NUMBERS COUNT

Mike Mudge investigates prime number density among simple polynomials.

This article concentrates upon only two questions from what is readily seen to be an immense area for conducting empirical research in number theory. Interested readers are encouraged from the outset to consider more general circumstances when writing programs and analysing their output.

Question 1 When is a quadratic polynomial with integer coefficients prime?

We consider the quadratic polynomial $f(x)=ax^2+bx+c$; where a, b and c are given integers and x takes integer values from 0 to N. V(f(x),N) is defined to be the number of x-values for which the modulus of f(x) is either prime or unity.

Test Case. For the Euler Polynomial $f(x)=x^2+x+41$ it is found that V(f(x),1000)=581.

E.Karst, New quadratic forms with high density of primes *Elem d Math* vol 28 1973, pp116-118, found a polynomial $g(x)=ax^2+c$ for which V(g(x),1000)=598.

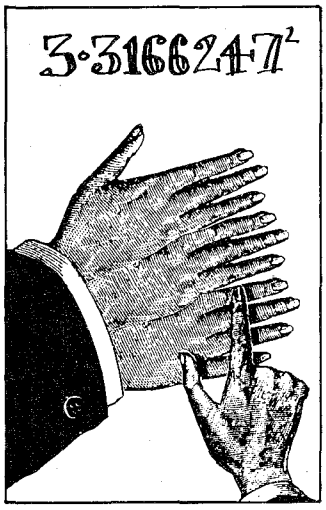
What is it? Can V(f(x),1000) be greater than 598 for quadratic f(x)?

Question 2 For how long can a polynomial of the form x^n+b remain composite (non-prime) where n and b are given positive integers and x takes the values 1,2,3,4...?

Consider the polynomial x^6+1091; this is composite for x=1,...3905, (Shanks, 1971).

However there exists a value for b such that x^6+b is composite for x=1,...7979. What is it?

Consider the polynomial $x^{12}+4094$; this is composite for x=1,2,...170624; however, there exists a value for b such that $x^{12}+b$ is composite for x=1,2,...616979. What is it? See



for example KS McCurley, The Smallest Prime Value of x^n+a, *Canadian J Math*, vol 38, 1986, pp925-936, also Polynomials with no small prime values, *Proc Amer Math Soc* vol 97, 1986, pp393-395.

Readers are encouraged to construct programs to evaluate firstly $V(ax^2+bx+c,M)$ for given a,b,c and M, and secondly the length of the initial composite value interval for x^n+b given n and b.

Test data for both programs and suggested targets for an initial search are to be found in the above text.

Readers are further invited to send their attempts at these problems to Mike Mudge, 'Square Acre', Stourbridge Road, Penn, South Staffordshire WV4 5NF, tel: (0902) 892141 to arrive by 1 December 1988. It would be appreciated if such submissions contained a brief description of the programs and a summary of the results obtained in a form suitable for publication in *PCW*.

These submissions will be judged using subjective criteria, and a prize will be awarded by *PCW* to the 'best' contribution received by the closing date.

Please note that submissions can only be returned if a suitable stamped addressed envelope is provided.

Review, April: Cryptology

This subject area attracted a remarkable response, including a detailed communication from Athens and several from Australia. Many submissions were quite sophisticated and all concerned are to be congratulated upon the interest which they have shown in this topic. It is hoped to produce a related Numbers Count article in the near future; meanwhile here is a selection of interesting points.

Firstly those readers who wish to study codes and cyphers in depth should consider contacting The American Cryptogram Association (ACA) at 12317 Dalewood Drive, Wheaton, Maryland 20902, USA. The Association presently has about sixteen members in the UK.

An interesting program in turbo BASIC suitable for an Amstrad PC1512 has been supplied by MR Barge, whilst the following readers' challenge is due to TK Boyd:

A3 123 B4 135 93 13D BF 13F 81 121 5A 11E 12D 91 B0 9A C0 129 89 67 F9 92 2A F4 E1 11D BC 108 7F 107 69 147 117 66 65 7D E5 108 116 92 9E B7 11A D6 AE 92

It was generated on an Acorn BBC B in Basic II — 'it may matter.' Note: TK Boyd also markets a full-blown 'user-friendly' encryptation package. Details of either of these are available on request.

This month's very worthy prizewinner is Mr Anthony Quas of 635 King's College, Cambridge, CB2 1ST, whose program was written initially in APL· 68000 on a SAGE and then transferred to APL*PLUS/PC on a PC, and finally into I-APL/PC.

Anthony will be delighted to discuss his work further with any interested readers, and can readily explain the underlying abstract algebra. A significant contribution of this work is the extension of the scope of the exponentiation cipher to deal with products of distinct primes.

An introduction to many aspects of this work can be obtained from *Cryptography: A primer*, by AG Konheim, Wiley-Interscience, New York 1981, whilst more experienced readers may consult PJ Hoogendoorn, On a Secure Public-key Cryptosystem in Computational Methods in Number Theory by HW Lenstra jr and R Tijdeman, part I pp159-168, *Math Centre Tracts 154*, Amsterdam, 1982.

Mike Mudge welcomes correspondence on any subject within the areas of number theory and other computational mathematics. Particularly welcome are suggestions, either general or specific, for future Numbers Count articles; all letters will be answered in due course.

Isolated readers can be put in contact with others sharing the same interests. However, greater efficiency regarding published problems should result from contacting the prizewinner.

UK BULLETIN BOARDS

The list of UK Bulletin Boards is updated monthly. People wishing to be included should contact the *Personal Computer World* editorial office.

London

Brixton ITeC (01) 735 6153
24 hrs; 1275

CIX (01) 399 5252
24hrs; 3-24; multi-user; conferencing

Communitel (01) 968 7402
24 hrs; 1275v

Crystal Tower (01) 886 2813
24 hrs; 3-24
Gen interest; Apple & IBM

Dark Crystal Fido
(01) 207 2989; 24 Hrs; 3-12

Distel (01) 679 1888
24 hrs; 300; Display electronics- Commercial 3/1275 on 01 679 6183

Gnome at home (01) 888 8894
24 hrs; 1275v

Hackney BBS (01) 985 3322
24 hrs; 1275v

Health data (01) 986 4360
24 hrs; 1275v

Infotel ROS (01) 581 3376
24hrs; 3/1275

Kybernesis (01) 673 7294
6pm-8am; 3-24 Support for charity computer users

Link Fido (01) 659 6992
24 hrs; 3-12

London U'gnd (01) 863 0198
24 hrs; 3-24 Wildcat BBS

Marctel (01) 346 7150
24 hrs; 3/1275 FBBS system

MBBS Mitcham (01) 648 0018
24 hrs; 3/1275

Metrotel (01) 941 4285
24 hrs; 1275v

NNBBS London (01) 455 6607
24 hrs; 3/1275

Nottingdale Tec Ctr
(01) 968 6033; 24hrs; 1275v; Communitel system

OSI Lives (01) 429 3047
24 Ring back; 300

PC Access (01) 853 3965
24 hrs; 3-24 For PC users

PD-SIG Headquarters*
(01) 864 2633; Greenford; 24hrs; 3-24M

Prometheus (01) 300 7177
24 hrs; 1275v; Astronomers' SIG

Skull's Tower (01) 943 1194
24 hrs; 3/1275; IBM etc s/w Towernet

Taecom (01) 573 8822
MF: 7pm-8am; WE:all day Sun 300 Interak micro section

TBBS Rovoreed (01) 542 4977
24 hrs; 3-24

TBBS London (01) 348 9400
24 hrs; 3-12

Techno Line (01) 450 9764
24 hrs; 1275v; Commercial

Techno-line 2 (01) 452 1500
MF: evenings; WE:24 hrs 1275v Commercial

The Star BBS (01) 586 6882
24 hrs; 3/1275; Atari ST area

The Village (01) 464 2516
24 hrs; 3-24
Atari 520ST based
24 hrs; 3/1275

WBBS Wimbledon (01) 542 3772
Sat 7pm - Mon 8am; 3/1275

The South East

Acorn BBS; Cambridge
(0223) 243 642 24 hrs; 1275v

Airtel - TBBS (0342) 717 800
W Sussex; 24 hrs; 3-24; Pilots' area

Andrew's Fido; Aylesbury
(08444) 4833; 24hrs; 3/1275
IBM-based system

Apple Crackers Basildon
(0628) 778956; 24hrs; 3-1275
Apple II/IIGS; also on 781318 and 771724

ARCNET; Colchester
(0376) 518 818 24 hrs; 300

Audio Output, Weybridge
(0932) 244906; 24hrs; 3/1275
Viewdata & scrolling

Banat Board; Oxford
(0993) 898 441 24 hrs; 3-24
FidoNet UK coordinator
multi-line TBBS

BBS09; Portsmouth
(0705) 736 025 24hrs; 3-12; OS9; Sci-Fi, Dragon, CoCo

BITEC; Basildon (0268) 22 177
24 hrs; 1275v

BOOG BB; Fleet; Hants
(0252) 626 233; 24 hrs; 3/1275
Osborne; MS-DOS; CP/M areas

C A T S Fido; Maidenhead
(0628) 824 852; 24 hrs; 3/1275
V22/bis coming

C View Rochford; Kent
(0702) 54 6373; 24 hrs; 1275v

CATS BBS*; Maidenhead
(0628) 824852; 24hrs; 3/1275
V22bis coming

CP/M User Group; Windsor
(0753) 868 196; 24 hrs; 3-24
CP/M and MS-DOS software

Datasoft Opus; Ilminster
(04605) 4615; 24 hrs; 3-24
Inc Datatalk Support area

Dr Solomon's Fido; Amersham
(0494) 724 946; 24 hrs; 3-24
mostly for IBM programmers