CS503
2023 Fall
Professor Alexander Ushakov

| |
|---|
| Divisibility. GCD. Congruences. |
| Units. Euler function. CRT. RSA. |
| Primality testing. Factorization problem. |
| Groups. Primitive elements. |
| DLP. DH. ElGamal. Algorithms for DLP. |
| Quadratic congruences. |
| Abelian groups. |
| Rings. Polynomials. Fields. |
| Classification of finite fields. |
| More on finite fields. Applications. |
| Elliptic curves. |
| ECDLP. ECC. |