# Large Prime Quadruplets

Tony Forbes

## Introduction

Except for the case $(2, 3, 5, 7)$ at the beginning of the number sequence it is impossible to have four consecutive primes $p_1, p_2, p_3, p_4$ with $p_4 - p_1 < 8$. An interval of seven or less cannot contain more than three odd numbers unless one of them is a multiple of three. On the other hand, groups of four primes $\{p, p+2, p+6, p+8\}$, usually called *prime quadruplets*, are fairly common. The first is $\{5, 7, 11, 13\}$, followed by $\{11, 13, 17, 19\}$, $\{101, 103, 107, 109\}$, $\{191, 193, 197, 199\}$, $\{821, 823, 827, 829\}$ and so on. Just as with *prime twins*, pairs of primes $\{p, p+2\}$, it is conjectured that the sequence of prime quadruplets goes on for ever. Indeed, the apparently simpler *prime twin conjecture* is currently an unsolved problem of mathematics although in 1973, Jing-Run Chen proved a weaker form (See Halberstam & Richert [3]): There are infinitely many primes $p$ such that $p + 2$ is either prime or the product of two primes. A similar result holds for quadruplets [3, Theorem 10.6]: There exist infinitely many primes $p$ such that $(p+2)(p+6)(p+8)$ has at most 14 prime factors. The prime quadruplet conjecture would then follow if we could reduce '14' to '3' but this seems be a problem of extreme difficulty.

One of the things mathematicians do when they don't fully understand something is to try and find bigger and better examples of the objects that are puzzling them. Such is true with prime quadruplets. Wells [8] lists a 45-digit quadruplet, the largest known at the time, discovered in 1982 by M. A. Penk (see Trigg [7]). More recently, as a result of a systematic search, Warut Roonguthai [5, 6] has found the smallest prime quadruplets of the form $\{10^n + x, 10^n + x + 2, 10^n + x + 6, 10^n + x + 8\}$ for $n = 99, 199, 299, 399, 499, 599$, and for $n = 699$ for which the quadruplet is

$$10^{699} + 547634621251, \quad 10^{699} + 547634621253,$$

$$10^{699} + 547634621257, \quad 10^{699} + 547634621259.$$

Then in September 1998, the 1000-digit barrier was broken when the author announced the discovery of the prime quadruplet

$$76912895956636885\ (2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} - 7,$$

$$76912895956636885\ (2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} - 5,$$

$$76912895956636885\ (2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} - 1,$$

$$76912895956636885\ (2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} + 1$$

at the end of a search which lasted about eight days and used 1400 MHz of Pentium computer power.

One obvious way to find a large prime quadruplet is to generate a long list of large primes and note whenever four numbers occur within a range of eight. However, after a moment's thought it is clear that this is not a very efficient way to proceed. Thousand-digit primes are not that easy to produce in large quantities and we would waste a lot of time looking in the wrong places.

A much better strategy is to split the process into three stages: (i) Some kind of *sieve* to quickly eliminate from further consideration quadruplets where one of four numbers has a small prime factor; (ii) a fast and efficient *probable-primality test* for checking the survivors from stage (i); and (iii) *primality proofs* for the probable-primes found in (ii).

## The sieve

Let

$$U = m\ (2^{3s} - 2^s) - 6 \cdot 2^s, \tag{1}$$

where $s$ is a fixed exponent which we shall specify, and the problem is to find $m$ such that all four numbers $U - 7$, $U - 5$, $U - 1$ and $U + 1$ are prime. The particular form of (1) is chosen mainly for the purpose of implementing the primality proofs. Meanwhile, we need only point out that $2^{3s} - 2^s$ is a product of the three consecutive numbers, $2^s - 1$, $2^s$, $2^s + 1$, and hence $U$ and $U - 6$ are divisible by $2^s$ and $2^s + 1$, respectively. For our primality proofs of $U - 7$ and $U - 5$ we need to choose $s$ such that $2^s + 1$ can be completely factorized.

Write $m = (k + k_0)Q + h$, where $Q = 223092870 = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot 23$ is the product of the primes up to 23, $k_0$ is a starting-point for the $k$s, and $h$ is any fixed number for which $\gcd((U - 7)(U - 5)(U - 1)(U + 1), Q) = 1$. Thus

$$U = ((k + k_0)Q + h)(2^{3s} - 2^s) - 6 \cdot 2^s$$

and the purpose of the sieve is to eliminate $k$s for which $(U - 7)(U - 5)(U - 1)(U + 1)$ is divisible by a small prime.

We make a list of $k$s, $k = 0, 1, 2, \ldots$ up to a given limit, say $0 \le k < 32,000,000$. For each prime $p$ from 29 up to $2^{31} - 1$ and for each factor $U + b$, $b = -7, -5, -1, 1$, we compute the smallest $k$, $k_p$, say, for which $U + b$ is divisible by $p$. We remove $k_p$ from the list of $k$s. Furthermore, and with hardly any extra effort, we can eliminate $k_p + p$, $k_p + 2p$, $k_p + 3p, \ldots$ from the list because $U + b$ will be also divisible by $p$ for these values of $k$.

We don't have to worry about primes $p$ less than 29, nor primes that divide $2^{2s} - 1$ because they have already been taken care of by the form of $U$. The sieve limit of $2^{31} - 1$ is a natural boundary, determined by the computer architecture, and allows the computation of $k_p$ to be done with 32-bit integer arithmetic.

## The Probable-Primality Test

Fermat proved: *If $n$ is prime then*

$$2^n \equiv 2 \pmod{n}. \tag{2}$$

Hence if $2^n \not\equiv 2 \pmod{n}$, then we can conclude that $n$ is composite. Conversely, if we compute $2^n \bmod n$ and the answer is 2, although we cannot prove anything, it turns out nevertheless that $n$ is quite likely to be prime. This is the basis for the second stage. Composite numbers that satisfy (2) are known as *pseudoprimes to the base* 2. Although comparatively rare, they do exist—341, for example—and therefore as a primality test (2) can sometimes give an erroneous result.

Every quadruple that survives the sieve is put to the test and we discard those which fail. We don't throw away any primes and we are reasonably confident that any quadruple all of whose members satisfy (2) will pass the final stage and indeed turn out to be a true prime quadruplet.

An aside: We usually regard (2) as a *compositeness* test. In theory, if (2) is false then definitely $n$ is composite whereas if (2) holds, $n$ is probably, but not necessarily, prime. However, I maintain that in practice—and somewhat perversely—it is exactly the opposite way round, at least for (2) taken in isolation with a large $n$ chosen more-or-less at random. Suppose $n$ has over a thousand digits and we compute $2^n \pmod{n}$. If the answer is different from 2, then either $n$ is composite, or $n$ is prime and the computer has made a mistake. We can't tell with any confidence unless we double-check the answer by another calculation of $2^n \pmod{n}$, preferably on a different type of computer. On the other hand, if the answer is 2 then we can be almost certain that the computer is functioning correctly, otherwise the final residue, 2, would be an incredible coincidence after such a long calculation. Moreover, we can be just as sure that $n$ is prime because the chance of accidentally stumbling across a large composite number that satisfies (2) is far too small to seriously worry about.

One further practical point: The form (1) is dominated by a small multiple of a large power of two. We exploit this feature in the reduction of $2^n \pmod{n}$. Write $n = m\ 2^{3s} - d$. We can reduce a number $x$ modulo $n$ very quickly by splitting it into

$$x = x_0 + x_1\, 2^{3s} = x_0 + (y_0 + my_1)2^{3s},$$

where $0 \le y_0 < m$ and $0 \le x_0 < 2^{3s}$. Then $x \equiv x_0 + y_0 2^{3s} + dy_1 \pmod{n}$, and $dy_1$ is considerably smaller than $n^2$ (but often it is larger than $n$, so a second iteration may be needed). One can determine $y_0$ and $y_1$ by long-dividing $x_1$ by $m$. Even though $m$ is comparatively small, dividing by it is still quite a complicated operation and one which we can avoid if we wish by using an alternative probable-primality test,

$$m^{n-1} \equiv 1 \pmod{n}.$$

Instead of reducing $x$ modulo $n$, we first multiply by $m$ and work instead with $mx = m(x_0 + x_1 2^{3s}) \equiv mx_0 + dx_1 \pmod{n}$.

## Primality Proofs

Although Fermat's theorem—or rather its converse—provides a very convenient probable-primality test, the mathematical community demands rigorous proof before a number can be accepted as prime. If $N$ is a large number that satisfies (2), it is usually very difficult to prove that $N$ is prime, unless it has some special structure that we can take advantage of. Suppose $N-1$ is partially factorizable, say $N-1 = FR$, where $F$ is even, $R$ is odd, $\gcd(F,R) = 1$ and $F$ is completely factorized into primes. Suppose also that for each prime factor $p$ of $F$ there is a number $a$ such that $a^{N-1} \equiv 1 \pmod{N}$ and $\gcd(a^{(N-1)/p} - 1, N) = 1$. Then by a theorem of Pocklington [4], any prime factor $q$ of $N$ must satisfy $q \equiv 1 \pmod{F}$. If it is also true that $F > N^{1/3}$ then either $N$ is prime, or $N$ is the product of two primes $\equiv 1 \pmod{F}$. To eliminate this last possibility, we prove the following.

LEMMA. *Let $N-1 = FR$, where $F > N^{1/3}$, and write $R = rF + t$ with $0 \le t < F$. If $N$ is a product of two primes $\equiv 1 \pmod{F}$ then there exists a positive integer $c$ such that $c^2 - tc + r = 0$.*

PROOF. We may write $N = (cF+1)(dF+1)$. Then, on the one hand, we have

$$cdF^2 + (c+d)F + 1 = FR + 1 = rF^2 + tF + 1,$$

that is, $(cd-r)F = t - (c+d)$. On the other hand, since $N < F^3$, we also have

$$(cF+1) + (dF+1) = cF + 1 + \frac{N}{cF+1} < F + \frac{N}{F} < F + F^2,$$

which implies $c + d < F$. Together, we deduce that $cd = r$, and hence $t = c + d = c + r/c$, so that the required result follows.

We can use the lemma, with Pocklington's theorem, to show that a given $N$ is prime by verifying that, with the corresponding values of $r$ and $t$, the quadratic equation

$$c^2 - tc + r = 0 \tag{3}$$

has no solutions in $c$.

That takes care of the case where $N-1$ can be sufficiently factorized. For the second member of our quadruplet,

$$N = 76912895956636885\,(2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} - 5, \tag{4}$$

this is indeed the case. We have

$$N - 1 = 106367679637 \cdot (2^{1093} + 1) \cdot (\text{composite}) \tag{5}$$

and the complete factorization of $2^{1093} + 1$ is known—which is the main reason for our choice of that particular exponent;

$$2^{1093} + 1 = 3 \cdot 306041 \cdot 149076457 \cdot P,$$

where $P$ is a prime of 315 digits. There are alternative exponents. As well as $2^s + 1$ completely factorized into primes, we also require $s \equiv \pm 1 \pmod 6$, for otherwise one of the four numbers will be divisible by 5 or 7. Apart from 1093—the smallest possible for generating numbers of at least 1000 digits—the only other values of $s < 1200$ known to the author at time of writing are 1111, 1117, 1121, 1141, 1145, 1171, 1189. These are the results of an active area of research known as the *Cunningham Project*, the objective of which is to determine the prime factors of $b^n \pm 1$ for $2 \leq b \leq 12$ and large $n$. Its origins and early history are described in Brillhart, Lehmer, Selfridge, Wagstaff & Tuckerman [2].

We can set

$$F = 106367679637 \cdot (2^{1093} + 1),$$

which is greater than $N^{1/3}$. The proof of the primality of (4) then follows once we verify that the conditions of Pocklington's theorem hold and that (3) has no integer solutions.

Similarly, the primality of the fourth member of the quadruplet,

$$76912895956636885\ (2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} + 1,$$

follows from the factorization

$$\begin{aligned} &76912895956636885\ (2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} \\ &\quad = 3033244481 \cdot 2^{1093} \cdot (\text{composite}). \end{aligned} \tag{6}$$

To deal with the first and third members, we are unable to factorize $N - 1$ sufficiently. However, we already have suitable factorizations of $N + 1$, in the form of (5) and (6). Furthermore there is a result of Morrison, corresponding to Pocklington's theorem, that enables us to construct primality proofs from a sufficient partial factorization of $N + 1$. The theory involves Lucas sequences and is a little more complicated. We will not go into details here but instead refer the interested reader to Theorem 19 in the paper of Brillhart, Lehmer & Selfridge [1]. It is straightforward to show that the conditions of the theorem are satisfied, from which it follows that

$$76912895956636885\ (2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} - 7$$

and

$$76912895956636885\ (2^{3279} - 2^{1093}) - 6 \cdot 2^{1093} - 1$$

are prime.

# Postsctript

The author has discovered further examples of prime quadruplets, the largest to date being

$$24947432928741915235\ (2^{3363} - 2^{1121}) - 6 \cdot 2^{1121} + b : b = -7, -5, -1, 1,$$

numbers of 1032 digits. The primality proofs use the fact that $2^{1121} + 1$ has been completely factorized.

# References


[1] J. Brillhart, D. H. Lehmer & J. L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, *Math. Comp.* **29** (1975), 620–647.

[2] J. Brillhart, D.H. Lehmer, J. Selfridge, S.S. Wagstaff Jr., & B. Tuckerman, Factorizations of $b^n \pm 1$, $b = 2$, 3, 5, 6, 7, 10, 11, 12 up to high powers, *Contemporary Mathematics* **vol. 22**, Second Edition, American Math. Society, 1988.

[3] H. Halberstam & H. -E Richert, *Sieve Methods*, Academic Press, London, 1974.

[4] H. C. Pocklington, The determination of the prime or composite nature of large numbers by Fermat's theorem, *Proc. Cambridge Philos. Soc.,* **v. 18** (1914-16), 29–30.

[5] Warut Roonguthai, Prime quadruplets, *M500,* **148** (February, 1996), 9.

[6] Warut Roonguthai, Large prime quadruplets, *M500,* **153** (December, 1996), 4–5.

[7] C. W. Trigg, A large prime quadruplet, *J. Rec. Math,* **14** (1981/1982), 167.

[8] David Wells, The Penguin Dictionary of Curious and Interesting Numbers, Penguin Books, Harmsworth, England, 1986.


---


*Mathematical Gazette* **84** no. 501 (November 2000), 447–452