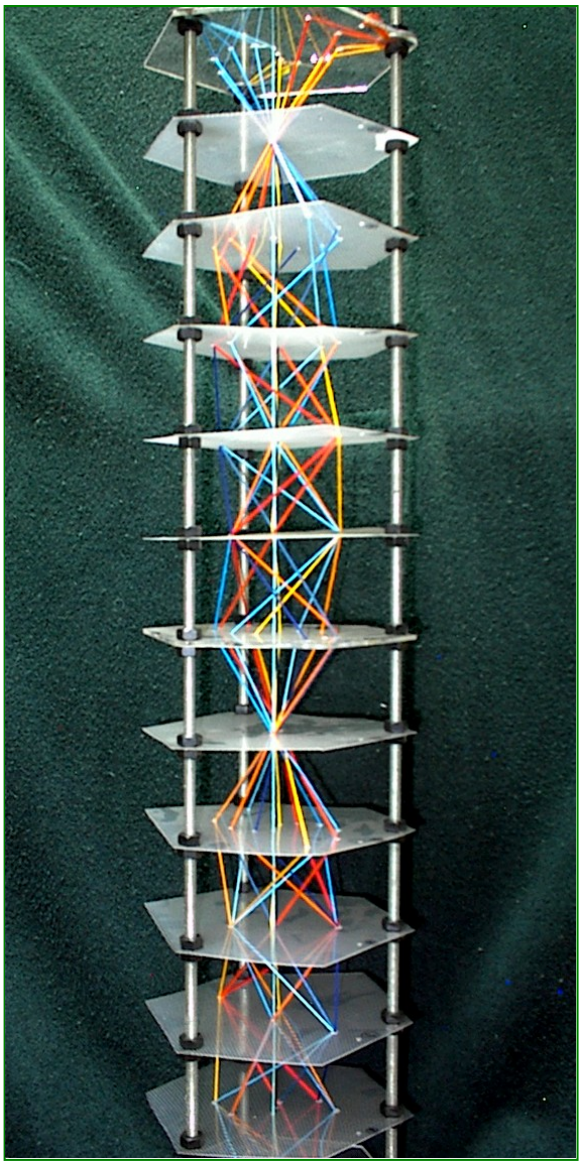
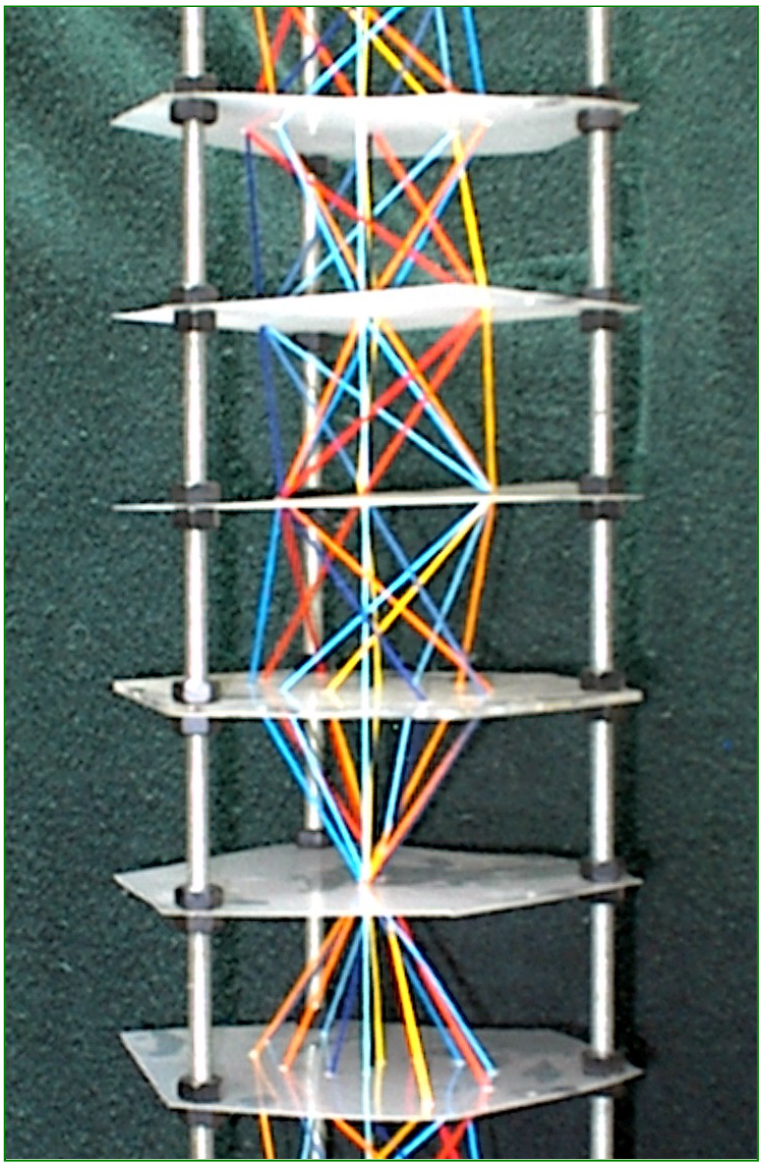
A string sculpture illustrating

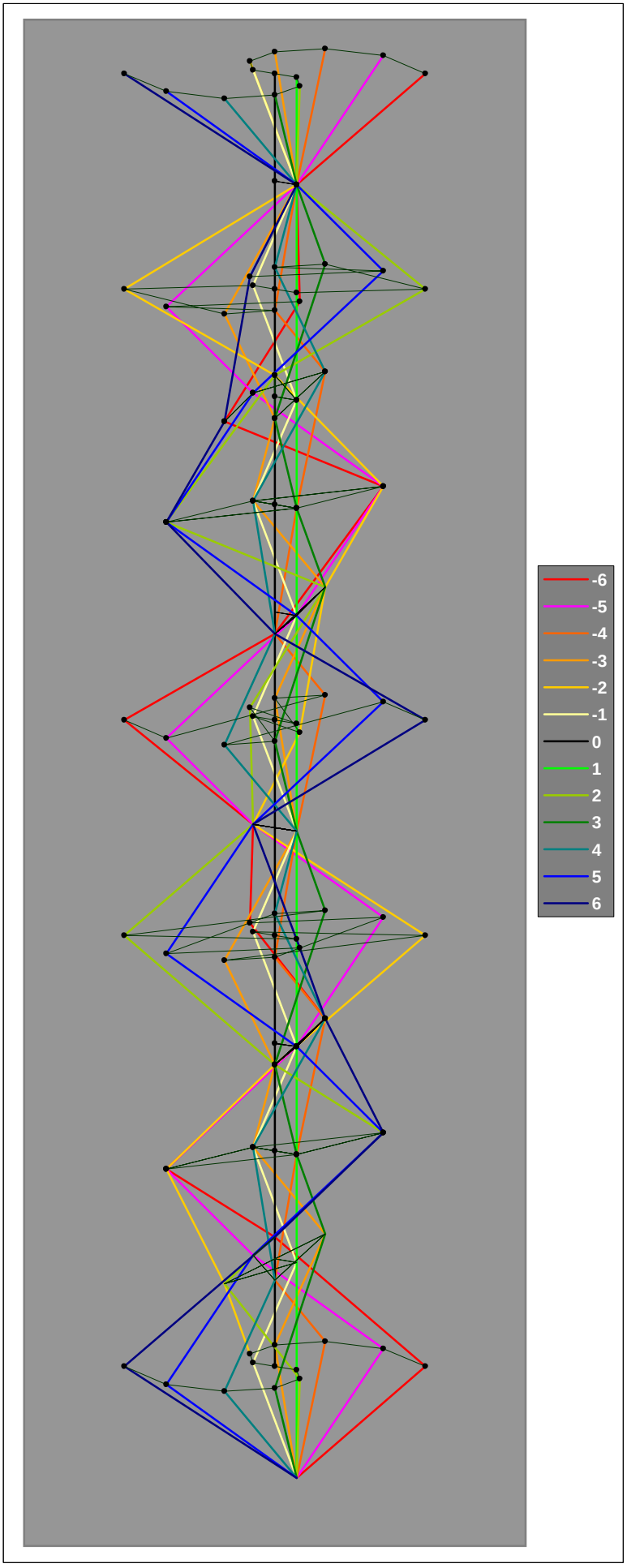
Fermat's Little Theorem

Jim Smith
San Cristóbal de Las Casas
Chiapas, Mexico
June 2007

Normal and close-up views of the completed sculpture






-6
-5
-4
-3
-2
-1
0
1
2
3
4
5
6

About Fermat's Little Theorem

If you search the Internet, you'll find a great deal about this theorem, including several proofs of it. I'll explain it briefly here, using the number 13 as an example.

If we divide a number by 13, there are only 13 possible remainders:

1,2,3,4,5,6,7,8,9,10,11, 12, and (if the number is a multiple of 13) zero.

Based upon this observation we can say that all integers belong to one of 13 groups:

Those that give the remainder	0	when divided by 13.
" "	1	" "
" "	2	" "
" "	3	" "
" "	4	" "
" "	5	" "
" "	6	" "
" "	7	" "
" "	8	" "
" "	9	" "
" "	10	" "
" "	11	" "
" "	12	" "

To save some effort when discussing these ideas, we call these groups the equivalence classes of modulus 13. This expression allows us to say, for example, that

"The numbers 1, 14, and 27 all belong to equivalence class [1], modulus 13"

rather than

"The numbers 1, 14, and 27 all belong to the set of numbers whose remainder is 1 when divided by 13".

If two numbers belong to the same equivalence class of modulus 13, we also say that they are congruent to each other with respect to that modulus. We use the symbol "≡" to say "is congruent to". Therefore, all of the following communicate the same information:

"The numbers 1, 14, and 27 all belong to the set of numbers whose remainder is 1 when divided by 13"

"The numbers 1, 14, and 27 all belong to equivalence class [1], modulus 13"

"$14 \equiv 27 \equiv 1$, modulus 13".

So: what does Fermat's Little Theorem assert?

For every integer $\boldsymbol{a}$, and every prime number $\boldsymbol{p}$, $\boldsymbol{a^p} \equiv \boldsymbol{a}$, mod $\boldsymbol{p}$.

That is, both $\boldsymbol{a}$ itself, and $\boldsymbol{a}$ raised to the exponent $\boldsymbol{p}$, give the same remainder when divided by $\boldsymbol{p}$. Equivalently,

For every integer $\boldsymbol{a}$, and every prime number $\boldsymbol{p}$, $\boldsymbol{a^{p-1}} \equiv 1$, mod $\boldsymbol{p}$.

Or in other words, if we raise any integer to an exponent that is 1 less than any prime number, then divide by that same prime number, the remainder will always be 1.

Please note the following alternative set of equivalence classes for Modulus 13

Instead of listing the equivalence classes as

[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]

we may also list them as

[0], [1], [2], [3], [4], [5], [6], [-6], [-5], [-4], [-3], [-2], [-1]

Why is this? Consider the class [7]. Each number that belongs to that class is 7 more than some multiple of 13. But that means that such a number is also 6 less than the next multiple of 13. Therefore, it is also congruent to -6 (which is 6 less than 13×0). By the same reasoning, the classes [m] and [m – 13] are always identical.

Because this alternative set is expressed using numbers that are symmetric about 0, it is used in this string sculpture.

About the sculpture

The framework consists of plastic sheets spaced along 1/4” threaded rods, at intervals of 2 inches. The upper, lower, and middle sheets are made of 1/8” acrylic for greater strength.

Each sheet represents an exponent from 0 to 13. The lowermost sheet represents “0”, and the rest are in ascending order.

In each sheet is drilled a pattern of numbered holes. Those patterns will be presented later.

Each string represents an equivalence class, mod 13. Its path through the sheets follows the sequence of equivalence classes through which any number of its class will pass as it is raised to exponents 0 through 13.

For example, consider the string for the equivalence class [$^{-}$6]. When we thread that string through the sheet that represents exponent **n**, we will thread it through the hole that bears the number

$$(^{-}6)^{n}, \text{ modulus } 13.$$

Note that “$(^{-}6)^{n}$, modulus 13” is just the remainder that results when $(^{-}6)^{n}$ is divided by 13. However, please see the page entitled “Please note the following alternative set of equivalence classes for Modulus 13” regarding the negative equivalence classes used when the remainder exceeds 6.

The sequence of holes through which the string for equivalence class [$^{-}$6] passes is as shown by the list of **red** numbers.

Exponent, **n**	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$(^{-}6)^{n}$, modulus 13	**1**	**$^{-}$6**	**$^{-}$3**	**5**	**$^{-}$4**	**$^{-}$2**	**$^{-}$1**	**6**	**3**	**$^{-}$5**	**4**	**2**	**1**	**$^{-}$6**

What Path Does Each Thread Follow?

On the next page, you will find a table showing the path for each thread. A portion of that table's information is reproduced below, using the thread for equivalence class $^{-}6$ as an example. Please note that the exponents are given in descending order, but that the description of each thread's path is in ascending order.

The thread for equivalence class $^{-}6$ passes through hole #1 in the lowest sheet (the sheet for exponent 0), then through hole $^{-}6$ in the sheet for exponent 1. It passes through hole $^{-}3$ in the sheet for exponent 2. Its complete path is

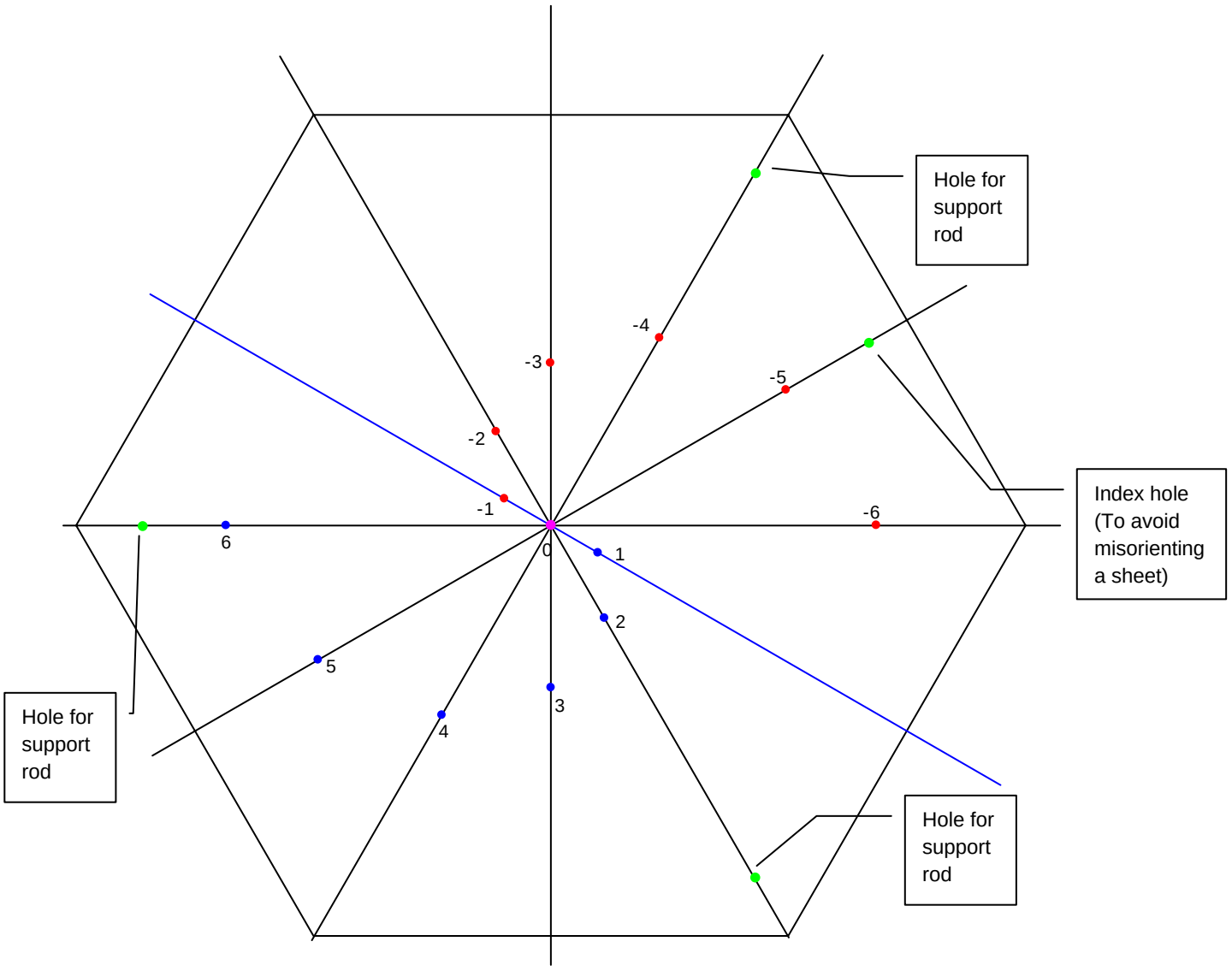
Exponent	**Number of the hole through which the thread for equivalence class $^{-}6$ passes**
13	$^{-}6$
12	1
11	2
10	4
9	$^{-}5$
8	3
7	6
6	$^{-}1$
5	$^{-}2$
4	$^{-}4$
3	5
2	$^{-}3$
1	$^{-}6$
0	1

Values of (a^n) mod 13

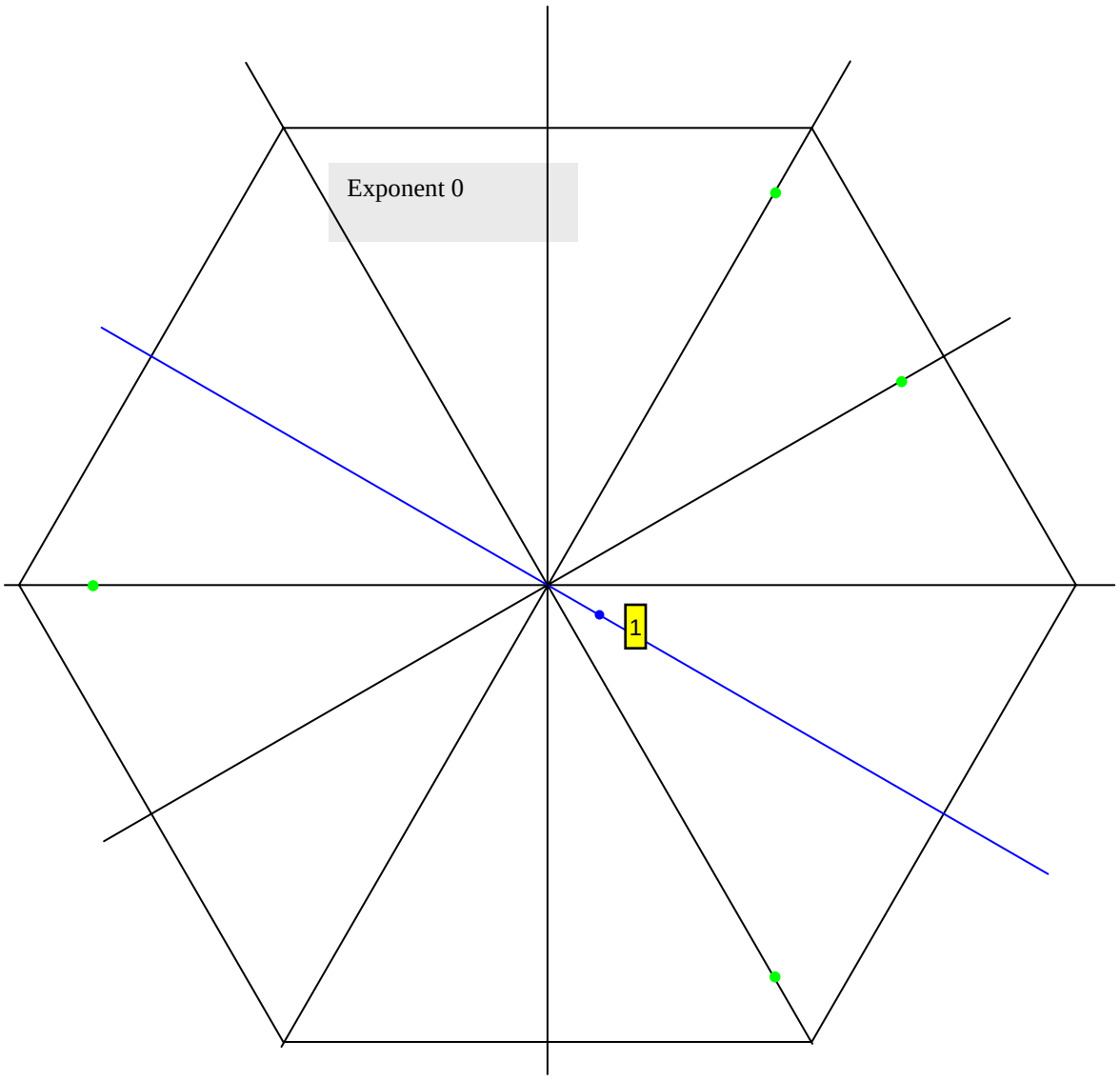
n (the exponents)	a (the equiv classes)												
	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
13	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
12	1	1	1	1	1	1	0	1	1	1	1	1	1
11	2	5	3	4	6	-1	0	1	-6	-4	-3	-5	-2
10	4	-1	-4	3	-3	1	0	1	-3	3	-4	-1	4
9	-5	-5	1	-1	-5	-1	0	1	5	1	-1	5	5
8	3	1	3	-4	-4	1	0	1	-4	-4	3	1	3
7	6	5	-4	-3	2	-1	0	1	-2	3	4	-5	-6
6	-1	-1	1	1	-1	1	0	1	-1	1	1	-1	-1
5	-2	-5	3	4	-6	-1	0	1	6	-4	-3	5	2
4	-4	1	-4	3	3	1	0	1	3	3	-4	1	-4
3	5	5	1	-1	5	-1	0	1	-5	1	-1	-5	-5
2	-3	-1	3	-4	4	1	0	1	4	-4	3	-1	-3
1	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
0	1	1	1	1	1	1	-	1	1	1	1	1	1

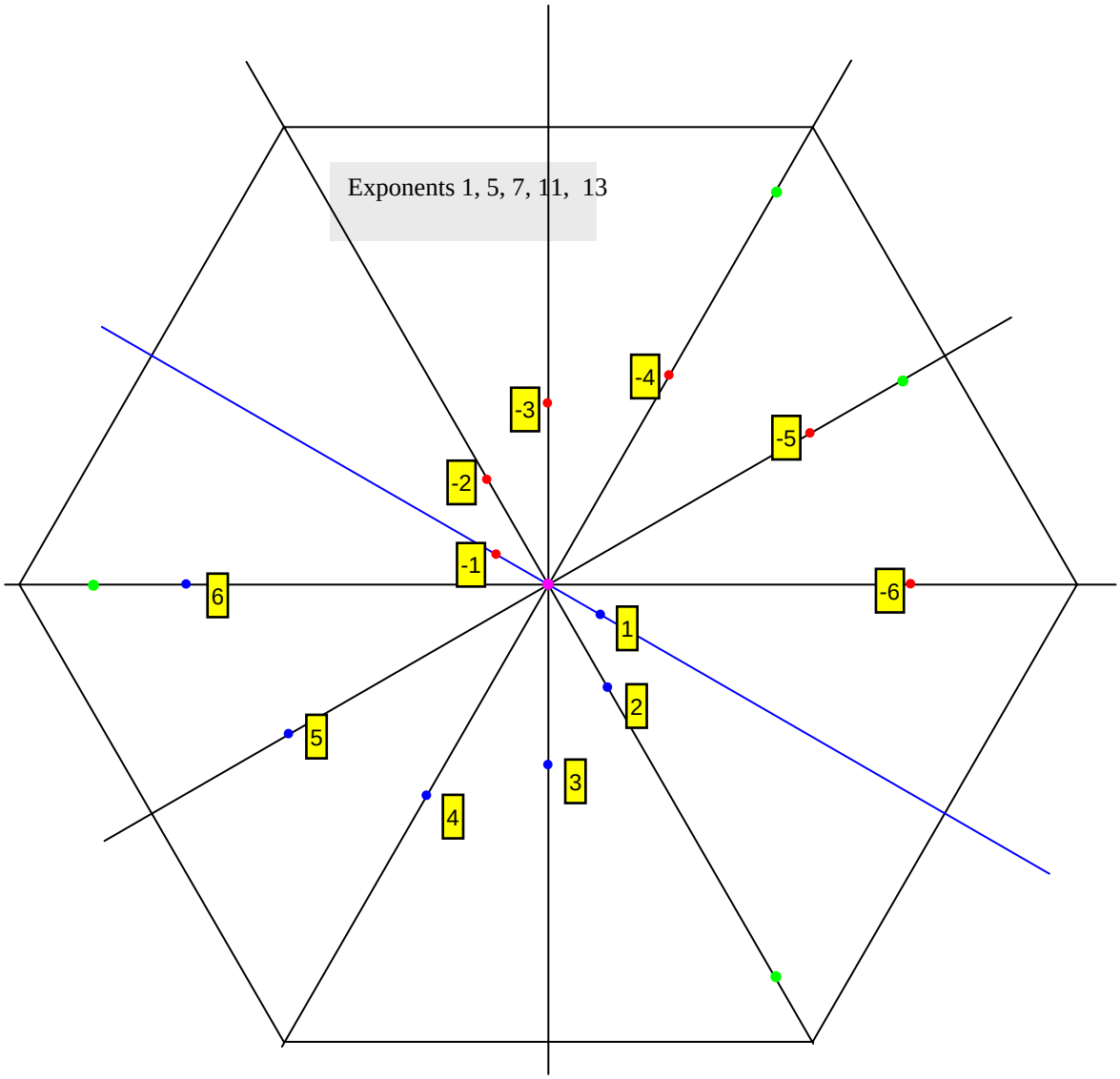
a	DMC Cotton Embroidery Thread Number·
-6	606
-5	608
-4	740
-3	741
-2	972
-1	973
0	I lost the number — it’s their black thread
1	3846
2	996
3	3843
4	995
5	825
6	820

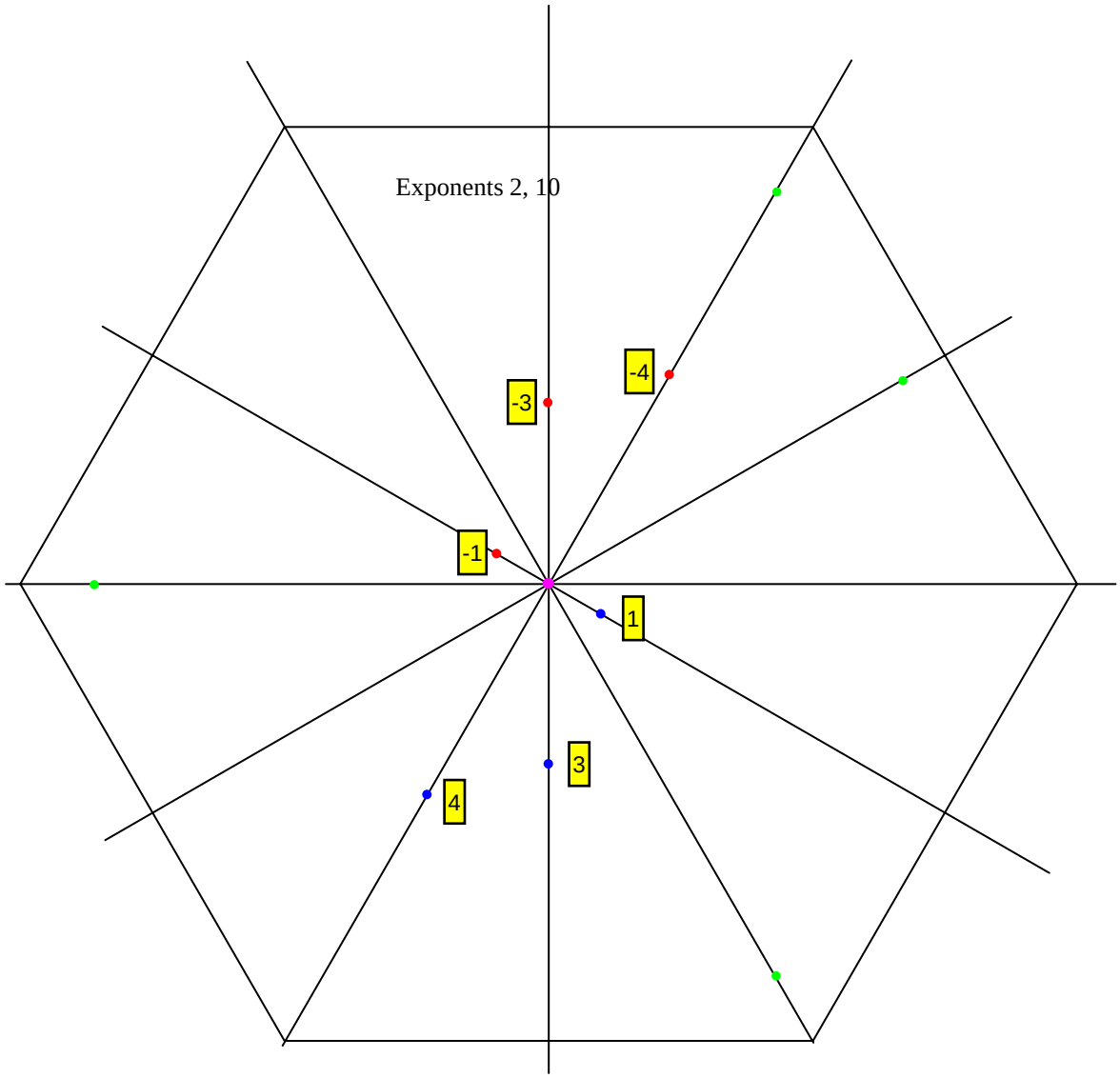
Master Template

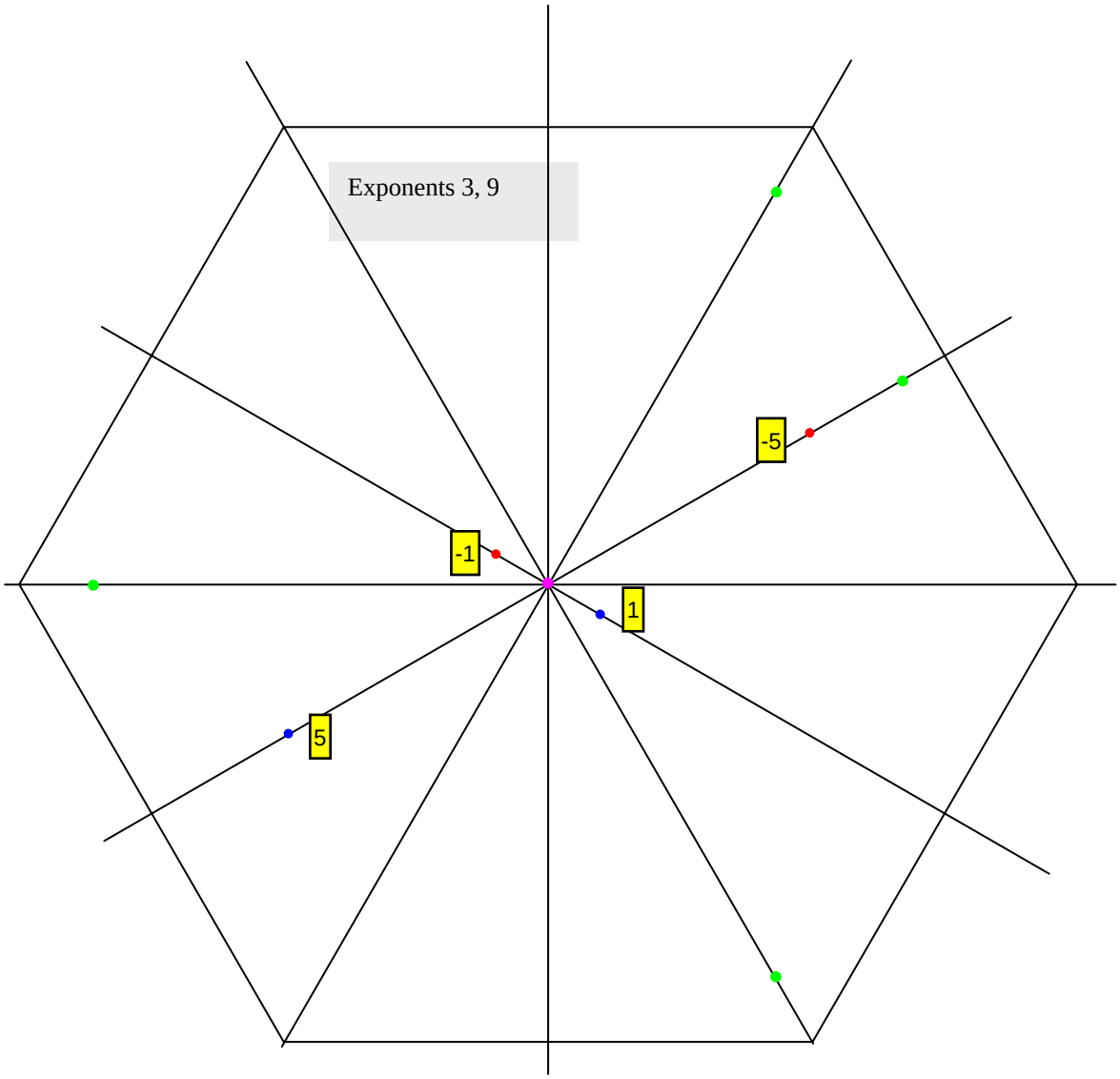


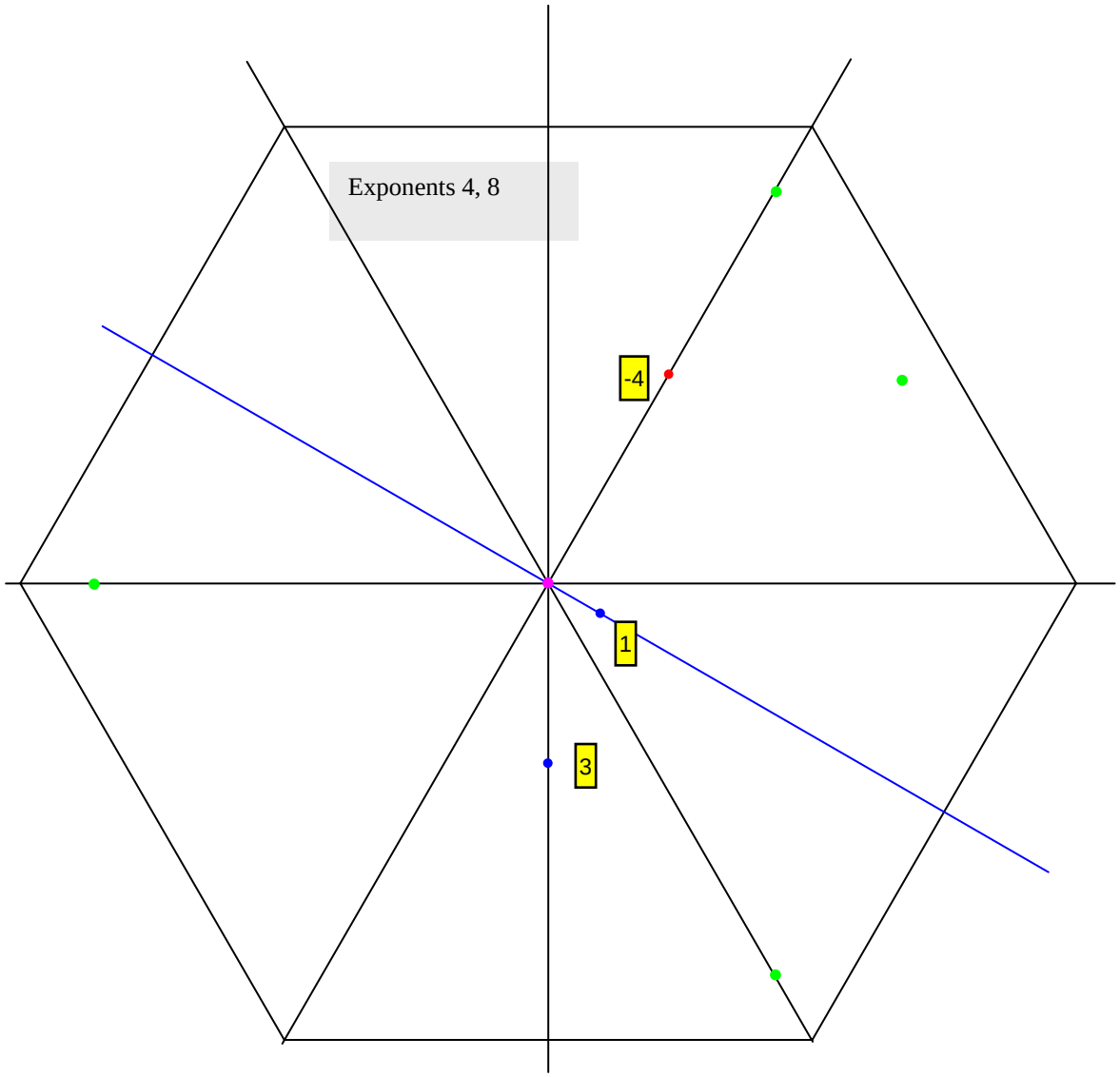
Templates for Each Exponent

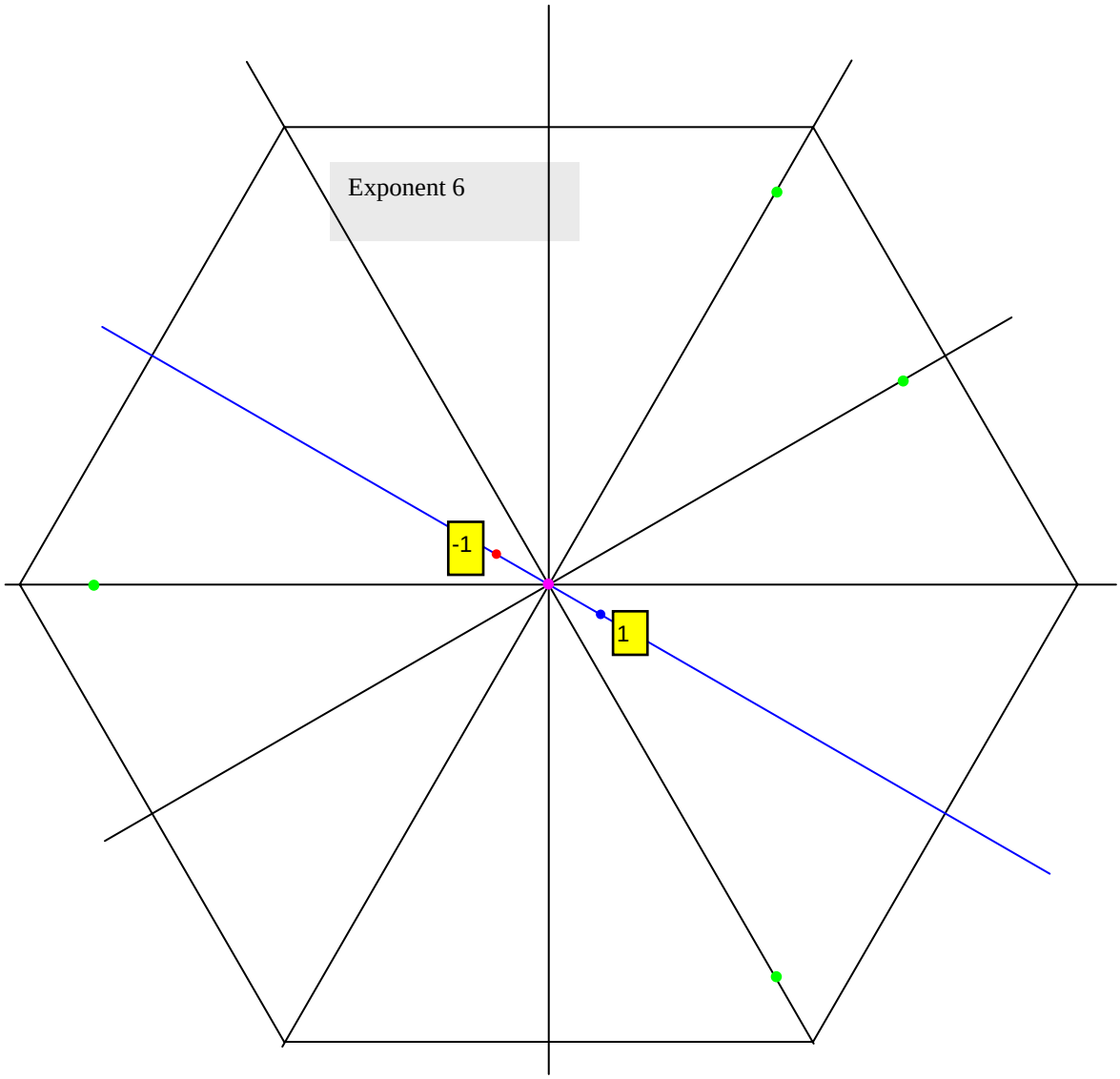


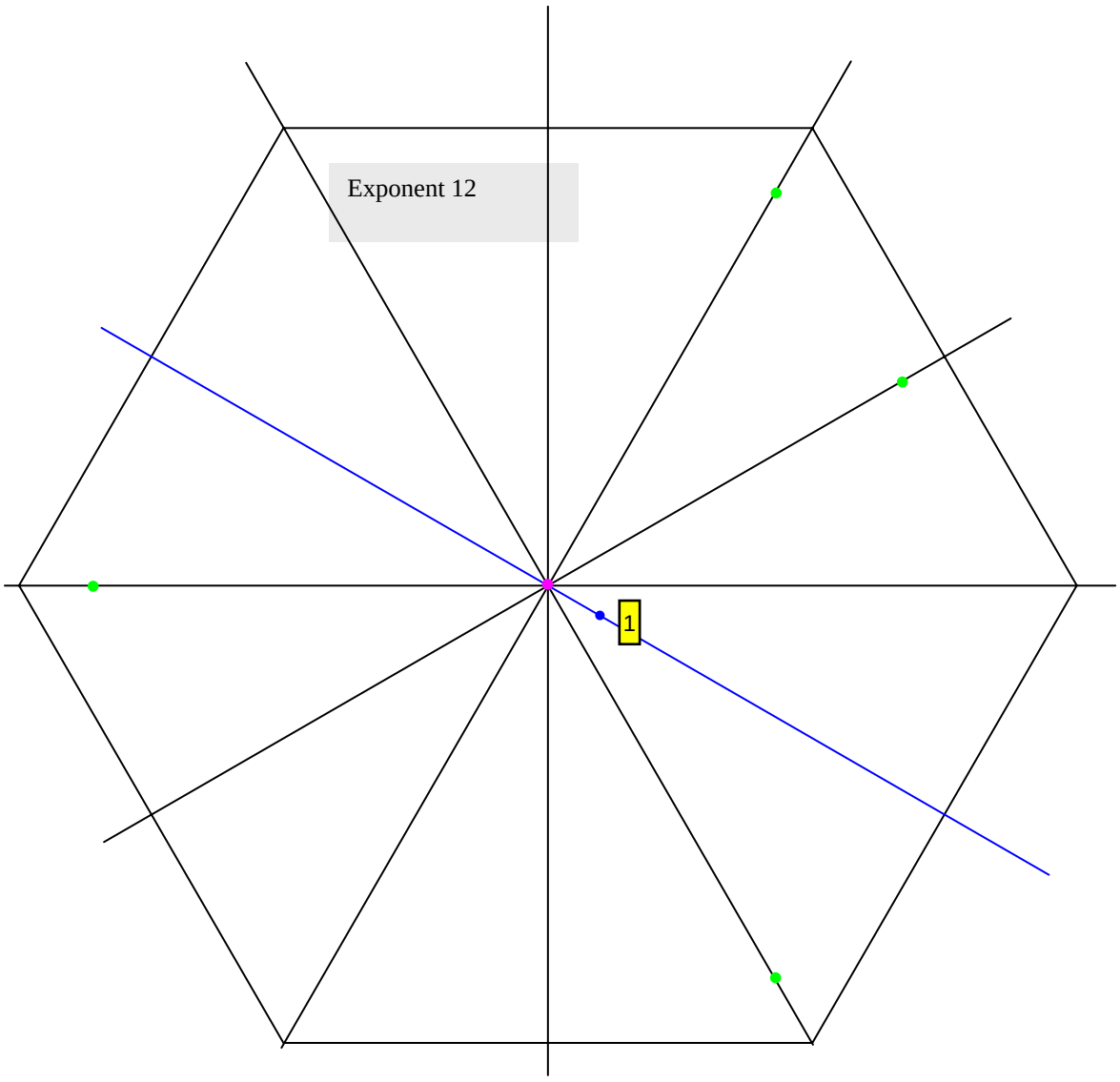

Exponents 1, 5, 7, 11, 13
-4
-3
-5
-2
-1
6
-6
1
2
5
3
4


Exponents 2, 10
-4
-3
-1
1
3
4


Exponents 3, 9
-5
-1
1
5


Exponents 4, 8
-4
1
3


Exponent 6
-1
1


Exponent 12
1

Fermat's Little Treasure

{In which I explain the designs on the cover.}

I'd done it: I'd finally proven Fermat's Little Theorem.

Now I'd better explain before you cringe and turn the page.

If the words "Fermat" and "theorem" ring a bell, that's probably because of Fermat's more-famous Last Theorem, which received much publicity when it was finally proven about ten years ago after intense work by generations of mathematicians. In contrast, proving Fermat's Little Theorem is no big deal—it was a problem in a textbook that I found in a bookstore here.[1]

After I'd finished that problem, I looked on the Internet and found that there are several ways to do it: some quick, and some longer but more elegant. One of the quick ways had occurred to me almost immediately upon reading the problem, but I'd then allowed myself to get sidetracked. As a result, I foolishly spent an unconscionable amount of time on another approach—also given on the Internet—whose key idea I never quite managed to perceive. Eventually I admitted to myself that I was getting nowhere, and gave my first idea a try. Much to my chagrin, I then solved the problem in about three minutes.

As the Germans say, "We grow too soon old and too late smart."

However, the time I'd spent on an idea that was beyond my abilities was not without reward: it gave me an idea for a string sculpture, which is something I'd never even imagined doing before. In my mind's eye, the sculpture looked like the designs on the cover, except that the strings glowed like laser lights as they spiraled upward from a common origin, reuniting and separating repeatedly.

My execution of that idea wasn't a work of such ethereal beauty. Some sort of framework was necessary for the sculpture, and the only thing I could think of was to use threaded steel rods and acrylic sheets, which gave the sculpture an unfortunate "industrial" aspect. However, one of my students perceived the beauties of the mathematics despite my artistically uninspired expression of them, and decided to make a similar sculpture himself.

It's the occasional experience like this one that makes learning and tutoring math a pleasure for me. Especially to students who have their doubts that it's worthwhile, but have decided to put their noses to the grindstone and make the best of it. Remember that I, too, was once a schoolchild struggling to make sense of square roots and long division. Like my students, I was trying to make good grades to receive the approval of teachers and parents, trusting—sometimes against my better judgment—in their assurances that the effort would one day pay off. The whole competitive routine of grades and tests and contests sometimes turned math into something that I'd really rather not have been doing. It wasn't until the summer between my junior and senior years of high school that my eyes were opened to its real wonders and beauties[2].

It didn't matter that most of them were, and would remain, beyond my understanding. I knew they existed, and the experience of becoming acquainted with them for the first time is recreated for me every time I see a student lift his or her nose from the grindstone, with eyes shining.

Now in good conscience, I can't end this essay that way because I know that reality will soon slam their noses back down on that grindstone. The education system in Chiapas is thoroughly corrupt, including the process of admission to universities and graduate studies. Therefore, I can't bring myself to tell students that their ability in math will bring them wonderful, fulfilling careers. Mere ability won't be enough for a student without family connections who's too poor to pay bribes or too moral to cheat on exams. Or in some cases, to sleep with teachers. The student whose eyes shone at seeing the beauties of mathematics for the first time will probably end up with broken dreams. However, I know that his or her joy at seeing math turn from drudgery to marvel is real, and that to experience it anew, all he or she will have to do is show a child a treasure like Fermat's Little Theorem.

San Cristóbal de Las Casas, 18 November 2006

---

1. I. N. Herstein, Álgebra moderna: grupos, anillos, campos, teoría de Galois, 2a edición, México: Trillas, 3a reimpresión, 1999 (Biblioteca de matemática superior). ISBN 968-24-3965-5. Translation of Topics in Algebra. I purchased it in Librería Soluna.

2. This was at the Summer Institute in Mathematics 1973, held at the University of Wisconsin at La Crosse. Our instructors were Professors David Bange, Tony Barkauskus, and Manmohan S. Aurora.