Mathematicians versus the Silicon Age: Who Wins?

Sheldon Axler

Mathematicians invented computers. Computers then changed the way mathematics progresses. Have computers made mathematicians, and the techniques they developed over the past few thousand years, obsolete? Are mathematicians merely trying to preserve their jobs by sticking with outmoded requirements, such as insisting on rigorous proofs even in the face of overwhelming numeric evidence? This possibility was envisioned by Alan Turing, a mathematician who helped create the dawn of the computer age (and who helped the Allies win World War II by playing a key role in cracking the German Enigma code), when in 1947 he wrote:

> The masters are liable to get replaced because as soon as any technique becomes at all stereotyped it becomes possible to devise a system of instruction tables which will enable the electronic computer to do it for itself. It may happen however that the masters will refuse to do this. They may be unwilling to let their jobs be stolen from them in this way. In that case they would surround the whole of their work with mystery and make excuses, couched in well chosen gibberish, whenever any dangerous suggestions were made. I think that a reaction of this kind is a very real danger.

Computer Triumphs

An early and dramatic example of the intrusion of computers into serious mathematics came with the resolution of the four-color conjecture. The four-color conjecture arose in 1852 as the question of whether every conceivable map of the world can be colored using only four colors so that no two adjacent countries have the same color. By 1922 this had been proved to be true for all maps that have at most 25 countries. The four-color conjecture stumped mathematicians until 1976, when Kenneth Appel and Wolfgang Haken of the University of Illinois announced that the four-color conjecture had become the four-color theorem. Press attention focused on Appel and Haken's massive use of computers to show that four colors always suffice.

Computer power has grown tremendously since 1976 when an expensive mainframe computer helped crack the four-color conjecture. Today for about a thousand dollars you can buy a fast personal computer. For a few hundred dollars more, you can add to it mathematical processing software that will put in your hands easily usable computational tools that allow you to answer questions that stumped mathematical giants of past centuries.

The two best known mathematical processing software programs are *Mathematica* and *Maple*. Both of these programs can effortlessly do almost everything you learned in high school mathematics, and they "know" number theory, calculus, differential equations, linear algebra, and much, much more. They come with many hundreds of built-in functions, extensive features for manipulating these functions, and a high-level computer language that allows you easily to create functions and procedures of your own. The two programs are roughly equivalent, and mathematicians are probably about evenly divided as to which they prefer. My personal preference is for *Mathematica*, so in the following when I write something like "my computer says" I am referring to an ordinary personal computer running *Mathematica*.

Let's look at some of the capabilities of *Mathematica* and *Maple*. At the lowest level, these programs can do arithmetic. But they surpass calculators in that they can perform exact arithmetic regardless of the number of digits involved. For example, choosing some random fractions and asking my computer to add them, I instantly see that

$$\frac{1874891749763074}{887248574093039728975} + \frac{2835278724546576432749}{5436366346875298592845297}$$

equals

$$\frac{2525789603922728419716366780370280559365253}{4823408289512496083848284985057003306983380575},$$

where the answer has automatically been displayed in reduced form with no common factors in the numerator and denominator. Instead of having the answer displayed as a fraction, I could have requested it to be displayed as a decimal.

As another example, my computer tells me instantly that 3^{101} equals

$$1546132562196033993109383389296863818106322566003.$$

As a final example of arithmetic, when I ask my computer to compute 1000!, it instantly gives all 2568 digits correctly. This last example particularly amuses me because when I was an undergraduate, before software such as *Mathematica* and *Maple* existed, I spent several weeks writing a computer program to compute 1000! exactly.

If we turn our attention to algebra, we will not be surprised to find that *Mathematica* can solve large systems of linear equations and that it knows the quadratic formula. Hardly any mathematicians know the cubic formula, but *Mathematica* does, telling me that one of the solutions of the equation

$$x^3 + 5x - 7 = 0$$

is

$$-5\left(\frac{2}{3\left(63+\sqrt{5469}\right)}\right)^{\frac{1}{3}}+\frac{\left(\frac{63+\sqrt{5469}}{2}\right)^{\frac{1}{3}}}{3^{\frac{2}{3}}}.$$

Mathematica also knows the quartic formula for finding the roots of fourth-degree polynomials. Alas, for fifth-degree and higher polynomials, *Mathematica* can usually provide only decimal approximations to the roots (accurate to thousands of decimal places, if so requested by the user), not exact roots. However, no person or computer could do better, because mathematicians have proved that no formula exists for finding roots of polynomials of degree higher than four.

Could you factor the polynomial

$$x^8 + 30x^7 + 233x^6 + 192x^5 + 141x^4 + 99x^3 + 163x^2 + 61x + 72$$

in less than a day? My computer instantly factors the polynomial above as

$$(x^3 + 17x^2 + 5x + 8)(x^5 + 13x^4 + 7x^3 + 2x + 9).$$

You should have learned in high school that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for every positive integer n. *Mathematica* knows that, and it also tells me that

$$1^8 + 2^8 + 3^8 + \cdots + n^8$$

equals

$$\frac{n(n+1)(2n+1)(5n^6 + 15n^5 + 5n^4 - 15n^3 - n^2 + 9n - 3)}{90}.$$

Instead of asking for the sum of eighth powers, I could have asked for the sum of eightieth or eight-hundredth powers and received equally quick answers from my computer.

Mersenne Primes

An integer greater than 1 is called *prime* if it has no divisors other than 1 and itself. For example, 13 is prime but 21, which is divisible by 3 and 7, is not. The first ten primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. The number 1 is excluded, by definition, from the list of primes because otherwise positive integers would not have unique factorizations into products of primes (here we regard two factorizations as the same if they differ only in the order of the factors).

Computers allow us to calculate with prime numbers in ways that would take mathematicians lifetimes without machines. My computer quickly tells

me that the one-millionth prime is 15485863 and the one-billionth prime is 22801763489. When I asked my computer for the one-trillionth prime, I had to wait almost seven minutes before getting the answer: the one-trillionth prime is 29996224275833. The ancient Greeks had proved that there are an infinite number of primes, so there is no largest prime number.

A *Mersenne prime* is a prime number of the form

$$2^n - 1,$$

where n is a positive integer. Mersenne primes are named in honor of the French monk Marin Mersenne, who in 1644 claimed that the only values of n for which $2^n - 1$ is prime are

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

For the first four values specified by Mersenne, we have

$$2^2 - 1 = 3$$
$$2^3 - 1 = 7$$
$$2^5 - 1 = 31$$
$$2^7 - 1 = 127,$$

all of which are obviously prime.

The next three values specified by Mersenne are not so obvious:

$$2^{13} - 1 = 8191$$
$$2^{17} - 1 = 131071$$
$$2^{19} - 1 = 524287.$$

However, the first of these had been shown to be prime in 1456, and the next two had been shown to be prime in 1588.

The next value specified by Mersenne,

$$2^{31} - 1 = 2147483647,$$

was shown to be prime by Euler in 1772.

The next value specified by Mersenne,

$$2^{67} - 1 = 147573952589676412927,$$

resisted all attacks until 1903, when the American mathematician Frank Cole discovered that
$$2^{67} - 1 = 193707721 \times 761838257287.$$

Thus $2^{67} - 1$ is the product of two large prime numbers, but it is not itself prime. Mersenne was wrong!

Mathematica gives the factorization above of $2^{67} - 1$ in under a second. The point here is that a problem that had stymied mathematicians for over two

centuries can now be answered quickly on an ordinary home computer. My computer also instantly disposes of the last two values specified by Mersenne, telling me that $2^{127} - 1$ is prime (as had Mersenne claimed) but that $2^{257} - 1$ is not.

At the time of this writing (Spring 2002), 39 Mersenne primes are known. The largest is

$$2^{13466917} - 1,$$

which was proved to be prime in 2001. In addition to being the largest known Mersenne prime, this number is also currently the largest known prime number of any type. It was discovered by the Great Internet Mersenne Prime Search, a remarkable network of tens of thousands of ordinary computers working in their idle time to find additional Mersenne primes. You can join the Great Internet Mersenne Prime Search, and perhaps have your computer be the discoverer of the next Mersenne prime, by downloading the free software from http://www.mersenne.org/prime.htm.

How many Mersenne primes await discovery? Most mathematicians strongly suspect that there are infinitely many Mersenne primes, but no one has been able to prove that. The brief survey of Mersenne primes given above looks like a victory for computers in the battle between mathematicians and machines.

Perfect Numbers

A positive integer greater than 1 is called *perfect* if the sum of its divisors, including 1 but not including itself, equals the number. For example, 6 is a perfect number because its divisors are 1, 2, 3 and $6 = 1 + 2 + 3$. The next perfect number is 28, with $28 = 1 + 2 + 4 + 7 + 14$. The next two perfect numbers are 496 and 8128. After that there is a big jump, as the next perfect number is 33550336.

Let's factor the first five perfect numbers to see if we can discover a pattern:

$$
\begin{array}{rcccc}
6 & = & 2 \times 3 & = & 2 \times (2^2 - 1) \\
28 & = & 2^2 \times 7 & = & 2^2 \times (2^3 - 1) \\
496 & = & 2^4 \times 31 & = & 2^4 \times (2^5 - 1) \\
8128 & = & 2^6 \times 127 & = & 2^6 \times (2^7 - 1) \\
33550336 & = & 2^{12} \times 8191 & = & 2^{12} \times (2^{13} - 1)
\end{array}
$$

The numbers in the last column above should look familiar from the previous section. As we see from the factorizations above, each of the first five perfect numbers is of the form

$$2^{n-1} \times (2^n - 1),$$

where $2^n - 1$ is a Mersenne prime.

An old theorem states that an even number is perfect if and only if it is of the form $2^{n-1} \times (2^n - 1)$, where $2^n - 1$ is a Mersenne prime. So the pattern noted above is not a coincidence. In fact, we can use the theorem just stated

to find the next even perfect number: the next Mersenne prime after $2^{13} - 1$ is $2^{17} - 1$, and thus $2^{16} \times (2^{17} - 1)$, which equals 8589869056, is a perfect number.

Note that the theorem mentioned in the paragraph above characterizes only the even perfect numbers. A longstanding unanswered question is whether there are any odd perfect numbers. No one has ever found an odd perfect number, but no one has been able to prove that none exist.

Thus I was surprised several years ago, when I was an Associate Editor of the *American Mathematical Monthly*, to receive a paper submitted for publication that had as its main result the following statement:

> For any odd number, the sum of its divisors (not counting itself) is less than the number.

Now if the sum of the divisors (not counting itself) of each odd number is less than the number, then it cannot equal the number, and hence the number cannot be perfect. So if the statement above is correct, then there would be no odd perfect numbers. Curiously, the paper did not point out that the claimed result would answer a famous previously unanswered question; if fact, the paper did not even mention perfect numbers.

Perfect numbers are far from my area of expertise, but I knew enough to realize that the claimed result in the submitted paper would, if correct, solve a big problem and make the author famous. Could the claimed result possibly be true? I experimented by checking the odd numbers less than 50. The table below shows the results, where I have not bothered to list the prime numbers, because the sum of the divisors of each prime number, not counting itself, obviously equals 1.

n	sum of divisors of n, not counting n
9	4
15	9
21	11
25	6
27	13
33	15
35	13
39	17
45	33
49	8

As we see from the table above, for each odd number less than 50, the sum of the divisors of the number is less than the number, and in fact usually considerably so. At that point I turned to my computer and asked it to check all odd numbers less than 1000. The computer found one counterexample to the claimed result. Specifically, the sum of the divisors of 945, not counting 945, equals 975.

So the claimed result in the paper was false, and the alleged proof must contain an error. I had trouble following the proof, but at one point it seemed

to me that the author was implicitly assuming that the odd number under consideration has no repeated prime factors. For example,

$$945 = 3^3 \times 5 \times 7,$$

so 945 has a repeated prime factor of 3. Could it be true for each odd number with no repeated prime factors that the sum of the divisors of the number (not counting itself) is less than the number?

To answer this question, I turned back to my computer and asked it to find all the odd numbers less than 7500 whose divisors (not counting the number itself) add up to more than the number. Here is the list the computer provided, along with the prime factorizations of those numbers (also provided by the computer):

$$945 = 3^3 \times 5 \times 7$$
$$1575 = 3^2 \times 5^2 \times 7$$
$$2205 = 3^2 \times 5 \times 7^2$$
$$2835 = 3^4 \times 5 \times 7$$
$$3465 = 3^2 \times 5 \times 7 \times 11$$
$$4095 = 3^2 \times 5 \times 7 \times 13$$
$$4725 = 3^3 \times 5^2 \times 7$$
$$5355 = 3^2 \times 5 \times 7 \times 17$$
$$5775 = 3 \times 5^2 \times 7 \times 11$$
$$5985 = 3^2 \times 5 \times 7 \times 19$$
$$6435 = 3^2 \times 5 \times 11 \times 13$$
$$6615 = 3^3 \times 5 \times 7^2$$
$$6825 = 3 \times 5^2 \times 7 \times 13$$
$$7245 = 3^2 \times 5 \times 7 \times 23$$
$$7425 = 3^3 \times 5^2 \times 11$$

As we see from the table above, for each odd number less than 7500 whose divisors (not counting the number itself) add up to more than the number, the number in question has a prime factorization that repeats some prime factor. Thinking that this result might be true in general, I extended the range of my computer's search, asking it to check the odd numbers less than 15000. My computer found fifteen odd numbers between 7500 and 15000 whose divisors (not counting the number) add up to more the number. When the computer factored those numbers I saw that they, too, have repeated prime factors.

By then I thought I had good numeric evidence to suggest strongly that repeated prime factors play a key role in this question. But I asked my computer to search once more, doubling my previous search range to the odd numbers between 15000 and 30000. Alas, my computer found six odd numbers between

15000 and 30000 that smashed my hopes. The smallest of these numbers is 15015. The sum of the divisors of 15015 (not countintg 15015) equals 17241, which obviously is larger than 15015. But

$$15015 = 3 \times 5 \times 7 \times 11 \times 13,$$

so 15015 has no repeated prime factors.

The computer was killing all my conjectures. Hoping to salvage something from this excursion, I looked at the prime factorizations of all the odd numbers less than 30000 whose divisors (not counting the number itself) add up to more than the number. Nothing jumped out at me except that each of these numbers has 3 as a factor. Could it be that for every odd number not divisible by 3, the sum of the divisors (not counting the number itself) is less than the number? My feeling was that surely this question should have a negative answer. To find an example showing this, I asked my computer to find an odd number not divisible by 3 whose divisors (not counting the number itself) add up to more than the number.

First I told my computer to test the odd numbers less than a million. It found no odd numbers not divisible by 3 whose divisors (not counting the number itself) add up to more than the number. So I extended the range of the test up to ten-million, but after working for an hour the computer stated that there are no examples in that range either. Finally I extended the range of the test up to one-hundred-million. Checking the odd numbers in that range took my computer fourteen hours, and again it told me that there are no examples of the kind I sought.

Either my intuition about this question was wrong or an example was too hard for a computer to find. So I begin thinking about it. Suppose that $p > 5$ is a prime number large enough such that

$$\frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots + \frac{1}{p} > 1.$$

In other words, suppose that the sum of the reciprocals of the primes from 5 to p is greater than 1. Rewrite the left side of the inequality above, putting everything over the common denominator $5 \times 7 \times 11 \times \cdots \times p$. The numerator will be a sum of terms, the first of which is $7 \times 11 \times \cdots \times p$, the second of which is $5 \times 11 \times \cdots \times p$, on so on. Because the fraction is greater than 1, the sum of the terms in the numerator is greater than the denominator of $5 \times 7 \times 11 \times \cdots \times p$. But each of the terms in the numerator is a divisor of $5 \times 7 \times 11 \times \cdots \times p$. Thus the sum of all the divisors of $5 \times 7 \times 11 \times \cdots \times p$, not counting this number itself (it does not appear in the numerator), must be greater $5 \times 7 \times 11 \times \cdots \times p$. Because $5 \times 7 \times 11 \times \cdots \times p$ is not divisible by 3, we will have found our example.

Now we just need to find a prime number $p > 5$ such that

$$\frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots + \frac{1}{p} > 1.$$

This is a problem that the computer can quickly do. My computer tells me that $p = 109$ is the smallest prime number larger than 5 that makes the inequality

above true. Thus $5 \times 7 \times 11 \times \cdots \times 109$, which (according to my computer) equals

$$4662249946964248936304602697867796 8279166205,$$

is not divisible by 3 but the sum of its divisors (not counting the number itself) is larger than the number. This number is much larger than one-hundred-million, which is why my earlier search did not find it.

In fact $4662249946964248936304602697867796 8279166205$ is not the smallest number with the desired property, but because the smallest such number is larger than one-hundred-million, a brute-force computer search would take too long. So for this problem a mathematician, with some small help from a computer, easily solved a problem that stumped the computer alone.

Before leaving this subject, let's consider a harder question. Suppose we want to show that there exists an odd number not divisible by 3 such that the sum of the divisors of the number (not counting the number itself) is greater than 2 times the number. Or greater than 100 times the number? Is that possible? Using the same reasoning as before, all we need to do is show that there exists a prime $p > 5$ such that

$$\frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots + \frac{1}{p}$$

is larger than 2, or larger than 100 for the even more difficult question. A famous theorem (proved by mathematicians, not by computers!) states that the sum of the reciprocals of all the prime numbers equals infinity. That means that the sum above can be as large as we want, provided we take p large enough. My computer tells me that to get the sum above to be larger than 2, we need to take $p = 483281$ (or of course any larger value of p will work). My computer cannot compute a choice of p that will make the sum above larger than 100 (the smallest such p will be incredibly huge), although mathematics proves that such a prime number p exists. In this case mathematicians outperform the computer!

The results in this section show that even though a mathematical conjecture is true for the first few million examples, the conjecture could still be false. A computer can check more examples in a few minutes than a mathematician could check in a century, but without a proof, we cannot be sure that a counterexample lurks in some unchecked example. If a conjecture involves an infinite number of possible examples (as is the case with the integers), then a computer cannot check them all. It can check a large number of them, hoping to find a counterexample, in which case the conjecture is false. But if no counterexample is found, even among millions of cases, we still need a mathematician to prove that the result is true (or to find a clever way of finding a counterexample).

Twin Primes

A twin prime is a pair of prime numbers differing by 2. The first ten twin primes are $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}$, $\{41, 43\}$, $\{59, 61\}$, $\{71, 73\}$,

$\{101, 103\}$, $\{107, 109\}$. Although humans have known for over two thousand years that there are an infinite number of primes, we do not know whether there are an infinite number of twin primes.

As I write this paragraph in Spring 2002, the largest known twin prime is

$$\{318032361 \times 2^{107001} - 1,\ 318032361 \times 2^{107001} + 1\}.$$

But the record for the largest twin prime has been broken twelve times in the last three years, so there will likely be a new champion twin prime soon. A list of the twenty largest twin primes currently known is kept up to date on the web at `http://www.utm.edu/research/primes/lists/top20/twin.html`. Finding twin primes of this size without using a computer would be impossible.

Just for fun, let's list the first ten twin primes and the sum of the two numbers in each twin prime pair:

twin prime	sum
$\{3, 5\}$	8
$\{5, 7\}$	12
$\{11, 13\}$	24
$\{17, 19\}$	36
$\{29, 31\}$	60
$\{41, 43\}$	84
$\{59, 61\}$	120
$\{71, 73\}$	144
$\{101, 103\}$	204
$\{107, 109\}$	216

Notice anything special about the sums above? Except for the first entry of 8, all of the other sums above are divisible by 12. Could this be true for all twin primes other than $\{3, 5\}$?

To answer this question, we turn again to a computer, asking it to check all twin primes less than a million. My computer says that the sums are all divisible by 12, except for $\{3, 5\}$. I get the same answer after asking my computer to check all twin primes less than ten-million. This may sound convincing, but in the previous section we looked at a mathematical statement that turned out to be false even though it was true for all numbers less than one-hundred million.

This time the evidence provided by the computer points in the right direction. It really is true that for each twin prime pair except $\{3, 5\}$, the sum of the two primes is divisible by 12. A computer cannot prove that, because the computer cannot check all possible twin primes. But you can prove it. I will leave this as a homework exercise for you. The proof does not require any high-powered tools, just some simple reasoning that can be discovered by anyone reading this article. Give it a try!

The Winner

Earlier I mentioned the proof via computer of the four-color theorem as one of the great and early triumphs of computers in mathematics. We have seen examples, however, emphasizing that computers can check only a finite number of cases. Because there are an infinite number of possible maps, how could a computer prove that each of them can be colored with at most four colors so that no two adjacent countries have the same color? What happened here is that mathematicians proved a theorem showing that only certain cases had to be checked. The number of cases that must be checked, according to this theorem, is finite. This finite number of cases is too large to check by hand, so computers were called in to finish the job.

The cooperation demonstrated in the proof of the four-color theorem between mathematicians and computers may be typical of much of the future progress of mathematics. Some problems a computer can solve simply by virtue of being able to calculate very quickly—an example would be the factorization of $2^{67} - 1$, which had been falsely suspected of being a Mersenne prime. Other problems are so hard that computers can provide no help; here one thinks of the remarkable proof of Fermat's Last Theorem by Andrew Wiles, who worked completely without computer assistance.

Computers still cannot provide the creative, clever, and imaginative proofs that give mathematics much of its beauty. But mathematicians do not cling to proofs just because we can do them better than computers. *We insist upon proofs because proof is the only method we have for determining most mathematical truths.*

A computer can check a hundred-million examples, provide evidence, carry out numeric experiments, draw fantastic pictures, and sometimes find counterexamples. Mathematicians need to take advantage of this wonderful tool. Working with computers, we can explore and discover at a pace that would have been inconceivable before the silicon age. Machines will not replace mathematicians, but computers will help mathematicians do mathematics better. Mathematics will emerge as the big winner in this collaboration between mathematicians and computers.

Department of Mathematics
San Francisco State University
San Francisco, CA 94132 USA

e-mail: `axler@sfsu.edu`
web site: `http://www.axler.net`