Dirichletino

INTA BERTUCCIONI
Chemin de la Raye, 11
CH-1024 Écublens, SWITZERLAND
Inta.Bertuccioni@gmail.com

In 1837 P. G. Lejeune Dirichlet published his celebrated theorem [**1**], stating that any arithmetic progression $a, a+b, a+2b, a+3b, \ldots$ wherein a and b have no common factor contains infinitely many prime numbers. All known proofs are difficult, and the most readable ones (see, for instance, Serre [**3**]) use nontrivial results of complex analysis. It can be shown [**4, 5**] that, in a very precise technical sense, elementary proofs are only possible when $a^2 \equiv 1$ modulo b, in particular for $a = 1$ and $a = -1$. Recently, Hillel Gauchman published a simple proof [**2**] for the case $a = 1$. We show here what we believe to be an even simpler proof, using an idea of Gauchman's [**2**] (the only idea we need, in fact) and a little lemma. To fix the notation, we restate what we want to prove.

THEOREM. *If N is any positive integer, there are infinitely many primes of the form $1 + mN$, $m = 1, 2, \ldots$.*

Proof. Let $q_1, \ldots, q_r$ be r primes of the form $1 + mN$. We will find another prime of this form. Let $p_1, \ldots, p_s$ be the distinct prime divisors of N. Consider, as in Gauchman [**2**], for $k = 1, \ldots, s$ the polynomials

$$f_k(X) = \frac{X^N - 1}{X^{N/p_k} - 1} = \left(X^{N/p_k}\right)^{p_k - 1} + \left(X^{N/p_k}\right)^{p_k - 2} + \cdots + 1.$$

Fixing an index k, we can decompose $f_k(X)$ into a product of irreducible monic polynomials in $\mathbb{Z}[X]$. Since $f_k(e^{2\pi i/N}) = 0$, one of these irreducible factors, say $f(X)$, must vanish at $e^{2\pi i/N}$. By a well-known lemma of Gauss, an integral polynomial that is irreducible in $\mathbb{Z}[X]$ is also irreducible in $\mathbb{Q}[X]$, and therefore $f(X)$ must be the minimal polynomial of $e^{2\pi i/N}$ over $\mathbb{Q}$. Thus $f(X)$ is the same for every k.

If t is a sufficiently large integer, then for $c = tp_1 \cdots p_s q_1 \cdots q_r$, we will have $f(c) \geq 2$. Let q be a prime divisor of $f(c)$, hence of $c^N - 1$. It must be different from each p_k and each q_k, because none of the primes p_k and none of the primes q_k divides $c^N - 1$. Furthermore, by the lemma below, q does not divide any of the $c^{N/p_k} - 1$. This means that $c^N \equiv 1 \pmod{q}$, whereas $c^{N/p_k} \not\equiv 1 \pmod{q}$. In other words, the multiplicative order of c modulo q is exactly N. On the other hand, by Fermat's little theorem, $c^{q-1} \equiv 1 \pmod{q}$; hence N divides $q - 1$, which is the same as $q = 1 + mN$ for some integer m. We have proved that, given any number of primes $q_1, \ldots, q_r$ of the form $1 + mN$, we can find another one. Thus there are infinitely many such primes. ∎

It remains to state and prove the lemma, that, as noticed by van der Waerden [**7**], goes back at least to Sylvester [**6**].

LEMMA. *Let c be any integer different from 1 and -1, N a positive integer and p a prime divisor of N. Let $q \neq p$ be a prime divisor of*

$$A = \frac{c^N - 1}{c^{N/p} - 1}.$$

Then q does not divide $c^{N/p} - 1$.

Proof. Setting $b = c^{N/p} - 1$ we have

$$A = \frac{(b+1)^p - 1}{b} = b^{p-1} + \binom{p}{1} b^{p-2} + \cdots + \binom{p}{p-1}$$

and therefore, if q were a divisor of b, it would also divide $\binom{p}{p-1} = p$, which contradicts the assumption $q \neq p$. ∎

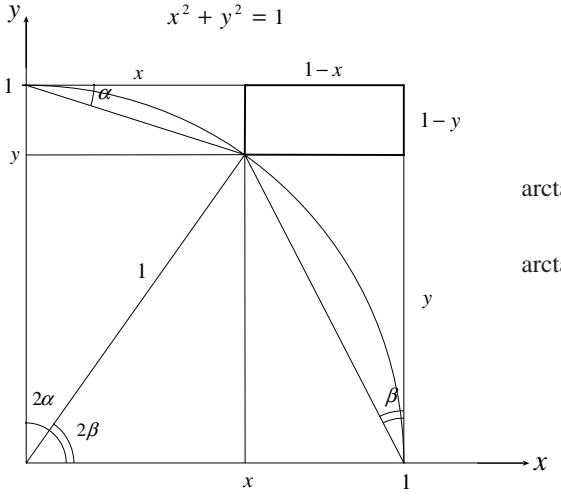
REFERENCES

1. P. G. Lejeune Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, *Abh. Preuss. Akad. Wiss.* (1837) 45–81. (Werke I, 313–342.)
2. Hillel Gauchman, A special case of Dirichlet's theorem on primes in an arithmetic progression, this MAGAZINE **74** (2001) 397–399.
3. Jean-Pierre Serre, *Cours d'arithmétique*, 2me édition, Presses Universitaires de France, Paris, 1977.
4. M. Ram Murty, Primes in certain arithmetic progressions, *J. Madras Univ.* **51** (1988) 161–169.
5. M. Ram Murty and Nithum Thain, Prime numbers in certain arithmetic progressions, *Funct. Approx. Comment. Math.* **35** (2006) 249–259.
6. James Joseph Sylvester, On the divisors of the sum of a geometrical series whose first term is unity and common ratio any positive or negative integer, *Nature* **37** (1888) 417–418. (Collected papers IV, 625–629.)
7. B. L. van der Waerden, *Elementarer Beweis eines zahlentheoretischen Existenztheorems*, *J. reine angew. Math.* **171** (1934) 1–3.

Proof Without Words: An Arctangent Identity

If $x, y > 0$ and $x^2 + y^2 = 1$, then

$$\arctan\left(\frac{1-x}{y}\right) + \arctan\left(\frac{1-y}{x}\right) = \frac{\pi}{4}.$$



$$\arctan\left(\frac{1-y}{x}\right) = \alpha$$

$$\arctan\left(\frac{1-x}{y}\right) = \beta$$

$$2\alpha + 2\beta = \frac{\pi}{2} \rightarrow \alpha + \beta = \frac{\pi}{4}$$

—HASAN UNAL
Yildiz Technical University
Istanbul 34210, TURKEY