P. means that the proof is also required.
Fx.y refers to chapter x.y of the book Freud-Gyarmati: Number theory
L refers to a link on the page of the class (`https://math.bme.hu/~merdelyi/nt`)

1. **Pythagorean triples and Fermat's last theorem.**
   Pythagorean triples, primitivity. **P**. Characterization of Pythagorean triples (F7.2).
   Statement of Fermat's last theorem, **P**. proof of the case $n = 4$ (F7.7).

2. **Gaussian integers and Euclidean domains.**
   Definition of domains, units, divisibilty, gcd, norm, euclidean domains, gcd, irreducibles, primes. Unique factorization theorem. **P**. Division with remainder in $\mathbb{Z}[i]$. **P**. Characterization of Gaussian primes (F7.4).

3. **Representation of integers as sum of squares.**
   Definition of $r_k(n)$. **P**. Sum of two squares theorem (F7.5). Sum of three squares theorem.
   P. Minkowski's theorem on lattices (L). **P**. sum of four squares theorem (L).

4. **Primitive roots and quadratic residues.**
   Definition and properties of the order modulo m. Primitive roots, **P**. Existence of primitive roots modulo a prime, discrete logarithm (F3.2-4). Definition and properties of quadratic residues. Legendre and Jacobi symbol and **P**. the evaluation of them. Quadratic reciprocity (F4.1-3).

5. **Cryptography.**
   Definition of symmetric and public key protocols. The RSA and ElGamal cryptosystems, public and private keys, encrypting and decrypting functions. **P** the decryption works (F5.8). Attacks on the RSA: the primes are too close and Wiener's attack (L).