Polynomial-Time Quantum Algorithms for Pell's Equation and the Principal Ideal Problem

Sean Hallgren

Caltech

Pell's Equation

- Given a positive non-square integer d, find integer solutions x, y of

$$x^2 - dy^2 = 1.$$

$d = 5$

$9^2 - 5 \cdot 4^2 = 1$

- One of the oldest studied problem in algorithmic number theory.
- Reduction: Factoring $\leq$ Pell's equation
- Buchmann/Williams cryptosystem based on Pell.
- Running time: $e^{n^{1/3}}$ $e^{n^{1/2}}$
- Quantum Algorithms for: 1) Pell's Equation

  2) Principal Ideal Problem
- Corollaries: break this cryptosystem, compute the class group
- The Hidden Subgroup Problem:
  - solvable when the group is abelian and finitely generated
  - for Pell's equation we extend the HSP to groups that are not finitely generated: the reals.

Classical Algorithm for Pell's Equation

Input: d

Rewrite $x^2 - dy^2 = 1$

as $\frac{\sqrt{x^2-1}}{y} = \sqrt{d}$

For large x, $\sqrt{d} \approx \frac{x}{y}$

Algorithm: compute the continued fraction expansion of $\sqrt{d}$

$$\sqrt{d} \longrightarrow \frac{x_1}{y_1}, \frac{x_2}{y_2}, \ldots, \frac{a}{b}, \ldots$$

$$a^2 - db^2 = 1$$

$\geq d^c$ steps, so exponential time.

This algorithm dates back 1000 years.

Solutions of Pell's Equations (Existence)

$$x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$$

A convenient way to write solutions:

$a + b\sqrt{d}$ is a solution if $(a + b\sqrt{d})(a - b\sqrt{d}) = 1$

Lagrange (1768):

There is a *fundamental solution* $a_0 + b_0\sqrt{d}$
and solutions of Pell's equation are given by

$$(a_0 + b_0\sqrt{d})^n \qquad n \in \mathbb{Z}_{>0}$$

Examples of Fundamental Solutions

Input: d

x^2	-	d	*	y^2	=	1
3^2	-	8	*	1^2	=	1
19^2	-	10	*	6^2	=	1
10^2	-	11	*	3^2	=	1
7^2	-	12	*	2^2	=	1
649^2	-	13	*	180^2	=	1
15^2	-	14	*	4^2	=	1
4^2	-	15	*	1^2	=	1
9801^2	-	29	*	1820^2	=	1
1766319049^2	-	61	*	226153980^2	=	1
158070671986249^2	-	109	*	15140424455100^2	=	1

Finding a solution $a + b\sqrt{d}$ is not in NP because the solutions are too big.

Solving Pell's Equation: the Regulator

Input: d

Let $a_0 + b_0\sqrt{d}$ be the fundamental solution.

Define the *regulator* as

$$R = \ln(a_0 + b_0\sqrt{d})$$

Any solution of Pell's equation is represented as:

$$nR = \ln((a_0 + b_0\sqrt{d})^n) \qquad n \in \mathbb{Z}_{>0}$$

Finding an integer multiple of R is in NP:

Given $x \in \mathbb{R}$, there is a poly-time algorithm to test if e^x is a solution of Pell's equation.

Polynomial-time classical algorithms:

- Closest integer to $R \longrightarrow R$ to any precision.
- Can compute least significant digits of $a_0 + b_0\sqrt{d}$ from R.

Background on Finding the Regulator *R*

Computational complexity:

$$R = \ln(a_0 + b_0\sqrt{d})$$

- Factoring reduces to finding *R*.
- Classical running times:

Factoring: $e^{n^{1/3}}$

$$n = \ln d$$

Pell (computing *R*): $e^{n^{1/2}}$

- Complexity classes:
  - Factoring $\in$ NP I CoNP
  - Finding an <u>integer multiple</u> of *R* is in NP:
  - Finding R:
    - Assuming the GRH, is in NP.
    - Without assumptions: not known to be in NP.

The Principal Ideal Problem

Given d, ideal $I \subseteq \mathbb{Z}[\sqrt{d}]$, is $I = \alpha\mathbb{Z}[\sqrt{d}]$? $\alpha \in \mathbb{Q}(\sqrt{d})$

Reductions: factoring $\leq$ finding R $\leq$ principal ideal problem.

Running times (classical)

- Factoring: $e^{n^{1/3}}$ $n = \ln d$
- Pell and PIP: $e^{n^{1/2}}$

Cryptosystem based on principal ideal problem.
(Buchmann, Williams 1989)

Quantum algorithm in polynomial (in $\ln d$) time.

- Breaks cryptosystem.
- Compute the class group of a real quadratic number field.

Towards a quantum algorithm: There is a function f on the reals s.t. $f(x) = f(x+y)$ iff $y = nR$.

Quantum Preliminaries

- State: $\sum_{g\in G} \alpha_g|g\rangle \in \mathbb{C}^{|G|}$ Measure: see g w.p. $|\alpha_g|^2$

  $\sum_g |\alpha_g|^2 = 1$

  Ex. $x \in \mathbb{Z}_2^n$, $x = \boxed{100110}$, $\sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$

- Evolution: unitary op, e.g. Fourier transform over G

$$\sum_{g\in G} \alpha_g|g\rangle \xrightarrow{F_G} \sum_{\chi\in\hat{G}} \hat{\alpha}_x|\chi\rangle$$

- 2 properties of F.T. over G:

  1) subgroup H $\longrightarrow$ perp group $H^\perp$

$$\sum_{h\in H} |h\rangle \longrightarrow \sum_{\chi\in H^\perp} |\chi\rangle$$

  2) convolution $\longrightarrow$ pt. wise multiplication

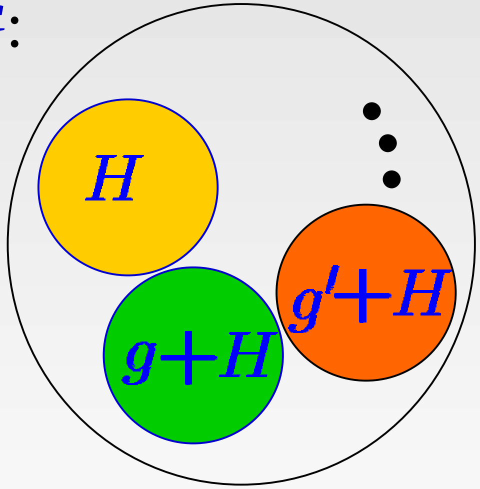
$$|g\rangle * \sum_{h\in H} |h\rangle \longrightarrow \sum_{\chi} \chi(g)|\chi\rangle \bullet \sum_{\chi\in H^\perp} |\chi\rangle$$

The Hidden Subgroup Problem

Given $f : G \to$ Colors, constant and distinct on cosets of subgroup H.

Find H.

G:



Examples

- Factoring N: $G = \mathbb{Z}_M, M = \phi(N)$
- Discrete log: $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$

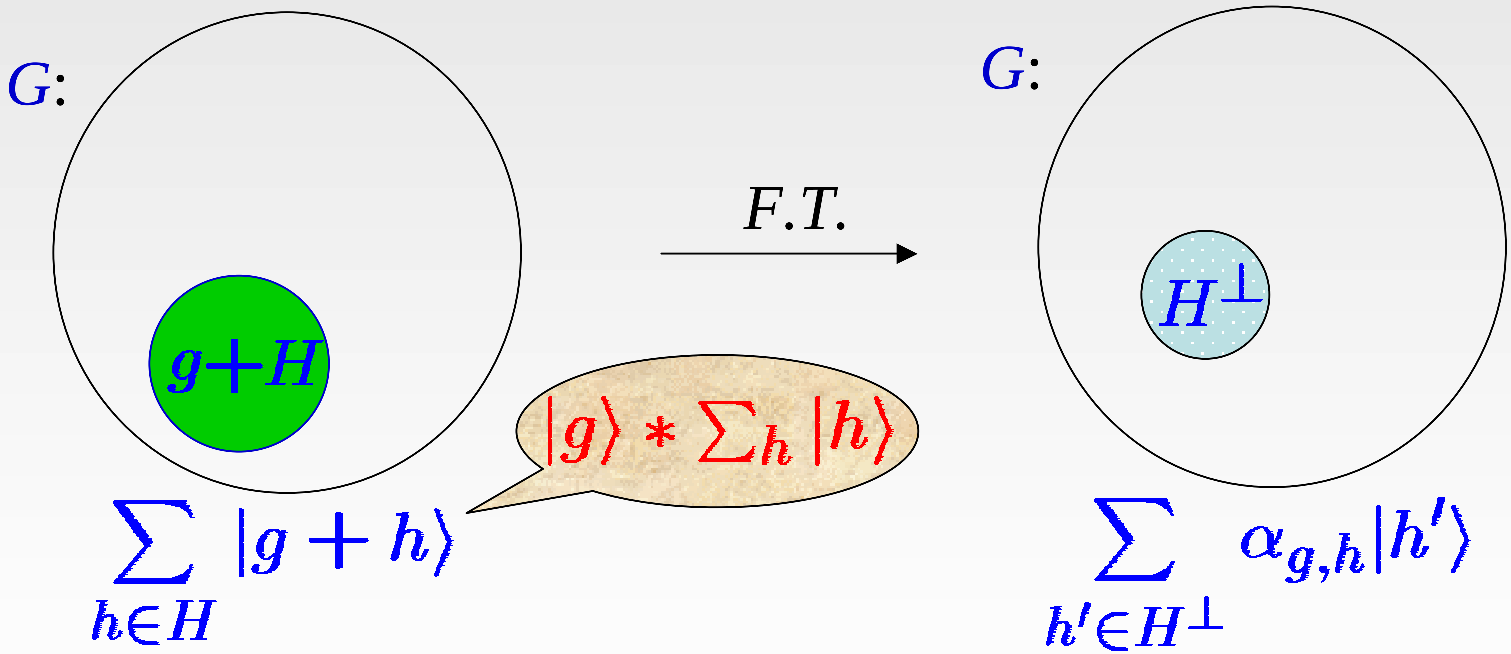
The Hidden Subgroup Problem Algorithm

Given $f : G \rightarrow$ Colors, constant and distinct on cosets of subgroup H.

Find H.

Algorithm:

1) Fourier sample:



Measure a random element of $H^{\perp}$.

2) (Classically) reconstruct H from the sample.

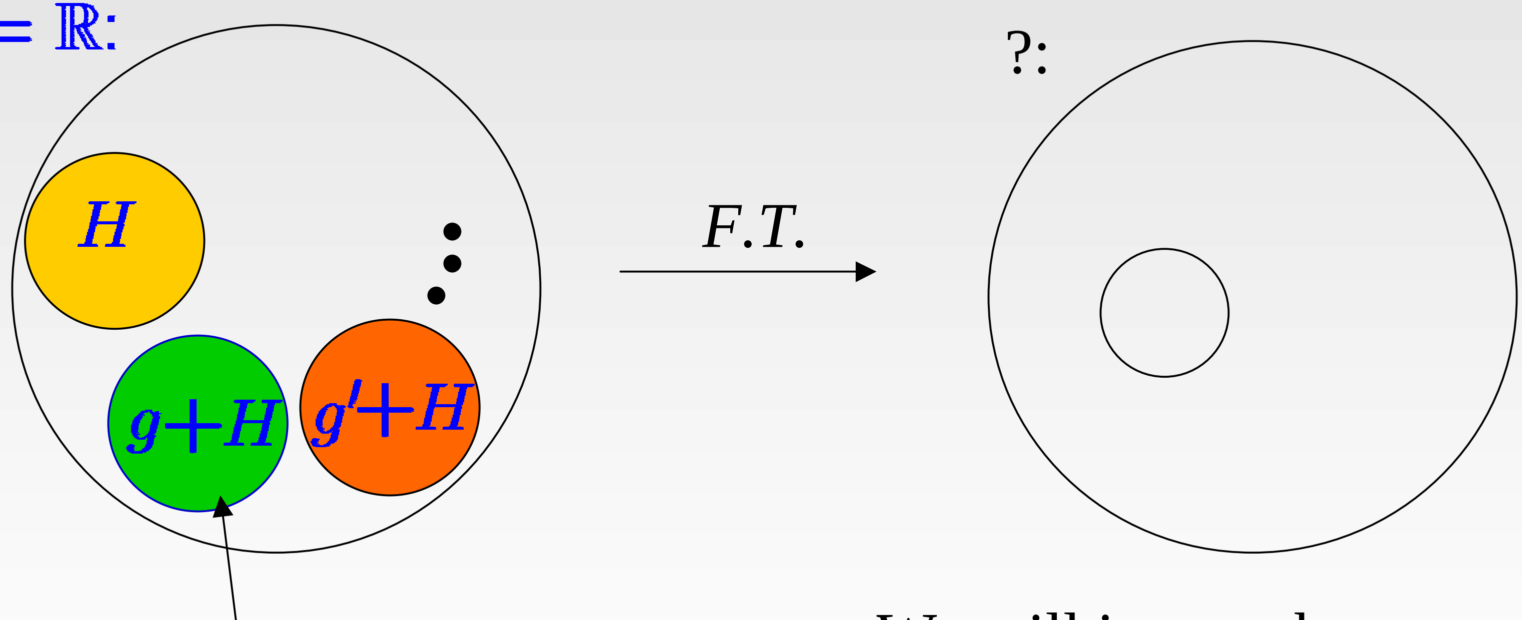
Pell: Underlying Hidden Subgroup Problem?

Yes, but $G = \mathbb{R}$, and H is generated by an irrational number.

$f : \mathbb{R} \to \text{Colors}$

1) Fourier sampling:

$G = \mathbb{R}$:



$$\sum_{x\in ?} |x\rangle$$

2) Classical reconstruction ?

We will ignore the coset in this talk, because Fourier sampling takes care of it.

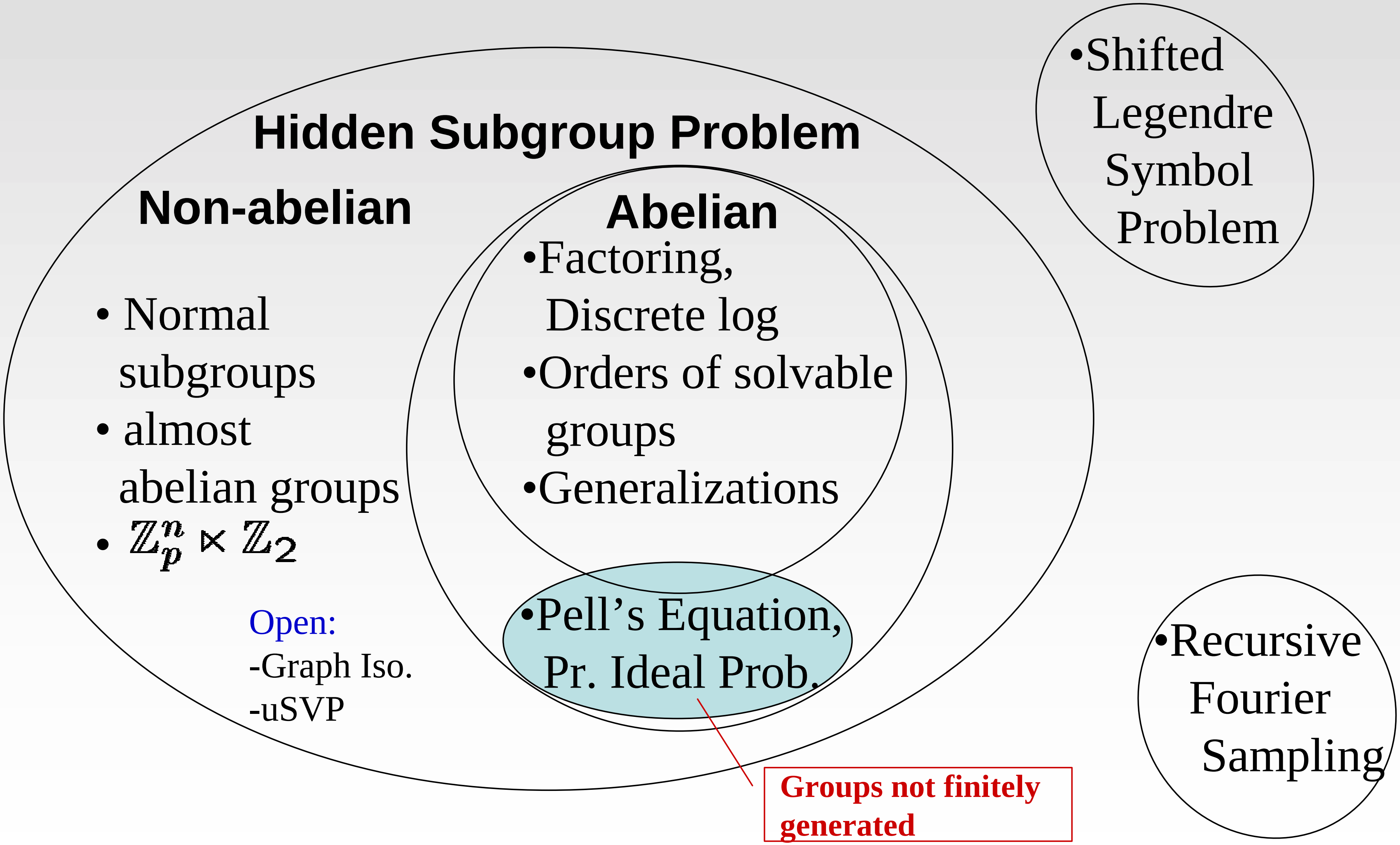
Since Shor's Algorithms

- Factoring, Discrete log [Shor 1994]

Hidden Subgroup Problem

- Nonabelian Case [H., Russell, Ta-Shma 2000]
  [Grigni, Schulman, Vazirani, Vazirani 2001]
  [Magniez, Santha 2002]
- Solvable Groups and Generalizations
  [Watrous 2001]
  [Ivanyos, Magniez, Santha 2001]
- Shifted Legendre Symbol Problem [van Dam, H., Ip 2001]

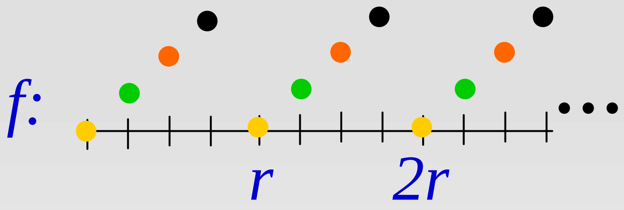
Quantum Algorithms



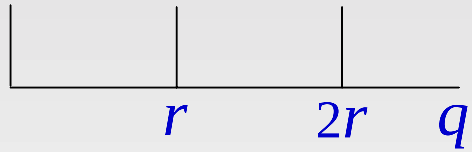
HSP Example: The Period Finding Problem

Given f, find its period.

f is defined on the integers.

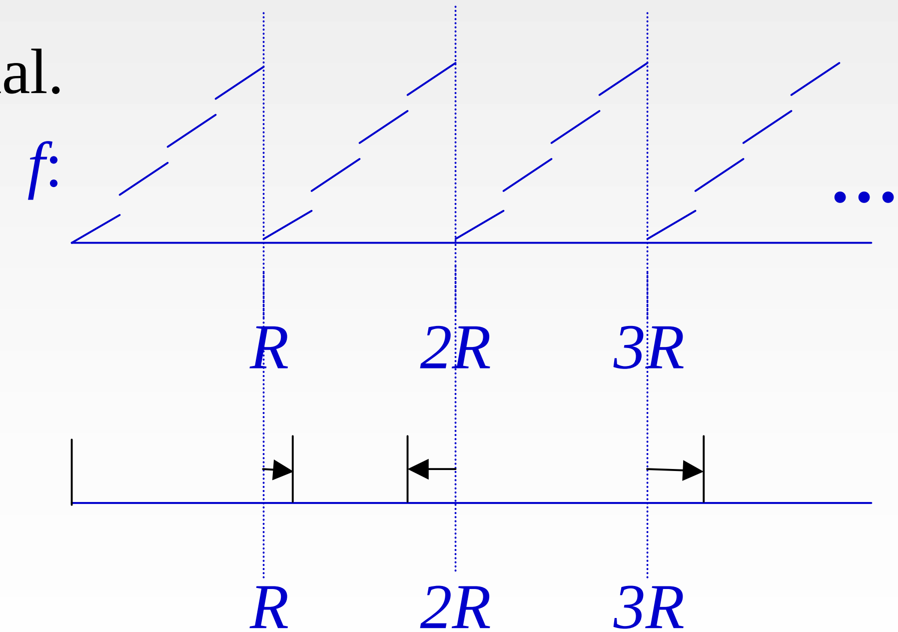


Fourier sample: $\sum_i |ir\rangle$



Solution to Pell: use a function f with period R.

Problem: The period R is irrational.



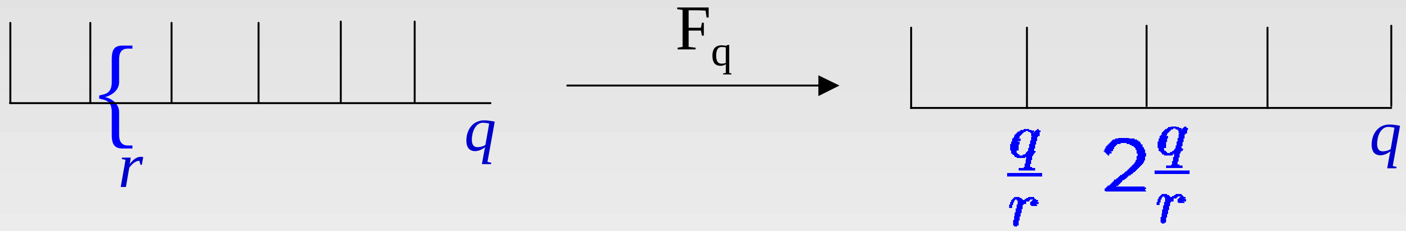
Fourier sample: $\sum_i |[iR]\rangle$

$[iR] = \lfloor iR \rfloor$ or $\lceil iR \rceil$

Period Finding: Integer Period r

Recall: we have a function f on the reals with period R.

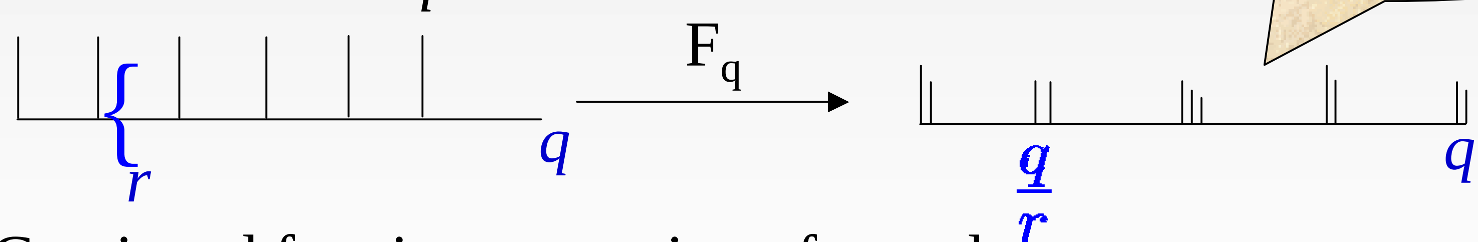
A) Exact case when r divides q.

1) 

2) Given $k\frac{q}{r}$: compute $\frac{k\frac{q}{r}}{q} = \frac{k}{r}$. $k \in \mathbb{Z}$

Sample: $[k\frac{q}{r}]$

B) r does not divide q.

1) 

2) Continued fraction expansion of sample:

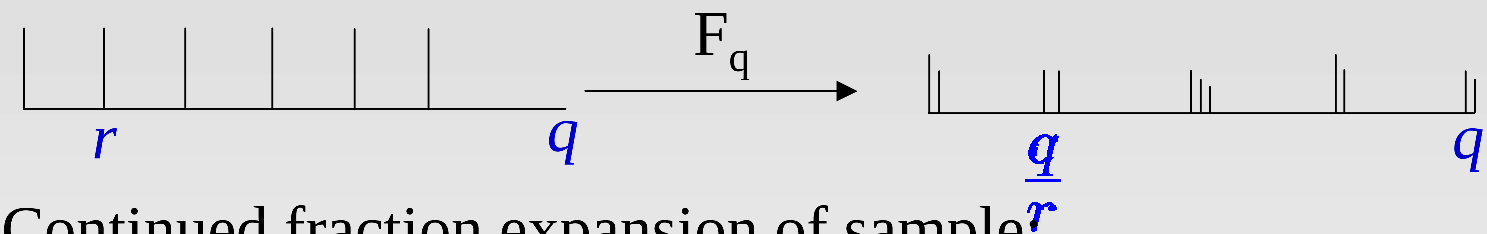
Given $[k\frac{q}{r}]$: compute $\frac{[k\frac{q}{r}]}{q} \longrightarrow \frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{r}, \ldots$

Theorem: If $q \geq r^2$ this will result in r.

Approach for Irrational Period

B) r does not divide q.

1)



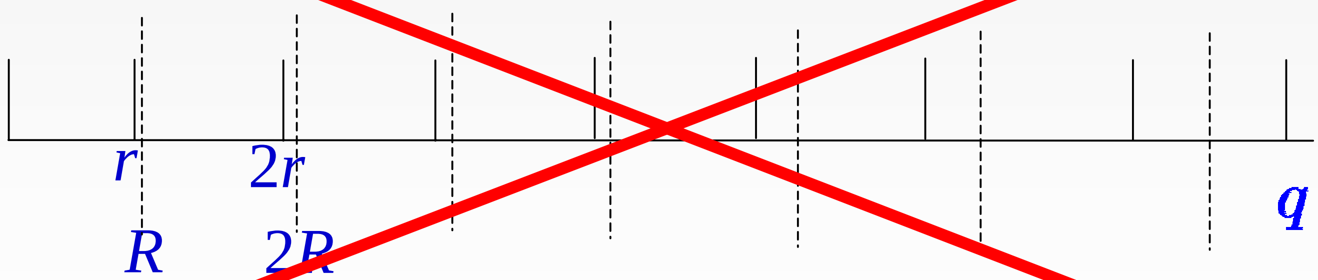
2) Continued fraction expansion of sample:

Given $[k\frac{q}{r}]$: compute $\frac{[k\frac{q}{r}]}{q} \longrightarrow \frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{r}, \ldots$

Theorem: If $q \geq r^2$ this will result in r.

C) R is irrational

Natural approach: reduction to the integer case (choose $r \approx R$).



$q \geq R^2$

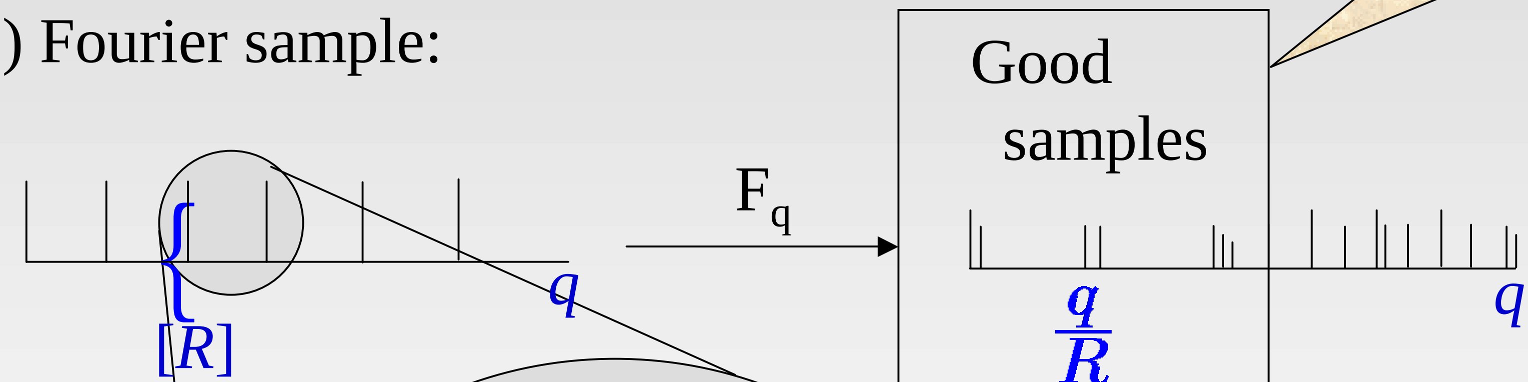
$$r = R - \epsilon \qquad r^2 = (R-\epsilon)^2 \approx (R^2 - \epsilon R)$$

Period Finding: Irrational Period (Sketch)

R is irrational.

If $q \ge R^3$

1) Fourier sample:

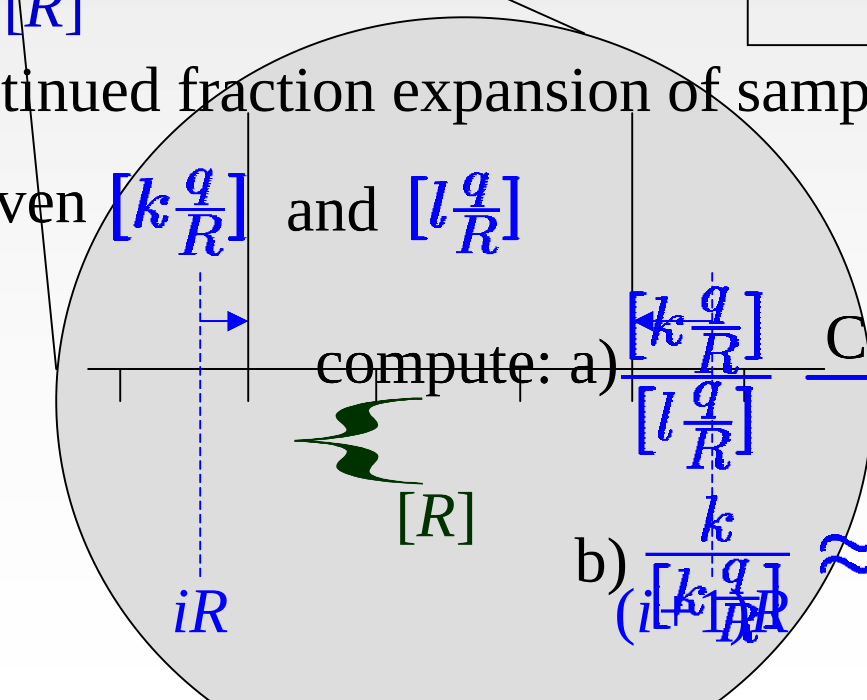


2) Continued fraction expansion of sample(s):

Given $[k\frac{q}{R}]$ and $[l\frac{q}{R}]$

compute: a) $\dfrac{[k\frac{q}{R}]}{[l\frac{q}{R}]} \xrightarrow{\text{CF}} \dfrac{a_1}{b_1}, \dfrac{a_2}{b_2}, \ldots, \dfrac{k}{l}, \ldots$

b) $\dfrac{k}{[k\frac{q}{R}]} \approx \dfrac{R}{q}$



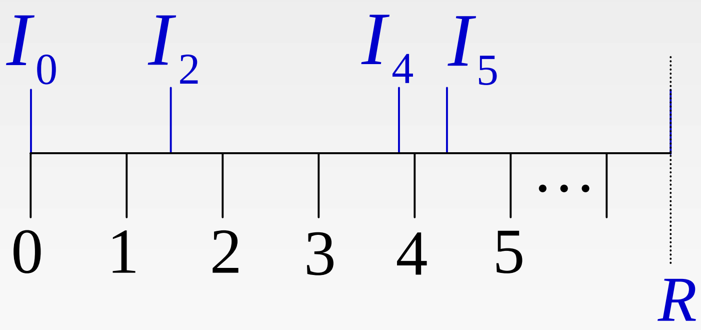
Principal Ideals, Distances of Ideals

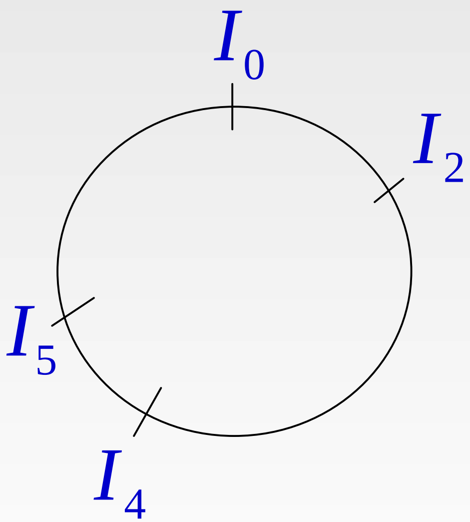
Input: d Define a set of ideals inside the ring $\mathbb{Z}[\sqrt{d}]$

$$I = a\mathbb{Z} + b\sqrt{d}\mathbb{Z} \subset \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \text{ integer}\}$$

The ideals have real-valued distances δ in $[0,R)$:

$$I = \alpha\mathbb{Z}[\sqrt{d}] \qquad \delta(I) \approx \ln(\alpha) \bmod R$$





Notation: I_x is the ideal to the left of x.

Distances modulo R add approximately:

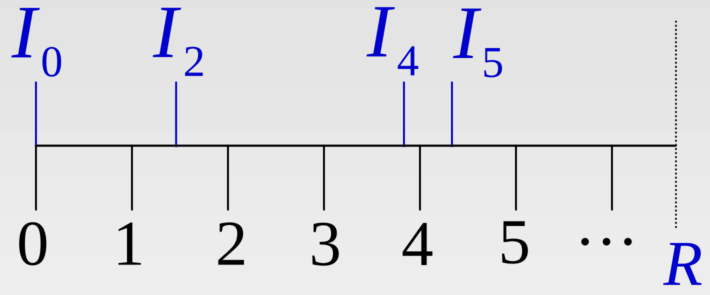
$$\delta(I_i \cdot I_j) = \delta(I_{i+j}) \pm \text{poly} \qquad I_i^a \approx I_{ia}, \;\; a \in \mathbb{Z}$$

Computation with Ideals

Input: d Define a set S of ideals inside the ring $\mathbb{Z}[\sqrt{d}]$

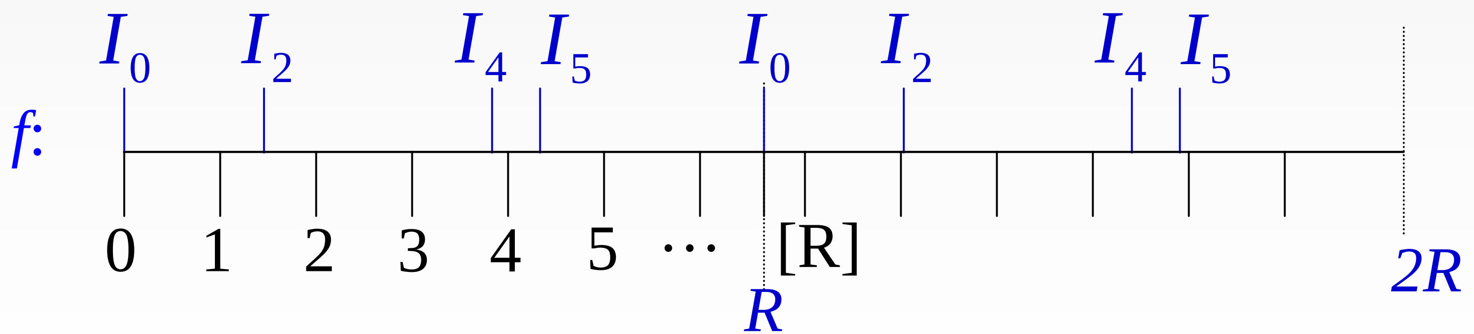
Facts about the computing with the ideals in S:

1) Exponential number of ideals
2) Represented by a pair of integers
3) Has a real-valued "distance"



4) Multiplication of ideals is group-like:
   - distances add approximately $I_2 \cdot I_2 = I_4$ or I_5.
   - abelian, but not associative!

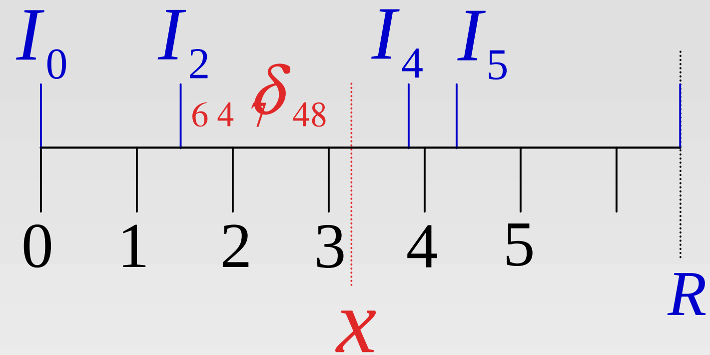
5) Given a real number x, can compute ideal closest to x in poly time



A Peridioc Function f on the Reals

Given d.

1) Injective on $[0,R)$:

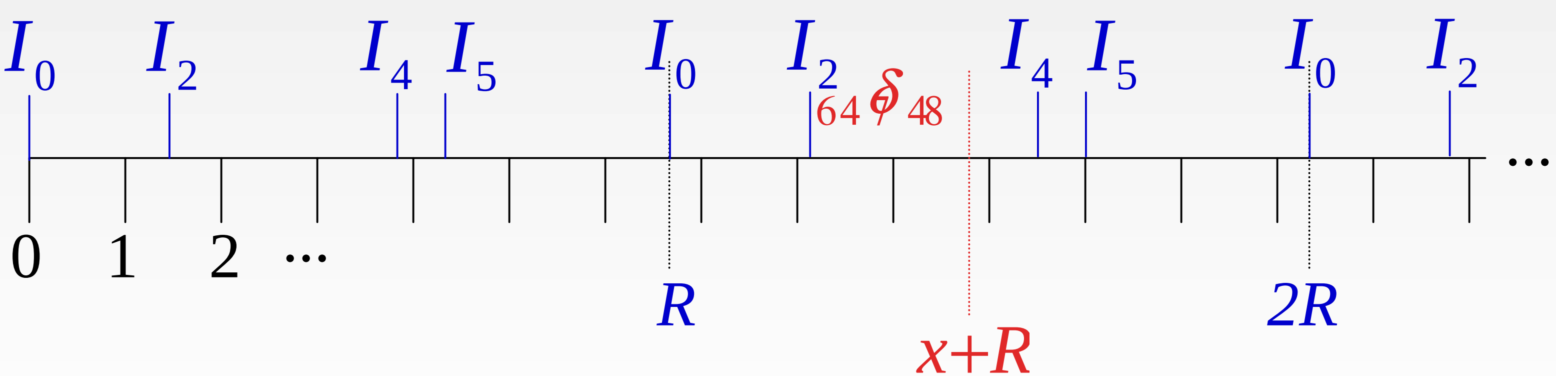


Mapping f:

$$[0,R) \leftrightarrow \text{Ideals} \times [0,R)$$

$$f(x)=(I_2,\delta)$$

2) Periodic on the reals:

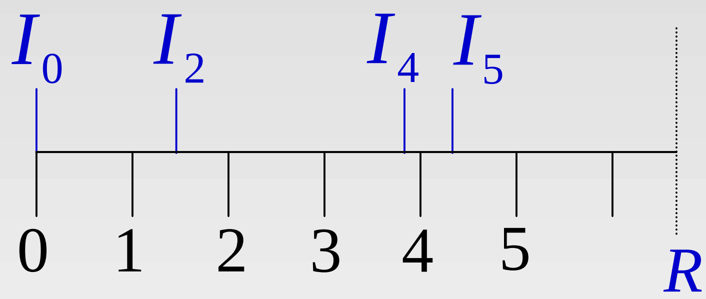


$$f(x+R)=(I_2,\delta)$$

Theorem: f is polynomial-time computable

Discrete-Log Using Ideals

6) Computing R $\leq$ computing the distance of an ideal.



(Specified as a pair of integers.)

Key Exchange [Buchmann, Williams ’89]:

<u>A</u>		<u>B</u>
Choose $a \in \mathbb{Z}$		Choose $b \in \mathbb{Z}$
	$\xrightarrow{I_a}$	
		Compute $I_a^b \approx I_{ab}$
	$\xleftarrow{I_b}$	
Compute $I_b^a \approx I_{ab}$		

Key: I_{ab}

Finding the Distance of an Ideal (Sketch)

<u>Discrete Log</u>

Finite field:

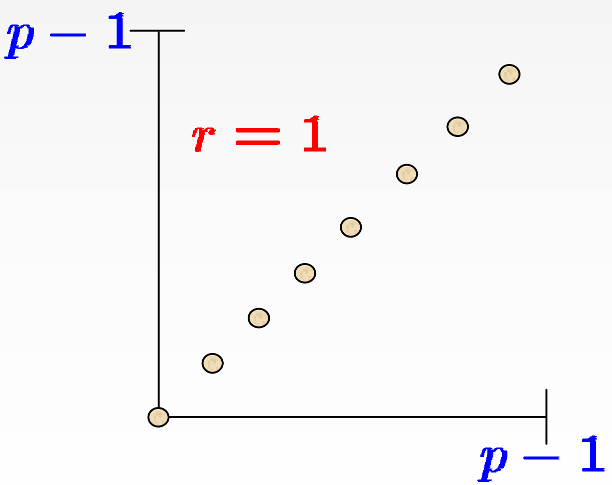
$\mathbb{Z}_p$, generator g

Given g^r, find r.

$$f(a,b) = g^{ar-b}$$

$$H = \{(a, ar)\}$$

(mod $p-1$)



Quadratic number field:

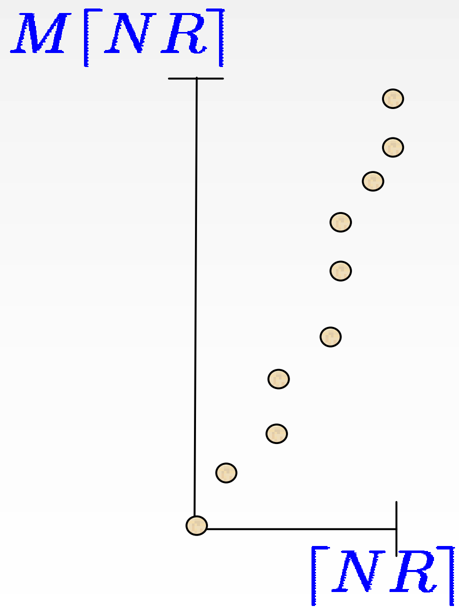
$\mathbb{Z}[\sqrt{d}]$

Given I_x, find x. $x \in \mathbb{R}$

$$f(a,b) = I_{ax+b/N}$$

$$\text{“}H\text{”} = \{(a, \lfloor -Nax \rfloor)\}$$

(mod R)



Computing $f(a,b)$:

1) $I_x \mapsto I_x^a \approx I_{ax}$

a must be an integer

2) $I_{ax} \cdot I_{b/N} \approx I_{ax+b/N}$

Decomposing Abelian Groups

Quantum Algorithms: Mosca/Cheung, Watrous

Given a set of generators $g_1, \ldots, g_n$, find a basis, etc.

Arbitrary group element: $g = g_1^{e_1} \cdots g_n^{e_n}$, $e_1, \ldots, e_n \in \mathbb{Z}$

Algorithm:

1) Solve a hidden subgroup problem:

$$\sum_{e_1,\ldots,e_n} |e_1, \ldots, e_n\rangle \longrightarrow \sum_{e_1,\ldots,e_n} |e_1, \ldots, e_n, \phi_g\rangle$$

resulting in a matrix B for the set of group relations.

2) Classically compute the Smith normal form of B, which gives the basis for the group.

Main issue: if no unique representative for a group element

$g = g_1^{e_1} \cdots g_n^{e_n}$ $\quad g' = g_1^{e_1'} \cdots g_n^{e_n'}$

$\bar{g} = \bar{g}'$ in the group, but g, g' are different strings.

Need $|\phi_g\rangle = |\phi_{g'}\rangle$

Class Group of a Real Quadratic Number Field

Given d:

$\mathcal{I}$: Fractional ideals of $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}(\sqrt{d})$

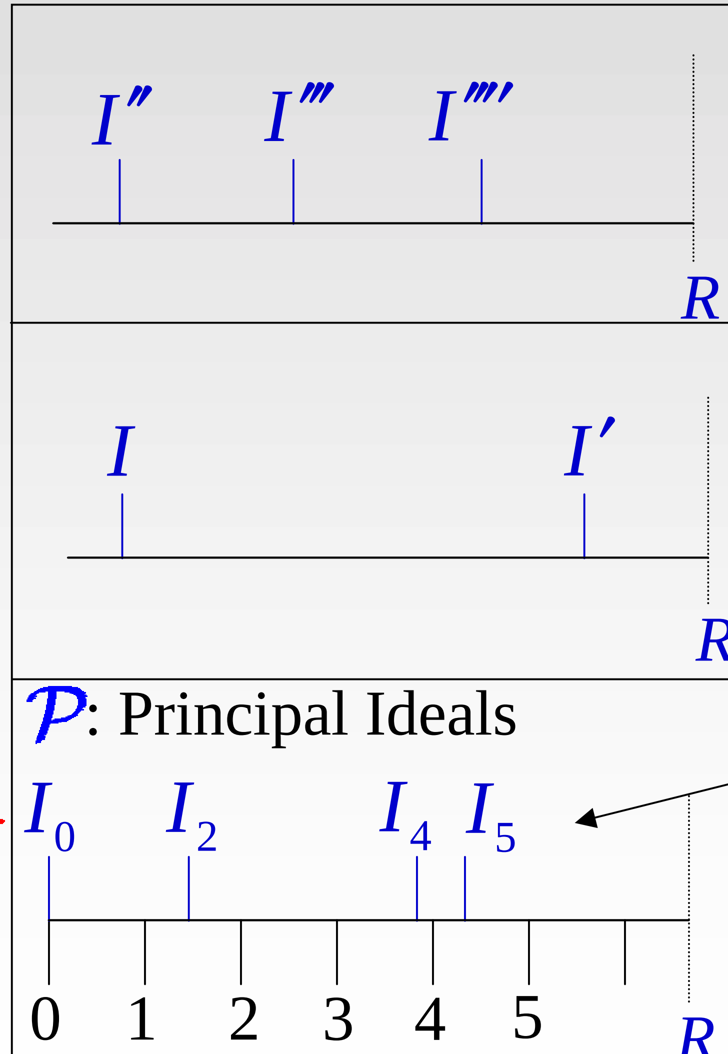
$\mathcal{I}$ is an abelian group under multiplication

$\mathsf{Cl} = \mathcal{I}/\mathcal{P}$

$= |I''\rangle + |I'''\rangle + |I''''\rangle$ $|g_3\rangle$

$= |I\rangle + |I'\rangle$ $|g_2\rangle$

$= |I_0\rangle + |I_2\rangle + |I_4\rangle + |I_5\rangle$ $|g_1\rangle$



Reduced principal ideals

Decomposing Finite Abelian Groups

- Here: show how to create a superposition representing an element in Cl.

Algorithm: given an ideal I, compute $|I\rangle \to |\bar{I}\rangle \approx |I\rangle + |I'\rangle$

1) Superposition over *distances from I*

$$\sum_j |j\rangle$$

2) Compute the ideal that is distance j from I

$$\sum_j |j, I_j\rangle$$

3) Compute the distance of I_j from I

$$\sum_j |0, I_j\rangle$$

Conclusions

- Polynomial-time algorithms for:
  - Pell’s Equation
    - integer period finding is in NP
    - Hales: relative to an oracle, irrational period finding outside MA
  - Principal Ideal Problem
- Corollaries:
  - Break a cryptosystem based on ideals in number fields
  - Compute the class group
- Open Problems
  - General number fields:
    - Unit Group, Regulator
    - Class group
  - Shortest Lattice Vector
  - Other cryptosystems based on number fields