Birch’s theorem: if $f(n)$ is multiplicative and has a non-decreasing normal order then $f(n) = n^\alpha$

Martin Klazar
May 22, 2018

Abstract
For pedagogical purposes (inclusion in lecture notes) we review the proof of the theorem stated in the title. At the end we state a problem.

1 Introduction
In 1967 B.J. Birch, later of the Birch and Swinnerton-Dyer conjecture fame, proved in [2] a most interesting result.

Theorem (Birch, 1967). The only multiplicative functions $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ that are unbounded and have a non-decreasing normal order are the powers of $n$, the functions $f(n) = n^\alpha$ for a constant $\alpha > 0$.

Multiplicativity means that $f(mn) = f(m)f(n)$ for every two coprime numbers $m, n \in \mathbb{N}$ (thus $f(1) = 1$ unless $f \equiv 0$), $\mathbb{N} = \{1, 2, \ldots\}$, and the clause about a non-decreasing normal order means that a non-decreasing function $g : \mathbb{N} \to \mathbb{R}_{> 0}$ exists such that for every $\varepsilon > 0$, $\#(n \leq x \mid \frac{f(n)}{g(n)} \not\in (1 - \varepsilon, 1 + \varepsilon)) = o(x)$ as $x \to +\infty$.

In this write-up I present the proof of Birch’s theorem, as given in Birch [2] and Narkiewicz [13, pp. 98–102] (see also [14]). It is a beautiful proof in the erdősian style. To be honest, I started with the intention to correct two errors I thought I had discovered in the argument. Fortunately, in the process of writing everything clarified and the errors disappeared. Still, I will point out the two steps I struggled with. To the interested reader, much smarter than me, they will certainly pose no difficulty.

*klazar@kam.mff.cuni.cz
2 The proof with two conundrums

We use notation of [2], so let

\[ b(n) = \log f(n) \quad \text{and} \quad c(n) = \log g(n) \, . \]

Birch [2, p. 149] writes just “If \( f \) is unbounded, then \( g(n) \) tends to infinity with \( n \), so we may suppose that \( c(n) > 0 \) for all \( n \).” but Narkiewicz [13, Lemat 2.5 on p. 98] gives more details. Assume for contrary that \( g(n) \) has a finite limit \( a > 0 \). Then, by the relation bounding \( f \) and \( g \), there are constants \( 0 < A < a < B \) such that for every \( x > 0 \) and \( n \leq x \) we have \( A < f(n) < B \), with \( o(x) \) exceptions. Let \( E \subseteq \mathbb{N} \) be the exceptions: \( E \) has density \( 0 \). Fix any \( M > B \). Since \( f \) is unbounded, there is an \( m \in \mathbb{N} \) with \( f(m) > M/A \). The sets \( \{nm + 1 \mid n \in \mathbb{N} \} \) and \( \{(nm + 1)m \mid n \in \mathbb{N} \} \) have positive densities and thus so has \( X = \{n \in \mathbb{N} \mid nm + 1, (nm + 1)m \notin E \} \). For any \( n \in X \) we get the contradiction \( B > f((nm + 1)m) = f(nm + 1)f(m) > Af(m) > M \).

Thus indeed \( \lim g(n) = +\infty \). Changing finitely many values of \( g(n) \) we may assume that always \( g(n) > 1 \) and \( c(n) > 0 \). By Birch [2], “Using the three conditions

\[ \text{given } \varepsilon > 0, \, |b(n) - c(n)| < \varepsilon \text{ for all but } o(x) \text{ integers } n < x; \]
\[ b(mn) = b(m) + b(n) \text{ if } (m, n) = 1; \]
\[ c(n) \geq c(m) > 0 \text{ for } n \geq m; \]

we gradually deduce more and more till everything collapses.” Let \( m, n \in \mathbb{N} \) and \( \varepsilon > 0 \) be arbitrary with \( |b(m) - c(m)|, |b(n) - c(n)| < \varepsilon \). We assume that \( m, n \geq 2 \). It follows that for any \( \eta \in (0, \frac{1}{2}) \) there is an \( S > 0 \) such that for every \( R \geq S \) there are \( s, t \in \mathbb{N} \) satisfying

\[ (1 - \eta)R < s < R < t < (1 + \eta)R, \quad s \equiv t \equiv 1 \pmod{mn} \]

and

\[ |b(s) - c(s)|, |b(ms) - c(ms)|, |b(t) - c(t)|, |b(nt) - c(nt)| < \varepsilon . \]

(Only \( o(R) \) of the integers \( s \in ((1 - \eta)R, R) \) violate the first or the second last displayed inequality, and so for large \( R \) we certainly find there an \( s \equiv 1 \pmod{mn} \) satisfying both. The same for \( t \).) From \( b(ms) = b(m) + b(s) \) and \( b(nt) = b(n) + b(t) \) we get

\[ |c(ms) - c(m) - c(s)|, |c(nt) - c(n) - c(t)| < 3\varepsilon . \]

We define by induction numbers \( s_0 < s_1 < \ldots \) and \( t_0 < t_1 < \ldots \) in \( \mathbb{N} \), all congruent to \( 1 \) modulo \( mn \), such that

\[ (1 - \eta)S < s_0 < S < t_0 < (1 + \eta)S \]

and, for every \( i, j \in \mathbb{N}_0 \),

\[ (1 - \eta)ms_i < s_{i+1} < ms_i, \quad nt_j < t_{j+1} < (1 + \eta)nt_j, \]

2
and

\[ |b(s_i) - c(s_i)|, |b(ms_i) - c(ms_i)|, |b(t_j) - c(t_j)|, |b(nt_j) - c(nt_j)| < \varepsilon . \]

(In the previous claim we first set \( R = S \) and get \( s_0 = s \), then we set \( R = ms_0(\geq S) \) and get \( s_1 = s \), and so on. Since \( m \geq 2 \) and \( \eta < \frac{1}{2} \), we stay above \( S \) and \( s_i \) increase. Similarly and more easily for \( t_j \).) Then, as we know, for every \( i \in \mathbb{N}_0 \) one has

\[ |c(ms_i) - c(m) - c(s_i)| < 3\varepsilon . \]

Monotonicity of \( c \) gives

\[ c(s_i) > c(ms_i) - c(m) - 3\varepsilon \geq c(s_{i+1}) - c(m) - 3\varepsilon \]

and so \( c(s_h) < c(S) + hc(m) + 3h\varepsilon \) for every \( h \in \mathbb{N} \) by iteration. On the other hand, \( s_h > (1 - \eta)^{k+1}m^hS \) by iterating the above inequalities. Similarly for \( t_j \) we get \( c(t_k) > c(S) + kc(n) - 3k\varepsilon \) for every \( k \in \mathbb{N} \) and \( t_k < (1 + \eta)^{k+1}n^kS \).

Now if \( h, k \in \mathbb{N} \) are such that \( m^h > n^k \), equivalently \( h \log m > k \log n \) (recall that \( \log m \neq 0 \)), we may select \( \eta > 0 \) so small that still

\[ (1 - \eta)^{h+1}m^h > (1 + \eta)^{k+1}n^k . \]

This implies that \( s_h > t_k \) and \( c(s_h) \geq c(t_k) \) (by monotonicity of \( c \)), hence

\[ hc(m) + 3h\varepsilon > kc(n) - 3k\varepsilon \]

and

\[ \frac{h}{k} > \frac{c(n) - 3\varepsilon}{c(m) + 3\varepsilon} . \]

It follows that

\[ \frac{\log n}{\log m} \geq \frac{c(n) - 3\varepsilon}{c(m) + 3\varepsilon} . \]

(But how come? *This is the first step I struggled with.* Don’t we assume that \( h/k > (\log n)/(\log m) \)? To combine inequalities by transitivity we would need this one be opposite!)

Nevertheless, we get

\[ \frac{c(n)}{\log n} - \frac{c(m)}{\log m} \leq 3\varepsilon \left( \frac{1}{\log m} + \frac{1}{\log n} \right) \]

and, changing the roles of \( m \) and \( n \), the reverse inequality \( \cdots \geq -3\varepsilon \). So we have proved that

\[ \left| \frac{c(n)}{\log n} - \frac{c(m)}{\log m} \right| \leq 3\varepsilon \left( \frac{1}{\log m} + \frac{1}{\log n} \right) \]

whenever \( |b(m) - c(m)| < \varepsilon \) and \( |b(n) - c(n)| < \varepsilon \). This implies

\[ \left| \frac{c(n)}{\log n} - \frac{c(m)}{\log m} \right| \leq (|b(m) - c(m)| + |b(n) - c(n)|) \left( \frac{3}{\log m} + \frac{3}{\log n} \right) . \]
for all $m, n$. (But how come? This is the second step I struggled with. Let’s say that the penultimate displayed inequality holds for every $m, n$ as an equality for $3\varepsilon$ replaced with $2\varepsilon$, and that we have $m, n$ such that $|b(m) - c(m)|, |b(n) - c(n)| < \varepsilon/4$. The last two displayed inequalities then contradict each other!).

Nevertheless, we conclude the proof. Obviously, $|b(n_i) - c(n_i)| \to 0$ for a sequence $n_1 < n_2 < \ldots$. The last displayed inequality shows that the values $c(n_i)/\log n_i$ are bounded. Passing to a subsequence we get $\lim_i c(n_i)/\log n_i = \alpha$, with a finite limit $\alpha$. Setting $n = n_i$ and letting $i \to \infty$ gives

$$|c(m) - \alpha \log m| \leq 3|b(m) - c(m)| \quad \text{and} \quad |b(m) - \alpha \log m| \leq 4|b(m) - c(m)|$$

for every $m \in \mathbb{N}$ (well, $m \geq 2$). Thus, given any $\varepsilon > 0$, $|b(m) - \alpha \log m| < \varepsilon$ for all but $o(x)$ numbers $m \leq x$. Let $E \subset \mathbb{N}$ be the set of exceptional $m$; it has density 0. We take any $m \in \mathbb{N}$. The set $X = \{n \in \mathbb{N} \mid (n, m) = 1, n, mn \not\in E\}$ has positive density. For any $n \in X$ we have

$$|b(n) - \alpha \log n|, |b(mn) - \alpha \log(mn)| < \varepsilon.$$

So, by the additivity of the functions $b$ and $\log, \varepsilon > |b(mn) - \alpha \log(mn)| \geq |b(m) - \alpha \log m| - |b(n) - \alpha \log n|$ and $|b(m) - \alpha \log m| < 2\varepsilon$. As this holds for any $\varepsilon > 0$, we get the desired equality

$$b(m) = \alpha \log m \quad \text{or} \quad f(m) = m^\alpha$$

for every $m \in \mathbb{N}$. We are done. Well, . . .

### 3 Concluding remarks

How do we resolve the two conundrums? In the first we have three real quantities $a = h/k$, $b = (\log n)/(\log m)$, and $c = (c(n) - 3\varepsilon)/(c(m) + 3\varepsilon)$ and we know that $a > b \Rightarrow a > c$. From $b > a, a > c$ we would get $b > c$ by transitivity. However, in our situation also $a > b \Rightarrow a > c$ implies $b \geq c$, via a more subtle argument relying on the density of $\mathbb{Q}$ in $\mathbb{R}$. The point is that we may select $a$ larger than $b$ and as close to $b$ as we wish. Assume for contrary that $c > b$. Then we select $a$ in-between as $c > a > b$, and $a > b \Rightarrow a > c$ gives $a > c$, a contradiction. Thus $b \geq c$. The second conundrum is more psychological and stems from assuming $\varepsilon > 0$ to be a fixed thing. But if we drop it and regard $\varepsilon$ as a variable on par with $m, n$, everything is clear. We know that $|b(m) - c(m)|, |b(n) - c(n)| < \varepsilon \Rightarrow [c(m)/\log n - c(n)/\log m] \leq 3\varepsilon (1/\log m + 1/\log n)$. Thus for $m, n \in \mathbb{N}$ (and $m, n \geq 2$) we just set $\varepsilon = |b(m) - c(m)| + |b(n) - c(n)|$ and the implication yields the stated conclusion (perturbing $\varepsilon$ a little bit we may assume that $|b(n) - c(n)| > 0$ for every $n \in \mathbb{N}$).

Birch’s article [2] is cited in [1, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14].

It all started when I read the recent preprint of Shiu [18] that reproves Segal’s result [16, 17] that Euler’s function $\varphi(n)$ does not have non-decreasing normal order, as a corollary of the next nice theorem.
Theorem (Shiu, 2016; Segal, 1964). If $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ has a non-decreasing normal order, $f(n) = O(n)$, and $\sum_{n \leq x} f(n) \sim Ax^2/2$ and $\sum_{n \leq x} f(n)^2 \sim Bx^3/3$ as $x \to +\infty$ for some constants $A, B > 0$, then $A^2 \geq B$.

For $f(n) = \varphi(n)$ (which is $O(n)$) we have $A = \prod_p (1 - p^{-2})$ and $B = \prod_p (1 - 2p^{-2} + p^{-3})$ (see [18] for proofs of these average orders). Since $A^2 < B$, we conclude that $\varphi(n)$ does not have non-decreasing normal order. It follows also from Birch’s theorem, since $\varphi(n)$ is multiplicative (and unbounded). For results on sets where $\varphi(n)$ itself is monotonous see Pollack, Pomerance, and Treviño [15].

Finally, I was inspired by all this and the discussion at [19] to pose the following problem.

Problem (MK, 2016). Does $\varphi(n)$ have an effective normal order? That is, is there a function $g : \mathbb{N} \to \mathbb{N}$ such that for every $\varepsilon > 0$, $\#(n \leq x \mid \frac{\varphi(n)}{g(n)} \notin (1 - \varepsilon, 1 + \varepsilon)) = o(x)$ as $x \to +\infty$, and one can compute $n \mapsto g(n)$ in time polynomial in $\log n$?

References

[1] J.-P. Allouche, M. Mendès France, and J. Peyrière, Automatic Dirichlet series, J. Number Theory 81 (2000) 359–373.
[2] B. J. Birch, Multiplicative functions with non-decreasing normal order, J. London Math. Soc. 42 (1967) 149–151.
[3] P. D. T. A. Elliott, On a conjecture of Narkiewicz about functions with non-decreasing normal order, Colloq. Math. 36 (1976) 289–294.
[4] P. D. T. A. Elliott, Probabilistic Number Theory. I. Mean-value Theorems, Springer-Verlag, New York–Berlin, 1979.
[5] P. D. T. A. Elliott, Arithmetic Functions and Integer Products, Springer-Verlag, New York, 1985.
[6] P. Erdős and C. Ryavec, A characterization of finitely monotonic additive functions, J. London Math. Soc. 5 (1972), 362–367.
[7] J.-M. de Koninck, Review of [5] and [12], Bull. Amer. Math. Soc. 18 (1988), 230–247.
[8] J.-M. de Koninck, N. Doyon, and P. Letendre, On the proximity of additive and multiplicative functions, Funct. Approx. Comment. Math. 52 (2015) 327–344.
[9] J.-M. de Koninck and F. Luca, *Analytic Number Theory. Exploring the Anatomy of Integers*, American Mathematical Society, Providence, RI, 2012.

[10] K. Kovács, On the characterization of additive and multiplicative functions, Studia Sci. Math. Hungar. 18 (1982) 1–11.

[11] L. Matthiesen, Correlations of the divisor function, Proc. Lond. Math. Soc. 104 (2012) 827–858.

[12] P. J. McCarthy, *Introduction to Arithmetical Functions*, Springer-Verlag, New York, 1986.

[13] W. Narkiewicz, *Teoria liczb*, Państwowe Wydawnictwo Naukowe, Warszawa, 1990 (in Polish).

[14] W. Narkiewicz, *Number Theory*, World Scientific Publishing Co., Singapore, 1983 (translated from the 1977 edition of [13] by S. Kanemitsu).

[15] P. Pollack, C. Pomerance, and E. Treviño, Sets of monotonicity for Euler’s totient function, Ramanujan J. 30 (2013) 379–398.

[16] S.L. Segal, A note on normal order and the Euler $\varphi$-function, J. London Math. Soc. 39 (1964) 400–404.

[17] S.L. Segal, On non-decreasing normal orders, J. London Math. Soc. 40 (1965) 459–466.

[18] P. Shiu, On functions without a normal order, preprint, arXiv:1606.04533, June 2016, 4 pages.

[19] How hard is it to compute the Euler totient function?, http://mathoverflow.net/questions/3274/

**Charles University, KAM MFF UK, Malostranské nám. 25, 11800 Praha, Czechia**