On discrete exponentiation

David Pierce

2006.02.17

Some of these remarks might be incorporated into my notes for Math 111, or an article on induction.

An **inductive** structure is one in which proof by induction is possible: so it is a structure that has a distinguished element and a singulary operation, but has no proper substructures. Usually the distinguished element is 0, and the operation is $x \mapsto x + 1$. On such a structure, the operations of addition and multiplication can be defined.

Let $\mathfrak{A}$ be an inductive structure. Then there is a homomorphism h from $(\omega, ', 0)$ into $\mathfrak{A}$. If A is infinite, then h is an isomorphism. If A is finite, then $\mathfrak{A}$ has two (finite) cardinal invariants, which determine its isomorphism class:

(1) $\min\{x \in \omega : \exists y\ h(x + y + 1) = h(x)\}$;

(2) $\min\{y \in \omega : \exists x\ h(x + y + 1) = h(x)\}$.

Indeed, call these numbers k and n; then A has $k + n + 1$ elements, say

$$0, 1, \dots, k, k + 1, \dots, k + n;$$

and $s^{\mathfrak{A}}(x) = x + 1$, if $x \neq k + n$, but $s^{\mathfrak{A}}(k + n) = k$. If $k = 0$, then the structure is isomorphic to $\mathbb{Z}/(n + 1)$.

Exponentiation on inductive structures is an operation

$$(x, y) \longmapsto x^y$$

such that

$$x^0 = 1;$$
$$x^{y+1} = x^y \cdot x.$$

The value of 0^y is unimportant and can be left undefined.

Naïvely, but wrongly, one might argue that expontiation exists by induction: For, x^0 is defined, and if x^y is defined, then x^{y+1} is defined.

A correct way to proceed would be to define a family of functions f_x, where $x \neq 0$, such that

$$f_x(0) = 1;$$
$$f_x(y + 1) = f_x(y) \cdot x.$$

One may define f_1 as $y \mapsto 1$; then one attempts to define f_{x+1} in terms of f_x. But the attempt must fail, since if the structure is $\mathbb{Z}/(3)$, then $2^0 = 1$, $2^1 = 2$, $2^2 = 4 = 1$, so $2^3 = 2$; but also $2^3 = 2^0 = 1$, so $2 = 1$, which is absurd.

However, exponentiation is well-defined as a function from

$$\mathbb{F}_p{}^{\times} \times \mathbb{Z}/(p-1)$$

into

$$\mathbb{F}_p.$$

This is by the Fermat theorem

$$x^{p-1} \equiv 1 \pmod{p}.$$

Also, $\mathbb{F}_p{}^{\times}$ has a generator, α. Then we have the inductive structure

$$(\mathbb{F}_p{}^{\times}, s, 1).$$

where s is $x \mapsto x \cdot \alpha$. We also have an isomorphism f_α from $\mathbb{Z}/(p-1)$ into this structure, namely

$$y \longmapsto \alpha^y.$$

Let f_1 be $y \mapsto 1$ as before, and given f_x as desired, define

$$f_{s(x)}(y) = f_x(y) \cdot f_\alpha(y).$$

Then $f_{s(x)}(0) = 1$, and

$$\begin{aligned} f_{s(x)}(y+1) &= f_x(y+1) \cdot f_\alpha(y+1) \\ &= f_x(y) \cdot x \cdot f_\alpha(y) \cdot \alpha \\ &= f_x(y) \cdot f_\alpha(y) \cdot x \cdot \alpha \\ &= f_{s(x)}(y) \cdot s(x). \end{aligned}$$