ALGANT Speed Talk

Jared Asuncion

May 23, 2019

Proposition

Let $N > 6$ be an integer. If there exists:

- *an integer m*
- *a prime q*
- *an elliptic curve E over $\mathbb{Z}/N\mathbb{Z}$*
- *and a point P on E*

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

then N is prime.

Take $N = 119855807162905754353441189410080934202575961246146091377534111947210463834224700079661530656853914646178581 93.$

Take $N = 119855807162905754353441189410080934202575961246146091377534111947210463834224700079661530656853914646178581 93.$
Take $m = 119855807162905754353441189410080934202575961246146091309982545463032816190467094815860123098034978198057000 84.$

Take $N = 119855807162905754353441189410080934202575961246146091377534111947210463834224700079661530656853914646178581 93.$
Take $m = 119855807162905754353441189410080934202575961246146091309982545463032816190467094815860123098034978198057000 84.$
Take $q = 209875686703974494560203805789173030403053794995703038646043541120390866762042261707396727425290639136473.$

Take $N = 11985580716290575435344118941008093420257596124614609137753411194721046383422470007966153065685391464617858193$.
Take $m = 11985580716290575435344118941008093420257596124614609130998254546303281619046709481586012309803497819805700084$.
Take $q = 20987568670397449456020380578917303040305379499570303864604354112039086676204226170739672742529063913647 3$. Note that

$$m = 2^2 \cdot 3 \cdot 4759 \cdot q.$$

Also, note that

$$q > (N^{1/4} + 1)^2.$$

Let $a = 0$.

Let $a = 0$.Let $b = 1$.

Let $a = 0$.Let $b = 1$.Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $a = 0$.Let $b = 1$.Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. Note that E has a total of m points.

Let $x = 592098849152126348043382635103262083813460685432096322$
$153067244931390445534828517215923984576162981330245737 2.$

Let $x = 592098849152126348043382635103262083813460685432096322153067244931390445534828517215923984576162981330245737 2$. Let $y = 14367090822666029905563381421425098359220484025894350725570681317132285822965897906798724028047367479066290 89$.

Let $x = 592098849152126348043382635103262083813460685432096322153067244931390445534828517215923984576162981330245737 2$. Let $y = 14367090822666029905563381421425098359220484025894350725570681317132285822965897906798724028047367479066290 89$. Note that $(m/q)P = (x, y) \neq \infty$ but $mP = \infty$.

Let $x = 592098849152126348043382635103262083813460685432096322153067244931390445534828517215923984576162981330245737 2$. Let $y = 143670908226660299055633814214250983592204840258943507255706813171322858229658979067987240280473674790662908 9$. Note that $(m/q)P = (x, y) \neq \infty$ but $mP = \infty$. But, we do not have a proof that q is prime. And so, let this q be the new N.

Take $N = 209875686703974494560203805789173030403053794995703038664604354112039086676204226170739672742529063913647313266382481614867561465366941101302287259990698021432199537183839319250910215691.$ Take $m = 209875686703974494560203805789173030403053794995703038655132663824816148675614653669411013022872599906980.$ Take $q = 352977892953582459798505613176056128378583293404682718278066939521431995371838393192509102156 9.$

Let $a = 68396179343058443193254569336009882294530113361505849366650234621912075061036045515634850882704725230406$. Let $b = 0$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 10548816112953365770892353040693843829232733530150887024780171561480554169187652540032985751800873427 32$. Let $y = 934113942527262928384146186464602865972787538548006695975582564138110026017150789722425374029368559046 95$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 352977892953582459798505613176056128378583293404682718278066939521431995371838393192509102156 9$. Take $m = 3529778929535824597985056131760561283785832934161649187929222547845047861147423787902330539893$. Take $q = 1432455952491974507028085736243255346231346691647848145325622986147712698018413060527 1$.

Let $a = 0$. Let $b = 608914073032113346670272489649664216853755083909168290197287321672075616730588346374956624 89$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 167401651193239365857257914103802790791721987176147949$
$376668594111906003201186431306564932842 5$. Let $y = 727142239868$
$750036248977011532781065362914902529492870859971242620222808 2$
31437999590574001150.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 14324559524919745070280857362432553462313466916478481453256229861477126980184130605271$. Take $m = 1432455952491974507028085736243255346231346600732912329754547980814276937215150818769 1$. Take $q = 47748531749732483567602857874775178207711553357763744325151599360475897907171693958 97$.

Let $a = 0$. Let $b = 114914794346515003147004889682167632254910000074633137126936478950848467329354310380 87$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 13713621212151837723021439553937425691583943793681235276413962247721230014462822773 32$. Let $y = 42274744302696675410123600171078909444233696643111157034539031222532634670059079 39916$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 47748531749732483567602857874775178207711553357763744325151599360475897907171693958 97$. Take $m = 4774853174973248356760285787477517820771155335776374325151599360475897907171693958 97$. Take $q = 5676024182357837501141523132117558320143735745182690696297606263113006165726893$.

Let $a = 1$. Let $b = 0$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 30358988460217433966741383324548327877641517188673766755735763595676617035803075161 94$. Let $y = 5072888014687169815403030641754096566613172213137924213754791967078298589029066197 1$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 5676024182357837501141523132117558320143735745182690$
$6962976062631130061657268 93$. Take $m = 5676024182357837501141523$
$1321175583201479318525243487603707520721658337940950 28$.
Take $q = 1452411510326979913291075519989139795329562910062525$
$27133335518735052041814 1$.

Let $a = 1$. Let $b = 0$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 22283957343826370146193909830592906599821027443742994372357558870416409283581 11$. Let $y = 20628413031626093570115702995081949586104264130789238824754183590607105327908 82$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 145241151032697991329107551998913979532956291006252527133335518735052041814 1$. Take $m = 1452411510326979913291075519989139795329562910062525271333355187350520418141$. Take $q = 1514506267285693340240954661093993530114840743472188556229055771880826523$.

Let $a = 145241151032697991329107551998913979532956291006252527133335518499766057762 9$. Let $b = 145241151032697991329107551998913979532956291006252527133196470365341399842 9$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 15835227290883059675256848178735965394296971466493355822289379591243712380 4$. Let $y = 10299998060278180059384605662607406637699177271974548426049829625141450979 0$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 151450626728569334024095466109399353011484074347218855622905577188082652393$. Take $m = 151450626728569334024095466109399352806746036875269017745457192159470122193$. Take $q = 4591625259702988228391724076430745504856765437749370689073135000181$.

Let $a = 0$. Let $b = 116985152300880497947440912881669746366755390462876614681718009347549468$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 20252850467634157328674260484648637075587737223843607908065021016844635 4$. Let $y = 3286855284210776065122037916636114450305829983111194846703705918099812 01$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 459162525970298822839172407643074550485676543774937068907313500018 1$. Take $m = 459162525970298822839172407643074123186521517139675403647973677050 0$. Take $q = 796465786592018773355025858877838895379915901369775201470899 7$.

Let $a = 1$. Let $b = 0$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 237427461890599071888969186920506112763408159072630086$
5812968469635. Let $y = 38367219002965994775673261806256076814$
$962129662727527961523547975 7$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 79646578659201877335502585887783895379915901369775201470899 7$. Take $m = 7964657865920187733550258588773810638939352775434555226023556$. Take $q = 46231964208132228131314046000451662674657832637364201781$.

Let $a = 1$. Let $b = 0$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 60414701403123490426690866902429638515117721858588270$
5962055. Let $y = 17247628314682306693012688190527951160557281$
4499246652383446.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 462319642081322281313140460004516626746578326373642017781$. Take $m = 462319642081322281313140460126024589750710797988236442 89$. Take $q = 269277855886647145626098181714329505192010862537$.

Let $a = 206777679108328028700194019213312000$. Let $b = 395329222117547444754594241709635758770590021809666286 1$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 4152168663824077484410871800875785348909511073656353384$. Let $y = 12714995926925125699262124877691657771661403525855322568$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 269277855886647145626098181714329505192010862537$.
Take $m = 26927785588664714562609742241658332688786076084 8$.
Take $q = 37139404500138797440849761860234366140 27$.

Let $a = 12139398828774616211924530580125158091584691777 0$. Let $b = 8929426572608661560449174737622124157676431719 9$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 1790912847420902704320665488235547330888775491 6$. Let $y = 5168078539300924906552242538548862732742647026 0$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 37139404500138797440849761860234366140 27$. Take $m = 37139404500138797440137060501731895838 83$. Take $q = 1892646613674708120070175839664266 21$.

Let $a = 0$. Let $b = 153043474036576283192901331448771942629 4$.
Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 346555956904808203665829694323454029937 1$. Let $y = 15455$ $6663705981753828916231341961895721 0$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 189264661367470812007017583966426621$. Take $m = 189264661367470811341443996762012552$. Take $q = 8272077124291510999390732633$.

Let $a = 189264661367470812007017583966426620$. Let $b = 0$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 2994552712719952937424639583567913 6$. Let $y = 7870057519$ $78694471103338071720280 6$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 827207712429151099939073263 3$. Take $m = 827207712429168767964247009 6$. Take $q = 596507384067483024 19$.

Let $a = 0$. Let $b = 529385735940965341344182 4898$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 6183657276380485715999330220$. Let $y = 31471716501985659$
70285659119.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Take $N = 596507384067483024 19$. Take $m = 5965073842169870259 3$.
Take $q = 2010269889182041$.

Let $a = 0$. Let $b = 348999695425202910 15$. Take the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $x = 355099178145127926 69$. Let $y = 59373401505423430 58$.

Take the point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$. One can show that

- $m = qs$ for some $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

But we do not have a proof that q is prime.

Recall that

$$q = 2010269889182041.$$

One can easily check that all primes below

$$\lceil \sqrt{q} \rceil = 44836034$$

do not divide q.
Hence q is prime. Thus 11985580716290575435344118941008093420257596124614609137753411194721046383422470007966153065685391464617858193 is prime.

Thank you for listening! Visit

https://pari.math.u-bordeaux.fr/Events/PARI2018/talks/ecpp.pdf

for more details.