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

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

Example:
$d = 5$
$9^2 - 5 \cdot 4^2 = 1$

Some history on this equation:

- Lagrange (1768): there exists an infinite number of solutions for each *d*

- First algorithm was found around 1000 years ago. The algorithm computes the continued fraction expansion of $\sqrt{d}$.

- An early appearance of the equation: the cattle problem of Archimedes (287-212 B.C.), with d=410286423278424 (15 digits).
  Smallest solution in this case has 100,000 digits.
  Eventually solved in 1880, but not by writing down 100,000 digits.

Specifics about the Solutions

- The nth solution x_n, y_n can be expressed in terms of the *fundamental* solution $x_1 + y_1\sqrt{d}$.

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

To see that these are solutions, rewrite

$$x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}).$$

Let $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.

Then $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$.

$$(x_1 + y_1\sqrt{d})^n = \sum \binom{n}{i} x_1^i y_1^{n-i} \sqrt{d}^{n-i}$$

Therefore: product = $x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n = 1$.

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 to write down.

Computing Solutions of Pell's Equation

- Goal: compute $x_1 + y_1\sqrt{d}$ …but it is exponentially large.

- Instead, there are two compact representations
  - –Power product representation
    (Lenstra) The answer to the cattle problem is

$$x_1+y_1\sqrt{d} = \frac{2^4 5^{14}(2175+\sqrt{d})^{18}(2184+\sqrt{d})^{10}(2187+\sqrt{d})^{20}(4341+2\sqrt{d})^{6}}{3^{27}7^{5}29^{9}31^{20}(2162+\sqrt{d})^{18}(4351+2\sqrt{d})^{10}}$$

  - –The closest integer to the regulator R

$$R = \log(x_1 + y_1\sqrt{d}).$$

(Solutions of Pell are integer multiples of R)

- These two representations are polynomial-time equivalent

- The main point of this talk is to find the regulator R.

Many Known Polynomial-Time Algorithms

- Given the closest integer to R, many things can be computed:

  1) Power product representation of the fundamental solution

  2) R to any precision

  3) The least/most significant digits of $x_1 + y_1\sqrt{d}$.

- Given an integer, it is possible to test if it is within one of a <u>multiple</u> of R.

  Assuming the GRH, can test if within one of R.

- A reduction from factoring to approximating R.

- Polynomial-time computable function that is periodic with period R, and is an HSP instance over the reals. (Description later)

Other Algorithms

- Running time of best classical algorithms

Factoring	$e^{n^{1/3}}$	$n = \log d$
Compute R	$e^{n^{1/2}}$	

- The Buchmann/Williams cryptosystem exploits this gap to improve on security of RSA.

Definition of the Problem

Problem: Given a function on the reals that has period *R*, find the closest integer to *R*. $f(x) = f(x+R)$

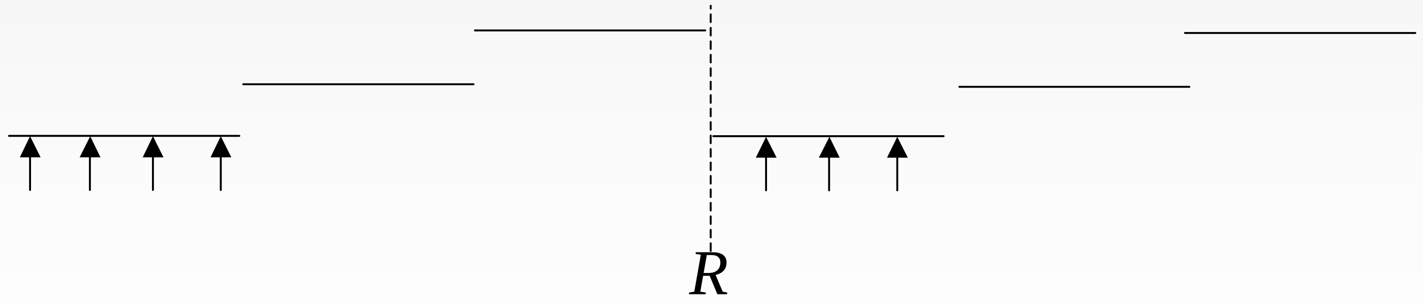
Approach: set up the following superposition and Fourier sample:

$$\sum_a |a, f(a)\rangle$$

What happens when the period is irrational?

1) In general, evaluating *f* at integer points yields nothing.

2) If f is a step function, clusters of points is possible



There is a general solution that works this way (Hales 2002).

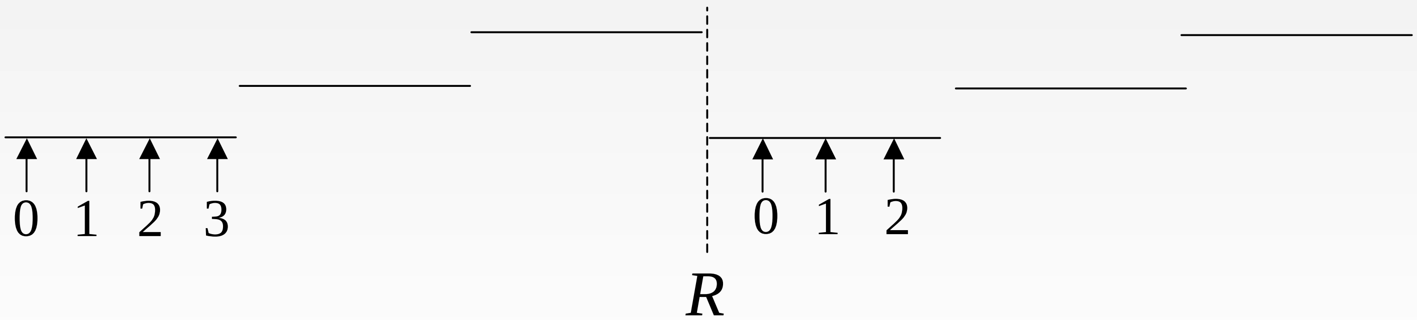
Definition of the Problem

Problem: Given a function on the reals that has period *R*, find the closest integer to *R*. $f(x) = f(x+R)$

Approach: set up the following superposition and Fourier sample:

$$\sum_a |a, f(a)\rangle$$

3) In this talk can compute the distance from the interval start

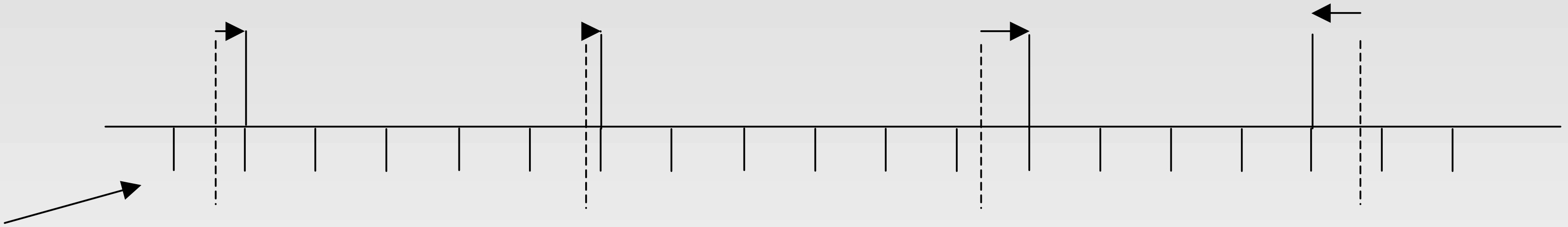


f(i) = (step value, label)

Adding these extra labels makes the function 1-1.

The Periodic Superposition

Measuring *f* gives a superposition with irrational period *R*.



Integers

Dotted lines separated by *R*

Amplitude is at a neighboring integer of each multiple of *R*.

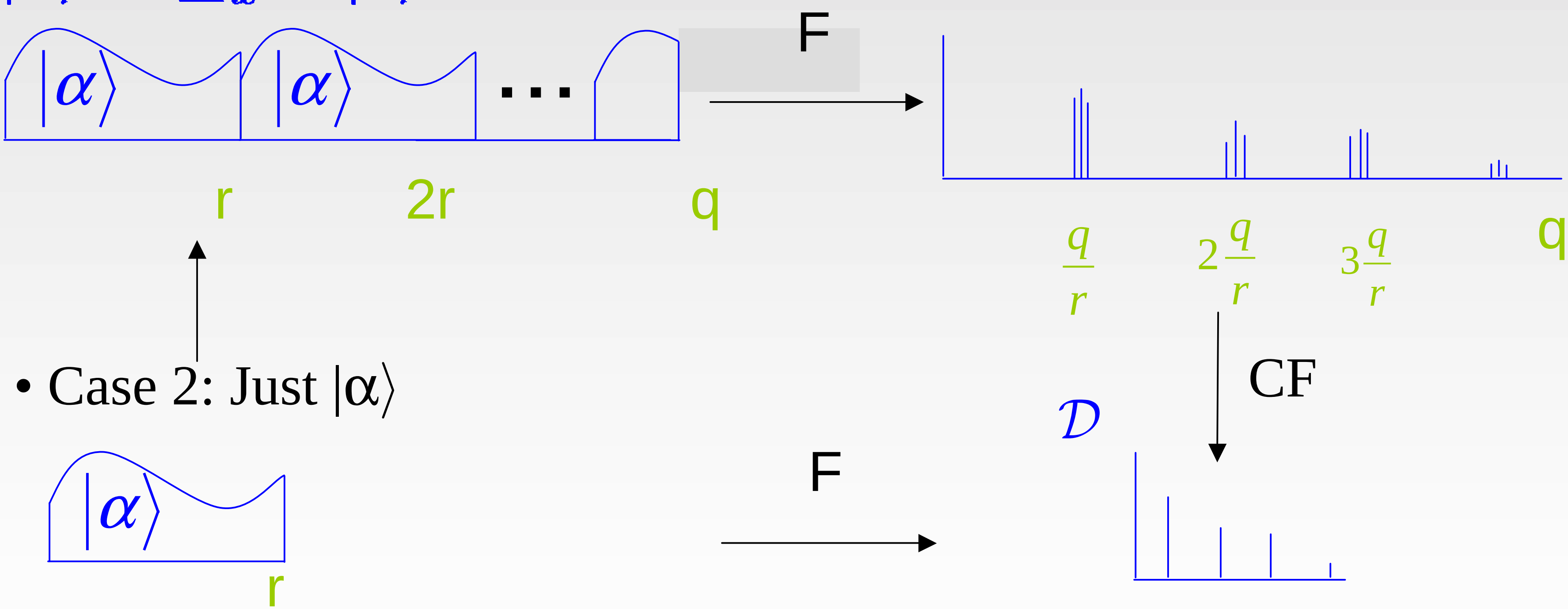
This is written as $\sum_a |[aR]\rangle$

where [aR] either rounds up or down

Fourier Sampling Theorem (Hales, H.)

- Case 1: Repeated superposition of some arbitrary state $|\alpha\rangle$

$$|\alpha\rangle = \sum_x \alpha_x |x\rangle$$

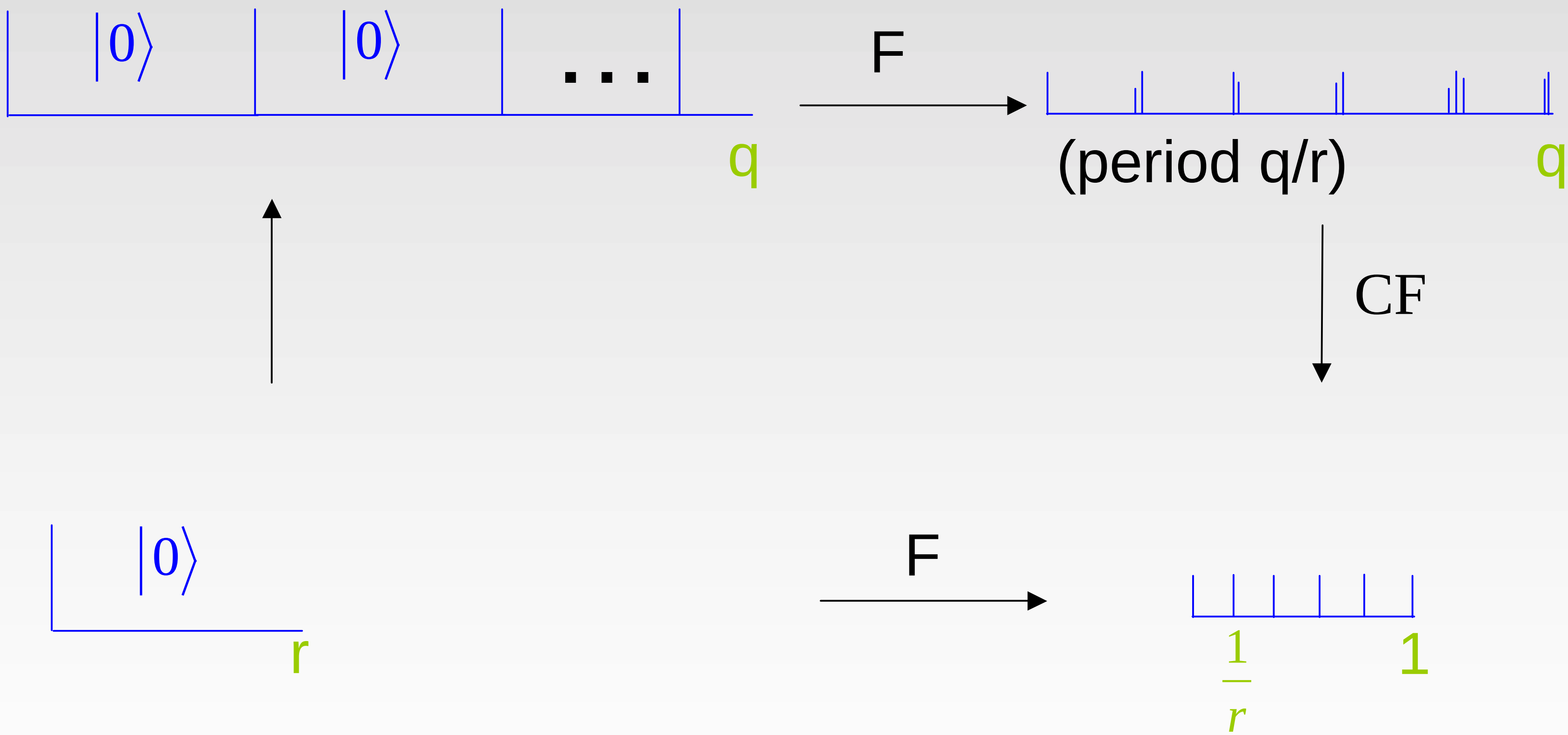


- Case 2: Just $|\alpha\rangle$

Theorem: $q > r^2$ implies this diagram commutes.

Example: Shor's Period Finding

In Shor's period finding algorithm, $|\alpha\rangle = |0\rangle$.

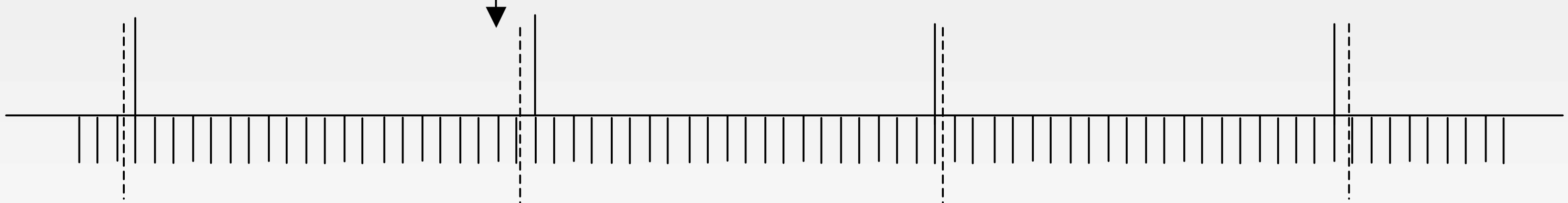


A superposition reflecting an irrational period is not quite the same...

Why Not Old Period Finding?

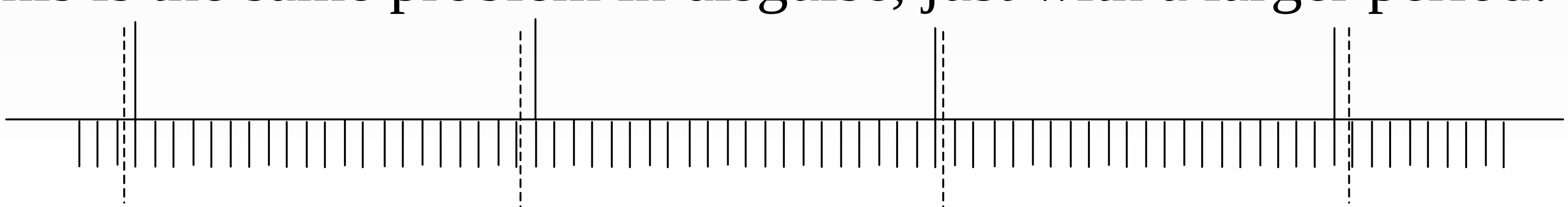
- Try to reduce to the integer case by approximating with rational numbers

Use a finer grid to decrease the rounding

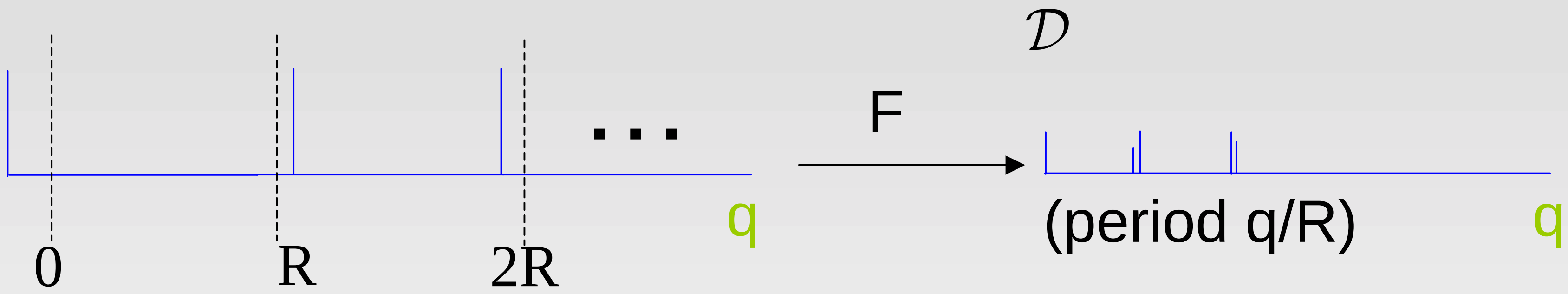


Looks more like the integer case.

But, this is the same problem in disguise, just with a larger period!



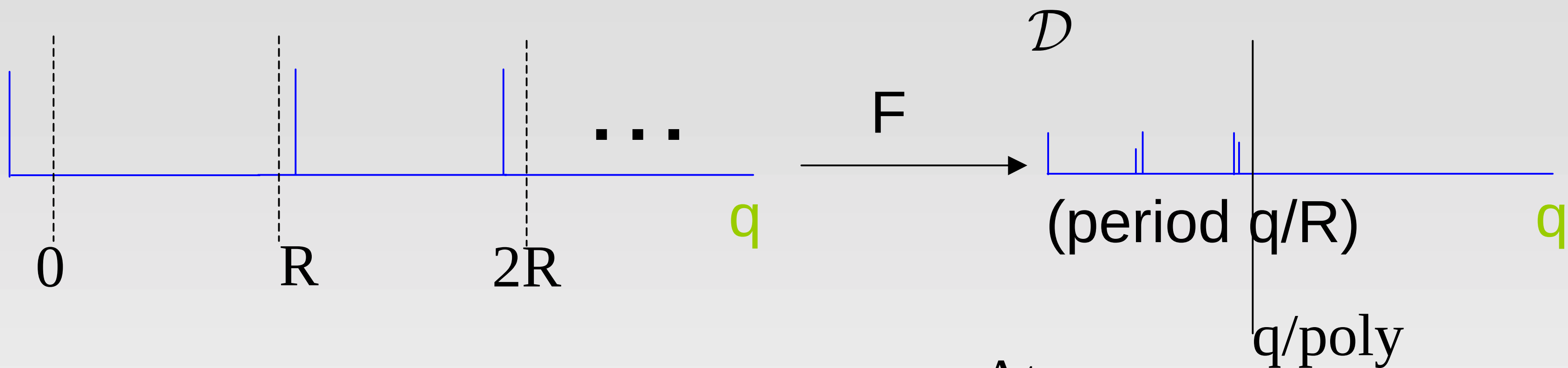
What if the Period is Irrational?



To get a working algorithm with the above setup we must,

1. reanalyze the distribution $\mathcal{D}$ induced
2. find a new way to compute R from samples of $\mathcal{D}$

Analysis of $\mathcal{D}$



$$\sum_a |[aR]\rangle$$

At c:

$$\alpha_c = \sum_a \omega^{[aR]c}$$

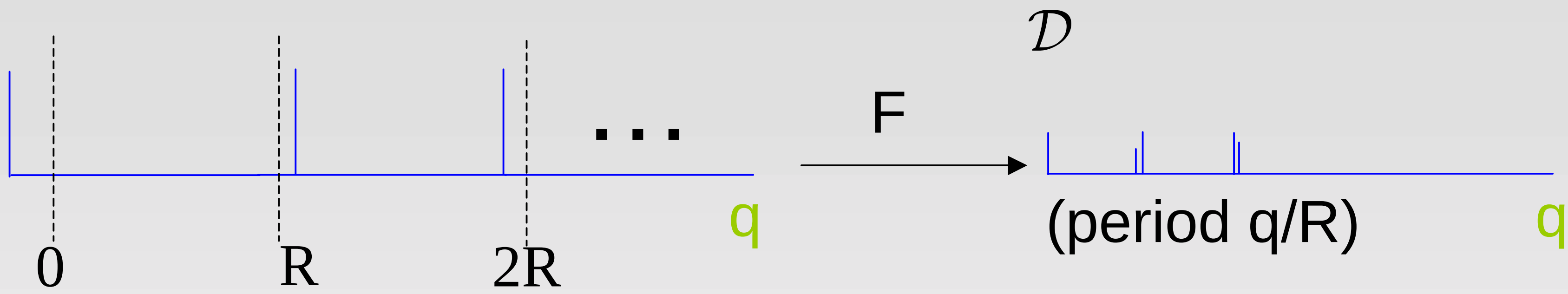
Without the rounding, this is just a geometric series

$$\alpha_c = \sum_{a=0}^{p-1} \omega^{aRc} = \frac{\omega^{pRc} - 1}{\omega^{Rc} - 1}$$

(straightforward to bound)

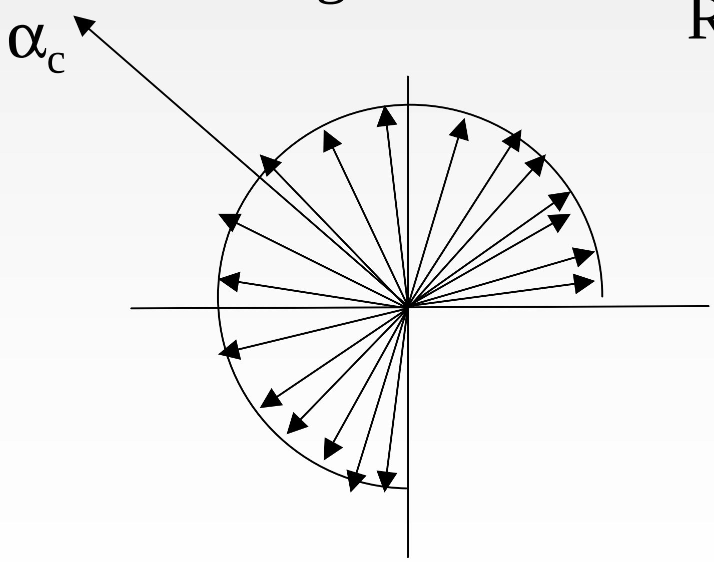
The rounding is actually quite bad. To control it, only use samples smaller than q/poly.

Analysis of $\mathcal{D}$

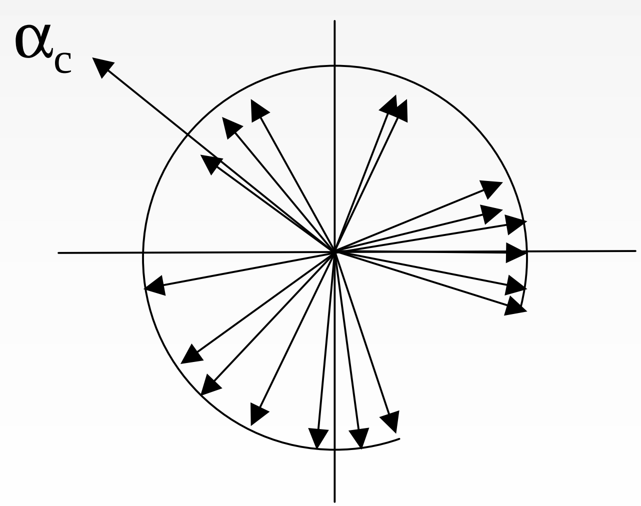


Amplitude at c is $|\alpha_c| = |\sum_i \omega^{[iR]c}|$

Without rounding:



Rounding perturbs by 1/poly max

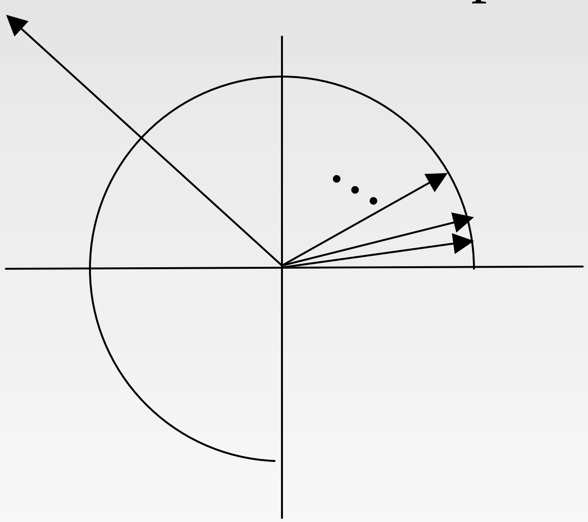


Proof Sketch of Lemma

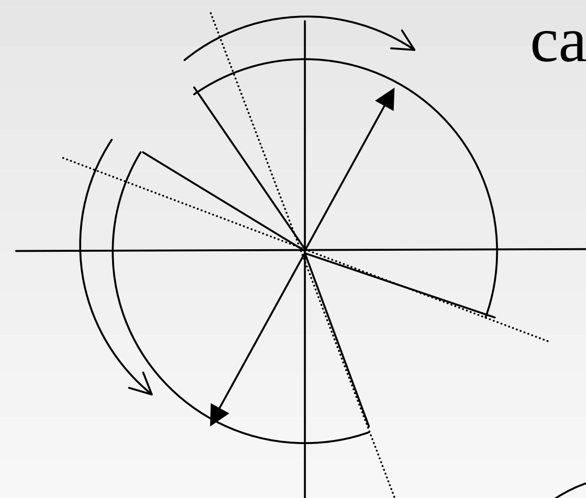
Lemma: If $c < q$/poly, measure c if $c = \lfloor k\frac{q}{R} \rceil$

Proof (sketch):

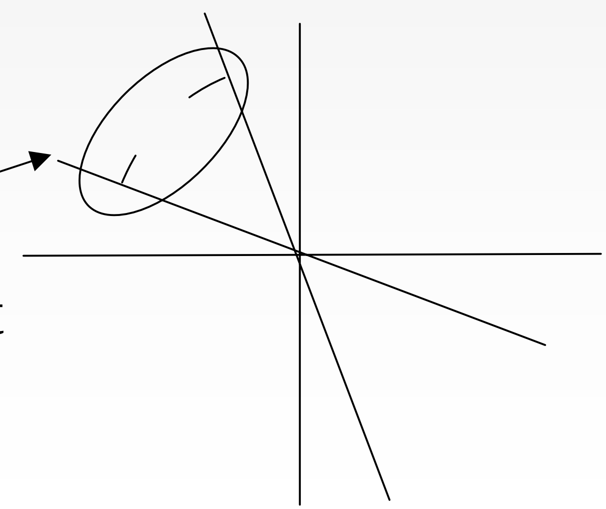
Pick worst case perturbation of points



Perturb



Opposite sides cancel out



Still have constant fraction of pts left

Using $\mathcal{D}$ to Find R

Recall the continued fraction expansion algorithm.

Input: *x*. Output: a sequence of fractions.

If a/b is output, then a/b is the best approximation to *x* with denominator at most b.

If the period is an integer *r*, samples are of the form $c = \lfloor k\frac{q}{r} \rceil$

Best approximation of $\frac{c}{q} = \frac{\lfloor k\frac{q}{r} \rceil}{q}$ is $\frac{k}{r}$

So, the continued fraction expansion of $\frac{c}{q}$ reveals *r*.

When the period is irrational, there is no reason for this solution to work.

Using $\mathcal{D}$ to Find R

- Given samples of the form $c = \lfloor k\frac{q}{R}\rceil$, $k \in \mathbb{Z}$.

- **New method** compute the ratio of the numerators of two samples *c* and *d*.

$$c = \lfloor k\frac{q}{R}\rceil \qquad d = \lfloor l\frac{q}{R}\rceil$$

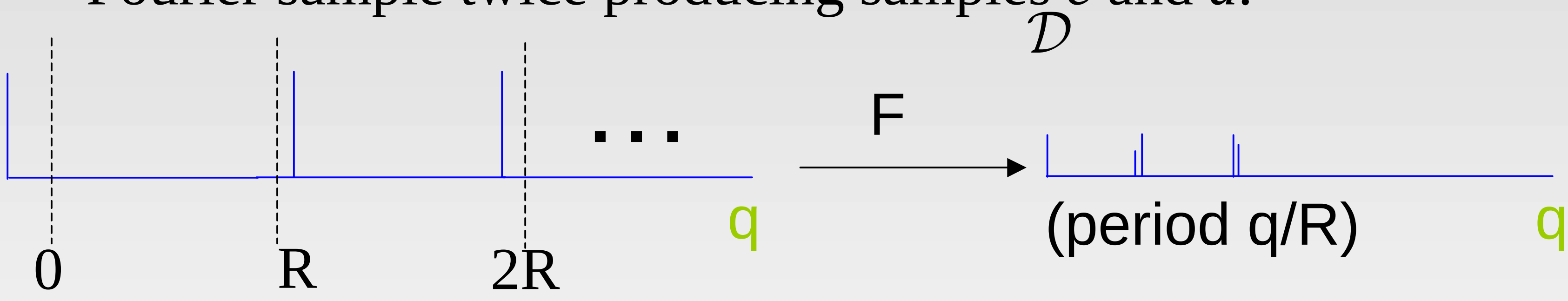
$\frac{k}{l}$ is the best approximation of $\frac{c}{d}$ with denominator at most l.

The continued fraction expansion of $\frac{c}{d}$ produces $\frac{k}{l}$.

Compute $\frac{kq}{c} = \frac{kq}{\lfloor k\frac{q}{R}\rceil} \approx R$

Summary: The Algorithm

- Quantum subroutine
  - Fourier sample twice producing samples *c* and *d*.



- Compute the continued fraction expansion of $\frac{c}{d}$ to find $\frac{k}{l}$.

- Compute $\frac{kq}{c} = \frac{kq}{\lfloor k\frac{q}{R} \rceil} \approx R$

Next

So where does this periodic function come from?

What about the cryptosystem?

The Bigger Picture

- Techniques for solving **Pell's equation** fits into the larger picture of computational algebraic number theory.
- Much research has been done in this field.
- The basics were known to Gauss, e.g. how to compute in the **class group**, defined using fractional ideals.
- In the 70's Shanks discovered a **distance function** on these ideals that led to much better algorithms.
- The three problems associated to these are solved in this work.

Results

Polynomial-time quantum algorithms for:

1. Computing the regulator R.
   This solves Pell's equation.
2. Computing the distance of an ideal.
   This provides a test for whether an ideal is principal.
3. Computing the class group of a real quadratic number field.
   Class group trivial iff the set of ideals is a PID.
4. Breaking the Buchmann/Williams cryptosystem based on hardness of (2).

These (1-3) are special cases of the main computational problems in algebraic number theory listed in Cohen's book.

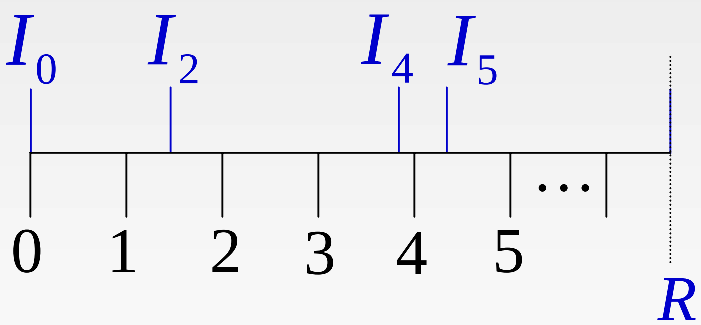
Principal Ideals, Distances of Ideals

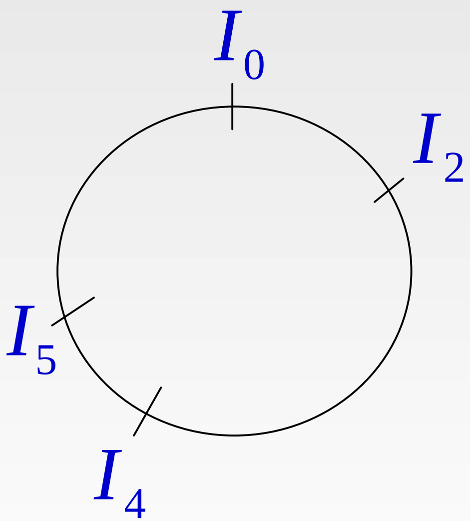
Input: d Define a set of ideals inside the ring $\mathbb{Z}[\sqrt{d}]$

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

The ideals have real-valued <u>distances</u> 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:

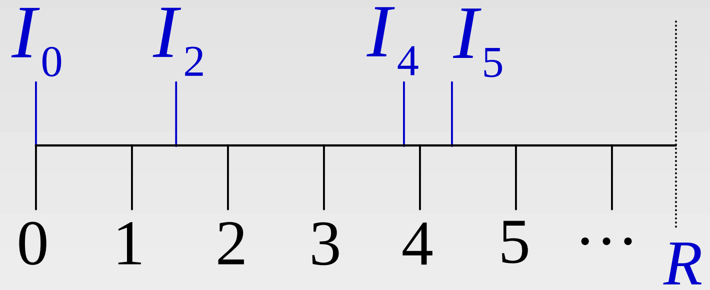
$$\delta(I_i \cdot I_j) = \delta(I_{i+j}) \pm \text{poly} \qquad I_i^a \approx I_{ia}, \;\; a \in \mathbb{Z}$$

Computation with Ideals

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

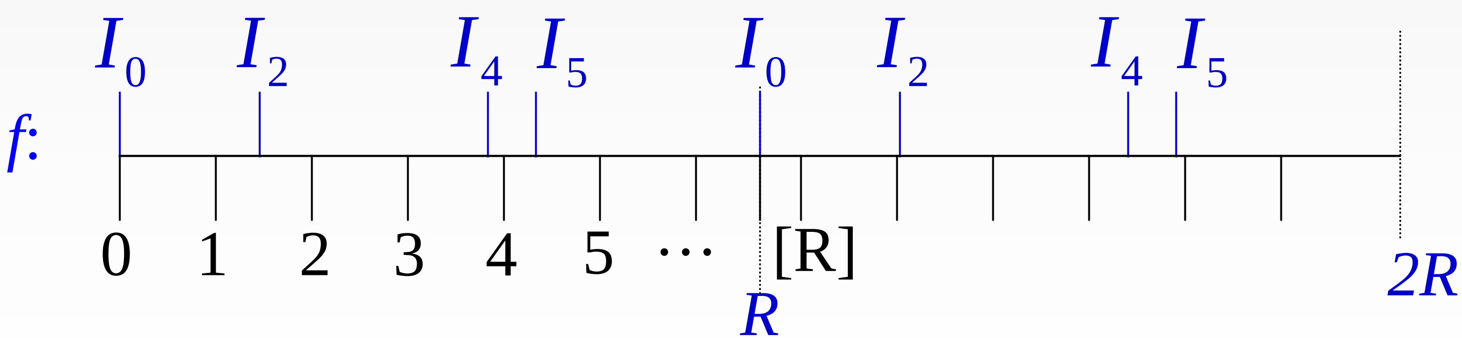
Facts about the computing with the ideals in S:

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!

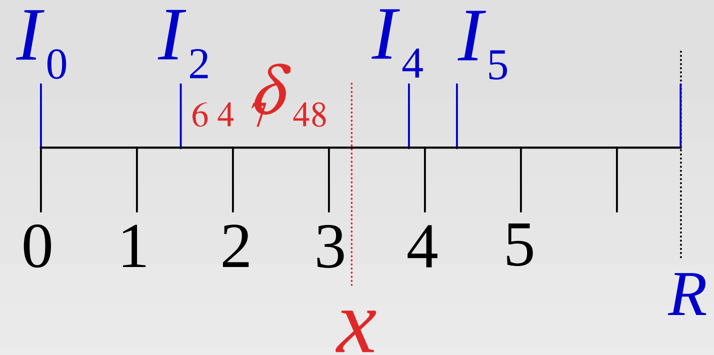
5) Given a real number x, can compute ideal closest to x in poly time



A Periodic Function f on the Reals

Given d.

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

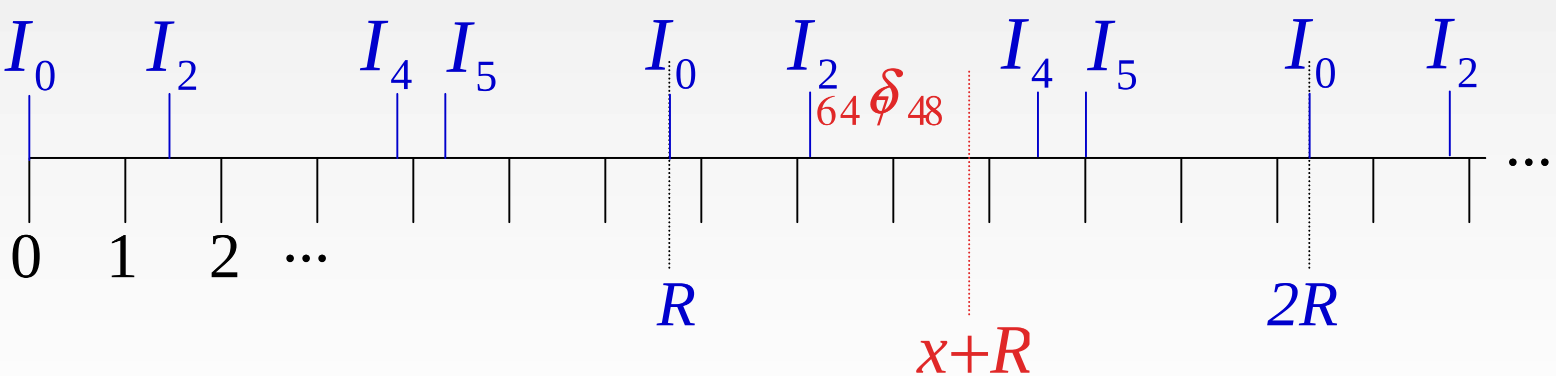


Mapping f:

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

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

2) Periodic on the reals:

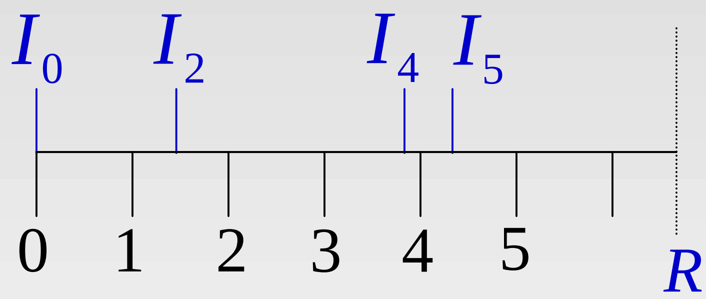


$$f(x+R)=(I_2,\delta)$$

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]:

A		B
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)

Discrete Log

Finite field:

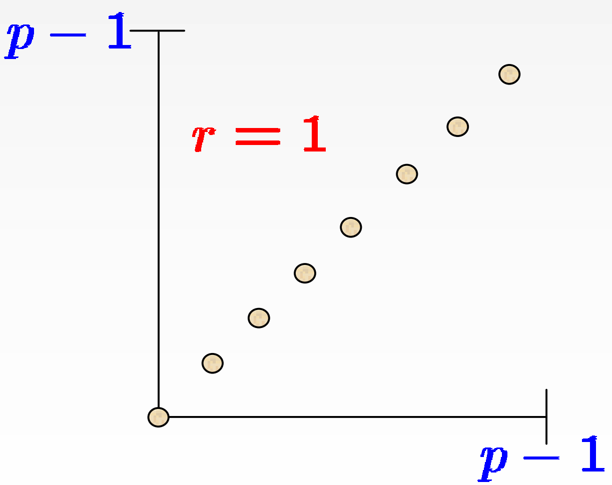
$\mathbb{Z}_p$, generator g

Given g^r, find r.

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

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

(mod $p-1$)



Quadratic number field:

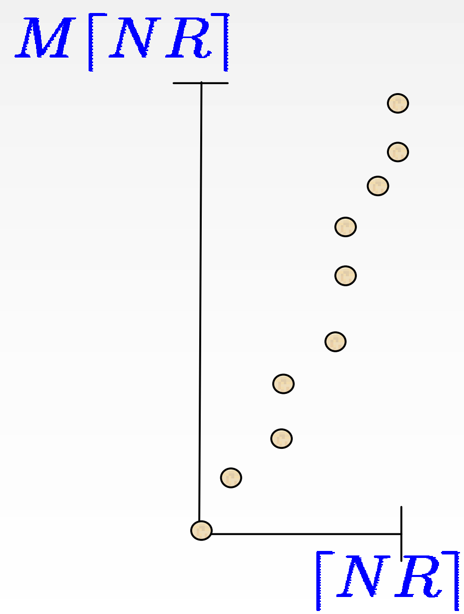
$\mathbb{Z}[\sqrt{d}]$

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

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

$\bar{g} = \bar{g}'$ 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 $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}(\sqrt{d})$

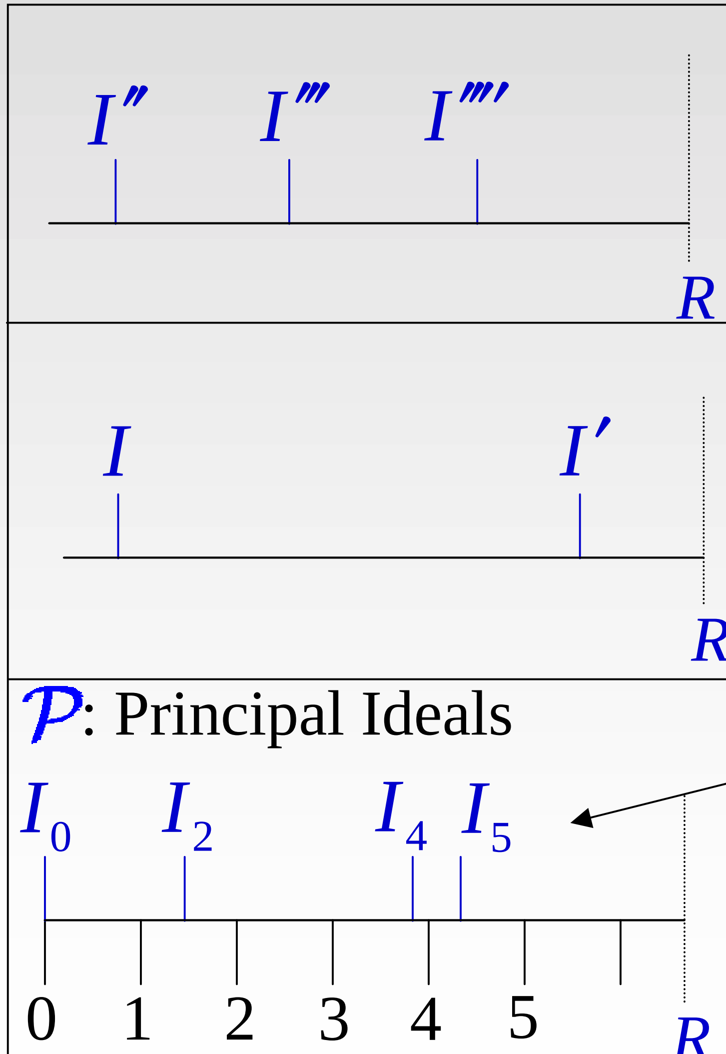
$\mathcal{I}$ is an abelian group under multiplication

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

$= |I''\rangle + |I'''\rangle + |I''''\rangle$ $\quad |\overline{g_3}\rangle$

$= |I\rangle + |I'\rangle$ $\quad |\overline{g_2}\rangle$

$= |I_0\rangle + |I_2\rangle + |I_4\rangle + |I_5\rangle$ $\quad |\overline{g_1}\rangle$



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 $|I\rangle \rightarrow |\bar{I}\rangle \approx |I\rangle + |I'\rangle$

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

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

Open Problem

- Find the unit group of a number field
  - Pell is a special case of this, since it is only one dimension
  - In general, must find a basis for an n-dimensional lattice L over the *reals*