CHINESE REMAINDER THEOREM

Oliver Knill, Math Circle, April 15, 2014

LINEAR EQUATIONS

$$x = 2 \mod 3$$

What are the solutions?

LINEAR EQUATIONS

$$x = 2 \mod 3$$
$$x = 3 \mod 5$$

Can you still solve it?

LINEAR EQUATIONS

$$x = 2 \mod 3$$

$$x = 3 \mod 5$$

$$x = 2 \mod 7$$

And now?

SHIS IS SUNZI'S PROBLEM FROM

2000 YEARS AGO!

SUN TZU

2nd or 3rd -century


孫子算經卷上

唐朝議奏行太史令上輕車都尉臣李淳風等奉 勅注釋

度之所起起於忽欲知其忽蠛蠓吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一氂十氂爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於黍十黍爲一絫十絫爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

“Sunzi’s problem”

$$x = 2 \bmod 3$$

$$x = 3 \bmod 5$$

$$x = 2 \bmod 7$$

x=23

Master Sun’s Mathematical Manual

The Mathematical Classic of Sunzi

ORIGINAL PROBLEM 26

"Now there are unknown number of things. If we count by threes, there is a reminder 2; if we count by fives, there is a remainder 3; if we count by sevens, there is a remainder 2. Find the number of things."

$$x = 2 \bmod 3$$

$$x = 3 \bmod 5$$

$$x = 2 \bmod 7$$

IBN AL-HAYTHAM

$x = 1 \mod 2$

$x = 1 \mod 3$

$x = 1 \mod 4$

$x = 1 \mod 5$

$x = 1 \mod 6$

$x = 0 \mod 7$

10th-century

x=721

QIN JIUSHAO

“Da Yan Method”

The da yan rule[2]

Let us first recall that the *da yan* rule describes that for a set of congruences $x \equiv a_i (\mathrm{mod}\, m_i)$ in which the m_i are pair wise relative primes, the solution is given by

$$x = \sum_{i=1}^{n} a_i b_i \frac{M}{m_1}$$

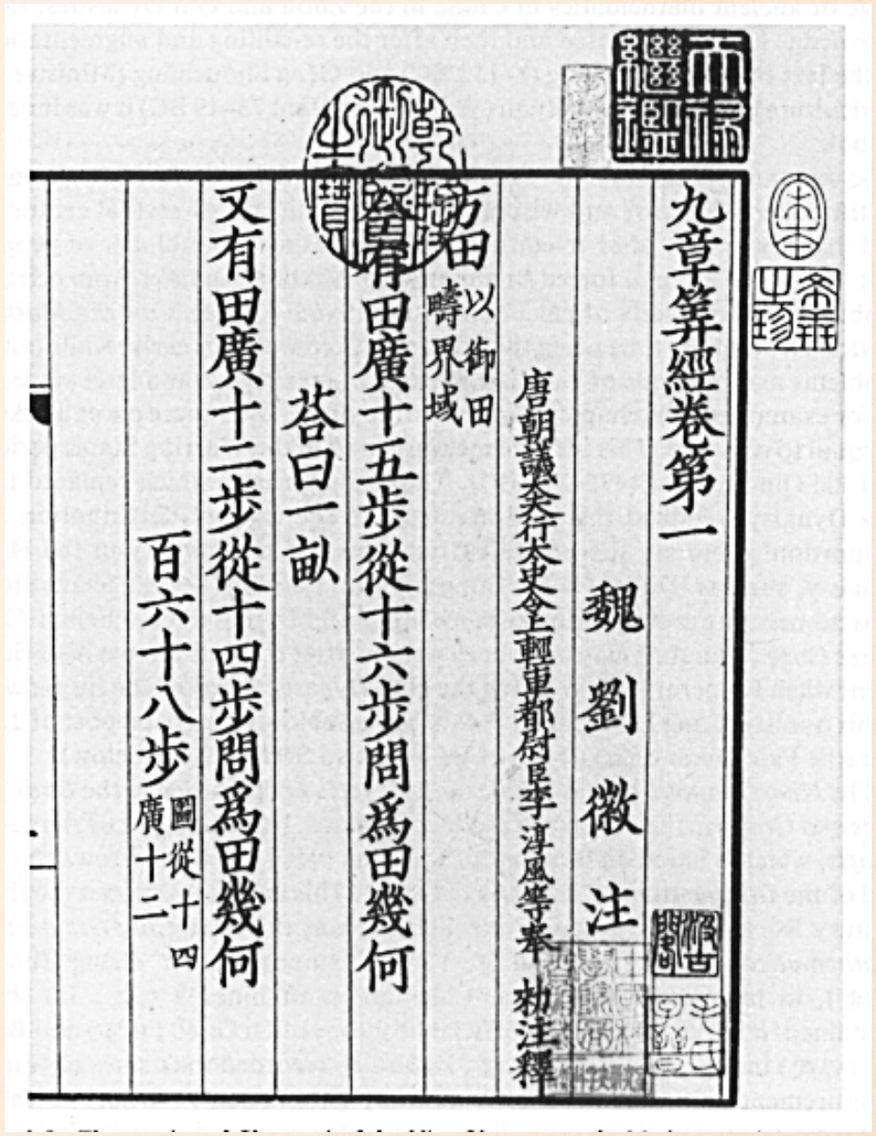
in which M is the product of all the m_i and the b_i are derived by the congruence relation $b_i \frac{M}{m_i} \equiv 1 (\mathrm{mod}\, m_i)$.

The Chinese version of the rule depends on a specific procedure which we will illustrate by a numerical example. See Needham (1959, 119-120), Libbrecht (1973, 333-354), Katz (1992,

[2] The name is in Western publications better known under its Wade-Giles transliteration *ta-yen*.

Regiomontanus and Chinese mathematics Albrecht Heeffer

13 th-century



Sushu Jiuzhang 1247

Mathematical Treatise in Nine Sections

Gauss (1801)

$$3x+5y+z = 4 \mod 12$$

$$2x+3y+2z = 7 \mod 12$$

$$5x+ y+3z = 6 \mod 12$$

(2,11,3), (5,11,6),(8,11,9),(11,11,0)

GAUSSIAN ELIMINATION

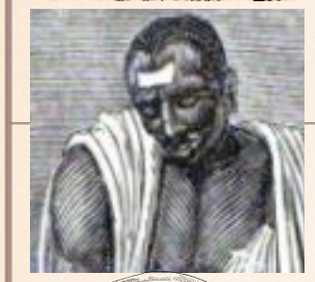
$$3x+5y+z = 4 \mod 12$$

$$+\quad 2x+3y+2z = 7 \mod 12$$

$$-\quad 5x+ y+3z = 6 \mod 12$$

HISTORY

Nicomachus of Gerasa	Pythagorei introd. aritith. libri duo	100	??



Sun Tsu Suan Ching	**Master Suns Mathematical Manual**	**300**	
Brahmagupta	Brahma Sphuta Siddhanta	600	

Ibn Al Haytham	Examples	1000	
Ibn Tahir al-Baghdadi	Number theory and algebra	1000	

Fibonacci	Liber Abaci	1200	

Qin Jiushao	**Shushu Jiuzhang**	**full algorithm**	**1247**

Gauss	Disquisitiones Arithmeticae	1801	
Schoenemann	1 linear eq. several variables	1839	

Alexander Wylie	Article in North China Herald	1852	

HOW DOES IT WORK?

$$x = 5 \bmod 7$$

$$x = 2 \bmod 31$$

Form $x = 2, 33, 64, 95, 126$ which solve the second equation. Then check the remainder with respect to 7.. We were lucky already with 33

DOES IT ALWAYS WORK?

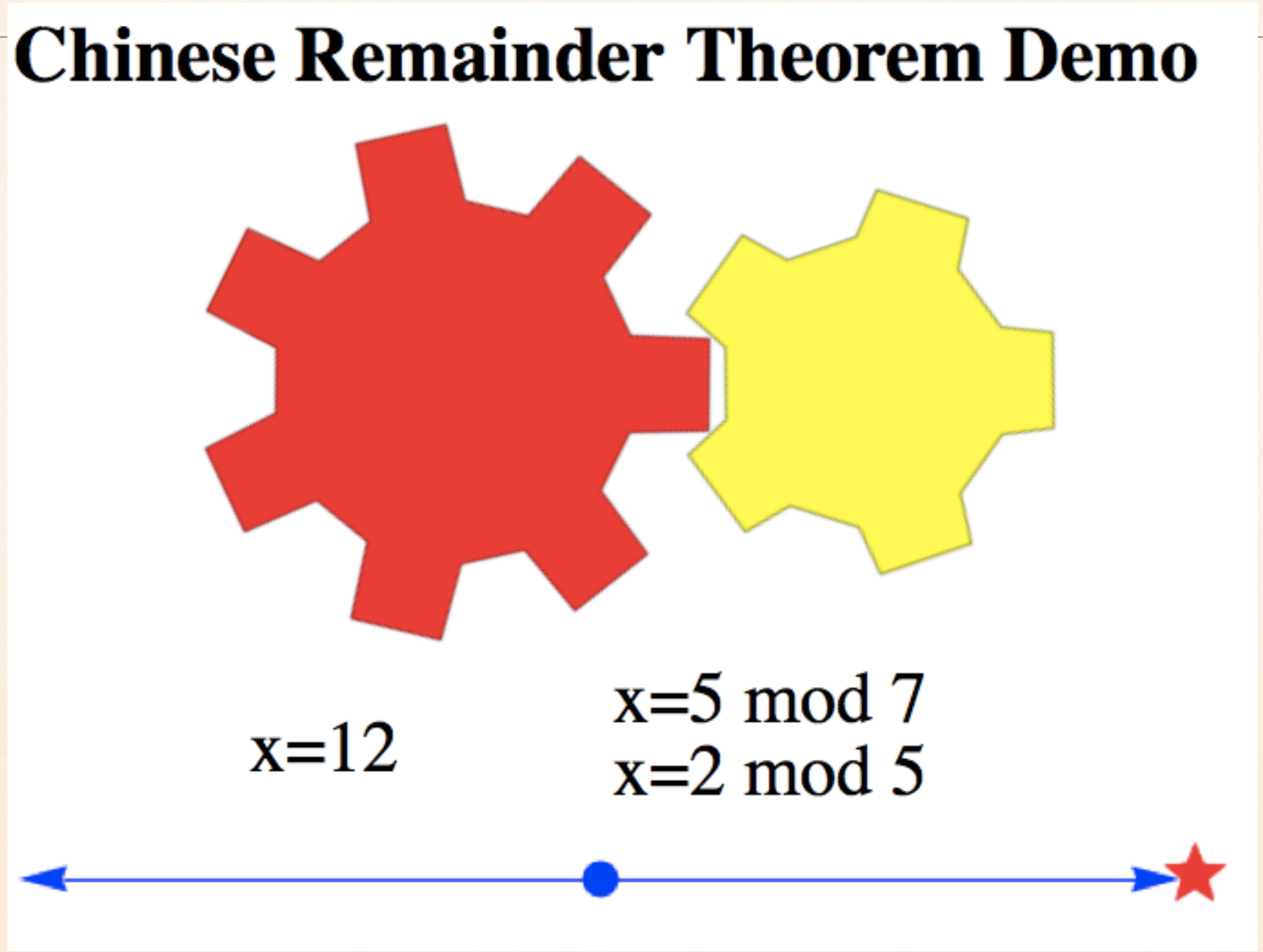
HOW DOES IT WORK?

$$x = 5 \bmod 7$$

$$x = 2 \bmod 14$$

Form x = 2,16,30,44,58,72,86 which solve the second equation. Then check the remainder with respect to 7. We do not find any solution now.

A DEMONSTRATION



```
<script>
// Oliver Knill, March 14, 2014,
// Online javascript illustration of the chinese remainder
// theorem.

var x1=40;    var y1=20;    // gear1 position
var a1=0;     var v1=0.2;   // gear1 angle
var x2=210;   var y2=20;    // gear2 position
var a2=0.2;   var v2=0.2;   // gear2 angle
var mm=0;     var nn=0;     // the variable x
var aa1;      var aa2;      // the values x mod 7 and x mod 5
var x=0;  var y=0;          // vector position
var xx=0; var yy=0;         // cursor position

function p(e){              // find mouse position
  if (navigator.appName=='Netscape'){xx=e.pageX; yy=e.pageY;} else{xx=event.clientX;yy=event.clientY;};
}

function c(){
  x=xx; y=yy;
  document.getElementById("curse").style.left=(x-20)  +"px";
  document.getElementById("curse").style.top =358 +"px";
  v1=(xx-255)/200;     v2=v1*7/5;
  a1=((a1+v1) % 360);  mm=mm+v1;
  a2=((a2-v2) % 360);
  aa1=Math.floor(a1*7/360)%7; aa2=Math.floor(-a2*5/360)%5;
  if (aa1<0) { aa1+=7; }      if (aa2<0) { aa2+=5; }
  nn=Math.floor(mm*7/360);
  n.innerHTML="x="+nn;
  eq1.innerHTML="x="+aa1+"  mod 7";
  eq2.innerHTML="x="+aa2+"  mod 5";
  document.getElementById("gear1").style.left = x1+"px";
  document.getElementById("gear1").style.top  = y1+"px";
  document.getElementById("gear1").style["WebkitTransform"]='rotate(' + a1 + 'deg)';
  document.getElementById("gear1").style["MozTransform"]   ='rotate(' + a1 + 'deg)';
  document.getElementById("gear1").style["transform"]      ='rotate(' + a1 + 'deg)';
  document.getElementById("gear2").style.left = x2+"px";
  document.getElementById("gear2").style.top  = y2+"px";
  document.getElementById("gear2").style["WebkitTransform"]='rotate(' + a2 + 'deg)';
  document.getElementById("gear2").style["MozTransform"]   ='rotate(' + a2 + 'deg)';
  document.getElementById("gear2").style["transform"]      ='rotate(' + a2 + 'deg)';
  setTimeout('c()',3);
}

document.onmousemove=setTimeout('c()',1);
document.onmousemove=p;

</script>
```

A MULTI-VARIABLE VERSION

From 2005

$$x + y = 3 \bmod 7$$

$$x - y = 5 \bmod 11$$

x=11

y=6

THEOREM

$$a\,x + b\,y = e \bmod m$$

$$c\,x + d\,y = f \bmod n$$

has a solution if

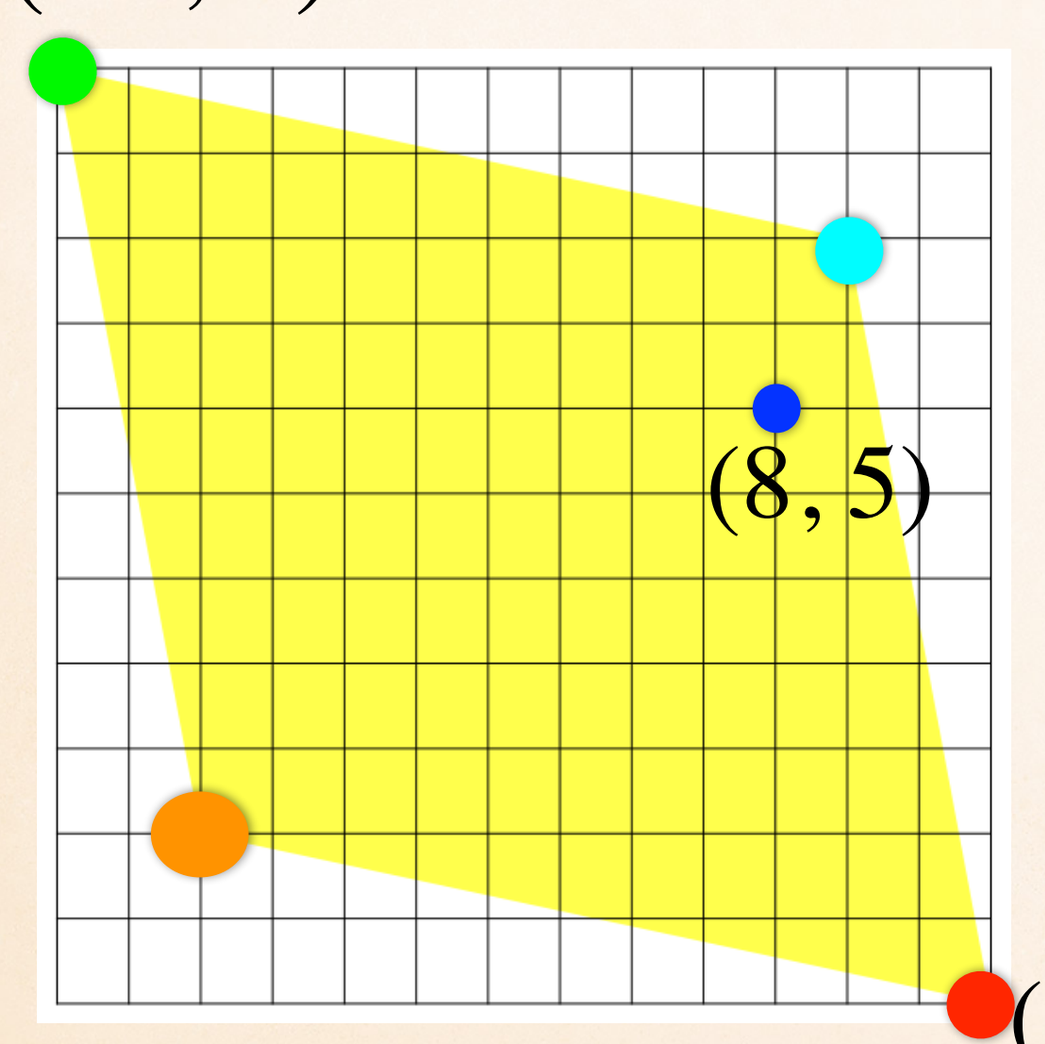
m,n have no common denominator
a or b are relatively prime to m
c or d are relatively prime to n

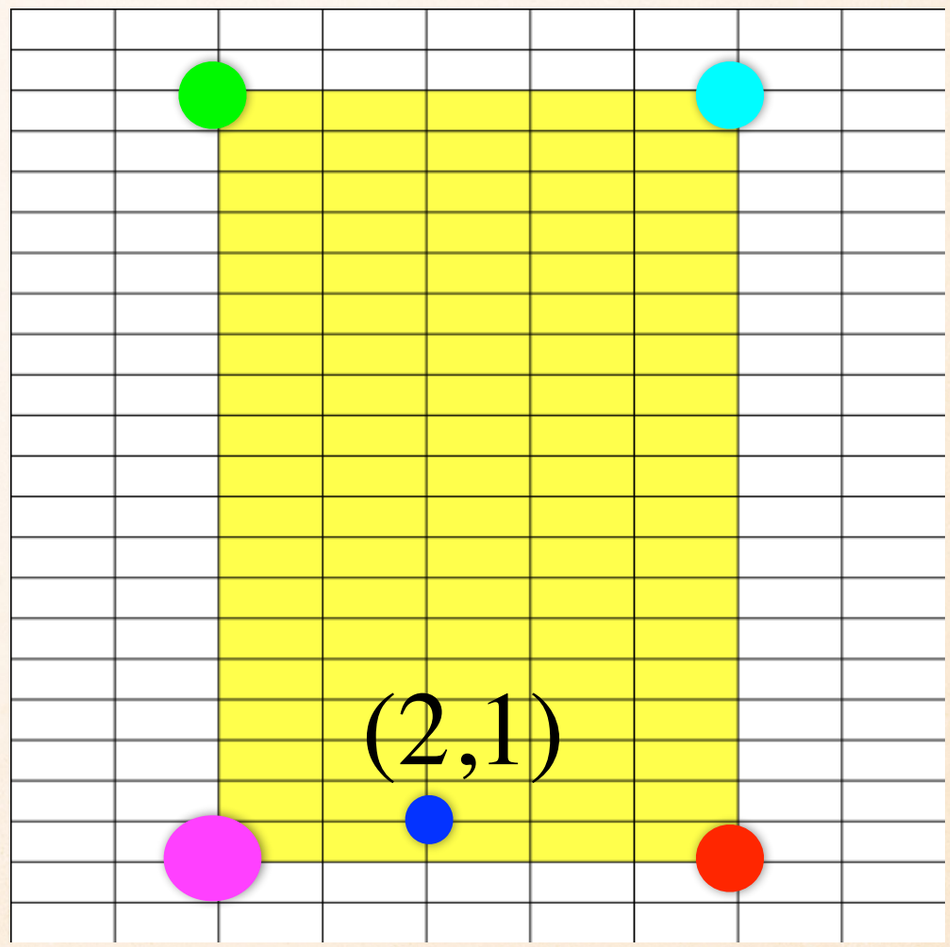
PROOF

First fix the first equation then the second equation etc.

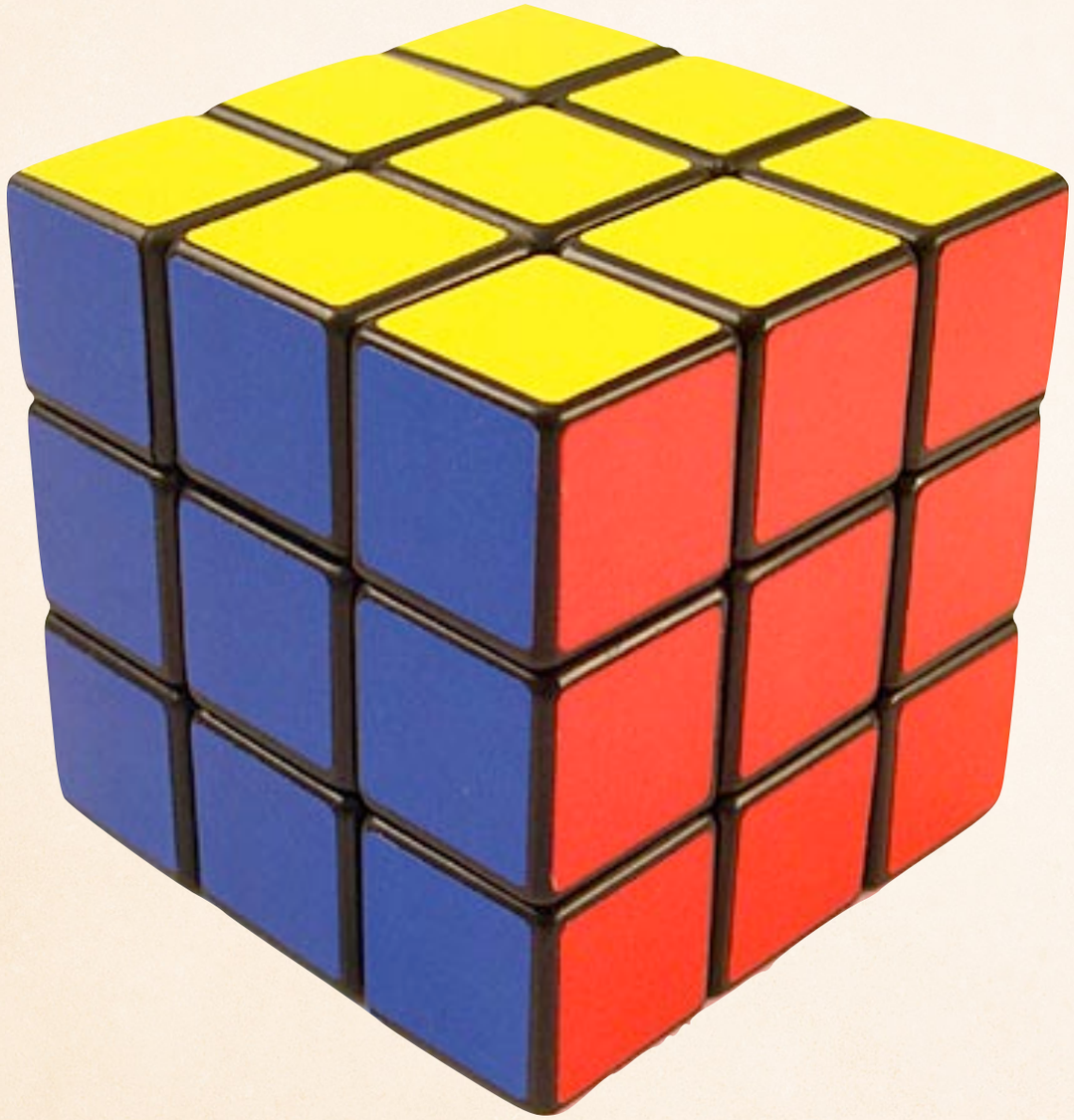
$$4x + 17y = 2 \bmod 5$$

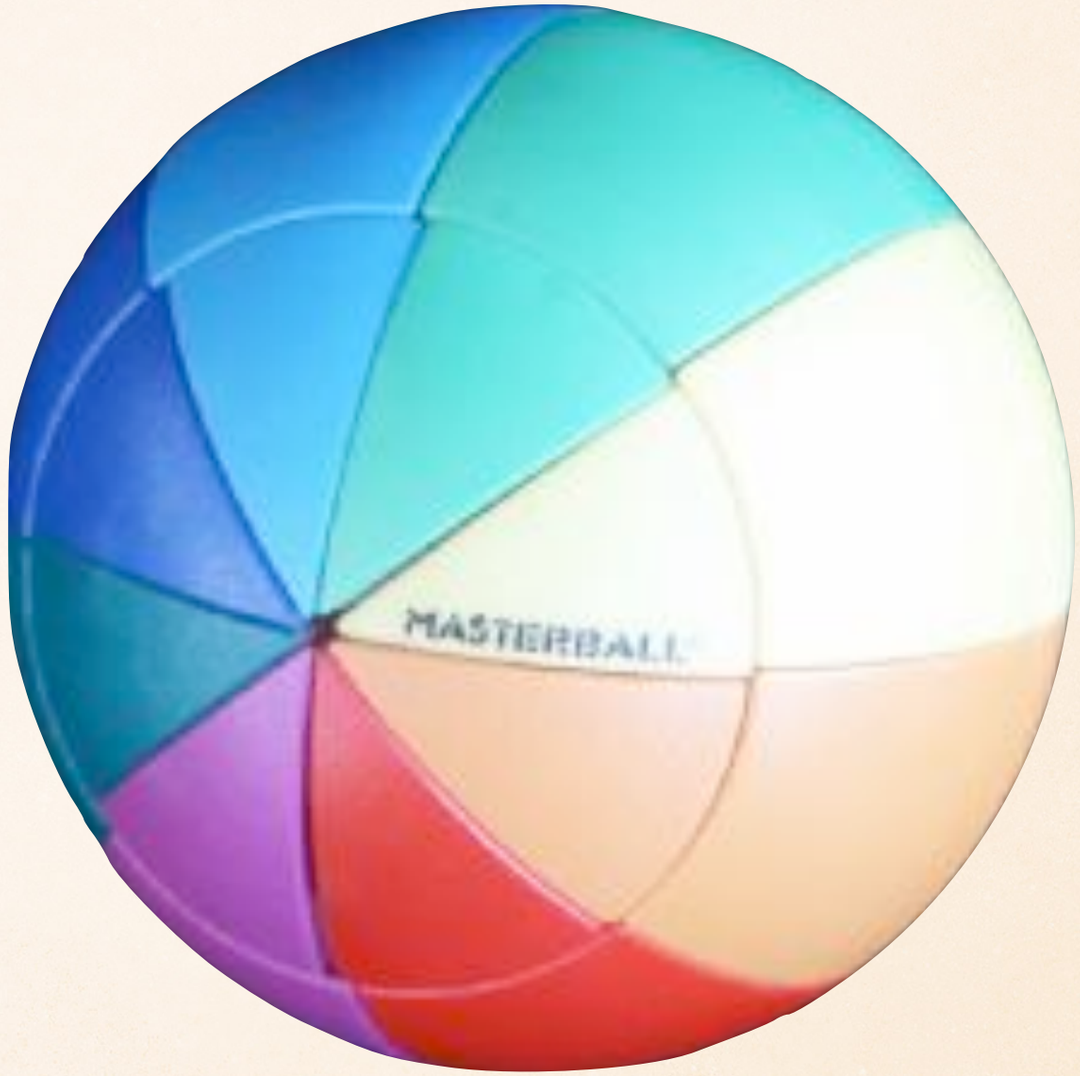
$$11x + 13y = 1 \bmod 19$$





SIMILAR IDEA





WHERE IS IT USED?

CALENDAR PROBLEMS

x is a Tuesday

x is the 11’th day in the year

$x = 2 \bmod 7$

$x = 11 \bmod 365$

CRYPTOLOGY AND CODES

FACTORIZATION

The **Holy Grail** of factoring $n = p\,q$ is to find x for which

$$x^2 \bmod n$$

is small.

Fermat, Quadratic sieve, Morrison Brillard,...

EXAMPLE

$$n = 62773913$$

Find $\sqrt{1} \mod n$

The answer is x=15695459

Now form gcd(x-1,n) = 7927
This is a factor of n.

HOLY GRAIL

Finding roots
modulo n
is equivalent to
factoring!

HOW DO WE FIND SQUARE ROOTS?

This is what I tried maybe over a decade ago and which brought me to the multidimensional Chinese Remainder theorem.

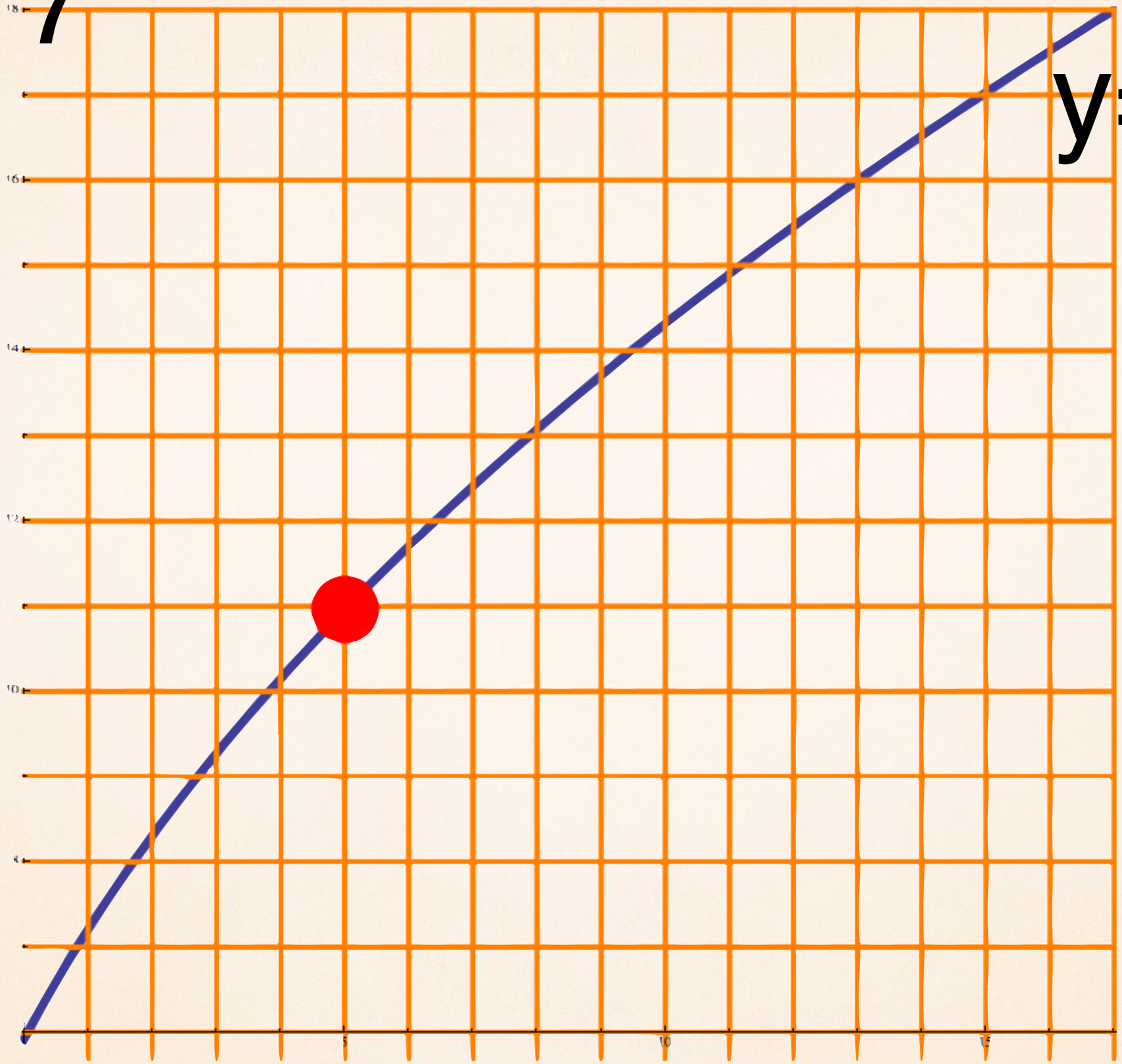
HERE WAS MY IDEA:

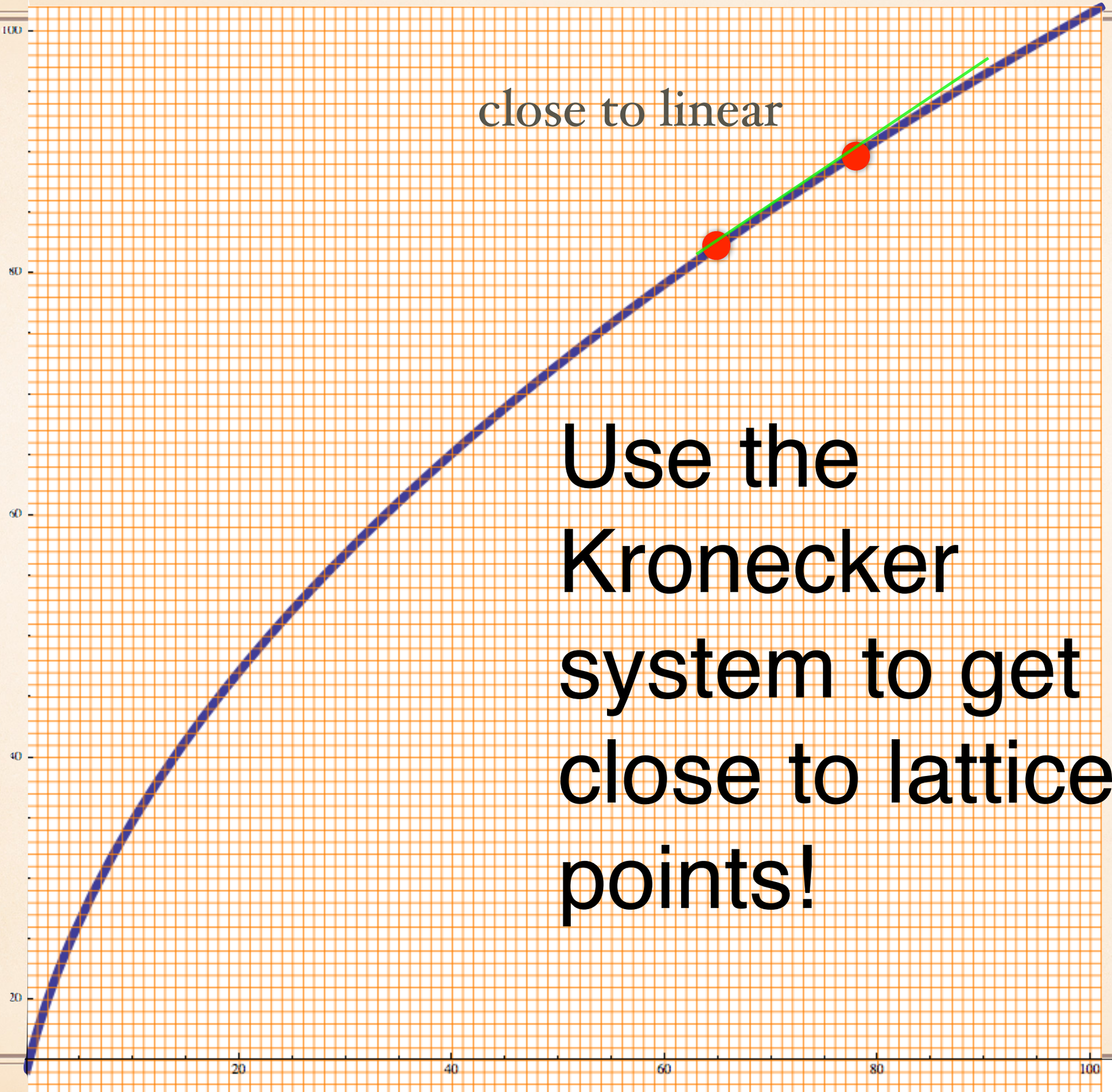
If

$$f(x) = \sqrt{2n^2 + x\,n + 1}$$

is very close to an integer y, then
y^2 is mall modulo n

n=17




close to linear
Use the Kronecker system to get close to lattice points!
100
80
60
40
20
20
40
60
80
100

AFTER LOTS OF TRIAL AND ERROR ...

We need a higher dimensional approximation which is better!

ONE OF MANY IDEAS ...

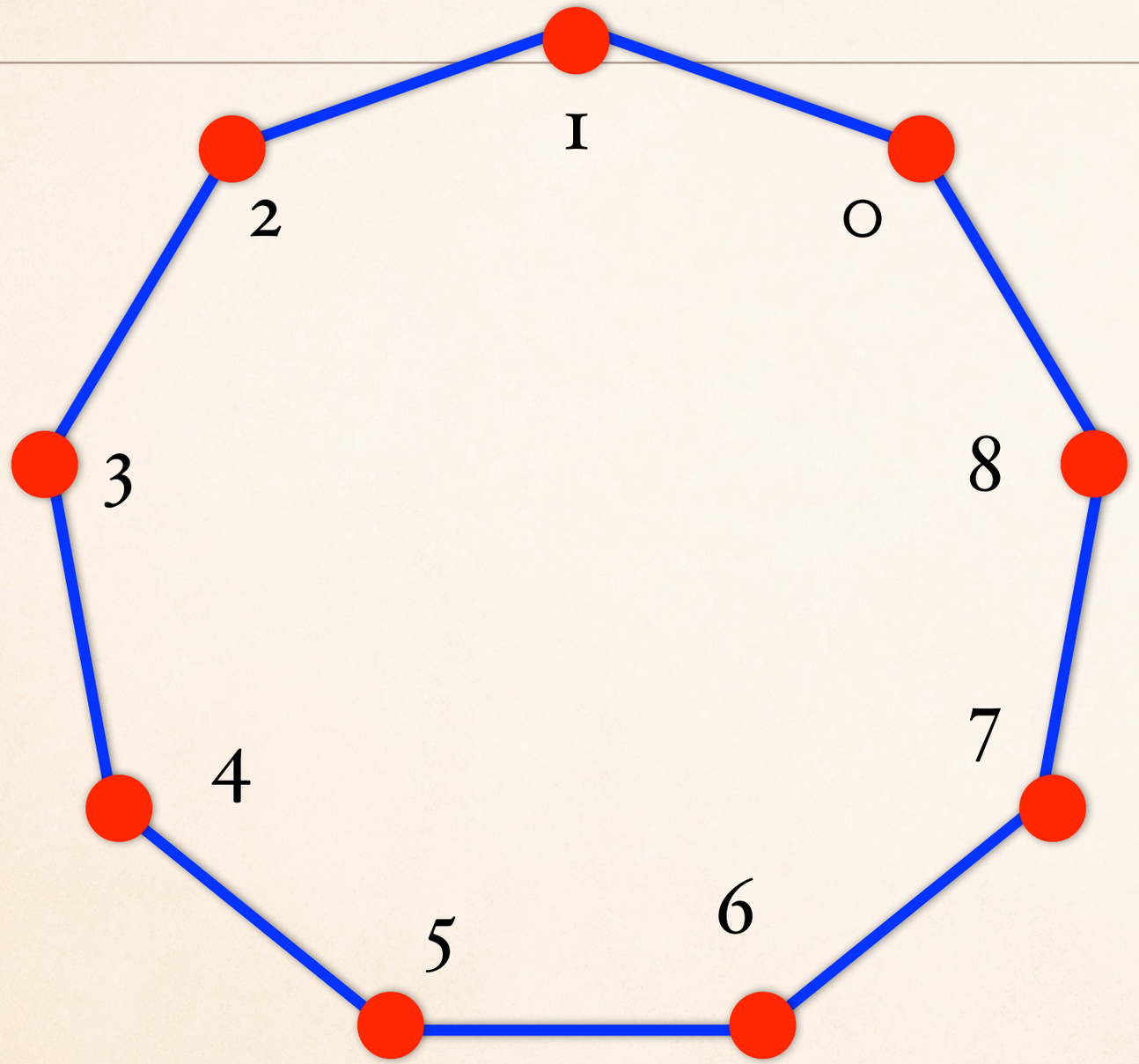
If

$$f(x) = \sqrt[3]{2n^3 + x\,n^2 + y\,n + 1}$$

is very close to an integer z, then z^3 is small modulo n. If we hit a lattice point, then gcd(n,z-1) is a factor.

WE NEED TO DO BETTER THAN LINEAR APPROXIMATION

KRONECKER



jump by 5
get to 0 from 3 to 0

$$2 + 5x = 0 \bmod 9$$

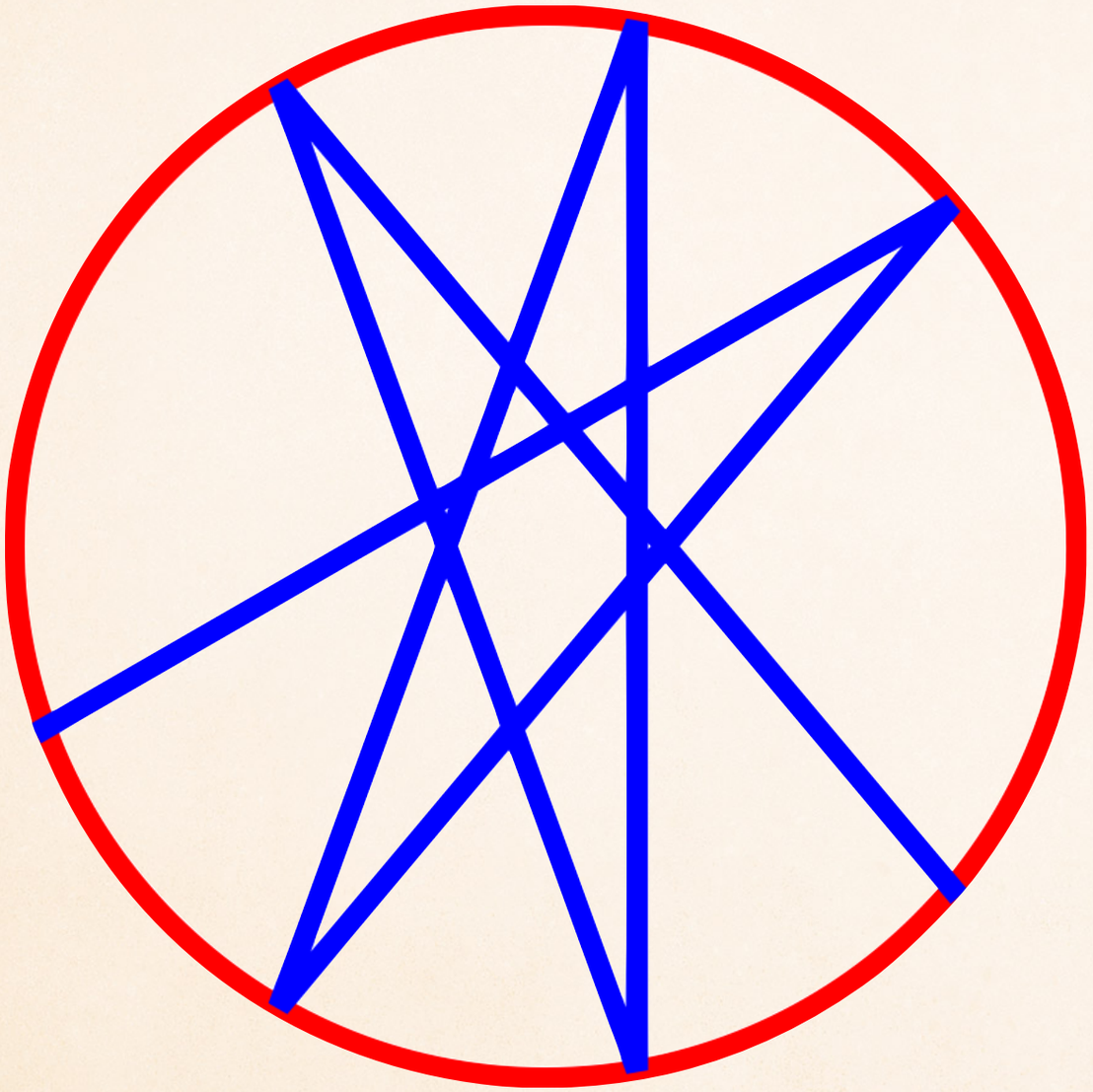
2,7,12,17,22,27,32,37,42,47,52,57,62,67,72,77,....

THE OFFICE

2007, Office Season 4

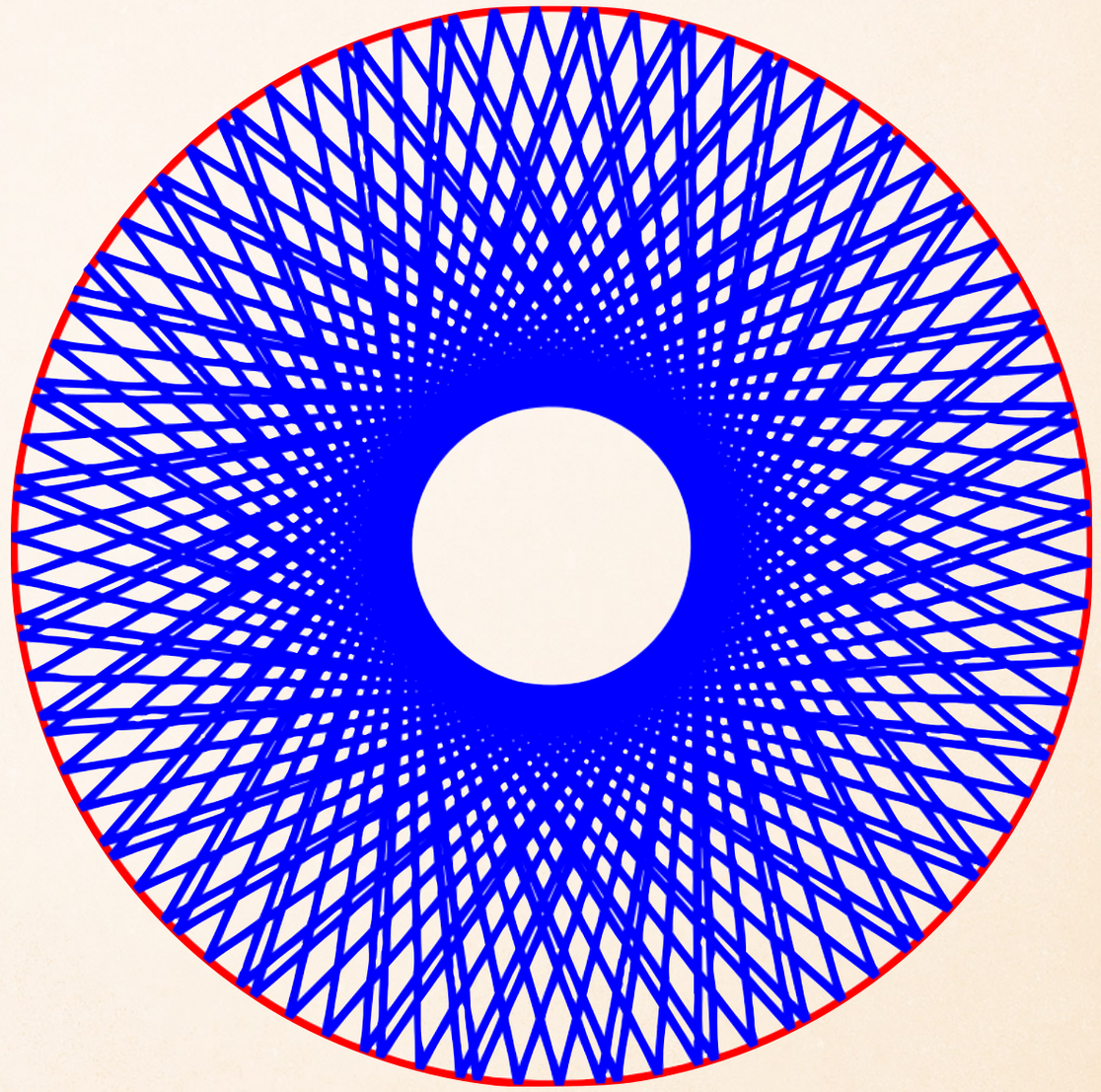
RATIONAL IRRATIONAL

Chinese Remainder Theorem



5/9

Kronecker,Khinchin



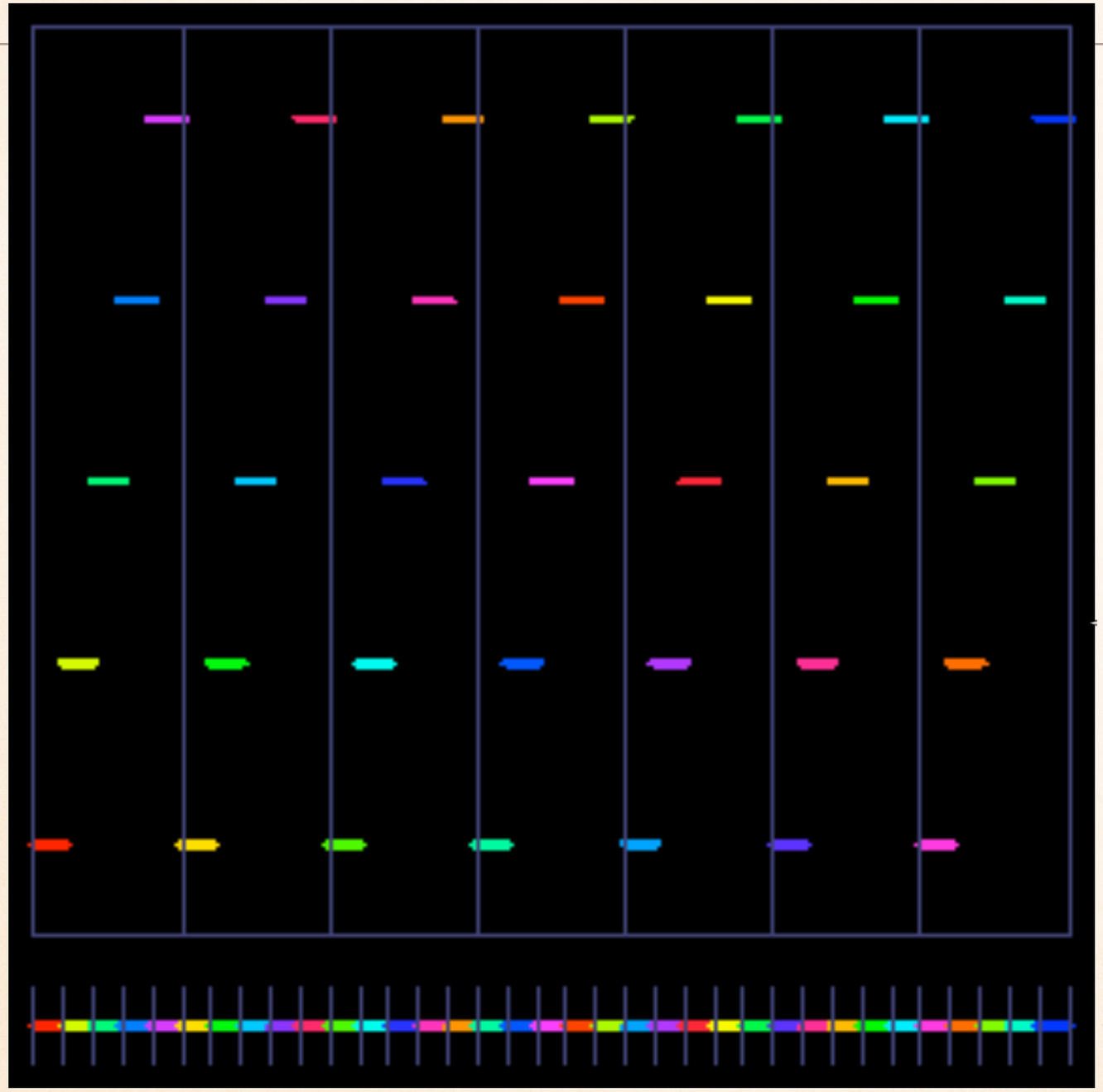
√2

LATTICE POINTS NEAR PLANES

$$a\,x + b\,y + d = z$$

Find pairs (n,m) for which an + b m + t is small modulo 1

TWO DIM RATIONAL



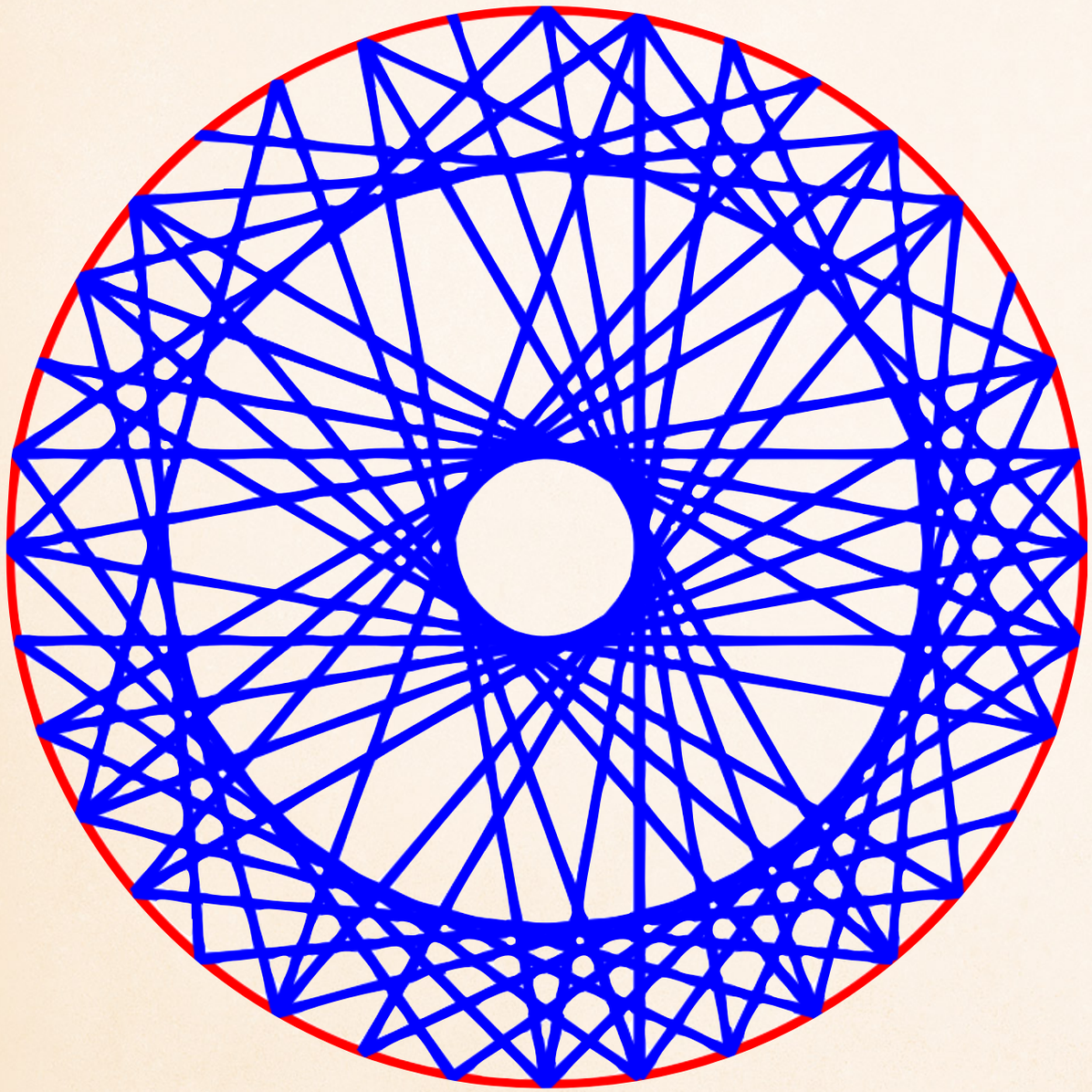
If $\alpha = p/q$

and $\beta = r/s$

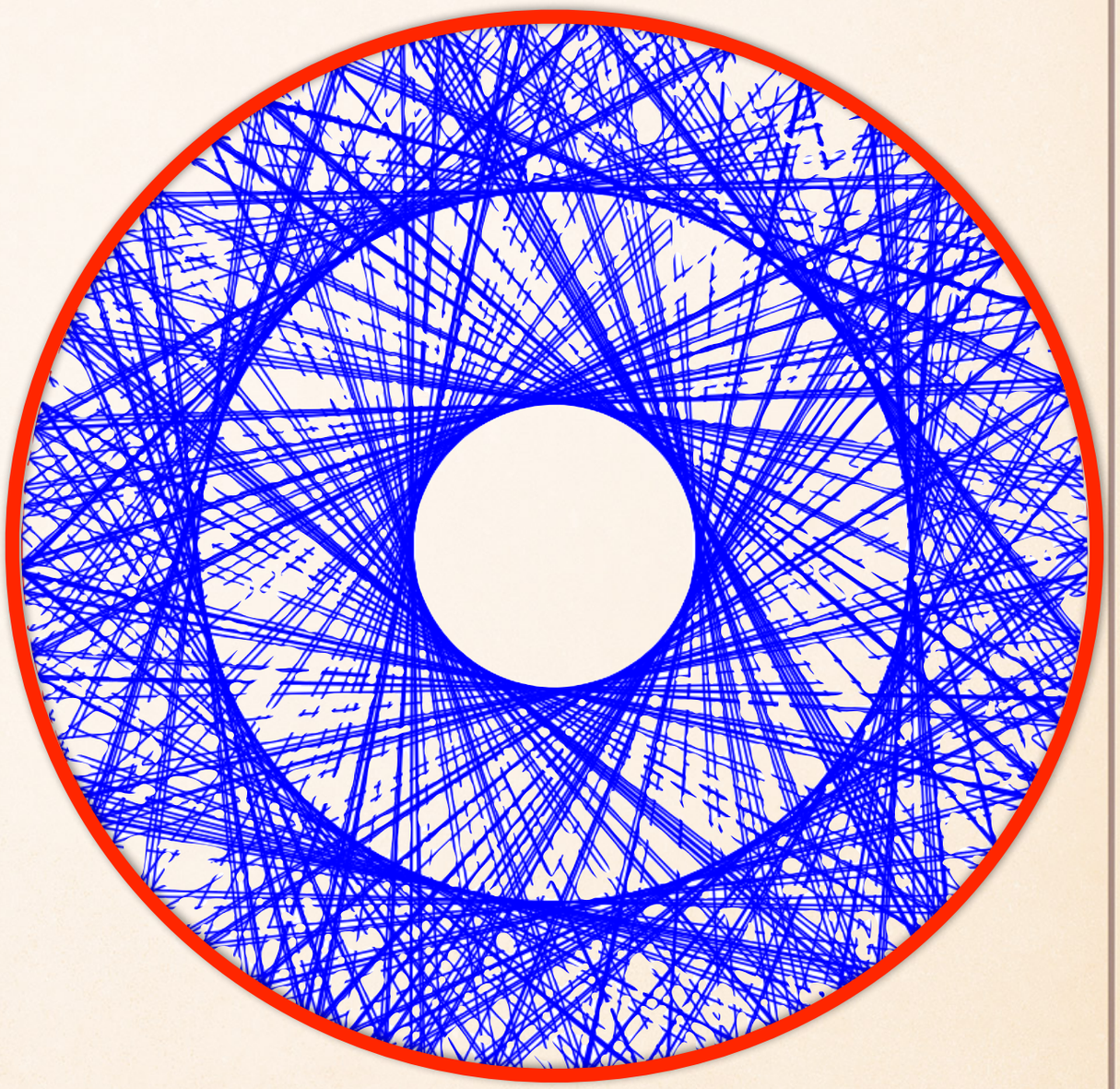
and $\gcd(q,s)=1$, then there are $m<q, n<s$ with

$$\alpha n+\beta m+t<1/(qs)$$

TWO DIMENSIONAL KRONECKER

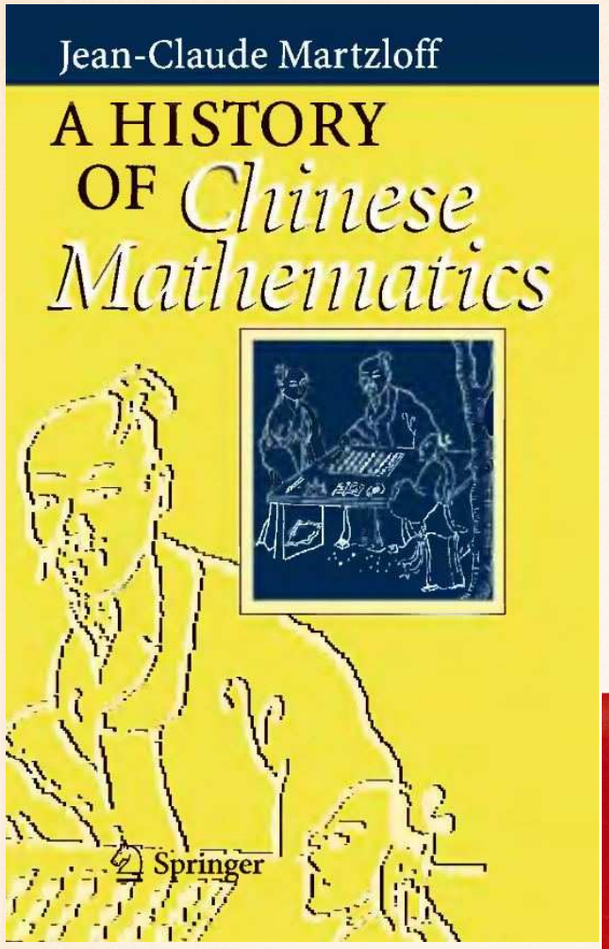


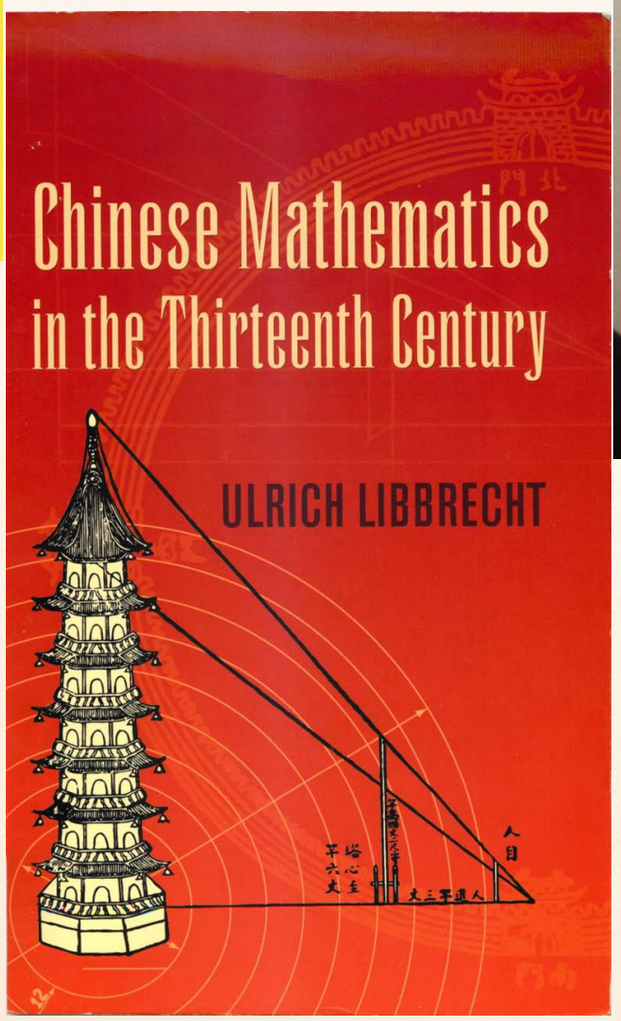
(5/9,4/9)

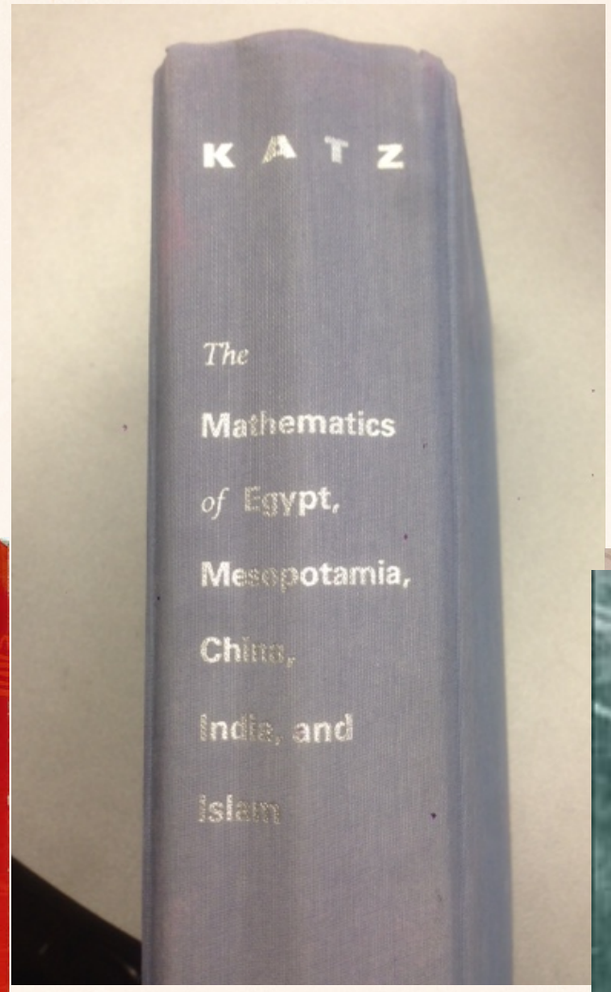


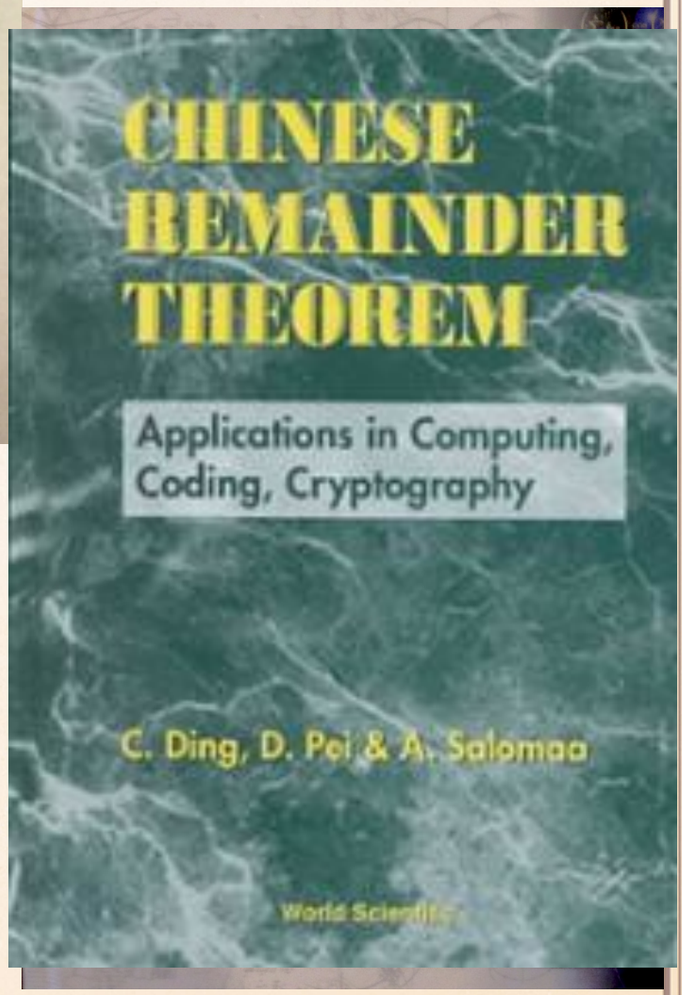
(√2,√3)

LITERATURE


Jean-Claude Martzloff
A HISTORY OF Chinese Mathematics
Springer


Chinese Mathematics
in the Thirteenth Century
ULRICH LIBBRECHT


KATZ
The
Mathematics
of Egypt,
Mesopotamia,
China,
India, and
Islam


CHINESE REMAINDER THEOREM
Applications in Computing, Coding, Cryptography
C. Ding, D. Pei & A. Salomaa
World Scientific