EPISODE 9

The intriguing Riemann Hypothesis

9.1. The famous short paper of Riemann

In 1859, Riemann was elected to the Berlin Academy of Sciences. Since every newly elected member of the Academy had to report on his most recent research, Riemann chose to submit a report entitled *On the number of primes less than a given magnitude*. The paper was read by Kummer at the meeting of the Academy on November 3, 1859. This famous eight-page paper [**183**] is often referred to as his *Memoir*. In it, Riemann studied the analytic behavior of $\zeta(s)$ in the complex plane. His goal was to derive a representation of $\pi(x)$ in the form of a series with principal term $\mathrm{Li}(x)$ (see the definition of $\mathrm{Li}(x)$ below). Unfortunately, no one can claim that his goal was achieved. Indeed, in his formula relating $\pi(x)$ with $\mathrm{Li}(x)$, there is no proof that $\mathrm{Li}(x)$ is the principal term of the asymptotic formula as x tends to infinity. For more on this, we refer the reader to the book of Maz'ya and Shaposhnikova [**157**]. Even though Riemann did not reach his goal of providing a rigorous proof of the prime number theorem, the results he obtained concerning the zeta function were groundbreaking and served as the key ingredient for obtaining a proof of the prime number theorem. More precisely, Riemann introduced a new approach that would later be used by Hadamard and de la Vallée Poussin to prove the prime number theorem. Even though Riemann's memoir is only eight pages long, it contains numerous original ideas and many new features including several representations of $\zeta(s)$ for complex s, the proof of the functional equation satisfied by $\zeta(s)$, a discussion on the location of the complex zeros of $\zeta(s)$, Fourier inversion techniques, explicit representations of $\pi(x)$ and the statement of the very famous Riemann Hypothesis (RH):

$$\boxed{\textit{If } \zeta(s) = 0 \textit{ with } 0 < \Re(s) < 1, \textit{ then } \Re(s) = \tfrac{1}{2}}$$

The Riemann Hypothesis is certainly one of the most important unsolved problems in mathematics. Therefore, it is not so surprising that it is the only problem appearing in two famous lists of problems:
(1) the challenging 23 problems presented by Hilbert on the occasion of the Second International Congress of Mathematics held in Paris in 1900 (the Riemann Hypothesis is number 8 in that list),
(2) the seven Millennium problems presented in 2000 by the Clay Mathematics Institute (see `www.claymath.org/millennium-problems`).

In the words of Riemann[1],

> *It is very probable that all roots are real. Of course one would like a rigorous proof here; I have for the time being, after some*

[1]This is a crude English translation of a few lines taken from Riemann's memoir.

fleeting vain attempts, put aside the search for this, as it appears unnecessary for the next objective of my investigation.

In his Memoir, Riemann alludes to the function $\xi(s)$ (defined in Problem 7.7) and expresses RH in the form "all the zeros of $\xi(s)$ are real", which in light of Problem 7.7 (ii) is the same as saying that all the complex zeros of $\zeta(s)$ are located on the line $\Re(s) = 1/2$.

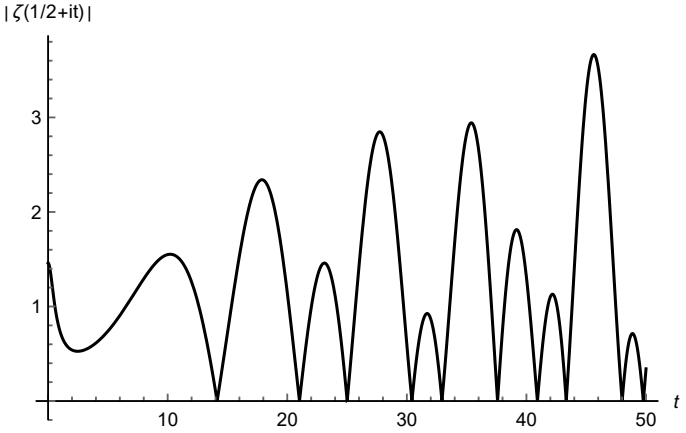
Since 1859, many have struggled to prove the Riemann Hypothesis. All have failed. As early as 1885 and as reported in the book of Narkiewicz [**168**], the Dutch mathematician Thomas Johannes Stieltjes thought he had proved RH. Indeed, he claimed that the series $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ converges for all real numbers $s > 1/2$, which would automatically imply RH (see Problem 9.6). In fact, in an undated letter to Hermite (most likely written in the first half of 1885), Stieltjes wrote "I have been quite lucky proving this property, announced as very probable by Riemann, that all roots of $\xi(t) = 0$ are real... But all these investigations need still much time... As I cannot actively continue this work at this instant because of other duties, I propose to take some breath and leave all this for a few months. I hope however that it will not be inconvenient to publish in Comptes Rendus the included note, which, it seems, will be of interest to geometers who did study Riemann's memoir." When Hermite asked for details of his proof, Stieltjes replied in a letter dated July 11, 1885, that his proof was based on the fact that the function $M(x)$ defined in Problem 8.5 satisfies $|M(x)| \leq C\sqrt{x}$ for some positive constant C for all $x \geq 1$ with possibly $C = 1$, a claim which amounts to the Mertens conjecture, which we now know to be false (more on this in Episodes 10 and 18). Then, in 1887, in a letter to Mittag-Leffler, Stieltjes wrote "But the proof of this lemma is purely arithmetic and very difficult. I obtained it as a result of a sequence of preliminary statements. I hope that this proof could be simplified but already in 1885 I did my best..." History shows that Stieltjes' proof of the Riemann Hypothesis had to be false, in particular because the Mertens conjecture was shown to be false in 1985 by Odlyzko and te Riele [**173**].

Thomas Johannes Stieltjes (1856–1894) was born in Zwolle, Netherlands. At the Polytechnical School of Delft, he rarely attended lectures, preferring to spend his time reading Gauss and Jacobi in the library. As a consequence, he failed his examinations. He was lucky that his father (also called Thomas Stieltjes) was a well-known civil engineer and politician and could therefore obtain for him a position at the Leiden Observatory when he was only 20. With this new job, he began writing to Charles Hermite about celestial mechanics, but the subject quickly turned to mathematics. This was the beginning of his career as a researcher. Stieltjes worked on almost all branches of analysis and number theory. He is sometimes called "the father of the analytic theory of continued fractions". He also made important contributions to discontinuous functions, divergent series, differential equations, the Gamma function and elliptic functions.

9.2. The successive zeros of $\zeta(s)$ on the critical line

There is no simple rule allowing one to predict the exact location of the successive zeros of $\zeta(s)$ on the critical line. The next graph tends to confirm this. Indeed,

we now show the graph of $|\zeta(\frac{1}{2}+it)|$ as t varies from 0 to 50, thereby displaying the first ten complex zeros $\rho = \frac{1}{2}+it$ at $t = 14.13\ldots$, $21.02\ldots$, $25.01\ldots$, $30.42\ldots$, $32.93\ldots$, $37.58\ldots$, $40.91\ldots$, $43.32\ldots$, $48.00\ldots$, $49.77\ldots$.



Note that van de Lune, te Riele and Winter [**209**] have shown that the first 1 500 000 001 complex zeros of $\zeta(s)$ all lie on the critical line.

9.3. Statements equivalent to the Riemann Hypothesis

As we will see in Problem 9.3, the two functions

$$\mathrm{Li}(x) := \int_0^x \frac{dt}{\log t} = \lim_{\varepsilon\to 0}\left(\int_0^{1-\varepsilon} + \int_{1+\varepsilon}^x\right)\frac{dt}{\log t} \tag{9.1}$$

and

$$\mathrm{li}(x) := \int_2^x \frac{dt}{\log t} \tag{9.2}$$

differ only by a constant since one can show that

$$\mathrm{Li}(x) = \mathrm{li}(x) + 1.04\ldots$$

(see Problem 9.3). Observe that a simple integration by parts yields

$$\mathrm{Li}(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right). \tag{9.3}$$

Observe also that three years after the 1896 proof of the prime number theorem, de la Vallée Poussin [**224**] showed that there exists a positive constant C such that

$$\pi(x) = \mathrm{Li}(x) + O\left(\frac{x}{e^{C\sqrt{\log x}}}\right).$$

Then, in 1901, the Swedish mathematician Niels Fabian Helge von Koch [**127**] showed that if the Riemann Hypothesis holds, then

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\ \log x) \tag{9.4}$$

(for a proof, see Theorem 5.21 in the book of Narkiewicz [**168**]). There is little hope that one could lower the size of the $O(\cdots)$ term in (9.4) because, as we will see in Episode 18, Littlewood showed in 1914 that $\pi(x) - \mathrm{Li}(x) > x^{1/2}\dfrac{\log\log\log x}{\log\log x}$ for infinitely many values of x tending to infinity.

Even though the Riemann Hypothesis is about the behavior of a complex valued function, surprisingly it is equivalent to various statements regarding the behavior of integer valued arithmetic functions. One of the best examples of this is a result by Jean-Louis Nicolas with an implication obtained by Guy Robin. Indeed, it follows from a result of Nicolas [**171**] that $\limsup_{n\to\infty} \dfrac{\sigma(n)}{e^\gamma n \log\log n} = 1$, where γ stands for the Euler-Mascheroni constant. Now, observe that

$$\frac{\sigma(n)}{e^\gamma n \log\log n} = 1.00556\ldots \quad \text{for } n = 5040.$$

Surprisingly, in 1985, Robin [**188**] showed that the Riemann Hypothesis is equivalent to the statement

$$\sigma(n) < e^\gamma n \log\log n \qquad \text{for all integers} \quad n \geq 5041. \tag{9.5}$$

Moreover, examining the sequence of *harmonic numbers* $(H_n)_{n\in\mathbb{N}}$, where

$$H_n := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n},$$

Jeff Lagarias [**132**], using Robin's result, proved that the Riemann Hypothesis is equivalent to the statement

$$\sigma(n) \leq H_n + e^{H_n} \log H_n \qquad \text{for all integers} \quad n \geq 1,$$

with equality holding if and only if $n = 1$.

All these observations confirm the fact that the Riemann Hypothesis plays a pivotal role in the study of the distribution of primes as well as the behavior of integer valued arithmetic functions.

9.4. The location of the zeros and the error term in the prime number theorem

Let $\Theta := \sup\{\sigma : \zeta(\sigma + it) = 0\}$. If follows from Theorem 8.3 and implications (8.9) that

$$\frac{1}{2} \leq \Theta \leq 1$$

and also that the Riemann Hypothesis is equivalent to the statement $\Theta = \frac{1}{2}$. Remarkably, it has been established that there exists a direct link between the location of the zeros of the Riemann zeta function and the size of the error term in the prime number theorem. More precisely, it has been shown that

$$\pi(x) - \mathrm{Li}(x) = O\left(x^\Theta \log x\right)$$

(see Theorem 5.10 in the book of William and Fern Ellison [**74**]).

Problems on Episode 9

Problem 9.1. Prove that, for $x \geq e^e$,

$$\mathrm{Li}(x) = \gamma + \log\log x + \sum_{n=1}^{\infty} \frac{\log^n x}{n \cdot n!},$$

where γ stands for the Euler-Mascheroni constant.

PROBLEM 9.2. With the help of a computer, obtain an approximation for $\mathrm{Li}(10^7)$ using the representation of $\mathrm{Li}(x)$ given in the preceding problem (retaining only the first 30 terms of the series). Compare your estimate with the known value $\pi(10^7) = 664\,579$.

PROBLEM 9.3.* Set $\Delta(x) := \mathrm{Li}(x) - \mathrm{li}(x)$. Prove that $\Delta(x)$ is bounded and in fact that $\lim_{x\to\infty} \Delta(x) = 1.04516\ldots$.

PROBLEM 9.4. Prove that a consequence of the estimate

$$\pi(x) - \mathrm{Li}(x) = O\left(x^{\Theta} \log x\right)$$

is that

$$\psi(x) = x + O(x^{\Theta} \log^2 x).$$

PROBLEM 9.5. Show that if

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2} \log x),$$

then, for any given small $\varepsilon > 0$, we have

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2+\varepsilon}).$$

PROBLEM 9.6. Stieltjes claimed that he could prove that the series $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ converges for all $s > 1/2$. We mentioned in the first section of this episode that Stieltjes' claim (assuming it were true) would imply the Riemann Hypothesis. Provide the details of this implication.

PROBLEM 9.7. Prove that $\sigma(n) \le n(\log n + 1)$ for each positive integer n.

PROBLEM 9.8. As n runs through the integers belonging to the interval $[e^e, 5040]$, how large can the quotient $\dfrac{\sigma(n)}{e^{\gamma} n \log\log n}$ be? For what integer n does it become that large?

PROBLEM 9.9. For all those squarefree integers $n > 5040$, can one prove that inequality (9.5) holds?

EPISODE 21

The multiplicative structure of integers

According to the *fundamental theorem of arithmetic*, any given integer $n \geq 2$ can be written as a product of primes, that is,

(21.1)
$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}, \text{ where } q_1 < q_2 < \cdots < q_r \text{ are primes and } \alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N},$$

and such a representation is unique. The form (21.1) is often called the *canonical representation* of the integer n.

In this episode, we examine the distribution of the prime factors q_i in the canonical representation of integers n, both globally and locally; then, we do the same for the exponents α_i.

21.1. The prime factors in the multiplicative structure of integers

Examining the canonical representation (21.1) of an integer n, one might wonder how large is q_r, the largest prime factor of n, which we commonly denote by $P(n)$. How often is $P(n)$ larger than $\sqrt{n}$? What is the median value of $P(n)$? What is the most frequent value of $P(n)$? All these questions arise naturally as we examine the multiplicative structure of integers. The notion of smooth (or friable[1]) numbers has been very useful in studying these problems. A *y-smooth* (or *y-friable*) number is a positive integer such that none of its prime factors exceeds y. For instance, the complete list of all 3-smooth numbers smaller than 100 is

$$2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 16,\ 18,\ 24,\ 27,\ 32,\ 36,\ 48,\ 54,\ 64,\ 72,\ 81,\ 96.$$

Crucial for the analysis of smooth numbers is the *de Bruijn function*

$$\Psi(x, y) := \#\{n \leq x : P(n) \leq y\} \qquad (2 \leq y \leq x),$$

a function which has been the focus of much research since the 1950's.

For a fixed x, the value of $\Psi(x, y)$ increases as y increases. Similarly, for a fixed y, the value of $\Psi(x, y)$ increases as y increases. One gets an indication of this by checking Figure 21.1.

In Figure 21.1, we show the graph of $\Psi(x, y)$ as x varies between 2 and 1000 and y varies between 2 and 47. Clearly, $\Psi(x, y)$ reaches its maximum value at $(x, y) = (1000, 47)$, and one can compute that $\Psi(1000, 47) = 526$.

One can establish bounds for the $\Psi(x, y)$ function. For instance, let us mention the classic upper bound

$$\Psi(x, y) \ll x \exp\left\{-\frac{1}{2}\frac{\log x}{\log y}\right\} \qquad (2 \leq y \leq x) \tag{21.2}$$

[1] In his recent book [**216**], Gérald Tenenbaum explains at length why the word "friable" is more appropriate than the word "smooth" to describe a number without large prime factors.

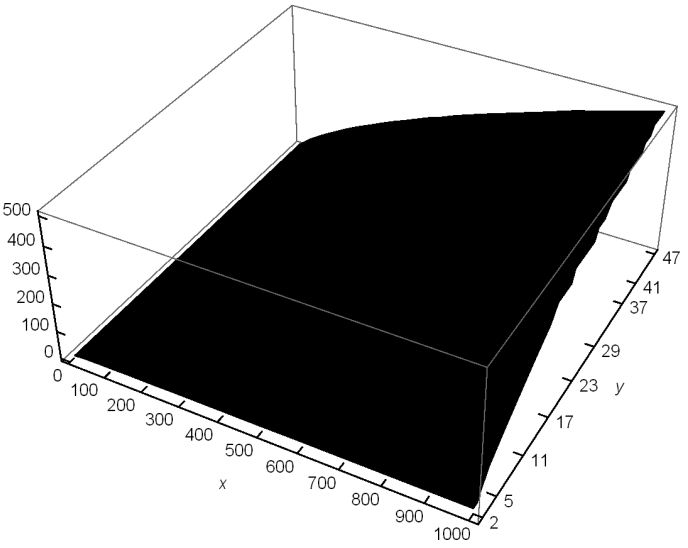
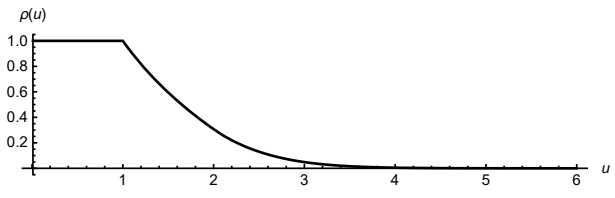


FIGURE 21.1. The function $\Psi(x, y)$ for $2 \le x \le 1000$ and $2 \le y \le 47$

(for a proof of inequality (21.2), see Theorem 9.5 in the book of De Koninck and Luca [**60**]). In 1930, the Swedish actuary Karl Dickman (1861-1947), in studying the distribution of those integers having no large prime factors, introduced [**65**] a function which would turn out to be extremely useful for describing the asymptotic behavior of $\Psi(x, y)$. This function now called the *Dickman function* is defined as the unique continuous function $\rho : [0, \infty) \to (0, 1]$ which is differentiable on $[1, \infty)$ and satisfies

$$\begin{aligned} &\rho(u) = 1 && \text{for} \quad 0 \le u \le 1, \\ &u\rho'(u) + \rho(u-1) = 0 && \text{for} \quad u \ge 1. \end{aligned}$$

As the following graph and table seem to indicate, the Dickman function $\rho(u)$ decreases very rapidly as u increases.



u	$\rho(u)$
1	1.00000000
2	0.30685282
3	0.04860838
4	0.00491092
5	0.00035472
6	0.00001965
7	0.00000087

In fact, one can show that $\rho(u) = \dfrac{1}{u^{u(1+o(1))}}$ as $u \to \infty$ (see Corollary 9.18 in the book of De Koninck and Luca [**60**]).

The very first interesting estimate regarding the behavior of $\Psi(x, y)$ goes back to 1951 as Nicolaas Govert de Bruijn [**31**] proved that, with $u := \log x / \log y$ and $\varepsilon > 0$ being an arbitrarily small number,

$$\Psi(x, y) = x\rho(u) \left(1 + O\left(\frac{\log(u+1)}{\log y}\right)\right) \tag{21.3}$$

holds for all $y > \exp\{(\log x)^{5/8+\varepsilon}\}$. In 1986, Adolf Hildebrand [**114**] improved the range of validity of the estimate (21.3) by showing that it holds for all $y > \exp\{(\log\log x)^{5/3+\varepsilon}\}$.

Can there be any further improvements regarding the range of validity of (21.3)? Perhaps, but this task would surely prove to be a difficult one. Indeed, in 1984, Hildebrand [**113**] proved that estimate (21.3) will hold uniformly for all $y > (\log x)^{2+\varepsilon}$ if and only if the Riemann Hypothesis is true.

For small values of y, the estimate of Granville [**96**]

$$\Psi(x, \log^A x) = x^{1-1/A+O(1/\log\log x)} \qquad \text{for any } A > 1$$

is also of great interest. Indeed, while (21.3) provides an estimate for the function $\Psi(x, y)$ when y is large with respect to x, Granville's estimate complements it by providing an approximation of $\Psi(x, y)$ that holds for smaller values of y.

The next theorem provides an easily proved estimate of $\Psi(x, y)$ which has the advantage of holding in the whole range $2 \le y \le x$. It is based on the famous *Buchstab identity*, a 1937 result of A.A. Buchstab [**33**],

$$\Psi(x, y) = \Psi(x, z) - \sum_{y<p\le z} \Psi\left(\frac{x}{p}, p\right) \qquad (x \ge 1,\ z \ge y > 0) \tag{21.4}$$

(see Problem 21.1).

THEOREM 21.1. *Uniformly for $2 \le y \le x$ and $u = \log x/\log y$, we have*

$$\Psi(x, y) = x\rho(u) + O\left(\frac{x}{\log y}\right). \tag{21.5}$$

PROOF. We only provide a sketch of the proof. We only need to prove (21.5) for $u \le \log\log y$. Indeed, if we assume the contrary, the error term $O\left(\dfrac{x}{\log y}\right)$ would be of larger order than the main term $x\rho(u)$, in which case estimate (21.5) follows trivially from inequality (21.2). The proof now goes by induction on $k = \lfloor u \rfloor \le \log\log y$. First, consider the case $1 \le u \le 2$. Using the Buchstab identity (21.4) with $z = x$, we get

$$\Psi(x, y) = \lfloor x \rfloor - \sum_{y<p\le x} \left\lfloor \frac{x}{p} \right\rfloor = x(1 - \log u) + O(\pi(x)) = x\rho(u) + O\left(\frac{x}{\log x}\right).$$

Since $y \le x$, the result follows. Using the induction hypothesis then completes the proof of Theorem 21.1. □

Unfortunately, the error term in the estimate of Theorem 21.1 can be as large as the main term (for instance for $y = x^\alpha$ for any real $\alpha \in (0, 1)$). This is not the case for the estimate presented in the next theorem.

THEOREM 21.2. *Given $2 \le y \le x$, let $u := \log x/\log y$. Then,*

$$\Psi(x, y) = (1 + o(1))x\,\rho(u) \qquad (x \to \infty).$$

For a proof, see Theorem 9.3 in the book of De Koninck and Luca [**60**].

It follows from this theorem and from the table giving various values of $\rho(u)$ (see page 128) that roughly 30.6% of integers n have their largest prime factor smaller than or equal to $\sqrt{n}$, while approximately 4.86% have their largest prime

factor smaller than or equal to $n^{1/3}$. Also, as observed by Selfridge and Wunderlich [**199**], one can show that the median value $M(x)$ of $P(n)$ as n runs from 2 to $\lfloor x \rfloor$ is $x^{1/\sqrt{e}+o(1)}$ as $x \to \infty$, that is around $x^{0.6065}$ (see Problem 21.4). Interestingly, when asked by Greg Martin if $M(x) < x^{1/\sqrt{e}}$ for all sufficiently large x, Eric Naslund [**169**] answered in the affirmative by showing that, given any fixed integer $k \geq 1$,

$$M(x) = e^{\frac{\gamma-1}{\sqrt{e}}} x^{1/\sqrt{e}} \left(1 + \frac{d_1}{\log x} + \cdots + \frac{d_k}{\log^k x} + O\left(\frac{1}{\log^{k+1} x}\right)\right),$$

where the d_i's are computable constants.

The curious reader might be interested in the survey paper of Hildebrand and Tenenbaum [**115**] or the more recent one of Granville [**96**]. Both provide a historical account of the various improvements regarding the behavior of the function $\Psi(x, y)$ but with different perspectives. Another survey of friable numbers and their numerous applications in number theory is the very nice paper of Cécile Dartyge [**51**].

21.2. The most frequent value of the largest prime factor in a given range

Given a real number $x > 1$, what is the most frequent value of the largest prime factor $P(n)$ as n runs in the interval $[1, x]$? More precisely, if we set

$$f(x, p) := \#\{n \leq x : P(n) = p\},$$

then, for a fixed $x > 1$, for which prime p does the function $f(x, p)$ reach its maximum value?

First observe that

$$f(x,p) = \sum_{\substack{n \leq x \\ P(n)=p}} 1 = \sum_{\substack{mp \leq x \\ P(m) \leq p}} 1 = \sum_{\substack{m \leq x/p \\ P(m) \leq p}} 1 = \Psi\left(\frac{x}{p}, p\right).$$

In 1994, the first author [**54**] showed that the maximum value of $f(x, p)$, for large x, is obtained at some prime $p = p(x)$ satisfying

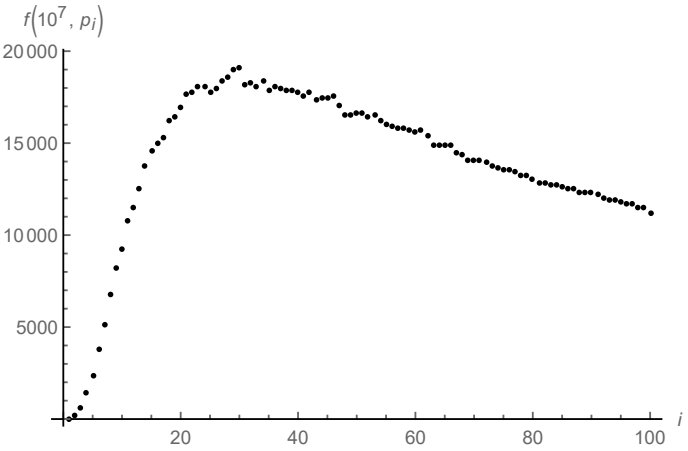
$$p = \exp\{(1 + o(1))\sqrt{(1/2)\log x \log\log x}\} \qquad (x \to \infty),$$

a result later improved by Nathan McNew [**159**], who showed that

$$p(x) = \exp\left\{\sqrt{\nu(x)\log x} + \frac{1}{4}\left(1 - \frac{\nu(x) - 3}{2\nu(x)^2 - 3\nu(x) + 1}\right)\right\} \times \left(1 + O\left(\left(\frac{\log\log x}{\log x}\right)^{1/4}\right)\right), \tag{21.6}$$

where $\nu(x)$ is the solution to the equation $e^{\nu(x)} = 1 + \sqrt{\nu(x)\log x} - \nu(x)$ and is given by

$$\nu(x) = \frac{1}{2}\log\log x + \frac{1}{2}\log\log\log x - \frac{1}{2}\log 2 + o(1) \qquad (x \to \infty).$$



THE GRAPH OF $f(10^7, p_i)$ FOR $i = 1, 2, \ldots, 100$

A quick glance at the above graph seems to indicate that the function $f(x, p)$ is not unimodular[2]. However, in a 2001 paper [**62**], De Koninck and Sweeney showed that this function is increasing for $p \in [2, \sqrt{\log x}]$ and decreasing for $p \in [\sqrt{x}, x]$, while it clearly oscillates near its maximal value.

A prime number p_0 is said to be *popular* if there exists an interval $[2, x]$ such that in that interval, the function $f(x, p)$ attains its maximal value at $p = p_0$. The first elements of the set of popular primes are

$$3, 5, 7, 13, 19, 23, 31, 43, 47, 73, 83, 109, 113, 199, 283, 467, 661, 773, 887, 1109, \ldots .$$

One will notice that each popular prime p, starting with $p = 43$, is followed by several composite numbers. Interestingly, in the same paper [**159**], McNew showed that a positive proportion of the primes are not popular.

Table 21.1 indicates at which prime p the function $f(x, p)$ reaches its maximum value as x runs through powers of 10.

TABLE 21.1. Most popular primes

x	most popular prime $p \in [2, x]$
10	2, 3
10^2	5
10^3	7
10^4	19
10^5	31
10^6	73
10^7	113
10^8	199

[2]A *unimodular curve* is one which has only one local maximum.

21.3. The exponents in the multiplicative structure of integers

A positive integer n is said to be squarefree if $p \mid n$ implies that $p^2 \nmid n$. Our first observation is that roughly 60% of the positive integers (more precisely a proportion of $6/\pi^2 = 0.6079\ldots$) are squarefree. To show this, we only need to prove that

$$\frac{1}{x}\sum_{n\le x}|\mu(n)| = \frac{1}{\zeta(2)} + o(1) \qquad \text{as } x \to \infty. \tag{21.7}$$

To do so, first observe that, for $s > 1$,

$$\sum_{n=1}^{\infty}\frac{|\mu(n)|}{n^s} = \prod_p\left(1+\frac{1}{p^s}\right) = \frac{\prod_p\left(1-\frac{1}{p^{2s}}\right)}{\prod_p\left(1-\frac{1}{p^s}\right)} = \frac{\zeta(s)}{\zeta(2s)},$$

and then apply Wintner's theorem (see page 310) to the function $f(n) = |\mu(n)|$, in which case (21.7) follows immediately.

Our second observation is that the average value of the exponents α_i in the canonical representation of an integer n is 1. This is a consequence of the following result of the first author [**53**]:

$$\frac{1}{x}\sum_{2\le n\le x}\frac{\Omega(n)}{\omega(n)} = 1 + \frac{c+o(1)}{\log\log x} \qquad \text{as } x \to \infty,$$

where $c = \displaystyle\sum_p \frac{1}{p(p-1)}$.

Examining the canonical representation of integers n, one might be curious about the average size of its smallest exponent and that of its largest exponent, that is the average size of

$$h(n) := \min\{\alpha : \text{ the exists } p \text{ such that } p^\alpha \| n\}$$

and

$$H(n) := \max\{\alpha : \text{ the exists } p \text{ such that } p^\alpha \| n\}.$$

This was examined in 1969 by Ivan Niven [**172**] as he showed that, as $x \to \infty$,

$$\begin{aligned} \frac{1}{x}\sum_{n\le x} h(n) &= 1 + \frac{c+o(1)}{\sqrt{x}}, \quad \text{where } c = \zeta(3/2)/\zeta(2), \\ \frac{1}{x}\sum_{n\le x} H(n) &= B + o(1), \end{aligned} \tag{21.8}$$

where $B := 1 + \displaystyle\sum_{k=2}^{\infty}\left(1 - \frac{1}{\zeta(k)}\right) \approx 1.705.$

Here, we choose to provide the proof of (21.8). For this first observe that, for each integer $k \ge 2$,

$$S_k(x) := \sum_{\substack{n\le x\\ n \ k-\text{free}}} 1 = \frac{x}{\zeta(k)} + O(x^{1/k}), \tag{21.9}$$

a very old estimate obtained in 1885 by Gegenbauer [**92**]. Here, by a *k-free integer*, we mean one which is not divisible by the k-th power of any prime. Now, set

$$E_k(x) := S_k(x) - \frac{x}{\zeta(k)} \qquad (k \geq 2)$$

and observe that

$$\sum_{\substack{n \leq x \\ H(n)=k-1}} 1 = S_k(x) - S_{k-1}(x) \qquad (k \geq 2).$$

Let $J = J(x) := \left\lfloor \dfrac{\log x}{\log 2} \right\rfloor$, observing that $S_{J+1}(x) = \lfloor x \rfloor$. For convenience, we set $S_1(x) = 1$. Using (21.9), we can then write

$$\begin{aligned}
\sum_{n \leq x} H(n) &= \sum_{k=2}^{J+1} (k-1) \sum_{\substack{n \leq x \\ H(n)=k-1}} 1 \\
&= \sum_{k=2}^{J+1} (k-1)(S_k(x) - S_{k-1}(x)) \\
&= J\lfloor x \rfloor + \sum_{k=2}^{J} (k-1) S_k(x) - \sum_{k=1}^{J} k S_k(x) \\
&= x + x \sum_{k=2}^{J} \left(1 - \frac{1}{\zeta(k)}\right) - \sum_{k=2}^{J} E_k(x) - 1. \qquad (21.10)
\end{aligned}$$

Using the fact that

$$1 - \frac{1}{\zeta(k)} < \frac{1}{2^{k-1}} \qquad (k \geq 2),$$

we have that

$$\begin{aligned}
\sum_{k=2}^{J} \left(1 - \frac{1}{\zeta(k)}\right) &= \sum_{k=2}^{\infty} \left(1 - \frac{1}{\zeta(k)}\right) - \sum_{k=J+1}^{\infty} \left(1 - \frac{1}{\zeta(k)}\right) \\
&= B - 1 + O\left(\sum_{k=J+1}^{\infty} \frac{1}{2^{k-1}} \right) \\
&= B - 1 + O\left(\frac{1}{2^{J-1}} \right) \\
&= B - 1 + O\left(\frac{1}{x} \right),
\end{aligned}$$

which substituted in (21.10) yields (21.8).

Our final observation regarding the exponents in the canonical representation of an integer n is that the exponents larger than 1 are generally attached to its smallest prime factors, that is, "most of the time" the prime divisors p of n such that $p^2 \mid n$ are very small. This is reflected in the following result.

LEMMA 21.3. *The number of positive integers $n \leq x$ such that $p^2 \mid n$ for some $p > \log\log n$ is $o(x)$ as $x \to \infty$.*

PROOF. Let S be the set of those positive integers n which have a prime divisor p such that $p^2 \mid n$ and $p > \log\log n$, and let $S(x) := \#\{n \le x : n \in S\}$. To prove our claim, we only need to prove that $S(x) = o(x)$ as $x \to \infty$. Clearly, the number of those $n \in S$ such that $n < x/\log x$ is at most $x/\log x = o(x)$. Hence, we only need to consider those $n \in I_x := [x/\log x, x]$. For $n \in I_x$, we have

$$\log\log n \ge \log\log(x/\log x) = \log\log x + \log\left(1 - \frac{\log\log x}{\log x}\right) > \frac{1}{2}\log\log x, \tag{21.11}$$

provided that x is sufficiently large, say $x \ge x_1$. Now, because of (21.11), each $n \in S \cap I_x$ (with $x > x_1$) has a prime divisor p such that $p^2 \mid n$ and $p > \log\log n > \frac{1}{2}\log\log x$. It follows that, for $x > x_1$,

$$\begin{aligned} \#(S \cap I_x) &\le \sum_{p > \frac{1}{2}\log\log x} \sum_{\substack{n \le x \\ p^2 \mid n}} 1 = \sum_{p > \frac{1}{2}\log\log x} \left\lfloor \frac{x}{p^2} \right\rfloor \le \sum_{p > \frac{1}{2}\log\log x} \frac{x}{p^2} \\ &\le x \int_{\frac{1}{2}(\log\log x) - 1}^{\infty} \frac{dt}{t^2} = \frac{x}{\frac{1}{2}(\log\log x) - 1} = o(x) \qquad \text{as } x \to \infty, \end{aligned}$$

which together with the fact that $S(x) \le o(x) + \#(S \cap I_x)$ proves our claim. □

Problems on Episode 21

PROBLEM 21.1. Prove the Buchstab identity (21.4).

PROBLEM 21.2. Show that the Dickman function ρ satisfies the three properties

(i) $\rho(u) = \dfrac{1}{u}\displaystyle\int_{u-1}^{u} \rho(v)\,dv$ for all $u \ge 1$,
(ii) $\rho(u) > 0$ for all $u \ge 0$,
(iii) $\rho'(u) < 0$ for all $u > 1$.

PROBLEM 21.3. Show that $\rho(u) = 1 - \log u$ for $1 \le u \le 2$.

PROBLEM 21.4. Use Theorem 21.2 to show that the median value of $P(n)$ as n runs from 2 to $\lfloor x \rfloor$ is $x^{1/\sqrt{e}+o(1)}$ as $x \to \infty$.

PROBLEM 21.5.* Use Theorem 21.1 to establish that

$$\sum_{n \le x} \log P(n) = Cx\log x + O(x\log\log x),$$

where $C = 1 - \displaystyle\int_1^{\infty} \frac{\rho(v)}{v^2}\,dv = 0.62433$.

PROBLEM 21.6. Given an integer $k \ge 2$, consider the arithmetic function

$$f_k(n) := \begin{cases} 1 & \text{if } n \text{ is } k\text{-free}, \\ 0 & \text{otherwise}, \end{cases}$$

so that in particular, $f_2(n) = |\mu(n)|$ for all $n \in \mathbb{N}$. Prove a result somewhat weaker than the one stated in (21.9), expressly that, for each integer $k \ge 2$,

$$\frac{1}{x}\sum_{n \le x} f_k(n) = \frac{1}{\zeta(k)} + o(1) \qquad \text{as } x \to \infty.$$

PROBLEM 21.7. For each real $\delta > 0$, let

$$A_\delta = \left\{ n : \left| \frac{\omega(n)}{\log\log n} - 1 \right| > \delta \right\}.$$

Prove that the set A_δ is of density zero.

PROBLEM 21.8.* Write the prime factorisation of an integer n as

$$n = P_r(n)P_{r-1}(n)\cdots P_3(n)P_2(n)P(n),$$

where $P_r(n) \le P_{r-1}(n) \le \cdots \le P_3(n) \le P_2(n) \le P(n)$ stands for all the prime factors of n. Prove that the most frequent value of $P_2(n)$, the second largest prime factor of n, is the prime number 3.

PROBLEM 21.9.* In this episode, we proved Niven's estimate

$$\frac{1}{x}\sum_{n\le x} H(n) = 1 + \sum_{k=2}^{\infty}\left(1 - \frac{1}{\zeta(k)}\right) + o(1) \qquad (x \to \infty).$$

Prove that the constant appearing on the right-hand side of this estimate can also be written as $1 - \displaystyle\sum_{m=2}^{\infty} \frac{\mu(m)}{m(m-1)}$.

PROBLEM 21.10. Generalize Lemma 21.3 by showing that, given any function $\phi(n)$ which tends to ∞ as $n \to \infty$, the number of positive integers $n \le x$ such that $p^2 \mid n$ for some $p > \phi(n)$ is $o(x)$ as $x \to \infty$.

EPISODE 29

The Fermat factorisation algorithm

29.1. The fascination with factoring large integers

The factorisation of large integers has always been an intriguing topic. However, for a long time, many mathematicians did not consider this topic as one of the utmost importance. But then, as we will see in Episode 36, starting in the late 1970's, actually with the birth of the RSA cryptography algorithm, seeking efficient techniques for factoring large integers became very important. This explains in part why factoring methods have improved dramatically between 1980 and 2020. Take for instance Mersenne numbers, that is, those numbers $M_p := 2^p - 1$, where p is a prime number. Some three hundred years ago, Mersenne thought that the 76-digit number M_{251} was factorable, but he had no idea how to accomplish this task. For more than 100 years, only the two smallest prime factors of M_{251} were known (see Problem 19.2), as its complete factorisation remained a mystery. In fact, in 1976, since computers were "slow" and because of the inefficiency of the factoring methods of that time, it was believed that more than 10^{20} years of computer time would be necessary to factor M_{251} (see Pomerance [**177**]). Constant progress made with factoring techniques and more powerful computers contributed in accelerating the factorisation of large numbers. As a consequence, as reported in a February 1984 issue of TIME magazine, a team of mathematicians working at the Sandia National Laboratories in Albuquerque were successful in obtaining the complete factorisation of M_{251}; their task took 32 hours using a Cray-1 computer. Today, using a desktop computer and a fairly good a computing software, one can obtain the complete factorisation of M_{251} in less than one minute. Clearly, today's computers are highly more efficient than in 1984, but it is fair to say that the progress made through the creation of some clever factoring algorithms is also remarkable. In this episode and in the following six, we explore how some of these algorithms evolved over time and allowed for the complete factorisation of several large integers.

29.2. The original Fermat method

Pierre de Fermat is the author of a factorisation algorithm that bears his name (many call it the *Fermat factorisation method*) and which consists in using the fact that for any given positive odd integer n, there exist two positive integers a and b such that $n = a^2 - b^2$, in which case $n = (a - b)(a + b)$ gives a non-trivial factorisation of n (provided $a - b \neq 1$).

First of all, let us prove the fact that given an odd composite integer n, one can always find two such integers a and b. Indeed, if $n = rs$ with $1 < r < s$, one can easily check that the numbers $a = (s + r)/2$ and $b = (s - r)/2$ will work. But how does one find two such integers $a > b$ satisfying $n = a^2 - b^2$? Since $n = a^2 - b^2 < a^2$, we have $a > \sqrt{n}$, so that $a \geq \lfloor \sqrt{n} \rfloor + 1$. So, let us start by setting $a = \lfloor \sqrt{n} \rfloor + 1$; if

$a^2 - n$ is a perfect square, say $a^2 - n = b^2$, then we have found a and b as required; otherwise, we choose $a = \lfloor \sqrt{n} \rfloor + 2$, and so on, until we find a positive integer k such that the number $a = \lfloor \sqrt{n} \rfloor + k$ has the property that $a^2 - n$ is a perfect square, which we then write as b^2. This process has an end, in the sense that we will eventually find a number b such that $b^2 = a^2 - n$, because $b = (s - r)/2$ will eventually work.

Programmed with MATHEMATICA, this method can be formulated as follows.

```
a = Floor[Sqrt[n]] + 1; While[!IntegerQ[b = Sqrt[a^2 - n]], a++];
Print[a, " ", b, "⟶ n =", a - b, " × ", a + b]
```

The example provided by Fermat to illustrate his method was for the factorisation of $n = 2\,027\,651\,281$. He computes $\lfloor \sqrt{n} \rfloor = 45\,029$ and starts with $a = 45\,029 + 1 = 45\,030$; since $45\,030^2 - 2\,027\,651\,281 = 49\,619$ is not a perfect square, he moves to $a = 45\,031$, which also fails to produce a perfect square, and so on until he gets to $a = 45\,041$, which yields $b = \sqrt{45\,041^2 - 2\,027\,651\,281} = \sqrt{1\,040\,400} = 1\,020$. Fermat then concludes that

$$\begin{aligned} n &= 2\,027\,651\,281 = 45\,041^2 - 1\,020^2 \\ &= (45\,041 - 1\,020)(45\,041 + 1\,020) = 44\,021 \cdot 46\,061. \end{aligned}$$

29.3. The number of steps in the Fermat method

Is Fermat's method really efficient ? To answer this question, let us compute the number of basic operations required to run the Fermat method. By a basic operation, we mean addition, subtraction, multiplication, division, raising to a power and extracting the square root. Instead of talking of basic operations, we will often use the term "steps". We will even say that an algorithm is "fast" if it can be executed in a few steps. Now, assume that $n = d_1 d_2$ is an odd composite integer which is not a perfect square, where d_1 is the largest divisor of n not exceeding $\sqrt{n}$ and $d_2 = n/d_1$; we call them the *middle divisors* of n. One can show that the number k of steps required to factor n using the Fermat factorisation method is exactly

$$k = \frac{d_1 + d_2}{2} - \left\lfloor \sqrt{d_1 d_2} \right\rfloor, \tag{29.1}$$

that is, essentially the difference between the arithmetic mean and the geometric mean of the divisors d_1 and d_2. Indeed, as we saw above,

$$n = d_1 d_2 = a^2 - b^2, \qquad \text{where} \quad a = \frac{d_2 + d_1}{2} \quad \text{and} \quad b = \frac{d_2 - d_1}{2}. \tag{29.2}$$

Running the algorithm consists in searching for the smallest integer $k \geq 1$ such that

$$\sqrt{\left(\underbrace{\lfloor \sqrt{n} \rfloor + k}_{a} \right)^2 - n} = \text{ an integer.}$$

Since $\lfloor \sqrt{n} \rfloor + k = a$ implies that $k = a - \lfloor \sqrt{n} \rfloor$, (29.1) clearly follows from (29.2).

29.4. Accelerating the Fermat algorithm

It follows from (29.1) that the time required to factor an integer n using Fermat's algorithm will be short if its middle divisors are close to each other, that is, close to $\sqrt{n}$. Indeed, assume that the middle divisors $d_1 < d_2$ of n are such that the distance $\Delta = d_2 - d_1$ which separates them satisfies $\Delta < d_1$ and if k stands for the number of steps required to factor n using the Fermat method, it follows from (29.1) that

$$k < \frac{d_1 + d_1 + \Delta}{2} - \sqrt{d_1(d_1 + \Delta)} + 1 = d_1 + \frac{\Delta}{2} - d_1\sqrt{1 + \frac{\Delta}{d_1}} + 1. \tag{29.3}$$

On the other hand, observe that inequality

$$\sqrt{1+y} > 1 + \frac{y}{2} - \frac{y^2}{8} \qquad \text{holds for all } y \in (0,1). \tag{29.4}$$

Setting $y = \Delta/d_1$ in (29.4), it follows from (29.3) that

$$k < d_1 + \frac{\Delta}{2} - d_1\left(1 + \frac{1}{2}\frac{\Delta}{d_1} - \frac{1}{8}\frac{\Delta^2}{d_1^2}\right) + 1 = \frac{1}{8}\frac{\Delta^2}{d_1} + 1,$$

a number which is "small" when Δ is not too large.

However, if the middle divisors of n are far from each other, then running the algorithm will take more time than trial division. Indeed, suppose for instance that the challenge is to factor a 20-digit integer n, which is in fact the product of a 5-digit prime and a 15-digit prime. Again, if k stands for the number of steps required to factor n using the Fermat method, we then obtain, using (29.1),

$$k > \frac{10^4 + 10^{14}}{2} - \sqrt{n} > \frac{10^{14}}{2} - 10^{10} > 10^{13},$$

whereas using trial division, the number of steps required to factor n will be $< \sqrt{n} < 10^{10}$, implying in this case that trial division is at least one thousand times faster than the Fermat method!

A way to avoid this scenario consists in first performing trial division by small primes. For example, assume that we dare try to factor the 16-digit number $n = 48^9 + 3 = 1\,352\,605\,460\,594\,691$. Naively applying Fermat's method may cause us to abandon after a few million steps. A more clever approach consists in identifying the possible small prime factors of n, namely by verifying divisibility of n by "small" prime numbers, say those less than 10 000, a task which will take less than one second using a computing software. One then discovers that our number n is divisible by 3 and 1 249. The problem now consists in factoring the number

$$n_1 = \frac{n}{3 \times 1\,249} = 360\,983\,576\,353.$$

Applying the method of Fermat to this new number yields

$$n_1 = 587\,201 \times 614\,753$$

after only 157 steps. Gathering our computations, we finally obtain

$$n = 1\,352\,605\,460\,594\,691 = 3 \times 1\,249 \times n_1 = 3 \times 1\,249 \times 587\,201 \times 614\,753.$$

This is why, if after having taken care of the small prime factors of n, Fermat's method still takes too long to reveal its large prime factors, it is reassuring to learn that there exist other avenues.

Another approach is to apply Fermat's method to a number larger than n itself, in fact to a multiple of n. Take for example the number $n = 54\,641$. Since this number is relatively small, one will obtain its factorisation by using Fermat's algorithm, obtaining $n = 101 \times 541$, and do so in 87 steps, a number which is nevertheless quite large compared with the (small) size of n. However, had we known that one of the prime factors was approximately 5 times the other prime factor, we could have started by multiplying n by 5, thereby allowing the new number $5n$ to have its middle divisors to be about the same size, in which case applying the Fermat method to the number $5n$ would have revealed the factors 505 and 541 in only one step. Then, it only remains to verify which of 505 and 541 captured the artificial factor 5, which is, of course, child's play. Clearly, this is easily done when we know that one of the factors is close to a multiple of another factor, an information not available in advance! Can one nevertheless explore this approach to factor an arbitrary composite integer n? The idea would be to consider the number $n \times r$ for an appropriate choice of r. For example, if $n = pq$ and $r = uv$, we have $nr = pu \times qv$, and if we are lucky, the two new divisors pu and qv (of nr) will be sufficiently close to each other for us to apply Fermat's method with success.

In 1974, using a refinement of this idea, R. Sherman Lehman [**139**] was able to show that one can indeed accelerate the Fermat method and factor an odd integer n in no more than $O(n^{1/3})$ steps.

In 1999, James F. McKee [**158**] also proposed a variant of Fermat's algorithm that provides a factor of an odd integer n in no more than $O(n^{1/4})$ steps.

In 2012, William B. Hart [**108**] introduced a different algorithm which allows one to obtain a factor of an odd integer n in no more than $O(n^{1/3})$ steps. Although less efficient than McKee's algorithm, its interesting feature is its remarkable simplicity. It goes as follows. Start with $i = 1$, compute $s = \left\lceil \sqrt{ni} \right\rceil$ and let $m = s^2 \pmod{n}$; if m is a square, then $\mathrm{GCD}(n, s - \sqrt{m})$ will yield a factor of n. Here, we used for the first time the notation $\lceil y \rceil$ which stands for the smallest integer greater than or equal to y.

Using MATHEMATICA, Hart's program can be written as follows:

```
i=j=1; While[{s=Ceiling[Sqrt[n*i]]; m=Mod[s^2,n]};
!IntegerQ[Sqrt[m]],i++];Print[i-j,"⟶",GCD[n,s-Sqrt[m]]]
```

Here $i - j$ represents the number of steps required to find a factor of n.

For example, applying this program to $n = 799\,819$, one finds the factor 101 (note that $n = 101 \cdot 7919$) in 76 steps, a number indeed smaller than $\lfloor n^{1/3} \rfloor = 98$, compared with 3115 steps using the standard Fermat factorisation method.

Problems on Episode 29

PROBLEM 29.1. Use the Fermat factorisation method to find two proper divisors of 289 751.

PROBLEM 29.2. The Fermat factorisation method guarantees that to each odd integer $n > 1$ there correspond two positive integers a and b such that $n = a^2 - b^2$. Are those two integers unique?

PROBLEM 29.3. Let $n > 1$ be an odd integer which is not a perfect square and let $d_1 < d_2$ be its middle divisors. Show that $\dfrac{d_1 + d_2}{2} - \left\lfloor \sqrt{d_1 d_2} \right\rfloor$ (expressly the right-hand side of (29.1)) is a positive integer.

PROBLEM 29.4. Let n be an integer which is the product of two primes $p < q$ for which $q - p < 2\sqrt{2p}$. Show that n can be factored using the Fermat factorisation method in only one step.

PROBLEM 29.5. Prove that every integer of the form $4k^4 + 1$ can be factored using the Fermat factorisation method at the very first step of the algorithm. Then, use this information to find the complete factorisation of the number $2^{58} + 1$.

PROBLEM 29.6. In order to factor $10^{22} + 1$, first check its divisibility by "small primes", say those below 200, and then apply the Fermat factorisation method to the "reduced number".

PROBLEM 29.7. Obtain the complete factorisation of the 13-digit number $n = (12^{13} - 1)/11$ using the Fermat factorisation method, the Hart method and finally the basic approach of checking divisibility by small primes. Which of these three methods requires the least number of steps?

PROBLEM 29.8. Prove that if the middle divisors d_1 and d_2 of an odd integer n satisfy $d_1 < d_2 < 2d_1$ and if δ is the real number defined implicitly by $\dfrac{d_2}{d_1} = 1 + \delta$, then the number k of steps required to factor n satisfies $k \approx \dfrac{d_1 \delta^2}{8}$.

PROBLEM 29.9. Let n be an odd integer which is the product of two primes whose first half of the digits are the same. Prove that in this case, n can be factored very quickly using the Fermat factorisation method.

EPISODE 34

Algebraic factorisation

34.1. Introduction

Through the previous five episodes, we explored several factorisation algorithms. Most computing softwares use these algorithms to reveal the factorisation of integers, provided these integers are not too large. However, at times, some integers will resist being factored, especially those with hundreds of digits, even though they have an obvious particular algebraic structure. For instance, try factoring the 597-digit number $n = 2^{1980} - 1$ using a computing software. It will certainly come up with some 53 or 54 of its prime factors, but will most likely fail to deliver its largest two, which have 62 and 73 digits, respectively (see Problem 34.24). This is because most computing softwares do not consider the various algebraic representations that a given integer n might have. For instance, in searching for the factorisation of a given integer $n > 1$, one could examine the possibility of expressing it in the form of some polynomial $Q(x, y)$ which can be factored, such as those polynomials of the form $x^{2r+1} \pm y^{2r+1}$ for some positive integer r or perhaps of some other polynomial which can be factored. In this episode, we search for such polynomials.

34.2. Cyclotomic polynomials

Before we find such appropriate reducible polynomials, we introduce a special kind of irreducible polynomial, the family of *cyclotomic polynomials*.

First, for a fixed integer $n \geq 1$, let us consider the equation

$$x^n - 1 = 0. \tag{34.1}$$

One obvious solution to this equation is $x = 1$. However, if $n > 1$, there are other solutions, some of which may be complex numbers. First, let us choose $n = 4$, in which case equation (34.1) is then equivalent to

$$(x^2 - 1)(x^2 + 1) = 0$$

and to

$$(x - 1)(x + 1)(x^2 + 1) = 0, \tag{34.2}$$

which reveals the four solutions of (34.1) in the case $n = 4$, that is,

$$x = 1, \qquad x = -1, \qquad x = i, \qquad x = -i.$$

Given any positive integer n, we define the n-th *cyclotomic polynomial*, which we denote by $\Phi_n(x)$, as the irreducible factor (over $\mathbb{Q}$) of $x^n - 1$ which is not a factor of any polynomial $x^m - 1$ for any positive integer $m < n$. Note that, as we will see later, $\Phi_n(x)$ exists for every $n \in \mathbb{N}$. With this definition, let us see

how we can build the cyclotomic polynomials one by one. For $n = 1$, we have $\Phi_1(x) = x-1$. For $n = 2$, since $x^2-1 = (x-1)(x+1)$ and since $x-1$ has "already been used", we have $\Phi_2(x) = x+1$. For $n = 3$, since $x^3 = (x-1)(x^2+x+1)$, we have $\Phi_3(x) = x^2+x+1$. For $n = 4$, it follows from (34.2) that $\Phi_4(x) = x^2+1$. And so on. Observe that by our definition, we may write

$$\Phi_n(x) = \frac{x^n-1}{\prod\limits_{\substack{d|n\\ d<n}} \Phi_d(x)}, \tag{34.3}$$

from which it follows that

$$\prod_{d|n} \Phi_d(x) = x^n - 1 \qquad (n \geq 1). \tag{34.4}$$

Using the Möbius inversion formula (see page 307), it follows from (34.4) that

$$\Phi_n(x) = \prod_{d|n} (x^d-1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d}-1)^{\mu(d)} \tag{34.5}$$

(see Problem 34.11).

For instance, when $n = 4$, we get

$$\Phi_4(x) = (x-1)^{\mu(4)}(x^2-1)^{\mu(2)}(x^4-1)^{\mu(1)} = \frac{x^4-1}{x^2-1} = x^2+1,$$

which coincides with our first finding for $\Phi_4(x)$. Similarly, using formula (34.5) for successive values of n, we find that the first twelve cyclotomic polynomials are

$$\begin{aligned}
\Phi_1(x) &= x-1,\\
\Phi_2(x) &= x+1,\\
\Phi_3(x) &= x^2+x+1,\\
\Phi_4(x) &= x^2+1,\\
\Phi_5(x) &= x^4+x^3+x^2+x+1,\\
\Phi_6(x) &= x^2-x+1,\\
\Phi_7(x) &= x^6+x^5+x^4+x^3+x^2+x+1,\\
\Phi_8(x) &= x^4+1,\\
\Phi_9(x) &= x^6+x^3+1,\\
\Phi_{10}(x) &= x^4-x^3+x^2-x+1,\\
\Phi_{11}(x) &= x^{10}+x^9+\cdots+x^2+x+1,\\
\Phi_{12}(x) &= x^4-x^2+1.
\end{aligned}$$

By the way, one easily sees that $\Phi_p(x) = x^{p-1}+x^{p-2}+\cdots+x^2+x+1$ for every prime p. It remains to show that each $\Phi_n(x)$ obtained through definition (34.3) is indeed an irreducible polynomial. For this, one can check the nice paper of Weintraub [**230**] where several proofs are given.

It follows from (34.4) that

$$x^n+1 = \frac{x^{2n}-1}{x^n-1} = \prod_{\substack{d|2n\\ d\nmid n}} \Phi_d(x) \qquad (n \geq 1). \tag{34.6}$$

Observe that using (34.4) and (34.6), we immediately obtain the particular identities

$$\begin{aligned} x^{12}-1 &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) \\ &= (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1) \end{aligned} \tag{34.7}$$

and

$$x^{12}+1=\Phi_8(x)\Phi_{24}(x)=(x^4+1)(x^8-x^4+1). \tag{34.8}$$

34.3. Aurifeuillean factorisation

In 1871, the French mathematician Léon-François-Antoine Aurifeuille (1822–1882) obtained the complete factorisation of $2^{58}+1$ (see Problem 34.9) after observing that

$$2^{58}+1=2^{4\cdot 14+2}+1=4\cdot\left(2^{14}\right)^4+1=(2\cdot 2^{28}-2\cdot 2^{14}+1)(2\cdot 2^{28}+2\cdot 2^{14}+1),$$

which is clearly a particular case of the more general identity

$$2^{4k+2}+1=(2^{2k+1}-2^{k+1}+1)(2^{2k+1}+2^{k+1}+1) \qquad (k=1,2,\ldots). \tag{34.9}$$

Such a relation is called an *Aurifeuillean factorisation*. The above identity and similar ones proved to be very helpful in the context of the Cunningham project. The goal of this project (initiated in 1925 by Allan Joseph Champneys Cunningham and Herbert J. Woodall) was to obtain the factorisation of numbers of the form $b^n\pm 1$, where $b=2,3,5,6,7,10,11,12$ and n is a large integer. A brief history of the project is given in the 2004 paper of Wagstaff [**227**]. The book of Brillhart, Lehmer, Selfridge, Tuckerman and Wagstaff [**28**] contains the factorisations of many of the numbers $b^n\pm 1$, and further updated factorisations are constantly added on the web site of the Cunningham project (see [**49**]).

The factorisation of any such number $b^n\pm 1$ can be partly obtained through the relations (34.4) and (34.6). This is why it is often convenient to be able to factor $\Phi_d(x)$ for particular values of d and x. Of much interest is therefore an old paper of Lucas [**149**], where we find the identity

$$\Phi_n(x)=C_n(x)^2-nxD_n(x)^2, \tag{34.10}$$

where both $C_n(x)$ and $D_n(x)$ are polynomials with integer coefficients which are symmetric and monic. For instance, in the case of $n=5$, one can check that the two polynomials $C_5(x)=x^2+3x+1$ and $D_5(x)=x+1$ do verify (34.10) (see Problem 34.15).

Even though $\Phi_n(x)$ is irreducible as a polynomial, an interesting feature regarding identity (34.10) is that if we find an integer x_0 such that nx_0 is a square, the right-hand side of (34.10) becomes a difference of two squares, which immediately yields a proper factorisation of the integer $\Phi_n(x)$.

One might ask how one can obtain those key polynomials $C_n(x)$ and $D_n(x)$ appearing in (34.10). Interestingly, Richard P. Brent [**24**] came up with an efficient algorithm for computing these polynomials in the case where $n\equiv 1 \pmod 4$. Other cases are included in Appendix 7 of the book of Riesel [**184**].

Although cyclotomic polynomials $\Phi_n(x)$ are irreducible over the integers (by definition), if $n=b$ and $x=b^h$, where $b>2$ is a squarefree integer, $h\in\mathbb{N}$, Schinzel [**194**] showed in 1962 that $\Phi_b(b^h)$ can be written as a difference of two squares and

can therefore be factored. Here is a special case of one of Schinzel's results, as stated by Wagstaff [**228**]:

> **Theorem A.** *Let $b > 2$ be a squarefree integer. Then there exist polynomials $C_b(x)$ and $D_b(x)$ with integer coefficients and degrees $\phi(b)/2$ and $\phi(b)/2-1$, respectively, having the following properties. Let h be an odd positive integer. If $b \equiv 1 \pmod 4$, then*
>
> $$\Phi_b(b^h) = C_b(b^h)^2 - b^{h+1} D_b(b^h)^2,$$
>
> *and if $b \equiv 2$ or $3 \pmod 4$, then*
>
> $$\Phi_{2b}(b^h) = C_b(b^h)^2 - b^{h+1} D_b(b^h)^2.$$

To show how one can use Schinzel's Theorem A to factor a particular integer of a suitable form, we choose to factor the numbers $n_1 = 14^{14}+1$ and $n_3 = 14^{14\cdot 3}+1 = 14^{42}+1$. First observe that

$$14^{14h}+1 = \frac{14^{28h}-1}{14^{14h}-1} = \frac{\prod_{d|28}\Phi_d(14^h)}{\prod_{d|14}\Phi_d(14^h)} = \Phi_4(14^h)\Phi_{28}(14^h) = (14^{2h}+1)\Phi_{28}(14^h).$$

In light of Theorem A, we have

$$\begin{aligned} \Phi_{28}(14^h) &= C(14^h)^2 - 14^{h+1} D(14^h)^2 \\ &= (C(14^h) - 14^{\frac{h+1}{2}} D(14^h))(C(14^h) + 14^{\frac{h+1}{2}} D(14^h)), \end{aligned} \tag{34.11}$$

where the polynomials $C(x)$ and $D(x)$ are given (see the book of Riesel [**184**], p. 444) by

$$\begin{aligned} C(x) &= x^6 + 7x^4 + 3x^4 - 7x^3 + 3x^2 + 7x + 1, \\ D(x) &= x^5 + 2x^4 - x^3 - x^2 + 2x + 1. \end{aligned}$$

Using these polynomials $C(x)$ and $D(x)$ (with $x = 14^h$) in (34.11), we obtain that, starting with the case $h = 1$,

$$\begin{aligned} 14^{14}+1 &= (14^2+1)(11391031 - 611745)(11391031 + 611745) \\ &= 197 \cdot 2826601 \cdot 19955461 \\ &= 29^2 \cdot 113 \cdot 197 \cdot 3361 \cdot 176597. \end{aligned}$$

Proceeding in the same manner, we find that

$$14^{42}+1 = 29^2 \cdot 37 \cdot 113 \cdot 197 \cdot 1033 \cdot 1597 \cdot 3361 \cdot 10333 \cdot 176597 \cdot 12471556693 \cdot 15697516297.$$

Similarly one can find the factorisation of $p^p + 1$ for any given prime $p \equiv 3 \pmod 4$. Indeed, first observe that

$$p^p + 1 = \frac{p^{2p}-1}{p^p-1} = \frac{\prod_{d|2p}\Phi_d(p)}{\prod_{d|p}\Phi_d(p)} = \Phi_2(p)\cdot\Phi_{2p}(p) = (p+1)\Phi_{2p}(p).$$

By Theorem A,

$$\Phi_{2p}(p) = C_p(p)^2 - p^2 D_p(p)^2. \tag{34.12}$$

So, assume we want to factor the number $n = 11^{11}+1$. The corresponding polynomials $C_{11}(x)$ and $D_{11}(x)$ (see page 444 in Riesel [**184**]) are

$$C_{11}(x) = x^5 + 5x^4 - x^3 - x^2 + 5x + 1 \quad \text{and} \quad D_{11}(x) = x^4 + x^3 - x^2 + x + 1.$$

Using these polynomials in (34.12), we find that

$$\begin{aligned}\Phi_{2p}(p) &= (p^5+5p^4-p^3-p^2+5p+1)^2-p^2(p^4+p^3-p^2+p+1)^2\\ &= (4p^4-2p^2+4p+1)(2p^5+6p^4-2p^3+6p+1),\end{aligned}$$

which, setting $p=11$, yields

$$\Phi_{22}(11)=58367\times 23\times 89\times 199.$$

From this we conclude that the complete factorisation of $n=11^{11}+1$ is

$$n=2^2\times 3\times 23\times 89\times 199\times 58367. \tag{34.13}$$

34.4. Other identities

As explained by Granville and Pleasants [**97**], one can generalize the Lucas and Schinzel technique by seeking polynomials $g(x)\in\mathbb{Z}[x]$ such that $g(x)\pm 1$ factors over $\mathbb{Z}$, and then substitute values for x to obtain partial factorisations of numbers under investigation in the Cunningham project. For instance, choosing $g(y)=(2y^2)^2$, we then have

$$(2y^2)^2+1=(2y^2+1)^2-(2y)^2=(2y^2-2y+1)(2y^2+2y+1), \tag{34.14}$$

which, letting $y=x^k$, yields the original Aurifeuillean factorisation (34.9).

More generally, setting $g(y)=\pm(ay^2)^\ell$ with $a\neq\pm 1$, we find the identities

$$\frac{(3y^2)^3+1}{3y^2+1} = (3y^2+1)^2-(3y)^2, \tag{34.15}$$

$$\frac{(5y^2)^5-1}{5y^2-1} = (25y^4+15y^2+1)^2-(5y)^2(5y^2+1)^2, \tag{34.16}$$

$$\frac{(7y^2)^7+1}{7y^2+1} = (7y^2+1)^6-(7y)^2(49y^4+7y^2+1)^2. \tag{34.17}$$

We also have the interesting Aurifeuillean factorisation

$$\begin{aligned}\frac{(11y^2)^{11}+1}{11y^2+1} &= (11y^2+1)^2\cdot(11^4y^8+4\cdot 11^3y^6-5\cdot 11^2y^4+4\cdot 11y^2+1)^2\\ &\quad -(11y)^2\cdot(11^4y^8+11^3y^6-11^2y^4+11y^2+1)^2.\end{aligned} \tag{34.18}$$

The right-hand side of (34.18) being a difference of squares, it can be written as

$$\begin{aligned}&(1-11y+55y^2-11^2y^3-11^2y^4+11^3y^5-11^3y^6-11^4y^7+5\cdot 11^4y^8-11^5y^9+11^5y^{10})\\ &\times(1+11y+55y^2+11^2y^3-11^2y^4-11^3y^5-11^3y^6+11^4y^7+5\cdot 11^4y^8+11^5y^9+11^5y^{10}),\end{aligned}$$

an expression one could then use to obtain the factorisation of $11^{11}+1$ in a different manner (see Problem 34.17).

Remark 34.1. As explained in Granville and Pleasants [**97**], given any prime $p\equiv 3 \pmod 4$, the corresponding polynomial $f(y):=\dfrac{(py^2)^p+1}{py^2+1}$ can be written as a difference of two squares (of polynomials). This means that $f(y)$ can be written as the product of two polynomials $f_1(y)$ and $f_2(y)$, each of degree $p-1$. Most computing softwares are designed to quickly expose these two polynomials[1]. This can then be useful to find the complete factorisation of p^p+1 for some large primes

[1] In the next episode, we explain that factorisation of polynomials can be done fairly quickly, that is, in "polynomial time".

$p \equiv 3 \pmod 4$, by simply setting $y = 1$ in equation $f(y) = f_1(y) \times f_2(y)$ (see Problems 34.25 and 34.26).

34.5. Lucas numbers

Another interesting Aurifeuillean factorisation involves *Lucas numbers*. The sequence of Lucas numbers $(L_k)_{k\geq 0}$ is defined by $L_0 = 2$, $L_1 = 1$ and $L_k = L_{k-1} + L_{k-2}$ for each integer $k \geq 2$. This recurrence formula produces the sequence

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, \ldots .$$

The Lucas numbers are connected to the Fibonacci numbers (which are defined by $f_0 = 0$, $f_1 = 1$, $f_k = f_{k-1} + f_{k-2}$ for each $k \geq 2$) through several identities amongst which we find

$$L_k = f_{k-1} + f_{k+1} \quad \text{and} \quad f_k = \frac{L_{k-1} + L_{k+1}}{5} \qquad (k \geq 1).$$

According to *Binet's Fibonacci number formula*,

$$f_n = \frac{1}{\sqrt{5}}\,(\alpha^n - \beta^n) \qquad (n = 0, 1, 2, \ldots), \tag{34.19}$$

where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$ (see Problem 34.18). An analogous formula can be established for the Lucas numbers, giving $L_n = \alpha^n + \beta^n$ valid for all integers $n \geq 0$. Using these formulas for f_n and L_n one can establish the relation

$$f_{2n} = f_n \cdot L_n \qquad (n \geq 0) \tag{34.20}$$

(see Problem 34.20). An interesting Aurifeuillean factorisation involving these two sequences comes from the identity

$$L_{10k+5} = L_{2k+1} \cdot \left(5f_{2k+1}^2 - 5f_{2k+1} + 1\right) \cdot \left(5f_{2k+1}^2 + 5f_{2k+1} + 1\right) \qquad (k \geq 0) \tag{34.21}$$

(see Problem 34.21).

Problems on Episode 34

Problem 34.1. Why is $n^4 + 324$ a composite number for each integer $n \geq 1$?

Problem 34.2. Let $m \geq 4$ be an even integer and let $a \geq 2$ be an integer. Prove that

$$\frac{m^a}{2} + \frac{m}{2} - 1$$

is a composite number.

Problem 34.3.* Prove that there exist infinitely many pairs of positive integers $\{m, n\}$ satisfying the two conditions

(1) m and n have the same prime factors,
(2) $m + 1$ and $n + 1$ have the same prime factors.

Problem 34.4. Prove that the sequence $2^{2^n} + 3$, $n = 1, 2, \ldots$, contains infinitely many composite numbers.

Problem 34.5. Prove that $2^{2^6} + 15$ is a composite number.

Problem 34.6. Use the identity $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ and the fact that $2071 = 7^3 + 12^3$ to obtain the complete factorisation of 2 071.

PROBLEM 34.7. Use the fact that $3\,080\,802\,816 = 81^3 + 1455^3 = 456^3 + 1440^3 = 904^3 + 1328^3$ to find its complete factorisation.

PROBLEM 34.8. Show that the polynomial $4x^4 + y^4$ can always be factored and use this result to find the complete factorisation of the number $4 \times 10^8 + 75^4$.

PROBLEM 34.9. Find the complete factorisation of $2^{58} + 1$.

PROBLEM 34.10. Use formula (34.5) to prove that the degree of the polynomial $\Phi_n(x)$ is $\varphi(n)$.

PROBLEM 34.11. Apply the Möbius inversion formula to the identity

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

to show that, for each $n \in \mathbb{N}$,

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} \qquad (n \geq 1).$$

PROBLEM 34.12. Use formula (34.13) to write explicitly the cyclotomic polynomial $\Phi_{105}(x)$.

PROBLEM 34.13. Show that, for each $n \in \mathbb{N}$,

$$\Phi_n(x) = x^{\varphi(n)} \prod_{d|n} \left(1 - \frac{1}{x^d}\right)^{\mu(n/d)}.$$

PROBLEM 34.14. Use formula (34.7) to factor the number $8^{12} - 1$ and formula (34.8) to factor the number $9^{12} + 1$.

PROBLEM 34.15. Make good use of relation (34.10) to quickly obtain the factorisation of the number $45^5 - 1$.

PROBLEM 34.16. Use identity (34.17) to obtain the factorisation of $7^7 + 1$.

PROBLEM 34.17. Use identity (34.18) with $y = 1$ to obtain the factorisation of $11^{11} + 1$.

PROBLEM 34.18. First establish that the numbers

$$\alpha = \frac{1 + \sqrt{5}}{2} \qquad \text{and} \qquad \beta = \frac{1 - \sqrt{5}}{2}$$

satisfy $1 + \alpha = \alpha^2$ and $1 + \beta = \beta^2$, and then use induction to prove Binet's formula (34.19).

PROBLEM 34.19. Let $(L_k)_{k\geq 0}$ and $(f_k)_{k\geq 0}$ stand for the Lucas and Fibonacci sequences, respectively. Prove the identity

$$f_{k-3} + f_{k+3} = 2L_k \qquad (k \geq 3).$$

PROBLEM 34.20. Prove that $f_{2n} = f_n \cdot L_n$ for each integer $n \geq 0$ (formula (34.20)) and deduce from the particular case $n = 4$ that $987 = 21 \times 47$.

PROBLEM 34.21. Prove formula (34.21) and use it to establish the complete factorisation of $L_{35} = 20\,633\,239$.

PROBLEM 34.22. Given a prime $p>2$, consider the number $n=(p^p+1)/(p+1)$. Show that each prime factor $q>3$ of n such that $(q,p+1)=1$ is of the form $q=2kp+1$ for some positive integer k.

PROBLEM 34.23. Use the result of Problem 34.22 to find the complete factorisation of the 32-digit number $23^{23}+1$.

PROBLEM 34.24.* Using a computer and appropriate algebraic identities, find the complete factorisation of $n=2^{1980}-1$, a number with 65 distinct prime factors, the largest two having 62 and 73 digits, respectively.

PROBLEM 34.25.** In light of Remark 34.1, find the complete factorisation of the 361-digit number $n=163^{163}+1$.

PROBLEM 34.26.* * In light of Remark 34.1, can one find the largest prime factor of the 3426-digit number $n=1123^{1123}+1$?

PROBLEM 34.27. How would you go about obtaining the complete factorisation of the number 1 004 006 004 001 with only pen and paper?

PROBLEM 34.28. Prove that if $k=2^r$, with $r\in\mathbb{N}$, then, provided n is sufficiently large, all numbers $k\cdot 2^{2^n}+1$ are composites.

PROBLEM 34.29. Assume that four positive integers a,b,c,d are such that $ab=cd$. Explain why the number $a^2+b^2+c^2+d^2$ is necessarily composite and use your technique to find the factorisation of $1292^2+1330^2+1530^2+1575^2$.

PROBLEM 34.30.* Show that the only set of four distinct primes $\{p_1,p_2,p_3,p_4\}$ such that

$$p_1p_2p_3p_4 \mid (2p_1-1)(2p_2-1)(2p_3-1)(2p_4-1)$$

is the set $\{19,29,37,73\}$.

PROBLEM 34.31.* For a prime p, define $S_1(p)$ as the successor set of p containing all the prime divisors of $p+2$. For example, $S_1(2)=\{2\}$, $S_1(3)=\{5\}$ and $S_1(13)=\{3,5\}$. Also set $S_2(p):=\cup_{q\in S_1(p)}S_1(q)$, so that $S_2(p)$ can be seen as the successor of the successor set of p. For example, $S_2(2)=\{2\}$, $S_2(3)=7$ and $S_2(13)=\{5,7\}$. For each integer $k\geq 3$, we set

$$S_k(p):=\cup_{q\in S_{k-1}(p)}S(p).$$

Finally define $S_\infty:=\cup_{k\geq 1}S_k(p)$. For instance $S_\infty(2)=\{2\}$ and $S_\infty(29)=\{3,5,7,11,13,31\}$. Find all the primes p such that $p\in S_\infty(p)$.

EPISODE 37

The present and future life of primes

The number of open problems concerning prime numbers increases almost daily. In previous episodes, we examined several of these. For instance, we have seen that no proofs yet exist where any one of the families of twin primes, Mersenne primes, perfect numbers or Wieferich primes is infinite. Prime number theory contains many more open problems that will keep mathematicians very busy for centuries. Here, we only state a few of our favorite open questions, some perhaps unknown to the reader. We also mention recent developments in number theory relying on techniques beyond the scope of this book and discuss how the evolution of computers might reshape the future of cryptography and factorisation algorithms.

37.1. Conjectures on the density of special families of primes

37.1.1. The prime k-tuples conjecture. We start with a natural extension of the twin prime conjecture and of the infinitude of prime clusters (see Episode 16), first stated by L.E. Dickson [**66**] in 1904.

CONJECTURE 37.1 (Prime k-tuples conjecture). Let $a_1, a_2, \ldots, a_k$ and b_1,b_2,..., b_k be integers such that $a_i \geq 1$ and $(a_i, b_i) = 1$ for $i = 1, 2, \ldots, k$ and such that for every prime $p \leq k$, there exists a positive integer n such that none of the integers $a_i n + b_i$ for $i = 1, 2, \ldots, k$ is divisible by p. Then there exists an infinite number of positive integers n for which $a_i n + b_i$ is prime for $i = 1, 2, \ldots, k$.

This conjecture, if true, would have numerous applications. A simple one is presented in Problem 37.7.

37.1.2. The Bunyakovsky conjecture. It is conjectured that the sequence $(n^2+1)_{n\geq 1}$ contains infinitely many primes, and in fact numerical evidence supports that claim. Now, observe that the polynomial $x^2 + 1$ is irreducible over $\mathbb{Z}$. Hence, somehow it seems natural to make the same claim about any irreducible polynomial. This was done in 1857 by the Russian mathematician Viktor Bunyakovsky [**34**].

CONJECTURE 37.2 (Bunyakovsky). Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of positive degree and with positive leading coefficient such that the greatest common divisor of $f(1), f(2), \ldots$ is 1. Then there exist infinitely many values of n for which $f(n)$ is prime.

The condition "the greatest common divisor of $f(1), f(2), \ldots$ must be 1" is necessary. Indeed, consider the polynomial $f(x) := x^2 + x + 2$; even though it is irreducible, each of the numbers $f(1), f(2), f(3), \ldots$ is even.

If the Bunyakovsky conjecture is true, then any given cyclotomic polynomial $\Phi_k(x)$, with $k \geq 2$, is such that the sequence $\Phi_k(1), \Phi_k(2), \ldots$ contains infinitely many primes (see Problem 37.4).

The Bunyakovsky conjecture also has unexpected applications. One of them is related to the multiplicative structure of consecutive integers. Let $F(3,2)$ be the set of those integers $n > 2$ such that $P(n)^3 \mid n$ and $P(n+1)^2 \mid n+1$. One can check that the ten smallest elements of $F(3,2)$ are 8, 6859, 12167, 101250, 328509, 453962, 482447, 536238, 598950 and 5619712. Most likely the set $F(3,2)$ is infinite. However, this has not been proved. Recently, De Koninck and Moineau [**61**] showed that if the Bunyakovsky conjecture is true, then $F(3,2)$ is indeed infinite. To show this, they first considered the identity

$$(2m^3+1)^2 - 1 = 4m^3(m+1)(m^2-m+1) \qquad (m = 1, 2, \ldots). \tag{37.1}$$

It is clear that if $m = p$, a prime, and if the largest prime factor of $p^2 - p + 1$ is less than p, then it follows from (37.1) that $n = 4p^3(p^3+1) \in F(3,2)$. Now, it so happens that if the Bunyakovsky conjecture holds, then there exist infinitely many positive integers k such that $9k^2 + 6k + 2$ is prime. For each such k, write $p = 9k^2 + 6k + 2$, in which case $p - 1 = (3k+1)^2$. Since $p \equiv 2 \pmod 3$, we have that $p + (3k+1) \equiv 0 \pmod 3$. We may therefore write

$$p^2 - p + 1 = (p - \sqrt{p-1})(p + \sqrt{p-1}) = 3(p - (3k+1))\frac{p + (3k+1)}{3}.$$

Clearly $p - (3k+1) < p$. On the other hand,

$$\frac{p + (3k+1)}{3} = \frac{1}{3}(p + \sqrt{p-1}) < p,$$

thereby implying that $P(p^2 - p + 1) < p$, thus completing the proof that the set $F(3,2)$ is infinite.

Similarly, it can be shown that if the Bunyakovsky conjecture is true, then the set

$$F(4,2) := \{n \in \mathbb{N} : P(n)^4 \mid n \text{ and } P(n+1)^2 \mid n+1\} \tag{37.2}$$

is infinite (see Problem 37.6).

37.1.3. Hypothesis H (or the Schinzel Hypothesis). The following is a generalization of both the prime k-tuples conjecture and the Bunyakovsky conjecture, which was first stated in 1958 by A. Schinzel and W. Sierpiński [**195**].

Conjecture 37.3 (Hypothesis H). Let $f_1(x), \ldots, f_\ell(x)$ be ℓ irreducible polynomials with integer coefficients and positive leading coefficient. Assume that there are no integers > 1 dividing the product $f_1(n) \cdots f_\ell(n)$ for all positive integers n. Then, there exist infinitely many positive integers m such that all the numbers $f_1(m), \ldots, f_\ell(m)$ are simultaneously primes.

This conjecture, if it were true, would imply that there are infinitely many *Ruth-Aaron numbers*, namely those positive integers n such that $\beta(n) = \beta(n+1)$, where $\beta(n)$ stands for the sum of the prime factors of n taken with multiplicity, that is, $\beta(n) = \sum_{p^\alpha \| n} \alpha p$. For instance the number $n = 714$ is such a number since $\beta(714) = \beta(715) = 29$. The name "Ruth-Aaron" was chosen by Carl Pomerance in honor of the baseball players Babe Ruth and Hank Aaron, as Ruth's career regular-season home run total was 714, a record which Aaron eclipsed on April 8, 1974. That same year, Nelson, Penney and Pomerance [**170**] showed that if the four numbers $s = 2k+1$, $p = 8k+5$, $q = 48k^2+24k-1$ and $r = 48k^2+30k-1$ are all primes, then, by choosing $n = pq$, we get that $n+1 = 4sr$ so that $\beta(n) = \beta(n+1) = 48k^2+32k+4$,

implying that n is a Ruth-Aaron number. For instance, choosing $k = 3$ produces the primes $s = 7$, $p = 29$, $q = 503$ and $r = 521$, which reveals the Ruth-Aaron number $n = 14\,587$ with $\beta(n) = \beta(n+1) = 532$. Now, Hypothesis H guarantees that the above numbers s, p, q, r are simultaneously primes infinitely often. Incidently, one could also ask how many Ruth-Aaron numbers there are below a given number x. In a paper written in memory of Paul Erdős, Carl Pomerance [**178**] showed that the number $N(x)$ of Ruth-Aaron numbers not exceeding x is $O(x/\log^2 x)$ and suggests that for any given integer $r \geq 2$, we have $N(x) = O(x/\log^r x)$.

One could also consider the analogous function $\beta_0(n)$ which stands for the sum of the distinct prime factors of n, that is, $\beta_0(n) = \sum_{p|n} p$. Observe that $\beta_0(n) = \beta(n)$ if n is squarefree. If we were to redefine *Ruth-Aaron numbers* as those numbers n such that $\beta_0(n) = \beta_0(n+1)$, the problem of establishing whether or not there exist infinitely many such numbers would be just as difficult. For more on this question, see Problem 37.7 or the very interesting nine-minute YouTube presentation of Ruth-Aaron numbers by Carl Pomerance.

37.1.4. The Bateman-Horn conjecture. In 1962, P.T. Bateman and R.A. Horn [**15**] formulated the following quantified form of Hypothesis H.

CONJECTURE 37.4 (Bateman-Horn). Given k polynomials $f_1, \ldots, f_k \in \mathbb{Z}[x]$ such that $f_i(x) > 0$ for $i = 1, \ldots, k$ and all $x > 0$, assume that each of these polynomials is irreducible over $\mathbb{Z}$ and that pairwise they do not differ by a constant. Then, there exists a positive constant $C = C(f_1, \ldots, f_k)$ such that the number $N(x)$ of positive integers $n \leq x$ for which the k numbers $f_1(n), \ldots, f_k(n)$ are simultaneously primes satisfies

$$N(x) = (C + o(1)) \int_2^x \frac{dt}{\log^k t} \qquad (x \to \infty).$$

In their paper [**15**], Bateman and Horn provide the following explicit form of the conjectured constants:

$$C(f_1, \ldots, f_k) = \frac{1}{D} \prod_p \frac{1 - N(p)/p}{(1 - 1/p)^k}, \tag{37.3}$$

where D is the product of the degrees of the polynomials $f_1, \ldots, f_k$ and $N(p)$ is the number of solutions n mod p of the congruence $f(n) \equiv 0 \pmod{p}$, with $f = f_1 \cdots f_k$.

The Bateman-Horn conjecture has far-reaching consequences. For instance, it not only asserts that the twin prime conjecture is true, but it also provides an asymptotic estimate of the number of such pairs not exceeding a certain number x. Three implications of this conjecture are given in the problems listed at the end of this episode.

37.1.5. The intriguing Sophie Germain primes. A prime p is called a *Sophie Germain prime* if $2p + 1$ is also a prime number. The Sophie Germain primes below 400 are

$$3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359.$$

There exists a fairly simple criterion for singling out Sophie Germain primes, that is for determining if $2p + 1$ is prime whenever p is a prime (see Problem 37.2).

Marie-Sophie Germain (1776-1831) was born in Paris, France. At the age of 13, reading the story of the murder of Archimedes by a cruel Roman soldier, she was moved and decided to study mathematics. Because of the opposition of her parents, she did it on her own, reading Newton and Euler's work at night, hiding under her blankets. Then, her parents gave in, allowing her to pursue her passion for mathematics, even supporting her financially throughout her whole life. In order to gain acceptance from the mathematical community, she wrote her work under the name of Monsieur Le Blanc. She obtained support from Lagrange, Legendre and Gauss, who all praised her, even more so when they learned that Monsieur Le Blanc was actually a woman. Her theorem on the solutions of the diophantine equation $x^5+y^5 = z^5$ is the first significant result regarding Fermat's last theorem.

Gauss was so impressed by Sophie Germain that he suggested that she be awarded an honorary degree form Göttingen University. Sadly, she died from breast cancer at the early age of 55, before she could receive this distinction (Hauchecorne and Suratteau [**109**]).

Sophie Germain primes are interesting because Sophie Germain showed that if p is a prime such that $2p + 1$ is also prime, then there are no positive integers x, y, z, none of which are divisible by p, such that $x^p + y^p = z^p$, an important first step towards the proof of Fermat's last theorem.

Although the list of Sophie Germain primes appears to be infinite, no one has yet been able to prove it. Even if we cannot prove that fact, a conjectured asymptotic expression exists for the number $G(x)$ of Sophie Germain primes $p \le x$. Indeed, as a consequence of the Bateman-Horn conjecture stated above,

$$G(x) = (1 + o(1))2C\frac{x}{\log^2 x} \qquad (x \to \infty),$$

where C is the twin prime constant, namely $C = \prod_{p\ge 3} \frac{p(p-2)}{(p-1)^2} \approx 0.660161$ (see Problem 37.10). As x becomes larger, the quotient $G(x)/(x/\log^2 x)$ seems to tend to a constant, as the following data indicates.

x	$G(x)$	$G(x)/(x/\log^2 x)$
10^1	3	1.590
10^2	11	2.333
10^3	38	1.813
10^4	191	1.620
10^5	1172	1.553
10^6	7747	1.479

x	$G(x)$	$G(x)/(x/\log^2 x)$
10^7	56033	1.456
10^8	423141	1.436
10^9	3308860	1.421
10^{10}	26569516	1.409
10^{11}	218116524	1.399
10^{12}	1822848478	1.392

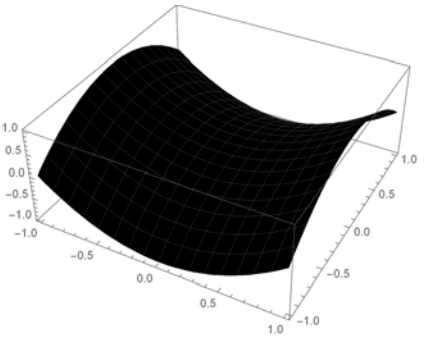
In light of this numerical evidence, it is quite frustrating that no one has yet been able to prove that the number of Sophie Germain primes is infinite.

37.1.6. Primes and the ingenuity of Maryam Mirzakhani *. Sophie Germain has made history because of her important work on primes. More than two centuries later, another female mathematician also obtained important results related to primes, but this time prime geodesics. Maryam Mirzakhani was an Iranian mathematician who lived in the 21st century and became the first woman to

receive the highly praised Fields medal. Her research work was related to the prime number theorem and to geodesics. Before we explain very briefly the nature of her work, let us lay down the proper mathematical context.

It is often said that the shortest path between two points is a straight line. While this is true on a flat surface, it is not so on the surface of a sphere.

Indeed, the shortest path between two points on the surface of a sphere is the arc of a great circle whose center coincides with the center of the sphere. This is why trajectories of oversea flights look curved on a flat map. In geometry, we define a *geodesic* as a curve representing the shortest path between two points on a surface. We are about to introduce the notion of "primes" on a surface, but first, one more definition.



Hyperboloid $h(x, y) = x^2 - y^2$ for $-1 \leq x \leq 1$ and $-1 \leq y \leq 1$

A *hyperbolic surface* is a surface where any triangle drawn on it has the sum of its interior angles smaller than 180 degrees. Such a surface is shown in the above 3D graph. What does all this have to do with primes, let alone the prime number theorem ? On a hyperbolic surface, a *prime geodesic* is a geodesic which is a closed curve and which traces out its image exactly once. According to a result known as the "prime number theorem for geodesics", the number of closed geodesics (*closed geodesics* are geodesics which are also closed curves, that is, curves that close up into loops) of length not exceeding L is asymptotic to $(e^L)/L$. Now, the analogous counting problem for simple closed geodesics was an open problem (*simple* means that it does not cross itself). In her 2004 Ph.D. thesis, Maryam Mirzakhani solved this problem and gained instant fame. And that was only the beginning of a brilliant career.

Maryam Mirzakhani (1977-2017) was born in Tehran, Iran. While a teenager, she won gold medals in the 1994 and 1995 International Mathematical Olympiads for high-school students. In 2004, she obtained her Ph.D from Harvard University. The title of her thesis was *Simple Geodesics on Hyperbolic Surfaces and the Volume of the Moduli Space of Curves*. In 2008, she became a professor at Stanford University. In 2014, she became the first woman (and first Iranian) to win the prestigious Fields Medal for her contributions to the dynamics and geometry of Riemann surfaces. She was known in the mathematical community as a highly original mathematician. Her pioneering work bridges several mathematical disciplines, including hyperbolic geometry, complex analysis, topology and dynamics. Tragically, Maryam Mirzakhani died of breast cancer at the early age of 40. As written in the obituary put out by Stanford University "Mirzakhani worked on math problems like an artist scribbling formulas around her doodles, a process her young daughter once described as painting".

37.2. Conjectures connecting the multiplicative structure of integers to their additive structure

37.2.1. The *abc* conjecture. One of the most intriguing conjectures in number theory is the *abc* conjecture. Its difficulty rests on the fact that it relates the multiplicative structure of integers with their additive structure. As we will see in the problems of this episode, it has far-reaching consequences.

CONJECTURE 37.5 (*abc* conjecture). *Let $\varepsilon > 0$. There exists a positive constant $M = M(\varepsilon)$ such that, given any coprime integers a, b, c verifying the conditions $0 < a < b < c$ and $a + b = c$, we have*

$$c < M \cdot \left(\prod_{p|abc} p \right)^{1+\varepsilon}.$$

The *abc* conjecture is the outcome of a discussion, held in Bonn in 1985, between David W. Masser (Basel University, Switzerland) and Joseph Oesterlé (Université de Paris VI, France). The reader may be interested by the excellent survey paper of Granville and Tucker [**98**].

37.2.2. The Erdős-Mollin-Walsh conjecture. A positive integer n is called a *powerful number* if $p \mid n \Rightarrow p^2 \mid n$. It is convenient to include the number 1 in the list of powerful numbers. This way, if f is the indicator function of the set of powerful numbers (that is $f(n) = 1$ if n is powerful and $f(n) = 0$ otherwise) then f is a multiplicative function. The first ten powerful numbers are 1, 4, 8, 9, 16, 25, 27, 32, 36 and 49. Observe that 8 and 9 constitute the first pair of consecutive powerful numbers. It has been shown by Solomon W. Golomb [**95**] that there are infinitely many pairs of consecutive powerful numbers. In fact, since we know that the number of solutions $\{x, y\}$ of the Fermat-Pell equation $x^2 - 2y^2 = 1$ is infinite, one can easily show that there are infinitely many integers n such that both n and $n + 1$ are powerful (see Problem 37.12).

On the other hand, no one has ever found three consecutive powerful numbers. According to the *Erdős-Mollin-Walsh conjecture*, there are no such triplets.

Observe that if the *abc* conjecture (see the above subsection 37.2.1) is true, one can prove that there can only exist a finite number of integers n such that $n, n + 1, n + 2$ are each powerful (see Problem 37.13). One reason why the Erdős-Mollin-Walsh conjecture is most likely true is the following. Given an integer $n \geq 2$, let $\gamma(n) := \prod_{p|n} p$ stand for the product of the primes dividing n and let $\lambda_0(n)$ be the index of composition, already defined on page 120, setting for convenience $\gamma(1) = \lambda_0(1) = 1$. In particular, if $n > 1$ is powerful, then $\lambda_0(n) \geq 2$. In 2003, we proved [**56**] that if the *abc* conjecture is true, then, for any fixed $\varepsilon > 0$, there is only a finite number of numbers n such that $\min(\lambda_0(n), \lambda_0(n+1), \lambda_0(n+2)) > \frac{3}{2} + \varepsilon$. We also proved that without any conditions there exist infinitely many numbers n such that $\min(\lambda_0(n), \lambda_0(n + 1), \lambda_0(n + 2)) > \frac{3}{2} - \varepsilon$. Incidentally, letting $n = 85\,016\,574$, we find that

$$\ell_0 := \lambda_0(n) \approx 1.72085, \quad \lambda_0(n + 1) \approx 1.80738 \text{ and } \lambda_0(n + 2) \approx 1.97442,$$

so that $\min(\lambda_0(n), \lambda_0(n + 1), \lambda_0(n + 2)) > 1.72$. Assuming that ℓ_0 is indeed the largest possible value of $\min(\lambda_0(n), \lambda_0(n+1), \lambda_0(n+2))$ as n runs through the positive integers, this would be in contradiction with the existence of three consecutive

powerful numbers n_1, n_1+1, n_1+2, essentially because for these three numbers we would obviously have $\min(\lambda_0(n_1), \lambda_0(n_1+1), \lambda_0(n_1+2)) \geq 2$.

37.2.3. Largest prime factors of consecutive integers. Recalling that $P(n)$ stands for the largest prime factor of n, it seems reasonable to believe that the density of the set of positive integers n for which $P(n) < P(n+1)$ is $\frac{1}{2}$. However, this has not yet been proved and in fact it is an old conjecture of Paul Erdős [**79**]. In 2011, the authors considered [**58**] the function $\delta(n)$ which stands for the distance to the nearest $P(n)$-smooth number, that is, to the nearest integer whose largest prime factor is no larger than that of n. This brought the authors to state the following conjecture.

Conjecture 37.6 (De Koninck – Doyon). Given a fixed integer $k \geq 2$ and any permutation $a_1, a_2, \dots, a_k$ of the numbers $0, 1, \dots, k-1$, then

$$\frac{1}{x}\#\{n \leq x : P(n+a_1) < P(n+a_2) < \cdots < P(n+a_k)\} \sim \frac{1}{k!} \qquad (x \to \infty).$$

Assuming that Conjecture 37.6 is true, the authors could prove [**58**] that

$$\sum_{n \leq x} \frac{1}{\delta(n)} = (4\log 2 - 2 + o(1))x \qquad (x \to \infty).$$

It seems clear that we are very far from proving this conjecture, even in the (apparently simple) case $k = 2$. In 1978, Erdős and Pomerance [**81**] considered the case $k = 3$ and proved that there exist infinitely many integers n such that $P(n) < P(n+1) < P(n+2)$. As is mentioned in the solution to Problem 37.20, Antal Balog [**12**] proved in 2001 that the number of positive integers $n \leq x$ such that $P(n) > P(n+1) > P(n+2)$ is $\gg x^{1/2}$. However, both these results represent a very small step towards the proof of Conjecture 37.6 in the case $k = 3$. Nevertheless, there were significant developments in recent years. Indeed, in 2018, Zhiwei Wang [**229**] proved that the two sets of consecutive integers $n, n+1, n+2$ with the pattern $P(n) > P(n+1) < P(n+2)$ or $P(n) < P(n+1) > P(n+2)$ each have a positive proportion. Wang also proved that, given an arbitrary integer $k \geq 3$ and any integer k_0 with $0 \leq k_0 \leq k$, the k-tuple consecutive integers with the two patterns

$$P(n+k_0) < \min_{\substack{0 \leq j \leq k-1 \\ j \neq k_0}} P(n+j) \quad \text{and} \quad P(n+k_0) > \max_{\substack{0 \leq j \leq k-1 \\ j \neq k_0}} P(n+j)$$

have a positive proportion respectively. The same year, Joni Teräväinen made an important step towards the proof of Conjecture 37.6 in the case $k = 2$. Indeed, if we define the *logarithmic density* $\delta_0(A)$ of a set $A \subset \mathbb{N}$ by

$$\delta_0(A) := \lim_{x \to \infty} \frac{1}{\log x} \sum_{\substack{n \leq x \\ n \in A}} \frac{1}{n},$$

Teräväinen [**218**] proved that

$$\delta_0(\{n \in \mathbb{N} : P(n) < P(n+1)\}) = \frac{1}{2}.$$

Also, more recently, Terence Tao and Joni Teräväinen [**212**] investigated the density of local patterns in arbitrary sets of integers. As an application of their general results, they showed that $(\omega(n+1), \omega(n+2), \omega(n+3)) \pmod 3$ takes all

the 27 possible patterns in $(\mathbb{Z}/3\mathbb{Z})^3 = \{(0,0,0),(0,0,1),\dots,(2,2,2)\}$, each with positive lower density. They also showed that each of the sets

$$\{n \in \mathbb{N} : P(n+1) < P(n+2) < P(n+3) > P(n+4)\}$$

and

$$\{n \in \mathbb{N} : P(n+1) > P(n+2) > P(n+3) < P(n+4)\}$$

has positive lower density. This is an impressive step towards proving a more general version of the Erdős conjecture mentioned above.

37.2.4. The Chowla conjecture. Since the values $\lambda(n)$ of the Liouville function alternate between $+1$ and -1, there is some cancellation effect that refrains the sum $S(x) := \sum_{n\le x} \lambda(n)$ from getting too large as x increases. One can indeed prove that $S(x) = o(x)$ as $x \to \infty$, as was shown in Problems 12.14 and 12.15. In fact, it was shown that the prime number theorem is equivalent to the statement $S(x) = o(x)$ as $x \to \infty$. Again because of the cancellation phenomenon, one can expect that the sum $\sum_{n\le x} \lambda(n)\lambda(n+1)$ is also $o(x)$ as $x \to \infty$. This is probably true, but no one has yet proved it. In fact, in 1965, the British mathematician Sarvadaman Chowla (1907-1995) conjectured [**43**] that for any given integer $k \ge 1$,

$$\sum_{n\le x} \lambda(n)\lambda(n+1)\cdots\lambda(n+k-1) = o(x) \qquad (x \to \infty),$$

a statement often referred to as the *Chowla conjecture*[1].

Not much is known regarding Chowla's conjecture. Probably the most important step so far towards a proof of that conjecture is the estimate

$$\sum_{n\le x} \frac{\lambda(n)\lambda(n+1)}{n} = o(\log x) \qquad (x \to \infty) \tag{37.4}$$

recently proved by Terence Tao [**211**]. One can show that the Chowla conjecture implies the Tao result (see Problem 37.21), but, of course, no one has yet proved the reverse implication.

37.2.5. Consecutive integers divisible by a fixed power of their largest prime factor. Using a computer, one can easily establish that the number $n = 1\,294\,298$ is the smallest positive integer such that the numbers $n, n+1, n+2$ are each divisible by the square of their largest prime factor. Indeed,

$$\begin{aligned} 1\,294\,298 &= 2\cdot 61\cdot 103^2, \\ 1\,294\,299 &= 3^4\cdot 19\cdot 29^2, \\ 1\,294\,300 &= 2^2\cdot 5^2\cdot 7\cdot 43^2. \end{aligned}$$

The next smallest five integers with that property are

$$9\,841\,094, \quad 158\,385\,500, \quad 1\,947\,793\,550, \quad 5\,833\,093\,013, \quad 11\,587\,121\,710,$$

[1]The actual Chowla conjecture is more general and it can be stated as follows: Let $h_1 < \cdots < h_k$ be nonnegative integers and $a_1,\dots,a_k$ be positive integers with at least one of the a_i odd; then,

$$\sum_{n\le x} \lambda(n+h_1)^{a_1}\cdots\lambda(n+h_k)^{a_k} = o(x) \qquad (x \to \infty).$$

and one can find many more. Are there infinitely many integers n with this property ? Most likely, but no one can prove it. In fact, this question can be generalized. First, a definition. Given fixed integers $k \geq 2$ and $\ell \geq 2$, set

$$E_{k,\ell} := \{n \in \mathbb{N} : P(n+i)^\ell \mid n+i \ \text{ for each } i = 0, 1, \ldots, k-1\}.$$

Many elements of the sets $E_{2,2}$, $E_{2,3}$, $E_{2,4}$, $E_{2,5}$ and $E_{3,2}$ are given in the book of the first author [**55**].

It follows from the fact that the Fermat-Pell equation $x^2 - 2y^2 = 1$ has infinitely many solutions in positive integers x, y that the set $E_{2,2}$ is infinite. Moreover, setting $E(x) = \#\{n \leq x : n \in E_{2,2}\}$, De Koninck, Doyon and Luca [**59**] showed that there exists a positive constant c such that

$$\frac{x^{1/4}}{\log x} \ll E(x) \ll x \exp\{-c\sqrt{\log x \log\log x}\}.$$

(See Problem 37.22 for a proof of the lower bound.)

In March 2014, Peter Burcsi and Gabor Gévay (Eötvös Lorand University), using a clever algorithm along with a powerful computer, could prove that the 77-digit integer

$$\begin{aligned} n_0 \ = \ & 10128834955510335895866370114673406465 8 \\ & 53401274472331052424438595083379069057 \end{aligned}$$

is such that

$$\begin{aligned} n_0 - 1 \ &= \ 2^7 \cdot 53 \cdot 4253 \cdot 27631 \cdot 27953 \cdot 1546327 \cdot 2535271 \\ &\qquad \cdot 17603683 \cdot 1472289739 \cdot 16476952799^3, \\ n_0 \ &= \ 3^6 \cdot 19 \cdot 37 \cdot 787 \cdot 711163 \cdot 2181919 \cdot 137861107 \\ &\qquad \cdot 318818473 \cdot 937617607 \cdot 7323090133^3, \\ n_0 + 1 \ &= \ 2 \cdot 12899 \cdot 133451 \cdot 421607 \cdot 2198029 \cdot 8046041 \\ &\qquad \cdot 19854409 \cdot 555329197 \cdot 32953905599^3, \end{aligned}$$

thereby showing that $n_0 - 1 \in E_{3,3}$. Perhaps this number is the smallest element of $E_{3,3}$, but this has not been proved. Other integers (with 77 digits and larger) belonging to $E_{3,3}$ as well a 113-digit number belonging $E_{2,6}$ are given in the paper of De Koninck and Moineau [**61**].

On the other hand, no elements of $E_{4,2}$ are known. In fact, if n belongs to $E_{4,2}$, then a heuristic argument shows that most likely $n > 10^{57}$ (see [**61**]).

Nevertheless, it seems reasonable to conjecture that, given any fixed integers $k \geq 2$ and $\ell \geq 2$, the set $E_{k,\ell}$ is infinite.

We also conjecture that, given any two integers $k \geq 2$ and $\ell \geq 2$, there exists a positive constant $C = C_{k,\ell}$ such that for any k-tuples of primes $(p_0, p_1, \ldots, p_{k-1})$ satisfying $\min_{0 \leq i \leq k-1} p_i > C$, there exists $n \in E_{k,\ell}$ for which

$$P(n+i) = p_i \quad \text{for } 0 \leq i \leq k-1. \tag{37.5}$$

However, it was shown in [**59**] that given fixed integers $k \geq 2$ and $\ell \geq 2$ and a particular k-tuple of primes $(p_0, p_1, \ldots, p_{k-1})$, the number of positive integers $n \in E_{k,\ell}$ satisfying condition (37.5) is finite.

37.3. Potential breakthroughs in factoring

37.3.1. Hittmeir's factorisation algorithm. In 2017, Markus Hittmeir [**116**] provided what is considered so far as the theoretically fastest deterministic factorisation algorithm. To find the prime factors of a large integer n, the number of basic operations required using Hittmeir's algorithm is less than

$$O\left(\frac{n^{1/4}}{\exp\left\{\frac{C\log n}{\log\log n}\right\}}\right)$$

for some positive constant C. It is important to mention that Hittmeir's algorithm does not contain any random steps and that the proof of its running time does not rely on any conjecture. It means that even if in practice, other algorithms may be faster with almost certainty (such as the quadratic sieve), Hittmeir's result is of great theoretical interest. Hittmeir's improvement relies essentially on a faster way to find the order of a modulo n. He achieved this by modifying the baby step giant step method which we briefly describe here.

Say we want to find an integer $x < n$ such that $a^x \equiv 1 \pmod{n}$. We write $x = y + mz$ with $m = \lfloor\sqrt{n}\rfloor$ so that $1 \equiv a^{y+mz} \equiv a^y a^{mz} \pmod{n}$ or equivalently $a^y \equiv (a^{-m})^z \pmod{n}$. We now build two lists. The first one contains the *baby steps* and is given by

$$L_1 := \{a^y \pmod{n} : y = 1, 2, \ldots, m\}$$

while the second list contains the *giant steps* and is given by

$$L_2 := \{(a^{-m})^z \pmod{n} : z = 1, 2, \ldots, \lfloor n/m\rfloor\}.$$

Assume that we have found a common element in the two lists, say $a^{y_0} \equiv (a^{-m})^{z_0} \pmod{n}$. Setting $x = y_0 + mz_0$ will reveal a solution to $a^x \equiv 1 \pmod{n}$ with $x < n$. The beauty of this approach is that it requires performing only $m + \lfloor n/m\rfloor \approx 2\sqrt{n}$ exponentiations. This is advantageous compared to the n exponentiations that could be required if one would naively try to compute $a^1, a^2, \ldots$ until reaching a value of x such that $a^x \equiv 1 \pmod{n}$.

37.3.2. The strange world of quantum computing *. What if someone could come up with some way to factor an arbitrarily large integer in polynomial time? Someone did, in 1995. Someone by the name of Peter Shor. He is an American mathematician who developed a factorisation algorithm which runs in polynomial time [**200**], that is, much faster than any other factorisation algorithm we presented so far in this book! The only inconvenience is that Shor's algorithm requires the use of a quantum computer.

Quantum mechanics in general and quantum computing in particular defy intuition. The inherent randomness of quantum physics was so troubling to Albert Einstein that he wrote in a 1926 letter to Max Born, one of the founders of quantum physics: "Quantum theory yields much, but it hardly brings us close to the Old One's secrets. I, in any case, am convinced He does not play dice with the universe." Despite this, quantum mechanics provides a consistent mathematical theory. The idea of building quantum computers can be traced back to Nobel prize winner Richard Feynman, who wrote in 1982: "If you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful

problem, because it doesn't look so easy." Let us first provide some of the basic features of quantum computing.

37.3.2.1. *Bits and qubits.* The fundamental unit of computer memory is the bit. A bit can either be in state 0 or in state 1. This makes two possible states and therefore a system of n bits can be in a total of 2^n different states. We will refer to these states as *classical* to emphasize that they can occur in classical (that is, non-quantum) computers. For quantum computers, things are quite different. Their fundamental information storage unit is the qubit. A *qubit* is a superposition of the classical state 0 and of the classical state 1. It can be represented by a normalized vector of length 2. For instance, the qubit $(1/\sqrt{2}, 1/\sqrt{2})^t$ can be interpreted to be in the classical state 0 with probability 1/2 and in the classical state 0 with probability 1/2. Interestingly, the entries of a vector representing the state of a qubit do not have to be nonnegative real numbers as "normal" probabilities do. Instead the state of a qubit can be represented by any vector $u = (u_1, u_2)^t$ in $\mathbb{C}^2$ such that $\|u\| = \sqrt{|u_1|^2 + |u_2|^2} = 1$. The probability that the qubit is in the classical state 0 is $|u_1|^2$ whereas the probability that it is in the classical state 1 is $|u_2|^2$. What happens when we have more than one qubit is interesting. Two classical bits can be in either of the four states 00, 01, 10 and 11. The state of two qubits will be a superposition of these four classical states and will be represented by a vector $u = (u_1, u_2, u_3, u_4)^t \in \mathbb{C}^4$ with $\|u\| = 1$. The value of $|u_1|^2$ stands for the probability that the qubit is in the classical state 00 while the value of $|u_2|^2$ stands for the probability that the qubit is in the state 01, and so on. Similarly the state of n qubits corresponds to a superposition of the 2^n possible classical states of n bits. This is why it is represented by a vector $u \in \mathbb{C}^{2^n}$ such that $\|u\| = 1$.

37.3.2.2. *Measuring a qubit.* The state of a qubit or of several qubits is represented by a complex vector. However, the entries of these complex vectors can never be accessed by the user or considered as an output of the algorithm. While one cannot "read" these complex coefficients, one can (and must) perform a *measurement* step in order to make use of a quantum computation. Measuring an n qubit system will return a single classical state of an n bit system, and the probability to obtain a given classical state is equal to the square norm of the corresponding coefficient. For example, consider the 2 qubit state $(0, 1/\sqrt{3}, \sqrt{2}/\sqrt{3}, 0)^t$. Measuring this system returns the classical state 01 with probability 1/3 and the classical state 10 with probability 2/3.

37.3.2.3. *Entanglement.* Consider again the 2 qubit state $(0, 1/\sqrt{3}, \sqrt{2}/\sqrt{3}, 0)^t$. One could measure only the first bit of the system obtaining 0 with probability 1/3 and 1 with probability 2/3. Observe that knowing the value of this first bit reveals the value of the second one. For instance, since the only possible states are 01 and 10, if the first bit is in state 1 the second one will be in state 0, and reciprocally. When reading the state of one bit gives information about the states of other bits, we say that the system is *entangled*. On the contrary, considering the 2 qubit system $(\sqrt{2}/3, 1/3, 2/3, \sqrt{2}/3)^t$, the first bit is equal to 0 with probability $(\sqrt{2}/3)^2 + (1/3)^2 = 1/3$, whereas the second bit is equal to 0 with probability 2/3. Since the state of each bit is independent from the other in terms of probability (this is easy to verify), we can say that this system is *not entangled*.

REMARK 37.7. While entanglement is nothing special from a purely mathematical perspective, some of its physical implications are counterintuitive. For instance, assume that the 2 qubit system corresponds to two coins whose possible

outcomes are either HEADS or TAILS and assume that the state of the two coins is entangled. You keep a coin for yourself and send the other one to a friend living far away. Looking at the outcome of your coin can allow you to learn instantaneously the outcome of the faraway coin. This idea has been used by Charles H. Bennett and Gilles Brassard [**17**] to develop the concept of quantum cryptography.

37.3.2.4. *Basic operations in quantum computing.* Now that we have discussed the measurement operation which is necessary to get an output out of a quantum algorithm, what are the other elementary operations of quantum computing ? It turns out that the elementary operations acting on systems of n qubits can be represented by multiplications by unitary, complex and invertible matrices of size $2^n \times 2^n$. Let us illustrate how to build such an operator with a concrete example. Suppose that we want to build a quantum operator that performs a simple one bit addition and return the value $x + y$ where $x, y \in \{0, 1\}$. Explicitly, this operator should compute $0+0 = 00$, $0+1 = 01$, $1+0 = 01$ and $1+1 = 10$. First observe that since $1 + 0 = 0 + 1$, this operation is not invertible and cannot be represented by an invertible matrix. To overcome this difficulty, let us modify the output so that the first bit of the output is equal to x and the second bit is equal to the last digit of the sum $x+y$. This yields $0+0 = 00$, $0+1 = 01$, $1+0 = 11$ and $1+1 = 10$. We can observe that no information is lost as to the value of the sum. We can encode the values of the input and output in vectors of length four. Explicitly, the input is encoded as

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix} \leftrightarrow x = y = 0, \quad \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \leftrightarrow x = 0, y = 1, \quad \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \leftrightarrow x = 1, y = 0, \quad \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \leftrightarrow x = y = 1$$

whereas the output is encoded as

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix} \leftrightarrow 00, \qquad \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \leftrightarrow 01, \qquad \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \leftrightarrow 10, \qquad \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \leftrightarrow 11.$$

This way, our operator is equivalent to the mapping

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix} \to \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \qquad \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \to \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \qquad \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \to \begin{bmatrix}0\\0\\0\\1\end{bmatrix}, \qquad \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \to \begin{bmatrix}0\\0\\1\\0\end{bmatrix}.$$

Hence the quantum addition of one bit integers can be represented by the matrix

$$A = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}.$$

Observe that while we constructed the operator A only from considerations on the classical 2 bit states, its action on any 2 qubit state is well defined. Consider for

example the 2 qubit state $u = (0, i/\sqrt{2}, -1/\sqrt{2}, 0)^t$; the action of A on u will return

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ i/\sqrt{2} \\ -1/\sqrt{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i/\sqrt{2} \\ 0 \\ -1/\sqrt{2} \end{bmatrix}.$$

37.3.3. A glance at Shor's factoring algorithm *. From the definition of quantum unitary operation, it can be said that a single operation on a system of n qubits acts simultaneous on each of the 2^n possible classical states ! This is why one might hope that a quantum algorithm could speed up computations exponentially. However, things are not so easy since the mandatory measurement step returns the value of a single classical state in a probabilistic manner. This is why, when Shor constructed a clever quantum algorithm able to factor an integer in polynomial time, it was an outstanding achievement. At the heart of this algorithm is a resolution of the discrete logarithm problem in polynomial time. If a and b are coprime positive integers, it is always possible to find a positive integer x with $a^x \equiv 1 \pmod{b}$ and, as we saw in Episode 24, the smallest such value of x is called the order of a modulo b. However, finding this value of x, that is, solving the discrete logarithm problem, is computationally difficult, and for the time being, no classical algorithm can achieve this in polynomial time. This is where Shor uses quantum computing to improve classical algorithms and constructs the first polynomial time factoring algorithm.

Peter Williston Shor was born August 14, 1959, in New York City, USA. Already at a very young age, he demonstrated his brilliancy in mathematical competitions: he placed third in the 1977 USA Mathematical Olympiad and after graduating that year, he won a silver medal at the International Math Olympiad in Yugoslavia. He was a Putnam Fellow in 1978. He received several prestigious prizes for the factoring algorithm that bears his name: he was awarded the Rolf Nevanlinna Prize in 1998, the Gödel Prize in 1999 and the Dirac Medal in 2017. He became a professor at MIT in 2003 and was inducted into the American Academy of Arts and Sciences in 2011.

37.4. Primes and the future of computers

As we saw in Episode 36, our inability to factor large integers serves us well as it is the cornerstone of RSA cryptography. The RSA method can be used to send secret messages but is more often used to securely verify the identity of the sender of a message (as we saw in Problem 36.5). However, our ability to factor large integers has increased considerably as computers have become exponentially more powerful as predicted by Moore's law[2] (see Brock [**29**]). In response to this, cryptography schemes using elliptic curves have been developed as an alternative to RSA. These algorithms rely on the difficulty to find an integer x such that $ax = b$ on a modular elliptic curve. The security of this approach could be challenged if computer power continues to increase exponentially in the coming years. Whether this will happen is unclear as theoretical physics suggests fundamental limitations to the speed of computers. Needless to say, if the use of quantum computers becomes the norm,

[2]According to which the number of transistors in a dense integral circuit would double every 18 months.

the speed and efficiency of all algorithms used in number theory will have to be re-evaluated given the difference in what constitutes a basic operation. Whether or not this will happen is also unclear. Although some progress has been made in the development of larger quantum computers (see Knight [**125**]), they are still unable to compete with classical computers and some physicists believe that there might be fundamental limits preventing their use for large scale computations (see Kalai [**123**]).

Problems on Episode 37

PROBLEM 37.1. The statement "For every integer $n > 1$, the number $n^4 + 4^n$ is composite" is often attributed to Sophie Germain. Prove that this statement is correct.

PROBLEM 37.2. Let p be a prime and let $n = 2p + 1$. Assuming that n is not a multiple of 3 and that $2^{n-1} \equiv 1 \pmod{n}$, show that n must be a prime.

PROBLEM 37.3. Regarding the statement of the Bunyakovsky conjecture, show that even though the polynomial $f(x) := x^9 - x^3 + 2520$ is irreducible, each of the integers $f(1)$, $f(2)$, $f(3), \ldots$ is a composite number.

PROBLEM 37.4. Fix an integer $k \geq 2$. Show that if the Bunyakovsky conjecture is true, then the sequence $(\Phi_k(n))_{n\geq 1}$ contains infinitely many primes.

PROBLEM 37.5. The seventh smallest element in the set $F(4, 2)$ (defined in (37.2)) is the number 969 697 050. Find the six smallest by first considering the set

$$A := \{mP(m)^3 : m = 2, 3, \ldots, 200\,000\}$$

whose elements n all satisfy $P(n)^4 \mid n$ and then by checking those $n \in A$ such that $P(n + 1)^2 \mid n + 1$.

PROBLEM 37.6. Using the identity

$$(2p^4 - 1)^2 - 1 = 4p^4(p + 1)(p - 1)(p^2 + 1)$$

and focusing on the primes p of the form $p = 4k^2 + 2k + 1$, prove that, if the Bunyakovsky conjecture is true, then the set $F(4, 2)$ is infinite.

PROBLEM 37.7. Let $\beta_0(n)$ be the function defined on page 233. Show that by considering those integers n such that $n = 4pq$ and $n + 1 = rs$, where p is a prime for which the corresponding numbers $r = 6p - 1$, $s = 10p - 1$ and $q = 15p - 4$ are also primes and assuming that the prime k-tuples conjecture stated on page 231 is true, then $\beta_0(n) = \beta_0(n + 1)$ has infinitely many solutions n.

PROBLEM 37.8. Show that the sum of the reciprocals of the Ruth-Aaron numbers converges.

PROBLEM 37.9. Show that as a consequence of the Bateman-Horn conjecture, the number $N_2(x)$ of pairs of twin primes up to x should satisfy

$$N_2(x) = (1 + o(1))C_2 \int_2^x \frac{dt}{\log^2 t} \qquad (x \to \infty),$$

where

$$C_2 = 2 \prod_{p\geq 3} \left(1 - \frac{1}{(p - 1)^2}\right).$$

PROBLEM 37.10. Show that if the Bateman-Horn conjecture is true, then

$$G(x) := \#\{p \le x : 2p+1 \text{ prime}\},$$

that is the number of Sophie Germain primes not exceeding x satisfies

$$G(x) = (1+o(1))c_g \frac{x}{\log^2 x} \qquad (x \to \infty),$$

where $c_g = 2\displaystyle\prod_{p\ge 3} \frac{p(p-2)}{(p-1)^2} \approx 1.32032$.

PROBLEM 37.11. Show that as a consequence of the Bateman-Horn conjecture, the number

$$P(x; p, p+2, p+6, p+8) := \#\{p \le x : p+2, p+6, p+8 \text{ are primes}\}$$

satisfies

$$P(x; p, p+2, p+6, p+8) = (1+o(1))\frac{27}{2}\prod_{p\ge 5}\frac{p^3(p-4)}{(p-1)^4}\int_2^x \frac{dt}{\log^4 t} \qquad (x\to\infty).$$

PROBLEM 37.12. It is known that the Fermat-Pell equation (*) $x^2 - 2y^2 = 1$ has infinitely many solutions in positive integers x, y. In fact, letting $\{x_1, y_1\} = \{3, 2\}$ be the "smallest" solution of (*), one can show that all other solutions $\{x_k, y_k\}$ of (*) are given by the recurrence relations

$$x_{k+1} = x_1x_k + 2y_1y_k \quad \text{and} \quad y_{k+1} = x_1y_k + y_1x_k \qquad (k \in \mathbb{N})$$

(see for instance the wonderful paper of H. W. Lenstra Jr. [**144**] in which he uses results from elementary algebra and number theory to examine the existence of solutions to the general Fermat-Pell[3] equation $x^2 - dy^2 = 1$, where d is not a square). Use this result to show that there are infinitely many positive integers n such that n and $n+1$ are simultaneously powerful.

PROBLEM 37.13. Show that if the *abc* conjecture holds, then there is only a finite number of integers n such that $n, n+1, n+2$ are simultaneously powerful.

PROBLEM 37.14. Prove that there are no integers n such that $n, n+1, n+2, n+3$ are each powerful.

PROBLEM 37.15. Taking logarithms on both sides of the "*abc* inequality" appearing in Conjecture 37.5, we obtain successively

$$\begin{aligned} \log c &< \log M + (1+\varepsilon)\log\gamma(abc), \\ \frac{\log c}{\log\gamma(abc)} &< \frac{\log M}{\log\gamma(abc)} + 1 + \varepsilon, \end{aligned}$$

which indicates that the quotient $Q(a,b,c) := \log c/\log\gamma(abc)$ should become smaller (and not bigger!) as we examine various triples of coprime integers a, b, c. This explains why those studying the *abc* conjecture are usually interested in finding coprime integers a, b, c satisfying $a + b = c$ and such that the corresponding

[3]One may be surprised to learn that the English mathematician John Pell (1611–1685) has nothing to do with this equation. It was Euler who mistakenly attributed to Pell a solution method that had in fact been found by William Brouncker (1620–1684), another English mathematician, who had been challenged by Fermat to find the solutions of this equation. This explains why it is called by some the *Fermat-Pell equation* and by others simply the *Pell equation*.

quotient $Q(a,b,c)$ is as large as possible. The largest known such quotient was found by Éric Reyssat:

$$a=2, \quad b=3^{10}\cdot 109, \quad c=23^5 \quad \text{with} \quad Q(a,b,c)=1.629912.$$

One can find a nearly as big quotient by examining a fairly small set of powerful numbers. Indeed, using a computer, first generate the set A of all 21 043 powerful numbers smaller than 100 million. Then, write a program that considers all those coprime numbers $a,b\in A$ and compute the corresponding quotient $Q(a,b,c)$. You will quickly find integers $a<b<c$ with $Q(a,b,c)=1.62599$. Identify these integers a,b,c.

PROBLEM 37.16. Show that there exist infinitely many pairs of integers $\{m,n\}$ such that $\gamma(m+i)=\gamma(n+i)$ for $i=0,1$. Is the same true if we replace the requirement $i=0,1$ by $i=0,1,2$?

PROBLEM 37.17. Let $S:=\sum_{\substack{n=1\\ n \text{ powerful}}}^{\infty}\frac{1}{n}$. Write S as an infinite product on primes and then use some of the identities displayed in (4.6) to show that $S=\dfrac{315}{2\pi^4}\zeta(3)$.

PROBLEM 37.18. Let $\varepsilon>0$ be an arbitrarily small number. Prove that if the *abc* conjecture holds, then there exists $k_0=k_0(\varepsilon)$ such $\lambda_0(2^k-1)<1+\varepsilon$ for all integers $k\ge k_0$.

PROBLEM 37.19. Prove that $P(n^2+1)\le n$ for infinitely integers n.[4]

PROBLEM 37.20.* Prove that there exist infinitely many integers n such that

$$P(n-1)<P(n)<P(n+1).$$

PROBLEM 37.21. Show that the Chowla conjecture implies Tao's estimate (37.4).

PROBLEM 37.22. By considering the identity $(2p^2-1)^2-1=4p^2(p-1)(p+1)$, which holds for all primes p, show that the number of integers $n\le x$ such that $P^2(n)\mid n$ and $P^2(n+1)\mid n+1$ is at least $cx^{1/4}/\log x$ for some positive constant c.

PROBLEM 37.23.* Let $Q\in\mathbb{Z}[x]$ be a nonconstant polynomial with integer coefficients. Show that

$$\limsup_{n\to\infty}\ \omega(Q(n))=\infty.$$

PROBLEM 37.24.* Let $Q\in\mathbb{Z}[x]$ be a nonconstant polynomial with integer coefficients such that $Q(0)\neq 0$. Show that

$$\limsup_{n\to\infty}\ \frac{\omega(Q(n))}{\omega(n)}=\infty.$$

[4]Curiously, no one can prove that there are infinitely many primes p such that $P(p^2+1)\le p$ (see for instance Dartyge, Martin and Tenenbaum [**52**]).