining $k$ and no primes have yet been found! The Riesel conjecture is the equivalent for $k\times 2^n-1$, and here $k=509203$ is conjectured to be the smallest Riesel number, with 53 values of $k$ remaining for which no prime is known. The computational attack on these conjectures has so far yielded the largest known Proth and Riesel primes, with 3.9 and 1.9 million digits respectively. The astute reader will observe that if the conjectures are false, then this is a fool's errand since one of the remaining $k$ must therefore exhibit no primes!

Recent developments of efficient primality testing programs which can not only use volunteer's CPUs, but also powerful modern graphics processors (GPUs) has allowed PrimeGrid to mount a serious attempt on the world record for largest known prime, which has been held by GIMPS for the last 17 years. This is based on the Generalised Fermat Number (GFN) prime search. GFNs have the form $b^{2^n}+1$ and PrimeGrid is carrying on the work of a previous search effort, looking for primes in the ranges $15<n<22$. So far, we have found 4 primes for $n=19$, each with over 2 million digits, and many more for smaller values of $n$. Details of our search results can be found in [5]. In mid-October 2013, the $n=22$ search reached the point where the numbers being tested are larger than the current record of 17.4 million decimal digits, meaning that any prime found now in this search will be a new world record, and the first non-Mersenne to hold the record since 1989!


Figure 2: A Cray T94 supercomputer, similar to the one used to prove primality of $2^{1257787}-1$ in 1996. Photo from www.craysupercomputers.com/

If you are interested in joining the search for world record primes, or would like to learn more about the project, please visit www.primegrid.com. To participate in the project, all you need is to follow the simple instructions to download a program called the BOINC (Berkeley Open Infrastructure for Network Computing) Manager and select PrimeGrid from the list of available projects. Your computer will then automatically download and process work from PrimeGrid, and with some luck you could become the next world record holder. You will also find a welcome on the very lively discussion forum, and can join a team of other users from the same country to compete in monthly challenges, focusing on one of the sub-projects that PrimeGrid is working on. Whatever your particular mathematical interest or computing hardware, you are sure to find something that will work for you. Happy crunching!

**Iain Bethune**
University of Edinburgh

References

1 www.primegrid.com
2 http://primes.utm.edu/
3 www.mersenne.org/
4 Sierpinski, W. (1960) Sur un problème concernant les nombres $k\cdot 2n+1$, *Elem. Math.* vol. 15, pp. 73–74.
5 Bethune, I. and Goetz, M. (2013) Extending the generalized Fermat prime search beyond one million digits using GPUs, 10th International Conference PPAM 2013, *Lecture Notes in Computer Science* (in press).