ECC summer school, 1 September 2016, Izmir

Overview - Algebraic Number Theory in Cryptography

Razvan Barbulescu
CNRS and IMJ-PRG

Starting point

Notations

- q prime
- g a generator of $(\mathbb{F}_q)^*$
- X a (secret) integer less than q
- $Y = g^X \bmod q$.

Quote

"Computing X from Y, on the other hand can be computed much more difficult and, for certain carefully chosen values of q, requires on the order of $q^{1/2}$ operations [...]"

Diffie and Hellman 1976

Indeed, the best known algorithm in 1976 was Baby step giant step.

The DLP was as hard for $(\mathbb{F}_q)^*$ as for any other group (e.g. elliptic curves).

The L notation

For any integer $Q = e^n$, $L_Q(\alpha, c) = \exp\left(cn^\alpha(\log n)^{1-\alpha}\right)$.
When c is not specified we write $L_Q(\alpha)$.

Example

- $L_Q(1, \frac{1}{2}) = \exp\left(\frac{1}{2}n\right) = \sqrt{\exp(n)} = \sqrt{Q}$ (exponential algorithm).
- $L_Q(0, 3) = \exp\left(3\log n\right) = n^3$ (cubic algorithm)
- $L_Q(1/2, 1) = \exp\left(\sqrt{n}\sqrt{\log n}\right) \approx \exp\left(\sqrt{n}\right) = e^{\sqrt{n}}$ (sub-exponential algorithm).

Exercice

- $L_{L_x(\alpha)}(\beta) = L_x(\alpha\beta)$.
- $L(\alpha)L(\beta) = L(\max(\alpha, \beta))^{1+o(1)}$.

History

- One year after the introduction of DLP in cryptography, a subexponential algorithm was proposed by Adleman (complexity $L(1/2)$).
- In 1978 when RSA was proposed, it was known that the continued fractions method of factorization was very fast. In early 80s Dixon and Pomerance proved that there are algorithms of complexity $L(1/2)$.
- Ideas traveled from factorization to discrete logarithm in finite fields and vice-versa.

Chronology

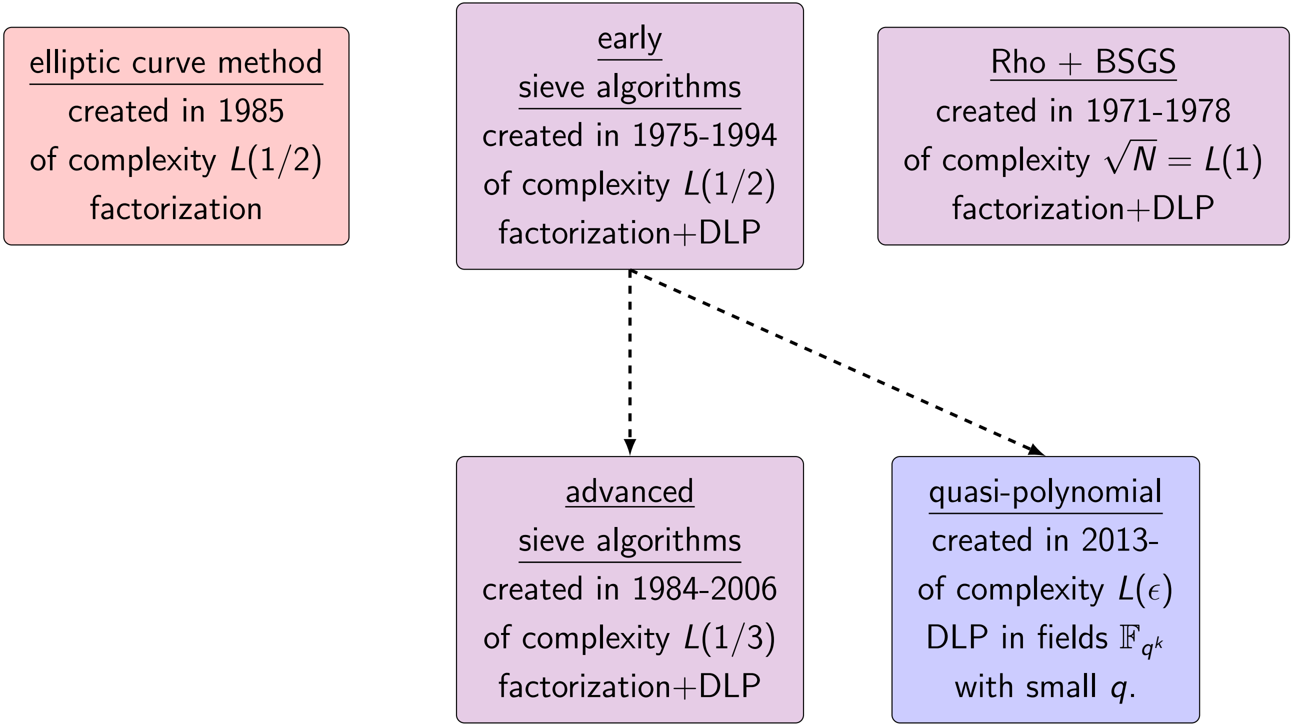
Dates below give the publication year of the first algorithm of each class. For discrete logarithm, one uses different algorithms depending on the characteristic of the field, which have distinct publication dates.

complexity	factorization	DLP in finite fields
$L_Q(1/2)$	1970[a]	1979 – 1994
$L_Q(1/3)$	1989	1984 – 2006
$L_Q(\epsilon)$	––	2013–

[a] complexity unknown until 1980 (after the introduction of RSA)

Algorithms families

Let us use red for factoring, blue for DLP and violet for both.



elliptic curve method

created in 1985

of complexity $L(1/2)$

factorization

early sieve algorithms

created in 1975-1994

of complexity $L(1/2)$

factorization+DLP

Rho + BSGS

created in 1971-1978

of complexity $\sqrt{N} = L(1)$

factorization+DLP

advanced sieve algorithms

created in 1984-2006

of complexity $L(1/3)$

factorization+DLP

quasi-polynomial

created in 2013-

of complexity $L(\epsilon)$

DLP in fields $\mathbb{F}_{q^k}$

with small q.

Plan of the lecture

- Introduction
- Index Calculus
- Quadratic sieve (QS/MPQS)
- Sieving

Smoothness

Integers

- definition An integer is B-smooth if all its prime factors are less than B.
- computation One finds small prime divisors with ECM, which
  - is probabilistic;
  - relies on a conjecture of analytic number theory;
  - given an integer x, it finds all its factors less than B in average time $L_B(1/2, \sqrt{2})^{1+o(1)} \log(x)^4$. In practice, the dependency in $\log x$ is quadratic.

Polynomials

- definition A polynomial in $\mathbb{F}_q[t]$ is m-smooth if all its irreducible factors have degree less than or equal to m.
- computation One tests if a polynomial $P(t)$ is m-smooth by one of the two methods below:
  - by factoring it (correctness is trivial, probabilistic, slow);
  - by taking gcd with $P'(t) \cdot (t^{q^m} - t)$ (prove it!, deterministic, faster).

Smoothness

Integers

- definition An integer is B-smooth if all its prime factors are less than B.
- computation One finds small prime divisors with ECM, which
  - is probabilistic;
  - relies on a conjecture of analytic number theory;
  - given an integer x, it finds all its factors less than B in average time $L_B(1/2,\sqrt{2})^{1+o(1)}\log(x)^4$. In practice, the dependency in $\log x$ is quadratic.

Polynomials

- definition A polynomial in $\mathbb{F}_q[t]$ is m-smooth if all its irreducible factors have degree less than or equal to m.
- computation One tests if a polynomial $P(t)$ is m-smooth by one of the two methods below:
  - by factoring it (correctness is trivial, probabilistic, slow);
  - by taking gcd with $P'(t)\cdot(t^{q^m}-t)$ (prove it!, deterministic, faster).

It is not known how to define smooth elements on an elliptic curves with a fast smoothness test.

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$7^{5} \bmod p \;=\; 4706 = 2 \cdot 13 \cdot 181$$

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$\begin{aligned} 7^5 \bmod p &= 4706 = 2 \cdot 13 \cdot 181 \\ 7^{6} \bmod p &= 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23 \end{aligned}$$

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$\begin{aligned}
7^5 \bmod p &= 4706 = 2 \cdot 13 \cdot 181 \\
7^6 \bmod p &= 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23 \\
7^7 \bmod p &= 675 = 3^3 \cdot 5^2
\end{aligned}$$

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$\begin{aligned} 7^5 \bmod p &= 4706 = 2 \cdot 13 \cdot 181 \\ 7^6 \bmod p &= 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23 \\ 7^7 \bmod p &= 675 = 3^3 \cdot 5^2 \end{aligned}$$

The last relation gives:

$$7 = 3 \log_7 3 + 2 \log_7 5$$

DLP: an example (1)

Parameters

- $p = 12101$
- $g = 7$ is a generator of $G = (\mathbb{Z}/p\mathbb{Z})^*$
- $\ell = 11$ is a prime factor of $(p-1) = \#G$
- $B = 10$ is the smoothness bound
- factor base $2, 3, 5, 7$

Finding relations among logs

$$\begin{aligned} 7^5 \bmod p &= 4706 = 2 \cdot 13 \cdot 181 \\ 7^6 \bmod p &= 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23 \\ 7^7 \bmod p &= 675 = 3^3 \cdot 5^2 \\ 7^8 \bmod p &= \dots \end{aligned}$$

The last relation gives:

$$\begin{aligned} 7 &= 3 \log_7 3 + 2 \log_7 5 \\ 25 &= 8 \log_7 2 + 1 \log_7 3 \\ 42 &= 6 \log_7 2 + 2 \log_7 5. \end{aligned}$$

DLP: an example (2)

Thanks to the Pohlig-Hellman reduction

we do the linear algebra computations modulo $\ell = 11$.

Linear algebra computations

We have to find the unknown $\log_7 2$, $\log_7 3$ and $\lg_7 5$ in the equation

$$\begin{pmatrix} 0 & 3 & 2 \\ 8 & 1 & 0 \\ 6 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} \log_7 2 \\ \log_7 3 \\ \log_7 5 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 25 \\ 42 \end{pmatrix} \mod 11.$$

Conjecture

The matrix obtained by the technique above has maximal rank.

We can drop all conjectures by modifying the algorithm, but this variant is fast and, even if the matrix has smaller rank we can find logs.

Solution

We solve to obtain $\log_7 2 \equiv 0 \mod 11$; $\log_7 3 \equiv 3 \mod 11$ and $\log_7 5 \equiv 10 \mod 11$. For this small example we can also use Pollard's rho method and obtain that

$$\log_7 3 = 8869 \equiv 3 \mod 11.$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

Smoothing by randomization

Consider a residue modulo p which is not 10-smooth, e.g. $h = 151$. We take random exponents a and test is $(g^a h) \bmod p$ is B-smooth.

$$7^{3} 151 \bmod p \;=\; 3389$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

Smoothing by randomization

Consider a residue modulo p which is not 10-smooth, e.g. $h = 151$. We take random exponents a and test is $(g^a h) \bmod p$ is B-smooth.

$$\begin{aligned} 7^3 151 \bmod p &= 3389 \\ 7^4 151 \bmod p &= 11622 = 2 \cdot 3 \cdot 13 \cdot 149 \end{aligned}$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

Smoothing by randomization

Consider a residue modulo p which is not 10-smooth, e.g. $h = 151$. We take random exponents a and test is $(g^a h) \bmod p$ is B-smooth.

$$\begin{aligned}
7^3 151 \bmod p &= 3389 \\
7^4 151 \bmod p &= 11622 = 2 \cdot 3 \cdot 13 \cdot 149 \\
7^5 151 \bmod p &= 8748 = 2^2 \cdot 3^7
\end{aligned}$$

DLP: an example (3)

At this point, we know discrete logarithms of the factor base and of smooth numbers:

$$\log_7(10) = \log_7 2 + \log_7 5 \equiv 10 \mod 11.$$

Smoothing by randomization

Consider a residue modulo p which is not 10-smooth, e.g. $h = 151$. We take random exponents a and test is $(g^a h) \bmod p$ is B-smooth.

$$\begin{aligned} 7^3 151 \bmod p &= 3389 \\ 7^4 151 \bmod p &= 11622 = 2 \cdot 3 \cdot 13 \cdot 149 \\ 7^5 151 \bmod p &= 8748 = 2^2 \cdot 3^7 \end{aligned}$$

The discrete logarithms of the two members are equal:

$$5 + \log_7(151) = 2 \log_7 2 + 7 \log_7 3.$$

We find $\log_7(151) \equiv 3 \mod 11$.

Remark

This part of the computations is independent of the relation collection and linear algebra stages. It is called individual logarithm stage.

Index Calculus

Input: p prime, g generator of $(\mathbb{Z}/p\mathbb{Z})^*$, ℓ prime divisor of $(p-1)$
h integer less than p

Output: $\log_g h \mod \ell$

```
Set $B$ to its optimal value
Make the list $\mathcal{F}$ of the primes less than $B$ (factor base)          ▷ Initialization
repeat
    $a \leftarrow$Random([1,p-1])
    if $(g^a \bmod p)$ is $B$-smooth then
        relations=relations $\bigcup \{a\}$                                     ▷ Relations collection
    end if
until $\#$relations $\geq \#\mathcal{F}$
Construct the matrix $M = (m_{a,q})$, $a$ in relations, $q \in \mathcal{F}$ as follows
            $m_{a,q} = \mathrm{val}_q\,(g^a \bmod p)\,.$                        ▷ Linear algebra
Solve the linear system        $Mx = (a)_{a \text{ in relations}}.$
repeat
    $b \leftarrow$Random([1,p-1])
until $(g^b h \bmod p)$ is $B$-smooth
Factor $(g^b h \bmod p) = \prod q_i^{e_i}$                                       ▷ Individual logarithm
return $x = \sum e_i \log_g(q_i) - b$
```

Plan of the lecture

- Introduction
- Index Calculus
- Quadratic sieve (QS/MPQS)
- Sieving

Fermat's idea

Idea

Fermat (XVII century) computed solutions of the equation

$$X^2 \equiv Y^2 \mod N. \tag{1}$$

It became a classical idea for factoring, e.g. mechanical machines were built in France in early XX century to solve the above equation.[a]

[a] "Discovery of a lost factoring machine", Shallit, Wiliams, Morain

Lemma

If $N = pq$, Equation (1) *has four solutions Y for each $X \neq 0$.*

Proof.

Using the identity $X^2 - Y^2 = (X - Y)(X + Y)$ we have $Y \equiv \pm X \mod p$ and $Y \equiv \pm X \mod q$. We call X' the unique integer less than N which satisfies the system

$$\begin{aligned} Y &\equiv -X \mod p \\ Y &\equiv X \mod q. \end{aligned}$$

Then the solutions of Equation (1) are $Y = X$, $Y = -X$, $Y = X'$ and $Y = -X'$. □

Fermat's idea

Idea

Fermat (XVII century) computed solutions of the equation

$$X^2 \equiv Y^2 \mod N. \tag{1}$$

It became a classical idea for factoring, e.g. mechanical machines were built in France in early XX century to solve the above equation.[a]

[a] "Discovery of a lost factoring machine", Shallit, Wiliams, Morain

Lemma

If $N = pq$, Equation (1) has four solutions Y for each $X \neq 0$.

Proof.

Using the identity $X^2 - Y^2 = (X - Y)(X + Y)$ we have $Y \equiv \pm X \mod p$ and $Y \equiv \pm X \mod q$. We call X' the unique integer less than N which satisfies the system

$$\begin{aligned} Y &\equiv -X \mod p \\ Y &\equiv X \mod q. \end{aligned}$$

Then the solutions of Equation (1) are $Y = X$, $Y = -X$, $Y = X'$ and $Y = -X'$. □

$$\boxed{\text{50\% of the solutions, i.e. } X' \text{ and } -X'\text{, give } \gcd(X - Y, N) = p \text{ or } q.}$$

Factoring: an example (1)

Not squares but smooth numbers

Let us factor $N = 2041$. We search integers a such that $a^2 - N$ is a square. In order to keep $a^2 - N$ small, we take a approximately equal to $\sqrt{N}$: 46, 47, ... Squares seem to be rare! Kraitchik (1922) proposed to collect integers which are 10-smooth.

We call factor base the set of primes less than 10: 2, 3, 5 and 7.

Collecting relations

$$46^2 - N \;=\; 75 \;= 3 \cdot 5^2$$

Factoring: an example (1)

Not squares but smooth numbers

Let us factor $N = 2041$. We search integers a such that $a^2 - N$ is a square. In order to keep $a^2 - N$ small, we take a approximately equal to $\sqrt{N}$: 46, 47, ... Squares seem to be rare! Kraitchik (1922) proposed to collect integers which are 10-smooth.

We call factor base the set of primes less than 10: 2, 3, 5 and 7.

Collecting relations

$$\begin{aligned} 46^2 - N &= 75 &&= 3 \cdot 5^2 \\ 47^2 - N &= 168 &&= 2^3 \cdot 3 \cdot 7 \end{aligned}$$

Factoring: an example (1)

Not squares but smooth numbers

Let us factor $N = 2041$. We search integers a such that $a^2 - N$ is a square. In order to keep $a^2 - N$ small, we take a approximately equal to $\sqrt{N}$: 46, 47, ... Squares seem to be rare! Kraitchik (1922) proposed to collect integers which are 10-smooth.

We call factor base the set of primes less than 10: 2, 3, 5 and 7.

Collecting relations

$$\begin{aligned} 46^2 - N &= 75 &= 3 \cdot 5^2 \\ 47^2 - N &= 168 &= 2^3 \cdot 3 \cdot 7 \\ 48^2 - N &= 263 &= 263^1 \end{aligned}$$

Factoring: an example (1)

Not squares but smooth numbers

Let us factor $N = 2041$. We search integers a such that $a^2 - N$ is a square. In order to keep $a^2 - N$ small, we take a approximately equal to $\sqrt{N}$: 46, 47, ... Squares seem to be rare! Kraitchik (1922) proposed to collect integers which are 10-smooth.

We call factor base the set of primes less than 10: 2, 3, 5 and 7.

Collecting relations

$$\begin{aligned} 46^2 - N &= 75 \; = 3 \cdot 5^2 \\ 47^2 - N &= 168 = 2^3 \cdot 3 \cdot 7 \\ 48^2 - N &= 263 = 263^1 \\ 49^2 - N &= 360 = 2^3 \cdot 3^2 \cdot 5 \end{aligned}$$

Factoring: an example (1)

Not squares but smooth numbers

Let us factor $N = 2041$. We search integers a such that $a^2 - N$ is a square. In order to keep $a^2 - N$ small, we take a approximately equal to $\sqrt{N}$: 46, 47, ... Squares seem to be rare! Kraitchik (1922) proposed to collect integers which are 10-smooth.

We call factor base the set of primes less than 10: 2, 3, 5 and 7.

Collecting relations

$$\begin{aligned}
46^2 - N &= 75 = 3 \cdot 5^2 \\
47^2 - N &= 168 = 2^3 \cdot 3 \cdot 7 \\
48^2 - N &= 263 = 263^1 \\
49^2 - N &= 360 = 2^3 \cdot 3^2 \cdot 5 \\
50^2 - N &= 459 = 3^3 \cdot 17
\end{aligned}$$

Factoring: an example (1)

Not squares but smooth numbers

Let us factor $N = 2041$. We search integers a such that $a^2 - N$ is a square. In order to keep $a^2 - N$ small, we take a approximately equal to $\sqrt{N}$: 46, 47, ... Squares seem to be rare! Kraitchik (1922) proposed to collect integers which are 10-smooth.

We call factor base the set of primes less than 10: 2, 3, 5 and 7.

Collecting relations

$$\begin{aligned}
46^2 - N &= 75 = 3 \cdot 5^2 \\
47^2 - N &= 168 = 2^3 \cdot 3 \cdot 7 \\
48^2 - N &= 263 = 263^1 \\
49^2 - N &= 360 = 2^3 \cdot 3^2 \cdot 5 \\
50^2 - N &= 459 = 3^3 \cdot 17 \\
51^2 - N &= 560 = 2^4 \cdot 5 \cdot 7
\end{aligned}$$

Factoring: an example (2)

Combining relations

With the previous relations we have, for all non-negative integers u_{46}, u_{47}, u_{49}, u_{51}:

$$\left(46^{2u_{46}}47^{2u_{47}}49^{2u_{49}}51^{2u_{51}}\right) \equiv 2^{3u_{47}+3u_{49}+4u_{51}}3^{u_{46}+u_{47}+2u_{49}}5^{2u_{46}+u_{49}+u_{51}}7^{u_{47}+u_{51}} \mod N$$

Linear algebra stage

We find u_{46}, u_{47}, u_{49}, u_{51} in $\mathbb{Z}/2\mathbb{Z}$ satisfying

$$\begin{aligned} u_{47}+3u_{49}+4u_{51} &\equiv 0 \mod 2\\ u_{46}+u_{47}+2u_{49} &\equiv 0 \mod 2\\ 2u_{46}+u_{49}+u_{51} &\equiv 0 \mod 2\\ u_{47}+u_{51} &\equiv 0 \mod 2. \end{aligned}$$

We obtain $u_{46}=u_{47}=u_{49}=u_{51}=1$.

Factoring: an example (3)

Computing X

We multiply the left sides of all the relations to find

$$\begin{aligned} X &= 46^{u_{46}} 47^{u_{47}} 49^{u_{49}} 51^{u_{51}} \mod N \\ &= 46 \cdot 47 \cdot 49 \cdot 51 \mod N \\ &= 311. \end{aligned}$$

Computing Y

We multiply the right sides of all the relations to find

$$\begin{aligned} Y &= \left(2^{3u_{47}+3u_{49}+4u_{51}} 3^{u_{46}+u_{47}+2u_{49}} 5^{2u_{46}+u_{49}+u_{51}} 7^{u_{47}+u_{51}}\right)^{1/2} \mod N \\ &= 2^5 \cdot 3^2 \cdot 5^2 \cdot 7 \mod N \\ &= 1416. \end{aligned}$$

Euclid gives the factorization!

Since $X \not\equiv \pm Y \mod N$, we succeed. We compute

$$\gcd(Y - X, N) = \gcd(1416 - 311, 2041) = 13.$$

The factorization is $2041 = 13 \cdot 157$.

Quadratic sieve

Input: integer $N = pq$ for two primes p and q
Output: p and q

```
Set $B$ to its optimal value
Make the list $\mathcal{F}$ of the primes less than $B$ (factor base)        ▷ Initialization
$a \leftarrow \lfloor \sqrt{N} \rfloor$
repeat$a \leftarrow a + 1$
    if $(a^2 - N)$ is $B$-smooth then
        relations=relations $\bigcup \{a\}$        ▷ Relations collection
    end if
until  $\#\text{relations} \geq \#\mathcal{F}$
 Construct the matrix $M = (m_{a,q})$, $a$ in relations, $q \in \mathcal{F}$ as follows
                $m_{a,q} = \text{val}_q\left(a^2 - N\right).$        ▷ Linear algebra
Solve the linear system        $\text{transpose}(x) M \equiv 0 \mod 2.$
Compute $X = \prod_{a \text{ in relations}} a^{x_a}$.
Compute $Y = \prod_{q \in \mathcal{F}} q^{(\sum_a x_a)/2}$.
Compute $g = \gcd(X - Y, N)$        ▷ Square root
if $g \neq 1$ or $N$ then
    return $p = g$, $q = N/g$
else
    Find more relations and do the linear algebra again.
end if
```

Plan of the lecture

- Introduction
- Index Calculus
- Quadratic sieve (QS/MPQS)
- Sieving

The idea of sieving

What we need

In QS, we collect integers $a = \lceil\sqrt{N}\rceil + x$, where x is a small integer, such that $a^2 - N$ is B-smooth.

We need to find the smooth values of $Q(x)$, when $Q(x) = \left(\lceil\sqrt{N}\rceil + x\right)^2 - N$.

Eratosthenes sieve

Given a polynomial $Q(x) \in \mathbb{Z}[x]$, one can compute the values x in an interval $[E_1, E_2]$ such that $Q(x)$ is prime. One marks with a line every value of x which is divisible by two, then by three and so on. The values of x which have no marks correspond to prime values of Q.

The idea of sieving

What we need

In QS, we collect integers $a = \lceil \sqrt{N} \rceil + x$, where x is a small integer, such that $a^2 - N$ is B-smooth.

We need to find the smooth values of $Q(x)$, when $Q(x) = \left(\lceil \sqrt{N} \rceil + x \right)^2 - N$.

Eratosthenes sieve

Given a polynomial $Q(x) \in \mathbb{Z}[x]$, one can compute the values x in an interval $[E_1, E_2]$ such that $Q(x)$ is prime. One marks with a line every value of x which is divisible by two, then by three and so on. The values of x which have no marks correspond to prime values of Q.

$\boxed{\text{Numbers which have many marks are smooth.}}$

Sieving: an example

Problem

Find values a in the interval $[3,7]$ such that $Q(a) = a^2 + 1$ is prime, respectively 6-smooth.

Table of sieving

a	3	4	5	6	7
ticks					
$\log(a^2+1)$	$\log 10$	$\log 17$	$\log 26$	$\log 37$	$\log 50$

Computations

Sieving: an example

Problem

Find values a in the interval $[3,7]$ such that $Q(a) = a^2 + 1$ is prime, respectively 6-smooth.

Table of sieving

a	3	4	5	6	7
ticks					
$\log(a^2+1)$	$\log 10$	$\log 17$	$\log 26$	$\log 37$	$\log 50$

Computations

Consider primes less than 6 and their powers less than $\max\{Q(a) \mid a \in [2,7]\}$:

- $\underline{p = 2,}$ solutions of $a^2 + 1 \equiv 0 \mod 2$ are $\{1\}$;

Sieving: an example

Problem

Find values a in the interval $[3, 7]$ such that $Q(a) = a^2 + 1$ is prime, respectively 6-smooth.

Table of sieving

a	3	4	5	6	7
ticks	/		/		/
$\log(a^2+1)$	$\log 5$	$\log 17$	$\log 13$	$\log 37$	$\log 25$

Computations

Consider primes less than 6 and their powers less than $\max\{Q(a) \mid a \in [2, 7]\}$:

- $\underline{p = 2}$, solutions of $a^2 + 1 \equiv 0 \mod 2$ are $\{1\}$;
- $\underline{q = 2^2}$, solutions of $a^2 + 1 \equiv 0 \mod 4$ are $\varnothing$;

Sieving: an example

Problem

Find values a in the interval $[3,7]$ such that $Q(a) = a^2 + 1$ is prime, respectively 6-smooth.

Table of sieving

a	3	4	5	6	7
ticks	$/$		$/$		$/$
$\log(a^2+1)$	$\log 5$	$\log 17$	$\log 13$	$\log 37$	$\log 25$

Computations

Consider primes less than 6 and their powers less than $\max\{Q(a) \mid a \in [2,7]\}$:

- $\underline{p = 2}$, solutions of $a^2 + 1 \equiv 0 \mod 2$ are $\{1\}$;
- $\underline{q = 2^2}$, solutions of $a^2 + 1 \equiv 0 \mod 4$ are $\varnothing$;
- $\underline{p = 3}$, solutions of $a^2 + 1 \equiv 0 \mod 3$ are $\varnothing$;

Sieving: an example

Problem

Find values a in the interval $[3,7]$ such that $Q(a) = a^2 + 1$ is prime, respectively 6-smooth.

Table of sieving

a	3	4	5	6	7
ticks	$/$		$/$		$/$
$\log(a^2+1)$	$\log 5$	$\log 17$	$\log 13$	$\log 37$	$\log 25$

Computations

Consider primes less than 6 and their powers less than $\max\{Q(a) \mid a \in [2,7]\}$:

- $\underline{p = 2}$, solutions of $a^2 + 1 \equiv 0 \mod 2$ are $\{1\}$;
- $\underline{q = 2^2}$, solutions of $a^2 + 1 \equiv 0 \mod 4$ are $\varnothing$;
- $\underline{p = 3}$, solutions of $a^2 + 1 \equiv 0 \mod 3$ are $\varnothing$;
- $\underline{p = 5}$, solutions of $a^2 + 1 \equiv 0 \mod 5$ are $\{2,3\}$;

Sieving: an example

Problem

Find values a in the interval $[3,7]$ such that $Q(a)=a^2+1$ is prime, respectively 6-smooth.

Table of sieving

a	3	4	5	6	7
ticks	$//$		$/$		$//$
$\log(a^2+1)$	0	$\log 17$	$\log 13$	$\log 37$	$\log 5$

Computations

Consider primes less than 6 and their powers less than $\max\{Q(a) \mid a\in[2,7]\}$:

- $\underline{p=2}$, solutions of $a^2+1\equiv 0 \mod 2$ are $\{1\}$;
- $\underline{q=2^2}$, solutions of $a^2+1\equiv 0 \mod 4$ are $\varnothing$;
- $\underline{p=3}$, solutions of $a^2+1\equiv 0 \mod 3$ are $\varnothing$;
- $\underline{p=5}$, solutions of $a^2+1\equiv 0 \mod 5$ are $\{2,3\}$;
- $\underline{p=5^2}$, solutions of $a^2+1\equiv 0 \mod 25$ are $\{7,18\}$

Sieving: an example

Problem

Find values a in the interval $[3,7]$ such that $Q(a)=a^2+1$ is prime, respectively 6-smooth.

Table of sieving

a	3	4	5	6	7
ticks	$//$		$/$		$///$
$\log(a^2+1)$	0	$\log 17$	$\log 13$	$\log 37$	0

Computations

Consider primes less than 6 and their powers less than $\max\{Q(a) \mid a \in [2,7]\}$:

- $\underline{p=2}$, solutions of $a^2+1\equiv 0 \mod 2$ are $\{1\}$;
- $\underline{q=2^2}$, solutions of $a^2+1\equiv 0 \mod 4$ are $\varnothing$;
- $\underline{p=3}$, solutions of $a^2+1\equiv 0 \mod 3$ are $\varnothing$;
- $\underline{p=5}$, solutions of $a^2+1\equiv 0 \mod 5$ are $\{2,3\}$;
- $\underline{p=5^2}$, solutions of $a^2+1\equiv 0 \mod 25$ are $\{7,18\}$

Sieving: an example

Problem

Find values a in the interval $[3,7]$ such that $Q(a) = a^2 + 1$ is prime, respectively 6-smooth.

Table of sieving

a	3	4	5	6	7
ticks	//		/		///
$\log(a^2+1)$	0	$\log 17$	$\log 13$	$\log 37$	0

Computations

Consider primes less than 6 and their powers less than $\max\{Q(a) \mid a \in [2,7]\}$:

- $\underline{p = 2}$, solutions of $a^2 + 1 \equiv 0 \mod 2$ are $\{1\}$;
- $\underline{q = 2^2}$, solutions of $a^2 + 1 \equiv 0 \mod 4$ are $\varnothing$;
- $\underline{p = 3}$, solutions of $a^2 + 1 \equiv 0 \mod 3$ are $\varnothing$;
- $\underline{p = 5}$, solutions of $a^2 + 1 \equiv 0 \mod 5$ are $\{2,3\}$;
- $\underline{p = 5^2}$, solutions of $a^2 + 1 \equiv 0 \mod 25$ are $\{7,18\}$

Conclusion

The prime values of Q are $Q(4) = 17$ and $Q(6) = 37$.
The 6-smooth values of Q are $Q(3) = 10$ and $Q(7) = 50$.

Algorithm for sieving

Algorithm

Input: a monic polynomial $Q(x)$ in $\mathbb{Z}[x]$ and parameters B, E_1, E_2;
Output: all the integers $x \in [E_1, E_2]$ for which $Q(x)$ is B-smooth.

```
Make a list $(p^k, r)$ of prime powers $p^k \leq \max\{|Q(x)|, x \in [E_1, E_2]\}$, with $p < B$,
and integers $0 \leq r < p^k$ such that $Q(r) \equiv 0 \bmod p^k$
Define an array indexed by $x \in [E_1, E_2]$ and initialize it with $\log_2 |Q(x)|$
for all $(p^k, r)$ considered above do
    for $x$ in $[E_1, E_2]$ and $x \equiv r \bmod p^k$ do
        Subtract $\log_2 p$ from the entry of index $x$;
    end for
end for
Collect the indices $x$ where the array is close to 0 (numerical errors).
```

Cofactorization

In practice we sieve on primes smaller than a bound **fbb** $< B$ and we collect indices x whose value is smaller than a threshold. Then we test smoothness with ECM on the survivals in a step called cofactorization. In the literature, the smoothness bound B is called **lpb**, “large prime bound”, to distinguish from **fbb**, “factor base bound”.

Exercice

What is the condition on **fbb** and **lpb** such that ECM is not needed, i.e., we know that there is only one large prime.