Feasibility of p-adic Polynomials

Davi da Silva
University of Chicago

July 27, 2011

Motivation and applications

Davi da Silva
University of
Chicago

- Cryptography
- Factoring rational polynomials
- Number theory

Motivation and applications

- Cryptography
- Factoring rational polynomials
- Number theory
- **Question**: given a system of polynomials over $\mathbb{Q}_p$, what are its roots?

What are the p-adics?

- Recall from real analysis that the real numbers $\mathbb{R}$ are the Cauchy sequence completion of $\mathbb{Q}$ with respect to the metric $d(x, y) = |x - y|$, where $|\cdot|$ is the usual absolute value, where the normal operations on $\mathbb{Q}$ are naturally extended to $\mathbb{R}$.

What are the p-adics?

- Recall from real analysis that the real numbers $\mathbb{R}$ are the Cauchy sequence completion of $\mathbb{Q}$ with respect to the metric $d(x, y) = |x - y|$, where $|\cdot|$ is the usual absolute value, where the normal operations on $\mathbb{Q}$ are naturally extended to $\mathbb{R}$.
- For a fixed prime number p, we can construct a metric from a different absolute value function. Note that for any nonzero rational number q, we can give it a unique prime factorization, allowing negative exponents (e.g., $28/9 = 2^2 3^{-2} 7^1$).

What are the p-adics?

- Recall from real analysis that the real numbers $\mathbb{R}$ are the Cauchy sequence completion of $\mathbb{Q}$ with respect to the metric $d(x, y) = |x - y|$, where $|\cdot|$ is the usual absolute value, where the normal operations on $\mathbb{Q}$ are naturally extended to $\mathbb{R}$.
- For a fixed prime number p, we can construct a metric from a different absolute value function. Note that for any nonzero rational number q, we can give it a unique prime factorization, allowing negative exponents (e.g., $28/9 = 2^2 3^{-2} 7^1$).
- If p^k appears in the factorization of q, then we define the p-adic absolute value of q to be $|q|_p = p^{-k}$. (E.g., $|28/9|_2 = 2^{-2} = 1/4$, $|28/9|_3 = 3^2 = 9$, $|28/9|_5 = 5^{-0} = 1$.)

What are the p-adics?

- Recall from real analysis that the real numbers $\mathbb{R}$ are the Cauchy sequence completion of $\mathbb{Q}$ with respect to the metric $d(x, y) = |x - y|$, where $|\cdot|$ is the usual absolute value, where the normal operations on $\mathbb{Q}$ are naturally extended to $\mathbb{R}$.
- For a fixed prime number p, we can construct a metric from a different absolute value function. Note that for any nonzero rational number q, we can give it a unique prime factorization, allowing negative exponents (e.g., $28/9 = 2^2 3^{-2} 7^1$).
- If p^k appears in the factorization of q, then we define the p-adic absolute value of q to be $|q|_p = p^{-k}$. (E.g., $|28/9|_2 = 2^{-2} = 1/4$, $|28/9|_3 = 3^2 = 9$, $|28/9|_5 = 5^{-0} = 1$.)
- If we additionally define $|0|_p = 0$, then the function $d_p(x, y) = |x - y|_p$ defines a metric. We define the p-adic numbers $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to this

Basic facts

- We can extend $+$, $\cdot$, and $|\cdot|_p$ to $\mathbb{Q}_p$, turning $\mathbb{Q}_p$ into a field containing $\mathbb{Q}$.

Basic facts

- We can extend $+$, $\cdot$, and $|\cdot|_p$ to $\mathbb{Q}_p$, turning $\mathbb{Q}_p$ into a field containing $\mathbb{Q}$.
- Every p-adic number q can be expressed uniquely in the form:

$$\sum_{i=k}^{\infty} a_i p^i$$

where the a_i are integers between 0 and $p-1$. This is called the p-adic expansion of q.

Basic facts

- We can extend $+$, $\cdot$, and $|\cdot|_p$ to $\mathbb{Q}_p$, turning $\mathbb{Q}_p$ into a field containing $\mathbb{Q}$.
- Every p-adic number q can be expressed uniquely in the form:

$$\sum_{i=k}^{\infty} a_i p^i$$

  where the a_i are integers between 0 and $p-1$. This is called the p-adic expansion of q.
- $\mathbb{Q}_p$ cannot be turned into an ordered field and is totally disconnected.

Polynomials over $\mathbb{Q}_p$

Davi da Silva
University of Chicago

- Systems of p-adic polynomials can be reduced to single polynomial equations through trickery. Over $\mathbb{R}$, it is easy to see that a system of polynomials $f_1, \ldots, f_n$ has a root if and only if the following polynomial has a root:

$$(f_1)^2 + (f_2)^2 + \cdots + (f_n)^2$$

- Something similar, but more complicated is possible over $\mathbb{Q}_p$

Polynomials over $\mathbb{Q}_p$

Davi da Silva
University of
Chicago

- Two levels of complexity: number of variables and number of terms.
- Define $\mathcal{F}_{n,m}$ to be the set of polynomials in n variables and m terms.
  E.g., if $f(x, y) = 4 + 2x^{10}y^4 + x^{15}y^6$, then $f \in \mathcal{F}_{2,3}$.

Polynomials over $\mathbb{Q}_p$

Davi da Silva
University of Chicago

- Two levels of complexity: number of variables and number of terms.
- Define $\mathcal{F}_{n,m}$ to be the set of polynomials in n variables and m terms.
  E.g., if $f(x, y) = 4 + 2x^{10}y^4 + x^{15}y^6$, then $f \in \mathcal{F}_{2,3}$.
- But we can reduce further...

Honest polynomials

- Consider again $f(x, y) = 4 + 2x^{10}y^4 + x^{15}y^6$. We know that $f \in \mathcal{F}_{2,3}$.
- Substitute $z = x^5y^2$. Then f reduces to:

$$g(z) = 4 + 2z^2 + z^3$$

- Then we need only solve $g \in \mathcal{F}_{1,3}$. The set of solutions of f is then $\{(x, y) : x^5y^2 = z \text{ for some } z \text{ where } g(z) = 0\}$.

Honest polynomials

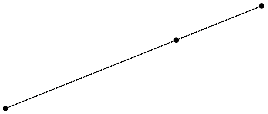
- Consider again $f(x, y) = 4 + 2x^{10}y^4 + x^{15}y^6$. We know that $f \in \mathcal{F}_{2,3}$.
- Substitute $z = x^5y^2$. Then f reduces to:

$$g(z) = 4 + 2z^2 + z^3$$

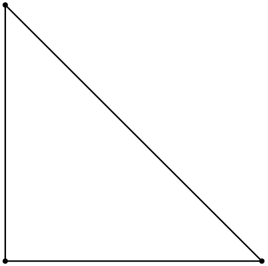
- Then we need only solve $g \in \mathcal{F}_{1,3}$. The set of solutions of f is then $\{(x, y) : x^5y^2 = z \text{ for some } z \text{ where } g(z) = 0\}$.
- Can this be done for other polynomials?

Honest polynomials

- $f(x, y) = 4x^0y^0 + 2x^{10}y^4 + x^{15}y^6$
- Each term has a factor of x and a factor of y; we can think of the exponents on each term as a vector in $\mathbb{Z}^2$, namely, $(0, 0), (10, 4), (15, 6)$ for the above three terms respectively.
- If we plot these points, they form a line. We call polynomials for which this happens *dishonest*, and all others *honest*.
- Example: $f(x, y) = 3 + x + 7y$ is honest, because its exponent vectors $(0, 0), (1, 0)$ and $(0, 1)$ do not lie in a line.
- We can always reduce dishonest polynomials to honest ones by change-of-variable methods as seen before. Thus, we can restrict study to honest polynomials. We denote by $\mathcal{F}^*_{n,m}$ the set of honest polynomials in n variables and m terms.



Newton polytope for $f(x,y) = 4x^0y^0 + 2x^{10}y^4 + x^{15}y^6$



Newton polytope for $f(x,y) = 3 + x + 7y$

Simple cases

- Monomials
  - $x_1^{d_1} \cdots x_n^{d_n} = 0$, same as in real case (if and only if some $x_i = 0$ when $d_i x \neq 0$).

Simple cases

Davi da Silva
University of Chicago

- Monomials
  - $x_1^{d_1} \cdots x_n^{d_n} = 0$, same as in real case (if and only if some $x_i = 0$ when $d_i x \neq 0$).
- Binomials
  - $x^2 + 1 = 0$?

Hensel's Lemma

Theorem (Hensel's Lemma)

Let $f \in \mathcal{F}_{1,n}$, and suppose we have $x \in \mathbb{Q}_p$ such that:

- $f(x) \equiv 0 \bmod p$ *and*
- $f'(x) \not\equiv 0 \bmod p$.

Then there exists $x_0 \in \mathbb{Q}_p$ such that:

- $f(x_0) = 0$, *and*
- $x_0 \equiv x \bmod p$

- Uses adapted Newton's method
- Can be extended to higher powers of p, multiple variables

Hensel's lemma: example

- Consider $f(x) = x^2 + 1$ in $\mathbb{Q}_5$.

Hensel's lemma: example

- Consider $f(x) = x^2 + 1$ in $\mathbb{Q}_5$.
- $f(2) = 5 \equiv 0 \mod 5$ $f'(2) = 4 \not\equiv 0 \mod 5$, thus by Hensel's lemma, there exists an x_0 in $\mathbb{Q}_5$ satisfying $x_0^2 = -1$.

Hensel's lemma: example

Davi da Silva
University of Chicago

- Consider $f(x) = x^2 + 1$ in $\mathbb{Q}_5$.
- $f(2) = 5 \equiv 0 \mod 5$ $f'(2) = 4 \not\equiv 0 \mod 5$, thus by Hensel's lemma, there exists an x_0 in $\mathbb{Q}_5$ satisfying $x_0^2 = -1$.
- -1 has a square root! Which proves that $\mathbb{Q}_5$ cannot be ordered.

More complicated polynomials

Davi da Silva
University of Chicago

- We can apply a version of Hensel's lemma more generally.

Theorem (Birch and McCann)

Given a polynomial f in any number of variables over $[Q]_p$, there exists an integer $D(f)$ such that if for some x we have

$$|f(x)|_p < |D(f)|_p$$

then we can refine x to a true root of f. Moreover, we can calculate $D(f)$.

Birch and McCann

- Good news: we can, in finite time, check if a polynomial has a root. Just brute force check for:

$$f(x) \equiv 0 \mod p^R$$

where $p^R > |D(f)|_p^{-1}$.

Birch and McCann

- Good news: we can, in finite time, check if a polynomial has a root. Just brute force check for:

$$f(x) \equiv 0 \mod p^R$$

where $p^R > |D(f)|_p^{-1}$.

- Bad news: $D(f)$ is resource-intensive to calculate. If n is the number of variables and d the degree, then

$$L(D(f)) < (2^n dL(f))^{(2d)^{4^n} n!}$$

  - taking $f(x) = x^7 + 4$, we get:

$L(D(f)) <$ 1933326428133495947869005351579566442338794676438145065454226255104180462889721182185 7
6871426590561959658753898205091640503148428908169392425185932175576810 3376445308792092395636 98
2970726504712524486476057166330728844298342919517364978030022251473663 8819063756054018996578 41
7761161992648760557018169228488048159680497348475599240382107647372869 5312773690906318088821 99
2423143837913284235360086572243436971731852708267608608416224987193888 8677462199545204970555 60
2530090205227886457244539696443077971220811050217647331617753931550473 7442700616966710750405 41
3824882162922569391197219345384430610117124584911245229330939654415004 2749350635739975298083 53
8011918846230441297647208396630888129631926621760950435205570044116659 2095616366763077550826 99
7877574871219345599338919610932098495256107502874357513111580297287287 5017417391401647059564 06
4950066460741775965193149538964142854642578728529899818673738874796709 8445214990565353557984 30
7668178575234627495103485837349022565685845524720865993770884625119910 7405814333425952132570 47
7241759069891554646175191972671878828350001258276425170821998791185113 9878923777642394356217 65
1320177769255664094994575716401817267792819131529949168032944957511541 5617590729186976136790 50
3349446731832134961647515366095987698998487383009238538840803314159656 8581825396697105743135 69
9827033566051394313338149330768459510942242979383995013895360809123904 6703009338564116802956 54
3789412419321547220236549888490281529589008816784610245865704248022588 7435331343129363352560 42
5117327358126484805714690040674385421597109612903329678594555493335001 1304959545354276194661 56
0399191510424525279150769097652553148263820279250828459068579674941950 8901911415524650284010 15
3169586496626760414000330198843819694296841079735426025475416495720510 2052718244954510496788 77
6474155910297918835391398923683986493677650251936004575387818689363688 6732077250727937308517 48
0499366898312839571513071389651061533372015688742785032852250207936198 7175565656664660441552 67
2214316009301522994672051315282706792270482251971164290477935589863473 1738440673855855074289 18
9106504454062855087485450284643979346120040531744059090084373803645025 9929435833057640800140 34
0675580027066187887338364379957201763353854223804520124778777814477912 8976968873539226623343 56
0175028044065660381812015102977968112688031951783579489534741050738872 0465964068971800301122 77
5746466960506239155665268750324608746540891226250399065114160736002020 2560845457322492298255 77
7882727651119842761188037971152914466738633927204203067903374584227372 2078373655692934641435 24
3466229911717153016824182022205447176953710557428643965545073094155945 8138729416628572756945 61
4580007333344148260808345326229548535122591715680334219522227727531010 0056392555409233637617 97

27768705387653848808502366866577584791105714266 66881598470090481050677593054802693440880997883
85982036073163160832932477867963576821959030015186533621720941008315015 504160092821390735480165
47318465682680309962544613001738751406244803284251876238081702639973720 099357911229890754313928
42336562700347091805934986871124657561284033657287280886982248662682562 241811358293232432490640
18175862105910195923866165532003638015759767903852485188295474455130646 650060441235786353751939
79074297411341574306775686465474749570396600692976031957206847936581853 364939828657022142291630
25826882105401506904154687732454567649386763313664787533708805414185716 607282015716280661495690
03475514071123140770910881617353462138740161407020480964910267341366363 386694331921901029902647
27178384279292572319978770251201942341885583289430904732318070667536373 361029938151627076336827
34977764794176041995566630284153509116149280406460558406254653016765481 191901211824078508712411
82020196569756332376277970721742903455306283108140271765750884054569215 527310974751331409290414
63481622571228814937504034608105402501909469669611410022016435585923923 363240934753811667740366
61323460081008757931577900412470495111016037256321514136995011526211977 786432742730585992201195
69926119769216607970465317662535906651432786691930552490650588015412896 684981956267188059173275
23026473913171570217118754890034393295229821684153887275109724643141065 580947487331216089698205
50767346719149449407829771518312931643119046576373685739172984257329613 352451644433194463613254
43631667653958971127361707058839371842915550067669380683396662335744863 302058728455339340742884
87873904747217468102827636135881589104199395460719082336552822227847839 994979786057775290439288
37821221791960808002358620129273322413924431474821160667463918058739328 869607267495687774928463
21577240087964606847224518339097272775527052971137311372009405901418184 425259318797366930531206
89456635677316334592649553612486273271126877768340541662028274656674208 824373642498448933563461
89112484397740789557964879428682459619480223155587283567199114686125082 246820920465879510745958
24335746769564731021487842759117878077329316908146492044902784767207036 634452982653706064309916
14138235337409041735604566627971538918009671764678462487196142402677790 031796725537116127711331
14213816253177083561407775074463980226563641725316804245424290316206483 399866051686597563237691
37014731393251948140130030014107093773194710533383389766874103489667546 648667629520704566315521
91195483231677700831274028230628234346120361603059938033790508704029725 505614739205239934359158
28683667190845566116268964793485699794760881331857746316192783388429221 150983400602588410701009
45378698571147841770407629033538122506061902053668940321003797173491040 065261430937893744944195

4551942021091893315046582487397778114102740801 2870075184156515765420094346277611889470238678444
2685518244394188204540141287071531832668108835353447180803864257950835 480057761657836409566495
8921581750897046105875263423274341134280008680498272389043329299124763 244513279266348627135466
9491078284960131973849224931991173322743277977413512404191667984602906 615307497789977273783557
7986542134517133910075032188637732275234029805130660935874662855959492 330141800833329253231398
5333047962320439733280363688402448393283160624104349053309994029946516 541782874026652098068682
0133956700670542877366085497270431101337962307541619535454942878984823 024631451411435315077516
2012070637341894811249663271899917592170940381209119342678566768003503 520664350559452345079898
6502241502526713020475266318316765586193597329207863536907595606123799 226269594166710188024823
9622449766218636029191906195577932407980135466833969496624040124843449 664434998303562124599572
2472926216209467798290985426363226746020920881874576325567137568696360 340286397674827314068619
6642751409721311959318990898567051595729288753041692997497726786776787 766657800060443191026989
5146916184453460928039963292547510599979832884205964074785590540141837 778365515979716826496711
8038343759836539876312800296043537050973083174980001672055931722611853 440183948113240402534108
6165601055844482426420971617585219502951952603180185843459857422239317 671591845658867751981969
4075912707130237858511272581698736398278993723959122146129628657983577 520845908402670805939127
7009422742494596662504954799596383541037946452743275979447367026249361 289179836969190130151721
5710685557304016443177938347849178261208604558636478869398460620307716 489153297426252497033560
3785252109654884535122050706836417167686568383080726299669648450112620 761317662037176884855323
2372854161296432137383203602302892795329353462748398745976357965484916 514040814551016905796873
4401420295329861549724996214850019901641793735244392199477734135012413 122642914518082952444152
7919834495511336751551833436225889582099931180735639547771819072089269 205331109150595445244131
2847816320411705439888346906101020628960920759310335161319585780675532 634935478758251861508709
1086877493610527761447194233697953316826998399779374766758801826205367 158940562190716233719022
6543511217996939592481390814910120220576876612743453849390322954894769 940635059600929089582407
5888309147483415772282335022074415179733036699579983472842447980716356 822332217231665013459300
9041501062569385740085497539124231737227329432947011927354180251786879 406420012583938126746145
1695775313324459085996358921010174431727332982945463813543156612632508 448937192274863650940936
8953907671884804763187705163750951698671390248312022915784478142101053 631622424509275875982395

4981499329734625753956056408466254565855807880 412360754237539611684435891368408017428014701914
5928309054801248486292561098139657284944466082012135932641240835876708 218471169745652558683184
6009310526284468778703179786543021247185894066821715033013600196181513 345898913620218124237575
9887552038268612696911755419194394725935929625976261687472889791141638 886183728104305643944654
2983760339622802780125162672489764200362758344685630093770055060741060 762001246118311319893347
6716506514025379996483030608324172623555255326909648198100374876418304 535252129822826053866843
9019874114167929509509173480440815541564923141182359372409118644544732 084300516002146873272116
5581369877615686034360876930273543338201753898290985560860760981506111 352506243794566089323741
8555455622494975399278363613444740752987111006979598141751516216118734 903884322547085607936959
9088785230456241835849268578883769845115694129636217642725977720850251 691230901671066760314469
2006315387695304307696631812330404859286569857224365099301333167812240 407599878708994281851100
2907184121892327134509956170592235148257374494966000030800513040305842 141730224196215762683275
4282227006426878484585132636753334520888930866731162170669630885288947 313137430305978831860137
6370276678632156613075326973827465731371851496924476827601783224541117 660365225083541558750352
1638812172848855092635565413574159829951572539703092215072741841807056 834433532861973325107257
3491930529582856966091371776210150946261256284258255556802208436555942 709320641781369244221514
5935098890771278152305206115997893526683576513273378475013627418690457 293566188096279026948455
3244764782243887823486962712664063775831018884755806580476266182826472 528374458570131025865380
4682589771425886376600047632568685627883087087466633200688798182340570 112861071586708084463968
7465794756938575979957710217670938072888485422191914636416862806942091 028665616749074216292213
9013670720793670410130459850164000150045389752692140585220900441045644 724948332993443379600507
9178481261506414525413296217795933518952004771244780403441977357143147 293123769075759192383599
0086076433038737442785063322610345425510972514528801944016234737388323 031587481119436087131528
9493817711567467416785996468096229672026992938040310717063437525442653 729531557604205465346928
5242075515310118427054165809046196614908485780377719880641848311091668 977011182356581499446350
3586199260108567459723387788949465123595538222677165433011388971469578 673281110110972978658056
7269452367791169552797256332057936803753229342159625070574017613584033 106290666689138039222884
5533128362653139838192214806564710071930544384271195308540742333806169 882572179772768792824638
8069503805249506876655159191076166515836255389617798602831995998968095

9258569189421579248896856071334730561897959614452315812016458345276275 8192254557076226576514244
4750016386128182627818451574714826448540531212380982773234558981478939 9361167801250307679525651
1410109219719584140746947407093180153154716007934873672193053764621482 0089724391324490178107821
1017096211807581786340102542674303493576417353270321262104393045939175 9852311208494922706470428
8850779300591592625223568222936047134259113232323617758192275451621117 0928990962375221063279900
0717154815040766507255570456978561517958891352342515792731266291633373 1131823344983095462936361
1527704840359327341209375579332711362022023030290270919346971830858002 7264436625083781298432201
1007786336248236776985785619828577367009966060476590825523642025151934 9970032249436089831805141
1251385397748099806369394361868251837656564999550021086755706652361564 4805946299358872965252686
6787029179457110904283865468305849945233218958064333605993464701290217 6199595693387692049295597
7116469023990635871018497682049117591825215915280537815915871962893198 0962486990140519060951516
6624532619480842013070311806548223666815029094102062730669036550259386 3658884026981501861782375
5727228114933230059567795880662731346520428145543992531173899770920088 9829440992110687527935588
8343156375221804788803563756996449738681623729312217421535902950467261 7057392092547971146884470
0598895372923229171299325815273972290059598281501805853176974464464020 4860172099939388911654599
9350507175299173524917421313603698106554426707217938259727506627385348 7469380509217963723553867
7582514271379868665747454582623807900587044429890165506827155306306571 2644212685253691886171198
8109890282824383408385485490725447498125742637978395466623516461462809 4023663603706583082428846
6694333324288723276763636471983316000037700956435118678397573774769878 3871009846005636679486877
7397920285310853739748325041833382776748347936616663172705910102576712 0216380875475074295034937
7671123864535245084097229358710254565652838504860969861755888459168529 4732579446897675099351507
7209991932706811056011820661743340005563203390572447494043978246308658 4473927210390488413815946
6352846154667776280575820666901510805471839253416474258687312371960862 3196513530905520523941026
6824617911767714089655710718050760519806128710542068921241876884472869 4758444864772525467468528
8602985677616600341949288841987509029539428042321736958370474486865212 9318104787573037526003373
3049466752679447682703639607172365967127147323092638568128000247203007 7785581312796485083572738
8829267366454417373343825993756449773116118717968933558628939365169806 6709615807135068775641467
7815777044556384498552806649943510425361801462614177381401881391551683 1101378389183622313645220
0344584923456616307202138982006731832473778779286103310591826580086935 5640438299135807480491132

7199188373246741206605662801845319362060219134350275144916498005561185 435417398963127406844736
5538620550159360799713028854768438041523993496680243159594865969623349 509885983284037547555886
4282948266930427067312266731837490218714684892871738100493261649529839 517126074062603440152335
1904567686533547695258057556529762684247408869236632016577754326954093 220772545191185824460885
8382903329116638642694709861429945910962893254169827026500193379290507 265576743814223150500427
3059454155099652315999917772543786265038710239359963379244033365151731 910808135932283662645119
3728142063493966638550293417192037419090382748878522357286489270695126 703350266761225380513883
4474494157361045369193981305946055505242046508174899347373502807919216 225133107360515367112175
9451139108131566649581159196400487942775849692765994637669846977935071 264404520058190326545320
8603389475304124976992255439235798922936179059319476653541800250591617 055746244341942788970946
2072884378399426521794656412568689321087294219610252736870006284081581 453020096178489800518281
0564015402000593209088756461030608775460159145662775675729930496629315 523678554736482735480720
8685050449983283316889070625920757243214457091817699287375536927414745 106229183285799137076031
6278883362246691879734019313491117063081318900131028527973178631567546 412437475598660765943115
0238502333563561904336211374115633317502339088378404419179762591439327 406081823145247848468515
3971068837470718402236792978382026600980199675909467363203546454674990 286921085310491923147279
0278755850894558206116429818462011053557073212761035286647747807963540 139692004852927253409713
7725426345146956701018294688315450061189086730205218119081036790348152 686324767569343478221644
9015466789889714268406717359828844402096033897759983872158916658254816 814356150618922266102596
5273199787639340087920590289639360277067412915200195263965247512822498 693063646454593577899457
8887091657458828605013087610309080738617604412507010602465972099204920 822495088410775850448055
5669686424215682855430282139431917902045975913113849145474067646281070 190368217408980956169859
7835317856209812906951200524451707221275990672778236299023304965806815 026799799600113157760551
8210622344783311114700198503061053952743901132834902116905644225345550 799473398541975476734484
8319978464062783091149653770204702544317112890715322760473604803001373 033905636613301806853236
8772214025516731598169016766669903755887525430684490625459370870357507 857644675408677733966854
7210949705964050091695973580249262485118940967059521205606504799313985 073347029485867024740045
0130888647292924606264538178213031040820515644282770463889992688266035 198547246528965615022961
5931683798331665646581179999108917791761114099001769238562209575112929 204225794965821911549948

4858944343561458439132622102614695719129830478982352293011207825526602 7371401028721231469204553675177858358704638367318321867269465636610668103456184824246233177077 4537389170649749807724578829233300644173100299921989735395524004421126612325745497807342190161 8308991829711270432432110588231311141044006494777147145445809224383164130697218871604719463200 3819054356298331615307226250921799515833044989750619232338163523080812096290138363992374368086 5795181223942854111604031542466692763465671137372864507782029818944015777436093339622269983412 0499083457461455647570817953791812427357058435862349363327929144235223597597348834369848767975 3605546935295392103489381656932565675474648226666935461365547939980161781610890483167266991240 0475580776625521955547905239858832167163041879599154644170455233787863728420494955189228080186 7108086094205474762565781032586375234331733338906181684963029802621133953349565160559573593064 1880777504984282690591694321535259646020421571169496018403612934258042250644714685152596572359 5686467779434204894608541279198160672625618738700502846620271798199070611558671230733863674724 7241989145133477315072169176256621193455139416694994156442223947119209638107009139873533439123 5721747042942674643494518010769309507089020100008112497113839303216324981723181952629251399772 4515241696922857077021837781056883511185500589675371469648537434035499678202848832296633941114 6011501493306928652556239705544398060382982857585769756120760800794335970962469675992697917926 6453323021169043231165683048188494816226118688899046166605142246323833299229104553358823112703 8011209955382752001056625295892996485164656792119952609817811192920911554027479387110657041536 8657622848628077222439437557739883892952878597407243581889190997708295978928521532624431679828 2591762705323556575677271130751322785292672608016674212564342794263920679187638026506260932774 1252099792422980013154946328065242617721405844817349367040566205386773481746146771115842954618 5839116620409972521597353678274745935574702161885293397155313822120364727455648666967893392501 8576111429376554362718535877993192307322044186342626125376324128388922321339535019789208940386 6953868490412342883169766714327023944375785839793374980112238792666530441838045142845793089525 9076469538122463872065764436168036876193200398888635968390276653753398110039829006695184665589 6630213299258863108271607461380580432629817388972009252184127953071743683164539992634766639736 0298334095025359054099021942578010271247807899674399864860330601567261282206900988018841216512 1457041963505051707456914587479731783477099523726581259400491039415288613588571004377699667991 3791506817410130400732204196739136158661479043401739719003122508331626519602143646155693582390 1757205717060181726435

0796019994058290280157421295579005015248751326060110425010146736260030 107935434900507146983725
2747575636407137429318806814266500288111124454802856386357388113847046 201119868703815115456950
6918047534728745652931837314202669019699786819522249164134775315502688 293957495159996661330617
2164221743875742326480934895175910241980838152311681865693753220074578 356253449404114372621335
8422916672320928540774134381780996068455843776190296000004594483481108 406335146942435138882597
5364284162934532412295651506297344469237130869337989625068928844830652 309957700073035585035426
2689496066683791679137945056073667757030299542145784364976990040728336 171741784033839293713728
6155443619182693805380648353286742423772086224617911686275935704922990 950107052745646302131346
6439571085797828405847640731317461189582472087233909379669552298817827 772341512321406307344967
8462008176278717688168761491760124249647464191755884573322332582647923 179428941519683831060182
5653099284666018558494681985608958687748106818202361802474656120253777 103868611564313463346680
6061570999973074346684007738128548434504149439479683412047705313813859 468915686002637790106754
9621069096434362996035114007326743075234263659617662555790584040785186 445294055515218486354179
0178552220399242452493636477741738508948252626990998450973741356439740 030497868634013238772455
9912289739089351327840821454848179828920198928056232301101127453195782 774815876581467986024680
8860340759511362617963333433501827077326566822912399658925853798155304 549934348840465904361510
5558149666971040156413729691378329746121431783717804745235867058038514 004329814747006713613554
3680811103936630564961418119437341723242226318294872268277783945511589 328473869183389587844641
3364146043150665917059369780029008293299219597013992778003864301078792 395336398816120805354337
4173601781214416186048510639966182231824648689570041567863753216639534 099026122346117453596040
9775906481351210103368109247835742219175393395763206740912644019072730 717403702143041605413025
6444095186656062571144322680938655684116915490412657269794303132017033 179604367954810023901052
8578255734003673151877904775398582849166026386576057005166801737623802 869815560651585309703581
8736127994423611289775666839916845557927997829107727621958479271109590 818877806799644714193097
9231408441322144345564668305275411394696136564091845412673652219856196 590587623259484545230799
9915815700607437446495655889867881589033605545795704931674389845467335 881492982493505034676048
4742846290355186055540837887824927286236479503038844508369239761484371 449411708725154987967517
6041919740016367734987309687250753794881134720678864790804199167651142 062983909977519014533994
6634990776686637758838156555184792450294060363206762460863477325489979 091564455129003169655505

Feasibility of p-adic Polynomials

Davi da Silva
University of Chicago

6499783532699065215359952122405024749296670048568960960100000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000

Davi da Silva
University of Chicago

0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000

More sophisticated results

Davi da Silva
University of
Chicago

- We can do better, though:

More sophisticated results

- We can do better, though:

Theorem (Avendano, Ibrahim, Rojas, Rusek)

For a fixed prime p, finding a root to a function in $\mathcal{F}_{1,3}$ is **NP**. *Furthermore, allowing p to vary, finding roots for almost all polynomials in one variable with integer coefficients is* **NP**, *as it is for $\bigcup_n \mathcal{F}^*_{n,n+1}$.*

More sophisticated results

- We can do better, though:

Theorem (Avendano, Ibrahim, Rojas, Rusek)

For a fixed prime p, finding a root to a function in $\mathcal{F}_{1,3}$ *is* **NP**. *Furthermore, allowing p to vary, finding roots for almost all polynomials in one variable with integer coefficients is* **NP**, *as it is for* $\bigcup_n \mathcal{F}^*_{n,n+1}$.

- **NC** $\subseteq$ **P** $\subseteq$ **NP** $\subseteq$ **EXPTIME**

More sophisticated results

- We can do better, though:

Theorem (Avendano, Ibrahim, Rojas, Rusek)

For a fixed prime p, finding a root to a function in $\mathcal{F}_{1,3}$ is **NP**. *Furthermore, allowing p to vary, finding roots for almost all polynomials in one variable with integer coefficients is* **NP**, *as it is for $\bigcup_n \mathcal{F}^*_{n,n+1}$.*

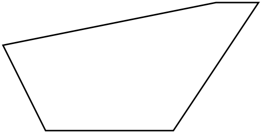
- **NC** $\subseteq$ **P** $\subseteq$ **NP** $\subseteq$ **EXPTIME**
- For $f(x) = 4 + x^7$, taking $p = 2$, finding a root would require checking for a root to an associated polynomial over $\mathbb{Z}/32\mathbb{Z}$. Much better!

Neat result

- Define the p-adic Newton polytope of a polynomial $f(x) = a_0 x^{d_0} + \cdots + a_n x^{d_n}$ to be the convex hull of $\{(d_i, -\log_p |a_i|_p) : i = 0, \ldots, n\}$.
- It can be shown that if a lower edge of the p-adic Newton polytope has an inner normal vector of the form $(1, k)$ and horizontal length m, then f has exactly m roots with p-adic absolute value p^k in $\mathbb{C}_p$.

Neat result

- Define the p-adic Newton polytope of a polynomial $f(x) = a_0x^{d_0} + \cdots + a_nx^{d_n}$ to be the convex hull of $\{(d_i, -\log_p |a_i|_p) : i = 0, \ldots, n\}$.
- It can be shown that if a lower edge of the p-adic Newton polytope has an inner normal vector of the form $(1, k)$ and horizontal length m, then f has exactly m roots with p-adic absolute value p^k in $\mathbb{C}_p$.
- Consider $f(x) = 1875 - (24875x)/4 + (24125x^2)/4 - (9605x^3)/4 + (1783x^4)/4 - 37x^5 + x^6$. Then the 2-adic Newton polytope tells us that there is one root with absolute value 1/4, two with absolute value 2, and ohe with absolute value 1. The roots of f are 20, 1/2,3/2, and 5 (with multiplicity three).



Acknowledgements

Davi da Silva
University of
Chicago

I would like to thank Dr. Rojas for his knowledge and support.

References

- Martín Avendaño, Ashraf Ibrahim, J. Maurice Rojas, and Korben Rusek. *Faster p-adic feasibility for certain multivariate sparse polynomials.* Preprint, 2011.
- B.J. Birch and K McCann. *A Criterion for the p-adic Solubility of Diophantine Equations*. The Quarterly Journal of Mathematics, Oxford Series, Vol. 18. 1967.
- Marvin J. Greenberg. *Strictly Local Solutions of Diophantine Equations*. Pacific Journal of Mathematics, Vol. 51, No. 1. 1974.