Genus 1 point counting in quadratic space and essentially quartic time

Andrew V. Sutherland

Massachusetts Institute of Technology

January 11, 2011

http://math.mit.edu:/~drew

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Algorithm	Time	Space
Totally naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly less naive	$O(e^{n+\epsilon})$	$O(n)$
Baby-step giant-step	$O(e^{n/4+\epsilon})$	$O(e^{n/4+\epsilon})$
Pollard kangaroo	$O(e^{n/4+\epsilon})$	$O(n^2)$
Schoof	$O(n^5 \operatorname{llog} n)$	$O(n^3)$
SEA	$O(n^4 \log^3 n \operatorname{llog} n)$	$O(n^3 \log n)$
SEA (Φ_ℓ precomputed)	$O(n^4 \operatorname{llog} n)$	$O(n^4)$
Today's talk	$O(n^4 \log^2 n \operatorname{llog} n)$	$O(n^2)$
Amortized	$O(n^4 \operatorname{llog} n)$	$O(n^2)$

A quote from the 2007 record holder (2500 digits)

"Despite this progress, computing modular polynomials remains the stumbling block for new point counting records. Clearly, to circumvent the memory problems, one would need an algorithm that directly obtains the polynomial specialised in one variable."

INRIA Project TANC

Schoof's algorithm

Schoof's original algorithm

Determine $t \bmod \ell$ by computing the action of π on $E[\ell]$ (using the ℓth division polynomial $f_\ell(X)$).

f_ℓ has degree $O(\ell^2)$.

Elkies' improvement

Compute the action of π on a stable subgroup of $E[\ell]$. (using $\Phi_\ell(X,Y)$ to obtain a divisor g_ℓ of f_ℓ).

g_ℓ has degree $O(\ell)$.

The Classical Modular Polynomial $\Phi_\ell(X, Y)$

$\Phi_\ell \in \mathbb{Z}[X, Y]$ parameterizes pairs of ℓ-isogenous elliptic curves.
It is symmetric, with degree $\ell + 1$ in both X and Y.
Its total size is $O(\ell^3 \log \ell)$ bits.

ℓ	coefficients	largest	average	total
127	8258	7.5kb	5.3kb	5.5MB
251	31880	16kb	12kb	48MB
503	127262	36kb	27kb	431MB
1009	510557	78kb	60kb	3.9GB
2003	2009012	166kb	132kb	33GB
3001	4507505	259kb	208kb	117GB
4001	8010005	356kb	287kb	287GB
5003	12522512	454kb	369kb	577GB
10007	50085038	968kb	774kb	4.8TB

Size of $\Phi_\ell(X, Y)$

Computing Φ_ℓ with the CRT

Strategy: compute $\Phi_\ell \bmod p$ for sufficiently many primes p and use the CRT to compute Φ_ℓ (or $\Phi_\ell \bmod q$).

- For "special" primes p we can compute $\Phi_\ell \bmod p$ in time $O(\ell^2 \log^3 p \operatorname{llog} p)$ using isogeny volcanoes [BLS 2010].
- Assuming the GRH, we can efficiently find sufficiently many such primes with $\log p = O(\log \ell)$.

Computes Φ_ℓ in $O(\ell^3 \log^3 \ell \operatorname{llog} \ell)$ time and $O(\ell^3 \log \ell)$ space.

We can directly compute $\Phi_\ell \bmod q$ using $O(\ell^2(n + \log \ell))$ space. But this is still bigger than we want (or need)...

Computing $\phi_\ell(Y)$ with the CRT (take 1)

Strategy: lift $\mathrm{j} = \mathrm{j}(E)$ from $\mathbb{F}_q$ to $\mathbb{Z}$ and then compute

$$\phi_\ell(Y) = \Phi_\ell(\mathrm{j}, Y) \bmod p$$

for sufficiently many (special) primes p and use the explicit CRT to obtain $\phi_\ell \bmod q$.

This uses $O(\ell^2 \mathsf{M}(\log p))$ time for each p, in $O(\ell \log p)$ space.

However, "sufficiently many" is $O(\ell n)$.
Total time is $O(\ell^3 n \mathsf{M}(\log \ell)$, using $O(\ell n + \ell \log \ell)$ space.

In situations where $n \ll \ell$ this may be useful, but not in SEA.

Computing $\phi_\ell(Y)$ with the CRT (take 2)

Strategy: lift $\mathrm{j}, \mathrm{j}^2, \mathrm{j}^3, \ldots, \mathrm{j}^{\ell+1}$ from $\mathbb{F}_q$ to $\mathbb{Z}$ and then compute

$$\phi_\ell(Y) = \Phi_\ell(\mathrm{j}, Y) \bmod p$$

for sufficiently many (special) primes p and use the explicit CRT to obtain $\phi_\ell \bmod q$.

This uses $O(\ell^2 \log^3 p \operatorname{llog} p)$ time for each p, in $O(\ell^2 \log \ell)$ space, and this can be reduced to $O(\ell^2)$.

Now "sufficiently many" is $O(\ell + n)$.
Total time is $O(\ell^2 n \log^3 \ell \operatorname{llog} \ell)$, using $O(\ell n + \ell^2)$ space.

This is perfect for SEA, and can also be applied to the partial derivatives of Φ_ℓ, which we need to construct $\tilde{E}$.

Alternative modular polynomials

In practice, the modular polynomials Φ_ℓ are not used in SEA. There are alternatives (due to Atkin, Müller, and others) that are smaller by a large constant factor (100x to 1000x is typical).

The isogeny-volcano approach of [BLS 2010] can compute many types of (symmetric) modular polynomials derived from modular functions other than $\mathfrak{j}(z)$, but these do not include the modular polynomials commonly used with SEA.

They do include modular polynomials $\Phi_\ell^{\mathfrak{f}}$ derived from the Weber function $\mathfrak{f}(z)$. These are smaller than Φ_ℓ by a factor of 1728, but they have never (?) been used with SEA before.

Numerical results: 5011-digit point counting record

The number of points on the elliptic curve E defined by

$$y^2 = x^3 + 2718281828x + 3141592653,$$

modulo the prime $p = 16219299585 \cdot 2^{16612} - 1$ is

832376989144494660061901849139137826006983637060450015930966792818374113674093822766991283099784662700961700402058294019077483170516664837812554817443350162223605440005388394920224519114859867338191660095508592165253852678528425242409787965445004279587342458591036506936232600658549556769058427604042111029080666232135885662070661039670759580341918109430064160840690748363019037103169978894180556726367014400296781983798513562269371401276427209286702254047174078470090179859044119920875037921597111234401965330999966802919477217848269921000166896074288408594435094209873544111246489768281188102940915774276149848136182361339830763026929994181385485521401057780125259890724056418895533398724332427935709677002908601694738205973033005180695050658325875333086707480480086369839004271346457865324407167865202282210199065495326810929978854624298288481916297348239030843306705546043295502481730932870433180532793495744878882506348393787807087351238867988051327037590331790801872453585872437467694874112726738073095037665888862659824866162979710551480066332118269833639587932989704356263549436446848603965666427837093575009979091922302413453716095887661432089373163729653025768255602712754566610542223232815622048111888283590483215892528728153087049654418794163034575764891117186500373809179386465716056073958857886659984917838400020437572986666397067817373843456657959297914239933377113677822538016636015241053779745447935639933068437226703067711612870475974728874060256153829424355309461429412863767016010448708725782340275978368434887328902748704620332776144279810260429883073285589599324633304714799454649284242674253031456570427212647114749626733565213374345500028792023241372392282583915035121274950736034773585892234313092778077346572608561779267925193030390180619815277308025700377636113052880114730236382334852026580407537787327013748289451197304667942877768553427530620392209638743777840561094515693650744099608411973081430390148262649852081364154006404443107834285953988209092622350423727240848811543270022694783971162521206171333600227255606557931688499109786737684979633157645270846925902311597415122278761062286676906752206603683529582116823691851305917272462661882973555769988656469584293610818091626921816662703380667041026811998131268436795000766254728604090647491868154452743670675868434070554634021891358398165724885432541336551115909636456700693477449865260368511045411205847035453060636486512589217930914523201112950463798415869418991750541041378713105362188790883183727300546588120061627174480168248774745589818525177228021451045150114779535554987684535229998681835176117651014768576344140108558104150453207370935052150913863261504324212007549804732358464553488560987919468961144855825465612614456411458521607747389949586595126074306085812134617236309956765621860727156856482046150112012015113007122286669299590274282107690933890300810525603558710045399536727403969324912420806389527152955993943311641026894824263736268535534370585102219836177805656167035861860036286963374250257588182644200835242804131190172272014414549659547457165879852600232647304991195644305287939827885207654988125751221239741075244973427819843776465089557666171337403497596850461399835327434541250151698094846056890996956914938171459951860900669270969498525993914751206760782244790625122626848753012733495289200641795967184561011226439252930596090031649974277634943933178938510726596259437826466293379162132564825895692129029330256714749154770003140032780641102586358889574523411175821853412004266108458134154747384432584651586199896849475842009365338952535884111160271960868999014742012591971478237292524813948600029227796125549029381598957721574805007478966997024108691274018357785171489306377152166096191664750803979956621679571978953552211724552632230710653244433669331067442040140391602456581858747401436772403284080454895008255550795224583691902547110401601200028499012649426967495115480636409733058979879385173976155641587413347889866280720195063520341789370965254624825613341783545292573171574068856106332164105705546182508456321207036745733148635468184175804925273259911659543081743640608001131591890082864513124247013731366137271496104705809743302158675109390889574544168419533671577041268632135079678739148622473861201691171573910748109246384543318314688276420589755569247414674972449048459237063849256993349700502878104803273489709762283329564338910078621708691577072530052908791072355075140131878757664736457176693861844062055499081418120739457763916345883494926768779319474713905005440022152143445859931404486738106328557238092332971352015340561574971125269604744349474765249731664806205766695327115242584334178977061606455707943523640635302902056014101531410341976502953492117706562557777468840876985785880425171189659103579440672885660293916184222152877072058211236432771563185676589784830224123142162854459467530132302366194216041499317839619687745599634112882779536927947477382799373586829793689942951249691202887109327063284624677436722012981685194580777814009291336645358525962424649443734012222395524 8

Numerical results: 5011-digit point counting record

Task	Total CPU Time
Compute ϕ_ℓ^{f}	32 days
Find a root $\tilde{\jmath}$	995 days
Compute g_ℓ	3 days
Compute $\pi \bmod g_\ell, E$	326 days
Find λ_ℓ	22 days

$\phi_\ell^{\mathrm{f}}(Y) = \Phi_\ell^{\mathrm{f}}(X, \jmath(E))$ was computed for ℓ from 5 to 11681.
Exactly 700 of 1400 were found to be Elkies primes.
Atkin primes were not used.

The largest ϕ_ℓ^{f} was under 20MB in size and took about two hours to compute using 1 core.

Genus 1 point counting in quadratic space and essentially quartic time

Andrew V. Sutherland

Massachusetts Institute of Technology

January 11, 2011

http://math.mit.edu:/~drew