List of Topics for the Final

Final will be, with one exception, Closed book: no textbook, no notes, no cooperation. Electronic means of communication (cell phones, smartphones, tablet pc, laptops, etc) will be forbidden. The exception is as follows: you are **allowed to bring** and use during entire exam **one sheet** of A4/lettersize paper filled on one side with your handwriting.

For the final, you need to know notions, methods, statements and their proofs in the list below. In particular, you need to able to reproduce (of course, not necessarily word by word, but correctly) definitions, statements and proofs; know basic examples of definitions and theorems; be able to apply theorems, ideas in their proofs, and methods in the list below to solve problems.

This list is mainly a union of the corresponding lists for the four midterms (order is slightly different). Items labeled by
• appeared on the list for some midterm; those labeled by
◦ were included in some midterm material but didn't get a separate mention just then (or were worded differently); those labeled by
◇ were never included in any midterm.

Please, see also a disclaimer after the list of topics. It's about how names and titles of topics in this list relate to actual contents of the course.

There may be changes to this list, but no later than May 2nd.

(1) *Preliminaries and early number theory.*
- Binomial coefficients, Pascal's triangle.
- Mathematical induction.
- Polygonal numbers (triangular, oblong, square, m-gonal): definition, basic properties, simple "picture proofs".
- Method of finite differences. Connection to Pascal's triangle.
- Method of indeterminate coefficients.
- Finding sum of values of a polynomial at integer points $1, 2, \ldots, n$ (for example $1^2 + 2^2 + \ldots + n^2$).

(2) *Divisibility of integers: basic facts.*
- Division algorithm.
- Representing integers in arbitrary base. Converting to and from arbitrary base. Multiplication table, long addition and long multiplication in arbitrary base.
- Definition and basic properties of divisibility.
- Greatest common divisor: definition, basic properties, Bezout's theorem (linear expression of gcd), Euclid's lemma. Bezout's theorem for multiple numbers.

(3) *Primes.*
- Definition of prime and composite numbers.
- Fundamental theorem of arithmetic (Unique prime factorization for integers).
- ◦ Canonical (prime power) form of integers, deciding divisibility and finding gcd and lcm (the least common multiple) using canonical form.
- Infinitude of primes: Euclid's proof, Euler's proof. Infinitude of primes of the form $4k + 3$.
- Sieve or Eratosthenes.

- No integer polynomial that takes only prime values.

(4) *Linear Diophantine equations.*
- Finding gcd via Euclidean algorithm.
- Finding linear expression of gcd via reverse Euclidean algorithm.
- Notion of a Diophantine equation.
- Solving a linear Diophantine equation in two variables.

(5) *Congruences.*
- Definition of congruence modulo n. Basic properties of congruence.
- Tests for divisibility by 2, 3, 5, 9, 10, 11, 2^k and 5^k (the last one is optional, although it's no different from 2^k).
- Tests for divisibility by 7, 11, 13.
- Canceling out a factor in a congruence. Coprime and not coprime cases.
- Solving a single linear congruence. Number of solutions of a single linear congruence.
- Chinese remainder theorem, relation to solving multiple linear congruences with coprime bases.
- ∘ Solving a system of linear congruences using CRT.

(6) *Fermat's theorem and related questions.*
- Fermat's little theorem.
- Converse statement to Fermat's theorem: notion of an absolute pseudoprime, existence of (at least one) absolute pseudoprime.
- Wilson's theorem.

(7) *Number-theoretic functions.*
- Notion of a number-theoretic function. Number of divisors τ and sum of divisors σ. Expression of τ and σ using canonical form of an integer.
- Multiplicative number-theoretic functions. Basic examples: ε, $\mathbf{1}$, n. Multiplicativity of τ and σ.
- Dirichlet product $*$. Connection of Dirichlet product to multiplication of Dirichlet series.
- Sum of values of a function f at divisors of n as $f * \mathbf{1}$. Multiplicativity of $f * \mathbf{1}$, of $f * g$.
- Möbius function μ: definition, multiplicativity. Main property $\mu * \mathbf{1} = \varepsilon$.
- Möbius inversion formula. Multiplicativity of f given multiplicativity of $f * \mathbf{1}$.

(8) *Euler's function. Euler's theorem.*
- Euler's function φ: definition, two proofs of multiplicativity.
- Expression of $\varphi(n)$ through prime decomposition of n. Expression of φ through Möbius function.
- Euler's theorem (two proofs).

(9) *Quadratic congruences modulo prime p.*
- Reduction of a quadratic congruence mod odd prime p to a congruence of the form $x^2 \equiv a \pmod{p}$.
- Quadratic residues and nonresidues, Euler's criterion.
- Legendre symbol, basic properties of Legendre symbol. Finding $\left(\frac{-1}{p}\right)$. Infinitely many primes of the form $4k+1$.

- Reduction of computing $\left(\frac{n}{p}\right)$ to prime numerators $\left(\frac{q}{p}\right)$.
- Gauss's Lemma. Reformulation of Gauss's Lemma using the integer part function (a.k.a. the greatest integer function, or the floor function).
- Corollaries of Gauss's Lemma: finding $\left(\frac{2}{p}\right)$, infinitely many primes of the form $8k-1$.
- Quadratic Reciprocity Law. Using quadratic reciprocity law to compute arbitrary $\left(\frac{n}{p}\right)$ assuming availability of prime decompositions.

(10) *Quadratic congruences modulo composite n.*
- Hensel's lemma for x^2. Solving a congruence $x^2 \equiv a \pmod{p^k}$ for odd prime p, $k \geq 1$ and $\gcd(a,p)=1$.
- Solving a congruence $x^2 \equiv a \pmod{2^k}$ for odd a and $k \geq 1$.
- Solving a congruence $x^2 \equiv a \pmod{n}$ for arbitrary $n > 1$ and $\gcd(a,n)=1$.
  - Blum's remote coin flipping protocol, connection to the prime factorization problem.

(11) *Primitive roots.*
- Order of a number modulo n. Order of a power and other properties of order.
  - Primitive roots: definition, basic properties.
  - Lagrange theorem. Existence of primitive roots modulo prime p. Quantity of primitive roots if at least one exists.
    - Using primitive roots to solve congruences of the form $x^k \equiv a \pmod{n}$ if n possesses a primitive root and $\gcd(a,n)=1$.

(12) *Continued fractions.*
- Continued fractions: definition of infinite and finite continued fractions, simple fractions, periodic fractions. Convergents C_k of a continued fraction.
- Numerators p_k and denominators q_k of convergents, recursive formulas for p_k, q_k. Main technical lemma connecting $p_k, p_{k-1}, q_k, q_{k-1}$.
- Existence of value (limit of convergents) of an infinite continued fraction.
  - A number is rational iff it is a value of a finite continued fraction.
  - A number is irrational iff it is a value of an infinite continued fraction. Representing a given irrational number by an infinite continued fraction. Uniqueness of infinite continued fraction with a given value.
- Convergents as approximations of value of a continued fraction. "Quadratic" error of approximation by convergents.
- Periodic infinite continued fractions represent quadratic irrationalities.
- Quadratic irrationalities are represented by infinite periodic continued fractions (no proof required).
    - Geometric (grid paper) interpretation of convergents of a continued fraction (no proof required).

(13) *Application of number theory to cryptography.*
    - Diffie–Hellman key exchange protocol, connection to the discrete log problem.
    - RSA (Rivest–Shamir–Adleman) public key cryptosystem, connection to the prime factorization problem.

(Please see next page for a disclaimer.)

Disclaimer.

Sometimes different things have the same (or very similar) names. The terms and notation in the list above refer to *things relevant to this course*. Knowlegde of other topics that have the same names, *by itself*, will not earn you any points on the final. Instead of the list above, I could give painfully detailed descriptions of each topic to avoid any misinterpretation. I am not doing this. One reason is that I want to keep this list reasonably readable; another (perhaps, more substantial) reason is that one of points of taking any math course is to be able to recognize and understand silent conventions that are implied in a math text.

This is a somewhat vague statement, so here is a number of examples to make it hopefully more clear. And in any case, if, when studying, you are unsure whether something specific is on final, do not hesitate to ask me.

- Suppose, on exam in History of British Literature you are asked to write a brief biography of Conan Doyle. If you cite exciting exploits of a successful present-day Irish rugby player Conan Doyle and skip prominent writer Conan Doyle, that will probably merit you 0 for this question, despite the fact that you wrote about someone named Conan Doyle. (And vice versa, in a course on present-day Irish Rugby, should there exist such a thing, writer Conan Doyle would be of no relevance.)
- In the same spirit, for example, τ in the list above refers specifically to the number of divisors function. So, for example, if you are asked on the final to give a definition and a basic formula to compute τ, the answer

  > "τ is torsion of a curve α, and can be computed as $\tau = (\alpha' \times \alpha'') \cdot \alpha'''/\|\alpha' \times \alpha''\|^2$."

  will merit you 0 despite the fact this is a (mostly) correct statement about torsion. Similarly,

  > "τ is Ramanujan's tau-function, defined through weight 12 modular form Δ"

  will also give you 0 points, despite the fact that this is (somewhat) correct *and* about number theory.
- I would like to emphasize that irrelevant knowledge is worth nothing in terms of your grade only *by itself*. If you somehow manage to actually use things not covered in class (or arbitrary things that have no immediate relation to the course) to correctly solve problems given on the final, you will be credited, depending on how self-contained your argument is.

  For example, if you are asked to prove infinitude of primes of the form $4k + 3$ and you use some amazing argument involving curves in $\mathbb{R}^3$ and their curvatures and torsions, you may get full credit (if your argument is correct and does not involve any statements that are actually hard). On the other hand, text

  > "This follows immediately from Dirichlet's theorem."

  gives you 0 because it uses a very strong and difficult theorem not proven in class to prove a simple statement that can be easily derived by techniques covered in class.

P.S. Sorry if my mention of torsion brings up painful memories.