SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Publikasi Jurnal & Penelitian Teknik Informatika
Vol. 1 Nomor 1, Oktober 2016
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Membangkitkan Bilangan Prima Marsenne dengan metode Bilangan Prima Probabilistik Solovay – Strassen

Muhammad Khoiruddin Harahap
Politeknik Ganesha Medan
choir.harahap@yahoo.com

Abstrak — Bilangan Prima adalah bilangan yang bila difaktorkan hanya habis dibagi oleh angka 1 dan dengan dirinya sendiri. Dan lawan dari bilangan prima adalah bilangan komposit, yaitu bilangan habis dibagi oleh bilangan yang lain lebih dari 2. yang Keunikan bilangan prima membuatnya jadi kunci penting dalam keamanan data, terutama pada Kriptografi. Semakin besar jumlah digit bilangan prima, akan susah untuk difaktorkan. Solovay – Strassen merupakan metode pengujian bilangan prima yang sifatnya probabalistik. Yaitu perlu dilakukan pengujian berkali kali untukmendapatkan tingkat keakurasian. Dan Bilangan Mersenne adalah bilangan prima yang berasal dari pemangkatan bilangan 2 dipangkatan dengan prima – 1. Yang sifatnya juga masih probabilistik, sehingga harus diuji berkali kali. Dan bilangan prima Mersenne memudahkn untuk mendapatkan bilangan prima dengan jumlah digit yang besar. Dalam hal ini akan membangkitkan bilangan prima di atas 200 digit.

Keywords—Prima, Probabilistik, Mersenne, Uji prima, Solovay-Strassen

I. LATAR BELAKANG

Teori bilangan prima dengan berbagai metode, banyak yang dapat dipelajari, namun masih sebatas bilangan prima dengan jumlah digit yang sederhana (kecil) misalnya 2, 3, 5, 7, 11, 17, 23, 29 dan seterusnya Sehingga metode untuk mendapatkan bilangan prima yang besar perlu dikupas lagi. Data yang dilansir oleh http://primes.utm.edu/ mengeluarkan bilangan prima yang terbesar saat ini ditemukan oleh manusia adalah $\mathbf{2^{74207281}-1}$ dengan jumlah 22.338.618 digit.

II. LANDASAN TEORI

II.1. Bilangan Prima dan Bilangan Komposit

Bilangan Prima yaitu bilangan bulat positif yang lebih besar dari 1 dan hanya habis dibagi dirinya sendiri dan bilangan 1. Misalnya bilangan 2, 3, 5, 7, 11, 13, 17, 19 dan seterusnya. Dan bilangan komposit adalah bilangan bulat selain bilangan prima. Bilangan prima banyak dibutuhkan dalam bidang ilmu *Computer Security* seperti RSA (Rivest Shamir Adleman). Dimana semakin besar angka bilangan prima tersebut maka semakin susah untuk difaktorisasi.

Untuk menentukan keprimaan sebuah bilangan dapat dilakukan dengan memfaktor bilangan tersebut dan bila dapat difaktorkan dengan bilangan selain dirinya sendiri dan bilangan 1, maka bilangan tersebut bukanlah prima.

Contoh berikut ini :

Faktor dari 1 adalah 1; satu faktor
Faktor dari 2 adalah 1 dan 2; dua faktor
Faktor dari 3 adalah 1 dan 3; dua faktor
Faktor dari 4 adalah 1, 2, dan 4; tiga faktor
Faktor dari 5 adalah 1 dan 5; dua faktor
Faktor dari 6 adalah 1, 2, 3, dan 6; empat faktor
Faktor dari 7 adalah 1 dan 7; dua faktor
Faktor dari 8 adalah 1, 2, 4, dan 8; empat faktor
Faktor dari 9 adalah 1, 3, dan 9; tiga faktor

Berdasarkan hasil faktorisasi di atas, maka dapatlah diambil kesimpulan bahwa 2, 3, 5 dan 7 adalah bilangan prima, dan bilangan lainnya adalah komposit.

II.2.Bilangan Prima Marsenne

Bilangan prima Mersenne adalah sebuah bilangan yang sifatnya masih probabilistik, yaitu kemungkinan merupakan Prima dan masih perlu diuji untuk pembuktian keprimaannya.

Bilangan Mersenne adalah bilangan 2 yang dipangkatkan dengan bilangan prima dikurang 1. Dan

memiliki kecenderungan prima. Secara matematis dapat dituliskan sebagai berikut :

$Mp = 2^{(p)} - 1$[CITATION Zha10 \l 1033]

Dimana Mp = Bilangan Mersenne
p = bilangan prima

Misalkan p = 3 (bilangan prima)

$Mp = 2^{(3)} - 1$
$= 7$
(menghasilkan prima)

Misalkan p = 5 (bilangan prima)
Mp $= 2^{(5)} - 1$
$= 7$ *(menghasilkan prima)*

Misalkan p = 7
Mp $= 2^{(7)} - 1$
$= 127$ *(menghasilkan prima)*

Berdasarkan beberapa contoh di atas maka dapat diambil kesimpulan bahwa bilangan Mersenne masih bersifat probabilistik dan harus diuji keprimaannya. Dalam tulisan ini akan di uji menggunakan pengujian bilangan prima Solovay – Strassen.

II.3.Bilangan Prima Deterministik dan Probabilistik

Bilangan Prima Deterministik adalah bilangan yang secara pasti bisa ditetapkan sebagai bilangan prima dengan melakukan pembuktikan secara matematis.

Bilangan Prima Probabilistik merupakan bilangan yang masih diduga mungkin Prima. Dugaan kemungkinan prima ini tidak bisa memastikan keprimaannya karena uji coba yang dilakukan adalah dengan mengambil beberapa bilangan secara acak, Karena tidak diuji coba dengan semua angka secara rumus matematis tertentu, sehingga bilangan tersebut dianggap Probabilistik Prima. Beberapa metode yang dilakukan dalam uji coba probabilistic prima seperti Miller-Rabin, Solovay-Strassen, *Fermat's Last Theorem* dan lainnya. Dan pembahasan selanjutnya hanya membahas uji keprimaan dengan metode Solovay-Strassen.

II.4.Simbol Jacobi

Jacobi simbol (m/n), didefinisikan untuk setiap n bilangan ganjil. Ia memiliki sifat-sifat berikut yang memungkinkan untuk dengan mudah dihitung.

$(a/n) = (b/n)$ if $a = b \bmod n$.

$(1/n) = 1$ and $(0/n) = 0$.

$(2m/n) = (m/n)$ if $n = \pm 1 \bmod 8$

Otherwise $(2m/n) = -(m/n)$[CITATION Con \l 1033]

Misal m/n = (1236/20003)
= -(618/20003)
= (309/20003)
= (227/309)
= (82/227)
= -(41/227)
= -(22/41)
= -(11/41)
= -(8/11)
= (4/11)
= -(2/11)
= (1/11)
= 1

II.5.*Greatest Common Divisor (GCD)* menggunakan algoritma Euclidean

Greatest Common Divisor (GCD) atau sehari – hari kita sebut dengan Faktor Persekutuan Terbesar yaitu bilangan bulat N yang paling besar yang habis membagi dua buah bilangan bulat.

Misalnya dua buah bilangan bulan 12 dan 8.

12 habis dibagi oleh : 1, 2, 3, **4**, 6, 12.

8 habis dibagi oleh : 1, 2, **4**, 8.

Berdasarkan pembagian di atas maka dapat disimpulkan bahwa GCD dari 12 dan 8 adalah **4**.

Algoritma Euclidean dalam mendapatkan GCD adalah dengan menggunakan *reminder*. Algoritmanya adalah bilangan yang lebih besar (m) dibagi dengan bilangan yang lebih kecil (n) atau m >= n. Hasil sisa pembagian m dan n disimpan dalam sebuah bilangan r. Kemudian m diberikan nilai n dan n diberikan nilai r. Proses berulang sampai hasil bagi mencapai 0. Dan GCD nya adalah bilangan r sebelum 0.[CITATION Sap12 \l 1033]

Lebih mudah memahaminya dengan menggunakan contoh. Perhatikan contoh berikut ini.
Misalkan m = 42, n = 15

42 = 2 * 15 + 12
15 = 12 + 3
12 = 4 * **3** + 0

Maka gcd(42,15) = **3**

Algoritma Euclidean nilai m harus lebih besar dari n atau m>n, jika n < m maka perlu dilakukan *switch value* terhadap nilai m dan n sehingga m >= n.

II.6.Uji Prima dengan metode Solovay – Strassen

Untuk *n* merupakan suatu bilangan komposit yang ganjil $\left(\frac{b}{n}\right)$ merupakan symbol Jacobi. Jika *n* merupakan sebuah bilangan prima maka berlaku persamaan berikut ini :

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right)(mod\, n).$$

[CITATION Sen10 \l 1033]

Dasar algoritma Solovay – Strassen dapat dilihat pada poin – poin berikut ini

a. Pilih sebuah bilangan *b* acak dimana $0 < b < n$
b. Hitunglah nilai $d = gcd(b,n)$ menggunakan algoritma Euclid.
c. Jika didapatkan $d > 1$,maka bisa diambil sebah kesimpulan bahwa d adalah bilangan komposit.
d. Jika d = 1, maka lakukan persamaan Solovay – Strassen terhadap base *b*. Jika tidak lulus persamaan maka bilangan tersebut adalah komposit.
e. Jika lulus persamaan, maka probalitas n sebagai bilangan prima semakin besar. Lakukan percobaan berkali – kali dengan mengambil nilai acak dari *b*. Percobaan berkali kali akan memperkuat keprimaan bilangan *n*.

III. PEMBAHASAN DAN UJI COBA

Untuk mendapatkan bilangan prime Mersenne yang besar perlu dikombinasikan antara kedua algoritma di atas, yaitu penggabungan antara metode Solovay-Strassen dengan Mersenne. Adapun yang dibahas dalam menemukan bilangan prima yang besar tadi sebagai berikut :

```
Function Mersenne(n)
    Mersenne = 2^(n-1) – 1
Return Mersenne

Function CekPrimeSolovay_Strassen()
    b^((n-1)/2) ≡ (b/n) (mod n)
Return True or False

Loop for A = C → B
    Call CekprimeSolovay_Strassen(A)
    If A = prime:
      Call Mersenne(A)
      If
CekprimeSolovay_Strassen(Mersenne){
          Result Bigprime number;
          }
      Else{
          Result composite
      }
End.
```

Berdasarkan *Pseudocode* di atas, maka dapat dilihat pada contoh berikut ini :

Misalkan B = 100 dan C = 1500. Makan dilakukan pengecekan nilai bilangan prima antara B dan C dengan daftar sebagai berikut :

101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193

Dengan daftar bilangan prima di atas, dilakukan percobaan dengan menghitung bilangan Marsenne dan dilakukan pengecekan apakah Mersenne merupakan sebuah bilangan prima atau Komposit.

Daftar bilangan prima di atas dilakukan uji coba prima terhadap bilangan Mersenne. Misalnya :

P = 101

Mp $= 2^p - 1$

$= 2^{101} - 1$

= 2535301200456458802993406410751

Dan berdasarkan uji coba Solovay-Strassen bilangan tersebut adalah Komposit

P = 103

Mp = $2^{103}-1$

= 10141204801825835211973625643007

Uji coba solovay-Strassen adalah komposit

Contoh berikut adalah untuk nilai P = 521

Dan berdasarkan Prime Marsenne

Mp = $2^{521}-1$

= 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151 (uji coba Solovay-Strassen dinyatakan **bilangan Prima**)

P = 607

Mp =

531137992816767098689588206552468627329593117727031923199444138200403559860852242739162502265229285668889329486246501015346579337652707239409519978766587351943831270835393219031728127 (uji coba Solovay-Strassen dinyatakan **bilangan Prima**)

KESIMPULAN

Berdasarkan percobaan di atas, maka ditarik kesimpula bahwa Metode pengujian Bilangan Prima dengan Solovay-Strassen cepat dalam mendapatkan daftar bilangan prima. Dan untuk mendapatkan bilangan bilangan prima yang besar bisa digabungkan dengan metode Marsenne Prima yang kemudian hasil Marsenne Prime itu diuji coba dengan Solovay-Strassen lagi, sehingga bisa mendapatkan bilangan prima yang besar dengan waktu yang sangat singkat. Ini dikarenakan tidak perlu melakukan proses iterasi yang panjang dan makan waktu yang lama.

Kelemahan dari hasil uji coba yang dilakukan terjadinya error yang belum terdeteksi penyebabnya untuk angka bilangan prima yang lebih besar dari contoh yang tersaji pada tulisan ini. Yang mana dalam hal ini dirasakan bahwa metode Last Fermat's Theorem bagus digunakan untuk angka yang lebih besar, walaupun belum mampu menyimpulkan algoritma mana yang lebih baik di antara keduanya.

DAFTAR PUSTAKA

Conrad, K. (n.d.). *THE SOLOVAY–STRASSEN TEST.*

Kromodimoeljo, S. (2010). *Teori dan Aplikasi Kriptografi.* Jakarta.

Saputra, O. (2012). Kompleksitas Algoritma Euclidean dan Stein(FPB Biner). *Makalah IF2091 Struktur Diskrit – Sem. I Tahun 2011/2012*.

Sibao, Z., Ma, X., & Zhou, L. (2010). Some Notes on the Distribution of Mersenne. *Applied Mathematics*.