OSTROWSKI'S THEOREM

The prime numbers also arise in a very surprising manner, having little to do with factoring integers. Namely they arise as the possible ways of defining absolute values on $\mathbb{Q}$. We begin by defining what an absolute value is.

We say that a function $f : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ is an absolute value if it satisfies the following properties, for all x, $y \in \mathbb{Q}$:
(i) We have $f(0) = 0$ and $f(x) > 0$ for $x \neq 0$.
(ii) Multiplicativity: $f(xy) = f(x)f(y)$.
(iii) Triangle inequality: $f(x + y) \leq f(x) + f(y)$.

Remarks. From (i, ii) we see that $f(1) = f(-1) = 1$. Moreover, to define f on $\mathbb{Q}$, by (ii) it suffices to define it on $\mathbb{Z}$. Since $f(1) = 1$ using (iii) it follows that $f(n) \leq |n|$ for all $n \in \mathbb{Z}$.

Example 1. The usual absolute value, $f(x) = |x|$, plainly satisfies these properties.

Example 2. Let $0 \leq \alpha \leq 1$, and take $f(x) = |x|^\alpha$. Check that this is an absolute value. The case $\alpha = 0$ gives a 'trivial' absolute value: $f(0) = 0$, $f(x) = 1$ for all $0 \neq x \in \mathbb{Q}$.

Example 3. Let p be a prime number. If $0 \neq n \in \mathbb{Z}$ we write $n = p^a b$ with $p \nmid b$. Define $|n|_p = p^{-a}$. If $m/n \in \mathbb{Q}$ set $|m/n|_p = |m|_p/|n|_p$. This gives an example of an absolute value, called the p-adic valuation. Note that the p-adic absolute value satisfies a stronger version of the triangle inequality:

$$|x + y|_p \leq \max(|x|_p, |y|_p).$$

This inequality is sometimes called the *ultrametric inequality*, and p-adic absolute values are termed *non-Archimedean*.

Example 4. Let $\alpha \geq 0$ be a real number, and take $f(x) = |x|_p^\alpha$. Such f are also absolute values.

Theorem (Ostrowski). *Examples 2 and 4 give all the possible absolute values on* $\mathbb{Q}$.

Case 1. Suppose first that there is some natural number n such that $f(n) < 1$. We may consider the least such natural number, and because of (ii) that least number must be a prime p. We now claim that the absolute value f corresponds to the p-adic absolute value $|\cdot|_p$ as in Examples 3 and 4. Take an integer b, and write it in base p; say $b = b_0 + b_1 p + \ldots + b_k p^k$ with $0 \leq b_j \leq p - 1$, and $b_k \geq 1$. Then

$$f(b) \leq f(b_0) + f(b_1) + \ldots + f(b_k) \leq (k + 1)(p - 1) < \Big(\frac{\log b}{\log p} + 1\Big)(p - 1),$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

since we know that $f(b_j) \leq b_j \leq p-1$. This inequality holds for all natural numbers b, and therefore it holds for b^n for any natural number n:

$$f(b)^n = f(b^n) \leq \Big(n\frac{\log b}{\log p} + 1\Big)(p-1).$$

Letting $n \to \infty$ above we obtain that $f(b) \leq 1$ for all integers b.

Knowing $f(p) < 1$ we possess all the values $f(p^k)$ for $k \geq 1$. To show that f corresponds to the p-adic absolute value, we now need that $f(b) = 1$ for all $(b,p) = 1$. Now if $(b,p) = 1$ then $(b^n, p^n) = 1$, and so we may find integers x_n and y_n with $1 = b^n x_n + p^n y_n$ so that

$$1 = f(1) \leq f(b^n x_n) + f(p^n y_n) \leq f(b)^n + f(p)^n.$$

Now $f(p) < 1$ so that as $n \to \infty$ we have $f(p)^n \to 0$, and so we must have $f(b) \geq 1$. Since we already know that $f(b) \leq 1$ we have shown that $f(b) = 1$ as needed.

Case 2. We may now suppose that $f(n) \geq 1$ for all natural numbers n. Let $a \geq 2$ be a natural number. Writing $b = b_0 + b_1 a + \ldots + b_k a^k$ in base a we find that

$$f(b) \leq (a-1)(1 + f(a) + \ldots + f(a)^k) \leq (k+1)(a-1)f(a)^k < \Big(\frac{\log b}{\log a} + 1\Big)(a-1)f(a)^{\frac{\log b}{\log a}}.$$

Replacing b by b^n above we get that

$$f(b)^n \leq \Big(n\frac{\log b}{\log a} + 1\Big)(a-1)f(a)^{n\frac{\log b}{\log a}}.$$

Letting $n \to \infty$ we obtain that

$$f(b) \leq f(a)^{\frac{\log b}{\log a}}.$$

Interchanging the roles of a and b we conclude that

$$f(b)^{\frac{1}{\log b}} = f(a)^{\frac{1}{\log a}},$$

for all natural numbers a, $b \geq 2$. Thus if we write $f(2) = 2^\alpha$ with $0 \leq \alpha \leq 1$, it follows that $f(n) = n^\alpha$ for all n, and we are in the situation of Example 2.