Is there a greater role for prime numbers in our schools?[1]

Grant Cairns
La Trobe University
<g.cairns@latrobe.edu.au>

Prime numbers play an extremely important role in modern mathematics. Apart from still being the object of intense research activity, their applications in banking and security underline a key phenomenon: in the modern world, useful applications of mathematics often come from very 'pure' abstract theories.[1]

Curiously, despite their undeniable importance, prime numbers are largely absent from school curricula. Prime numbers are typically encountered in Year 7. There one looks at the sieve of Eratosthenes, which students use to find the primes up to some limit, like 100. Another common thing to do at this age is to explore Goldbach's conjecture: that every even number ≥ 4 is the sum of two primes. Students might be asked to find all pairs of primes that add up to 76, for example. Sadly, this is often the only material on primes that some students see in their entire school studies.

At the other end of the spectrum, there is a vast amount of literature on primes and number theory in general that is focused on the introductory university level. There are many excellent books with inviting titles like *My Numbers, My Friends* (Ribenboim, 2000) and *A Friendly Introduction to Number Theory* (Silverman 1996). In particular, there are many fine books on number theory in the Dover editions that are reasonably priced. However, very few of these are suitable for use in high schools. Indeed, there is an enormous gulf between Year 7 and university, with few appropriate texts, and little use of primes in school syllabuses. Why is this so, and how can more material on primes be introduced into school curricula?

My contention is that the key problem with the available material on number theory is their use of modular arithmetic, often called *clock arithmetic*. On a normal twelve-hour clock, eight o'clock plus six hours brings you to two o'clock; in symbols, one writes $8 + 6 \equiv 2$ (modulo 12). Working in a more general context, say on a clock based on the number 9 instead of 12 for example, one would have $8 + 6 \equiv 5$ (modulo 9). Similarly, one has statements

1. This is an expanded version of a keynote address given at the Mathematics Association of Victoria Conference, 4 December 2003.

like $8 \times 6 \equiv 9$ (modulo 13). This 'modular arithmetic' is a common starting point for many introductory books on number theory, and while it is not out of the reach of many high school students, it does require mathematical maturity; using it in high schools to prove facts about numbers would no doubt present quite a challenge.

The object of this paper is to present some of the key questions and elementary ideas concerning number theory and primes in particular that can be explored without modular arithmetic. It is by no means a survey of modern number theory; instead it aims to provide a selection of ideas, some old, some modern, that can be comprehended and explored without modular arithmetic. These topics could, I believe, provide possible subject material for introduction into school curricula, thus hopefully enabling a greater role for prime numbers in school mathematics.

There are infinitely many primes

A good recent introduction to primes is given in Rasmussen (2004). Recall that a prime number is an integer $p \geq 2$ whose only positive divisors are itself and 1. Let p_i denote the ith prime. So $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. A fundamental conceptual breakthrough, which goes back to antiquity, comes with an understanding of why there are infinitely many primes; that is, why does the list of primes go on for ever, or expressed differently, why is there not a last prime beyond which there are no more primes?

There are many ways to see this. The classical proof in Euclid's *Elements* uses what today are called the *primorial numbers*. For a given prime p, the primorial number P is the product of the primes up to and including p. So if p_k denotes the kth prime, then $P_k = p_1.p_2 \ldots p_k$. For example,[2]

$P_1 = 2$
$P_2 = 2 \,.\, 3 = 6$
$P_3 = 2 \,.\, 3 \,.\, 5 = 30$
$P_4 = 2 \,.\, 3 \,.\, 5 \,.\, 7 = 210$
$P_5 = 2 \,.\, 3 \,.\, 5 \,.\, 7 \,.\, 11 = 2310$
$P_6 = 2 \,.\, 3 \,.\, 5 \,.\, 7 \,.\, 11 \,.\, 13 = 30030.$

Suppose there is a last prime, p_k say. Then, P_k is the product of all primes. Consider $P_k + 1$. Every natural number greater than 1 is divisible by a prime. So $P_k + 1$ must be divisible by some prime p_i. Since P_k is the product of all the primes, P_k is divisible by p_i. Thus $1 = (P_k + 1) - P_k$ is also divisible by p_i — but this is impossible! We conclude that our assumption that there is a last prime must be wrong. So there are infinitely many primes.

One striking aspect of the above proof is its use of 'argument by contra-

2. The term 'primorial' is cute; it is of course adapted from 'factorial' which is a product of the natural numbers, but it is also like 'primordial', and primorial numbers are certainly primordial, from a number theory perspective.

diction'. The proof starts by assuming there is a last prime; that is, one starts by assuming the opposite of what one wants to prove. A contradiction is obtained: the impossibility that 1 is divisible by a prime. The conclusion is then drawn: the initial assumption must be false. Most people have an intuitive understanding of 'argument by contradiction' and they use it in their daily lives. However, even at university, there are many students who have trouble getting the argument straight, and in particular, writing such an argument down coherently in words. In my opinion, this classic proof is an excellent way to help students learn to argue by contradiction.

A second aspect of the proof concerns a subtle point that is easily misunderstood; it has to do with what the proof does not prove. It does not prove that $P_k + 1$ is prime for every k. In fact, for $k = 1, 2, 3, 4, 5$, the numbers $P_k + 1$ are 3, 7, 31, 211, 2311, which are prime, but $P_6 + 1 = 30031$ is *not* prime; $30031 = 59 \times 509$. Primes of the form $P_k + 1$ (or $P_k - 1$) are called *primorial primes*; we do not know if there are infinitely many such primes, though this is conjectured to be the case (see Caldwell & Gallot, 2002).

Conjecture.
There are infinitely many primorial primes.

Prime numbers provide a host of easily stated questions like the above conjecture. This is useful, because it is instructive for students to learn that mathematics is continually developing, and that there are many open problems that are the object of active investigation.

Table 1. Calculation for the greatest common divisor of 5194 and 3850.

5194	3850
1344	3850
1344	2506
1344	1162
182	1162
182	980
182	798
182	616
182	434
182	252
182	70
112	70
42	70
42	28
14	28
14	14
0	14

There are infinitely many primes, and they are actually quite common

The abundance of the primes is a recurring theme in number theory. Not only are there infinitely many primes, but there are infinitely many primes of many different kinds. The most famous, and oldest result of this kind is Dirichlet's theorem.

Dirichlet's Theorem.
If a and b are coprime, then there are infinitely many primes in the arithmetic progression $a, a + b, a + 2b, a + 3b\ldots$

To understand the statement of Dirichlet's theorem, recall that given two integers a and b, their *greatest common divisor* is the largest integer which is a divisor of both a and b; we denote it $\gcd(a,b)$. The gcd can be calculated by *Euclid's algorithm*, which can be easily done on a spreadsheet (or calculator): starting with a and b, we replace the smaller of the two by the difference between them. We repeat this procedure until one of the numbers eventually goes to zero; the gcd is the last non-zero number. The calculation in Table 1

shows that gcd(5194,3850) = 14. (Experimenting with calculations of the gcd on a spreadsheet quickly leads one to the question: how can the program be modified to make it work in fewer steps?). Two integers a and b are said to be coprime if their gcd is 1; in other words, a and b have no common prime factor. For example, 3 and 10 are *coprime*. So in this case, Dirichlet's theorem says that there are infinitely many primes in the sequence 3, 13, 23, 33, 43…

In addition to results like Dirichlet's theorem, that attest to the abundance of the primes, there is a superabundance of open questions and conjectures which flow from a general conviction that there are so many primes that everything is possible. Of these the two most famous are:

> ***The twin prime conjecture.***
> There are infinitely many twin primes.

A twin prime is a pair of primes of the form p, $p + 2$, like 5, 7 or 29, 31, or 347, 349, or 265 237 079 981, 265 237 079 983, for example.

> ***Goldbach's Conjecture.***
> Every even number can be written as the sum of two primes.

Goldbach's conjecture has been verified up to 10^{17} (see e Silva). A prize of US$1 000 000 for a solution of Goldbach's conjecture was temporarily offered as publicity for the printing of the English addition of the amusing novel by Doxiadis (2000). For a compilation of classic papers on Goldbach's conjecture, see Wang (1984).

There are infinitely many primes, but they are actually quite sparse

Some infinite families have a greater presence than others. For example, the family of squares, 1, 4, 9, 16, 25, 36, 49… is an infinite family, but the gap between successive members becomes arbitrarily large. This may be compared for example, with the infinite family of odd numbers, 1, 3, 5, 7, 9, 11… which has no more members than the family of squares, but here the gap between successive members is constant, at 2.

The family of prime numbers has arbitrarily large gaps in it. Consider the kth primorial number P_k. The number $P_k + 1$ may or may not be prime, as we saw before. Consider the next $p_{k+1} - 2$ integers:

$$P_k + 2,\ P_k + 3,\ P_k + 4 \ldots\ P_k + p_{k+1} - 1.$$

None of these numbers is prime. Indeed, for $2 \le i \le p_{k+1} - 1$, the number i is divisible by some prime $p \le p_k$, and P_k is divisible by p, and so $P_k + i$ is divisible by p. Thus $P_k + i$ is not prime. Since p_{k+1} becomes arbitrarily large as we

increase k, this shows that there are arbitrarily long gaps between the primes.

For a given prime p, the gap until the next prime is called the prime gap and is denoted $g(p)$; that is, $g(p_k) = p_{k+1} - p_k$. There is an enormous amount of work that has been done on prime gaps — how $g(p)$ increases with p, what numbers appear as gaps, and how often they appear — but there is very much that remains to be answered. It is not known if every even number is a prime gap or even if every even number can be written as the difference between two (not necessarily successive) primes. This is:

Polignac's Conjecture.
Every even number can be written as the difference of two primes.

Notice the similarity between Polignac's conjecture and Goldbach's conjecture. Actually, Polignac also conjectured that every even number can be written as the difference of two primes in infinitely many ways. In particular, if this is true for the even number 2, then the twin prime conjecture would follow.

The prime numbers are difficult to visualise on the real number line, but the situation stands out nicely on the Cartesian plane. Here, one considers the integer lattice, and one shades the unit square centred at the integer point (x, y) with a shade which depends on the number $\gcd(x, y)$. Figure 1 gives the plot for the numbers (x, y) with x and y between 0 and 10. Squares with gcd = 1 are shaded black while squares with higher gcd receive a light hue, which decreases as the gcd increases. At this scale there is not much to see. There is a vertical black line at $x = 1$; this is because $\gcd(1,y) = 1$, for all y. Similarly, there is a horizontal black line at $y = 1$. Indeed, the figure is symmetrical about the line $y = x$.

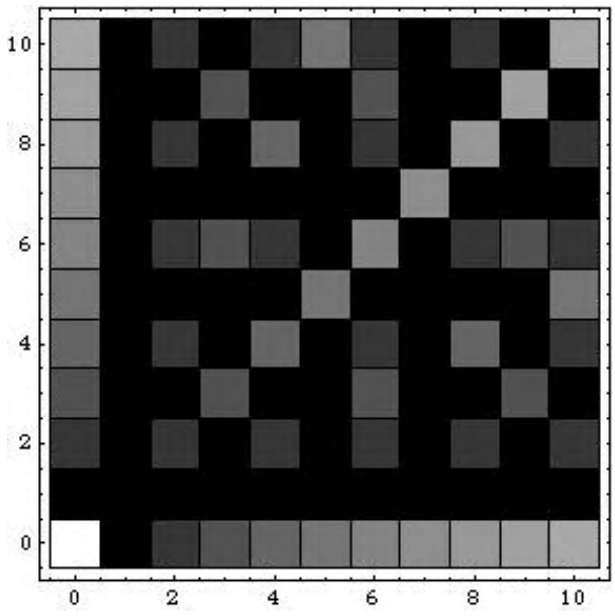

Figure 1. 10 × 10 integer lattice illustrating greatest common divisors of x and y, for points (x, y) on the plane.

Figure 2 gives the plot with x and y between 0 and 50. More of a pattern is immerging here. For each prime p the vertical line $x = p$ is black except for a few squares; this is because $\gcd(p,y) = 1$, except when y is a multiple of p. So Figure 2 displays several vertical and horizontal lines which are (almost entirely) black. Notice the two black vertical lines at $x = 29$ and $x = 31$. These are twin primes, and all twin primes will appear as similar vertical black lines two units apart; for example, 41 and 43 form another twin pair visible in

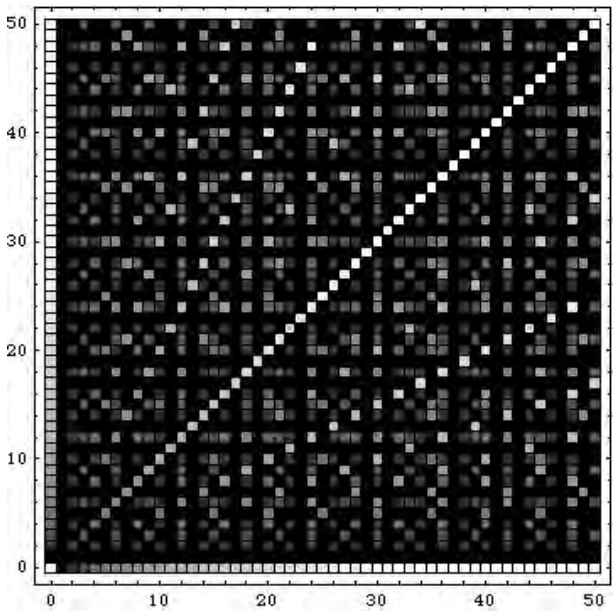

Figure 2. 50× 50 integer lattice illustrating greatest common divisors of x and y, for points (x, y) on the plane.

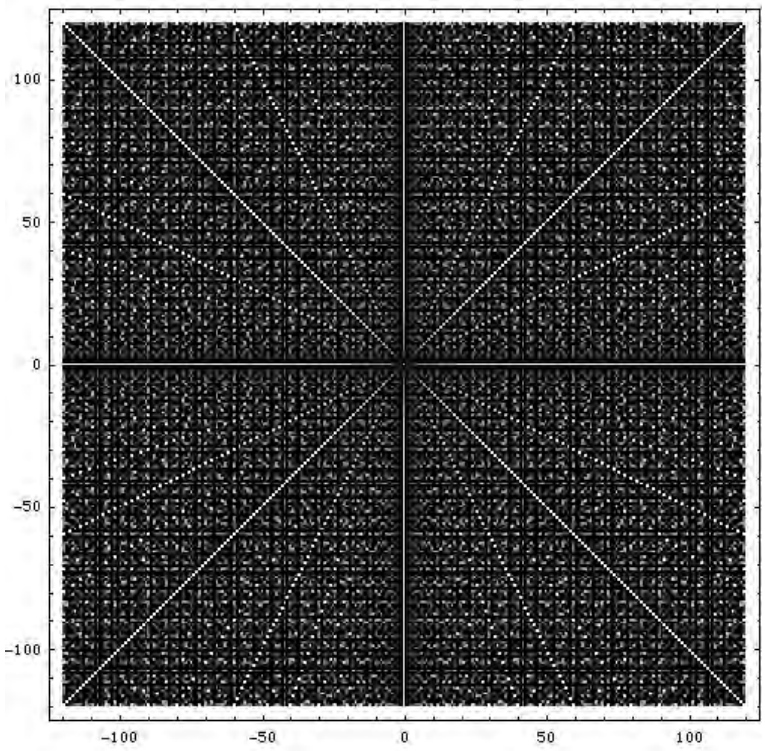

Figure 3. Plot illustrating Polignac's conjecture

Figure 2. Notice also that there are several black lines at 45 degrees to the axes, along lines of the form $y + x = n$. One such line is $y + x = 37$. Indeed, if $y + x$ is a prime p, then $\gcd(x,y) = 1$, except when both x and y are multiples of p. Goldbach's conjecture says that for every even number n, the line $y + x = n$ contains a point (x,y) whose coordinates x,y are both prime. Although it is harder to observe them in Figure 2, there also several black lines of the form $y - x = n$. One such line is $y - x = 17$. Polignac's conjecture says that for every even number n, the line $y - x = n$ contains a point (x,y) whose coordinates x,y are both prime. Figure 3 gives the plot of the numbers (x,y) with $|x|, |y| < 120$. It is much harder to read the axes now. The way I suggest the reader views this figure is to hold it at arms length, appreciate it as one would a painting, and simply admire the beauty of numbers.

We know nothing

Seeing the number of open conjectures that we have discussed so far, one might well believe that there is still much to discover about primes (and about mathematics in general). In fact, we have not even scratched the surface; there are so many open problems just about primes, that it is a daunting prospect just to keep track of them. The most famous problem on primes (and perhaps the most famous outstanding problem in mathematics) is the so-called *Riemann hypothesis*. It is one of the 'millennium problems'; there is a prize of US$1 000 000 for the solution of any of these. There is an excellent survey article on the Riemann hypothesis by Conrey (2003), and there are three recent popular books on the subject: Derbyshire (2003), du Sautoy (2003) and Sabbagh (2003). Before reading any of these, check out their Mathematical Association of America reviews (MAA).

To get some idea of the quality of unsolved conjectures and open problems (and how little we really know), consider the twin prime conjecture: there are infinitely many prime pairs p, $p + 2$. It is actually also conjectured that there are infinitely many prime triplets p, $p + 2$, $p + 6$, and infinitely many prime triplets p, $p + 4$, $p + 6$, and infinitely many prime quadruplets p, $p + 2$, $p + 6$, $p + 8$, and so on[3] (people have found prime 18-tuplets; see Forbes, 2004). It is conjectured that for every even natural number k, there are infinitely many prime pairs p, $p + k$ (this is just a restatement of Polignac's conjecture).

In fact it is also conjectured that for every n, there are n consecutive primes in arithmetic progression; at the time of writing, the longest such string consists of 10 primes (see Caldwell, 2004b). A major recent breakthrough has been made by Ben Green and the Australian mathematician Terence Tao. They have shown that there are arbitrarily long arithmetic sequences of (not necessarily consecutive) primes (see Peterson).

I have already mentioned that the numbers $P_k + 1$ are sometimes prime.

3. It is a waste of time looking at triples of the form p, $p + 2$, $p + 4$ since every such triple includes a number divisible by 3.

When they are not, consider the smallest natural number d such that $P_k + d$ is prime; Reo Fortune conjectured that the numbers d are themselves prime: they are called the *fortunate numbers* (Golomb, 1981). Fortune was a well-known anthropologist; see Banderier for some amusing details about his life.

Of course, it is easy to ask questions that cannot be answered. Concerning the conjecture that there are infinitely many primorial primes, Pólya is reported to have commented: 'There are many questions which fools can ask that wise men cannot answer' (Eves, 1988). Some conjectures are based on little evidence. For example, if one looks at the gaps between the primes, one finds that for low numbers, the most common prime gap is 2. As one looks at bigger numbers, the most common prime gap is 2 or 4, until one gets up to 563, at which point it jumps to 6. The most common gap (termed the jumping champion by John H. Conway) remains at 6 for most numbers that have been calculated. Nevertheless it is believed that eventually (around 10^{35}?) it is replaced by 30, and again (around 10^{425}?) by 210, and that in fact, apart from the number 4, the jumping champions are actually the primorial numbers 2, 6, 30, 210, 2310, etc. (Odlyzko, Rubinstein &Wolf, 1999). Go figure!

We know everything

It is often commented that the primes are shrouded in a mystery that humanity may never fully comprehend. And to this day it is regularly asserted that, 'There is no known formula for the nth prime number, nor any recursion formula that allows one to find the $(n + 1)$th prime number from the first n primes'. Thus, it may come as a shock to some readers to learn that there are many known formulas for the nth prime (see Dudley, 1983). Perhaps the most striking is the 1971 formula by J. M. Gandhi. This formula is doubly surprising because of its simplicity. In order to present it, let us first consider the divisors of the kth primorial P_k. There are, of course, k divisors of P_k that consist of a single prime: these are just the primes $p_1 \ldots p_k$.

There are $\binom{k}{2}$ divisors which are products of 2 primes, and in general, for each i with $1 \le i \le k$, there are $\binom{k}{i}$ divisors involving i primes.

So altogether there are

$$1 + k + \binom{k}{2} + \ldots + \binom{k}{k-1} + 1 = 2^k$$

divisors of P_k. For example, the divisors of $P_4 = 2 \cdot 3 \cdot 5 \cdot 7$ are:

$$\begin{array}{c} 2 \cdot 3 \cdot 5 \cdot 7 \\ 2 \cdot 3 \cdot 5 \quad 2 \cdot 3 \cdot 7 \quad 2 \cdot 5 \cdot 7 \quad 3 \cdot 5 \cdot 7 \\ 2 \cdot 3 \quad 2 \cdot 5 \quad 2 \cdot 7 \quad 3 \cdot 5 \quad 3 \cdot 7 \quad 5 \cdot 7 \\ 2 \quad 3 \quad 5 \quad 7 \\ 1 \end{array}$$

For each divisor d, we set $\mu(d) = 1$ if d involves an even number of primes, and we set $\mu(d) = -1$ if d involves an odd number of primes (μ is called the Möbius function; see Silverman for example). Now consider the following sum over the divisors d:

$$\sum_{d|P^k} \frac{\mu(d)}{2^d - 1}$$

For example, for $k = 2$, the primorial P_2 is 2.3 and the sum is:

$$\frac{1}{2^1-1} - \left(\frac{1}{2^2-1} + \frac{1}{2^3-1} \right) + \frac{1}{2^{2.3}-1} = \frac{1}{1} - \left(\frac{1}{3} + \frac{1}{7} \right) + \frac{1}{63} = 1 - \frac{10}{21} + \frac{1}{63} = 1 - \frac{29}{63}$$

Now consider the following procedure: subtract $\frac{1}{2}$ from the sum, take the logarithm to base 2, subtract your answer from 1 and take the integer part. The claim is that this gives the next prime!

Ghandi's formula.
The prime p_{k+1} is:

$$p_{k+1} = \left\lfloor 1 - \log_2 \left(-\frac{1}{2} + \sum_{d|p_k} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor$$

Let us apply Gandhi's formula in the case $k = 2$, and verify that it gives the expected result $p_3 = 5$. In this case the sum is, from above,

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = 1 - \frac{29}{63}$$

so

$$-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2} - \frac{29}{63}$$

and

$$\log_2 \left(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1} \right) \sim \log_2 0.04 \sim -4.6$$

Thus

$$p_3 = \lfloor 1 - (-4.6) \rfloor = \lfloor 5.6 \rfloor = 5$$

as desired!

Why does Gandhi's formula work? I will not go into it here, but merely comment that it results from just two things: the sieve of Eratosthenes, and the infinite series expansion

$$\frac{1}{2^d - 1} = \frac{1}{2^d} + \frac{1}{2^{2d}} + \frac{1}{2^{3d}} + \ldots$$

Actually, the number 2 is irrelevant; if you prefer, you could replace 2 by 10 or e, and then use logarithms to base 10 or natural logarithms. A nice

account of Gandhi's formula and its different proofs is given in Ribenboim (1996).

Pseudoprimes to the rescue

Of course, the problem with Gandhi's formula is that it is useless for computing primes. The number of terms in the summation grows exponentially, so that by the time you try to compute the 25th prime (which is 97), the summation involves over 30 million terms. Fortunately there are faster ways to find primes. A tried and true technique is to split the problem into two parts:

1. Find numbers which you are pretty sure are prime, and then
2. Verify that these numbers really are prime.

In order to accomplish the first task, one standard method is to use pseudoprimes. It has been known for hundreds of years that if p is prime, then $2^p - 2$ is divisible by p; this is a consequence of Fermat's *Little Theorem*. It is usually proved using modular arithmetic, but this is not necessary. Let us pause a moment to give Euler's original simple proof (see Sandifer, 2003). By the binomial expansion,

$$(1+1)^p = 1 + p + \binom{p}{2} + \ldots + \binom{p}{p-1} + 1$$

we have

$$2^p - 2 = p + \binom{p}{2} + \ldots + \binom{p}{p-1}$$

If p is prime, each of the terms $\binom{p}{i}$ is divisible by p,

and so $2^p - 2$ is divisible by p, as required.

It turns out that there are numbers that pass this test and are not prime; for example, $2^{341} - 2$ is divisible by 341, but 341 is not prime: $341 = 11 \times 31$. Numbers like 341 that pass the test but are not prime are said to be *pseudoprime*. The fortunate thing about them is that they are quite rare, so if a number p satisfies the condition that $2^p - 2$ is divisible by p, then we can be reasonably confident that it is prime.[4]

To verify that a given number p really is prime, there are a number of known methods and a great deal of interest in developing faster algorithms. It had long been conjectured that there is an algorithm whose duration is a polynomial function of the number of digits in the given number p. In 2002, Manindra Agrawal, Neeraj Kayal and Nitin Saxena, from the Indian Institute of Technology in Kanpur, shocked the world by finding such an algorithm.

4. One can also use other numbers apart from 2: if p is prime and $1 < a < p$, then the argument I used above can be extended to show that $a^p - a$ is divisible by p.

Their discovery was widely reported in the press, and the website posting their algorithm received over 2 million hits in the first ten days. There is an excellent article on the AKS (Agrawal Kayal Saxena) algorithm by Folkmar (2003). The starting point of their remarkably simple algorithm is a generalisation of Fermat's little theorem[5]: if $1 < a < p$, then p is prime if and only if the coefficients of the polynomial $(x - a)^p - (x^p - a)$ are all divisible by p.

There is currently a lot of work being done on just how practical the algorithm is. As Chris Caldwell (2004c) notes: 'This field is in great deal of flux at this time!'.

Activities with primes

One of the features of the study of primes numbers is that it lends itself well to student projects. There are so many different kinds of primes (Sophie Germain primes, Fermat primes, Mersenne primes, factorial primes, primorial primes, etc.), and so many different questions about them. So there are plenty of good project topics. For example: 'Find out what is a "Sophie Germain prime", what is the largest known Sophie Germain prime, and find out something about the person Sophie Germain'.

The other thing that comes readily to mind is the possibility of computer computations. If you have access to some software, then students can learn a lot by writing programs. The obvious thing to do is to write a program that will calculate the primes up to some given limit. There is also a variety of software that can be downloaded from the web. As well, one can get involved in one of the collaborative prime searching projects; this would make an excellent class group project; one is the *Great Internet Mersenne Prime Search* (GIMPS).

Finally, one thing one can do with primes is use them as a vehicle for teaching 'proofs'. Although proofs are probably not very popular with students, nor with most teachers, proofs remain the main tool of the working mathematician. Prime numbers provide a possible context for exploring proofs and proof strategies, and could conceivably play the role in schools that was once held admirably by the logical arguments of classical geometry. Perhaps the cleanest and nicest thing to do with prime numbers is to prove the fundamental theorem of arithmetic: every integer can be written as a product of primes in an essentially unique way. This material is completely self-contained, and it provides an excellent example of the necessity for mathematical clarity, not to mention a great example of the nature of mathematical proof.

For the study of primes at high schools, there is a great deal of information available on the Internet, although one has to be a little wary. The Web has many bogus proofs of key conjectures, not to mention those that see spiritual significance in the primes, and those for whom 'the distribution of prime

5. This can also be proved easily using the binomial expansion, without using modular arithmetic.

numbers is actually the structural plan of the universe' — but there are many excellent websites devoted to the primes. Here are just a few, that the reader may wish to use as starting places: MacTutor; Caldwell (2004a); Gallot and Gallot; Wikipedia; Rivera; Brown; Richstein; Alfeld; Math Forum; EFF; join in the hunt for primes (Caldwell, 2004d); listen to a BBC radio program (Singh); listen to the music of the primes (AT); explore prime problems for school students (Brooke Weston CTC); and challenging computational prime problems (Rock).

There are also a number of 'prime questions' on the Web that can be done without much background. As an example of the sort of thing that is available, here are three typical questions, taken from the Manhattan Mathematical Olympiad:

1. Prove that, when we divide any prime number by 30, we get a remainder which is equal to either 1 or a prime number.
2. Find all prime numbers p for which $p + 10$ and $p + 14$ are also prime.
3. Prove that if a prime number m has the property that $m^2 + 2$ is also prime, then $m^3 + 2$ must also be prime.

Conclusion

Prime numbers remain an exciting and important part of mathematics. They offer many open problems that high school students can understand. And in this vibrant area of research, there are regularly new breakthroughs and important discoveries. But sadly, prime numbers enjoy a very low profile in our school curricula. I believe that part of the problem lies with the fact that, commonly, introductory teaching materials on number theory start with modular arithmetic, which by its nature, leads one down an austere, abstract path which may not be suitable for the school teaching/learning context.

In this paper I have attempted to show that there is a wealth of important material on prime numbers that can be explored without resorting to modular arithmetic. There are theoretic investigations: such as the fact that the gap between successive primes can be arbitrarily large (see Section 3 above), and Fermat's little theorem (see Section 6 above). There is an historical dimension to primes, with famous conjectures like Goldbach's conjecture and the twin prime conjecture, and personalities like Reo Fortune and Sophie Germain. There are challenging problems, and there are informative investigations that can be carried out by spreadsheet, or by calculator. Perhaps most importantly, prime numbers provide a excellent vehicle for the development of analytic and deductive reasoning skills.

So, is there a greater role for prime numbers in our schools? The realist may answer: what would you have primes replace? Of course, few people are willing to venture that students do not really need to know this or that piece of the current curriculum. In fact, curriculum content is a difficult matter. The curriculum no doubt has a considerable amount of inertia, and this is probably a good thing. Many of us who teach mathematics have our focus on the teaching, rather than the content, since the teaching is the obvious thing

one can change on a day-to-day basis. However, the curriculum is critical, and against a tide that would water it down, perhaps there is a case for including something additional, such as the material offered by the primes.

References

Alfeld, P. (n.d.). *The Prime Machine*. Retrieved 25 October 2004, from: http://www.math.utah.edu/~alfeld/math/machine.html.

AT open publisher (n.d.). *Aesthetics of the Prime Sequence*. 25 Retrieved October 2004, from: http://www.2357.a-tu.net/index.php?link=Music.

Banderier, C. (n.d.). *Fortunate and Unfortunate Primes: Nearest Primes from a Prime Factorial*. Retrieved 25 October 2004, from: http://algo.inria.fr/banderier/Computations/prime_factorial.html.

Borneman, F. (2003). PRIMES is in P: A breakthrough for 'Everyman'. *Notices of the American Mathematical Society, 50*, 545–552.

Brooke Weston CTC (n.d.). *Mathematics Masterclasses: Prime Number Challenges*. Retrieved 25 October 2004, from: http://www.bwctc.northants.sch.uk/html/master/maths/autumn99/primech.htm.

Brown, K. (n.d.). *Mathpages: Number Theory*. Retrieved 25 October 2004, from: http://www.mathpages.com/home/inumber.htm.

Caldwell, C. K. (2004a). *The Prime Pages*. Retrieved 25 October 2004, from: http://www.utm.edu/research/primes.

Caldwell, C. K. (2004b). Consecutive primes in arithmetic progression. *The Prime Pages*. Retrieved 25 October 2004, from: http://primes.utm.edu/top20/page.php?id=13.

Caldwell, C. K. (2004c). Finding primes and proving primality. *The Prime Pages*. Retrieved 25 October 2004, from: http://www.utm.edu/research/primes/prove/prove4_3.html.

Caldwell, C. K. (2004d). The top 5000: Finding large primes. *The Prime Pages*. Retrieved 25 October 2004, from: http://primes.utm.edu/primes/background/finding.php.

Caldwell, C. K. & Gallot, Y. (2002). On the primality of n! ± 1 and 2 x 3 x 5 x … x p ± 1. *Mathematics of Computation, 71* (237), 441–448.

Conrey, J. B. (2003). The Riemann hypothesis. *Notices of the American Mathematical Society, 50*, 341–353.

Derbyshire, J. (2003). *Prime Obsession*. Washington, DC: Joseph Henry Press.

Doxiadis, A. (2000). *Uncle Petros and Goldbach's Conjecture*. New York: Bloomsbury.

du Sautoy, M. (2003). *The Music of the Primes*. Harper Collins.

Dudley, U. (1983). Formulas for primes. *Mathematics Magazine, 56*, 17–22.

e Silva, O. (n.d.). *Goldbach Conjecture Verification*. Retrieved 25 October 2004, from: http://www.ieeta.pt/~tos/goldbach.html.

EFF Cooperative Computing Awards (n.d.). *Prime Number Resources and Information*. Retrieved 25 October 2004, from: http://www.eff.org/awards/prime-info.html.

Eves, H. (1988). *Return to Mathematical Circles*. Boston: PWS-KENT Publishing Co.

Forbes, T. (n.d.). *Prime k-tuplets*. Retrieved 27 October 2004, from: http://www.ltkz.demon.co.uk/ktuplets.htm.

Gallot, L. & Gallot, Y. (n.d.). *The Chronology of Prime Number Records*. Retrieved 25 October 2004, from: http://perso.wanadoo.fr/yves.gallot/primes/chrrcds.html.

GIMPS (n.d.). *The Great Internet Mersenne Prime Search (GIMPS) home page*. Retrieved 25 October 2004, from: http://www.mersenne.org/prime.htm.

Golomb, S. W. (1981). The evidence for Fortune's conjecture. *Mathematics Magazine, 54*, 209–210.

Mathematics Association of America (n.d.). *MAA Online Book Review*. Retrieved October 25, 2004, from: http://www.maa.org/reviews/reviews_index.html.

O'Connor, J. & Robertson, E. (n.d.). Prime numbers. *MacTutor History of Mathematics archive*. Retrieved 25 October 2004, from: http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Prime_numbers.html.

Math Forum (n.d.). Middle School Prime Numbers. Retrieved 25 October 2004, from: http://mathforum.org/library/drmath/sets/mid_prime_numbers.html.

Odlyzko, A., Rubinstein, M. & Wolf, M. (1999). Jumping champions. *Experimental Mathematics, 8*, 107–118.

Peterson, I. (2004). Progressive primes. *Science News Online, 165* (17). Retrieved 25 October 2004 from: http://www.sciencenews.org/articles/20040424/mathtrek.asp.

Rasmussen, D. (2004). Prime number. *Prime Number, 19*, 23–28.

Ribenboim, P. (1996). *The New Book of Prime Number Records*. New York: Springer-Verlag.

Ribenboim, P. (2000). *My Numbers, My Friends*. New York: Springer-Verlag.

Richstein, J. (n.d.) *Verifying the Goldbach Conjecture up to 4.104*. Retrieved 25 October 2004 from: http://www.informatik.uni-giessen.de/staff/richstein/ca/Goldbach.html.

Rivera, C. (n.d.). *The Prime Puzzles and Problems Connection*. Retrieved 25 October 2004 from: http://www.primepuzzles.net.

Rock, D. (n.d.). *Ole Miss: Problem of the Week*. Retrieved 25 October 2004 from: http://www.olemiss.edu/mathed/pow/powold.htm

Sabbagh, K. (2003). *The Riemann Hypothesis: The Greatest Unsolved Problem in Mathematics*. Farrar, Strauss and Giroux.

Sandifer, E. (2003). *Fermat's Little Theorem. How Euler Did It*. Retrieved 25 October 2004 from: http://www.maa.org/news/howeulerdidit.html.

Silverman, J. H. (1996). *A Friendly Introduction to Number Theory*. Prentice Hall.

Singh, S. (2003). *Another 5 Numbers: The Largest Prime Number*. Retrieved 25 October 2004 from: http://www.bbc.co.uk/radio4/science/another53.shtml.

Wang Y. (1984). *Goldbach Conjecture*. Singapore: World Scientific Publishing Co.

Wikipedia (n.d.). *Prime number*. Retrieved 25 October 2004, from: http://en.wikipedia.org/wiki/Prime_number