Malleability of RSA moduli

Luis Dieulefait and Jorge J. Urroz, UB and UPC, Barcelona

Popayan, June, 2019

Problem. (Malleability of Factoring) Given and RSA modulus n find another integer n' so that the factorization of n' will help to factorize n.

Problem. (Malleability of Factoring) Given and RSA modulus n find another integer n' coprime to n :) so that the factorization of n' will help to factorize n.

Conjecture. Factoring is not malleable.

Conjecture. Factoring is not malleable.

Theorem. Given any $n = pq$ RSA modulus there exist another integer n' so that factoring n' allow us to factor n in polynomial time.

Conjecture. Factoring is not malleable.

Theorem. Given any $n = pq$ RSA modulus there exist another integer n' so that factoring n' allow us to factor n in polynomial time.

$n' = 2^n - 1$

A particular case

Theorem (L. Dieulefait and J. Jiménez Urroz, 2009)

Let $n = pq$ $z < p, q < 2z$, *be and RSA modulus such that either we have* $2^{p-1} \not\equiv 1 \pmod{q}$ *or* $2^{q-1} \not\equiv 1 \pmod{p}$ *and let* $n' = 2^n - 1$. *Then, with the factorization of* n' *we can find a prime divisor of* n *in polynomial time.*

A particular case

Theorem (L. Dieulefait and J. Jiménez Urroz, 2009)

Let $n = pq$ $z < p, q < 2z$, be and RSA modulus such that either we have $2^{p-1} \not\equiv 1 \pmod q$ or $2^{q-1} \not\equiv 1 \pmod p$ and let $n' = 2^n - 1$. Then, with the factorization of n' we can find a prime divisor of n in polynomial time.

Proof To factor n we use an oracle $\mathcal{O}$ that allow us to factor any given n‘ coprime to n. Let $S = \{r \pmod n \neq 1, r|n', \text{ prime}\}$

A particular case

Theorem (L. Dieulefait and J. Jiménez Urroz, 2009)

Let $n = pq$ $z < p, q < 2z$, be and RSA modulus such that either we have $2^{p-1} \not\equiv 1 \pmod{q}$ or $2^{q-1} \not\equiv 1 \pmod{p}$ and let $n' = 2^n - 1$. Then, with the factorization of n' we can find a prime divisor of n in polynomial time.

Proof To factor n we use an oracle $\mathcal{O}$ that allow us to factor any given n‘ coprime to n. Let $S = \{r \pmod{n} \neq 1, r|n', \text{ prime}\}$

Algorithm.

- Send n' in binary form to $\mathcal{O}$.
- Take $r \in S$ and compute $(r-1, n) = p$.

Step 1. There exist such r. Indeed if every prime of $2^n - 1$ is 1 modulo n then $2^n - 1 \equiv 1 \pmod{n}$ or $2^{n-1} \equiv 1 \pmod{n}$

$$2^{n-1} \equiv 1 \pmod{p}, \text{ and } 2^{n-1} \equiv 1 \pmod{q}$$

But

$$2^{n-1} = 2^{(p-1)q+q-1} \equiv 2^{q-1} \pmod{p}$$

So,

$$2^{q-1} \equiv 1 \pmod{p}, \text{ and } 2^{p-1} \equiv 1 \pmod{q}$$

Step 1. There exist such r. Indeed if every prime of $2^n - 1$ is 1 modulo n then $2^n - 1 \equiv 1 \pmod{n}$ or $2^{n-1} \equiv 1 \pmod{n}$

$$2^{n-1} \equiv 1 \pmod{p}, \text{ and } 2^{n-1} \equiv 1 \pmod{q}$$

But

$$2^{n-1} = 2^{(p-1)q+q-1} \equiv 2^{q-1} \pmod{p}$$

So,

$$2^{q-1} \equiv 1 \pmod{p}, \text{ and } 2^{p-1} \equiv 1 \pmod{q}$$

Step 2. $2^n \equiv 1 \pmod{r}$ and $2^{r-1} \equiv 1 \pmod{r}$ Hence

$$2^{(n,r-1)} \equiv 1 \pmod{r}$$

and $(n, r-1) \neq 1, n$. Note that $(n, r-1) = (n, r \pmod{n} - 1)$

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

The previous algorithm does not work for pseudoprime modulus.

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

The previous algorithm does not work for pseudoprime modulus.

Are there any?...

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

The previous algorithm does not work for pseudoprime modulus.

Are there any?...well... yes 341 is the smallest

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

The previous algorithm does not work for pseudoprime modulus.

Are there any?...well... yes 341 is the smallest

Are there infinitely many pseudoprimes?

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

The previous algorithm does not work for pseudoprime modulus.

Are there any?...well... yes 341 is the smallest

Are there infinitely many pseudoprimes?

Theorem. (Alford, Granville, Pomerance, 1994) There are infinitely many Charmichael numbers.

A Charmichael number is a composite number n such that $b^{n-1} \equiv 1 \pmod{n}$ for all $(b, n)) = 1$. Example $561 = 3 \cdot 11 \cdot 17$.

Theorem. (Pomerance, 1981) Given $x > 0$, the number of pseudoprimes up to x is less than

$$x \exp(-\frac{1}{2} \log x \log \log \log x / \log \log x)$$

Theorem. (Pomerance, 1981) Given $x > 0$, the number of pseudoprimes up to x is less than

$$x \exp(-\frac{1}{2} \log x \log \log \log x / \log \log x)$$

Proposition For large z, the number of RSA moduli $n = pq$, $z < p, q < 2z$ pseudoprimes are less than

$$\left(\frac{z}{\log z}\right)^2 \frac{(\log \log z)^2}{\log z}$$

Proof.
$2^{(p-1,q-1)} \equiv 1 \pmod{n}$ not possible if $(p-1, q-1) < \log z$. Let $\pi(d,z) = |\{p \equiv 1 \pmod{d}, z < p < 2z\text{prime }\}|$.

$$\sum_{\substack{z<p,q<2z \\ (p-1,q-1)>\log z}} 1 = \sum_{\log z<d<z} \pi(d,z)^2 \sim \sum_{\log z<d<z} \left(\frac{z}{\varphi(d)\log z}\right)^2$$

Since

$$\varphi(d) = d\prod_{p|d}\left(1-\frac{1}{p}\right) > d\prod_{p<\log d}\left(1-\frac{1}{p}\right) > \frac{Cd}{\log\log d}$$

$$\sum_{\log z<d<z}\frac{1}{\varphi(d)^2} < c\sum_{\log z<d<z}\frac{(\log\log d)^2}{d^2} < \frac{c(\log\log z)^2}{\log z}.$$

Theorem. (Barban-Davenport-Halberstam, 1963-1966)

$$\sum_{d \leq z^{1-\varepsilon}} \left| \psi(d, z) - \frac{z}{\varphi(d)} \right|^2 \ll \frac{z^2}{(\log z)^A},$$

with a constant depending only in ε and A.

Primitive roots and the general case.

To avoid the pseudoprime moduli, we will choose another integer m and $n' = m^n - 1$ with a prime factor not 1 modulo n.

Primitive roots and the general case.

To avoid the pseudoprime moduli, we will choose another integer m and $n' = m^n - 1$ with a prime factor not 1 modulo n.

Definition. Given a prime p, a primitive root modulo p is an integer so that $< m >= \mathbb{F}_p^*$. $m^d \not\equiv 1 \pmod{p}$ for any $d < p - 1$.

Primitive roots and the general case.

To avoid the pseudoprime moduli, we will choose another integer m and $n' = m^n - 1$ with a prime factor not 1 modulo n.

Definition. Given a prime p, a primitive root modulo p is an integer so that $< m >= \mathbb{F}_p^*$. $m^d \not\equiv 1 \pmod{p}$ for any $d < p - 1$.

If $n = pq$, $q < p$ and m is a primitive root modulo p, $m^{n-1} \not\equiv 1 \pmod{n}$, since $m^{q-1} \not\equiv 1 \pmod{p}$.

Question. How difficult is to find a primitive root modulo p without knowing p?.

There are $\varphi(p-1)$ primitive roots modulo p. Hence the probability to find one is

$$\frac{\varphi(p-1)}{p-1} = \prod_{q|p-1}\left(1-\frac{1}{q}\right) > \prod_{q<\log p}\left(1-\frac{1}{q}\right) > \frac{c}{\log\log p}.$$

Question. How difficult is to find a primitive root modulo p without knowing p?.

There are $\varphi(p-1)$ primitive roots modulo p. Hence the probability to find one is

$$\frac{\varphi(p-1)}{p-1} = \prod_{q|p-1}\left(1-\frac{1}{q}\right) > \prod_{q<\log p}\left(1-\frac{1}{q}\right) > \frac{c}{\log\log p}.$$

In particular a random set of size $C\log\log p$ should have positive probability to contain a primitive root modulo p. Since $p < n$ a set of size $C\log\log n$ should have positive probability to contain a primitive root modulo p. The probability for a set of this size to contain no primitive roots is

$$\left(1-\frac{c}{\log\log p}\right)^{C\log\log p} \sim e^{-Cc}.$$

Results.

(E. Bach, 1997) Let $g(p)$ the least prime primitive root modulo p. Heuristically we have

$$g(p) \leq e^{\gamma} \log p (\log \log p)^2 (1 + \varepsilon).$$

Results.

(E. Bach, 1997) Let $g(p)$ the least prime primitive root modulo p. Heuristically we have

$$g(p) \leq e^{\gamma} \log p (\log \log p)^2 (1+\varepsilon).$$

Theorem (V. Shoup, 1992) Under GRH, $g(p) \ll (\log p)^6$

Results.
(E. Bach, 1997) Let $g(p)$ the least prime primitive root modulo p. Heuristically we have

$$g(p) \leq e^{\gamma} \log p (\log\log p)^2 (1+\varepsilon).$$

Theorem (V. Shoup, 1992) Under GRH, $g(p) \ll (\log p)^6$

Conjecture (Artin, 1927) Any given integer a not $1, -1$ or a perfect square is a primitive root for a positive proportion of primes,

$\prod_q \left(1 - \frac{1}{q(q-1)}\right) \sim 0.37395$, for squarefree $a \neq 1 \pmod 4$.

Results.

(E. Bach, 1997) Let $g(p)$ the least prime primitive root modulo p. Heuristically we have

$$g(p) \leq e^{\gamma} \log p (\log \log p)^2 (1+\varepsilon).$$

Theorem (V. Shoup, 1992) Under GRH, $g(p) \ll (\log p)^6$

Conjecture (Artin, 1927) Any given integer a not $1, -1$ or a perfect square is a primitive root for a positive proportion of primes,

$\prod_q \left(1 - \frac{1}{q(q-1)}\right) \sim 0.37395$, for squarefree $a \neq 1 \pmod 4$.

Theorem. (Heath-Brown, 1986) Among $3, 5, 7$ there is a primitive root for infinitely many p

For each integer m set $n'_m = (m^n - 1)/(m - 1)$, and $S_m = \{r \pmod{n} \neq 1 : r \text{ prime } r | n'_m\}$.

For each integer m set $n'_m = (m^n - 1)/(m-1)$, and
$S_m = \{r \pmod{n} \neq 1 : r \text{ prime } r | n'_m\}$.

Algorithm The m-ary representation of n'_m is c independent of m

- m=2
- Send (c, m) to $\mathcal{O}$
- $S =, \ m = m + 1$. Return
- take $r \in S$ and compute $d = (r - 1, n)$.

For each integer m set $n'_m = (m^n - 1)/(m-1)$, and $S_m = \{r \pmod n \neq 1 : r \text{ prime } r | n'_m\}$.

Algorithm The m-ary representation of n'_m is c independent of m

- m=2
- Send (c, m) to $\mathcal{O}$
- $S =$, $m = m + 1$. Return
- take $r \in S$ and compute $d = (r - 1, n)$.

Theorem (L. Dieulefait and J. Jiménez Urroz)

Let $n = pq$ $z < p, q < 2z$, be and RSA modulus . Then, under GRH the previous algorithm gives a prime divisor of n in polynomial time.

Proof

Lemma Let $n = pq$ and RSA modulus and m such that $(m-1, n) = 1$. Then $(n'_m, m-1) = 1$. If $r|(n'_m, m-1)$, then $n'_m = \sum_{j=0}^{n-1} m^j \equiv n \pmod{r}$.

Step 1. There exist such r. Indeed if every prime of n'_m is 1 modulo n then $n'_m \equiv 1 \pmod{n}$ or $m^{n-1} \equiv 1 \pmod{n}$

$$m^{n-1} \equiv 1 \pmod{p}, \text{ and } m^{n-1} \equiv 1 \pmod{q}$$

But

$$m^{n-1} = m^{(p-1)q+q-1} \equiv m^{q-1} \pmod{p}$$

which is not possible.

Proof

Lemma Let $n = pq$ and RSA modulus and m such that $(m-1, n) = 1$. Then $(n'_m, m-1) = 1$. If $r|(n'_m, m-1)$, then $n'_m = \sum_{j=0}^{n-1} m^j \equiv n \pmod r$.

Step 1. There exist such r. Indeed if every prime of n'_m is 1 modulo n then $n'_m \equiv 1 \pmod n$ or $m^{n-1} \equiv 1 \pmod n$

$$m^{n-1} \equiv 1 \pmod p, \text{ and } m^{n-1} \equiv 1 \pmod q$$

But

$$m^{n-1} = m^{(p-1)q+q-1} \equiv m^{q-1} \pmod p$$

which is not possible.

Step 2. $m^n \equiv 1 \pmod r$ and $m^{r-1} \equiv 1 \pmod r$. Hence

$$m^{(n,r-1)} \equiv 1 \pmod r$$

and $(n, r-1) \neq 1, n$. Note that $(n, r-1) = (n, r \pmod n - 1)$

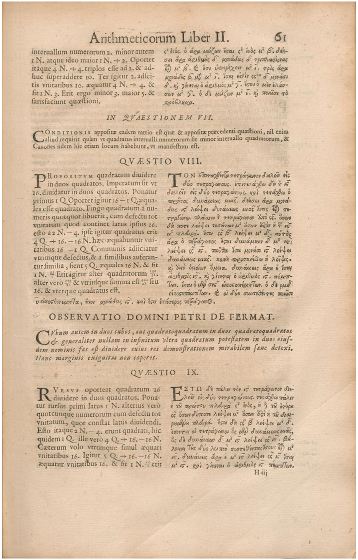
And... ¿Without cheating?

And... ¿Without cheating? We are looking for a number n' which helps to factorize n.

And... ¿Without cheating? We are looking for a number n' which helps to factorize n.

elliPtiC cUuuuurvesssss

Arithmeticorum, 1670, Diophanti Alexandrini



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto a 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & a similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

H iij

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

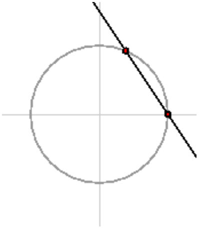
Find the integral solutions of $x^2 + y^2 = z^2$

Find the integral solutions of $x^2 + y^2 = z^2$

Find the rationals solutions of $x^2 + y^2 = 1$

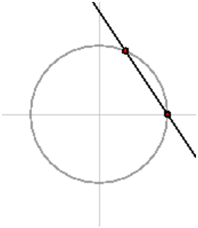
Find the integral solutions of $x^2 + y^2 = z^2$

Find the rationals solutions of $x^2 + y^2 = 1$



Find the integral solutions of $x^2 + y^2 = z^2$

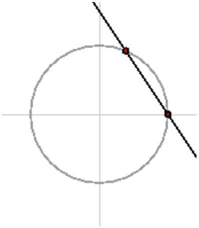
Find the rationals solutions of $x^2 + y^2 = 1$



$y = t(x - 1)$

Find the integral solutions of $x^2 + y^2 = z^2$

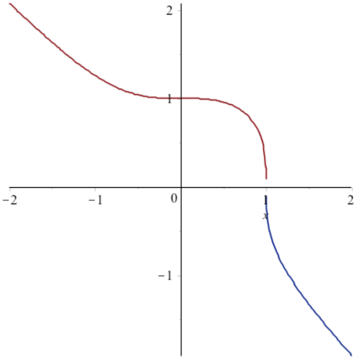
Find the rationals solutions of $x^2 + y^2 = 1$



$$y = t(x-1) \text{ , then } x = \frac{t^2-1}{t^2+1} \quad y = \frac{2t}{t^2+1}$$

Find the rational solutions of $x^3 + y^3 = 1$

Find the rational solutions of $x^3 + y^3 = 1$



We parametrize by $y = t(x-1)$, to get

$$(t^3+1)x^2 + (1-2t^3)x + (1+t^3) = 0$$

Changing variables $x = u + t$, $y = u - t$, we get

$$2u^3 + 6ut^2 = 1$$

Changing variables $x = u + t$, $y = u - t$, we get

$$2u^3 + 6ut^2 = 1$$

Multiplying by $(6/u)^3$, and letting $6/u = X, 36t/u = Y$, we get

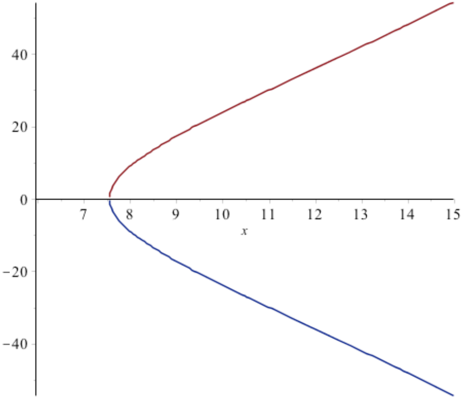
$$Y^2 = X^3 - 432.$$

Changing variables $x = u + t$, $y = u - t$, we get

$$2u^3 + 6ut^2 = 1$$

Multiplying by $(6/u)^3$, and letting $6/u = X, 36t/u = Y$, we get

$$Y^2 = X^3 - 432.$$



Every cubic can be written as $y^2 = x^3 + ax + b$,

Every cubic can be written as $y^2 = x^3 + ax + b$,

Definition

Given a field K. An elliptic curve over K is the set

$$E/K := \{(x, y) \in K \times K \, : \, y^2 = x^3 + ax + b, a, b \in K\} \cup \{O\}$$

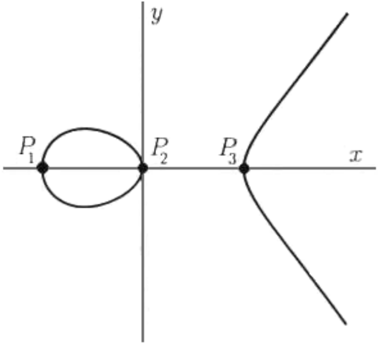
$$4a^3 + 27b^2 \neq 0.$$

Every cubic can be written as $y^2 = x^3 + ax + b$,

Definition

Given a field K. An elliptic curve over K is the set

$$E/K := \left\{(x, y) \in K \times K \; : \; y^2 = x^3 + ax + b, a, b \in K\right\} \cup \{O\}$$
$$4a^3 + 27b^2 \neq 0.$$



Key point on the theory of elliptic curves:

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

$(E(\mathbb{Q}), +)$ is a finitely generated abelian group

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q})$$

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

$(E(\mathbb{Q}), +)$ is a finitely generated abelian group

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q})$$

Group law:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \left(\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}\right)$$

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

$(E(\mathbb{Q}), +)$ is a finitely generated abelian group

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q})$$

Group law:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \left(\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}\right)$$

Theorem

(Mazur, 1978) If C_n denotes the cyclic group of order n, then the groups that appear as $E_{tors}(\mathbb{Q})$ are C_n with $1 \leq n \leq 10$, C_{12} and $C_2 \times C_2$, $C_2 \times C_4$, $C_2 \times C_6$, and $C_2 \times C_8$.

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

$(E(\mathbb{Q}), +)$ is a finitely generated abelian group

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q})$$

Group law:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \left(\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}\right)$$

Theorem

(Mazur, 1978) If C_n denotes the cyclic group of order n, then the groups that appear as $E_{tors}(\mathbb{Q})$ are C_n with $1 \le n \le 10$, C_{12} and $C_2 \times C_2$, $C_2 \times C_4$, $C_2 \times C_6$, and $C_2 \times C_8$.

The rank, r, is highly unknown.

Very nice. But what do we do now? Can we find points?

Very nice. But what do we do now? Can we find points?

On the elliptic curve $y^2 = x^3 + 877x$, the smallest non trivial point is

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}$$

Very nice. But what do we do now? Can we find points?

On the elliptic curve $y^2 = x^3 + 877x$, the smallest non trivial point is

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}$$

Try to generalize Hasse's principle: Every quadratic form has integer solutions, if and only if has solutions in every completion of $\mathbb{Q}$

Very nice. But what do we do now? Can we find points?

On the elliptic curve $y^2 = x^3 + 877x$, the smallest non trivial point is

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}$$

Try to generalize Hasse's principle: Every quadratic form has integer solutions, if and only if has solutions in every completion of $\mathbb{Q}$

Corollary

$x^2 + 2y^2 = 5z^2$ has no non-trivial integer solutions.

Theorem (Hasse, 1930)

$E/\mathbb{F}_q$ is an abelian group of size

$$|E/\mathbb{F}_q| = q + 1 - a_q$$

where

$$|a_q| \leq 2\sqrt{q}.$$

Theorem (Hasse, 1930)

$E/\mathbb{F}_q$ is an abelian group of size

$$|E/\mathbb{F}_q| = q + 1 - a_q$$

where

$$|a_q| \leq 2\sqrt{q}.$$

Example Consider the curve $y^2 = x^3 - 1$ and $q \equiv 2 \pmod 3$. Then, $E(\mathbb{F}_q) = q + 1$.

Defintion. Given an integer $n = pq$ an elliptic curve modulo n is the set

$$E_n := E/\mathbb{F}_p \times E/\mathbb{F}_q.$$

Defintion. Given an integer $n = pq$ an elliptic curve modulo n is the set

$$E_n := E/\mathbb{F}_p \times E/\mathbb{F}_q.$$

$$|E_n| = |E/\mathbb{F}_p| \times |E/\mathbb{F}_q|.$$

Defintion. Given an integer $n = pq$ an elliptic curve modulo n is the set

$$E_n := E/\mathbb{F}_p \times E/\mathbb{F}_q.$$

$$|E_n| = |E/\mathbb{F}_p| \times |E/\mathbb{F}_q|.$$

Lemma. Let $n = pq$ with $p \approx q$. Then,

$$||E_n| - n| \leq cn^{3/4}.$$

Theorem (L. Dieulefait and J. Jiménez Urroz, 2019)

Let $n = pq$, and E_n and elliptic curve modulo n. Then knowing the factors of $|E_n|$ we can factor n in polynomial time.

Theorem (L. Dieulefait and J. Jiménez Urroz, 2019)

Let $n = pq$, and E_n and elliptic curve modulo n. Then knowing the factors of $|E_n|$ we can factor n in polynomial time.

Proof.

Theorem (J. Cilleruelo-J. Jiménez Urroz)

In an arc of lenght $cn^{1/4}$ of the hyperbola $xy = n$ there are at most 4 points of integer coordinates.

Theorem (L. Dieulefait and J. Jiménez Urroz, 2019)

Let $n = pq$, and E_n and elliptic curve modulo n. Then knowing the factors of $|E_n|$ we can factor n in polynomial time.

Proof.

Theorem (J. Cilleruelo-J. Jiménez Urroz)

In an arc of lenght $cn^{1/4}$ of the hyperbola $xy = n$ there are at most 4 points of integer coordinates.

So, we ask the oracle for the factors of E_n of size $n^{1/2}$. Note that $p + 1 - a_p$ and $q + 1 - a_q$ are two of those points.

Theorem (L. Dieulefait and J. Jiménez Urroz, 2019)

Let $n = pq$, and E_n and elliptic curve modulo n. Then knowing the factors of $|E_n|$ we can factor n in polynomial time.

Proof.

Theorem (J. Cilleruelo-J. Jiménez Urroz)

In an arc of lenght $cn^{1/4}$ of the hyperbola $xy = n$ there are at most 4 points of integer coordinates.

So, we ask the oracle for the factors of E_n of size $n^{1/2}$. Note that $p + 1 - a_p$ and $q + 1 - a_q$ are two of those points. Use Coppersmith algorithm to find p.

Theorem (Coppersmith)

If we know an integer $n = pq$ and we know the high order $\frac{1}{4} log_2 N$ bits of p, then we can recover p and q in polynomial time in $log(n)$

.

Theorem

Finding the number of points of elliptic curves modulo n is equivalent to factoring n.

Theorem

Finding the number of points of elliptic curves modulo n is equivalent to factoring n.

N. Kunihiro and K. Koyama in communications of NTT science lab prove to be computationally equivalent, assuming uniform distribution of a_p.

Theorem

Finding the number of points of elliptic curves modulo n is equivalent to factoring n.

N. Kunihiro and K. Koyama in communications of NTT science lab prove to be computationally equivalent, assuming uniform distribution of a_p.

S. Martin, P. Morillo and J. Villar find an algorithm that with input the order of a point, find the factorization of n with positive probability.

Let $\hat{E}, \tilde{E}, \bar{E}$ the three possible twists of E. Then

$$\begin{aligned}
E &= (p - a_p)(q - a_q) = n - pa_q - qa_p + a_pa_q \\
\hat{E} &= (p + a_p)(q + a_q) = n + pa_q + qa_p + a_pa_q, \\
\tilde{E} &= (p - a_p)(q + a_q) = n + qa_q - qa_p - a_pa_q, \\
\bar{E} &= (p + a_p)(q - a_q) = n - pa_q + qa_p - a_pa_q.
\end{aligned}$$

Lemma

$$|E| + |\hat{E}| + |\tilde{E}| + |\bar{E}| = 4n$$
$$E\hat{E} = \tilde{E}\bar{E}.$$

Then, knowing E and $\hat{E}$, we compute its product, $M = E\hat{E}$ and its sum $L = E + \hat{E}$, and we have

$$\tilde{E}\bar{E} = M$$
$$\tilde{E} + \bar{E} = 4n - L$$

so $\tilde{E}$ and $\bar{E}$ are the solutions of the quadratic polynomial $X^2 - (4n - L)X + M$.

Lemma

$$|E| + |\hat{E}| + |\tilde{E}| + |\bar{E}| = 4n$$
$$E\hat{E} = \tilde{E}\bar{E}.$$

Then, knowing E and $\hat{E}$, we compute its product, $M = E\hat{E}$ and its sum $L = E + \hat{E}$, and we have

$$\tilde{E}\bar{E} = M$$
$$\tilde{E} + \bar{E} = 4n - L$$

so $\tilde{E}$ and $\bar{E}$ are the solutions of the quadratic polynomial $X^2 - (4n - L)X + M$.

$\gcd(E + \bar{E}, n) = p$