*

ISSN 1350-8539

M500 226

354299348571012144756835792047990094063607418035581522634786787005589748123666286792176218665829067088480634114503383033577740099043362118455121351
537215326975741605665145660612909282548465798505661719389202146784030607574615678472152978471637799667218853067988748086675972932604612794184865918
841261209865529829476927796757949787565956715588002113548012971507846921953395474665939918746620916251564271225117895086045406414115213786977134082
872441787874615521189161051082066456152981678263814931608306766639022999297117222658645741453361404762823747353304232115586670609671505719714930187
479155190217063845219792797591849007738566024805470968341377897208930040265442523014953284886371725249779153278362065833921831460754621564097632158
895495272858739007812737112338202230854295584503182600092403556562329915231563278295643485077968784006411966506730771913671317718965536857657154565
206612807058757413819674073555066691013222109750999170983638873287652624796774349132414129334977655820555627622071242200091192399059421290095712010
232125978599560582255999359658347459198474330206699881752618814206236570785965004587375776780953196404647575775261583251692069264754786193869836504
213227724774879417672779455828375743393367415017832078664404744605901444311522952411768325817942507467574684321839816867132467900691446001408277335
012603078851276522187455651690429432694392556446346731028684857300190192005402182541218701581889405428009600035049701874021917821384521592191880786
802996437446692704103312858469297929899335632063352587569195458911523972176665123611494800562890577620251203051718729793096505135151354356793021720
211623069054432854351035527058069703783977036523024355876882977420856077471582336175904670321628962918533953764914544774109873442838306694034985687
326529046781637314098777154497982928112146244705314018732539560368065219162531594492557127505681267417026364632395638582755803696514500141050616574
019923973767005437128262067866848826833611499840245632554495147235550476495216424228769507244763750003161399317648204959380352008962471387636911904
436477739023475080421428565686432593539808881199806951057245656781224110622512202122912592617490634123349389109437211625899856140738887511619292776
161080974497056930798809717271787542297579326504455034260862303842409504551467793762281454444702492074271864082947311241785091084213971881184267782
055717093340822111973791733455728882650472982605409960841639509811285323102703896314504085121542244020472460790457165428647428105257963985646165122
492019083051369755165632581559162844064395388903848564848159482047308988130086896721178557827668603891958164635208279198982541343969108499567166442
740456829731166396566038899874063404935475624629133415355345541841214135696281794221873712613227447639600891093070858914876305395151387697528761175
908001329737267651646488035080625593676029290455626275096680713280757590064735196755958988051082580406624277572559844270779267925358809540736533275
773905347840999268194560177349082459205435062532659746966810420530299879490281621736626170014060590761484089012943712413044855276508900865779020419
828710624984354363195214458749870340087350067031366970505725593031318987511597167420308890978153893869540979582023771711696918829066905380649414848
054318380329455914924986673386197561614359849254754301647359399906330992590248679141360555673602283461937449802943347191437519552351486585795457896
573167214450994495936949118947708340647916847898802307038519869315281938132727863901768149545789151528009803861031250641140400393448743667557370267
209921684299578859545373171370237526074145686053806104081998034055878437984316952753026609092380768107148366667463876860175628456443072542768317926
297970561497896373300011575913227554540737508007288687132790834250846557685113782370764493824866610052165295535677207174497539355175034168213553623
323154263283548812257308472868353105270594643282487085267526364693354983199328157423962526789745865136941140249590394693109625681788945597406068787
998181893604803354152730829470990628818826184893734788376332589239704552492122038174020015656624439527607508522825181438218633572205280022589834405
608823804431816594697556803350654834560396013216547409579058744909795425187917573391973926739575838277509203096989643253404155764163423462911233507
817938716595190525728049855398211813107814181640004185951225292492929932569994320020903742606826319668143700303099192418122558842782799589019215125
037716105081246350681268499650285387051687978412214032286019274411336181656696010777724256895418838923059520149224916943393474697793393217549981054
235937202043902605551819251755915288049093904847024642257352518665903738699686702377009345374461247316689310149580724150729565925896833559647384300
845872045689657679047575724062436837007645528663897014163944746828086257807986488524269980136621678012135726252134607019285664972035707161895043982
289037387753723286658387986027432958495020889359583340102463776397349965149777090594145987721737514422897340299508080491194147609317642200453533114
598630554334311324788453905988185521056827898170523239853099239259118245645806506721735308521149479004383887267782257790283978888228867905443522168
353299740506811354023905246255180410707911175015882989072955969953495581021278673648340462302699542846156176666021631237262263745323303560484924226
142599029306676038116772070270813896266421697270476398576159819132385043120660264746408911956445820555336015957626057075519890605941348616212970760
452280440921648928488753946364060539318065315175661719366776070961565138162603218150569525500483989684971236582574994959103542080272700746266125996
358021802270757800434297036766217974108737339549076165534985813104322636342312995933688788321654364687023654337789987300626847339867088771906533549
029092429086315773962896874238015366213311531275162891034532894838801919132891237203536999748370795556966982851277779420185610058975842924319720349
077308667508430292521302066029904386206622562856295698881110599942342838914040811409111261740143386492430408958081822444917416716494686608361163110
297703789188430360291481441946458712422029054261646363258444682875734876032483009395589449106997566383484410712264698412256538016973349076276575688
612000066415244264390571471579155922109745072637854385671532422680463419749816614525929314143821480983156618523961468884897299334846859522422930454
0863582838240402598174093932164659536960016289581883498950870292780006048278157939493698701456055575670506118158418093039128727971853851030803604808
427965454971186696976419823199925464989493194018785471689644925173867557118605805852443178037903762020982900606663123948561059578299777815414438342
469084586804454176761378771761433531928038354852382982648067429699882225678779565060739595238867271076035193002226776726076893183282311622971501941
966657667900915375026198498555638474138562672995313536282882380614376692009798953340837943316992812147279641055959689215718511055313758866609633105
351844453395679576562535141675953926333149620875395424854263604408534866033494134318693450176149787154790779252905112348912480194602030321758213039
277763843254221572053940836448514032464406113982831635887912990030931266543132718537181863618122831769196857617331612135372500244501747446865878597
680949923985140791500542258058847187485546317942249061964744195230654187256329230297736262383024617406628341520464548343482772955240667089249910868
222191168312247058824498557596461564606048927642571622869487538211631876837289724807666034464220189484160223458815712925727261859503843561396099112
400802926483634159515425764703147244034898339008079239802211915178473626023447631080903182592644366863202012022692928052732917633252040768203961107
970845810354362561836082221976658571961631409056097368544194912907351883492587320580507576002179155389577181938638007134661491946153494631826464045
031253620140479458393416298594034799588038177585519393946839783753930558100918426637601238473401772603639049466598089375988426366260393270553530981
709889554286453029409067068628519528316313444985139228460554607286351674001427724781433684407916318342846421871957960380768571599051819721095627222
983819494764732944174227198917657365907916545208118732066570801002110957061845257462199983750673196657118924619184049339633377595287777365282477534
300331146183337242541037177772862798477828302381964012830387464945745076809142429793977345210125114873307538848905907607909741615487111715503180575
674979813003230455040499298057812594854295831660392081387834597185621327543892274733275654011187630923999858047363309383463259149996352229145440101
801659864812761702016935103561269203289175736187274287983379184827927465005090990657318423341012461703993704769556942087335585301803490343272285969
555563615666812592547819688849498585946207050526262841432852946981889058235931094435191344525681400351464932700793641019883401764071284673502472056
451988456952213736282762067213475286961191875825849566715648180873818704671045973057556731814197500541707246279785988274694790460028641553126786756
204992776800994028340844146574411000278029013240069064280329676505934612808420701509700887376445906609695306019876926244037248707793203256804462348
313689438953983885239293900581887518921472347370018253031094921241162559067701160917073152154182901797519270190824288688790117126878027584061793458
125230378235318446848062326490062374840992466756428262612067536623743288670303809930731764263733759800282999329473140102841663257005079128349860385
333260587762141909458128169849641681220083377545279250162473132879854965471027625328256835038076333606953205886563169228058120488440710660929972722
750778175525581917159051226346593544350611670051747367143924666269675217128977830230384442595670914368862387508874513225500465749257317733047225089
041504992458647606124480058639141821895013001696013746338281744273280333988563101629764310948385028344652399409756031980227224070926393638798198246
842379689065430261712485100935554441964665011774232629037751835649039332040901762714636497906452148091863096421991544663400560446664277396595767438
009339702765920705205561208018366042110825309667327 $+\ d$, $d = 0, 2, 6$, are prime.

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: www.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 September Weekend is a residential Friday to Sunday event held each September for revision and exam preparation. Details available from March onwards. Send s.a.e. to Jeremy Humphries, below.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details, send a stamped, addressed envelope to Diana Maxwell, below.

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 Tony Forbes, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation. If you use a computer, please also send the file to tony@m500.org.uk.

Functions $f : \mathbb{Z}^+ \to \mathbb{Z}$

Tommy Moorhouse

Introduction: A ring of functions

A ring is a mathematical structure whose properties are a generalization of those of the integers. In a ring one can add elements to get other elements and one can multiply elements together. Just as in the ring of integers the elements of a general ring need not have a multiplicative inverse, but they must have a 'negative' or additive inverse.

Ring multiplication need not be commutative (so that if a and b are elements we need not have $ab = ba$) but the ring considered in this article is commutative. We will consider a particular ring of functions and explore some of its properties. You may find this an interesting exercise in itself, and hopefully if you have little knowledge of rings you will be motivated to learn more.

The ring $\mathfrak{F}$

The functions $f : \mathbb{Z}^+ \to \mathbb{Z}$, which are integer valued for all positive integer arguments, inherit many of their properties from $\mathbb{Z}$, which is the best known example of a ring. In the ring of functions the elements can be added to give another element; there is a 'negative' for every element, such that $f + (-f) = z$ where z is the zero element, i.e. the function such that $z(n) = 0$ for all $n \in \mathbb{Z}^+$; and there is multiplication between non-zero elements. The non-zero elements need not have inverses (an inverse of an element t is an element s such that $st = ts = 1$, where 1 denotes the multiplicative identity element of the ring: for our functions this is denoted by I). We will denote the ring of functions $f : \mathbb{Z}^+ \to \mathbb{Z}$ by $\mathfrak{F}$.

In the ring of functions we have ordinary (pointwise) addition:

$$(f + g)(n) = f(n) + g(n).$$

The addition on the right is just the addition of the integers $f(n)$ and $g(n)$. The fact that we are ultimately concerned with the addition of integers strongly suggests that the properties of $\mathbb{Z}$ largely determine those of $\mathfrak{F}$. Our multiplication is the Dirichlet 'convolution' product

$$f * g(n) = \sum_{dd'=n} f(d)g(d'),$$

which is shown by Apostol [1] to be commutative, associative and distributive over addition.

Exercise 1 With addition and multiplication so defined show that $\mathfrak{F}$ is a ring.

The main theme of this article is an exploration of the structure of $\mathfrak{F}$. The first property is established in Exercise 2.

Exercise 2 Show that there are no divisors of zero in $\mathfrak{F}$ (that is there do not exist non-zero functions f and g such that $f * g = z$).

A suggested answer is given at the end of the article. Commutative rings with this property will be called 'entire', following Lang [2].

Now we consider ideals in $\mathfrak{F}$. An ideal in $\mathfrak{F}$ is a subset $\mathfrak{I}$ of $\mathfrak{F}$ that is closed under addition (i.e. if $f \in \mathfrak{I}, g \in \mathfrak{I}$ then $f + g \in \mathfrak{I}$) and such that if $a \in \mathfrak{F}$ and $b \in \mathfrak{I}$ then $ab \in \mathfrak{I}$. A simple example of an ideal in the ring $\mathbb{Z}$ is that of the even numbers: two even numbers can be added to give another even number, and if we multiply any integer by an even number we get an even number.

Characteristic sets $C(n)$

We now turn to the behaviour of functions $f : \mathbb{Z}^+ \to \mathbb{Z}$ on some special subsets of $\mathbb{Z}^+$. We define the set $C(n)$ for any $n \in \mathbb{Z}$ as

$$C(n) = \{d \in \mathbb{Z}^+ : d|n\},$$

where the notation $d|n$ means that d divides n. Thus $C(n)$ is the set of all (positive) divisors of n.

Definition 1 $C(n)$ is the set of all divisors of n.

It is then quite straightforward to establish that for any n the set of functions f such that $f(d) = 0$ for all $d \in C(n)$ forms an ideal, say $\mathfrak{I}_n$, the most important step in the proof forming Exercise 3.

Definition 2 The set of functions vanishing on $C(n)$ is an ideal $\mathfrak{I}_n$.

Exercise 3 Show that the product of any $f \in \mathfrak{F}$ with any $g \in \mathfrak{I}_n$ is again in $\mathfrak{I}_n$. (Hint – this follows from the definition of the convolution product.)

More generally, the functions f such that $f(d) \equiv 0 \pmod{p}$ for $d \in C(n)$ form an ideal for each n and for each prime number p.

The sets $C(n)$ are characteristic of the convolution product and indeed any convolution product has its own characteristic sets. Multiplicative functions vanishing (or congruent to 0 mod p) on any $C(n)$ also vanish on any integer divisible by any divisor of n.

Definition 3 A *prime ideal* $\mathfrak{p}$ is an ideal such that if $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (or both).

Exercise 4 Show that the ideals $\mathfrak{I}_n$ are not prime except when $n = 1$. Hint: find functions that do not vanish on all divisors of n but whose product does vanish on at least one such divisor.

The ideal $\mathfrak{I}_1$ is prime but not maximal (the proof involves looking at the quotient ring $\mathfrak{F}/\mathfrak{I}_1$ and noting that not every element has an inverse). This means that there is at least one proper ideal of $\mathfrak{F}$ containing $\mathfrak{I}_1$.

We conclude that $\mathfrak{I}_1$ is contained in some maximal ideal. In fact there are many maximal ideals containing $\mathfrak{I}_1$. These are the ideals determined by primes p and generated by the elements f with $p|f(1)$, which clearly contain $\mathfrak{I}_1$ since $p|0$ for all n. (This is a consequence of the fact that for all n we have $n \times 0 = 0$.)

We can put this on a more rigorous footing by introducing a valuation on a quotient ring of $\mathfrak{F}$. In our case a valuation is a function, denoted by $||_v$, from a ring into $\mathbb{Z}$ (but valuations are usually considered as functions into a field such as $\mathbb{C}$).

Definition 4 A *valuation* on $\mathfrak{F}$ is a function into $\mathbb{Z}$ satisfying

$$\begin{aligned} |f * g|_v &= |f|_v |g|_v, \\ |f|_v &= 0 \text{ iff } f = z, \text{ and} \\ |f + g|_v &\leq |f|_v + |g|_v. \end{aligned}$$

To ensure that the second condition holds we form the quotient $\mathfrak{F}_1 = \mathfrak{F}/\mathfrak{I}_1$ and define

$$|f|_v = |f(1)|$$

on this quotient, where the right-hand side is the usual absolute value. Then the maximal ideals are generated by elements f with p a prime and $p||f|_v$. The quotients $\mathfrak{F}_1/(f)$ are then isomorphic to the fields $\mathbb{Z}_p$. Other (non-maximal) ideals are generated by functions f such that $|f|_v = n$ with composite n. This also tells us that the ideals of $\mathfrak{F}$ are finitely generated and in fact principal. With this valuation we see that $\mathfrak{F}_1$ contains a subring isomorphic to $\mathbb{Z}$.

The set of elements such that $|f|_v = 1$ forms a multiplicative subgroup of $\mathfrak{F}_1$ called the unit group.

Types of function

It is sometimes useful to consider functions with certain properties, and clearly define what we mean by these properties. The definitions below are intended to illustrate this.

Definition 5 *EP:* a function is said to be *EP* or *eventually periodic* (with period M) if there exist integers M, N such that for all $n \geq N, f(n+M) = f(n)$.

Definition 6 *EC:* a function is said to be *EC* or *eventually constant* if there is an integer M such that for all $n \geq N, f(n+1) = f(n)$.

Definition 7 *Bounded:* a function is said to be *bounded* if there is a positive integer N such that for all n, $|f(n)| \leq N$.

Definition 8 *EM:* a function is said to be *EM* or *eventually monotonic* if there are positive integers M, N such that for $n \geq M, f$ is either EC or for all $n \geq M$ we have $S(f(n+1) - f(n)) \geq 0$ or for all $n \geq M$ $S(f(n+1) - f(n)) \leq 0$.

Here $S(n)$ is the sign of n: either $+1$ if $n > 0$, -1 if $n < 0$, and 0 if $n = 0$. A monotonic function, if it changes at all, always increases or always decreases.

Exercise 5 Show that an EC function is EP. Show also that a bounded EM function is EC.

The map $\mathcal{L} : \mathfrak{F} \to \mathfrak{L}$

We define $\mathfrak{L}$ to be the collection of all integer logarithm functions on $\mathbb{Z}^+$. Each of these functions derives from (at least) one function in $\mathfrak{F}$ as follows:

$$\mathcal{L}(f)(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = \sum_i k_i f(p_i).$$

We see that $\mathcal{L}(f)$ is a function on $\mathbb{Z}^+$ of the logarithm type. The image of $\mathcal{L}$ is the whole of $\mathfrak{L}$, but $\mathcal{L}$ is not injective (one to one).

If we restrict our attention to completely multiplicative functions $\mathcal{L}$ has an interesting property:

$$\mathcal{L}(f * g) = \mathcal{L}(f) + \mathcal{L}(g).$$

The proof is as follows: since f and g are completely multiplicative we must have $f(1) = g(1) = 1$. But f and g are completely determined (unlike general multiplicative functions) by their values on the primes. Moreover, $f * g$ is completely multiplicative and so $f * g(p) = f(1)g(p) + f(p)g(1) = f(p) + g(p)$. Since $\mathcal{L}$ depends only on the values of $f * g$ at the primes the property is established.

We easily see that for all the 'constant' functions kI in $\mathfrak{F}$, $kI(1) = k$, $kI(n) = 0$, $\mathcal{L}(kI)$ is the zero function z. Thus $\mathcal{L}(kI * f) = k\mathcal{L}(f)$; $\mathcal{L}$ defines a group isomorphism from the group of completely multiplicative functions to the group of completely additive (i.e. logarithm type) functions.

We can consider $\mathcal{L}$ as a map from the (completely) multiplicative functions into the set of derivations on $\mathfrak{F}$ since each logarithm type function defines a derivative through $\nabla f(n) = \mathcal{L}(g)(n)f(n) = L_g(n)f(n)$.

Cohomolgy

The ring of functions $\mathfrak{F}$ with its ideals defined through the characteristic sets $C(n)$ give concrete examples of certain cohomological ideas, although we shall not take them very far in this article. The sets $C(n)$ cover $\mathbb{Z}$ in the sense that any $m \in \mathbb{Z}$ is contained in countably many $C(n)$. The collection

$$\{C(n) : n \in \mathbb{Z}\}$$

does not form a topology for $\mathbb{Z}$ but the intersection $C(n) \bigcap C(m) = C((n,m))$, where (n,m) is the greatest common divisor of m and n, so it makes sense to work with these sets. We can form any finite intersection $C(n_1) \bigcap C(n_2) \bigcap \cdots \bigcap C(n_r)$ and this is again of the form $C(r)$ for some integer r. These intersections are always non-empty because $C(1) \subset C(n)$ for all n.

We now consider collections of functions into $\mathbb{Z}$, each function defined on a particular $C(n)$. Denote these collections of functions $\{f_n, C(n)\}$ (called 'function elements') where each function f_n is defined on $C(n)$ and even if $C(m) \subset C(n)$ f_m need not be the restriction of f_n to $C(m)$. The conditions for which the restriction relation $f_m = f_n|_{C(m)}$ holds are quite special.

Exercise 6 Let f_n be defined on $C(n)$ and let $f_n(d) = (n,d)$ (the greatest common divisor of n and d). Show that the f_n are actually the restictions of a single 'global' function f to each $C(n)$ and describe this function. Further show that the collection $g_n(d) = n/d$ does not define a global function.

We can define operators δ_i on the collection of functions defined on i-fold collections of characteristic sets. First define, for a global function $f : \mathbb{Z}^+ \to \mathbb{Z}$,

$$(\delta_0 f)_n = f|_{C(n)},$$

the restriction of f to $C(n)$ for each n. We thus obtain a collection of the type $\{f_n, C(n)\}$ with f_n defined only on $C(n)$. Next, for any collection of the type $\{f_n, C(n)\}$ define

$$(\delta_1 f_n)_m = f_n|_{C((n,m))} - f_m|_{C((n,m))},$$

which is of the type $\{f_{nm}\}$ with the functions $f_{nm} = -f_{mn}$ defined for each (ordered) pair of characteristic sets $C(n), C(m)$. You should check that the kernel of δ_1 includes the collection of restrictions of global functions. The image of δ_1 is a set of antisymmetric function elements lying in the kernel of δ_2, which you may like to attempt to define on function elements of the type $\{f_{nm}, C(n), C(m)\}$ (i.e. $(\delta_2 f_{nm})_r = \cdots$).

The question of whether the image of δ_0 is actually equal to the kernel of δ_1 (and so on) is the subject of cohomology, which we will not pursue further.

Appendix: Suggested proof that $\mathfrak{F}$ is entire

Suppose there are functions f and g, not zero for all n, such that

$$f * g(n) = z(n) = 0.$$

First we show by induction that if $f(1) \neq 0$ so that $g(1) = 0$ (since $f(1)g(1) = 0$ and $f(1)$ and $g(1)$ are both ordinary integers) we must have $g = z$. Now, for any prime p, $0 = f * g(p) = f(1)g(p)$ so that $g(p) = 0$. To carry out the induction suppose that $g(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = 0$ for all arguments with $\sum k_i$ prime factors or fewer, and consider $0 = f * g(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q) = f(1)g(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q)$, where q is any prime, since g vanishes on all other factors. This establishes that $g(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q) = 0$.

Now suppose $f(1) = 0$ and $g(1) = 0$. Since f and g are non-zero there are integers m and n such that $f(n) \neq 0$ and $g(m) \neq 0$. Let k, l be the smallest such pair so that $f(k) > 0$ and $g(l) > 0$, and suppose $kl = n$, say. Then

$$f * g(n) = \sum_{dd'=n} f(d)g(d') = f(k)g(l) \neq 0,$$

with only one term in the sum since if $dd' = n$ $(= kl)$ with $d > k$, say, we must have $d' < l$ and, since l is the smallest integer for which g is non-zero, we have $g(d') = 0$. The same argument applies for $d' > l$, when $f(d)$ vanishes. Thus $f * g \neq z$.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer 1998.

[2] S. Lang, *Algebra* (revised third edition), Springer 2002.

Problem 226.1 Conway's prime machine

Tony Forbes

Denote by Q_i the ith element of the list

$$Q = \left(\frac{17}{91}, \frac{78}{85}, \frac{19}{51}, \frac{23}{38}, \frac{29}{33}, \frac{77}{29}, \frac{95}{23}, \frac{77}{19}, \frac{1}{17}, \frac{11}{13}, \frac{13}{11}, \frac{15}{14}, \frac{15}{2}, 55\right).$$

Perform the following procedure.

> Start with $n = 2$. In general, replace n by nQ_i, where i is the smallest index r such that nQ_r is an integer.

For example, the first number you should obtain is 2, the starting point of the iteration. The second number is 15 because the first element of Q that has a denominator that divides 2 is $Q_{13} = \frac{15}{2}$, and $15 = 2 \cdot \frac{15}{2}$. The third number is $825 = 15 \cdot 55$ since no other number in the list has a denominator that divides 15. Next, $825 = 3 \cdot 5^2 \cdot 11$ and the relevant fraction is $Q_5 = \frac{29}{33}$; hence the fourth number is $825 \cdot \frac{29}{33} = 725$. Continuing in this way produces the sequence

$$\begin{gathered}
2, 15, 825, 725, 1925, 2275, 425, 390, 330, 290, 770, 910, 170, 156, \\
132, 116, 308, 364, 68, 4, 30, 225, 12375, 10875, 28875, 25375, \\
67375, 79625, 14875, 13650, 2550, 2340, 1980, 1740, 4620, 4060, \\
10780, 12740, 2380, 2184, 408, 152, 92, 380, 230, 950, 575, 2375, \\
9625, 11375, 2125, 1950, 1650, 1450, 3850, 4550, 850, 780, 660, 580, \\
1540, 1820, 340, 312, 264, 232, 616, 728, 136, 8, 60, \ldots .
\end{gathered}$$

Now concentrate on the 20th and 70th numbers, namely 4 and 8. Notice that both of these are powers of 2 and moreover the exponents are prime; $4 = 2^2$ and $8 = 2^3$. This is no coincidence. If you look further, you will see that the 281st number is 2^5, the 708th number is 2^7, the 2364th number is 2^{11}, the 3877th number is 2^{13}, the 8069th number is 2^{17}, and so on, all prime powers of 2.

All we want you to do is explain why this works. In other words, show that whenever a power of two appears its exponent is prime. Are all primes generated in this way?

The algorithm is described by Richard Guy in an article about John Conway printed in the book *Mathematical People: Profiles and Interviews*, edited by D. J. Albers and G. L. Alexanderson.

The Pascal tetrahedron

Stuart Walmsley

Denote by W_1, W_2, ... the sequence 1, 1, 3, 7, 19, 51, ... introduced by Patrick Walker in M500 **223**. Here it is discussed in terms of the three-dimensional analogue of the Pascal triangle (the Pascal tetrahedron?).

It is recalled that the elements of Pascal's triangle are binomial coefficients defined by

$$\binom{n}{j} = \frac{n!}{j!(n-j)!}.$$

It is more convenient in the present context to replace them by a symmetrical notation:

$$(j,k) = \frac{(j+k)!}{j!k!}.$$

Higher-index coefficients are then readily defined, but attention is here confined to the three-index terms:

$$(j,k,l) = \frac{(j+k+l)!}{j!k!l!}.$$

In the Pascal triangle, a given term is the sum of the two immediately above it. In the new notation

$$(j,k) = (j-1,k) + (j,k-1),$$

a form which emphasizes the essential symmetry of the relation. It is easily proved that the corresponding relation for the three symbol is

$$(j,k,l) = (j-1,k,l) + (j,k-1,l) + (j,k,l-1).$$

The three-dimensional analogue of the Pascal triangle is a tetrahedron in which successive faces have the following form.

$$\begin{array}{ccccccccccc}
(0,0,0) & & & (1,0,0) & & & & & (2,0,0) & & \\
& & (0,1,0) & & (0,0,1) & & & (1,1,0) & & (1,0,1) & \ldots \\
& & & & & & (0,2,0) & & (0,1,1) & & (0,0,2)
\end{array}$$

Each successive layer is a progressively bigger equilateral triangle. The layers with explicit values of the coefficients are shown below. Any particular element is the sum of the three elements above it and the sum of the elements in a plane is a power of 3.

The triangle formed by Patrick Walker shares these two properties, but it is the sum of the elements in a horizontal line which is a power of 3. The sequence referred to in the title is found in the central vertical column.

$$
\begin{array}{ccccc}
 & & 1 & & \\
 & 1 & 1 & 1 & \\
1 & 2 & 3 & 2 & 1
\end{array}
$$

It is not surprising that the two are related. The elements in the triangle are sums of vertical columns of elements in the planes of the tetrahedron as shown.

$$
\begin{array}{cccccccccccccccc}
1 & & 1 & & & & 1 & & & & & & 1 & & & \\
 & 1 & & 1 & & 2 & & 2 & & & & 3 & & 3 & & \\
 & & & & 1 & & 2 & & 1 & & 3 & & 6 & & 3 & \\
 & & & & & & & & & 1 & & 3 & & 3 & & 1 \\
 & & & & & & & & & & & & & & & \\
1 & 1 & 1 & 1 & 1 & 2 & 3 & 2 & 1 & 1 & 3 & 6 & 7 & 6 & 3 & 1
\end{array}
$$

Walker points out that in the Pascal triangle the sums of alternate elements in a row are equal to one another and a power of two (or, as he puts it the difference of the two sums is zero). In the Walker triangle, the difference of the two sums is 1. The more direct analogue of the Pascal result is that the sum of every third term in a line is a power of 3. Then the elements in the sequence 1, 1, 3, 7, ... are related to the (j, k, l) symbols by

$$
\begin{aligned}
W_0 &= (0,0,0), \\
W_1 &= (1,0,0), \\
W_2 &= (2,0,0) + (0,1,1), \\
W_3 &= (3,0,0) + (1,1,1), \\
W_4 &= (4,0,0) + (2,1,1) + (0,2,2).
\end{aligned}
$$

These may be generalized, taking odd and even values of n separately:

$$
\begin{aligned}
W_{2n} &= \sum_{j=0}^{n} (2n-2j, j, j), \\
W_{2n+1} &= \sum_{j=0}^{n} (2n-2j+1, j, j).
\end{aligned}
$$

In this way, explicit formulae are found for the elements in the sequence.

Quaternions and permutation matrices

Dennis Morris

The eight 8×8 matrices

$$A = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix}, \quad B = \begin{bmatrix} 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix},$$

$$C = \begin{bmatrix} 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0 \end{bmatrix}, \quad D = \begin{bmatrix} 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0 \end{bmatrix},$$

$$E = \begin{bmatrix} 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{bmatrix}, \quad F = \begin{bmatrix} 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0 \end{bmatrix},$$

$$G = \begin{bmatrix} 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0 \end{bmatrix}, \quad H = \begin{bmatrix} 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0 \end{bmatrix}$$

with matrix multiplication form the quaternion group. (These are not the only permutation matrices that form this group.)

This group has four proper subgroups:

$$\{A,B\},\ \{A,B,C,D\},\ \{A,B,E,F\},\ \{A,B,G,H\}$$

which correspond to the four parts of the quaternion $\{1,\hat\imath,\hat\jmath,\hat k\}$. We have

$$\begin{aligned}\{A,B\} &\cong \{1,-1\}, & \{A,B,C,D\} &\cong \{1,-1,\hat\imath,-\hat\imath\},\\ \{A,B,E,F\} &\cong \{1,-1,\hat\jmath,-\hat\jmath\}, & \{A,B,G,H\} &\cong \{1,-1,\hat k,-\hat k\}.\end{aligned}$$

We form the quaternion algebra (non-commutative) thus. Using the algebraic equivalences

$$[1] \lhd \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad [-1] \lhd \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

we fold these 8×8 quaternionic permutation matrices into the 4×4 quaternionic permutation matrices like so:

$$F = \begin{bmatrix} 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0 \end{bmatrix} \lhd \begin{bmatrix} 0&0&-1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&-1&0&0 \end{bmatrix}.$$

When we do this, we get

$$A = \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix},\quad B = \begin{bmatrix} -1&0&0&0\\ 0&-1&0&0\\ 0&0&-1&0\\ 0&0&0&-1 \end{bmatrix},\quad C = \begin{bmatrix} 0&1&0&0\\ -1&0&0&0\\ 0&0&0&1\\ 0&0&-1&0 \end{bmatrix},$$

$$D = \begin{bmatrix} 0&-1&0&0\\ 1&0&0&0\\ 0&0&0&-1\\ 0&0&1&0 \end{bmatrix},\quad E = \begin{bmatrix} 0&0&1&0\\ 0&0&0&-1\\ -1&0&0&0\\ 0&1&0&0 \end{bmatrix},\quad F = \begin{bmatrix} 0&0&-1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&-1&0&0 \end{bmatrix},$$

$$G = \begin{bmatrix} 0&0&0&1\\ 0&0&1&0\\ 0&-1&0&0\\ -1&0&0&0 \end{bmatrix},\quad H = \begin{bmatrix} 0&0&0&-1\\ 0&0&-1&0\\ 0&1&0&0\\ 1&0&0&0 \end{bmatrix}.$$

These matrices, of course, form the quaternion group under matrix multiplication. We note that $\{B, D, F, H\}$ are the additive inverses of $\{A, C, E, G\}$. Putting independent real variables into $\{A, C, E, G\}$ and adding them (or $\{B, D, F, H\}$) produces the more usual matrix representation of the quaternions:

$$\mathbb{H} = \begin{bmatrix} a & c & e & g \\ -c & a & -g & -e \\ -e & -g & a & c \\ -g & e & -c & a \end{bmatrix}, \quad a, c, e, g \in \mathbb{R}.$$

Of course, one could start with the smaller permutation matrices.

If we replace each 8×8 permutation matrix element with a real independent variable and sum them, but ignore the identity, we get

$$\begin{bmatrix} 0 & b & c & d & e & f & g & h \\ b & 0 & d & c & f & e & h & g \\ d & c & 0 & b & g & h & f & e \\ c & d & b & 0 & h & g & e & f \\ f & e & g & h & 0 & b & c & d \\ e & f & g & h & b & 0 & d & c \\ h & g & e & f & d & c & 0 & b \\ g & h & f & e & c & d & b & 0 \end{bmatrix}.$$

(Incidentally, this is a copy of the Cayley table of the quaternion group.) We get a matrix that satisfies all the algebraic field axioms except multiplicative commutativity and the guaranteed non-singularity. However, if we exponentiate this matrix (the Baker–Campbell–Hausdorff formula confirms this is possible), because this matrix has trace zero, we will get a matrix with determinant unity. The determinant of the exponential of the identity is only zero if the identity is zero. We thus have, when exponentiated, a non-commutative division algebra, but it is more than the quaternion algebra.

Of course, we can do the same with any non-abelian group and thus find an infinite number of non-commutative division algebras.

Problem 226.2 – Eight sins

Show that

$$\sin^4\frac{\pi}{20}+\sin^4\frac{3\pi}{20}+\sin^4\frac{7\pi}{20}+\sin^4\frac{9\pi}{20}+\sin^4\frac{11\pi}{20}+\sin^4\frac{13\pi}{20}+\sin^4\frac{17\pi}{20}+\sin^4\frac{19\pi}{20} = \frac{13}{4}.$$

Problem 226.3 – Three functions

Define three functions P, Q and R by

$$\begin{aligned} P(z) &= 1 - 24 \sum_{k=1}^{\infty} \frac{k z^k}{1 - z^k}, \\ Q(z) &= 1 + 240 \sum_{k=1}^{\infty} \frac{k^3 z^k}{1 - z^k}, \\ R(z) &= 1 - 504 \sum_{k=1}^{\infty} \frac{k^5 z^k}{1 - z^k}, \end{aligned}$$

$|z| < 1$. Show that

$$z \frac{dP}{dz} = \frac{P^2 - Q}{12}, \qquad z \frac{dQ}{dz} = \frac{PQ - R}{3}, \qquad z \frac{dR}{dz} = \frac{PR - Q^2}{2}$$

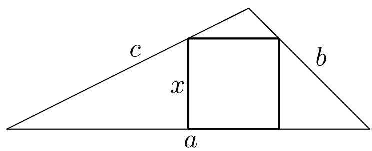
and that

$$Q^3 - R^2 = 1728\, z \prod_{n=1}^{\infty} (1 - z^n)^{24}.$$

Problem 226.4 – Three squares

Let $\mathcal{T}$ be a triangle with sides a, b, c and in-circle radius r. Let x be the side of the square such that (i) one side of the square shares a common border with side a of $\mathcal{T}$, (ii) the other two vertices of the square lies on sides b and c of $\mathcal{T}$. Define y and z similarly in terms of sides b and c respectively. Show that

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{r}.$$



Problem 226.5 – Three circles

Three circles touch each other externally and have radii a, b and c. A fourth circle of radius x touches the other three externally. Show that

$$\sqrt{\frac{a+b+x}{c}} + \sqrt{\frac{b+c+x}{a}} + \sqrt{\frac{c+a+x}{b}} = \sqrt{\frac{a+b+c}{x}}.$$

Solution 223.3 – Factorization

For which integer values of d does $x^4 - x - d$ factorize?

Steve Moon

Let $f(x) = x^4 - x - d$, $d \in \mathbb{Z}$. We look for factorizations of the form:

case (i): $f(x) = (x-a)g(x)$, $a \in \mathbb{Z}$, $g(x)$ a cubic polynomial in x which may or may not factorize further;

case (ii): $f(x) = (x + kx + l)(x^2 + mx + n)$, $k, l, m, n \in \mathbb{Z}$, and neither factor factorizes further.

Case (i)

If $f(x)$ factorizes into $f(x) = (x-a)g(x)$, then there exists some integer a such that $f(a) = a^4 - a - d = 0$. Hence $d = a^4 - a$, $x \in \mathbb{Z}$. Examples:

a	d	$f(x)$
-3	84	$(x+3)(x^3 - 3x^2 + 9x - 28)$
-2	18	$(x+2)(x^3 - 2x^2 + 4x - 9)$
-1	2	$(x+1)(x^3 - x^2 + x - 2)$
0	0	$x(x^3 - 1) = x(x-1)(x^2 + x + 1)$
1	0	$(x-1)(x^3 + x^2 + x)$
2	14	$(x-2)(x^3 + 2x^2 + 4x + 7)$
3	78	$(x-3)(x^3 + 3x^2 + 9x + 26)$

Case (ii)

We have

$$\begin{aligned} f(x) &= (x^2 + kx + l)(x^2 + mx + n) \\ &= x^4 + (k+m)x^3 + (l + n + km)x^2 + (kn + lm)x + nl. \end{aligned}$$

Equate coefficients with $f(x) = x^4 - x - d$; we have

$$k + m = 0, \qquad l + n + km = 0, \qquad kn + lm = -1, \qquad nl = d.$$

From the first two $k = -m$ and so

$$l + n - m^2 = 0. \tag{1}$$

From the first and the third, $-mn + lm = -1$. Therefore $m(l-n) = -1$ and hence $m = 1/(n-l)$. Hence

$$m^2 = \frac{1}{(n-l)^2}. \tag{2}$$

From (1) and (2), we have

$$(n-l)^2(n+l) \;=\; 1.$$

In particular, there are no solutions for $n = l$ (so d cannot be a square).

If $n \neq l$, $n, l > 0$, then $n-l$ and $n+l$ are both integers and $n-l \neq n+l$. But both factors cannot divide 1. Hence there are no solutions.

If we put $n = 0$, then $l = 1$, $d = 0$, $m = -1$, $k = 1$ and we get $f(x) = (x^2+x+1)(x^2-x) = (x^2+x+1)x(x-1)$, which we already found in case (i) for $d = 0$.

So the values of d for which $f(x) = x^4 - x - d$ factorizes are all of the form $a^4 - a$, $a \in \mathbb{Z}$.

Archaeology

Tony Huntington

Did anyone watch the TV drama series *Boneshakers* recently? It was a brave attempt to make archaeologists into exciting people with a Life instead of their stereotype of Very Sad and Boring Nerds. The final episode included one of the best dialogue lines I have heard in many years. Just before one of the main characters joined in a fight with the baddies, he listed a series of dates and events from British history and then yelled in a menacing voice:

"Don't mess with me ... I'm an archaeologist."

This ranks, in my books, alongside perhaps the most terrifying phrase ever uttered by an Angel of Mercy:

"Trust me ... I'm a nurse."

These two 'sound bites' set me wondering about other similar lines to strike terror into the hearts of even the bravest of souls. I offer the following as potential candidates:

"Honestly ... I'm a lawyer."

"I know what I'm talking about ... I'm a politician."

"Let me help you ... I'm from the government."

"I know what I'm doing ... I'm an engineer."

And of course,

"Count on me ... I'm a mathematician."

Beware the percentage

John Bull

Recently, with the credit crunch and the financial crisis, we hear the gyrations of the stock market reported on the news: today down five percent, then up eight percent, then down three percent, etc. Suppose we hear that the stock market fell by five percent, and then the next day we hear that it rose by five percent. We breathe a sigh of relief. At least it fully recovered. Well actually, no it didn't.

Suppose on day zero we start with a sum s, and on day zero the market falls by p percent. Then at the start of day 1 we have $s(1-p/100)$. Now suppose on day 1 the market rises by p percent, then at the start of day 2 we have $s(1-p/100)(1+p/100)$. Over successive days we have the following sequence:

$$
\begin{array}{ll}
\text{day } 0: & s, \\
\text{day } 1: & s\,(1-p/100), \\
\text{day } 2: & s\,(1-p/100)(1+p/100), \\
\text{day } 3: & s\,(1-p/100)^2(1+p/100), \\
\text{day } 4: & s\,(1-p/100)^2(1+p/100)^2, \\
\ldots, & \\
\text{day } n \text{ with } n \text{ odd:} & s\,(1-p/100)^{(n+1)/2}(1+p/100)^{(n-1)/2}, \\
\text{day } n \text{ with } n \text{ even:} & s\,(1-p/100)^{n/2}(1+p/100)^{n/2}.
\end{array}
$$

Suppose we start with 100 points, and go down 5 percent, up 5 percent, down 5 percent, up 5 percent, etc, then on successive days the profile would be:

day 0:	100.000000,		
day 1:	95.000000,	day 6:	99.251873,
day 2:	99.750000,	day 7:	94.289280,
day 3:	94.762500,	day 8:	99.003744,
day 4:	99.500625,	day 9:	94.053557,
day 5:	94.525594,	day 10:	98.756234.

After about 550 trading days, or 2.2 years, the market would be down to around 50; that is, it would have halved. After about 2500 trading days, or 10 years, it would be down to around 5; that is, to 5 percent of its starting value. After infinite time it falls to zero.

It matters little if the market rises first and then falls; that is, up 5 percent, down 5 percent, up 5 percent, down 5 percent, etc. The fate is the same. In this case the sums on successive days would be

$$\begin{array}{ll} \text{day } n \text{ with } n \text{ odd:} & s\,(1+p/100)^{(n+1)/2}(1-p/100)^{(n-1)/2}, \\ \text{day } n \text{ with } n \text{ even:} & s\,(1+p/100)^{n/2}(1-p/100)^{n/2}. \end{array}$$

A fall of 5 percent would need a rise of at least a 5.3 percent to maintain equilibrium. A rise of 5 percent would be corrected by a fall of no more than 4.7 percent. So in a volatile market, with swings of 5 percent not uncommon, the falls have greater significance than the rises. The mental, rule-of-thumb adjustment needed to correct back to square one is about plus or minus 0.3 percent.

Another common fallacy is that a rise of p percent, followed by a second rise of q percent, produces a rise of $p+q$ percent. No it doesn't; it produces a rise of $p+q+pq/100$ percent. So two successive rises of 5 percent produce an overall rise of 10.25 percent. Similarly, successive falls produce slightly greater losses than one might imagine.

None of this is particularly advanced mathematics, but it is interesting how news reports can be misleading, even to the mathematician who doesn't take care.

TF writes. There is a similar second-order differential effect which is known to anyone who has ever had an interest in horses, especially the racing thereof and the wagering thereon. Originally the process of betting was simple. Punters bet, horses raced, bookmakers paid the winners. However, all that changed when the Government decided to tax betting.

A simple 10 percent tax was levied on all monies paid out to punters by bookmakers. So see how it works, suppose you bet £20 on a horse to win a certain race. It wins! The odds are twenty-to-one. So the bookmaker must pay you £420. But the Government takes its share and the payout is reduced by £42 to £378. A significant part of your winnings is lost. This is even more serious if you had backed the favourite (in another race) at the short odds of ten-to-one on. In this case your return from the bookmaker when the horse wins, £22, is reduced by £2.20 to £19.80—you have actually lost money!

As a service to punters, most leading bookmakers once offered you the chance to pay the 10 percent tax on your stake. You pay the bookmaker £22 instead of £20 but your winnings of £420 remains untaxed, and you are extremely happy. However, this practice has been banned by law, since, contrary to what the example might lead one to believe, it actually works to the bookmaker's advantage. Can you see why?

Gigantic prime triplets

Tony Forbes

You may remember back in December 2002 we defined a *titanic* prime as a non-composite number consisting of at least 1000 decimal digits (Titanic prime quintuplets, M500 **189**, pages 12–13). In the same article I reported the discovery of a large prime quintuplet:

$$31969211688 \prod_{\substack{p\,<\,2400\\ p \text{ prime}}} p \;+\; 16061 \;+\; d, \qquad d = 0, 2, 6, 8, 12,$$

by Norman Luhn, and I was sufficiently impressed to place all 1034 digits of the first number on the front cover of that issue.

This novel and interesting usage of 'titanic' was introduced in an article by Samuel Yates in 1985. Well, the next power of ten up from one thousand is ten thousand, and, as you can imagine, there is also a technical term for primes of this magnitude. In 1992, when titanic primes were beginning to become commonplace, Yates again realized that a new word was needed; and so he made another definition.

> A *gigantic* prime is defined as a prime number which has at least 10000 decimal digits.

This same definition is used by Chris Caldwell in his database of large primes at http://primes.utm.edu/. You will obviously want to know that the smallest gigantic prime is $10^{9999} + 33603$. This was already 'well known' ever since computer programmers learnt how to do serious arithmetic, but the world had to wait until 2003 for a proof—by Jens Franke, Thorsten Kleinjung and Tobias Wirth.

Now, as I write this, two truly remarkable things have happened.

First, I was most surprised when the same **Norman Luhn** wrote to me on 13th October 2008 to report a new gigantic probable prime triplet,

$$2072644824759 \cdot 2^{33333} + d, \qquad d = -1, 1, 5, \tag{$*$}$$

at 10047 digits beating his own previous world record of 6223 digits (M500 **220**, cover). The first two members ($d = \pm 1$), each being a factorizable number plus or minus one, are easily proved to be prime by elementary methods. However, the third ($d = 5$) is not of this form, and therefore its primality proof would require a much greater effort. And at 10047 digits, it was at the time not at all clear how this could be done without about 6 months to a year of computing.

Then surprise turned into astonishment when a few weeks later, on 17th November, Norman reported that his third number had been verified in record time by **François Morain** with a new version of his elliptic curve primality prover, FastECPP. Using a cluster of nine AMD Athlon-64 3400^+ processors, Morain achieved the primality proof in a record 111 days of computer time and was able to deliver the required primality certificate in only three weeks, thus confirming $(*)$ as true prime triplet.

There is an element of history repetition here. A long time ago I reported the 1041-digit *probable* prime triplet

$$2^{3456} + 5661177712051 + d, \qquad d = 0, 2, 6,$$

found in July 1995 (M500 **145**, page 19). If the primes could have been verified quickly, it would have been the first ever titanic example of its kind. However, I had to wait a little longer than Norman—actually more than two years longer—for the primes to be certified by the same François Morain in January 1998 (M500 **161**, page 13).

Norman's triplet is printed full on the front cover of this magazine.

Some more prime number records, as at 18 December 2008. Notation: $x\# = \prod_{2 \le p \le x,\ p \text{ prime}} p$.

Largest prime: $2^{43112609} - 1$, August 2008, Edson Smith, George Woltman, Scott Kurowski, *et al.* (GIMPS), 12978189 digits.

Largest prime twins: $2003663613 \cdot 2^{195000} \pm 1$, January 2007, Eric Vautier, Dmitri Gribenko, Patrick W. McKibbon, Michaek Kwok, Andrea Pacini and Rytis Slatkevicius, 58711 digits.

Largest prime quadruplets: $4104082046 \cdot 4800\# + 5651 + d$, $d = 0$, 2, 6, 8, April 2005, Norman Luhn, Primo, 2058 digits.

Largest prime quintuplets: $283534892623 \cdot 2500\# + 1091261 + d$, $d = 0$, 2, 6, 8, 12, April 2006, Norman Luhn, 1069 digits.

Largest prime sextuplets: $328481121285 \cdot 1000\# + 16057 + d, d = 0$, 4, 6, 10, 12, 16, January 2006, Norman Luhn, 427 digits.

Largest prime septuplets: $251733155478 \cdot 650\# + 1146779 + d$, $d = 0$, 2, 8, 12, 14, 18, 20, January 2006, Norman Luhn, 282 digits.

Largest prime octuplets: $330846961 \cdot 503\# + 349129635971 + d$, $d = 0$, 2, 6, 8, 12, 18, 20, 26, February 2008, Jens Kruse Andersen, 218 digits.

Largest prime nonuplets: $3336884 \cdot 331\# + 80877403191701 + d, d = 0$, 2, 6, 8, 12, 18, 20, 26, 30, September 2007, Dirk Augustin and Jens Kruse Andersen, 140 digits.

Largest prime decuplets: $24698258 \cdot 239\# + 28606476153371 + d$, $d = 0$, 2, 6, 8, 12, 18, 20, 26, 30, 32, Sept. 2004, Jens Kruse Andersen, 104 digits.

Largest prime 11-tuplets: $24698258 \cdot 239\# + 28606476153371 + d$, $d = 0$, 2, 6, 8, 12, 18, 20, 26, 30, 32, 36, September 2004, Norman Luhn and Jens Kruse Andersen, 104 digits.

Largest prime dodecuplets: $8486221 \cdot 107\# + 4549290807806861 + d$, $d = 0$, 2, 6, 8, 12, 18, 20, 26, 30, 32, 36, 42, May 2006, Dirk Augustin and Jens Kruse Andersen, 50 digits.

Largest prime 14-tuplets: $381955327397348 \cdot 80\# + 18393209 + d$, $d = 0$, 2, 8, 14, 18, 20, 24, 30, 32, 38, 42, 44, 48, 50, December 2007, Norman Luhn, 46 digits. Includes largest prime 13-tuplets.

Largest prime 15-tuplets: $107173714602413868775303366934621 + d$, $d =$ 0, 2, 6, 8, 12, 18, 20, 26, 30, 32, 36, 42, 48, 50, 56, April 2008, Jens Kruse Andersen, 33 digits.

Largest prime 18-tuplets: $11298510058634407483251313 + d$, $d = 0$, 4, 6, 10, 16, 18, 24, 28, 30, 34, 40, 46, 48, 54, 58, 60, 66, 70, December 2008, Jaroslaw Wroblewski, 26 digits. Includes largest prime 16- and 17-tuplets.

Problem 226.6 – Two bombs

There is a collection of bombs, all of identical construction. Your task is to determine the minimum height from which a bomb must be dropped for the detonation mechanism to work. Great accuracy is not necessary. Measurement to the nearest 10 feet is all that is required. And fortunately there is a convenient very tall building whose floors are spaced ten feet apart.

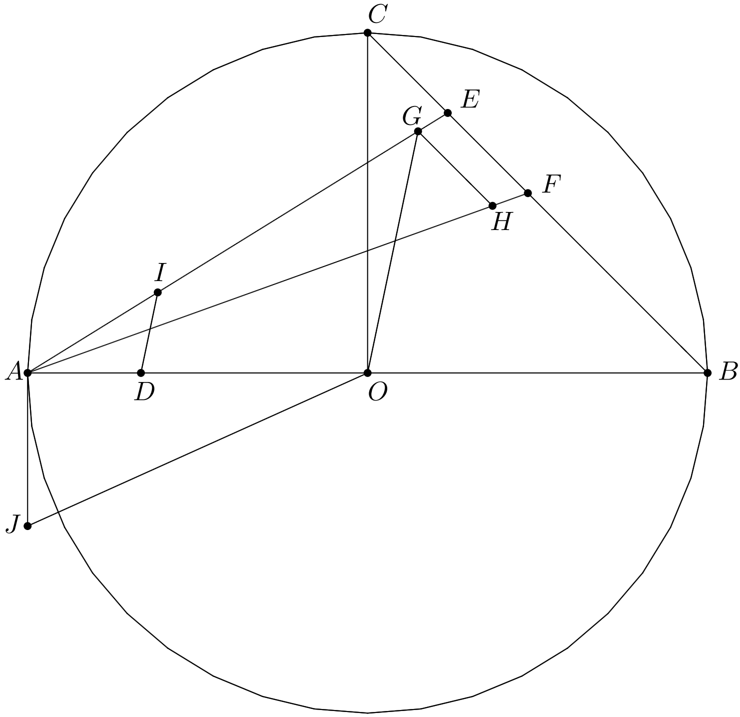
If you are given just one bomb to test, all you can do is this, starting at $n = 1$. Drop the bomb from floor n and see what happens. If it explodes, report '$10n$ feet'. If not, retrieve the bomb and repeat the test from floor $n + 1$. You may assume that a bomb which survives being dropped will not sustain any damage, and therefore a future test will be valid. On the other hand, once the bomb explodes it cannot be used again.

Now suppose instead you are given *two* test bombs. How can you improve your strategy?

Problem 226.7 – Squaring the circle

S. Ramanujan

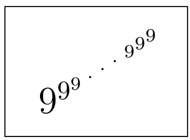
In the diagram, AOB is a diameter of the circle with centre O, The radius of the circle is $|OA| = 1$. Also CO is perpendicular to AB, $|AD| = |CE| = |EF| = \frac{1}{3}$, $|AH| = |AE|$, GH is parallel to EF, DI is parallel to OG, AJ is perpendicular to AB and $|AJ| = |AI|$. Show how to construct the diagram with ruler and compasses only. What is $3\sqrt{|OJ|}$?



Problem 226.8 – 999 nines

Emil Vaughan

What are the last nine digits of the number whose value is an exponential tower of 999 nines?



Contents