

100 grand for running a special screensaver?

O Rojas and G R W Quispel

Department of Mathematics and Statistics
La Trobe University, Victoria, 3086, Australia
Centre for Mathematics and Statistics of Complex Systems

September 17, 2008

Are you one of those persons that spends hours in front of a computer? While doing some other activities on your desk, do you ever get bored by looking at the same screensaver of particles moving from one end to the other or polygonal curves forming different shapes? Would you believe us if we told you that by installing a simple program that uses only a fraction of your computer's memory, almost the same amount as what your screensaver uses, you could win a hundred thousand american dollars? It does sound like a scam, one of those that are widely spread over the internet, we admit it. But sometimes, with the right tools at one's disposal, a bit of luck and a lot of patience, possibilities might turn into realities.

Last year, Edson Smith, who has been the Computing Manager for the UCLA (University of California, Los Angeles) Mathematics Department for the last 10 years, decided to replace the Lab's screen savers with the free software Prime95. This software communicates with the Internet PrimeNet Server and tries to find new prime numbers (numbers that are divisible only by themselves and 1) of a special kind, called *Mersenne primes*, of the form $2^p - 1$, where p is a prime. And voilà, on August 23rd, instead of particles or polygons, a computer emitted a sound notifying the discovery of the prime number $2^{43,112,609} - 1$, a number of almost 13 million digits, which qualifies for the Electronic Frontier Foundation's award of a hundred grand for the discovery of the first 10 million digit prime number. Smith's prime is thought to be the 45th known Mersenne prime. Not bad for some computer's idle time!

As sometimes happens with great discoveries, and with almost all aspect of the evolution of knowledge, as emphasized by Jung's concept of *synchronicity*, the 46th known Mersenne prime $2^{37,156,667} - 1$ of close to 11 million digits, was found two weeks after, on September 6th by Hans-Michael Elvenich in Langenfeld near Cologne, Germany. This number is smaller than Smith's and you might wonder why it didn't come first. As a matter of fact, it is the first Mersenne prime to be discovered out of order since 1988. This happened due to the random scattering in prime numbers, that is, there is not a clear pattern on how they are distributed. We will explain some of the ideas behind the difficulty of finding new Mersenne prime numbers in the next paragraph. You may decide to skip it if you want to follow the story and learn how you could earn not \$100,000 but \$150,000, \$250,000 or even a million dollars.

For example, if you were given the sequence of numbers 56, 58, 60, ... and

were asked to provide the following two numbers in the sequence, you wouldn't hesitate to call them. That is because the given sequence is a subset of the even numbers, numbers that are divisible by 2. However, if you were given the sequence 3, 7, 31, 127, . . . would you easily guess that the number 8191 is the next on the list? Actually, it took almost 17 centuries for this numbers to be guessed as part of the given sequence. The numbers belonging to this sequence can all be written down in the form $2^p - 1$ where p is a prime number, they are the first of the so called Mersenne primes. For example, $3 = 2^2 - 1$ whereas $127 = 2^7 - 1$ and our new number can be represented as $2^{13} - 1$. However, between 7 and 13, there is another prime, 11. This number fails to be a Mersenne prime, as shown in 1536 by Hudalricus Regius, since $2^{11} - 1 = 2047$ can be divided by 23 and 89. Even though Greeks, already in the year 350 B.C. knew about these kind of primes, the real search for Mersenne primes started when in 1644 Marin Mersenne, a French monk, friend of some of the mathematicians of the time, stated that the numbers $2^p - 1$ were prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257. It later turned out that 67 and 257 shouldn't be on the list and it took 300 years to prove that the other numbers were correct. The last Mersenne prime computed by hand was the 9th, a number of 127 digits obtained in 1876 by Lucas, who created a factorization algorithm that to this day is the best available to test if a given number is a Mersenne prime. The discovery of the next Mersenne prime had to wait 76 years until Robinson, with the aid of a computer at UCLA, where the winning number of the \$100,000 was also recently discovered, found 5 Mersenne primes, the smallest of them of 1,279 digits, twice as many as the one found by Lucas. From then on, the number of digits of the Mersenne primes found has kept increasing as new primes were discovered.

The modern search for Mersenne primes is led by GIMPS (Great Internet Mersenne Prime Search), a community established in 1996 with the initial efforts of George Woltman, who wrote the software Prime95, and Scott Kurowski, who implemented PrimeNet, one of the first world-wide distributed computing grids. GIMPS is a project that counts on the volunteered computer time of more than 100,000 users around the world. The idea of the GIMPS project is simple and, upon downloading the software, you might choose to assign you computer one of two tasks: verify if a given prime number is indeed a Mersenne prime or run primality testing work, which means searching for a new Mersenne prime. All candidates for new primes have to be tested independently at least twice. As for the recent Mersenne primes found, they have been verified already by Tom Duell in the USA and by Rob Giltrap from Wellington, New Zealand.

The 44th Mersenne prime was found in 2006 and fell short of the 10 million digits by only 200 thousand digits. Just by a little margin! The next challenge is up now, as George Woltman, founder of GIMPS said in a press communicate, "Our research project will soon offer the chance to achieve the next challenge, the \$150,000 award for an immensely more difficult 100 million digit prime. All you need to participate is our free software download, and a lot of patience." A price of \$250,000 is also offered for the first billion digit prime. And, if you find yourself lucky and have some confidence in mathematics, why not try to obtain the million dollars offered by the Clay Mathematics Institute to the first person that proves the Riemann Hypothesis, which asserts that the frequency of prime numbers is closely related to the behavior of an elaborate function $\zeta(s)$ called the Riemann Zeta function. All you have to do is prove that all interesting solutions of the equation $\zeta(s) = 0$ line on a certain vertical line. This has been

checked for the first billion and a half solutions but a proof that it is true in general has proved elusive for some of the greatest minds in the last 150 years. Good luck!