1 density of prime numbers

prime number theorem $\lim_{n\to\infty} \frac{\phi(n)}{n/\ln n} = 1$.

one simple approach to the problem of testing for primality is **trialdivision**. we tyr dividing n by each integer 2,3,...,$[\sqrt{n}]$. this works well only when n is very small or happens to have a small prime factor.

2 pseudoprimality testing

let $\mathcal{Z}_n^+$ denote the nonzero elements of $\mathcal{Z}_n$, we say that n is a *base-a pseudoprime* if n is composite and

$$a^{n-1} \equiv 1 \ (mod\ n). \tag{1}$$

surprizingly, the conerse of Fermat's theorem *almost* holds.

Algorithm 1 pseudoprime(n)

if $2^{n-1} \not\equiv 1 \ (mod\ n)$. **then**
    return composite
elsereturn prime
end if

surprizingly, it rarely err. actually the error rate on a randomly chosen β-bit number goes to zero as $\beta \to \infty$. we cannot entirely eliminate all errors by simply checking for a second base number, because there exist composite integers n, *carmichael numbers*, that safisty equation for all $a \in \mathcal{Z}_n^*$.

3 the miller-rabin randomized primality test

let $n - 1 = 2^t u$ where $t \geq 1$ and u is odd, therefore $a^{n-1} \equiv (a^u)^{2^t}$

Algorithm 2 witness(a, n)

let t and u as defined above
$x_0 = a^u \bmod n$
for $i = 1 \to t$ **do**
    $x_i = x_{i-1}^2 \bmod n$
    if $x_i == 1$ and $x_{i-1} \neq 1$ and $x_{i-1} \neq n-1$ **then**
        return true
    end if
end for
if $x_t \neq 1$ **then**
    return true
end if
return false

we detect whether a nontrival square root of 1 is discovered, We now examine the Miller-Rabin primality test based on the use of WITNESS. Again, we assume that n is an odd integer greater than 2

Algorithm 3 miller-rabin(n, s)

for $j = 1 \to s$ **do**
    a = random(1, n - 1)
    if witness(a, n) **then**
        return composite
    end if
end for
return prime

4 error rate of miller-rabin primality test

theorem if n is an odd composite number, then the number of witnesses to the compositeness of n is at least $(n-1)/2$.

theorem the probability that miller-rabin(n, s) errs is at most 2^{-s}.

by applying bayesian theorem, we can estimate the error rate more percisely.