

Number Theory - Prime numbers

Prime Numbers

- p is prime if 1 and p are its only divisors e.g 3, 5, 7, 11 ...
 - p and q are relatively prime (a.k.a. coprime) if $\gcd(p,q) = 1$
e.g $\gcd(4,5) = 1$
- ➔ There are infinitely many primes

Euler-Fermat Theorem

If $n = p \cdot q$ and $z = (p-1) \cdot (q-1)$

and a such that a and n are relative primes

Then $a^z \equiv 1 \pmod{n}$

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 $n = p \cdot q$