Een priemgetal is een natuurlijk getal groter dan 1 dat slechts deelbaar is door 1 en door zichzelf.

3 soorten methodes om te kijken of een getal priem is.
→ naieve methodes => aflopen van alle kleinere getallen en kijken of het een deler is, traag maar zeker
→ probablistische methodes => met een zekere zekerheid vaststellen
→ determinitisch => beide combineren, zeker zijn dat een getal priem is, en sneller nakijken

naieve methodes → kleinere getallen aflopen, eenvoudig & zeker maar traag
→ eerste manier => alle kleinere getallen aflopen => is dit wel nodig?
→ tweede manier => neen dit is niet nodig we moeten maar tot aan de wortel lopen als deler > wortel dan is het quotient < wortel , als de deler een gehele deler is, dan zou het quotiënt ook een moeten zijn en zouden we deze dus al moeten gevonden hebben.
→ derde manier => kan dit nog beter? Ja door enkel te testen op kleinere priemgetallen.
Vergelijkbaar met zeef van eratosthenes:

> Zeef van eratosthenes => onderaan beginnen en alle gevonden priemgetallen bijhouden.
> Veelvouden van priemgetallen schrappen.

Hier veelvouden schappen => vervangen door priemgetallen bijhouden en deze aflopen bij een volgend getal.

Probabilistische tests → waarschijnlijkpriem, niet zeker
→ Een getal dat priem is zal altijd als priem gevonden worden, de redenering werkt echter maar in een richting. Een samengesteld getal kan soms ook als priem gemeld worden.

> Wat is een samengesteld getal? => Een samengesteld getal is een positief geheel getal dat minstens 2x door een priemgetal is te delen bv 15 = 3 x 5 of 1332 = 2x2x3x3x37. In andere woorden een geheel positief getal dat geen priemgetal is , is een samengesteld getal.

Er is dus sprake van valse positieven, wat verklaart waarom de test niet met 100% zekerheid kan zeggen dat een getal priem is.
Oplossen door in het begin van de tests een aantal willekeurige waarden a te kiezen. De kans kan dan verkleind worden door een probabilistische test uit te voeren met de waarden a. Hoe meer a waarden we kiezen, hoe kleiner de kans op een vals positief.
De structuur van een probabilistische test is dus:
1. kies aantal waarden a
2. controleer een bepaalde gelijkheid, afhankelijk van het gebruikte algoritme. Als deze gelijkheid niet geld dan is het getal samengesteld en dus niet priem. A is dan de GETUIGE van het feit dat n samengesteld is.
3. herhalen vanaf stap 1 tot we een getuige hebben, of de vereiste zekerheid is bereikt.

→ Deze methode is sneller dan de naieve methodes, maar we hebben geen 100% zekerheid dat een getal priem is.

De probabilistische tests die ik zal bespreken is de priemtest van fermat. Deze wordt gebruikt voor rsa encryptie. Daarna zal benjamin de Miller-Rabin test bespreken. Om af te sluitel zal benjamin ook de determinische tests uitleggen.

Priemtest van fermat => gebaseerd op de kleine stelling van fermat (fermat's little theorem):
Als p een priemgetal is, dan geldt:
$a^p \equiv a \pmod p$ <=> a^(p-1) ≡ 1 mod p
De tweede vorm is enkel geldig als a & p relatief priem zijn, wat wil zeggen dat ze geen gemeenschappelijke delers hebben. (voorbeeld 8 en 15 zijn relatief priem) Dit komt doordat beide leden van de gelijkheid gedeeld moeten worden door a. Als a een veelvoud is van p dan is de rest en dus het linkerlid = 0 , dit zou enkel kunnen als a = 0, maar dan delen we door 0.

Bewijs van deze stelling:
stel getal a, positief en niet deelbaar door getal p.
Als we reeks veelvouden opschrijven van a:

a,2a,3a, …. , (p-1)a

En we vervolgens voor elk veelvoud enkel de rest overhouden , zal het resultaat een permutatie zijn van de getallenreeks:

1,2,3,4,5,6,... (p-1)

Als we in beide reeksen alle waarden vermenigvuldigen, moeten deze gelijk zijn op een veelvoud van p na:

a*2a*3a*4a*...*(p-1)a ≡ 1*2*3*4*5*...*(p-1) (mod p)

Dit kunnen we schrijven als

a^(p-1) (p-1)! ≡ (p-1)! (mod p)

We kunnen (p-1)! wegdelen , dan krijgen we:

a^(p-1) ≡ 1 (mod p)

In dit bewijs zijn er 2 creatieve overgangen :

→ De eerste overgang, is dat wel een permutatie ?
→ mogen we (p-1)! Zomaar wegdelen?

De eerste overgang; is dit een permutatie?

Eerst en vooral geen van de veelvouden a => a(p-1) kan rest 0 krijgen doordat al deze nummers relaties priem zijn met k (gegeven, a is positief en niet deelbaar door p).

Hierdoor kunnen we Euclid's dilemma toepassen. Dit dilemma vertelt ons: doordat er geen getal gemeenschappelijke delers heeft met p, moetenwe alle getallen in de rest terug vinden. Dit dilemma kan bewezen worden.

De tweede overgang ; mogen we (p-1)! Zomaar weglaten?

ux ≡ uy (mod p)
<=> x ≡ y (mod p)

Dit kunnen we terug aantonen met euclid's dillema. Dit zegt dat als b een product r*s deelt, b een deler moet zijn van minstens een van beide factoren. Hierboven komt dat erop neer dat als p | ux -uy = u(x-y) , p een deler moet zijn van u. dus mogen we u wegdelen vermits het geen invloed zal hebben op de rest ervan.

getallen voorbeeld bewijs:

vb a=3, p=7

dan is de eerste reeks veelvouden:

3,6,9,12,15,18

rest na deling door 7

3,6,2,5,1,4

Dat is dus een permutatie van

1,2,3,4,5,6

Als we deze getallen vermenigvuldigen krijgen we:

$3*6*9*12*15*18 \equiv 3*6*2*5*1*4 \equiv 1*2*3*4*5*6 \pmod 7$

Vereenvoudigen geeft

$3^6 * (1*2*3*4*5*6) \equiv (1*2*3*4*5*6) \pmod 7$

$3^6 \equiv 1 \pmod 7$

voorbeeld fermats test:

is p = 221 priem?

→ we kiezen een waarde a ; a = 38:

$a^{(n-1)} \equiv 1 \pmod{221}$

$32^{220} \equiv 1 \pmod{221}$

Volgens a = 38 is p priem. Getal a kan wel een leugenaar zijn!

Dus proberen we met nog een andere waarde a = 26:

$26^{220} \equiv 169 \not\equiv 1 \pmod{221}$

We hebben een waarde a gevonden die kan aantonen dat 221 niet priem is , getal 38 was dus een leugenaar.

Klopt dit => dit klopt 221 = 13 * 17 en is dus een samengesteld getal.