

A simple problem solved, with heuristics

We are asked to show

$$(0) \quad p \sqsubseteq \frac{f \cdot p}{f \cdot i * f \cdot (p-i)} \quad (= \text{ “ } p \text{ choose } i \text{ ” })$$

for all p prime and i satisfying $1 \leq i < p$. Here \sqsubseteq is the relation “divides”, and f is the factorial function. All variables in this document are of type positive natural.

Because our demonstrandum is about integers and divisibility, we would like to eliminate the quotient expression from (0). The right side of (0) is an integer, hence we have:

$$(1) \quad f \cdot i * f \cdot (p-i) \sqsubseteq f \cdot p \quad .$$

And now, thanks to (1), we may rewrite (0) equivalently as:

$$(2) \quad p * f \cdot i * f \cdot (p-i) \sqsubseteq f \cdot p \quad .$$

Noting the syntactic similarity between (1) and (2), it is sweetly reasonable to try to prove (0) by proving $(2) \Leftarrow (1)$. Since (2) is more complicated than (1), we begin our calculation with (2).

Formally speaking, our task is to remove a factor of p from the left side of (2), and we do this straight away by exploiting properties of \sqsubseteq and f :

$$\begin{aligned} & p * f \cdot i * f \cdot (p-i) \sqsubseteq f \cdot p \\ \equiv & \{ f \cdot p = p * f \cdot (p-1) , \text{ since } 1 \leq p \} \\ & p * f \cdot i * f \cdot (p-i) \sqsubseteq p * f \cdot (p-1) \\ \equiv & \{ \text{cancelling } p , \text{ since } p \neq 0 \} \\ & f \cdot i * f \cdot (p-i) \sqsubseteq f \cdot (p-1) \quad . \end{aligned}$$

So far so good: we created the left side of our goal, but missed the right side by a factor of p . We can guess, however, at the remaining shape of the proof, starting with the reintroduction of p :

$$\begin{aligned} & f \cdot i * f \cdot (p-i) \sqsubseteq f \cdot (p-1) \\ \Leftarrow & \{ ??? \} \\ & f \cdot i * f \cdot (p-i) \sqsubseteq p * f \cdot (p-1) \\ \equiv & \{ \text{property of } f \} \\ & f \cdot i * f \cdot (p-i) \sqsubseteq f \cdot p \quad , \end{aligned}$$

JAW0-1

a beautiful shape indeed!

To design a suitable step ??? , we suppress some of the hopefully irrelevant detail (namely f and i) , and ask when we can conclude more generally:

$$(3) \quad m \sqsubseteq n \iff m \sqsubseteq p * n \quad .$$

Here we are hit in the face by Euclid's theorem which states that (3) follows from:

$$m \mathbf{gcd} p = 1 \quad ,$$

or, since p is prime, equivalently:

$$p \not\sqsubseteq m \quad .$$

Returning to our main calculation, we see that step ??? therefore follows from:

$$(4) \quad p \not\sqsubseteq f.i * f.(p-i) \quad .$$

Thus we set our sights on establishing (4) .

The shape of (4) suggests that we exploit one of the defining properties of primality, namely that for p prime, and i ranging over any bag of integers, we have:

$$(5) \quad p \not\sqsubseteq \langle *i :: i \rangle \equiv \langle \forall i :: p \not\sqsubseteq i \rangle \quad .$$

(If this looks unfamiliar, consider the contrapositive!) With property (5) in hand, we calculate with (4) :

$$\begin{aligned} & p \not\sqsubseteq f.i * f.(p-i) \\ \equiv & \{ (5) \} \\ & p \not\sqsubseteq f.i \wedge p \not\sqsubseteq f.(p-i) \\ \equiv & \{ \text{unfolding } f \text{ completely, twice} \} \\ & p \not\sqsubseteq \langle *j : 1 \leq j \leq i : j \rangle \wedge p \not\sqsubseteq \langle *j : 1 \leq j \leq p-i : j \rangle \\ \equiv & \{ (5) \text{ twice} \} \\ & \langle \forall j : 1 \leq j \leq i : p \not\sqsubseteq j \rangle \wedge \langle \forall j : 1 \leq j \leq p-i : p \not\sqsubseteq j \rangle \\ \Leftarrow & \{ \text{widening the range, since } 1 \leq i < p \text{ implies } i < p \text{ and } p-i < p \} \\ & \langle \forall j : 1 \leq j < p : p \not\sqsubseteq j \rangle \\ \equiv & \{ \text{property of } \sqsubseteq \} \\ & \mathbf{true} \quad . \end{aligned}$$

Thus we have established (4) , which completes the proof of the main theorem.

To conclude, we summarize the entire proof:

$$\begin{aligned}
 & p * f.i * f.(p-i) \sqsubseteq f.p \\
 \equiv & \quad \{ \text{property of } f , \quad 1 \leq p \} \\
 & p * f.i * f.(p-i) \sqsubseteq p * f.(p-1) \\
 \equiv & \quad \{ \text{cancelling } p , \quad p \neq 0 \} \\
 & f.i * f.(p-i) \sqsubseteq f.(p-1) \\
 \Leftarrow & \quad \{ \text{Euclid's theorem and (4)} \} \\
 & f.i * f.(p-i) \sqsubseteq p * f.(p-1) \\
 \equiv & \quad \{ \text{property of } f \} \\
 & f.i * f.(p-i) \sqsubseteq f.p \quad .
 \end{aligned}$$

Santa Cruz, 18 October 2004

Jeremy Weissmann
 jeremy@mathmeth.com