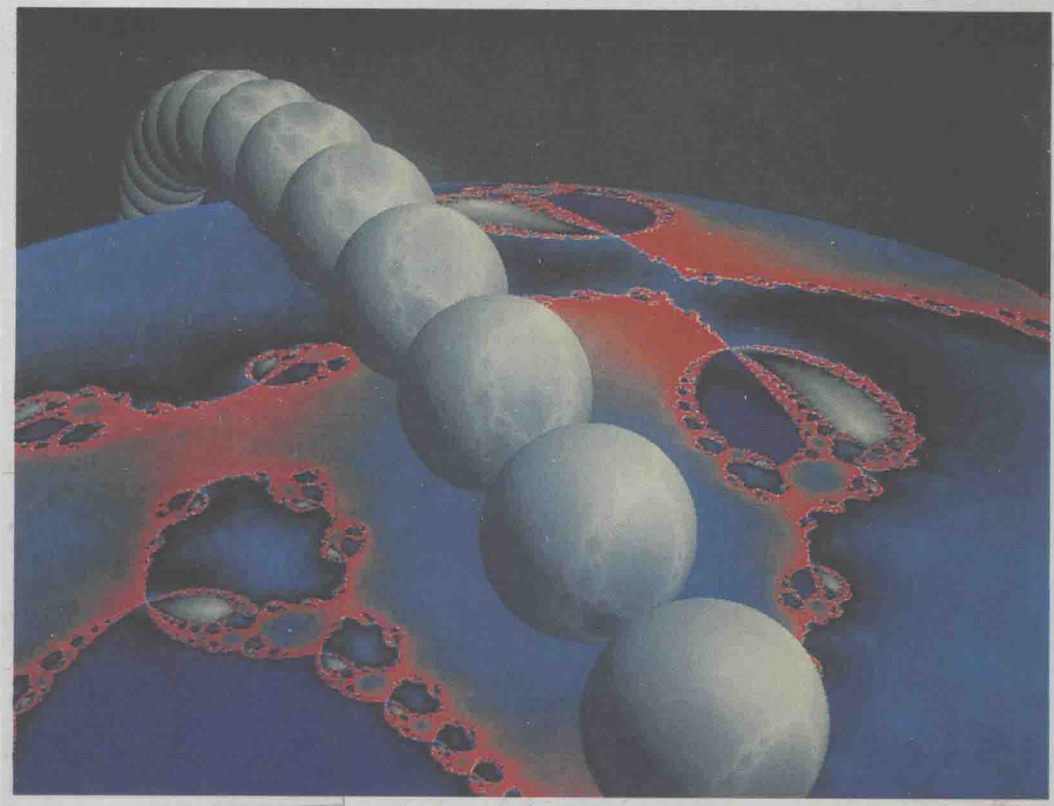
MATHEMATICS: THE NEW GOLDEN AGE



KEITH DEVLIN

Keith Devlin

Mathematics:

The New Golden Age

PENGUIN BOOKS

PENGUIN BOOKS

Published by the Penguin Group
27 Wrights Lane, London W8 5TZ, England
Viking Penguin Inc., 40 West 23rd Street, New York, New York 10010, USA
Penguin Books Australia Ltd, Ringwood, Victoria, Australia
Penguin Books Canada Ltd, 2801 John Street, Markham, Ontario, Canada L3R 1B4
Penguin Books (NZ) Ltd, 182–190 Wairau Road, Auckland 10, New Zealand

Penguin Books Ltd, Registered Offices: Harmondsworth, Middlesex, England

First published 1988
10 9 8 7 6 5 4 3

Typeset in 10/13pt Lasercomp Photina by
The Alden Press (London & Northampton) Ltd
Made and printed in Great Britain by
Richard Clay Ltd, Bungay, Suffolk

PELICAN BOOKS

MATHEMATICS: THE NEW GOLDEN AGE

Dr Keith Devlin has been a professional research mathematician since 1971, when he obtained his Ph.D. in mathematics from the University of Bristol. He has held positions at universities in England, Scotland, Norway, Germany, Canada and the USA. Since 1979 he has been Reader in Mathematics at the University of Lancaster in England. He has written some forty or so research articles and papers, and this is his ninth book on mathematics.

In addition to his research work, since 1983 he has written a regular column on mathematics for the *Guardian*, and has been involved in the production of a number of television programmes dealing with mathematical themes.

Preface

The New Golden Age of Mathematics. When was the old one? Was it the period of the Ancient Greek geometers around 300 BC? Or did it occur during the seventeenth century when Newton and Leibniz were developing the infinitesimal calculus and Fermat was doing his tremendous work on number theory? Or perhaps the mathematical career of Gauss alone (1777–1855) justifies the title of Golden Age. Or, still later, the period that saw the work of Riemann, Poincaré, Hilbert, and others – the mathematics produced between the mid 1800s and the start of the Second World War was truly prodigious.

As with any area of human endeavour, it is not possible to say which was the truly 'greatest period'. Each new generation builds upon the work of its predecessors. What can be said is that the present time is witnessing the undertaking of a phenomenal amount of mathematical research. The *International Directory of Mathematicians* lists some 25 500 professional mathematicians around the world, but this represents only a small fraction of the real total. If you include also the vast armies of 'amateur mathematicians' (some of whom have made some significant discoveries!) for whom mathematics is simply a pleasant pastime, then the true figure must be enormous. On grounds of numbers (admittedly shaky grounds, since quantity and quality are not at all closely related, especially in mathematics), we are in the middle of a new Golden Age right now. And since every book has to have a title, that is more or less what I have chosen to call this one.

What this book sets out to do is to try to convey to the interested layperson some of the most significant developments that have taken place in mathematics during recent times. To include every advance that could be called 'significant' would require several volumes, not one. So I have had to be selective – very selective. First of all I restricted myself to developments which have taken place in the twenty-five years from 1960 to 1985, with a bias towards the latter part of this period. Since the book is intended for the general reader, I included only topics which have merited attention in the world's press and which are capable of explanation at a suitable

level. And of course my own personal tastes and preferences played a role in my decisions.

For the most part, all that is required of you, the reader, is an interest in the subject that caused you to pick up the book in the first place, together with some degree of patience. (Understanding mathematics *takes time*, even at a superficial level.) There are, unavoidably, parts of the text where a reasonably good school mathematics education would enable you to get more from my account than would otherwise be possible, but I have tried to keep these to a minimum (and you can always skip over passages you find difficult, secure in the knowledge that it will soon get 'easier'). Though for the most part the chapters are quite independent of one another, they are ordered so that earlier ones might help in the appreciation of later ones.

Subject to all the above restrictions, plus the ever-present one of available space, I have tried to put across some of the richness and diversity of present-day mathematics. What you get is, I am afraid, just the tip of an iceberg. A book such as this is bound to fail in its aim; I only hope it does not fail too badly.

Keith Devlin
Lancaster, England
May 1986

Acknowledgements

Like all mathematicians nowadays, I can call myself an expert in just one tiny area of a vast and growing landscape. In attempting to provide a comprehensive coverage, then, I have had to rely on others to pick up the errors that inevitably arose in my first draft. So thanks are due to: Sir Michael Atiyah, Amanda Chetwynd, David Nelson, Stephen Power, Hermann te Riele, Morwen Thistlethwaite, and David Towers, each of whom read all or part of the manuscript and made helpful suggestions. Thanks too to Penguin Books who from the very start showed great enthusiasm for what must have seemed like the impossible task of trying to produce a 'popular' account of mankind's most impenetrable subject. All failures and errors are, of course, to be laid at my door.

K. D.

For permission to reproduce copyright material grateful acknowledgement is made to the publishers listed below.

Figures 8 and 17–23 are reproduced from *The Beauty of Fractals* (1986), by H. O. Peitgen and P. H. Richter, with the permission of Springer-Verlag.

Figures 9 and 10 are reproduced from *Fractals: Form, Chance and Dimension* (1977), by Benoit Mandelbrot, with the permission of W. H. Freeman and Co.

Figure 14 is reproduced from *Studies in Geometry* (1970), by L. M. Blumenthal and K. Menger, with the permission of W. H. Freeman and Co.

Figures 31 and 34 are reproduced from *Scientific American* with the permission of W. H. Freeman and Co.

Figure 57 is reproduced with the permission of Cordon Art BV.

Contents

1 Prime Numbers, Factoring, and Secret Codes

The Biggest Prime Number in the World

The biggest (known) prime number* in the world is a giant which requires 65 050 digits to write out in standard decimal format. Using exponential (or power) notation it has a more manageable form:

$$2^{216091} - 1.$$

That is, you get the number by multiplying 2 by itself 216 090 times and then subtracting 1 from the answer.

Exponential notation is deceptive. To try to obtain some idea of its power for representing large numbers, imagine taking an ordinary 8×8 chessboard and placing piles of counters 2 mm thick (the English 10p piece is a good example) on the squares according to the following rule. Number the squares from 1 to 64, as in Figure 1. On the first square place 2 counters. On square 2 place 4 counters. On square 3 place 8 counters. And so on, on each square placing exactly twice as many counters as on the previous one. Thus on square n you will have a pile of 2^n counters. In particular, on the last square you will have a pile of 2^{64} counters. How high do you think this pile will be? 1 metre? 100 metres? A kilometre? Surely not! Well, believe it or not, your pile of counters will stretch out beyond the Moon (a mere 400 000 kilometres away) and the Sun (150 million kilometres away) and

*See later for an explanation of this term.

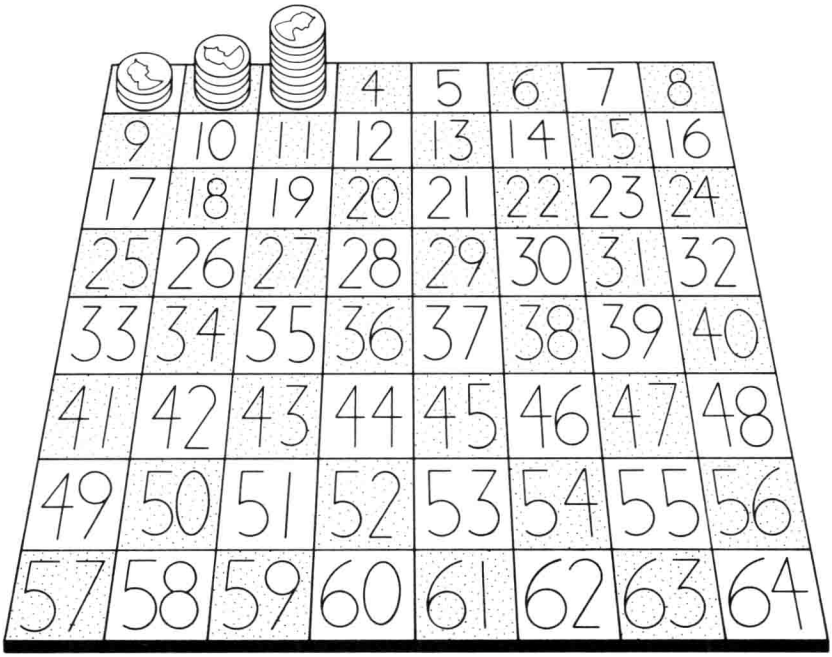


Figure 1. The astronomical chessboard number. By starting with two 2 mm thick coins on the first square and forming a pile twice as high on each successive square, the pile on the 64th square will stretch almost to the nearest star, Proxima Centauri, some 4 light years away.

will in fact reach almost to the nearest star, Proxima Centauri, some 4 light years from Earth. In decimal format the number 2^{64} is

18 446 744 073 709 551 616.

So much for 2^{64}. To obtain the number 2^{216091} which appears in the record prime expression you would need a chessboard with 216 091 squares – a board measuring 465 × 465 squares would do the trick!

Just how do you go about handling numbers of this size? For a start you use a computer. And not just any computer. The record prime mentioned above was discovered by using one of the most powerful computers in the world – a machine capable of performing two hundred billion* arithmetic

*Throughout this book 'billion' means a thousand million.

operations a second – and even then the calculation took over three hours. But computing power on its own is not enough; the skill of the mathematician is also required. How that skill was developed, and other uses to which it can be put, is the subject of the rest of this chapter.

Prime Numbers

'That action is best, which procures the greatest happiness for the greatest numbers', wrote Francis Hutcheson in 1725 (*Inquiry into the Original of our Ideas of Beauty and Virtue*, Treatise II, Section 3.8). It seems unlikely that he was thinking of *numbers* in the mathematical sense of greatest known primes and the like, but his statement nevertheless applies quite well to man's never-ending fascination with those most fundamental of mathematical objects – the *natural* (or *counting*) *numbers*, 1, 2, 3, ... These abstract mathematical objects are fundamental not only to our everyday life but to practically all of mathematics – so much so that the nineteenth-century mathematician Leopold Kronecker wrote (of mathematics): 'God created the natural numbers, and all the rest is the work of man.'

There are various properties which apply to natural numbers, splitting them into two classes (those with a property and those without). For instance, there is the property of being even. This splits the natural numbers into the class of those which *are* even (2, 4, 6, 8, ...) and those which are *not* (the odd numbers: 1, 3, 5, 7, ...). Or there is the property of being divisible by 3. (Here, as elsewhere in this book, when we say that one number *divides* another we mean that it does so exactly, leaving no remainder. Thus 3, 6, 9, 12 are all divisible by 3, whilst 1, 2, 4, 5, 7 are not.) The even–odd split is a natural and important one. (The split into those numbers divisible by 3 and those which are not is not so natural, nor of any great importance.) Another example of a natural and important split is given by the property of being a *perfect square*, like $1 = 1^2, 4 = 2^2, 9 = 3^2, 16, 25, 36, \ldots$. And there are many others. But by far the most important way of dividing up the natural numbers is into those which are *prime* and those which are not.

A natural number n is said to be a *prime number* if the only numbers which divide it are 1 and n itself. (The number 1 is a special case here, and it is conventional not to regard 1 as a prime number.)

Thus 2, 3, 5, 7, 11, 13, 17, 19 are all primes; 1, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 are not. (Numbers which are not prime are sometimes called *composite*.) For instance, 7 is prime because none of the numbers 2, 3, 4, 5, 6 divides it; 14 is not prime since both 2 and 7 divide it.

The main reason why the prime numbers are so important was already known to the Greek mathematician Euclid (*c.* 350–300 BC) who, in Book IX of his *Elements* (a thirteen-volume compilation of all the mathematical knowledge then available) proved what is nowadays known as the *fundamental theorem of arithmetic*: that every natural number greater than 1 is either prime, or else can be expressed as a product of primes in a way which is unique except for the order in which the primes are arranged.

For instance, the number 75 900 is a product of seven *prime factors* (two being *repeated factors*):

$$75\,900 = 2 \times 2 \times 3 \times 5 \times 5 \times 11 \times 23.$$

The expression on the right of the equals sign here is called the *prime factorization* of the number 75 900.

What the fundamental theorem of arithmetic tells us is that the prime numbers are the basic building blocks from which all the natural numbers are constructed. As such they are like the chemist's elements or the physicist's fundamental particles. Knowledge of the prime factorization of any number provides the mathematician with almost complete information about that number, as is dramatically illustrated later on in this chapter (see the section on secret codes). But for now, what about the prime numbers themselves?

The most basic question you can ask about prime numbers is how common they are. Is there, for instance, a biggest prime number, or do the primes go on for ever, getting larger and larger? At first glance they seem to be very common indeed. Of the first ten numbers beyond 1 (i.e. 2 to 11 inclusive), five are prime, namely 2, 3, 5, 7, 11, which is exactly half the collection. Of the next ten numbers, 12 to 21, there are three which are prime (13, 17, 19), a proportion of 0·3. Between 22 and 31 the proportion of primes is again 0·3, whilst for the next two groups of ten numbers the proportion falls to 0·2. So the primes seem to 'thin out' the further you go along the sequence of natural numbers. Table 1 shows how the number of primes less than n (denoted by $\pi(n)$) varies with n for selected values of n, and gives the 'density' figure $\pi(n)/n$ in each case.

So, the primes become rarer the higher up you go in the number sequence. But do they eventually peter out altogether? The answer is no.

n	$\pi(n)$	$\pi(n)/n$
1000	168	0·168
10000	1229	0·123
100000	9592	0·096
1000000	78498	0·078

Table 1. The distribution of primes, showing the number of primes $\pi(n)$ smaller than n for various values of n.

This was also demonstrated by Euclid, using an argument which to this day remains a superb model of elegant mathematical reasoning. To begin with, imagine the prime numbers listed in order of magnitude:

$$p_1, p_2, p_3, \ldots .$$

So $p_1 = 2, p_2 = 3, p_3 = 5$, and so on. The aim is to show that this list must continue for ever. To put it another way, it has to be demonstrated that if we are at any stage n in the list, having enumerated $p_1, p_2, \ldots, p_n$, then there has to be a further prime in the list beyond p_n. The trick is to look at the number

$$N = p_1 p_2 p_3 \ldots p_n + 1$$

obtained by multiplying together all the primes p_1, p_2, p_3 and so on up to p_n, and then adding 1 to the result. Obviously N is bigger than p_n, so if N happens to be prime then we know that there is a prime beyond p_n, which is what we are trying to prove. On the other hand, if N is not prime it must be divisible by some prime, call it p. But if you try to divide N by any of the primes $p_1, p_2, \ldots, p_n$ there will be a remainder of 1 (the same 1 that was added when we obtained N in the first place). So our p must be a different prime, and again we have proved what was required. So, in any event there will be a prime bigger than p_n, and we can conclude that the list of primes continues for ever.

Notice that we have no idea whether the number N in the above is prime or not. If you try a few examples you will discover that numbers of this form

often are prime. For instance,

$$\begin{aligned} N_1 &= 2 + 1 = 3, \\ N_2 &= 2 \times 3 + 1 = 7, \\ N_3 &= 2 \times 3 \times 5 + 1 = 31, \\ N_4 &= 2 \times 3 \times 5 \times 7 + 1 = 211, \\ N_5 &= 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311, \end{aligned}$$

are all primes. But the next three are not:

$$\begin{aligned} N_6 &= 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 \\ &= 30031 = 59 \times 509, \\ N_7 &= 19 \times 97 \times 277, \\ N_8 &= 347 \times 27953. \end{aligned}$$

In fact, no one knows whether infinitely many numbers of the form

$$N_n = p_1 p_2 \cdots p_n + 1$$

are prime, nor indeed whether infinitely many of these numbers are composite (though at least one of these two possibilities has to be true, of course). This is just one of dozens of easily stated questions about prime numbers whose answer is not known.

One of the most famous unanswered questions about prime numbers is *Goldbach's conjecture*. In a letter to Leonhard Euler written in 1742, Christian Goldbach conjectured that every even number greater than 2 is a sum of two primes. For instance,

$$\begin{aligned} 4 &= 2 + 2, \\ 6 &= 3 + 3, \\ 8 &= 3 + 5, \\ 10 &= 5 + 5, \\ 12 &= 5 + 7. \end{aligned}$$

Computer searches have verified Goldbach's conjecture for all even numbers up to 100 000 000, but to this day the conjecture has not been settled properly one way or the other.

Primality Testing

Though most of the classical problems concerning prime numbers have remained unsolved, the last few years have seen tremendous developments in methods by which numbers may be tested to see if they are prime or not. 'Methods for testing primality?' you cry. 'But surely it is obvious how to go about it?' And indeed, there is a perfectly natural, straightforward way of seeing if a number is prime or not. Given your number, n say, you first see if 2 divides it. If it does, then n is not prime and that is the end of the matter. Then you try 3. If 3 divides n, then n is not prime and again you are finished. Then try to divide n by 5. (You can skip past 4: since 2 does not divide n if you have got this far, 4 cannot divide n either.) If 5 fails to divide n, you try 7. (Again, you can skip past 6 since 2 and 3 do not divide n.) And so on. If you get as far as $\sqrt{n}$ without finding a number which divides n, then you know that n must be prime. (Because if n were not prime it would be a product of two numbers u and v between 1 and n, and either u or v will be no greater than $\sqrt{n}$, of course.)

The above process is known as *trial division*. Though it works well enough for moderately small numbers, it becomes unwieldy if the numbers are too large. To see just how impractical it becomes, suppose you were to write a highly efficient program to run trial division on the fastest computer available (alluded to at the start of this chapter). For a number of 10 digits the program would appear to run instantaneously – the answer would flash up immediately. For a 20-digit number it has a bit of a struggle and would take two hours. For a 50-digit number it would require a staggering ten billion years. A 100-digit number would require this many years:

1 000 000 000 000 000 000 000 000 000 000 000 000

(there are thirty-six zeros here). This is not just a trivial calculation of a very large number. As will be explained later in this chapter, primes with between 60 and 100 digits are required for one of the most secure forms of secret coding system in use today.

So just how do you go about deciding whether a 100-digit number is prime? The best method available at the moment is a highly sophisticated technique developed around 1980 by the mathematicians Adleman, Rumely, Cohen, and Lenstra, and often referred to by their initials as the ARCL test. When implemented on the same type of computer as mentioned above, the running times for the ARCL test are, for a 20-digit number, 10 seconds; for a 50-digit number, 15 seconds; for a 100-digit number, 40 seconds. The computer will even handle a 1000-digit number if you give it a week to work on the problem.

How does the test work? Well, it depends on a considerable amount of highly sophisticated mathematics – mathematics way beyond a typical undergraduate degree course – so it is not possible to give a complete answer here. But it is not hard to explain the central idea behind the method. This is a simple (though very clever) piece of mathematics due to the great French mathematician Pierre de Fermat (1601–65).

Though only an 'amateur' mathematician (he was a jurist by profession), Fermat produced some of the cleverest results mathematics has ever seen, even to this day. One of his observations was that if p is a prime number, then for any number a less than p, the number $a^{p-1} - 1$ is divisible by p. For instance, suppose we take $p = 7$ and $a = 2$. Then

$$a^{p-1} - 1 = 2^6 - 1 = 64 - 1 = 63,$$

and indeed 63 is divisible by 7. Try it yourself for any values of p (prime) and a (less than p). The result is always the same.

So here is a possible way of testing if a number n is prime or not. Compute the number $2^{n-1} - 1$. See if n divides it. If it does not, then n cannot be prime. (Because if n *were* prime, then by Fermat's observation you *would* have divisibility of $2^{n-1} - 1$ by n.) But what can you conclude if you find that n does divide $2^{n-1} - 1$? Not, unfortunately, that n has to be prime. (Though this is quite likely to be the case.) The trouble is, whilst Fermat's result tells us that n divides $2^{n-1} - 1$ whenever n is prime, it does not say that there are no composite numbers with the same property. (It is like saying that all motor cars have wheels; this does not prevent other things having wheels – bicycles, for instance.) And in fact there are non-primes which do have the Fermat property. The smallest one is 341, which is not prime since it is the product of 11 and 31. But if you were to check (on a computer) you would find that 341 does divide $2^{340} - 1$. (We shall see in a moment that there is no need to calculate 2^{340} in making this check.) Composite numbers which behave like primes as far as the Fermat property

is concerned are called *pseudoprimes*. So if, when you test for primality using the Fermat result, you discover that n does divide $2^{n-1} - 1$, then all you can conclude is that either n is prime or else it is pseudoprime. (In this case the odds are heavily in favour of n actually being prime. For though there are in fact an infinity of pseudoprimes, they occur much less frequently than the real primes. For instance there are only two such numbers less than 1000, and only 245 below one million.)

Incidentally, it makes little difference if instead of 2 you use some other number, say 3 or 5, in testing the Fermat property. Whichever number you use there will be pseudoprimes to prevent you obtaining an absolute answer to your primality problem.

In using the above test, it is not necessary to calculate the number 2^{n-1}, a number which we have already observed to be very large for even quite modest values of n. All you need to do is find out whether or not n divides $2^{n-1} - 1$. This means that multiples of n may be ignored *at any stage of the calculation*. To put it another way, what has to be calculated is the remainder that *would* be left *if* $2^{n-1} - 1$ *were* divided by n. The aim is to see if this remainder is zero or not, but since multiples of n will obviously not affect the remainder, they may be ignored. Mathematicians (and computer programmers) have a standard way of denoting remainders: the remainder left when A is divided by B is written as

$$A \bmod B.$$

Thus, for example, $5 \bmod 2$ is 1, $7 \bmod 4$ is 3, and $8 \bmod 4 = 0$.

As an example of the Fermat test, let us apply it to test the number 61 for primality. We need to calculate the number

$$(2^{60} - 1) \bmod 61.$$

If this is not zero, then 61 is not a prime. If it is zero, then 61 is either a prime or a pseudoprime (and in fact is a genuine prime, as we know already). We shall try to avoid calculating the large number 2^{60}. We start with the observation that $2^6 = 64$, and hence $2^6 \bmod 61 = 3$. Then, since $2^{30} = (2^6)^5$, we get

$$\begin{aligned} 2^{30} \bmod 61 &= (2^6 \bmod 61)^5 \bmod 61 = 3^5 \bmod 61 \\ &= 243 \bmod 61 = 60. \end{aligned}$$

So,