Tutorial on reasoning about recursion in Java

<table>
<tr><td>Q</td><td>You said in your lecture that reasoning about recursion in Java was just like in Haskell. I tried to reason about gcd but I'm finding it hard. Could you help?</td></tr>
<tr><td>A</td><td>Where exactly are you stuck?</td></tr>
<tr><td>Q</td><td>I showed the base case when y=0.
That is, I showed the result (=x) satisfies
<code>x≥0 & x|0 & x|x & □z:int(z|x & z|0 -> z|x).</code>

I used the definition of "|", that <code>z|x if x=m*z for some int m.</code>
Most of the properties are easy: <code>x|0 because 0*x=0.</code>

But I am not sure what the Ind. Hyp. should be.</td></tr>
<tr><td>A</td><td>You want to show that for any non-negative x and y the post-condition holds. Since you appear to be using induction on y ....</td></tr>
<tr><td>Q</td><td>I see – I let

<code>P(y) be □x:nat(r≥0 & r|x &.r|y & □z:int(z|x & z|y -> z|r),where r=gcd(x,y).</code>
<code>I can assume P(y') for all 0<=y'<y and try to show P(y) …</code></td></tr>
<tr><td>A</td><td>You don't seem to need me after all!</td></tr>
<tr><td>Q</td><td><code>Let X>=0 be an arbitrary int.</code>

How do I know what r is?</td></tr>
<tr><td>A</td><td>Use the program.</td></tr>
<tr><td>Q</td><td>Oh yes, of course.

<code>Since y>0, r=gcd(x,y)=gcd(y,x%y).</code>
<code>As x%y<y I can use the Hyp.</code></td></tr>
<tr><td>A</td><td>Why is x%y <y? Also, you need that x%y>=0 to use the hypothesis.</td></tr>
<tr><td>Q</td><td>OK! <code>A property of "%" is that 0<=x%y<y.</code>

<code>So then I can deduce from the hypothesis that</code>
<code>r≥0 & r|y & r|x%y & □z:int(z|y & z|x%y -> z|r)</code>

<code>And I have to show (i) r|x, and (ii) r|y and (iii) □z:int(z|x & z|y -> z|r).</code>
<code>(ii) is true from the hypothesis.</code>

I think I am stuck for sure now as the hypothesis doesn't seem to apply.</td></tr>
<tr><td>A</td><td>You give up too easily.
Call x%y = g and write down a property involving x, y and g.</td></tr>
<tr><td>Q</td><td>Mmmm. <code>g+k*y=x?</code></td></tr>
<tr><td>A</td><td>Correct.</td></tr>
<tr><td>Q</td><td>Ah! I see. Then this property holds also:

<code>for any z:int if z|g and z|y then z|x, and if z|x and z|y then z|g (**).</code>

<code>When I take r for z, I can deduce (i) from the hypothesis.</code>
<code>To show (iii), suppose that z|x and z|y. Then z|x%y follows by (**).</code>
<code>Therefore z|y and z|x%y so z|r, which is what I want.</code>

I think it’s done!</td></tr>
<tr><td>A</td><td>Excellent. (KB Feb 2002)</td></tr>
</table>