August 27, 2015

Math 3012 – Applied Combinatorics Lecture 4

William T. Trotter
trotter@math.gatech.edu

The Principle of Math Induction

Postulate If S is a set of positive integers, 1 is in S, and $k + 1$ is in S whenever k is in S, then S is the set of all positive integers.

Consequence To prove that a statement S_n is true for all n, it suffices to do the following two tasks. First show that S_n holds when $n = 1$. Second, assume that S_n is true when $n = k$ and show that it then holds when $n = k + 1$.

CS Students Use Induction Intuitively

```
int  my_function (int  a) {
  if (a   == 1) {
    return  42;              /* The Secret  */
  else return 3*my_function (a -1) - 80;
}
```

What is the value of:

my_function (3)

Answer 58

A More Challenging Example

```
int  update_value (int  a) {
   if (a  % 2  == 0) {                    /*  a % 2 = a mod 2 */
      return  a/2;
   else return 3*a + 1;
 }

int collatz_sequence (int a) {
   printf("%d \n", a);
   do while (a != 1) {a = update (a);}
   printf("Success!\n");
 }
```

Applying Math Induction (1)

Theorem The sum of the first n odd integers is n^2, i.e.,
$1 + 3 + 5 + 7 + \ldots + (2n - 1) = n^2$.

Proof $2 * 1 - 1 = 1^2 = 1$, so true when $n = 1$.
Assume true when $n = k$, i.e., assume
$1 + 3 + 5 + 7 + \ldots + (2k - 1) = k^2$.

Then

$$
\begin{aligned}
1 + 3 + 5 + 7 + \ldots + (2k - 1) + (2k + 1) &= k^2 + (2k + 1) \\
&= k^2 + 2k + 1 \\
&= (k + 1)^2
\end{aligned}
$$

QED

Avoiding Ambiguity (1)

Theorem The sum of the first n odd integers is n^2, i.e., $1 + 3 + 5 + 7 + \ldots + (2n - 1) = n^2$.

But … can we really be certain about what is meant with the expression of the left hand side? Let's take out the ambiguity. In the English language, we might say "the sum of the first n odd integers is n^2."

Here's an even more precise way. First, for a sequence $\{a_n:\ n \geq 1\}$, we define:

$$\sum_{i=1}^{1} a_i = a_1 \quad \text{and} \quad \sum_{i=1}^{k+1} a_i = a_{k+1} + \sum_{i=1}^{k} a_i$$

Avoiding Ambiguity (2)

Theorem $\sum_{i=1}^{n} 2i - 1 = n^2$

Proof $\sum_{i=1}^{1} 2i - 1 = 2(1) - 1 = 1 = 1^2$

Now assume $\sum_{i=1}^{k} 2i - 1 = k^2$

Then $\sum_{i=1}^{k+1} 2i - 1 = k^2 + [2(k+1) - 1]$
$= k^2 + 2k + 1$
$= (k+1)^2$

QED

Theory vs. Practice

Remark In practice most mathematicians, computer scientists and engineers prefer the informal notation as they feel it is more intuitive. However, whenever truly pressed, they could if absolutely forced, go the more formal and absolutely unambiguous route.

Also A combinatorial proof is usually preferable to a formal inductive proof … as this helps us to understand what is really going on behind the scenes.

Remember Usually means usually and not always.

Applying Math Induction (2)

Exercise Show that the following formula is valid:
$1^2 + 2^2 + \dots + n^2 = n(n+1)(2n+1)/6.$

Proof $1^2 = 1 = 1(1+1)(2*1+1)/6$, so true when $n = 1$.
Assume true when $n = k$, i.e., assume
$1^2 + 2^2 + \dots + k^2 = k(k+1)(2k+1)/6.$

Then

$$\begin{aligned}
1^2 + 2^2 + \dots + k^2 + (k+1)^2 &= k(k+1)(2k+1)/6 + (k+1)^2 \\
&= [(2k^3 + 3k^2 + k) + (6k^2 + 12k + 6)]/6 \\
&= (2k^3 + 9k^2 + 13k + 6)/6 \\
&= (k+1)(k+2)(2k+3)/6
\end{aligned}$$

QED

Applying Math Induction (3)

Theorem For all $n \geq 1$, $n^3 + (n + 1)^3 + (n + 2)^3$ is divisible by 9.

Proof When $n = 1$, $1^3 + 2^3 + 3^3 = 1 + 8 + 25 = 36$.

Assume true when $n = k$. Then, if $n = k+1$,

$$
\begin{aligned}
&(k+1)^3 + (k+2)^3 + (k+3)^3 \\
&\quad = (k+3)^3 + (k+1)^3 + (k+2)^3 \\
&\quad = (k^3 + 9k^2 + 27k + 27) + (k+1)^3 + (k+2)^3 \\
&\quad = [(k^3 + (k+1)^3 + (k+2)^3] + [9k^2 + 27k + 27]
\end{aligned}
$$

QED

An Exercise in Math Induction (1)

Exercise Show that for all $n \geq 2$,

$$1/\sqrt{1} + 1/\sqrt{2} + 1/\sqrt{3} + \ldots + 1/\sqrt{n} > \sqrt{n}$$

Solution (Which turned out to be more substantive than our other examples presented thus far.)

The base case is $n = 2$. Here the left hand is $1 + 1/\sqrt{2}$ while the right hand side is $\sqrt{2}$, so we want to show that $1 + 1/\sqrt{2} > \sqrt{2}$.

An Exercise in Math Induction (2)

Exercise (continued) Squaring both sides, this is equivalent to showing that

$$1 + 2/\sqrt{2} + 1/2 > 2$$ and this is equivalent to $$\sqrt{2} > 1/2$$ which is true since $\sqrt{2} > 1$.

So we have established that the inequality is valid when $n = 2$. Now assume that it is valid for some integer k, i.e.,

$$1/\sqrt{1} + 1/\sqrt{2} + 1/\sqrt{3} + \ldots + 1/\sqrt{k} > \sqrt{k}$$

An Exercise in Math Induction (3)

Exercise (continued) It follows that

$1/\sqrt{1} + 1/\sqrt{2} + 1/\sqrt{3} + \ldots + 1/\sqrt{k} + 1/\sqrt{(k+1)} > \sqrt{k} + 1/\sqrt{(k+1)}$.

Now what we want to prove is that

$1/\sqrt{1} + 1/\sqrt{2} + 1/\sqrt{3} + \ldots + 1/\sqrt{k} + 1/\sqrt{(k+1)} > \sqrt{(k+1)}$,

so it suffices to prove that

$\sqrt{k} + 1/\sqrt{(k+1)} > \sqrt{(k+1)}$

An Exercise in Math Induction (4)

Exercise (continued) Squaring both sides, the last inequality is equivalent to

$k + 2\sqrt{k}/\sqrt{(k+1)} + 1/(k+1) > k + 1$, which is equivalent to

$2\sqrt{k}/\sqrt{(k+1)} + 1/(k+1) > 1$. But this inequality holds if

$2\sqrt{k}/\sqrt{(k+1)} > 1$, which is not equivalent to
$4k > k+1$, which is true.

QED (Whew!)

Basis for Long Division

Theorem If m and n are positive integers, there are unique integers q and r with $q \geq 0$ and $0 \leq r < m$ so that

$$n = q\,m + r$$

Question Is this obvious or does it require an explanation/proof?

Yes!! It does require an argument.

Long Division Revisited

Strategy Make the following statement S_n: For all positive integers m, there exist q and r with $q \geq 0$ and $0 \leq r < m$ so that $n = q\,m + r$.

Proof When $n = 1$, if $m = 1$, then $1 = 1*1 + 0$, and if $m > 1$, then $1 = 0*m + 1$. So S_1 is true.
Now assume S_k is true, and let m be a positive integer. Choose q and r so that $k = q\,m + r$. Then $k + 1 = q\,m + (r + 1)$ works unless $r + 1 = m$. In this case, $k + 1 = (q + 1)\,m + 0$.

The uniqueness part is just high school algebra.

Finding Greatest Common Divisors

Problem If n and m are positive integers with $n \geq m$, find their greatest common divisor.

Solution ??? The following loop always works.

```
int  gcd (int  n, int m) {
   int  gotit = 0;
   answer = m;
   while (gotit == 0) do {
      if (n % answer == 0) return answer;
        gotit = 1;
      else answer = answer -1;
   }
}
```

The Limits of Computing Power

Remark There is no computer on the planet that will solve the following problem using the algorithm on the preceding slide:

gcd (275887499882303013399012285973582,
3747754982288837599088247)

Comment Maple reported that they are relatively prime in less than one second.

The Euclidean Algorithm

Setup Suppose n and m are positive integers with $n \geq m$. Choose q and r with $q \geq 0$ and $0 \leq r < m$ so that $n = q\,m + r$.

Fact If $r = 0$, then $\gcd(n, m) = m$.

Fact If $r > 0$, then $\gcd(n, m) = \gcd(m, r)$.

Explanation $n/d = (qm + r)/d = q\,(m/d) + r/d$.

An Improved Algorithm

```
int  gcd (int  n, int m) {
   int gotit = 0;
   while (gotit == 0) do {
      r = n % m;                    /*  r = n  mod  m   */
      if (r == 0) return  m;
        gotit = 1;
      else  n = m;
          m = r;
    }
 }
```

Concrete Example

Problem Find gcd(10262736, 85470).

$$
\begin{aligned}
10262736 \;\%\; 85470 &= 6336 \\
85470 \;\%\; 6336 &= 3102 \\
6336 \;\%\; 3102 &= 132 \\
3102 \;\%\; 132 &= 66 \\
132 \;\%\; 66 &= 0
\end{aligned}
$$

Answer **66** = gcd(10262736, 85470)

Quotients and Remainders

Problem Find gcd (n, m) when n = 10262736 and m = 85470.

10262736 = 120 * 85470 + 6336
85470 = 13 * 6336 + 3102
6336 = 2 * 3102 + 132
3102 = 23 * 132 + 66
132 = 2 * 66 + 0

6336 = 10262736 - 120 * 85470
3102 = 85470 - 13 * 6336
132 = 6336 - 2 * 3102
66= 3102 - 23 * 132

Problem Use back-tracking to find integers a and b so that a n + b m = gcd (n, m).

An Important Diophantine Equation

Fact When n and m are positive integers, there are integers a and b so that

$$\gcd(n, m) = a\,n + b\,m$$

Fact We can find a and b by back-tracking with the information gained in carrying out the Euclidean algorithm

Back Tracking Details

Problem Find a and b so that gcd (n, m) = an + b m
when n = 10262736 and m = 85470

$66 = 3102 - 23 * 132$ and $132 = 6336 - 2 * 3102$

$= -23 * 6336 + 47 * 3102$ and $3102 = 85470 - 13 * 6336$

$= 47 * 85470 - 634 * 6336$ and $6336 = 10262736 - 120 * 85470$

$= -634 * 10262736 + 76127 * 85470$

Solution a = -634 and b = 76127

Preferring Loops

Recommendation

Check out the program gcd_lcm.c on the course web site and see how to compute gcd's and solve the Diophantine equation $a\,n + b\,m = gcd(n, m)$ using a loop with no back tracking and very little memory.