Math T480: Elementary Number Theory

Darij Grinberg (darijgrinberg@gmail.com / darij.grinberg@drexel.edu)

An announcement

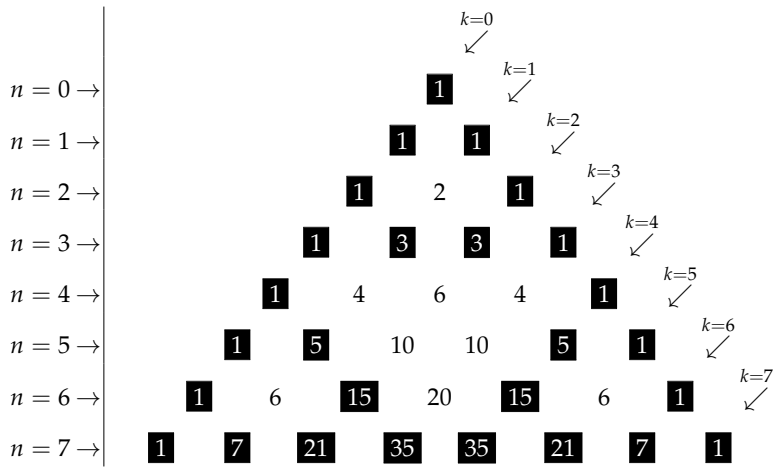
Number theory is the study of integers for no particular purpose. One of the oldest branches of mathematics, it has nevertheless been sidelined from the standard undergraduate curriculum in favor of supposedly more general, more useful or more abstract topics. Yet, very little in elementary number theory follows directly from abstract algebra; quite a few things have unexpected applications; and abstraction is hardly an aim to itself.

The course I plan to teach this Spring is **an undergraduate-level introduction to elementary number theory**, focussing on some of the most beautiful results and a few more modern developments. Its only prerequisite is Math 220 (Introduction to Proof). Familiarity with combinatorics or abstract algebra is welcome but not required. If you enjoyed Math 222 or Math 235, you will probably like this class. Topics include prime numbers, modular arithmetic, quadratic remainders, congruences (Euler, Fermat, Lucas, etc.) and representations of integers as sums of squares. We will follow David M. Burton's *Elementary Number Theory* (7th edition, 2011) for the standard topics, but notes will be posted on the website.

The course is planned to meet on **Monday and Wednesdays from 12:00 pm to 01:50 pm**.

Here are a few questions we will see answered in this course:

- Start with Pascal's triangle and color each odd entry black and each even entry white. Why are you seeing a fractal (a finite approximation, to be precise)?



- Relatedly, the binomial coefficients $\binom{2n}{2k}$ and $\binom{n}{k}$ always leave the same remainder when divided by 2. What about dividing by 4 ? By 8 ? What about the remainders of $\binom{pn}{pk}$ and $\binom{n}{k}$ when divided by p (for some prime number $p > 2$) ? by p^2 ? by p^3 ? How high can we go with this?

- Why is there always a prime number between n and $2n$ when n is a positive integer? And what does this have to do with binomial coefficients?

- Why is every nonnegative integer a sum of four perfect squares (e.g., $21 = 4^2 + 2^2 + 1^2 + 0^2$ and $19 = 4^2 + 1^2 + 1^2 + 1^2$)? Which integers are sums of two perfect squares? Which are sums of three perfect squares?[1] In how many ways can n be written as a sum of two squares?

- The product of k consecutive integers is always divisible by the product of the first k positive integers (that is, by $1 \cdot 2 \cdot \cdots \cdot k = k!$). This surprising-looking fact becomes less surprising once we realize that the ratio in question is a binomial coefficient:

$$\frac{n\,(n-1)\,(n-2)\cdots(n-k+1)}{k!} = \binom{n}{k},$$

known to be an integer because it counts k-element subsets of $\{1, 2, \ldots, n\}$.

However, stranger things are true. The product of the **pairwise differences** of k arbitrary(!) integers is always divisible by the product of the pairwise differences of the first k positive integers. For example, for $k = 4$, this is saying that

$(a-b)\,(a-c)\,(a-d)\,(b-c)\,(b-d)\,(c-d)$ is always divisible by $(1-2)\,(1-3)\,(1-4)\,(2-3)\,(2-4)\,(3-4) = 12$.

Why is this true?

What if we take the differences of the squares of the integers instead? What about the differences of the cubes? Do we ever run out of luck?

What is special about $1, 2, \ldots, k$ here? And where is this really coming from?[2]

[1] We won't actually answer this one. It's much harder than the two-squares and four-squares questions.

[2] There are several valid answers to this one; I hope to explain a connection to *phylogenetic trees*.