The Sieve of Eratosthenes

Around 250 BC the Greek mathematician Eratosthenes used a spectacularly simple method to find primes which has become known as the sieve of Eratosthenes. Here is how it finds all the prime numbers among the first 120 numbers, which are listed, with the exception of the number 1, in the following array:

–	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

The even numbers 4, 6, 8, 10, . . . are all composite since their respective factorizations are 2×2, 2×3, 2×4, 2×5, and so on. The first sieving, "based on the prime" 2, proceeds as follows: beginning with the number 4, "sieve," or delete, every second number by leaving the corresponding cell blank. This operation of skipping over numbers, or cells, to reach other ones involves nothing more than counting. When this is done the original array becomes

–	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	
101		103		105		107		109	
111		113		115		117		119	

Since the number 3 has not been sieved, it is the next prime and is used for the second sieving. Now empty every third cell after 3: one, two, delete, one, two, delete, and so on. It doesn't matter if a cell, such as that corresponding to 6, is already blank. The reason blank cells (corresponding to numbers that have already been sieved out) are never removed is to ensure that the skipping proceeds correctly at all stages. The blank cells are a vital record of where numbers were. After this second sieving, the array becomes

–	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			
101		103				107		109	
		113		115				119	

It is worth noting that the first number to be sieved by this second sieving based on 3 is its square, $9 = 3^2 = 3 \times 3$.

Since the number 5 has not been sieved by either of the two previous sievings, it must be the third prime and the basis for the next sieving. Leaving every fifth cell after 5 blank, the following array emerges:

–	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			
101		103				107		109	
		113						119	

This time the first number to bite the dust, having survived the previous two sievings, is $25 = 5^2 = 5 \times 5$. Now 7 is the first number appearing after 2, 3 and 5 in this latest array. Since it has survived all three previous sievings, it must be the next prime. Leaving every seventh cell after 7 blank gives the following array:

–	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							

30 primes < 120

Again note that the first new number deleted when skipping in sevens is 7^2, or 49. Now stop. Why? Because the next sieving, based on the prime 11, crosses out every eleventh number after 11. The first multiple of 11 which isn't already sieved is the eleventh; the lower multiples of 11 have already been deleted by those sievings based on one or other of the primes 2, 3, 5 and 7. Hence 121 (11^2) is the next natural number for the chop, so those thirty numbers less than 121 clearly visible in the last array are in no further danger. These survivors are the thirty primes less than 120. It took just four sievings to reveal them. (Do you now see why the first 120 numbers were chosen to demonstrate this remarkably simple algorithm? If not, check Appendix B, page 298.)

Although the sieve of Eratosthenes may look like a very laborious method, it is, in fact, a very fast procedure since, by contrast with the method of trial division, it does not make use of time-consuming divisions. It is a very nice programming exercise to get this working and fine-tuned. When you do get it going, it works like a charm and lists all the primes up to a given number in no time. It will fill the screen with the 1229 primes less than 10,000 before you have time to catch your breath. The fact that its output can be huge is something of a disadvantage, but I'm told that this simple principle is the basis of a very powerful modern method used in the constant quest for larger and larger primes.

I was to learn a lot about the difference between theory and practice during my first project in cryptography. I would come to appreciate that it wasn't good enough to know any old way of doing something—you have to find methods or techniques that implement the theory in highly efficient ways. This "real-life" aspect caught my interest. Great theory, but is it implementable? It's no use receiving a secret message scrambled in a highly secure way which says, "Evacuate immediately!" if it is going to take a day to work out what it is saying.

But there is some good news. The amazing thing is that there *are* other ways of figuring out if a number is prime, which work quite speedily on large numbers. But this is a story for later.

Is There an Infinite Number of Prime Numbers?

Although the ancients were able to find many primes with the sieve method, and today we actually know millions upon millions of primes, could they run out? This would mean that there is a largest prime number, after which all the remaining numbers stretching to infinity are composite. So is there only a finite number of primes, or is there an infinite number of them? I remember thinking how you would go about answering questions such as these. Do they necessarily have answers? I know that logically you can say that there is either an infinite number of primes or there isn't; it must be one or the other, but maybe it is not within our power to say which is the case. Subconsciously I wondered how people long since dead could have found answers to such questions.

Over two thousand years ago the Greek mathematician Euclid, who lived in Alexandria, Egypt, published in the sixth volume of his famous book on geometry a wonderfully simple proof that there is an infinite number of primes. You can find this proof in textbooks on number theory, but you can also find an excellent explanation of this beautiful result in Simon Singh's book *Fermat's Last Theorem*. (If you don't have a copy, you should get one because it's a great book.) Euclid's proof is an example of a "proof by contradiction." He begins by assuming that there is only a finite number of primes and then, by a simple but clever argument, shows that this assumption leads to a contradiction. Consequently there must be an infinite number of primes. It is a wonderful nonconstructive proof: it does not construct or exhibit an infinite set of primes explicitly, it just convinces you that there has to be an infinite number of them. It is an example of an "existence proof." It is similar to proving that there are at least two people in Dublin with the same number of hairs on their head, without actually producing two such people. You may know with certainty that they are out there somewhere, but please don't ask me to find them! (See Appendix B, page 298.)

Is There a Formula for Generating Prime Numbers?

Knowing that there is an infinite number of primes is different from knowing how to find any of them. Some gallant attempts have been made to find formulae that generate prime numbers only. Pierre Fermat (1601–1665), the great French mathematician renowned for his Last Theorem, mistakenly believed that each time a natural number n is substituted in the formula

$$F(n) = 2^{2^n} + 1$$

a prime is generated. Here $F(n)$ does not mean F multiplied by n, which would be written $F \times n$ or Fn. Read $F(n)$ as "the nth Fermat number." Then $F(1)$ is the first Fermat number, $F(2)$ is the second Fermat number, and so on. Fermat wasn't asserting that this formula would supply all the prime numbers, only that it would always produce a prime number each time a different natural number n is substituted into the formula. Of course, if he could have proved his assertion he would have had a proof different from Euclid's that there is an infinite number of primes.

Substituting 1 for n in the above formula gives

$$F(1) = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$$

So the first Fermat number, $F(1)$, is 5, which is a prime. The Fermat numbers obtained when 1, 2, 3 and 4 are substituted for n in turn in the above formula (note that 2^{2^3} means $2^{(2^3)}$ and not $(2^2)^3$) are

$$F(1) = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$$
$$F(2) = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$$
$$F(3) = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257$$
$$F(4) = 2^{2^4} + 1 = 2^{16} + 1 = 65{,}536 + 1 = 65{,}537$$