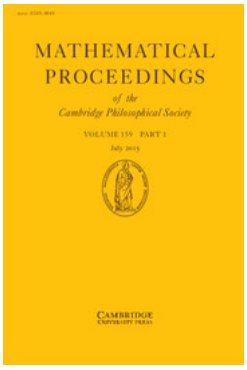

Note on a problem of Erdős

B. J. Birch

Mathematical Proceedings of the Cambridge Philosophical Society / Volume 55 / Issue 04 / October 1959, pp 370 - 373
DOI: 10.1017/S0305004100034150, Published online: 24 October 2008

REFERENCES

(1) Birch, B. J. The inhomogeneous minimum of quadratic forms of signature zero. *Acta Arithmetica*, 4 (1958), 85–98.
(2) Blaney, H. Indefinite quadratic forms in n variables. *J. Lond. Math. Soc.* 23 (1948), 153–60.
(3) Foster, D. M. E. Indefinite quadratic polynomials in n variables. *Mathematika*, 3 (1956), 111–16.
(4) Ridout, D. Indefinite quadratic forms. *Mathematika*, 5 (1958), 122–4.
(5) Watson, G. L. The minimum of an indefinite quadratic form with integral coefficients. *J. Lond. Math. Soc.* 32 (1957), 503–7.

University College
London

NOTE ON A PROBLEM OF ERDŐS

By B. J. BIRCH

Received 5 May 1959

1. In this note, I will prove the following conjecture ascribed to Erdős:

Theorem. *Let p, q be coprime integers. Then there is an $N(p,q)$ such that every $n > N(p,q)$ may be expressed as a sum of distinct numbers of the form $p^a q^b$, i.e. $n = \Sigma p^a q^b$ where the sum is over some set of distinct pairs of positive integers (a,b).*

Prof. Davenport has suggested that the result may be strengthened by requiring that the power q^b should be bounded independently of n. This may in fact be done on the lines of the present proof without any further idea—however, I shall not give the details, which are easy to supply, as they would make the work harder to follow.

The number $N(p,q)$ seems to be quite large, even when p and q are small. If one of p, q is 2, then trivially $N(2,q) = 0$ (since every number may be written in binary form). However $N(3,4) = 54$, $N(3,5) = 22$, $N(3,7) = 135$, and $N(4,5) > 400$.

I present the proof as I found it—that is, back to front. After two paragraphs of preparation, the argument will be in three steps, of which the first two simplify the problem, and the third completes the proof.

2. *Notation.* Any number of the form $p^a q^b$ is completely specified by the pair (a, b), which may be thought of as an integer lattice point in the first quadrant; we will denote the first quadrant by $\mathcal{Q}$. A sum of distinct $p^a q^b$ thus corresponds to a set $\mathscr{E}$ of lattice points with $\mathscr{E} \subseteq \mathcal{Q}$—we write

$$\sum_{(a,b)\in\mathscr{E}} p^a q^b = \phi_{p,q}(\mathscr{E}) = \phi(\mathscr{E})$$

for short.

We use $\cup$, $\cap$ for set-theoretic union and intersection; but $+$ and $-$ will refer to vector addition and subtraction. That is,

$$(a,b)\in[\mathscr{E}-(A,B)] \quad \text{if and only if} \quad (a+A, b+B)\in\mathscr{E}.$$

Note that $\phi(\mathscr{E}_1 \cup \mathscr{E}_2) = \phi(\mathscr{E}_1) + \phi(\mathscr{E}_2)$ if $\mathscr{E}_1$ and $\mathscr{E}_2$ are disjoint. The expression $\phi(\mathscr{E})$ retains its meaning even if $\mathscr{E}$ is not contained in $\mathscr{Q}$.

3. *Preliminary Lemmas.* First, we show that the theorem is at least plausible, in the sense that there is a sufficient supply of $\phi(\mathscr{E})$.

LEMMA 1. *Given X, let $E(X)$ be the number of sets $\mathscr{E}$ such that $\phi(\mathscr{E}) < X$. Then $E(X)/X \to \infty$ as $X \to \infty$.*

Proof. There are at least $\frac{1}{4}\log_p X$ powers of p less than $X^{\frac{1}{2}}$, and at least $\frac{1}{4}\log_q X$ powers of q less than $X^{\frac{1}{2}}$. Hence, there are at least $\frac{1}{16}\log_p X . \log_q X$ distinct $p^a q^b$ less than $X^{\frac{1}{2}}$. The sum of all of these is at most $X^{\frac{1}{2}}\log^2 X/16 \log p \log q$, which is less than X for large enough X; so any subset of them gives an $\mathscr{E}$ with $\phi(\mathscr{E}) < X$. Hence

$$E(X) \geqslant 2^{\frac{1}{16}\log_p X \log_q X} > X^2$$

for large enough X.

COROLLARY. *For any coprime p, q, there are disjoint sets $\mathscr{E}_1$, $\mathscr{E}_2$ contained in $\mathscr{Q}$ such that $\phi_{p,q}(\mathscr{E}_1) = \phi_{p,q}(\mathscr{E}_2)$.*

This is simply a tremendous weakening of the lemma. For example,

$$1 + 5^2 + 5.7 = 5 + 7 + 7^2 = 61, \quad 5^2.7 = 1 + 7^2 + 5^3 = 175.$$

We will also need

LEMMA 2. *There is an X_0 such that for every $X > X_0$ there is a $p^a q^b$ between $\frac{3}{4}X$ and X (that is, such that $\frac{3}{4}X < p^a q^b < X$).*

This is trivial; we may indeed find b bounded independently of X.

4. We may now start on the serious business of proving the theorem. Our first step is

Prop. A. The gaps between successive $\phi(\mathscr{E})$ (with $\mathscr{E} \subseteq \mathscr{Q}$) are bounded in length.

For, suppose that there was a gap from say X to $X + Y$, such that no ξ between X and $X + Y$ is of the form $\phi(\mathscr{E})$. Suppose that $X > X_0$; then $Y < \frac{1}{2}X$, otherwise Lemma 2 gives us a ξ of the form $p^a q^b$ between $X + \frac{1}{4}Y$ and $X + Y$. By Lemma 2 there is a $p^A q^B$ between $\frac{3}{4}X$ and X; and then no ξ' between $X - p^A q^B$ and $X + Y - p^A q^B$ is of the form $\phi(\mathscr{E}')$. (For if $\xi' = \phi(\mathscr{E}')$, then $\xi' < \frac{3}{2}X - p^A q^B < p^A q^B$; thus $(A, B) \notin \mathscr{E}'$, and $\xi = \xi' + p^A q^B$ would be a number between X and $X + Y$ of the form $\phi(\mathscr{E})$, with $\mathscr{E} = \mathscr{E}' \cup (A, B)$.) Hence if we have a gap from X to $X + Y$, with $X > X_0$, then we can find another earlier gap of the same length. Accordingly, the greatest gap-length must occur with some $X \leqslant X_0$; and so, by Lemma 2 again, the gaps between successive $\phi(\mathscr{E})$ never exceed X_0.

COROLLARY. *Given any X, there is a $Y < X_0$ and an $\mathscr{E} \subseteq \mathscr{Q}$ such that $X - Y = \phi(\mathscr{E})$.*

For example, in the case $(p, q) = (5, 7)$, the above line of argument shows that the longest gap-length must occur before 125. In fact, the longest gap is from 14 to 24 inclusive; this gap is repeated as 139–149.

5. The second step in our proof is

Prop. B. To prove the theorem it will be enough to show that the numbers $\phi(\mathscr{E})$ with $\mathscr{E} \subseteq \mathscr{Q}$ contain a complete arithmetic progression of the shape $m.p^A q^B + R$ for integer $m \geqslant 0$.

Indeed, if every $m.p^Aq^B+R$ is of the form $\phi(\mathscr{E})$, then every number of the progression $pq(m.p^Aq^B+R)$ is of the form $\phi(\mathscr{E}')$, where $\mathscr{E}'$ contains no point (a,b) with either a or b zero. So it is enough to show that we can fill in the gaps of this progression by adding on appropriate powers of p and appropriate powers of q. This is easy—any residue class modulo q^{B+1} is congruent to a sum of distinct powers of p^{A+1}, e.g. $p^{(A+1)D} \equiv 1 \pmod{q^{B+1}}$ if $D = \phi(q^{B+1})$, whence $\sum_{k=1}^{\rho} p^{(A+1)Dk} \equiv \rho \pmod{q^{B+1}}$; and similarly $q^{(B+1)E} \equiv 1 \pmod{p^{A+1}}$ for $E = \phi(p^{A+1})$. Thus, if $X \equiv T \pmod{p^{A+1}q^{B+1}}$, then

$$X - \Sigma(p^{(A+1)Dk} + q^{(B+1)Ek}) \equiv pqR \pmod{p^{A+1}q^{B+1}},$$

where the sum is taken from $k=1$ to $k = p^{A+1}q^{B+1}+T-pqR$; and then $X-\Sigma > 0$ so long as say $X > (pq)^F$ with $F = (A+B+1)(pq)^{2(A+B)}$. Thus $X-\Sigma = \phi(\mathscr{E}')$ by hypothesis, and the theorem will follow.

6. Now we come to our final step.

Prop. C. The numbers of the form $\phi(\mathscr{E})$ with $\mathscr{E} \subseteq \mathscr{Q}$ contain a complete arithmetic progression of form $m.p^Aq^B+R$, for $m \geqslant 0$.

The theorem will follow immediately when we combine this with Prop. B. It is convenient to prove Prop. C in the form

Prop. C'. There are integers $A \geqslant 0, B \geqslant 0$ and a rational number $r = R/p^Aq^B$ such that $m+r$ is of the shape $\phi[\mathscr{E}-(A,B)]$ with $\mathscr{E} \subseteq \mathscr{Q}$, for all integers $m \geqslant 0$.

To do this, we will use the Corollary of Lemma 1 to fill in the gaps left after Prop. A. Suppose that $\phi(\mathscr{E}_1) = \phi(\mathscr{E}_2)$ with $\mathscr{E}_1 \cap \mathscr{E}_2 = 0$. Take (A_1, B_1) in $\mathscr{E}_1 \cup \mathscr{E}_2$ so that (A_1+B_1) is as large as possible. Say $(A_1, B_1) \in \mathscr{E}_2$; then we have $p^{A_1}q^{B_1} = \phi(\mathscr{F}_1) - \phi(\mathscr{G}_1)$ where $\mathscr{F}_1 = \mathscr{E}_1$ and $\mathscr{G}_1 \cup (A_1, B_1) = \mathscr{E}_2$. Thus we have an identity

$$1 = \phi[\mathscr{F}_1 - (A_1, B_1)] - \phi[\mathscr{G}_1 - (A_1, B_1)],$$

where the sets $\mathscr{Q}, \mathscr{F}_1-(A_1,B_1), \mathscr{G}_1-(A_1,B_1)$ are disjoint.

To prove the proposition we will need several such identities. Suppose then that we have found points and sets $(A_i, B_i), \mathscr{F}_i, \mathscr{G}_i$ for $i = 1, \ldots, X_0$ such that

(i) $1 = \phi[\mathscr{F}_i-(A_i,B_i)] - \phi[\mathscr{G}_i-(A_i,B_i)]$ for $i = 1, \ldots, X_0$;

(ii) the $(2X_0+1)$ sets $\mathscr{Q}, \mathscr{F}_i-(A_i,B_i), \mathscr{G}_i-(A_i,B_i)$ are all disjoint;

(iii) the sequences $\{A_i\}, \{B_i\}$ are both increasing.

Write

$$r = \sum_{i=1}^{X_0} [\mathscr{G}_i-(A_i,B_i)], \quad A = \max(A_i), \quad B = \max(B_i),$$

so that in fact $A = A_{X_0}$, $B = B_{X_0}$. Then $r = R/p^Aq^B$, a rational number with denominator p^Aq^B. Suppose X is a positive integer. Then by Prop. A, Corollary, we can find $Y < X_0$ such that $X = Y + \phi(\mathscr{E})$ with $\mathscr{E} \subseteq \mathscr{Q}$. But now,

$$\begin{aligned} X+r &= Y + \phi(\mathscr{E}) + \sum_{i=1}^{X_0} \phi[\mathscr{G}_i-(A_i,B_i)] \\ &= \phi(\mathscr{E}) + \sum_{i=1}^{Y} \phi[\mathscr{F}_i-(A_i,B_i)] + \sum_{i=Y+1}^{X_0} \phi[\mathscr{G}_i-(A_i,B_i)], \text{ by (i)}, \\ &= \phi[\mathscr{H}-(A,B)] \end{aligned}$$

for short, where

$$\mathscr{H} = [\mathscr{E} + (A, B)] \cup \bigcup_{i=1}^{Y} [\mathscr{F}_i + (A - A_i, B - B_i)] \cup \bigcup_{i=Y+1}^{X} [\mathscr{G}_i + (A - A_i, B - B_i)];$$

so that $\mathscr{H}$ is, as required, a union of disjoint subsets of $\mathscr{Q}$.

This will complete the proof of Prop. C′ once we have shown how to find (A_i, B_i), $\mathscr{F}_i, \mathscr{G}_i$ to satisfy (i), (ii), (iii). But this is easy. We have already found $A_1, B_1, \mathscr{F}_1, \mathscr{G}_1$ by applying the Corollary to Lemma 1 with $P = p$, $Q = q$. Now we find $A_2, B_2, \mathscr{F}_2, \mathscr{G}_2$ by applying the Corollary with $P = p^{A_1+1}$, $Q = q^{B_1+1}$; $\mathscr{F}_2 - (A_2, B_2), \mathscr{G}_2 - (A_2, B_2), \mathscr{F}_1 - (A_1, B_1), \mathscr{G}_1 - (A_1, B_1)$ are disjoint since the points of $\mathscr{F}_2 - (A_2, B_2), \mathscr{G}_2 - (A_2, B_2)$ have coordinates altogether larger than those of the points of $\mathscr{F}_1 - (A_1, B_1), \mathscr{G}_1 - (A_1, B_1)$. After this we proceed inductively—at the ith stage, we find $A_i, B_i, \mathscr{F}_i, \mathscr{G}_i$ by applying the Corollary with $P = p^{A_{i-1}+1}$, $Q = q^{B_{i-1}+1}$.

This completes the proof of the theorem.

[*Note added in proof.*] The theorem of this note has been beautifully generalized by J. W. S. Cassels in a paper probably to be published in Acta Mathematica Szeged.

TRINITY COLLEGE
CAMBRIDGE

ON THE COEFFICIENTS OF UNIVALENT FUNCTIONS

BY W. K. HAYMAN

Received 30 January 1959

Suppose that $f(z) = \sum_1^\infty a_n z^n$ and $g(z) = \sum_1^\infty b_n z^n$ are regular in $|z| < 1$ and set

$$f(z) \circ g(z) = \sum_1^\infty \frac{a_n b_n}{n} z^n.$$

S. Mandelbrojt (*The New Scottish Book*, Problem 344) conjectured that if f and g are univalent in $|z| < 1$, then so is $f \circ g$. In particular if $f_p(z)$ is defined inductively by $f_1(z) = f(z), f_{p+1}(z) = f_p(z) \circ f(z)$, it would follow from this that if $f(z)$ is univalent, then so is $f_p(z)$ for every positive integer p.

We shall provide a counterexample to the above conjecture by proving the following

THEOREM. *Suppose that* $p \geqslant 3, (p-2)/p < \cos\lambda < 1$ *and* $b = 1 + e^{i\lambda}$. *Then*

$$f(z) = (1-z)^{-b} - 1$$

is univalent in $|z| < 1$ *but* $f_p(z)$ *is not.*

Elementary considerations show that

$$\zeta = \xi + i\eta = b \log [1/(1-z)]$$