**Divisibility Operations**

**Document Id 29**

Divisibility with Objects Partitioning

Dividing a sequence into subsequences

Divisibility with Numbers ⇒ number theory

1. GCD Euclid's algorithm

https://en.wikipedia.org/wiki/Euclidean\_algorithm

1. Prime test
2. Applications

**Applications**

Machine ⇒ parts ⇒composites

Taking a part and multiplying it by a prime, your can reduce the harmionics

caused by vibration.

Microwave grill ⇒ the cross beams are set at prime distances

⇒ eliminate arcing.

Cryptography ⇒ number theory => primes

* Prime numbers have the unique property in that they have

exactly two factors: 1 and themselves.

* public-key cryptography

https://en.wikipedia.org/wiki/RSA\_(cryptosystem)

public key = product of two large primes

secret key = the 2 prime factors of the public key

If you multiply two large prime numbers, you get a huge non-prime

number with only two (large) prime factors.

To break the key you use Prime decomposition

<https://en.wikipedia.org/wiki/Integer_factorization#Prime_decomposition>

Strongest method in practice we use gcd as part of the algorithm

<https://en.wikipedia.org/wiki/Euler%27s_factorization_method>

gcd(360,756)=36

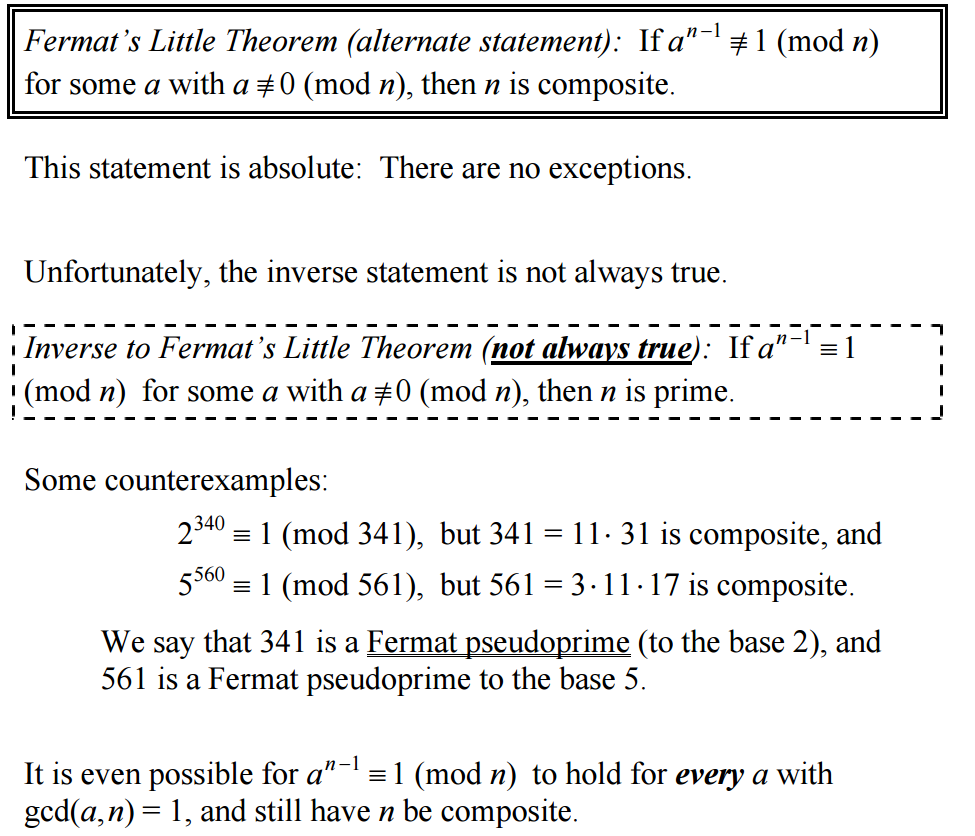
360/756=10/21.

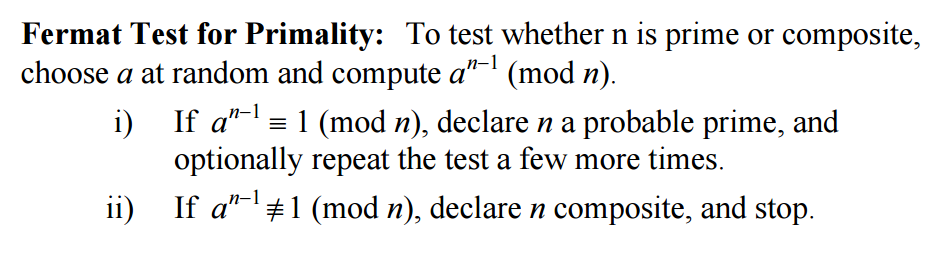
prime factorization

360=23×32×5 and 756=22×33×7.

gcd( a, n) = 1

Divisibility





Euler's method is expensive

https://en.wikipedia.org/wiki/Miller%E2%80%93Rabin\_primality\_test

