A Theorem on Prime Numbers

Leo Liberti

Centre for Process Systems Engineering
Imperial College of Science, Technology and Medicine

(l.liberti@ic.ac.uk)

2 August 2002

Abstract

The theorem presented in this paper allows the creation of large prime numbers (of order $o(n^2)$) given a table of all primes up to n.

Notation: in what follows, products taken over empty index sets are to be considered equal to 1.

Theorem
Let $p(i)$ be the i-th prime number and let I_1, I_2 be a partition of $\{1, \ldots, n\}$ such that

$$q_1 = \prod_{i \in I_1} p(i) - \prod_{i \in I_2} p(i) \quad \leq \quad (p(n))^2, \tag{1}$$

$$q_2 = \prod_{i \in I_1} p(i) + \prod_{i \in I_2} p(i) \quad \leq \quad (p(n))^2. \tag{2}$$

Then q_1, q_2 are prime numbers.

Proof. Suppose there is a non-unit prime $b \in \mathbb{Z}$ such that $b \leq \sqrt{q_1}$ and $b|q_1$. Then because $\sqrt{q_1} \leq p(n)$ we have $b \leq p(n)$; thus there is a $j \leq n$ such that $b = p(j)$. Assume without loss of generality $j \in I_1$ (a symmetric argument holds if we assume $j \in I_2$). Then $b|q_1$ and $b|\prod_{i \in I_1} p(i)$ imply $b|\prod_{i \in I_2} p(i)$, i.e. $j \in I_1 \cap I_2$, which is empty, so such a b cannot exist. Hence q_1 is prime. Similarly for q_2. □

This theorem allows us, given a table of prime numbers up to an integer n, to create prime numbers of order $o(n^2)$.