International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

The Concept of Prime Number and its Application

Jamel Ghanouchi

Professor of Mathematics, RIME Department of Mathematics, 6 Rue Khansa 2070 Marsa Tunisia

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

Keywords: Reals; Primes; Transcendentality; Cryptology

1. Introduction

The prime numbers are called primes because they are the bricks of the numbers: Each number n can be written as $\prod_j p_j^{n_j}$ when where p_j are primes and n_j are integers.

This writing is called the decomposition in prime factors of the number n. In fact, this definition is a very particular case of a much more general one. Indeed, if n_j are rationals, everything changes.

Considering that the decomposition in prime factors of an integer n when n_j are rationals $\prod_j p_j^{n_j}$. In this writhing, then the p_j have no reason to be the same than before and they become a convention. For example, if we decide that 16 is conventionally prime, we have 2 equal to 16 power 1/4 and each number can be written according to 16 and its rational exponent instead of 2.

If we decide conventionally that each Fermat number is prime, and it is possible by the fact that they are coprime two by two, then each new prime (new primes=bricks with rational exponents in the writing) replaces anther one in the list of the old primes (old primes=bricks with integral exponents in the writing).

Example: If by convention, the fifth Fermat number =4294967297=641.6700417 is prime, we can decide that it replaces 641 which becomes compound and 6700417 is prime or 641 is prime and 67004147 is compound.

In all cases, the advantage is that we have a formula which gives for each n a prime. And we can see the the primes are infinite. There is another interesting result: Let Ulam spiral. The Fermat numbers are all situated in the same line.

4. Theorem

p is prime then

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

2. 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 we have $\sqrt[q]{p}+1 = p^{\frac{1}{q}}+1$ when p is prime and we have

$\sqrt[2^i]{p}-1 = (p-1)(\sqrt[2^i]{p}+1)^{-1}(\sqrt[2^{i-1}]{p}+1)^{-1}...(\sqrt{p}+1)^{-1}$

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 divises 5 not the contrary!

3. 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)=y.

Proof of the theorem

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

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

5. 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

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

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

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

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

6. Applications to cryptology

Let us build real numbers P and Q. We have p_1 a prime and u_n a sequence.

We know that $p_n=1+\sqrt[u_n]{p_{n-1}}$ is a real. With N enough great, $P=p_N$. Also with another prime q_1 and another sequence v_n, we have

another real with M enough great, $Q=q_M$. As

$1+\sqrt{P}$ is real and $1+\sqrt{Q}$ is real, let $n=\sqrt{P}+\sqrt{Q}$. Let

$e=\alpha+u\sqrt{P}+v\sqrt{Q}$ and let d=kn-e,

If we have n and e public keys, the message is M = C+e+kn and the cypher is

C = M -e + k'n = M + d + k''n.

Another possibility is to take n=PQand

$e=\frac{\alpha}{(P-1)^u(Q-1)^v}$ then

n and e are the public keys and $M=C^e+kn$ then

$C=M^d+k'n$ with $d=\frac{(P-1)^u(Q-1)^v}{\alpha}$

Example :

$p=79,q=83$

$p_1=\sqrt[5]{79}+1=3.39621299$

$q_1=\sqrt[7]{83}+1=2.879983394$

$P=\sqrt{p_1}+1=2.842881708$

$Q=\sqrt{q_1}+1=2.697051392$

$n=PQ=7.629465043$

$$e=\frac{9378.2}{(P-1)^7(Q-1)^6}=5.737752231$$

$$\equiv 2.63415566((P-1)(Q-1))$$

$M=79.836$

$M^e=79.863^{2.63415566}\equiv 4.6268(n)$

$$d=\frac{(P-1)^7(Q-1)^8}{\alpha}=0.379628286$$

$13445X7.629465043+4.6268=102580.2768$

$C=102580.2768^{0.379628286}=79.86373604 \Rightarrow C=79.863$

7. Conclusion

We have generalized the concept of prime to the reals. It allowed to present an application to cryptology.

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 10^{13} first zeros of the Riemann zeta function, and zeros computation at very large 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, n° 1, 1925, p. 49–60.
[5] M. Odlyzko, The 10^{20}-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 the Riemann 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_TitchmarshE.C.Titchmarsh, « The Zeros of the Riemann Zeta-Function », Proceedings of the Royal Society, Series A,

Mathematical and Physical Sciences, vol. 151, n° 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, n° 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, n° 174, 1986, p. 667–681.