Primes at a (somewhat lengthy) glance

Takashi Agoh, Paul Erdős, and Andrew Granville

One can tell that

$$\begin{aligned} 17 &= 2^3 + 3^2 \\ 19 &= 2^4 + 3 \\ 37 &= 5^2 + 2^2 \cdot 3 \\ 47 &= 2 \cdot 5^2 - 3 \\ 53 &= 3^2 \cdot 7 - 2 \cdot 5 \\ 97 &= 3 \cdot 5 \cdot 7 - 2^3 \end{aligned}$$

are all prime, at a glance, since we have written each $n = A \pm B$ where each prime $\le \sqrt{n}$ divides exactly one of A and B (and thus n is coprime with every prime $\le \sqrt{n}$). This strange procedure is thoroughly investigated in [1]; in general, it is quite a challenge to so write a given prime n since the product of the primes $\le \sqrt{n}$ is around $e^{\{1+o(1)\}\sqrt{n}}$.

A similar but more complicated method to establish the primality of n goes as follows: let $p_1 = 2 < p_2 = 3 < \cdots < p_k$ be the sequence of primes $\le \sqrt{n}$. Write n in the form

$$n = N_1 \pm N_2 \pm \cdots \pm N_k, \tag{1}$$

where the set of prime divisors of N_j is precisely the set of all the primes up to p_k, other than p_j. Then, for each $j = 1, 2, \ldots, k$, we have $(n, p_j) = (N_j, p_j) = 1$ (since p_j divides N_i whenever $j \neq i$), and thus n is prime. This way of determining whether n is prime leads to our title. It turns out to be fairly easy to prove that there always is a representation as in (1):

Theorem. *Given $p_1 = 2 < p_2 = 3 < \cdots < p_k$ the first k primes and a positive integer $n \le \left(\prod_{i=1}^k p_i\right)\left(\sum_{j=1}^k \frac{1}{p_j}\right)$, free of prime factors $\le p_k$, there exist integers $N_1, N_2, \ldots, N_k$ with*

$$n = N_1 + N_2 + \cdots + N_k, \tag{1}$$

where each $|N_j| < \prod_{i=1}^k p_i$ and the prime divisors of N_j are precisely $\{p_1, p_2, \ldots, p_k\} \setminus \{p_j\}$.

In fact we shall determine all such solutions to (1) in our proof.

Proof. Let $m = \prod_{i=1}^{k} p_i$, and let $m_j = m/p_j$ for each j. Assume that n is an integer in the range $0 < n \leq \sum_{j=1}^{k} m_j$, which is coprime to m. Define α_j to be the least positive integer for which

$$n \equiv m_j \alpha_j \pmod{p_j}$$

for each j (such an α_j exists since $(m_j, p_j) = 1$). Moreover $0 < \alpha_j < p_j$ since $(n, p_j) = 1$ (because $(n, m) = 1$ and p_j divides m).

Define $N = m_1\alpha_1 + m_2\alpha_2 + \cdots + m_k\alpha_k$. Since each $\alpha_j \geq 1$, we deduce that $N \geq \sum_{j=1}^{k} m_j \geq n$. Also, since p_j divides m_i whenever $j \neq i$, we deduce that

$$N \equiv m_j \alpha_j \equiv n \pmod{p_j}$$

for each j, and so $N \equiv n \pmod{m}$ by the Chinese Remainder Theorem. Thus we may write $N = n + \Delta m$ for some integer $\Delta \geq 0$. We also note that since each $\alpha_j < p_j$ thus $\Delta m < N < m_1p_1 + m_2p_2 + \cdots + m_kp_k = km$, so that $\Delta < k$.

Now in any solution to (1), m_j divides N_j for each j, by the hypothesis, so we can write $N_j = m_j a_j$ for some integer a_j. Since p_j divides m_i, which divides N_i, whenever $j \neq i$, we deduce from (1) that

$$m_j \alpha_j \equiv n \equiv N_j = m_j a_j \pmod{p_j}.$$

Therefore $a_j \equiv \alpha_j \pmod{p_j}$ since $(m_j, p_j) = 1$.

The condition $|N_j| < m$ is equivalent to the condition $|a_j| < m/m_j = p_j$. The only integers that are $< p_j$ in absolute value, and $\equiv \alpha_j \pmod{p_j}$, are α_j itself and $\alpha_j - p_j$. Therefore $a_j = \alpha_j - \delta_j p_j$ where $\delta_j = 0$ or 1. Conversely if $a_j = \alpha_j - \delta_j p_j$ where $\delta_j = 0$ or 1, then $|a_j| < p_j$ so that $|N_j| < m$. Moreover, all of the prime divisors of a_j are then $< p_j$ and thus the prime divisors of $N_j = m_j a_j$ are a subset of $\{p_1, p_2, \ldots, p_k\} \setminus \{p_j\}$, as required by the hypothesis. Also, since $m_j a_j = m_j \alpha_j - \delta_j m$, we have

$$\begin{aligned} N_1 + N_2 + \cdots + N_k &= m_1a_1 + m_2a_2 + \cdots + m_ka_k \\ &= (m_1\alpha_1 - \delta_1 m) + (m_2\alpha_2 - \delta_2 m) + \cdots + (m_k\alpha_k - \delta_k m) \\ &= N - (\delta_1 + \delta_2 + \cdots + \delta_k)m. \end{aligned}$$

Therefore (1) holds if and only if $\delta_1 + \delta_2 + \cdots + \delta_k = \Delta$, where each $\delta_j = 0$ or 1. Since $0 \leq \Delta < k$, it is evident that there are solutions to this, and that they are given when exactly Δ of the δ_j equal 1, and the rest of the δ_j equal 0.

Example. To clarify the notation in the proof above we show how to find all solutions to (1) for the example with $n = 101$ and $k = 4$:

We have

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \text{ and } p_4 = 7,$$

so that $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ and

$$m_1 = 105, \ m_2 = 70, \ m_3 = 42, \text{ and } m_4 = 30.$$

From some simple modular arithmetic we determine that

$$\alpha_1 = 1, \quad \alpha_2 = 2, \quad \alpha_3 = 3, \text{ and } \alpha_4 = 5,$$

which leads to $N = 105 \cdot 1 + 70 \cdot 2 + 42 \cdot 3 + 30 \cdot 5 = 521$. Therefore $\Delta = (N - n)/m = (521 - 101)/210 = 2$; and thus if $a_j = \alpha_j - \delta_j m_j$ for $j = 1, 2, 3, 4$, then exactly two of the $\delta_j = 1$, the other two of the $\delta_j = 0$. This leads to $\binom{4}{2} = 6$ representations of 101 as in (1), namely:

$$\begin{aligned} 101 &= -105 + 140 + 126 - 60 = 105 - 70 + 126 - 60 = -105 - 70 + 126 + 150 \\ &= -105 + 140 - 84 + 150 = 105 + 140 - 84 - 60 = 105 - 70 - 84 + 150 \end{aligned}$$

Corollary. *Every prime $n \geq 11$ may be 'proved' to be prime by expressing it in the form (1), where $p_1 = 2 < p_2 = 3 < \cdots < p_k$ are precisely the primes up to $\sqrt{n}$, and N_j is the product of all of those primes other than p_j.*

Proof. For each prime $11 \leq n \leq 47$ we verify the result by computing an appropriate expression of the form (1):

$$\begin{gathered} 11 = 3 + 2^3; \quad 13 = 3^2 + 2^2; \quad 17 = 3^2 + 2^3; \quad 19 = 3 + 2^4; \quad 23 = 3^3 - 2^2; \\ 29 = 3^2 \cdot 5 - 2 \cdot 5 - 2 \cdot 3; \quad 31 = 3 \cdot 5 + 2 \cdot 5 + 2 \cdot 3; \quad 37 = 3 \cdot 5 + 2 \cdot 5 + 2^2 \cdot 3; \\ 41 = 3 \cdot 5 + 2^2 \cdot 5 + 2 \cdot 3; \quad 43 = 3 \cdot 5 + 2 \cdot 5 + 2 \cdot 3^2; \quad 47 = 3 \cdot 5 + 2^2 \cdot 5 + 2^2 \cdot 3. \end{gathered}$$

That such expressions exist for each prime $n \geq 53$ may be deduced directly from our Theorem, by using the following Lemma to ensure that the hypothesis of the Theorem holds when we take $p_1 = 2 < p_2 = 3 < \cdots < p_k$ to be the primes up to $\sqrt{n}$.

Lemma. *If $n \geq 49$ then* $\left(\prod_{p\leq\sqrt{n}} p\right)\left(\sum_{p\leq\sqrt{n}} \frac{1}{p}\right) \geq n$.

Proof. Bertrand's postulate asserts that there is a prime in the interval $(x, 2x]$ whenever $x \geq 1$. In particular, there are primes $q \in (\sqrt{n}/2, \sqrt{n}]$ and $r \in (\sqrt{n}/4, \sqrt{n}/2]$.

Therefore, if $n > 400$, then $2, 3, 5, q, r$ are distinct primes $\leq \sqrt{n}$, so that

$$\left(\prod_{p\leq\sqrt{n}} p\right)\left(\sum_{p\leq\sqrt{n}} \frac{1}{p}\right) \geq 2\cdot 3\cdot 5\cdot q\cdot r\cdot\left(\frac{1}{2}+\frac{1}{3}+\frac{1}{5}\right) = 31qr > 31\frac{\sqrt{n}}{2}\frac{\sqrt{n}}{4} > n.$$

If $121 \leq n \leq 400$, then $2, 3, 5, 7, 11$ are distinct primes $\leq \sqrt{n}$, so that

$$\left(\prod_{p\leq\sqrt{n}} p\right)\left(\sum_{p\leq\sqrt{n}} \frac{1}{p}\right) \geq 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot\left(\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}\right) = 2927 > n.$$

If $49 \leq n \leq 120$, then $2, 3, 5, 7$ are distinct primes $\leq \sqrt{n}$, so that

$$\left(\prod_{p\leq\sqrt{n}} p\right)\left(\sum_{p\leq\sqrt{n}} \frac{1}{p}\right) \geq 2\cdot 3\cdot 5\cdot 7\cdot\left(\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}\right) = 247 > n.$$

In many ways, this proof of primality seems to be entirely without merit—one needs to know all of the primes $\leq \sqrt{n}$ for it to be useful—moreover, the expression in (1) is, in practice, ridiculously long. However, it does express a proof of primality in a single, albeit unwieldy, expression.

Dedicatory: Paul Erdős passed away on 20th September, 1996, just a few weeks after this paper was accepted for publication.

Acknowledgement: Thanks to Carl Pomerance and John Selfridge for some useful comments. The third author is a Presidential Faculty Fellow and is supported, in part, by the National Science Foundation.

[1] R.K. Guy, C.B. Lacampagne, J.L. Selfridge, Primes at a glance, *Math. Comp.* **48** (1987), 183–202.

Takashi Agoh
Dept. of Math.
Science U. of Tokyo
Noda, Chiba 278, Japan
(agoh@ma.noda.sut.ac.jp)

Paul Erdős
Mathematical Institute
Hungarian Academy of Sciences
Reáltanoda u. 13-15,
Budapest, Hungary

Andrew Granville
Dept. of Math.
U. of Georgia
Athens, Georgia 30602, USA
(andrew@math.uga.edu)