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 \( \prod p_j^{n_j} \) 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 \( \pi, e, \ln(2) \). Of course, it is a convention, because, we can consider \( \pi^2 \) as prime and \( \pi \) will be no more prime. It is equivalent in what will follow.

Thus \( \sqrt[2]{p} = p^{1/2} \) is compound. Also \( \sqrt[2]{p} + 1 = p^{1/2} + 1 \) is prime when \( p \) is prime and we have

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

compound for \( p \) prime, for example.

Another example:

Thus \( \sqrt[3]{p^2} - \sqrt[3]{p} + 1 = (p + 1)(\sqrt[3]{p} + 1)^{-1} \)

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 :

\( p \neq q \Rightarrow \gcd(p, q) = 1 \)

\( mn < 0 \Rightarrow \gcd(p^n, p^m) = 1 \)

\( mn > 0; m > 0; \gcd(p^n, p^m) = p^\min(n, m) \)

\( mn < 0; m < 0; \gcd(p^n, p^m) = p^\max(n, m) \)

\( i \geq n_j \geq 1; \gcd(p_1^{n_1}, p_2^{n_2}, ..., p_r^{n_r}) = \prod_{i=1}^{r} \gcd(p_1^{n_1}, p_2^{n_2}) \)

So a real number \( y \) divides a real number \( x \) if \( \gcd(x, y) \) is different of 1.

Theorem

\( p \) is prime then

\( \forall a \in \mathbb{R}, \exists k \in \mathbb{R} ; a^p = a + kp \)

Proof of the theorem

\[
a.10^{-n} = \sum_{m=0}^{\infty} a_m.10^{-m}; a_m \in \mathbb{N}
\]

\[
\exists k, k'; a^p.10^{-m} = \sum_{m=0}^{\infty} a_m.p.10^{-m} + kp = \sum_{m=0}^{\infty} (a_m + k'.p).10^{-m} + kp = \sum_{m=0}^{\infty} a_m.10^{-m} + k^*p
\]
The probabilities

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

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

Effectively

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

And

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

How many primes are there between \(x\) 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 \(P_n = 1 + \sqrt[2]{P_{n-1}}\) 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 \(1 + \sqrt[2]{P}\) is prime and \(1 + \sqrt[2]{Q}\) is prime, let \(n = \sqrt[2]{P} + \sqrt[2]{Q}\). 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


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


