The Bulletin of Society for Mathematical Services and Standards *Online: 2013-12-02*
ISSN: 2277-8020, Vol. 8, pp 14-16
doi:10.18052/www.scipress.com/BSMaSS.8.14

THE GENERALIZATION OF THE CONCEPT OF PRIME NUMBER AND ITS APPLICATION

Jamel Ghanouchi Dr. K. Raja Rama Gandhi

RIME, département de Mathématiques, Tanisia

Professor in Mathematics, BITS-Vizag, India

Abstract. In this paper, we generalize the concept of prime number and define the real primes. It allows applying the new concept to cryptology.

Definition

A real number is compound if it can be written as $\prod_j p_j^{n_j}$ where p_j are primes and n_j are rationals. This decomposition in prime factors is unique. A prime real number or R-prime can be written only as p=p.1. Thus we define other real prime numbers like π, e, ln(2) . Of course, it is a convention, because, we can consider π^2 as prime and π will be no more prime. It is equivalent in what will follow.

Thus $\sqrt[q]{p} = p^{\frac{1}{q}}$ is compound. Also $\sqrt[q]{p}+1 = p^{\frac{1}{q}}+1$ is prime when p is prime and we have $\sqrt[2^j]{p}-1=(p-1)(\sqrt[2^j]{p}+1)^{-1}(\sqrt[2^{j-1}]{p}+1)^{-1}...(\sqrt{p}+1)^{-1}$ compound for p prime, for example.

Another example: $\sqrt[3]{p^2}-\sqrt[3]{p}+1=(p+1)(\sqrt[3]{p}+1)^{-1}$
It is 5/2 that divides 5 not the contrary!

Division of a real by a real
The GCD of two numbers
p and q are prime numbers :

$p \neq q \Rightarrow GCD(p,q)=1$

$nm<0 \Rightarrow GCD(p^n,p^m)=1$

$mn>0; m>0; GCD(p^n,p^m)=p^{\min(m,n)}$

$mn<0; m<0; GCD(p^n,p^m)=p^{\max(m,n)}$

$i \geq n_l \geq 1; GCD(\prod_{n=1}^{n=i} p_n^{m_n}, \prod_{l=1}^{l=j} p_{n_l}^{q_{n_l}}) = \prod_{l=1}^{l=j} GCD(p_{n_l}^{m_{n_l}}, p_{n_l}^{q_{n_l}})$

So a real number y divises a real number x if GCD(x,y) is different of 1.

Theorem

p is prime then

$\forall a \in R, \exists k \in R ; a^p = a + kp$

Proof of the theorem

$a.10^{-u} = \sum_{m=0}^{m=\infty} a_m.10^{-m}; a_m \in N$

$\exists k, k'; a^p.10^{-pu} = \sum_{m=0}^{m=\infty} a_m{}^p.10^{-m} + kp = \sum_{m=0}^{m=\infty} (a_m + k'p).10^{-m} + kp = \sum_{m=0}^{m=\infty} a_m.10^{-m} + k''p$

The probabilities

What the probability that a number between x+dx and x is prime? It is

$$p(x' \in [x, x+dx]) = \frac{dlog(x)}{x} = \frac{dx}{x^2}$$

Effectively

$$\log(1+\frac{dx}{x}) = \log(x+dx) - \log(x) = \frac{dx}{x} = d\log(x)$$

And

$$p(x' \in [x, x+dx]) = p(x' \in [0, x+dx]) - p(x' \in [0, x]) = \frac{\log(x+dx)}{x+dx} - \frac{\log(x)}{x}$$

$$= \frac{\log(x+dx)}{x} - \frac{\log(x)}{x} = \frac{d\log(x)}{x}$$

How many primes are there beyween x and x+dx ? There are

$$\pi(x) = \int \frac{dx}{d\log(x)} = \infty$$

Let us build real primes P and Q. We have p_I a prime and u_n a sequence.

We know that $p_n = 1 + \sqrt[u_n]{p_{n-1}}$ is prime. With N enough great, $P = p_N$. Also with another prime q_I and another sequence v_n , we have another real prime with M enough great, $Q = q_M$. As $1 + \sqrt{P}$ is prime and $1 + \sqrt{Q}$ is prime, let $n = \sqrt{P} + \sqrt{Q}$. Let e coprime with n and let d=kn-e,
If we have n and e public keys, we crypt M by M = C+e+kn and decrypt it by d and n with C = M - e + k'n = M + d + k''n.
Another possibility is to take n=(P-1)(Q-1) and e coprime with n then n and e are public keys and $M = C^e + kn$ then $C = M^d + k'n$.

References

[1] R. J. Backlund, « Sur les zéros de la fonction ζ(s) de Riemann », CRAS, vol. 158, 1914, p. 1979–1981.

[2] X. Gourdon, « The 1013 first zeros of the Riemann zeta function, and zeros computation at verylarge height »

[3] J.P.Gram, « Note sur les zéros de la fonction ζ(s) de Riemann », Acta Mathematica, vol. 27, 1903, p. 289–304.

[4] J.I.hutchinson « On the Roots of the Riemann Zeta-Function », Trans. AMS, vol. 27, no 1, 1925,p. 49–60.

[5] A. M. Odlyzko, The 1020-th zero of the Riemann zeta function and 175 million of its neighbors,1992.

[6] J.Barkley Rosser, J. M. Yohe et Lowell Schoenfeld, « Rigorous computation and the zeros of theRiemann zeta-function.», Information Processing 68 (Proc. IFIP Congress, Edinburgh, 1968), Vol. 1:Mathematics, Software, Amsterdam, North-Holland, 1969, p. 70–76.

[7] http://fr.wikipedia.org/wiki/Edward_Charles_Titchmarsh E.C.Titchmarsh, « The Zeros of theRiemann Zeta-Function », Proceedings of the Royal Society, Series A, Mathematical and PhysicalSciences, vol. 151, no 873, 1935, p. 234–255.

[8] E. C. Titchmarsh, « The Zeros of the Riemann Zeta-Function », Proceedings of the Royal Society, Series A, Mathematical and Physical Sciences, The Royal Society, vol. 157, no 891, 1936, p. 261–263.

[9] A.M.Turing, « Some calculations of the Riemann zeta-function », Proceedings of the LMS, Third Series, vol. 3, 1953, p. 99–117.

[10] J. van de Lune, H.te Riele et D. T. Winter, « On the zeros of the Riemann zeta function in the critical strip. IV », Mathematics of Computation, vol. 46, no 174, 1986, p. 667–681.