Math 5330 Notes
Spring 2009 **Introduction**

What is Number Theory?

Some time ago, I was working on the following strange problem: When is $\dfrac{(1-x^m)(1-x^n)}{(1-x^a)(1-x^b)}$ a polynomial in which every term is nonnegative? This was, in fact, just a small part of a bigger problem: When is $\dfrac{(1-x^{n_1})(1-x^{n_2})\cdots(1-x^{n_k})}{(1-x^{m_1})(1-x^{m_2})\cdots(1-x^{m_k})}$ a polynomial with nonnegative coefficients? I knew how do k = 1: $\dfrac{1-x^n}{1-x^m}$ is a polynomial with nonnegative coefficients exactly when n is divisible by m. For example,

$$\frac{1-x^{15}}{1-x^5} = 1 + x^5 + x^{10}.$$

I figured that in order to understand the general case, I had better understand what happens when $k = 2$. That leads back to $\dfrac{(1-x^m)(1-x^n)}{(1-x^a)(1-x^b)}$.

I should point out that this is NOT a number theory question, but number theory came up in looking at it. This is what I found for $\dfrac{(1-x^m)(1-x^n)}{(1-x^a)(1-x^b)}$. First, if m is divisible by a and n is divisible by b, then the expression is a nonnegative polynomial. For example,

$$\frac{(1-x^{15})(1-x^{28})}{(1-x^5)(1-x^7)} = (1 + x^5 + x^{10})(1 + x^7 + x^{14} + x^{21}).$$

However, there are other cases where the expression could be a nonnegative polynomial. Interesting are

$$\frac{(1-x^{35})(1-x^{12})}{(1-x^5)(1-x^7)} = 1 + x^5 + x^7 + x^{10} + x^{14} + x^{15} + x^{20} + x^{21} + x^{28} + x^{30} + x^{35}$$

and

$$\frac{(1-x^{35})(1-x^{13})}{(1-x^5)(1-x^7)} = 1 + x^5 + x^7 + x^{10} + x^{12} - x^{13} + x^{14} + x^{15} + x^{17} - x^{18}$$
$$+ x^{19} + x^{21} + x^{22} - x^{23} + x^{24} + x^{26} + x^{29} + x^{31} + x^{36}.$$

What makes 12 work but not 13? It turns out that what is special is that 12 = 5 + 7. More to the point, $5x + 7y = 12$ has a solution in nonnegative integers, but $5x + 7y = 13$ does not. Here is an example to show why this is important:

$5x + 7y = 29$ has a solution in nonnegative integers: $x = 3$, $y = 2$. Because of this,

$$1 - x^{29} = 1 - x^{5\cdot 3 + 7\cdot 2} = 1 - x^{15} + x^{15} - x^{29} = (1 - x^{15}) + x^{15}(1 - x^{14}).$$

Consequently,

$$\frac{(1-x^{35})(1-x^{29})}{(1-x^5)(1-x^7)} = \frac{(1-x^{35})(1-x^{15})}{(1-x^5)(1-x^7)} + x^{15}\,\frac{(1-x^{35})(1-x^{14})}{(1-x^5)(1-x^7)}$$
$$= \frac{1-x^{15}}{1-x^5}\,\frac{1-x^{35}}{1-x^7} + x^{15}\,\frac{1-x^{35}}{1-x^5}\,\frac{1-x^{14}}{1-x^7}$$

$$= (1 + x^5 + x^{10})(1 + x^7 + x^{14} + x^{21} + x^{28})$$
$$+ x^{15}(1 + x^5 + x^{10} + x^{15} + x^{20} + x^{25} + x^{30})(1 + x^7)$$

which will have nonnegative coefficients. In general, we have

Theorem. $\dfrac{(1-x^m)(1-x^n)}{(1-x^a)(1-x^b)}$ will be a nonegative polynomial exactly when one of the following conditions is met:

1) m is divisible by a or b and n is divisible by the other

or

2) one of the numbers m, n say m is divisible by both a and b, and there is a solution in nonnegative integers to $ax + by = n$.

I won't prove this theorem (although it is not hard) and I will not refer to it again in the course (except for this set of notes). What interests me here is the equation

$$ax + by = n.$$

Asking for **integer** solutions to this, or as above, **nonnegative integer** solutions, is a completely different type of problem than what we encountered in previous classes, where we were interested in all **real** solutions.

Here is a related question: For which n does there exist a solution in nonnegative integers to $5x + 7y = n$? Here are two possible reasons for investigating this question:

1) The answer will tell us which expressions of the form $\frac{(1 - x^{35})(1 - x^n)}{(1 - x^5)(1 - x^7)}$ are nonnegative polynomials.

2) Dumber but less exotic: Suppose you live in a country with only 5 and 7 dollar bills. What prices, n, of products can be purchased?

Here is a partial list of possible n's:

$$0,\ 5,\ 7,\ 10,\ 12,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21,\ 22,\ 24,\ 25,\ 26,\ 27,\ 28,\ 29,\ 30,\ \cdots.$$

It turns out that every number from 24 on has solutions to (1), (2) above.

So what is number theory? Roughly speaking, number theory is that branch of mathematics that deals with questions about integers (and sometimes rational numbers.) What is nice about number theory is that it is often easy to formulate questions about how things might work. What is not so nice is that some of these questions are very hard to answer! Here are some typical questions in number theory:

A **prime** number is an integer $p > 1$ which has only itself and 1 as divisors.

1) How many prime numbers are there?
2) How are they arranged?

A **perfect** number is one whose divisors sum to twice its value. For example, 28 has divisors 1, 2, 4, 7, 14, 28 and $1 + 2 + 4 + 7 + 14 + 28 = 56 = 2\cdot 28$, so 28 is a perfect number. Here are the oldest unanswered questions in all of mathematics:

3) How many perfect numbers are there?
4) Are all perfect numbers even?

These questions date back about 3000 years.

The most famous question in all of mathematics, called **Fermat's Last Theorem** stated that

5) $x^n + y^n = z^n$ has no solutions (x, y, z) in positive integers if $n \geq 3$.

This was a problem without a proof for over 300 years until Andrew Wiles gave a proof in 1995.

Not as old but still unproven is **Goldbach's Conjecture**:

6) Every even number larger than 2 can be written as a sum of two primes.

This question is only about 250 years old, as is the variant

7) Every odd number larger than 5 can be written as the sum of three primes.

(7) is proven **IF** you believe something called the **Extended Riemann Hypothesis**.