Course summary for Math 301A, Spring 2014

- Division algorithm
  - If n is an integer, and m is an integer, then there exist integers a and r, with $0 \leq r < m$, and $n = am + r$.
- Divisibility
  - If a and b are integers, a nonzero, and there exists an integer k such that $b = ak$, then we say a *divides* b.
  - Lots of nice little theorems about divisibility (e.g., divisibility is transitive).
- Infinitude of primes
  - You should know this proof by heart!
- GCD and the Euclidean algorithm
  - A big fact is that if d is the GCD of a and b, then there are integers m and n such that $d = am + bn$ (i.e., the GCD of two numbers can be written as a linear combination of them).
- Unique factorization (Fundamental Theorem of Arithmetic)
  - Every positive integer greater than one can be expressed in the form $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where the p_i are prime, and the α_i are positive integers; AND if we require $p_1 < p_2 \cdots < p_k$, then this representation if unique.
- Irrational numbers exist!
  - $\sqrt{2}$ (in fact, the square root of any integer that is not a square), $\frac{\ln 2}{\ln 3}$
- Arithmetic functions: τ, σ, and ϕ
  - $\tau(n) =$ the number of divisors of $n = \displaystyle\sum_{d|n} 1 = \prod_{p^\alpha || n} (\alpha + 1)$
  - $\sigma(n) =$ the sum of the divisors of $n = \displaystyle\sum_{d|n} d = \prod_{p^\alpha || n} \frac{p^{\alpha+1} - 1}{p - 1}$
  - $\phi(n) = \#\{0 < m < n : (m, n) = 1\} = \displaystyle\prod_{p^\alpha || n} \left(1 - \frac{1}{p}\right)$
- Congruences and modular arithmetic
  - If $m|(a - b)$, then $a \equiv b \pmod{m}$, and all that goes with it.
- Solving linear modular equations (i.e., $ax \equiv b \pmod{m}$)

- $Ax \equiv A \pmod{A}$ is your friend.

- Solving systems of congruences in one variable
  - The Chinese Remainder Theorem tells us that a system of congruences of the form $x \equiv a \pmod{m}$ has a unique solution modulo the product of the moduli provided the moduli are pairwise relatively prime.

- Euler's theorem and primitive roots
  - Euler's theorem: $a^{\phi(n)} \equiv 1 \pmod{n}$ if $(a, n) = 1$.
  - If the smallest $m > 0$ such that $a^m \equiv 1 \pmod{n}$ is $\phi(n)$, then a is a primitive root.

- Digit stuff
  - Find the last so many digits of something raised to a big power.
  - Zeros of $n!$ in this base or that
  - Digit-based tests for divisibility

- Linear diophantine equations
  - The equation $ax + by = c$ has solutions iff $(a, b)|c$.

- Frobenius coin problem
  - We've got one theorem: if the coin values are a and b, then $ab - a - b$ is the largest sum you cannot express with those coins.

- Pythagorean triples
  - There are infinitely many triples, and we can parametrize the primitive ones (a, b, c) by
  $$a = 2mn, \ b = m^2 - n^2, \ c = m^2 + n^2$$
  with $m, n > 0$, $(m, n) = 1$.

- Method of Descent
  - Applicable to equations like $x^4 + y^4 = z^2$ and $2x^2 + 3y^2 = z^2$.

- Sequences
  - Limit of ratio of consecutive terms of sequence defined by a recurrence relation.
  - Generating functions