Computational Complexity

Easy problems with prime numbers

- Generating a prime number p
- Addition, multiplication, exponentiation
- Inversion, solving linear equations

Hard problem with prime numbers

• Factoring primes e.g. given n find p and q such that $n = p \cdot q$

RSA - generating the key pair

- 1. Pick p and q two large prime numbers and calculate $n = p \cdot q$ (see primality tests)
- 2. Compute z = (p-1).(q-1)
- 3. Pick a prime number e < z such that e and z are relative primes
- → (e,n) is the public key
- 4. Solve the linear equation $e * d = 1 \pmod{z}$ to find d
- → (d,n) is the **private key**however p and q must be kept secret too