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 \( p=p\cdot1 \). 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 \( \sqrt[3]{p} = p^\frac{1}{3} \) is compound. Also \( \sqrt[3]{p} + 1 = p^\frac{1}{3} + 1 \) is prime when \( p \) is prime and we have \( \sqrt[3]{p} - 1 = (p - 1)(\sqrt[3]{p} + 1)^{-1}(\sqrt[3]{p^2} + 1)^{-1} \ldots (\sqrt{p} + 1)^{-1} \) compound for \( p \) prime, for example.

Another example: \( \sqrt{p^2} - \sqrt{p} + 1 = (p + 1)(\sqrt{p} + 1)^{-1} \)

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:

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

\[ mn < 0 \Rightarrow \gcd(p^n, q^n) = 1 \]

\[ mn > 0; m > 0; \gcd(p^n, q^n) = p^{\gcd(m, n)} \]

\[ mn > 0; m < 0; \gcd(p^n, q^n) = p^{\max(m, n)} \]

\[ i \geq n \geq 1; \gcd(\prod_{i=1}^{n} p_{n_i}^{m_i}, \prod_{i=1}^{n} p_{n_i}^{n_i}) = \prod_{i=1}^{n} \gcd(p_{n_i}^{m_i}, p_{n_i}^{n_i}) \]

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

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

\[ \exists k, k'; a^p \cdot 10^{-pu} = \sum_{n=0}^{\infty} a_n^p \cdot 10^{-n} + kp = \sum_{n=0}^{\infty} (a_n + k \cdot p) \cdot 10^{-n} + kp = \sum_{n=\infty}^{\infty} a_n \cdot 10^{-n} + k^* p \]
The probabilities

What is 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

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

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

How many primes are there 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 \( P_n = 1 + \sqrt[n]{P_{n-1}} \) 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


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


