School of Mathematics UEA NORWICH

Elliptic Divisibility Sequences

Suppose u[n] denotes the nth term of an integer divisibility sequence. This means all the terms are integers and

u[n] divides u[m] whenever n divides m.

The sequence is said to be an *Elliptic Divisibility Sequence* (hereafter EDS) if it satisfies the recurrence relation

$$u[m-n]u[m+n] = u[m+1]u[m-1]u[n]^2 - u[n+1]u[n-1]u[m]^2$$

for all $m \geq n \geq 0$. In Morgan Ward's terminology, the sequence is proper if u[0]=0, u[1]=1 and u[2]u[3]u[4] is non-zero. We will always assume our EDSs are proper in that sense.

There are some trivial examples such as the integers 0,1,2,3,4.. but non-trivial examples abound. An EDS which occurs a lot starts 0,1,1,-1,1, then continues

2,-1,-3,-5,7,-4,-28,29,59,129,-314,-65,1529,-3689,-8209,-16264,833313,113689,-620297,

2382785,7869898,7001471,-126742987,-398035821,168705471,-7911171597,...

This is sequence A006769 in the On-Line Encyclopedia of Integer Sequences maintained by Neil Sloane.

It might not be obvious but the sequence does have a growth rate: The term log|u[n]| is approximately cn^2 where c=.02555.. This growth rate is intimately related to the global height of a rational point on an elliptic curve. A recent paper gives more details.

How do you actually calculate values of an EDS? The relation above can be broken down into two simpler relations

$$u[2n+1] = u[n+2]u[n]^3 - u[n-1]u[n+1]^3 \text{ and}$$

$$u[2n]u[2] = u[n](u[n+2]u[n-1]^2 - u[n-2]u[n+1]^2).$$

Once the terms u[0]=0, u[1]=1, u[2], u[3] and u[4] are specified, these formulae can be used to compute all the other terms in the sequence. For example, the formulae above give

$$u[5]=u[4]u[2]^3-u[1]u[3]^3 \text{ and}$$

$$u[6]u[2]=u[3](u[5]u[2]^2-u[1]u[4]^2).$$

In our earlier example, we get $u[5]=1.1^3-1.(-1)^3=2$ and $u[6].1=(-1).(2.1^2-1.1^2)=-1$ and so on. One of the amazing things about EDSs is that if you specify the first five terms (and make sure u[2]|u[4]) then your sequence will always be a divisibility sequence if you use these two rules to calculate the rest of the terms.

Rachel Shipsey has recently written a very interesting thesis about EDSs which includes some applications to cryptography. EDSs are connected to heights of rational points on elliptic curves and the elliptic Lehmer problem . This was considered in the paper. The Chudnovskys considered prime values of EDSs in the 80's and a recent paper discusses their conjecture. For a more down to earth treatment of this material, consult this article.

Somos Sequences

EDSs are special cases of a class of sequences which satisfy bilinear recurrences. They are called *Somos Sequences* after Michael Somos. Jim Propp is creating a web page which gathers together details on these sequences.

This page maintained by: g.everest@mth.uea.ac.uk

Last updated: 10/15/2001 15:13:10

School of Mathematics UEA NORWICH

Elliptic Divisibility Sequences and the Elliptic Lehmer Problem

The canonical height of an algebraic point on an elliptic curve

A paper has recently appeared which shows how EDSs can be used to search for small height points in connection with the elliptic Lehmer problem. So we start by recalling the statement of this problem. For an excellent introduction to elliptic curves, consult Joe Silverman's two books The Arithmetic of Elliptic Curves and Advanced Topics in the Arithmetic of Elliptic Curves.

Let E denote an elliptic curve defined over an algebraic number field K. As usual, we denote the addition on the group E(K) of K-rational points of E by + and the group identity as O. Then O is the point at infinity on the projective curve. There is a function h called the *global canonical height* which satisfies the properties:

(1) for all P,Q in E(K), $h(P+Q)+h(P-Q)=2h(P)+2h(Q)$,

(2) $h(Q)=0$ if and only if Q is a torsion point.

Property (1) is called the parallelogram law. This height function is the analogue of the usual height of an algebraic number, which we will review later. In particular, problems such as the Lehmer problem are thought to have analogues. Although refinements of the basic problem exist, we can state the elliptic Lehmer problem as the following. Let d denote the degree of the field K. Then there is a constant $c>0$ which does not depend on E,K or Q such that

$$h(Q) \geq c/d \text{ provided Q is not a torsion point.}$$

Before we give some examples, it will help to agree some notation. An elliptic curve is given by a Weierstrass equation,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

This equation is usually codified in terms of the coefficients as a vector $[a_1,a_2,a_3,a_4,a_5]$. A (non-identity) point is usually written [x,y]. In the pari-GP calculator, this is the way to enter curves and points.

Suppose K=Q the field of rationals and Q lies in E(Q). The elliptic Lehmer problem implies that the global heights of all non-torsion rational points are uniformly bounded below. What are the smallest values currently known? The following were extracted by Noam Elkies from tables of elliptic curves made by John Cremona and they show how small the height can be.

1.E is [0,0,0,-412,3316], Q=[-18,70] has h(Q)=.00563..

2.E is [0,1,1,-310,3364], Q=[-19,-53] has h(Q)=.00670..

3.E is [1,0,0,-1415,20617], Q=[-26,213] has h(Q)=.00926..

The Elliptic Divisibility Sequence generated by 1. is

0,1,140, -1372000, -268912000000,1844736320000000000,...

It is sequence A058939 in The On-Line Encyclopedia of Integer Sequences maintained by Neil Sloane. Recently, Elkies has posted a list with some even smaller heights.

Algebraic Points

Silverman has a fast algorithm for computing heights of rational points on elliptic curves. There are no versions of Silverman's algorithm currently implemented over general number fields but some special calculations have been made. Let K=Q(i) where i=sqrt(-1). Here the elliptic Lehmer problem implies a bound for 2h(Q) so we give some examples of this value which we obtained from Cremona.

1.E is [0,1-i,i,-i,0], Q=[0,0] and 2h(Q)=.023..

2.E is [1,1+i,i,0,0], Q=[-1,1] and 2h(Q)=.0175..

In the paper referred to above, it was argued that EDSs provide a natural way of searching for small height points. The paper contains the following examples.

1.The field is Q(w) where w is a non-trivial cube root of 1. The curve E is [0,0,0,-243,3726+10368w] and the point is [3-12w,-108w^2]. The global height is .01032.. Although the curve might look a bit complicated, it actually arose from a simple EDS: The first 5 terms are 0,1,1+w,1+w,1+w,..

2.The field is Q(u) where u=(1+sqrt(5))/2. The curve is [0,0,0,-2214+1215u,40878-23328u] and the point is [3-9u,108-108u]. The global height is .00971.. Again, this comes from a simple sequence which begins 0,1,1-u,-2+u,5-3u,..

So far, nobody has found a value of dh(Q) below the smallest value known in the rational case.

Morgan Ward gives formulae for converting an EDS to a point on an elliptic curve. They can be found in his paper 'Memoir on elliptic divisibility sequences' Amer. J. Math. 70 (1948), 31-74. This paper is a must-read if you plan to find out more about EDSs. You can view these formulae by following this link.

The Projective Height

Let a denote an algebraic number and say it generates the number field K. The so called *projective height* is the quantity

$$h(a) = \Sigma_v \log \max\{1,|a|_v\},$$

where the sum runs over all the valuations of K. Notice that Kronecker's Theorem implies h(a)=0 if and only if a is a root of unity - in other words, a torsion point of the multiplicative group K*. The clasical Lehmer problem asks whether the non-zero values of the height are uniformly bounded below by

$$h(a) \geq c/d.$$

For more information about Lehmer's problem, consult the book .

Examples

1.If K is totally real then the non-zero heights are bounded below by log((1+sqrt(5))/2). So a stronger form of the Lehmer problem is true for totally real numbers, where the lower bound is even independent of the degree.

2.Suppose a is non-reciprocal then we can take c to be the log of the root of x^3-x-1 outside the unit circle. To say a is non-reciprocal means that the set of conjugates of a is different from the set of conjugates of 1/a.

3.No smaller positive value of c has been found than that coming from the 10th degree polynomial

$$x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1.$$

The roots of this polynomial are reciprocal. The minimal polynomial of a reciprocal algebraic number is symmetric in the sense that its sequence of coefficients reads the same backwards and forwards.

Perhaps it is possible to prove special cases of the elliptic Lehmer problem.

Using the projective height, we can write down Tate's formula for the global height h(Q) of a point Q. It is

$$h(Q) = \lim 4^{-n} 1/2\ h(x(2^n Q)).$$

Searching for Small Heights

It is known that the global height of a K-rational point on an elliptic curve is invariant under isomorphism. This is helpful in cutting down the searching. It means we only need to look for integral points for example.

A group of us have recently started to search using elliptic divisibilty sequences. Every integral point on an elliptic curve gives rise to an EDS. Given the equation of the curve as above, suppose each a[i] in O_K, the ring of integers of K. Define

$b_2 = a_1^2+4a_2$,
$b_4 = 2a_4+a_1a_3$,
$b_6 = a_3^2+4a_6$,
$b_8 = a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2$.

Define a sequence of polynomials in $O_K[x,y]$ as follows: F[0]=0, F[1]=1, and

$F[2] = 2y+a_1x+a_3$,

$F[3] = 3x^4+b_2x^3+3b_4x^2+3b_6x+b_8$,

$F[4] = F[2](2x^6+b_2x^5+5b_4x^4+10b_6x^3+ 10b_8x^2+(b_2b_8-b_4b_6)x+b_4b_8-b_6^2)$.

These polynomials are called *division polynomials*. For more information about these, and about elliptic curves in general, consult Silverman's books. Now define inductively

$F[2n+1] = F[n+2]F[n]^3-F[n-1]F[n+1]^3$ and
$F[2n]F[2] = F[n](F[n+2]F[n-1]^2-F[n-2]F[n+1]^2)$

If the point [x,y] is a non-identity element of E(K) then we obtain a sequence of numbers u[n] = F[n]. If the point started as an integral point then all the numbers u[n] will be integral and they form an EDS.

If D denotes the discriminant of the curve than we have shown that we can get at the height using quite simple formula. Let N denote the field norm from K to Q. Let T denote the set of primes which divide N (D). Let e[n]=|N(u[n])| and f[n] = the T-free part of e[n].

Then the global height is

$$1/d \lim 1/n^2 \log f[n],$$

where d denotes the degree of K over Q. For a proof, see the paper. The method will not give very high accuracy but it does give accuracy to 4 or 5 sig figs even for n=100. It is also easy to implement because it only requires polynomial arithmetic, such as is available in pari-gp.

This page maintained by: g.everest@mth.uea.ac.uk

Last updated: 05/06/2003 06:34:06

School of Mathematics UEA NORWICH

Prime Values of Elliptic Divisibility Sequences

If u[n] denotes the n-th term of an EDS then u[n] grows very quickly. In fact

$$\log|u[n]| \sim cn^2.$$

Chudnovsky and Chudnovsky considered some EDSs specified by writing down their first five terms and examined these sequences for prime terms. Since u[n] is a divisibility sequence, which grows so quickly, it is sufficient to examine prime occurence of terms u[n] with n prime. The sequences considered by the Chudnovskys are specified below by giving the first 5 terms, as well as the constant c and the occurrence of prime values for prime n up to 100.

0,1,1,1,-2	0.0560	5,7,11,13,23,61,71
0,1,1,1,6	0.1107	5,7,13,23,43,47
0,1,2,1,4	0.1262	5,7,71
0,1,1,2,7	0.1311	11,17,73
0,1,1,1,-9	0.1383	7,47,79
0,1,1,1,10	0.1432	7,13,41,61
0,1,1,4,1	0.1730	71,79
0,1,1,4,3	0.1737	5,7,13,53,71
0,1,1,5,2	0.2010	7,43

Some of the primes in this table are very large. For example, the term u[79] in the third sequence from the end is a prime with 469 decimal digits. It might look as though we should be able to keep computing terms and find larger and larger primes. But if you run the sequences out to n=500 you find no new primes. In a recent paper, there is a heuristic explanation of why these sequences should stop producing primes beyond a certain point. This also explains why there should be a uniform bound on the number of primes. A proof of finiteness under a hypothesis on 2-torsion is obtainable here.

Other Models

Suppose we ask the same question for an elliptic curve in homogeneous form,

$$x^3 + y^3 = c,$$

for a non-zero rational c. Suppose P is a non-torsion rational point. Write $x(nP)=A_n/B_n$ for integral A_n and B_n. The paper just referred to gives a proof that only finitely many terms B_n are prime.

Zsigmondy's Theorem

For the Mersenne sequence $M_n=2^n-1$, every term has a primitive divisor after n=6. A primitive divisor of M_n is a prime divisor which does not divide M_m for any smaller m. In a recent paper Igor Shparlinsky and I prove Zsigmondy's Theorem for EDSs.

Primes From Rational Points

It does look, in some cases, as though rational points on elliptic curves can produce primes in abundance if the Mordell-Weil rank of the curve is greater than 1. Let E denote such a curve, with two independent rational points P and Q. Let M and N denote integers and consider the bi-sequence MP+NQ, the denominator of the x-coordinate is always the square of an integer, let s(M,N) denote the square root of the denominator. We appear to have more joy looking for prime values of this bi-sequence. Simple heuristics (see below) suggest that the number of prime values of the sequence s(M,N) with |M| and |N| bounded by X is approximately

$$c \log X.$$

The constant c should depend upon the elliptic regulator. The paper just referred to gives examples where only finitely many primes occur. For curves in homogeneous form, only finitely many primes appear with no extra hypotheses on the torsion. Nailing precise criteria for finiteness is an open problem.

Cremona has a list of curves and points for conductors up to 6000. From these, the first few with rank 2 can be siphoned off to a separate list . Using this list, Peter Rogers is now collecting some data on this problem. Whether the heuristic argument is accurate or not, this method certainly produces some large primes.

Examples

1. e = [0,1,0, -25,39], P = [-5,8], Q = [-1,8]: s(118,31) is a prime with 2705 decimal digits. This curve appears as number 26 in the list .
2. e = [0, -1,1,-9,9], P = [1,0], Q = [7,15]: s(111,47) is a prime with 2541 decimal digits. This curve is number 34 on the list.

Heuristics for Prime Occurrence

There is an interesting history of heuristics associated to prime occurrence in integer sequences. Chris Caldwell gives a brief account of heuristics for prime occurrence in the Mersenne Sequence in his interesting Prime Pages. The basic idea is to reckon that the Prime Number Theorem gives the probability 1/logN that the integer N is prime. So if you have an increasing sequence a[n] of positive integers then you would reckon that the number of terms of a[n] with $n < X$ which are prime should be about

$$\Sigma\ 1/\log a[n],$$

summed over $n < X$. Hardy and Wright pointed out that this kind of argument suggests there should only be finitely many Fermat Primes. In general, this basic argument needs some refinement to make it work. The numbers a[n] could all be even for example in which case the argument would be nonsense! In specific cases, such as Mersenne, refinements can be made to work which fit the data. In that case, Merten's Theorem is used to predict approximately

$$v\log X$$

Mersenne Primes 2^n-1 with $n < X$, where the constant v is given explicitly by the formula

$$v = \exp(\gamma)/\log 2,$$

where γ is the Euler-Mascheroni constant. The paper gives a similar refinement for EDSs, using a combination of Merten's Theorem and Hasse's Theorem.

This page maintained by: g.everest@mth.uea.ac.uk

Last updated: 08/23/2002 11:01:00