OSTROWSKI'S THEOREM FOR Q

KEITH CONRAD

1. Introduction

Hensel created the p-adic numbers towards the end of the 19th century, and it wasn't until about 20 years later that Ostrowski [1] proved a fundamental theorem that explained in retrospect why Hensel's idea was natural: every nontrivial absolute value on $\mathbf{Q}$ is a power of the ordinary (archimedean) absolute value or a power of a p-adic absolute value for some prime number p, so every completion of $\mathbf{Q}$ with respect to a nontrivial absolute value is either $\mathbf{R}$ or some $\mathbf{Q}_p$.

Theorem 1 (Ostrowski, 1916)**.** *If $|\cdot|$ is a nontrivial absolute value on $\mathbf{Q}$ then there is $t > 0$ such that either $|\cdot| = |\cdot|_\infty^t$ or $|\cdot| = |\cdot|_p^t$ for a prime p.*

Proof. An absolute value on $\mathbf{Q}$ is determined by its values on the positive integers, so it suffices to show there is a $t > 0$ such that $|n| = n^t$ for all n in $\mathbf{Z}^+$ or $|n| = |n|_p^t$ for some prime p and all n in $\mathbf{Z}^+$.

Since $|\cdot|$ is nontrivial, $|n| \neq 1$ for some positive integer n. We consider two cases: $|n| > 1$ for some $n \geq 2$ or $|n| \leq 1$ for all $n \geq 2$. We will show in the first case that $|\cdot|$ is a power of the ordinary absolute value on $\mathbf{Q}$ and in the second case that $|\cdot|$ is a power of some p-adic absolute value.

Case 1: $|n| > 1$ for some $n \geq 2$.

First we prove that $|n| > 1$ for all $n \geq 2$ by proving the contrapositive: if $|n_0| \leq 1$ for some $n_0 \geq 2$ then $|n| \leq 1$ for all $n \geq 2$. Write n in base n_0:

$$n = a_0 + a_1 n_0 + \cdots + a_d n_0^d$$

where $0 \leq a_i \leq n_0 - 1$ and $a_d \neq 0$, so $n_0^d \leq n < n_0^{d+1}$. We have $|a_i| \leq |1 + 1 + \cdots + 1| \leq |1| + |1| + \cdots + |1| = a_i < n_0$, so

$$|n| \leq |a_0| + |a_1||n_0| + \cdots + |a_d||n_0|^d < n_0 + n_0|n_0| + \cdots + n_0|n_0|^d. \tag{1}$$

From $|n_0| \leq 1$, (1) implies $|n| \leq n_0(d+1) \leq n_0(\log_{n_0}(n) + 1)$. Replace n by n^k in this inequality to get $|n|^k \leq n_0(k \log_{n_0}(n) + 1)$, so

$$|n| \leq \sqrt[k]{n_0(k \log_{n_0}(n) + 1)}. \tag{2}$$

We have $\log_{n_0}(n) > 0$ since $n_0 > 1$ and $n > 1$, so letting $k \to \infty$ in (2) shows us that $|n| \leq 1$, and n was arbitrary.

The replacement of n with n^k is an idea we will use again. Let's call it the "power trick."

For any integers m and n that are greater than 2, $|m| > 1$ and $|n| > 1$. Picking $d \geq 0$ so that $m^d \leq n < m^{d+1}$, writing n in base m implies (in the same way that we proved (1) above)

$$|n| \leq m(1 + |m| + \cdots + |m|^d).$$

Since $|m| > 1$, summing up the finite geometric series on the right gives us

$$|n| \leq m(1 + |m| + \cdots + |m|^d) = m\frac{|m|^{d+1} - 1}{|m| - 1} < m\frac{|m|^{d+1}}{|m| - 1} = \frac{m|m|}{|m| - 1}|m|^d.$$

Since $d \leq \log_m(n)$,

$$|n| < \frac{m|m|}{|m| - 1}|m|^{\log_m(n)}.$$

Now it's time for the power trick. Replacing n with n^k,

$$|n|^k < \frac{m|m|}{|m| - 1}|m|^{k\log_m(n)}.$$

Taking kth roots,

$$|n| < \sqrt[k]{\frac{m|m|}{|m| - 1}}|m|^{\log_m(n)},$$

and letting $k \to \infty$,

$$|n| \leq |m|^{\log_m(n)}. \tag{3}$$

Writing $|m| = m^s$ and $|n| = n^t$ where $s > 0$ and $t > 0$, we get from (3) that $n^t \leq m^{s\log_m(n)} = n^s$, so $t \leq s$. The roles of m and n in this calculation are symmetric, so by switching their roles we get $s \leq t$ and thus $|m| = m^t$ and $|n| = n^t$.

Case 2: $|n| \leq 1$ for all $n \geq 2$.

For some $n \geq 2$ we have $|n| \neq 1$, so $0 < |n| < 1$. Let p be the smallest such positive integer. Since $0 < |p| < 1$ and also $0 < 1/p < 1$, we can write $|p| = (1/p)^t$ for some $t > 0$. We will prove $|n| = |n|_p^t$ for all $n \geq 1$.

The number p is prime, by contradiction: if $p = ab$ where a and b are positive integers that are both smaller than p then $|a| = 1$ and $|b| = 1$, so $|p| = |a||b| = 1$, which is false.

Next we show each positive integer m not divisible by p has $|m| = 1$. If $|m| \neq 1$ then $|m| < 1$. We are going to use the power trick again: let's look at p^k and m^k. Since $|p|$ and $|m|$ are both between 0 and 1, for a large k we have $|p|^k < 1/2$ and $|n|^k < 1/2$. Since p^k and m^k are relatively prime, there are x_k and $y_k \in \mathbf{Z}$ such that $1 = p^k x_k + m^k y_k$. Take the absolute value of both sides:

$$1 = |p^k x_k + m^k y_k| \leq |p^k||x_k| + |m^k||y_k| \leq |p|^k + |m|^k < \frac{1}{2} + \frac{1}{2} = 1,$$

which is a contradiction.

For all integers $n \geq 2$ pull out the largest power of p: $n = p^e n'$ where $e \geq 0$ and n' is not divisible by p. Then $|n'| = 1$, so $|n| = |p^e n'| = |p|^e|n'| = |p|^e = (1/p)^{et}$. Also $|n|_p = (1/p)^e$, so $|n| = |n|_p^t$. □

Here is a second proof that an absolute value $|\cdot|$ on $\mathbf{Q}$ such that $|n| > 1$ for some positive integer $n \geq 2$ must be a power of the ordinary absolute value on $\mathbf{Q}$.

First we show $|2| > 1$ by an argument very close to that used already in Case 1, but we repeat it here to keep our argument self-contained. Assuming $|2| \leq 1$ we will get a contradiction.

Write each integer $n \geq 2$ in base 2: $n = a_0 + a_1 \cdot 2 + \cdots + a_d 2^d$ where a_i is 0 or 1 and $a_d = 1$, so $2^d \leq n < 2^{d+1}$. Thus $|a_i|$ is 0 or 1, so by the triangle inequality

$$|n| \leq \sum_{i=0}^{d} |a_i||2|^i \leq \sum_{i=0}^{d} 1 = d + 1 \leq \log_2(n) + 1 \leq 2\log_2(n).$$

This holds for all $n \geq 2$, so if we replace n throughout with n^k for $k \geq 1$ then

$$|n^k| \leq 2\log_2(n^k) = 2k\log_2(n),$$

so

$$|n|^k \leq 2k\log_2(n).$$

Taking kth roots of both sides,

$$|n| \leq \sqrt[k]{2k\log_2(n)}.$$

Letting $k \to \infty$, this inequality becomes $|n| \leq 1$. We have proved this for all $n \geq 2$, but that contradicts the assumption $|n| > 1$ for some $n \geq 2$, so in fact we must have $|2| > 1$.

Since $|2|$ and 2 are both greater than 1, we can write $|2| = 2^t$ for some $t > 0$. We will prove $|n| = n^t$ for all $n \geq 2$ by proving $|n| \leq n^t$ (easier) and $|n| \geq n^t$ (trickier).

As we have already done, write an integer $n \geq 1$ in base 2: $n = a_0 + a_1 \cdot 2 + \cdots + a_d 2^d$ with a_i equal to 0 or 1 and $a_d = 1$, so $2^d \leq n < 2^{d+1}$. An upper bound on n follows easily from the triangle inequality:

$$|n| \leq |a_0| + |a_1||2| + \cdots + |a_d||2|^d \leq 1 + |2| + \cdots + |2|^d = \frac{|2|^{d+1} - 1}{|2| - 1}.$$

Writing $|2|$ as 2^t,

$$|n| \leq \frac{2^{t(d+1)} - 1}{2^t - 1} < \frac{2^{t(d+1)}}{2^t - 1} = \frac{2^t}{2^t - 1} 2^{td} \leq \frac{2^t}{2^t - 1} n^t.$$

It's time to use the power trick again: replacing n in this inequality by n^k with $k \geq 1$,

$$|n|^k < \frac{2^t}{2^t - 1} n^{kt}.$$

Taking kth roots of both sides implies

$$|n| \leq \sqrt[k]{\frac{2^t}{2^t - 1}} n^t.$$

Letting $k \to \infty$ (keeping n fixed), we get

$$|n| \leq n^t \tag{4}$$

for all $n \in \mathbf{Z}^+$ (it is obvious at $n = 1$).

To prove the reverse inequality $|n| \geq n^t$ for $n \geq 2$, once again write n in base 2: $n = a_0 + a_1 \cdot 2 + \cdots + a_d 2^d$ with $a_i = 0$ or 1 and $a_d = 1$, so $2^d \leq n < 2^{d+1}$. Once again we use the triangle inequality, but in a less obvious way:

$$|2^{d+1}| = |2^{d+1} - n + n| \leq |2^{d+1} - n| + |n|.$$

On the left side, $|2^{d+1}| = |2|^{d+1} = 2^{t(d+1)}$. On the right side, since $2^{d+1} - n$ is a positive integer we get $|2^{d+1} - n| \leq (2^{d+1} - n)^t$ by (4), so

$$2^{t(d+1)} \leq (2^{d+1} - n)^t + |n|.$$

From this we obtain a *lower bound* on $|n|$:

$$|n| \geq 2^{t(d+1)} - (2^{d+1} - n)^t.$$

To decrease this lower bound we can increase $2^{d+1} - n$: since n is between 2^d and 2^{d+1}, we have $2^{d+1} - n \leq 2^{d+1} - 2^d = 2^d$, so

$$|n| \geq 2^{t(d+1)} - 2^{td} = (2^t - 1)2^{td} \leq (2^t - 1)n^t.$$

One more time we will use the power trick: replace n by n^k and take kth roots to get

$$|n| \geq \sqrt[k]{2^t - 1}\, n^t.$$

Letting $k \to \infty$, we get $|n| \geq n^t$. Since we already showed $|n| \leq n^t$, we have shown $|n| = n^t$ for all $n \in \mathbf{Z}^+$.

References

[1] A. Ostrowski, *Über einige Lösungen der Funktionalgleichung*, Acta Arith. **41** (1916), 271–284.