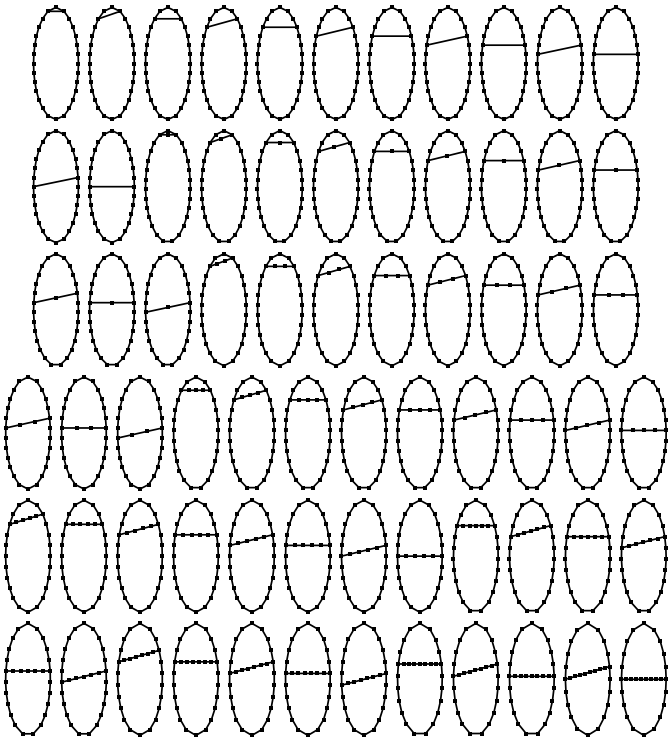
*

ISSN 1350-8539

M500

M500 275



The M500 Society and Officers

The M500 Society is a mathematical society for students, staff and friends of the Open University. By publishing M500 and by organizing residential weekends, the Society aims to promote a better understanding of mathematics, its applications and its teaching. Web address: m500.org.uk.

The magazine M500 is published by the M500 Society six times a year. It provides a forum for its readers' mathematical interests. Neither the editors nor the Open University necessarily agree with the contents.

The Revision Weekend is a residential Friday to Sunday event providing revision and examination preparation for both undergraduate and postgraduate students. For details, please go to the Society's web site.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details, please go to the Society's web site.

Advice to authors We welcome contributions to M500 on virtually anything related to mathematics and at any level from trivia to serious research. Please send material for publication to the Editor, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation. For more information, go to m500.org.uk/magazine/ from where a LaTeX template may be downloaded.

Gematria and isopsephy

Chris Pile

I enjoy the variety of articles and problems in M500 but now prefer the more 'recreational' topics rather than the serious mathematics! I can remember when our founding editor Marion Stubbs would often appeal for more 'rubbish'.[1]

I learnt recently that my next-door neighbour was studying 'ISOPSEPHY' and 'GEMATRIA'. Ancient Greek arithmetic was performed using letters as symbols for numbers; consequently words and phrases had numerical values obtained by adding the letters. Particular significance was given to words or phrases that had the same value and could be interchanged as a form of code. This is used by researchers into early biblical texts to gain greater insight into the Gospels. My neighbour was studying the Gospel of St John, Chapter 21, verses 1–14, concerning the significance of the 153 fish. The passage contains 276 words, and both 153 and 276 are triangular numbers (17th and 23rd). The product, $17 \times 23 = 391$, which is the value of the letters in 'Jesus' and also interchangeably with the phrase 'the lamb of God'. There are many other similar numerical identities in theological analysis of this type.

An article[2] in the April 2016 issue of the IMA publication *Mathematics Today* describes the inscription in Greek, dating from the 2nd century, on a stone found at Pergamon in Western Turkey. The inscription concerns the geometry of the sphere and cylinder, and consists of 41 lines of Greek text. If the Greek letters are replaced by their numerical values, almost every line adds up to the same total. The numbers associated with the Greek and Hebrew letters can be found on the Web.

All of the above led me to consider what value could be attributed to words using numbers 1–26 for the letters of the alphabet, A–Z. The principle here is to select examples which are interesting and ignore those that are not! For example, ODD $= 15 + 4 + 4 = 23$, which is odd, and EVEN $= 5 + 22 + 5 + 14 = 46$, which is equivalent to ODD + ODD and the therefore even!

PRIME = 61, which is reassuringly prime, COMPOSITE = 115, which is 5×23, SQUARE = 81, obviously square, and TRIANGLES = 105 are triangular! TRIANGLE = 86, which, arguably, could be interchanged with

[1] RUBBISH is the technical term for off-topic material appearing in this magazine.

[2] Richard Simpson, Historical Notes: A Mathematical Inscription from Ancient Pergamon.

PYRAMID = 86.

CIRCLE = 50, a nice round number, as is OVAL = 50. DICE = 21, which is the number of spots. And so on!! Self-defining examples are not easy to find. Here are a few.

TWO HUNDRED AND FIFTY ONE	=	251
FOURTEEN DOZEN	=	168
SIX TIMES FORTY THREE	=	258
TWO HUNDRED AND FIFTY NINE	=	259
FOUR TIMES SIXTY EIGHT	=	272
SEVEN TIMES THIRTY NINE	=	273
FOUR TIMES SEVENTY THREE	=	292
FOUR TIMES SEVENTY FOUR	=	296

This is obviously an open-ended amusement; however, I can conclude that

NUMBER ADDING = MATHEMATICS

(73 + 39 = 112) but

ADDING UP LETTERS = IS TOTAL RUBBISH

(39 + 37 + 99 = 28 + 68 + 79 = 175).

Problem 275.1 – Numbers to words to numbers

Tony Forbes

I've had this in my 'to do' file for some time. Chris Pile's contribution (pages 1–2) gives me a good excuse to use it.

The *word value* of a character string is the sum of its letters, assuming A = 1, B = 2, ..., Z = 26. Show that 251 and 259 are the only numbers that match the word values of their standard English expressions, or find another one.

If we allow simple divisions, as in SOMETHING OVER SOMETHING ELSE, we see that we can do much better. Are there infinitely many? It seems likely, as is suggested by the following.

ONE THOUSAND SIX HUNDRED AND THIRTY EIGHT OVER THREE	=	546
ONE THOUSAND NINE HUNDRED AND TWELVE OVER FOUR	=	478
TWO THOUSAND FIVE HUNDRED AND TWENTY OVER FIVE	=	504
THREE THOUSAND ONE HUNDRED AND NINETY EIGHT OVER SIX	=	533
THREE THOUSAND AND EIGHTY SEVEN OVER SEVEN	=	441
THREE THOUSAND NINE HUNDRED AND TWELVE OVER EIGHT	=	489
FOUR THOUSAND THREE HUNDRED AND FIFTY TWO OVER EIGHT	=	544
FOUR THOUSAND SIX HUNDRED AND SEVENTY TWO OVER EIGHT	=	584
THREE THOUSAND EIGHT HUNDRED OVER TEN	=	380
FOUR THOUSAND AND FOUR OVER ELEVEN	=	364
SIX THOUSAND THREE HUNDRED AND TWENTY FIVE OVER ELEVEN	=	575

EIGHT THOUSAND FIVE HUNDRED AND TWENTY SIX OVER FOURTEEN = 609
NINE THOUSAND ONE HUNDRED AND SIXTY EIGHT OVER SIXTEEN = 573
ELEVEN THOUSAND SIX HUNDRED AND TWENTY EIGHT OVER NINETEEN = 612
TEN THOUSAND ONE HUNDRED AND EIGHTY OVER TWENTY = 509
TEN THOUSAND FIVE HUNDRED AND FORTY OVER TWENTY = 527
FOURTEEN THOUSAND ONE HUNDRED AND NINETY OVER TWENTY TWO = 645
SEVENTEEN THOUSAND TWO HUNDRED AND SEVENTY THREE OVER TWENTY THREE = 751
FIFTEEN THOUSAND THREE HUNDRED AND SIXTY OVER TWENTY FOUR = 640
FIFTEEN THOUSAND SEVEN HUNDRED AND FOUR OVER TWENTY SIX = 604
TWENTY ONE THOUSAND TWO HUNDRED AND SEVENTY SIX OVER TWENTY SEVEN = 788
SIXTEEN THOUSAND AND NINETY FIVE OVER TWENTY NINE = 555
SEVENTEEN THOUSAND EIGHT HUNDRED AND SIX OVER TWENTY NINE = 614
NINETEEN THOUSAND SEVEN HUNDRED AND FORTY NINE OVER TWENTY NINE = 681
NINETEEN THOUSAND EIGHT HUNDRED AND NINETY FOUR OVER TWENTY NINE = 686
TWENTY ONE THOUSAND FOUR HUNDRED AND THIRTY ONE OVER TWENTY NINE = 739
TWENTY TWO THOUSAND TWO HUNDRED AND FORTY THREE OVER TWENTY NINE = 767
NINETEEN THOUSAND SEVEN HUNDRED AND SIXTEEN OVER THIRTY ONE = 636
TWENTY THOUSAND NINE HUNDRED AND EIGHTY SEVEN OVER THIRTY ONE = 677
TWENTY TWO THOUSAND SEVEN HUNDRED AND EIGHTY FIVE OVER THIRTY ONE = 735
TWENTY FOUR THOUSAND FIVE HUNDRED AND FIFTY TWO OVER THIRTY THREE = 744
TWENTY FOUR THOUSAND EIGHT HUNDRED AND FORTY NINE OVER THIRTY THREE = 753
TWENTY FIVE THOUSAND FIVE HUNDRED AND SIXTY EIGHT OVER THIRTY FOUR = 752
TWENTY FIVE THOUSAND ONE HUNDRED AND SIXTY FIVE OVER THIRTY FIVE = 719
TWENTY EIGHT THOUSAND FIVE HUNDRED AND THIRTY EIGHT OVER THIRTY EIGHT = 751
TWENTY SEVEN THOUSAND SIX HUNDRED AND TWELVE OVER THIRTY NINE = 708
TWENTY NINE THOUSAND ONE HUNDRED AND SEVENTY TWO OVER THIRTY NINE = 748
FOURTEEN THOUSAND OVER FORTY = 350
TWENTY FIVE THOUSAND FIVE HUNDRED AND TWO OVER FORTY ONE = 622
TWENTY SIX THOUSAND SIX HUNDRED AND FIFTY OVER FORTY ONE = 650

Just to drive home the point let us finish with an absurd example:

FIFTEEN DUOVIGINTILLION EIGHT HUNDRED AND TWENTY FOUR UNVIGINTILLION EIGHT HUNDRED AND EIGHTY EIGHT VIGINTILLION EIGHT HUNDRED AND EIGHTY EIGHT NOVEMDECILLION EIGHT HUNDRED AND EIGHTY EIGHT OCTODECILLION EIGHT HUNDRED AND EIGHTY EIGHT SEPTENDECILLION EIGHT HUNDRED AND EIGHTY EIGHT SEXDECILLION EIGHT HUNDRED AND EIGHTY EIGHT QUINDECILLION EIGHT HUNDRED AND EIGHTY EIGHT QUATTUORDECILLION EIGHT HUNDRED AND EIGHTY EIGHT TREDECILLION EIGHT HUNDRED AND EIGHTY EIGHT DUODECILLION EIGHT HUNDRED AND EIGHTY EIGHT UNDECILLION EIGHT HUNDRED AND EIGHTY EIGHT DECILLION EIGHT HUNDRED AND EIGHTY EIGHT NONILLION EIGHT HUNDRED AND EIGHTY EIGHT OCTILLION EIGHT HUNDRED AND EIGHTY EIGHT SEPTILLION EIGHT HUNDRED AND EIGHTY EIGHT SEXTILLION EIGHT HUNDRED AND EIGHTY EIGHT QUINTILLION EIGHT HUNDRED AND EIGHTY EIGHT QUADRILLION EIGHT HUNDRED AND EIGHTY EIGHT TRILLION EIGHT HUNDRED AND EIGHTY EIGHT BILLION EIGHT HUNDRED AND EIGHTY EIGHT MILLION EIGHT HUNDRED AND SEVENTY THREE THOUSAND AND SIXTY FOUR OVER EIGHT HUNDRED AND EIGHTY EIGHT VIGINTILLION EIGHT HUNDRED AND EIGHTY EIGHT NOVEMDECILLION EIGHT HUNDRED AND EIGHTY EIGHT OCTODECILLION EIGHT HUNDRED AND EIGHTY EIGHT SEPTENDECILLION EIGHT HUNDRED AND EIGHTY EIGHT SEXDECILLION EIGHT HUNDRED AND EIGHTY EIGHT QUINDECILLION EIGHT HUNDRED AND EIGHTY EIGHT QUATTUORDECILLION EIGHT HUNDRED AND EIGHTY EIGHT TREDECILLION EIGHT HUNDRED AND EIGHTY EIGHT DUODECILLION EIGHT HUNDRED AND EIGHTY EIGHT UNDECILLION EIGHT HUNDRED AND EIGHTY EIGHT DECILLION EIGHT HUNDRED AND EIGHTY EIGHT NONILLION EIGHT HUNDRED AND EIGHTY EIGHT OCTILLION EIGHT HUNDRED AND EIGHTY EIGHT SEPTILLION EIGHT HUNDRED AND EIGHTY EIGHT SEXTILLION EIGHT HUNDRED AND EIGHTY EIGHT QUINTILLION EIGHT HUNDRED AND EIGHTY EIGHT QUADRILLION EIGHT HUNDRED AND EIGHTY EIGHT TRILLION EIGHT HUNDRED AND EIGHTY EIGHT BILLION EIGHT HUNDRED AND EIGHTY EIGHT MILLION EIGHT HUNDRED AND EIGHTY EIGHT THOUSAND EIGHT HUNDRED AND EIGHTY EIGHT

$$= \frac{1582488888888888888888888888888888888888888888888888888888888888888888873064}{888888888888888888888888888888888888888888888888888888888888888888888888} = 17803$$

and you can verify that the word value of the expression is indeed 17803. I hope my spelling is correct.

Letters

Cattle

Dear Tony,

I admire your fortitude and your amazing computational capability in solving the problem of Archimedes' Cattle. This problem appeared in M500 some 37 years ago.

M500 **63**, p. 2 Howard Parsons, letter.
M500 **65**, p. 3 Eddie Kent, Archimedes' Cattle.
M500 **67**, p. 17 Verse form of the problem.
M500 **58**, p. 11 Steve Murphy, Pell's equation.
M500 **60**, p. 6 Steve Murphy, Continued fractions and Pell's equation.

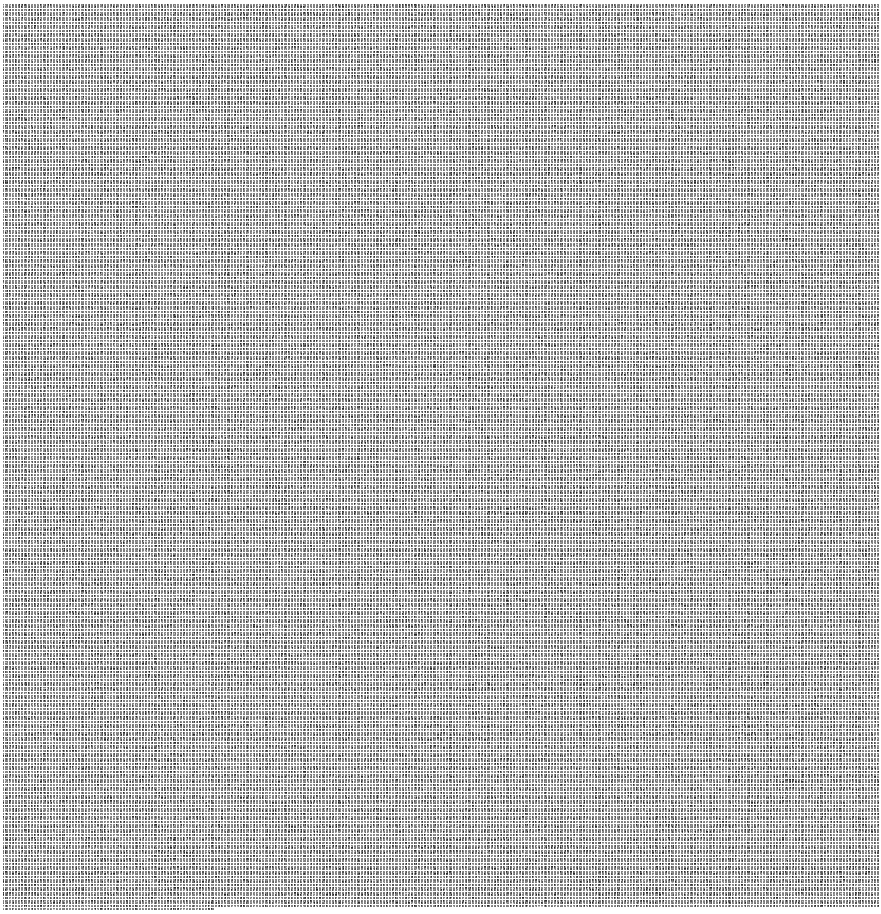
In M500 **65** we were advised not to attempt a solution! I did not have a computer in 1979, but about 20 years ago I wrote a simple QBASIC program (28 lines) based on the method described by John Reade in M500 **60** for the continued fraction for $\sqrt{X}$. I entered $X = 4729494$ and the (palindromic) result given in your article on page 13 of M500 **273** appeared after 75 seconds—much to my surprise! However, my ancient computer baulked at finding the convergent (and any number greater than 15 digits!). Each of your solutions would occupy about 100 pages of M500!

You are adept at dealing with enormous numbers in your quest for ever larger primes. It would be interesting (to me) to know how the calculation was done and how long it took to evaluate the numbers on page 14. I can only offer a facetious comment. Archimedes would have known (see his *The Sand Reckoner*) that the universe was too small to arrange this number of 'Cattle of the Sun' in planar square or triangular formation (with perchance of a wayward cow jumping over the moon—hey diddle diddle!). With *our* known extent of the universe with remote galaxies receding at the speed of light at a distance of around 10^{23} miles it would be very difficult to cram even 10^{80} cattle into the observable universe!

Best wishes for 2017,

Chris Pile

Tony Forbes writes — It really is amazing what one can do with MATHEMATICA running on a modern machine. After setting up the program and starting it I can safely hold my breath while waiting for the computer to perform all of the calculations described in M500 **273**, pp. 12–14, and then display *in full* the numbers that appear on page 14. Also I am impressed with LaTeX's capabilities. You obviously want to see the total number of cattle in Archimedes' problem. So, 37 years after it was first mentioned in M500, here it is, 344 lines of 600 digits plus one of 145. I fear it might be undecipherable in the paper magazine due to loss of resolution by the printing process but you should have no trouble with the PDF version.



Night

Dear Tony,

Re the item at the bottom of page 19 of M500 **273**, am I right to argue that if n = night, then $n^{n^n} = n^3$ follows from $n^n = 3$, which I solved numerically to give $n = 1.825$? This is in addition to the 'trivial' solutions: $n = 1$ as well as $n = 0$ since $0^0 = 1$ and $0^{\text{something greater than 0}} = 0$.

I'm not sure what the units of night are but as today [21 December 2016] is the winter solstice I guess they are larger than usual.

Bruce Roth

Factorization using the number field sieve – I

Roger Thompson

1 Introduction

The number field sieve is the fastest method currently available for factorizing numbers greater than 110 digits or so. While the basic aims of the method are straightforward, the technicalities, both theoretical and practical, involved in actually carrying it out are formidable. The papers in Lenstra and Lenstra (1993) provide an interesting insight into the struggle to conceive a practical algorithm, but make no concessions to readers without an extensive knowledge of algebraic number theory. In this article, I have attempted an explanation for a wider readership, though inevitably this means some aspects have to be taken on trust.

Factorization of M is achieved by finding $0 < x, y < M$, $\gcd(x, y) = 1$, such that $x^2 \equiv y^2 \bmod M$. Then

$$(x+y)(x-y) \equiv 0 \mod M, \quad x+y = ap, \quad x-y = bq,$$

with $pq = M$, so that

$$\gcd(x+y, M) = p, \quad \gcd(x-y, M) = q.$$

The aim is to build up a collection of candidates which can be grouped together to give us $x^2 \equiv y^2 \bmod M$. The left-hand side (x^2) is obtained by finding sets of candidate numbers $a + bm$ which are products of powers of small primes (in this case, we use every small prime less than some chosen value), where m is a particular integer to be defined in a moment, $0 < b \leq$ some maximum u, and $-u \leq a \leq u$. The right-hand side (y^2) is obtained by looking for analogous sets $a + bX$ operating on a particular polynomial in X. In this case, not every small prime is usable, for reasons that will be explained later.

A candidate which is the product of even powers of such primes is a square, so can be used immediately. However, sufficient individual candidates with some odd powers can be combined to make a square using Gaussian elimination (See Appendix A [to appear in M500 **276**]).

2 A simple example

The example is presented in terms of what is done, without any explanation as to why we're doing it, or in some cases how it is done. Subsequent sections then attempt an explanation, together with the techniques involved. A polynomial $f(x)$ can be constructed by taking the integral part of the dth

root of M, where d is odd, and calculating M to this base; f is suitable if it is irreducible (for otherwise it can be factorized into polynomials of smaller degree), and monic, i.e. the coefficient of $x^d = 1$. For our example, we will factorize 77827, and use its cube root to generate our polynomial. From now on, we will use f to represent appropriate polynomials in general, and ξ to represent our example polynomial. The integral part of $\sqrt[3]{77827} = 42$, and $77827 = 42^3 + 2 \times 42^2 + 5 \times 42 + 1$, so our polynomial ξ is $x^3 + 2x^2 + 5x + 1$, which is monic and irreducible. The m that we want is a value of x that makes $f \equiv 0 \bmod M$, i.e. 42 for ξ, so we want sets of numbers of the form $a + 42b$.

Algebra is conducted as normal, with $\bmod f$ used to indicate the remainder when some polynomial is divided by f. This is equivalent to evaluating polynomials with x set to one of the roots of $f = 0$. We will use X to indicate one of those roots, but also more importantly to allow polynomials to be treated as algebraic entities. In other words, $X^3 + 2X^2 + 5X + 1 \equiv 0 \bmod \xi$, so for example

$$\begin{aligned}(165X^2 + 784X + 224)^2 \\ &= (27225X + 204270)\xi + 143911X^2 - 697343X - 154094 \\ &\equiv 143911X^2 - 697343X - 154094 \mod \xi.\end{aligned}$$

We now need to find suitable a, b for $a + bX$.

Again without explanation, numbers of the form $(-b)^d f(-a/b)$ which are the product of small primes provide suitable a, b values, where d is the degree of the polynomial f. In our case, the numbers we need are of the form $a^3 - 2a^2b + 5ab^2 - b^3$. We also stipulate that $\gcd(a, b) = 1$ to eliminate what are essentially duplicates.

We now use a sieve to find examples of a and b that hold simultaneously for the numeric half and the algebraic half. These are then combined together to form squares. We shall leave details of the sieve until later.

Although it is necessary to get the powers of the primes all even in the algebraic half, this may not be sufficient. Also, the operations of building up products and taking square roots in the algebraic half are particularly complex. This initial example has been contrived so that none of this arises, so that the basics of the method can be demonstrated.

The example uses primes p up to 19 for the left-hand (numeric) side. We will call these primes the **arithmetic factor base**. For the right-hand (algebraic) side, we only pick primes that have integer roots for $f \equiv 0 \bmod p$ (standard texts explain how to do this simply). The bold entries in the

following table show such primes ≤ 47.

p	Roots	p	Roots	p	Roots
2	None	**13**	4	**31**	12, 24
3	1, 2	**17**	13	**37**	21
5	None	19	None	41	None
7	None	**23**	20	**43**	20
11	6	**29**	6	**47**	15, 38, 39

We will call the set

$$\{3, 11, 13, 17, 23, 29, 31, 37, 43, 47\}$$

the **algebraic factor base**. The tables below show some values of a, b for which $a + bm$ is the product of powers of primes in the arithmetic factor base, and simultaneously has $a^3 - 2a^2b + 5ab^2 - b^3$ as the product of primes in the algebraic factor base, with the idea of using Gaussian elimination to combine these to give squares on both sides. Since either side may be positive or negative, we need to treat the sign of each side as a separate factor, with parity 0 for positive values, and 1 for negative values. To save space, only primes with non-zero powers for at least one of the a, b entries are shown.

Arithmetic side

a	b	$a + 42b$	Powers				
			sign	2	3	5	19
38	1	$80 = 2^4 5^1$	0	4	0	1	0
25	8	$361 = 19^2$	0	0	0	0	2
3	16	$675 = 3^3 5^2$	0	0	3	2	0
-3	29	$1215 = 3^5 5^1$	0	0	5	1	0

Algebraic side

a	b	$a^3 - 2a^2b + 5ab^2 - b^3$	Powers					
			sign	3	11	17	31	47
38	1	$52173 = 3^2 11^1 17^1 31^1$	0	2	1	1	1	0
25	8	$13113 = 3^2 31^1 47^1$	0	2	0	0	1	1
3	16	$-517 = -11^1 47^1$	1	0	1	0	0	1
-3	29	$-37553 = -17^1 47^2$	1	0	0	1	0	2

The four entries multiply together to give us even powers on both sides. On the left-hand side, we therefore have $x^2 = 2^4 3^8 5^4 19^2$, giving $x = 153900$. Each entry on the right-hand side is taken as $a + bX$; so our product is

$$(X+38)(8X+25)(16X+3)(29X-3) \equiv 143911X^2 - 697343X - 154094 \bmod \xi.$$

This has the square roots $\pm(165X^2 + 784X + 224)$, as we saw above. Calculating square roots mod f is something we will return to later.

The final operation is to map the square root back to an integer y. Without explanation, this is done by evaluating the square root with $X = m$. Recalling that $m = 42$, this gives

$$y \;=\; \pm\,(165 \times 42^2 + 784 \times 42 + 224) \;=\; \pm\,324212.$$

We now calculate

$$\gcd(x - y, M) \;=\; \gcd(153900 - 324212, 77827) \;=\; 349,$$

so $77827 = 223 \times 349$.

Now that we have an example that works, we will explain what we've actually been doing. It is often a very successful tactic for solving problems to map them into another form, solve them there, then map the answers back. The maps concerned are $\sum_i a_i m^i \leftrightarrow \sum_i a_i X^i$, and $f(m) = M \leftrightarrow f(X) = 0$.

The crucial point about these mappings is that the operations of addition and multiplication are preserved throughout. In other words, for any operation in integers that involves addition or multiplication mod M, there is an equivalent that we can do in the algebra we have set up, which we can map back at the end. You might well ask what benefit we've gained from it. The answer to this is that, although the mapping preserves integers mod M, it doesn't necessarily preserve the integers themselves.

Since what we are trying to achieve is to find x and y such that $x^2 \equiv y^2 \bmod M$, we hope to be able to use the mapping to generate different y for the same x.

We now need to look more closely at the properties of polynomials mod f in more detail, continuing to use $\xi = X^3 + 2X^2 + 5X + 1$ as an example.

3 The norm of a polynomial mod f

Let g be a polynomial of degree at most d with integer coefficients, i.e. $g(X) = \sum_{i=0}^{d} G_i X^i$. Then if $f(X) = \prod_{j=1}^{d}(X - \alpha_j)$, where the α_j are the roots of f, we define the **norm** (sometimes called the field norm) of g, denoted by $N(g) = \prod_{j=1}^{d} g(\alpha_j)$. In particular, if $g(X) = a + bX$, then

$$\begin{aligned} N(g) \;&=\; (a + b\alpha_1)(a + b\alpha_2)\ldots(a + b\alpha_d) \\ &=\; (-b)^d(-a/b - \alpha_1)(-a/b - \alpha_2)\ldots(-a/b - \alpha_d) \;=\; (-b)^d f(-a/b). \end{aligned}$$

We can see immediately that norms are multiplicative, since

$$N(gh) \;=\; \prod_{j=1}^{d} gh(\alpha_j) \;=\; \prod_{j=1}^{d} g(\alpha_j)h(\alpha_j) \;=\; N(g)N(h).$$

Slightly less obviously, norms are integers. This is because the integer coefficient of X^n $(0 \le n \le d)$ in f is of the form $\sum_{i<j<\cdots<d,\ d-n \text{ suffixes}} \alpha_i\alpha_j\ldots$.

Far less obviously, there is an alternative way of calculating norms which doesn't involve roots. We construct the $d \times d$ matrix $A(g,f)$ such that $A_{ij}(g,f)$ is the coefficient of X^{i-1} in $X^{j-1}g(X) \bmod f$. Then

$$N(g) \;=\; \det(A(g,f))$$

(proof in Ash (2003)). For example, using

$$f \;=\; X^3 + PX^2 + QX + R, \quad \text{and} \quad g \;=\; aX^2 + bX + c,$$

$$A(g,f) \;=\; \begin{pmatrix} c & -aR & (aP-b)R \\ b & c-aQ & (aP-b)Q - aR \\ a & b-aP & (aP-b)P - aQ + c \end{pmatrix}.$$

Using

$$f \;=\; \xi \;=\; X^3 + 2X^2 + 5X + 1,$$

with $g = 3X^2 + X + 5$ we get $\det(A(g,f)) = 477$, with $g = 4X - 1$ we get $\det(A(g,f)) = -153$, and with

$$-23X^2 - 41X - 17 \;\equiv\; (3X^2 + X + 5)(4X - 1) \mod \xi$$

we get $\det(A(g,f)) = -72981 \;=\; 477 \times (-153)$.

4 Units and representations of primes

With the above definition of norm, we can see that the norm of an arithmetic prime number p is p^d. We might therefore suspect that if a prime p has an integer root for $f \equiv 0 \bmod p$, then p has factors mod f. For example,

$$\begin{aligned}(X^2 + X + 2)(2X^2 + 5X + 7) \;&\equiv\; (X^2 + 3X + 1)(7X^2 + 12X + 30) \\ &\equiv\; (2X^2 + 3X + 9)(-X^2 + 3X + 2) \;\equiv\; 11 \mod \xi,\end{aligned}$$

with the norm of the first factor 11, and the second 121. We will call a polynomial g with integer coefficients such that $\det(A(g,f)) = p$ a **representation** of p.

Now 6 is the only root of $\xi \equiv 0 \bmod 11$, and for $X = 6$,

$$X^2 + X + 2 \;\equiv\; X^2 + 3X + 1 \;\equiv\; 2X^2 + 3X + 9 \;\equiv\; 0 \mod 11.$$

We now show that all these representations are equivalent.

We find that $N(-X) = N(X^2 + 2X + 5) = 1$, so that $N((-X)^m) = N((X^2 + 2X + 5)^n) = 1$ for any m, n, and that $((-X)(X^2 + 2X + 5))^n \equiv 1 \bmod \xi$, i.e.

$$X^2 + 2X + 5 \ \equiv \ (-X)^{-1} \ \bmod \ \xi.$$

Expressions with norm ± 1 are called **units**. Also

$$\begin{aligned}(-X)(X^2 + X + 2) \ &\equiv \ X^2 + 3X + 1 \ \bmod \ \xi, \\ (X^2 + 2X + 5)(X^2 + X + 2) \ &\equiv \ 2X^2 + 3X + 9 \ \bmod \ \xi,\end{aligned}$$

etc. In other words, any of the representations can be turned into any other by multiplying by a unit.

By contrast, $\xi \equiv 0 \bmod 47$ has three roots 15, 38 and 39. We find that

$$\begin{aligned}(2X^2 + 4X + 7)(6X^2 + 8X + 9) \ &\equiv \ (2X^2 + 3X + 6)(5X^2 + 12X + 11) \\ &\equiv \ (X^2 + 3X + 7)(X^2 - 6X + 6) \ \equiv \ 47 \ \bmod \ \xi,\end{aligned}$$

with the norm of the first factor 47, and the second $2209 = 47^2$. Now $2X^2 + 4X + 7 \equiv 0 \bmod 47$ for $X = 15$, $2X^2 + 3X + 6 \equiv 0 \bmod 47$ for $X = 38$, and $X^2 + 3X + 7 \equiv 0 \bmod 47$ for $X = 39$. These representations are therefore not equivalent, so we must count them as separate primes when keeping track of powers. The algebraic side of the table in section 2 should therefore look like this.

a	b	$N(a+bX)$	Powers								
		$p \rightarrow$	sign	...3...		11	17	....31....		.....47.....	
		$r \rightarrow$		1	2	6	13	12	24	15	38	39
38	1	$3^2 11^1 17^1 31^1$	0	2	0	1	1	0	1	0	0	0
25	8	$3^2 31^1 47^1$	0	2	0	0	0	0	1	0	1	0
3	16	$-11^1 47^1$	1	0	0	1	0	0	0	0	1	0
-3	29	$-17^1 47^2$	1	0	0	0	1	0	0	0	0	2

If r is a root of $f \equiv 0 \bmod p$, then $f(r - kb^{-1}p) \equiv 0 \bmod p$ for any k; so

$$N(a + rb) \ = \ (-b)^d f(-ab^{-1}) \ \equiv \ (-b)^d f(r) \ \equiv \ 0 \ \bmod \ p$$

if $-ab^{-1} = r - kb^{-1}p$, i.e. $a + rb \equiv 0 \bmod p$. This determines which root of $f \equiv 0 \bmod p$ should be attributed to a given a, b combination.

The above analysis suggests that we might be able to represent at least some of the algebraic primes directly. Such representations do not form part of the algorithm. Indeed, most polynomials have only a small proportion

of primes that can be represented directly. Nevertheless, representations hopefully prove a useful tool in understanding why certain parts of the algorithm are necessary.

The following table uses p_r to indicate a root r of $\xi \bmod p$ and its representation, which we denote by $\rho(p_r)$ from now on. Note that we have only been able to find a representation for the square of one of the primes.

p	Representation	p	Representation
3_1^2	$X+2$ (Note the square here)	31_{12}	$-X^2-X+1$
3_2	$X+1$	31_{24}	X^2+3X+3
11_6	X^2+3X+1	37_{21}	X^2+3
13_4	$3X+1$	43_{20}	$2X+3$
17_{13}	$9X+2$	47_{15}	$3X+2$
23_{20}	$X+3$	47_{38}	$2X^2+3X+6$
29_6	X^2+3X+4	47_{39}	$-6X-1$

Using these representations, we see how they combine, possibly with powers of a unit, to form the table of a, b entries.

a	b	$N(a+bX)$	Representation mod ξ
38	1	$3_1^2 11_6^1 17_{13}^1 31_{24}^1$	$(-X)^{-4}\rho(3_1^2)\rho(11_6)\rho(17_{13})\rho(31_{24}) \equiv X+38$
25	8	$3_1^2 31_{24}^1 47_{38}^1$	$\rho(3_1^2)\rho(31_{24})\rho(47_{38}) \equiv 8X+25$
3	16	$-11_6^1 47_{38}^1$	$-(-X)\rho(11_6)\rho(47_{38}) \equiv 16X+3$
-3	29	$-17_{13}^1 47_{39}^2$	$-(-X)^{-5}\rho(17_{13})(\rho(47_{39}))^2 \equiv 29X-3$

The product of all the representations gives $(-X)^{-8}$ times even powers of representations, forming a square as required.

We found that 3_1 had no representation, but that 3_1^2 did. In fact, 3_1^2 has four distinct representations: $X+2$, $-X+1$, $2X+1$, X^2+X+1, linked by the identities

$$(X^2+X+1)^2 \;\equiv\; (-X+1)(2X+1) \;\equiv\; (-X)(X+2)^2 \mod \xi,$$

with a related identity

$$(2X+1)^2 \;\equiv\; (-X)(-X+1)^2 \mod \xi.$$

The example happened to have two sets of 3_1^2 with the same representation, so forming a square in the product. We might therefore expect to find products with even powers that are not a square because they only contain a single power of 3_1^2.

a	b	$N(a+bX)$	Representation mod ξ
-3	-22	$13_4^1 17_{13}^2$	$(-X)^{-5}\rho(13_4)\rho(17_{13})^2 \equiv -22X-3$
-8	-37	$3_1^2 13_4^1$	$(-X)^2(-X+1)\rho(13_4) \equiv -37X-8$

We can see that the powers of $-X$ and $-X+1$ are odd in the product of the representations, so the result is not a square, even though $13_4^1 17_{13}^2 3_1^2 13_4^1$ appears to be a square. However, suppose we add another entry.

a	b	$N(a+bX)$	Representation mod ξ
-3	-22	$13_4^1 17_{13}^2$	$(-X)^{-5}\rho(13_4)\rho(17_{13})^2 \equiv -22X-3$
-8	-37	$3_1^2 13_4^1$	$(-X)^2(-X+1)\rho(13_4) \equiv -37X-8$
1	-10	$3_1^2 13_4^2$	$(-X)^{-2}(-X+1)\rho(13_4)^2 \equiv -10X+1$

Then the product of the representations is

$$(-X)^{-5}(3X+1)^4(9X+2)^2(-X+1)^2 \equiv (-X)^{-6}(3X+1)^4(9X+2)^2(2X+1)^2,$$

so is a square. The next section but one examines how we would know that adding extra entries is necessary. First, we need to examine what happens if the product has an odd power of a unit.

5 Integers and rationals

Consider the following.

a	b	$N(a+bX)$	Powers			Representation mod ξ
		$p \to$	sign	...3...		
		$r \to$		1	2	
1	4	$9 = 3_2^2$	0	0	2	$(-X)\rho(3_2)^2 \equiv 4X+1$

We find that $(2X^2+1)^2 \equiv 3^2(4X+1) \bmod \xi$, but $4X+1$ has no square root mod ξ with integer coefficients. In other words, a possible square found by considering even powers of primes may only have a square root with rational, but not integer coefficients. This problem can be easily overcome by multiplying by $f'(X)^2$. Justifying this requires a rather lengthy explanation, which can be found in Appendix B [M500 **276**] (where we also introduce the **trace** $T(g) = \sum_{j=0}^{d-1} g(\alpha_j)$, which is related to the norm of g). The number field sieve algorithm does not rely on any special properties of the particular f used, so multiplying by $f'(X)^2$ in all cases takes care of the odd unit powers problem if it exists, and is harmless if it does not exist. Obviously, we also have to compensate on the arithmetic side by multiplying by $f'(m)^2$ (recall that $f(m) = M$).

In our case, $\xi'(X) = 3X^2 + 4X + 5$, so

$$[\xi'(X)]^2 \equiv -11X^2 + X + 19 \mod \xi,$$

and

$$[\xi'(X)]^2(4X+1) \equiv 81X^2 + 297X + 63 \equiv (3X^2 - 6X - 3)^2 \mod \xi.$$

6 Detecting non-squares

For this section, we will consider the algebraic half of the factorization of 121879 using another cubic polynomial,

$$\eta \;=\; X^3 + X^2 + 37X + 16, \quad \text{with} \;\; \eta(49) \;=\; 121879;$$

η has no units with low coefficient values other than ± 1 (see section 9). The following table shows primes up to 200 that have roots r.

p	r	p	r	p	r	p	r	p	r
2	0	23	7	83	33	137	23, 56, 67	181	33
3	2	29	7	97	15	139	76	191	139
5	1	31	16, 29	101	67	149	77	193	14, 184, 187
7	6	37	8	103	64	151	46	199	144
11	1	43	15	107	57	163	3, 64, 95		
13	5	53	12	109	20	167	93		
17	2	61	4, 9, 47	113	110	173	79		
19	9	67	46	131	53	179	172		

Of these, the primes listed in the next table have representations with low coefficient values (see section 9 for other representations).

p	Representation	p	Representation
19_9	$2X + 1$	101_{67}	$-3X - 1$
29_7	$-11X^2 - 76X - 31$	107_{57}	$-9X^2 - 20X - 7$
37_8	$1213X^2 + 1610X + 471$	113_{110}	$X + 3$
43_{15}	$7X^2 + 4X + 257$	163_3	$-X + 3$
61_9	$2X^2 + X + 73$	191_{139}	$46X^2 + 26X + 1691$
67_{46}	$-2X^2 + 6X + 3$	193_{14}	$-66X^2 - 54X - 11$
97_{15}	$X^2 - 2X - 1$		

The following table shows a set of primes which have such representations, and with a set of a, b whose entries when multiplied together give an even power for each prime.

a	b	$N(a+bX)$	Powers					
		$p \rightarrow$	sign	19	43	97	101	191
		$r \rightarrow$		9	15	15	67	139
-651	-1625	$19^3 43^1 97^1 191^1$	0	3	1	1	0	1
-1	-3	101^1	0	0	0	0	1	0
15	-1	$43^1 97^1$	0	0	1	1	0	0
69	5	$19^1 101^1 191^1$	0	1	0	0	1	1

The representation products work as expected.

a	b	$N(a+bX)$	Representation mod η
-651	-1625	$19_9^3 43_{15}^1 97_{15}^1 191_{139}^1$	$\rho(19_9)^3\rho(43_{15})\rho(97_{15})\rho(191_{139})$ $\equiv -1625X - 651$
-1	-3	101_{67}^1	$-3X-1$
15	-1	$43_{15}^1 97_{15}^1$	$\rho(43_{15})\rho(97_{15}) \equiv -X+15$
69	5	$19_9^1 101_{67}^1 191_{139}^1$	$\rho(19_9)\rho(101_{67})\rho(191_{139}) \equiv 5X+69$

Consider the following.

a	b	$N(a+bX)$	Powers			
			sign	2	3	5
4	1	$2_0^2 3_2^2 5_1^1$	0	2	2	1
176	359	$2_0^{10} 3_2^6 5_1^3$	0	10	6	3

Now

$$(X+4)(359X+176) \equiv -X(X+4)^4 \mod \eta,$$

and $-X$ is not a square. Similarly, the next table has

$$(-X+32)(-X+11) \equiv (X+4)^2(X^2+29) \mod \eta,$$

and X^2+29 is not a square.

a	b	$N(a+bX)$	Powers			
			sign	2	3	5
32	-1	$2_0^4 3_2^7$	0	4	7	0
11	-1	$3_2^1 5_1^4$	0	0	1	4

However, we find that

$$-X(X^2+29) \equiv (X+4)^2 \mod \eta,$$

so combining the two tables would form a square. To encourage this, we need to consider possible squares modulo primes p with integer roots for $f \equiv 0 \bmod p$ that are not in our algebraic factor base (or primes from this factor base that are unused on the algebraic side in the list of a, b entries). We will call the primes in this list the **supplementary base**. If the product of the $a+bX$ is a square, this must also be true modulo each such p. Since the product of the $a+bX$ is done modulo f, X must be an integer root r of $f \equiv 0 \bmod p$.

If $a + rb \equiv 0 \bmod p$ for some a, b in our list, we cannot use this combination of p, r, since otherwise the product of the $a+rb$ would always be $\equiv 0 \bmod p$, and we would obtain no information. For the same reason, we

exclude p, r combinations for which $f'(r) \equiv 0 \bmod p$. With these combinations excluded, we can use Jacobi symbols to raise the probability that the product is a square, i.e. a quadratic residue modulo p. If the Jacobi symbol $\left(\frac{a+rb}{p}\right) = -1$, then $a + rb$ is not a quadratic residue modulo p, but if it is 1, it may or may not be. In order that the product of the $a + rb$ is a quadratic residue modulo p, the number of Jacobi symbols that are equal to -1 must be even. We can keep track of these using the usual parity system, giving the following table for η.

a	b	Jacobi symbol								
	$p \rightarrow$	7	11	13	17	19	23	29	.....31.....	
	$r \rightarrow$	6	1	5	2	9	7	7	16	29
4	1	−1	1	1	−1	−1	−1	−1	1	1
176	359	−1	−1	−1	−1	1	−1	−1	−1	1
32	−1	−1	1	1	1	1	1	1	1	−1
11	−1	−1	−1	−1	1	−1	1	1	−1	−1

Using all four entries, we get even parity for all the primes and roots shown, but not if the first two and last two entries are considered separately. Note that squares with rational coefficients (see section 5) all have Jacobi symbols equal to 1, since any rational $x/y \equiv xy^{-1} \bmod p$, where y^{-1} is an integer.

How many prime/root examples do we need to have a good chance of constructing a square? Some complicated theory suggests $3 \log M / \log 2$ is more than adequate (around 49 for the example M values).

7 Finding algebraic square roots

In this section, we will show how to find square roots in principle, then show what modifications are required for realistic cases. The idea is to calculate square roots with the coefficients calculated mod primes p. We will use the notation mod f, p to indicate that algebra is conducted mod f as usual, but that all coefficients are calculated mod p. The primes p we use are those for which $f \equiv 0 \bmod p$ has no integer roots. We will refer to these as I primes (I for irreducible or inert). As shown in my article on the Perrin sequence in M500 **269**, we can add a symbolic element to the field of integers modulo p such that f has three roots (or d roots for a polynomial of degree d). The element is one of the roots itself, which we will denote by X. Putting

$$J = p^d,$$

the article also shows that $X^J \equiv X \bmod f, p$, hence $X^{nJ} \equiv X^n \bmod f, p$ so

if $g = \sum_i a_i X^i$ is any polynomial mod f, $g^J \equiv g \bmod f, p$, and so $g^{J+1} \equiv g^2 \bmod f, p$.

If d is odd, and $p \equiv 3 \bmod 4$, $J + 1 \equiv 0 \bmod 4$, so $g^{(J+1)/4} \equiv \pm\sqrt{g} \bmod f, p$. We have seemingly found a method for calculating square roots, at least in principle, but it has a fatal flaw. To illustrate, we will take the square from section 2:

$$143911X^2 - 697343X - 154094.$$

The above calculation for I primes 7, 19 and 59 gives a square root of

$$\begin{aligned} 4X^2 &\mod f, 7, \\ 6X^2 + 14X + 4 &\mod f, 19, \\ 47X^2 + 17X + 47 &\mod f, 59. \end{aligned}$$

Had we used the negative root $13X^2 + 5X + 15 \bmod f, 19$, the Chinese Remainder Theorem would combine these to give

$$165X^2 + 784X + 224 \mod f, 7847$$

as required, but instead we get

$$3882X^2 + 1610X + 2702 \mod f, 7847.$$

Since we are likely to need hundreds of I primes in real implementations, checking all combinations of roots is computationally infeasible.

For a workable method, we need somehow to identify which is the correct root to use. We can use $g^J \equiv g \bmod f, p$ as above, giving $g^{J-1} \equiv 1 \bmod f, p$. Since norms are multiplicative, we have $N(g^{p-1}) = [N(g)]^{p-1}$; so

$$N(g^{p-1}) \mod p \equiv [N(g)]^{p-1} \mod p = 1$$

by Fermat's Little Theorem. So we have

$$N(g^{p-1}) \equiv g^{J-1} \equiv 1 \mod f, p.$$

Since we are working modulo p, we can take $(p-1)$th roots on both sides, giving $N(g) \equiv g^K \bmod f, p$, where

$$K = (p^d - 1)/(p - 1).$$

We will also need the following (proof in Ash(2003)):

$$\mathrm{disc}(f(X)) = (-1)^{d(d-1)/2} N(f'(X)),$$

where disc is the discriminant of f; so

$$\mathrm{disc}(f(X)) \;\equiv\; (-1)^{d(d-1)/2} f'(X)^K \mod f, p.$$

Let

$$S \;=\; f'(X)^2 \prod_{a,b} (a + bX)$$

be the polynomial for which we are trying to find the square root, and let R be the square root of S such that $N(R)$ has the same sign as $\mathrm{disc}(f(X))$. For this to be unique, we require that the degree d of the polynomial is odd. Taking norms, we have

$$N(S) \;=\; N(f'(X)^2) N\left(\prod_{a,b} (a + bX) \right) \;=\; \left[\mathrm{disc}(f(X))\right]^2 \prod_q q^{2a_q},$$

where the $2a_q$ are the powers of q in the product of algebraic factors. We therefore have

$$N(R) \;=\; \mathrm{disc}(f(X)) \prod_q q^{a_q}.$$

Now

$$RN(R) \;\equiv\; R \times R^K \;\equiv\; S^{(1+K)/2} \mod f, p;$$

so dividing both sides by $N(R)$, we have our square root modulo p:

$$R \;\equiv\; \left[f'(X)^2 \prod_{a,b} (a + bX) \right]^{(1+K)/2} \left[\mathrm{disc}(f(X)) \prod_q q^{a_q} \right]^{-1} \mod f, p.$$

For ease of reference in the table below for various I primes p, we will refer to

$$f'(X)^2 \prod_{a,b} (a + bX) \mod f, p \text{ as } S_p,$$

and

$$\mathrm{disc}(f(X)) \prod_q q^{a_q} \mod p \text{ as } M_p,$$

i.e.

$$R \;\equiv\; S_p^{(1+K)/2} M_p^{-1} \mod f, p.$$

The following uses the example in section 2, with all calculations done mod p after each multiplication.

Prime	S_p	M_p	M_p^{-1}	$R \bmod p$
2	X^2	1	1	X
5	$3X^2+3$	2	3	X^2+4X+2
7	$6X^2+4X+5$	1	1	$3X^2+6$
19	$12X^2+18X+1$	8	12	$5X^2+13X+9$
41	$23X^2$	21	2	$8X$
59	$33X^2+X+30$	51	22	$57X^2+7X+17$

The powers of S_p used in calculating R are large, so if $Z(n) = 2^n$, a table of $\left\{S_p^{Z(n)}\right\}$ is constructed by repeated squaring, so that S_p^a for arbitrary a can be calculated by multiplying the table values corresponding to the binary expansion of a. Using the Chinese Remainder Theorem, we get

$$R \;=\; 1886X^2 + 5789X + 902 \mod 3217270.$$

From section 2, the square root we found was $\pm(165X^2 + 784X + 224)$, which when multiplied by $f'(X)$ gives $\mp(1886X^2 + 5789X + 902)$.

In realistic cases, we need to modify the Chinese Remainder Theorem slightly to avoid unnecessary working with numbers with millions of digits. The Chinese Remainder Theorem states that if $x \equiv r_i \bmod p_i$ for a set of p_i, r_i, then $x \equiv \sum_i r_i P_i a_i \bmod P$, where

$$P \;=\; \prod_i p_i, \qquad P_i \;=\; P/p_i, \qquad a_i \;\equiv\; P_i^{-1} \mod p_i.$$

We can calculate the a_i without calculating P_i as follows:

$$P_i \mod p_i \;\equiv\; \prod_{j\neq i}(p_j \mod p_i) \mod p_i.$$

For the X^2 coefficient in the above example, we have the following.

p_i	r_i	a_i	$a_i r_i / p_i$	$a_i r_i P_i \bmod M$
2	0	1	0	0
5	1	4	0.8	5525
7	3	2	0.85714	33715
19	5	10	2.63158	61184
41	0	10	0	0
59	57	38	36.71186	48421
			Sum = 41.00058	Sum = 148845

Let $z = \sum_i r_i P_i a_i$, and let y be the unique integer such that $z - yP = x$, so that $z/P = y + x/P$. If $|x/P| < 1/(2+\varepsilon)$, then $y = \lfloor 0.5 + z/P \rfloor$. Now

$$\frac{z}{P} \;=\; \sum_i \frac{r_i P_i a_i}{P} \;=\; \sum_i \frac{r_i a_i}{p_i},$$

which we calculate using floating point arithmetic, so subject to rounding errors, hence the ε above. We therefore have

$$x \mod M \equiv \left(\left(\sum_i (a_i r_i P_i \mod M)\right) - y(P \mod M)\right) \mod M.$$

Note that

$$P_i \mod M \equiv (P \bmod M) p_i^{-1} \mod M,$$

where $P \bmod M \equiv \prod_i p_i \bmod M$, which only has to be calculated once. Theory from Lenstra and Lenstra (1993) indicates

$$x \sim d^{(d+5)/2} M \left(2u\sqrt{d} M^{1/d}\right)^{S/2},$$

where u is $\max |a|, |b|$ over the S factors of $(a + bX)$ used in the product, allowing a sufficiently large P to be estimated. Empirically, this exceeds 10^{10000} for $M \sim 10^{35}$.

Returning to our example, we have $y = 41$, $yP \bmod M = 69132$; so

$$x \equiv (148845 - 69132) \mod M = 1886,$$

as required.

8 Sieving and optimization

The analysis in Crandall and Pomerance (2001) shows that the typical number of a, b pairs required to give a factorization using the number field sieve method is proportional to

$$\exp\left(((64/9)^{1/3} + o(1))(\log M)^{1/3}(\log\log M)^{2/3}\right),$$

compared with

$$\exp\left((1 + o(1))(\log M)^{1/2}(\log\log M)^{1/2}\right)$$

corresponding entries for the quadratic sieve or elliptical curve methods, so might be expected to be faster if M has more than about 110 digits. Optimizing the actual implementation of the sieving process depends on the nature of the computing hardware available—what is appropriate for a massively parallel machine does not necessarily apply to single processor implementations. The references do not discuss the optimal size of the arithmetic and algebraic factor bases in any depth. For example, there is clearly a tradeoff between the greater ease of finding suitable (a, b) pairs for larger factor bases, and the number needed for Gaussian elimination to find a square.

9 Further reading and notes

Stewart and Tall (2002) or Jarvis (2014) are worth exploring, with Jarvis presenting an outline of the number field sieve in ring-theoretical terms. The examples given are confined to quadratic polynomials, largely because of the difficulty in computing various quantities if higher powers are used. I have not found prime representations described elsewhere (though I'm sure they must be). There seem to be many properties of representations worthy of further investigation. For example: Are representations always unique (apart from multiples of units)? Do all prime and root combinations for $X^3 + 2X^2 + 5X + 1$ exist apart from 3_1? Are there polynomials with representations / no representations for all / infinite / finite prime and root combinations? Are there efficient methods of generating representations?

My method of generating the example representations used in this article is certainly not efficient, involving factorization of norms $N(g)$ for a large number of different g. For example, using the polynomial $X^3+X^2+37X+16$ (η in section 6), we find that $g = -5X^2 - 24X - 6 = \rho(2_0 5_1^3 19_9 37_8)$, i.e. $N(g) = 2 \times 5^3 \times 19 \times 37$, with $g \equiv 0 \bmod 2$ for $X = 0$, $g \equiv 0 \bmod 5$ for $X = 1$ etc. Similarly, $X^2 - 88X + 122 = \rho(2_0 5_1^2 19_9 37_8^3)$. We therefore have

$$\rho(5_1) \;=\; \frac{(-5X^2 - 24X - 6)\rho(37_8)^2}{X^2 - 88X + 122}.$$

We evaluate this fraction F using the root $R = -0.43532460075\ldots$ (to several hundred decimal places) of η, and hope to find integers A, B, C, D with $D = \pm 1$ such that $AR^2 + BR^1 + CR^0 + DF = 0$ using an integer finding algorithm such as PSLQ. We find

$$\rho(5_1) \;=\; -19220600X^2 + 54846689X + 27518561.$$

As a check, we find $\rho(5_1)\rho(19_9)\rho(37_8^3)\rho(2_0)U_2 \equiv X^2 - 88X + 122 \bmod \eta$, where U_2 is one of the units of η, found in a similar manner:

$$\begin{aligned} U_1 \;=\;& -1326193941350712800903 0X^2 + 276238224624677636492374X \\ & + 122766531936375987478045, \\ U_2 \;=\;& 881066580202864621268036670842417218844220527 46X^2 \\ & + 4975166229418602449272245038685778904441572316 6X \\ & + 3238288224225732356146792551500931740685006063477. \end{aligned}$$

Other examples:

p	Representation
2_0	$29680745960X^2 + 16759987075X + 1090891565838,$
3_2	$-2510610112326X^2 - 1109313218038X - 7131867757,$
7_6	$2970374784X^2 + 9997137131X + 3789091407.$

References

Ash, R. B. (2003) Norms, Traces and Discriminants (online), available at www.math.uiuc.edu/~r-ash/Ant/AntChapter2.pdf.

Crandall, R. and Pomerance, C. (2001) *Prime Numbers: A Computational Perspective*, New York, Springer.

Jarvis, F. (2014) *Algebraic Number Theory*, New York, Springer.

Lenstra, A. K. and Lenstra, H. W. Jr. (eds.) (1993) *The Development of the Number Field Sieve*, New York, Springer.

Stewart, I. and Tall, D. (2002) *Algebraic Number Theory and Fermat's Last Theorem*, Natick MA, AK Peters.

Weiss, E. (1998) *Algebraic Number Theory*, Mineola NY, Dover.

Equilateral triangles

Tommy Moorhouse

This investigation is concerned with fitting an equilateral triangle inside a square. The square has a horizontal base and has sides of length 1 ('unit sides').

Part 1 If an equilateral triangle with unit sides rests inside the square with one edge coincident with the base of the square show that the area of the triangle is less than 1/2. Try to do this geometrically, without using the area formula.

Part 2 Now consider an equilateral triangle with area 1/2. It sits with one vertex coincident with the lower right vertex of the square and a second vertex resting on the left vertical side. What is the height of the third vertex above the base of the square? Is this vertex inside the square?

Part 3 An equilateral triangle is drawn inside the square such that one vertex is in the bottom left corner of the square and the other two vertices rest on the top and right-hand sides of the square respectively. What is the area of this triangle?

Part 4 Is the triangle in Part 3 the largest equilateral triangle that can be drawn inside the square? Imagine moving the triangle vertex away from that of the square along an edge, rotating the triangle to keep the other vertices touching the edges of the square. By finding a quadratic equation for the length of the edge of the triangle or otherwise show that the smallest equilateral triangle that can be drawn with all three vertices touching the sides of the square is the triangle with unit sides.

Solution 273.3 – Rational integral

Show that

$$I \;=\; \int_0^{2\pi} \frac{(\cos x)\left(\sin\dfrac{x}{2}\right)}{\left(\cos\dfrac{x}{3}\right)\left(\sin\dfrac{x}{4}\right)}\,dx \;=\; -\frac{368}{55}.$$

Bruce Roth

Let $x = 12\theta$ to get rid of the fractions:

$$I \;=\; 12\int_0^{\pi/6} \frac{(\cos 12\theta)(\sin 6\theta)}{(\cos 4\theta)(\sin 3\theta)}\,d\theta.$$

From the identities $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ and $\sin 2\theta = 2\sin\theta\cos\theta$ we get

$$\begin{aligned} I \;&=\; 12\int_0^{\pi/6} \frac{(4\cos^3 4\theta - 3\cos 4\theta)}{\cos 4\theta}\cdot\frac{2\sin 3\theta\cos 3\theta}{\sin 3\theta}\,d\theta \\ &=\; 12\int_0^{\pi/6} (4\cos^2 4\theta - 3)(2\cos 3\theta)\,d\theta \\ &=\; 24\int_0^{\pi/6} \big(4(\cos^2 4\theta)(\cos 3\theta) - 3\cos 3\theta\big)\,d\theta. \end{aligned}$$

From the identity $\cos^2\theta = (1+\cos 2\theta)/2$,

$$\begin{aligned} I \;&=\; 24\int_0^{\pi/6} \big(2(1+\cos 8\theta)(\cos 3\theta) - 3\cos 3\theta\big)\,d\theta \\ &=\; 24\int_0^{\pi/6} \big(2(\cos 8\theta)(\cos 3\theta) - \cos 3\theta\big)\,d\theta. \end{aligned}$$

From the identity $2(\cos A)(\cos B) = \cos(A+B) + \cos(A-B)$,

$$\begin{aligned} I \;&=\; 24\int_0^{\pi/6} \big(\cos 11\theta + \cos 5\theta - \cos 3\theta\big)\,d\theta \\ &=\; 24\left[\frac{\sin 11\theta}{11} + \frac{\sin 5\theta}{5} - \frac{\sin 3\theta}{3}\right]_0^{\pi/6} \\ &=\; 24\left(\frac{-1/2}{11} + \frac{1/2}{5} - \frac{1}{3}\right) \;=\; -\frac{368}{55}. \end{aligned}$$

Problem 275.2 – Elliptic polygon

Tony Forbes

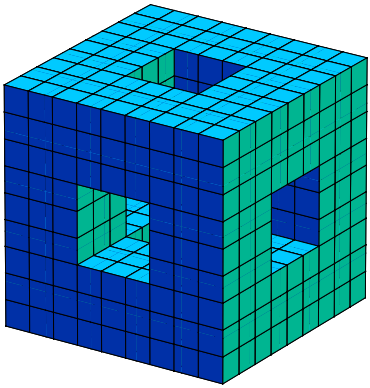
How do you draw a convex equilateral polygon such that all of its vertices lie on the ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1?$$

Note that this is not the same as merely dividing up an ellipse into arcs of equal length, the method I used for the theta graphs on the front cover. To do the job properly we must insist that the straight lines forming the sides of the polygon all have the same length. I do not have an answer except for the 4-gon. If it makes life easier, assume a vertex is at $(0, b)$.

Problem 275.3 – 540 cubes

This is a combination of Problem 274.2 – Holey cube and Problem 274.5 – 27 cubes. There are 540 cubes, where each face is painted using one of the five colours red, blue, green, yellow, cyan (or, if you prefer, white, light grey, medium grey, dark grey, black). Moreover, the 540 cubes can be assembled in five ways to form either a red, blue, green, yellow, or cyan version of the structure illustrated on the right, a $9 \times 9 \times 9$ cube with orthogonal 3×3 holes. Can it be done?



The numbers work out exactly: the 540 cubes have 3240 faces altogether of which $648 = 3240/5$ are exposed when the big hollow cube is built.

Problem 275.4 – Hidden die

A special X-ray scanner can detect the results of a hidden die rolled inside a box. The results are 90 per cent accurate. The scanner shows that a six has been rolled. What is the probability that the die in the box actually shows a six?

Several and varied answers were offered when the problem was aired at the 2017 M500 Winter Weekend in January. Thanks to Rob and Judith Rolfe for suggesting it.

M500 Mathematics Revision Weekend 2017

The forty-third M500 Revision Weekend will be held at

Kents Hill Park Training and Conference Centre,
Milton Keynes, MK7 6BZ
from Friday 12th to Sunday 14th May 2017.

The standard cost, including accommodation (with en suite facilities) and all meals from dinner on Friday evening to lunch on Sunday is £265 for single occupancy, or £230 per person for two students sharing in either a double or twin bedded room. The standard cost for non-residents, including Saturday and Sunday lunch, is £150.

Members may make a reservation with a £25 deposit, with the balance payable at the end of February. Non-members must pay in full at the time of application and all applications received after 28th February 2017 must be paid in full before the booking is confirmed. Members will be entitled to a discount of £15 for all applications received before 11th April 2017. The Late Booking Fee for applications received after 11th April 2017 is £20, with no membership discount applicable.

There is free on-site parking for those travelling by private transport. For full details and an application form, please go to the Society's web site at www.m500.org.uk.

The Weekend is open to all Open University students, and is designed to help with revision and exam preparation. We expect to offer tutorials for most undergraduate and postgraduate mathematics OU modules, subject to the availability of tutors and sufficient applications.

Please note that the venue is not the same as in 2016.

Problem 275.5 – Buses

The following conjecture was first stated by Theo Pender and communicated to me (TF) by Carrie Rutherford. Either prove the conjecture, or find a counter-example. There are two parts.

(i) If a bus has an *odd* number of doors, there are no restrictions on their utilization; you may enter or exit the bus via any door.

(ii) If a bus has an *even* number of doors, they are partitioned into two (disjoint) sets, entrances and exits. You must join the bus via an entrance and leave it via an exit.

By a *bus* we mean one of those large road vehicles that are used for the transportation of living people, who have to either pay fares or be in possession of some kind of permit in order to enjoy the right to travel.

Problem 275.6 – Pistachio nuts

Tony Forbes

There is a bowl containing n pistachio nuts. How many times would you expect to perform the following procedure in order to consume all of the edible material in the bowl?

(i) You select uniformly at random one object from the bowl. It might be a whole pistachio nut in its shell, or it might be half of a pistachio nut shell.

(ii) If it is a half-shell, you just return it to the bowl.

(iii) Otherwise you split the shell into two halves, remove the kernel, which you eat, and return the two shell fragments to the bowl.

Front cover The 69 theta graphs with 29 edges.