Math 211

Term 1 Review

Note: See the overheads on the web site for a more detailed summary of each topic.

Chapter 1: Integers

– divisibility, gcd (definitions, properties)

– the division algorithm (definition of $\mathrm{rem}(a, m)$ and of $\mathrm{quot}(a, m)$)

– the (extended) Euclidean algorithm

– the GCD-criterion, Euclid's Lemma (2 versions)

– finding the general solution of a linear Diophantine equation (2 or 3 variables), solving linear Diophantine equations with contraints (2 or 3 variables)

– prime numbers, the Unique Factorization Theorem ($\rightarrow \mathrm{expt}_p(n)$)

– applications: proving irrationality, GCD-formula

Chapter 2: Modular Arithmetic

– congruences: $a \equiv b \pmod{m}$ (definition, computational rules)

– computing $\mathrm{rem}(a^n, m)$ via the power-mod algorithm

– the cancellation law

– solving the congruence equation $ax \equiv b \pmod{m}$

– the ring $\mathbb{Z}/m\mathbb{Z}$ and the field $\mathbb{F}_p$

– the Chinese Remainder Theorem

– Fermat's Theorem (and Corollaries 1,2,3); application to computing $\mathrm{rem}(a^n, p)$, etc.

– PK Cryptography and the RSA Method (not on the exam)

Chapter 3: Polynomials

– complex numbers: basic operations, complex conjugate $\overline{z}$, absolute value $|z|$, polar form, De Moivre's formula, solving $z^n = a$

– polynomials: basic operations, degree

– the division algorithm (for polynomials), $\mathrm{rem}(f, g)$, $\mathrm{quot}(f, g)$

– the Remainder Theorem, Factor Theorem, substitution method (for finding $\mathrm{rem}(f, g)$)

– the (extended) Euclidean algorithm, gcd (for polynomials)

– the GCD-criterion, Euclid's Lemma (for polynomials)

– irreducible polynomials (definition, properties), quadratic formula

– the Unique Factorization Theorem for $F[X] \to \mathrm{expt}_p(f)$, multiplicity of a root, GCD-formula (for polynomials)

– Factoring Methods over $\mathbb{Q}$: Rational Root Test, Gauss's Lemma, Modular Test

– Fundamental Theorem of Algebra, the Factorization Theorem for $\mathbb{C}[X]$

– the Factorization Theorem for $\mathbb{R}[X]$, application to factorization methods