# The Great Prime Number Record Races

*Günter M. Ziegler*

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 |
| 31 | 37 | 41 | 43 | 47 | 53 | 59 | 61 | 67 | 71 |
| 73 | 79 | 83 | 89 | 97 | 101 | 103 | 107 | 109 | 113 |
| 127 | 131 | 137 | 139 | 149 | 151 | 157 | 163 | 167 | 173 |
| 179 | 181 | 191 | 193 | 197 | 199 | 211 | 223 | 227 | 229 |
| 233 | 239 | 241 | 251 | 257 | 263 | 269 | 271 | 277 | 281 |
| 283 | 293 | 307 | 311 | 313 | 317 | 331 | 337 | 347 | 349 |
| 353 | 359 | 367 | 373 | 379 | 383 | 389 | 397 | 401 | 409 |
| 419 | 421 | 431 | 433 | 439 | 443 | 449 | 457 | 461 | 463 |
| 467 | 479 | 487 | 491 | 499 | 503 | 509 | 521 | 523 | 541 |
| 547 | 557 | 563 | 569 | 571 | 577 | 587 | 593 | 599 | 601 |
| 607 | 613 | 617 | 619 | 631 | 641 | 643 | 647 | 653 | 659 |
| 661 | 673 | 677 | 683 | 691 | 701 | 709 | 719 | 727 | 733 |
| 739 | 743 | 751 | 757 | 761 | 769 | 773 | 787 | 797 | 809 |
| 811 | 821 | 823 | 827 | 829 | 839 | 853 | 857 | 859 | 863 |
| 877 | 881 | 883 | 887 | 907 | 911 | 919 | 929 | 937 | 941 |
| 947 | 953 | 967 | 971 | 977 | 983 | 991 | 997 | 1009 | 1013 |
| 1019 | 1021 | 1031 | 1033 | 1039 | 1049 | 1051 | 1061 | 1063 | 1069 |
| 1087 | 1091 | 1093 | 1097 | 1103 | 1109 | 1117 | 1123 | 1129 | 1151 |
| 1153 | 1163 | 1171 | 1181 | 1187 | 1193 | 1201 | 1213 | 1217 | 1223 |
| 1229 | 1231 | 1237 | 1249 | 1259 | 1277 | 1279 | 1283 | 1289 | 1291 |
| 1297 | 1301 | 1303 | 1307 | 1319 | 1321 | 1327 | 1361 | 1367 | 1373 |
| 1381 | 1399 | 1409 | 1423 | 1427 | 1429 | 1433 | 1439 | 1447 | 1451 |
| 1453 | 1459 | 1471 | 1481 | 1483 | 1487 | 1489 | 1493 | 1499 | 1511 |
| 1523 | 1531 | 1543 | 1549 | 1553 | 1559 | 1567 | 1571 | 1579 | 1583 |
| 1597 | 1601 | 1607 | 1609 | 1613 | 1619 | 1621 | 1627 | 1637 | 1657 |
| 1663 | 1667 | 1669 | 1693 | 1697 | 1699 | 1709 | 1721 | 1723 | 1733 |
| 1741 | 1747 | 1753 | 1759 | 1777 | 1783 | 1787 | 1789 | 1801 | 1811 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

The year 2003 ended with several prime number records. For example, an effort headed by Jens Franke (Bonn University) led to the solution of the RSA-576 decoding problem: the factorization of a 174-digit decimal number.

We also have a new "largest known prime number": a Mersenne prime number with 6320430 digits, $M = 2^{20996011} - 1$. The media attribute the discovery to Michael Shafer, a chemical engineering student at Michigan State University—but that is only part of the story.

## Mersenne Numbers

The GIMPS project ("Great Internet Mersenne Prime Search", `http://www.mersenne.org`) was started in 1996. Its purpose is to search for larger and larger Mersenne prime numbers. The distributed computing project recruited volunteers who, via the Internet, get the GIMPS computer programs as well as "their" numbers for testing, who have their personal computers do slave labor, and who report their results back to the project via the Internet.

Michael Shafer got the number $n = 20996011$ to test whether $2^n - 1$ is prime. His PC "did it" with the GIMPS software, and it turned out that the anwer is "yes!!" for this $n$. *Mathworld* reports that upon this success he performed a victory dance, called his wife and friends and began to celebrate.

Let us recall: In honor of the French monk Marin Mersenne (1588–1648) the numbers of the form $M_n = 2^n - 1$ are called *Mersenne prime numbers*—if they are prime. For this it is necessary (a nice exercise from elementary number theory) that $n$ itself is a prime. But this is not sufficient: $n = 11$ is the first counter-example. In 1644 Mersenne claimed that $M_n$ is a prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and $257$, but for no other prime number smaller than 257 (and thus he got it wrong for exactly five cases). Mersenne prime numbers are rather rare: It is not known whether there are infinitely many. Only the first 38 of them are known, plus only two more, including the newly discovered $M_{20996011}$ which is now also the largest known prime number.

It is quite remarkable that numbers with more than six million digits can effectively be tested for primality. This is the genuine scientific (and programming) achievement on which the new

*Günter M. Ziegler is professor of mathematics at the Technical University, Berlin. His email address is* `ziegler@math.tu-berlin.de`. *This article was translated by the author from his article "Primzahl-Rekordjagd,* Mitteilungen der Deutschen Mathematiker-Vereinigung *2003-4, S. 5-7. He acknowledges support from the DFG Research Center FZT-86 "Mathematics in Key Technologies" in Berlin and from a DFG Leibniz grant.*

record is based—that the number $n = 20996011$ must be prime is only a little warm-up exercise for the new record.

## Primality Tests

It has been shown only recently that there are exact prime number tests that work in polynomial time—see the report in the May 2003 *Notices*, pp. 545-552. This was a theoretical breakthrough, but it is not yet suitable for use "in practice." The GIMPS project applies for each prime $n$ a sequence of more classical tests, which are nicely described at `http://www.mersenne.org/math.htm`:[1]

In *Phase I* one looks for small prime divisors $q$ of $2^n - 1$. These have to satisfy (again a nice exercise) $q \equiv 1 \bmod 2n$ and $q \equiv \pm 1 \bmod 8$. Using a modified "Sieve of Eratosthenes" adapted to such factors, prime divisors of $M_n$ up to approximately 40000 (if any) are found. For this one can exploit the fact that divisibility tests for numbers of the form $2^n - 1$ can be performed very effectively in binary arithmetic.

In *Phase II* one then uses a special case of the so-called "$(p-1)$-method" of Pollard (1974), which can be used to find factors of the form $q = 2kn + 1$, for which $q - 1 = 2kn$ consists of many small prime factors, or (in an improved version) are highly decomposable except that one prime factor may be a bit larger: To find $q$ such that all prime factors are smaller than $B$, one forms the product $E := \prod_{p<B} p$ of all prime numbers that are smaller than $B$, and then computes $x := 3^{E2n}$. The gcd of $x - 1$ and $2^n - 1$ will then catch the divisor of $2^n - 1$ one is looking for.

Only in *Phase III* the GIMPS project uses a method which is *guaranteed* to decide whether $2^n - 1$ is prime, the so-called Lucas–Lehmer test (1878, 1930–1935) for Mersenne numbers: $M_n$ is prime if and only if $\ell_{n-1} \equiv 0 \bmod M_n$, where the $\ell_k$ is defined recursively by $\ell_1 = 4$ and $\ell_n = \ell_{n-1}^2 - 2$. To do this computation effectively, one has to square huge numbers really fast modulo $2^n - 1$. For this the numbers are decomposed into large blocks, and then one works with a special version of a Fast Fourier Transform (FFT), in this case with an FFT with respect to an irrational basis that was introduced by Richard Crandell and Barry Fagin (1994). On the web pages `http://mathworld.wolfram.com` of the *Mathematica* project, which advertise the new record, it is suggested that GIMPS worked with a *Mathematica* implementation, but that seems to slightly stretch the facts. (The connection they can legitimately make is that Crandell has worked on implementing his method for the prime number tests in *Mathematica*.) Indeed, GIMPS works with a highly optimized assembly code. They use floating point arithmetic because this is more effective on Intel Pentium processors, but this also means that the errors of floating point arithmetic have to be detected and eliminated separately.

**Marin Mersenne, 1588–1648.**

## Primality and Factoring

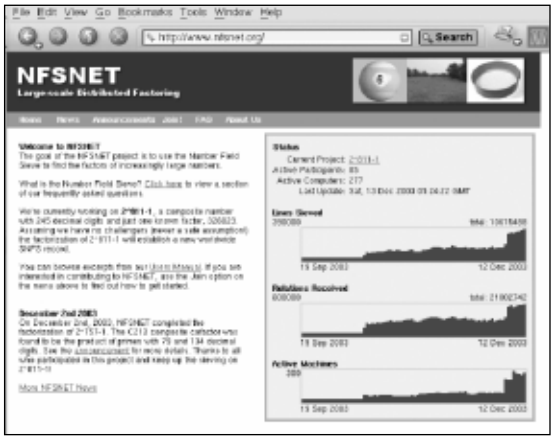
Phases I and II of the GIMPS-sequence really do produce divisors in the case of a decomposable $M_n$, *if* they find any, but the third and decisive phase doesn't. In that case the answer will only be "decomposable!" or not, without an explicit prime divisor as a certificate. Thus a complete primality test is performed, but no factorization is produced.

And there are good reasons for this: Not even in the special case of Mersenne numbers does one know an effective method for factoring. A method that would be able to factor *arbitrary* numbers with a few hundred digits would be interesting and threatening, because the cryptographic methods that guarantee the security of, for example, online banking and the internet are based on the assumption that factoring and similar problems (such as computing "discrete logarithms") are computationally hard.

## RSA

The by-now classical example of an encryption method based on the hardness of factoring is the "public key" encryption scheme by Ron Rivest, Adi Shamir and Leonard Adleman published in 1978.


[1] *For algorithmic prime number theory the experts recommend Richard Crandell and Carl Pomerance: "Prime Numbers. A Computational Perspective", Springer-Verlag, New York 2001. For a computer algebra perspective on primality tests (and lots of other interesting topics) see Joachim von zur Gathen and Jürgen Gerhard: "Modern Computer Algebra", Cambridge University Press, second edition, 2003.*




This RSA method is currently treated in every new elementary number theory text book, and also used extensively in practice—see the manual pages for `ssh` on your PC, or the homepage `http://www.rsasecurity.com` of Rivest, Shamir and Adleman's company. The security of their method against unauthorized decoding depends on the fact that with current technology it is very difficult to decompose products with 150 or 200 decimal digits into their prime factors. The company "RSA Securities" has even offered prizes for factoring their challenge problems.[2] The first of them is/was a prize of $10,000 for factoring the number "RSA-576"

188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059

with 174 decimal digits, that is, 576 binary digits (bits). This problem has been cracked by Jens Franke of Bonn University, as reported by *Heise Online* news service on December 8, 2003: The number has factors

398075086424064937397125500550386491199064362342526708406385189575946388957261768583317

and

472772146107435302536223071973048224632914695302097116459852171130520711256363590397527

(87 digits each) and these are prime—which again with the current methods is very easy to verify. For his factorization Franke has used the "General Number Field Sieve (GNFS)." This method was introduced by Lenstra, Lenstra, Manasse and Pollard (1990). It has a running time of $\exp(O(\sqrt[3]{n \log n}))$ for $n$-digit numbers; this is not quite polynomial, but is *nearly* so. The GNFS had already been used to factor the smaller test problems, ranging from RSA-100 to RSA-512, the latter in August 1999.

[2] `http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html`.

## More Records

And there are even more current records with respect to factorization: Indeed, people are not only trying to test Mersenne numbers for primality, but also to decompose them completely into prime factors. NFSNET (`http://www.nfsnet.org`) is another distributed computing project, which recently (success announced on December 2, 2003) managed in Internet joint work to factorize the Mersenne number $2^{757} - 1$ completely. The prime factors 9815263 and 561595591 of this number were known before, but the 212 digits of the other two factors made for a hard piece of work: It was now decomposed into the prime factors

57221370220020678242482279750958577491513128278093884069623462531821289169645 93

and

24033821640983508088736273403005965446689002356344332130565066643193813901119771090424269412054543072714914742665677774247325292327559.

This achievement is based on the "Special Number Field Sieve (SNFS)"—a faster specialized version of the GNFS, which is applicable only for special numbers, such as those of the form $b^n \pm 1$.

## Record Chase

The chase for new records will continue. In 2000, the "Electronic Frontier Foundation" (`http://www.eff.org/`) paid their first prize, $50,000, for the first prime number with more than one million digits. For the identification of a prime number with more than ten million decimal digits they have offered a prize of $100,000. This adds to the excitement, and the GIMPS project is looking for fellow combatants who would enlist their computers for the record chase.

At the same time, the larger RSA challenge problems wait to be attacked. RSA-640, a number with 193 decimal digits, is the next one on the list: $20,000 has been offered for it.

And the next Mersenne number on the hit list of NFSNET is $2^{811} - 1$. This project is looking for collaborators as well.

So, many poor little PCs will be fed numbers and tortured with prime number tests and decomposition methods, in the hope that their owners might be able to cash in on a part of the fame and glory (and the prize money) for the next record, which surely is soon to be achieved.