ECS 20 – Fall 2021 – P. Rogaway Numbers and Induction

https://www.cs.wm.edu/~tadavis/cs243/ch05s.pdf

Number Theory

1. constant symbol: 0
2. predicate symbol: <
3. function symbol: S (1-ary) (successor function)
   $+$ (2-ary)
   $\cdot$ (2-ary)
   E (2-ary) omit because it's not part of PA?

Always add equality (=), which is reflexive, symmetric, transitive.

Already rich enough to make powerful statements in number theory.
Eg: **Fermat's Last Theorem**: no three positive integers a, b, and c satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2:

$$(\forall a)\ (\forall b)\ (\forall c)(\forall n)(a\ E\ n + b\ E\ n = c\ E\ n \rightarrow n > S(S(0)))$$

(Show how to define > using <, =, and negation). Or, similarly, write **Goldbach's Conjecture** in this language of number theory: that every even number more than 2 is the sum of two primes.

PA axioms from where? Now finding http://www.cs.toronto.edu/~sacook/csc438h/notes/page96.pdf, which doesn't include 7, 8…

Axioms of arithmetic ("Peano arithmetic")(Giuseppe Peano, 1889)

1. $(\forall x)\ (S(x) \neq 0)$
2. $(\forall x)(\forall y)(S(x) = S(y) \ \rightarrow\ x = y)$
3. $(\forall x)\ (x + 0 = x)$
4. $(\forall x)(\forall y)(x + S(y) = S(x+y))$
5. $(\forall x)\ (x \cdot 0 = 0)$
6. $(\forall x)(\forall y)(x \cdot S(y) = x \cdot y + x)$
7. $(\forall x)(\forall y)\ )(\forall c)\ (x < y \rightarrow\ x + c \leq y + c)$
8. $(\forall x)(\forall y)\ )(\forall c)\ (x < y \rightarrow\ x \cdot c \leq\ y \cdot c)$

9. For all predicates P

   $$(P(0)\ \wedge\ (\forall n)(P(n) \rightarrow P(n{+}1)) \ \rightarrow\ \wedge\ (\forall n)(P(n))$$

Not a 1st order property

Alternatively: If a **set** contains zero and the successor of every **number** is in the set, then the set contains the natural numbers. This form does not seem as directly useful.

Principle of mathematical induction *Different statement*

To prove a proposition $P(n)$ for all integers $n \geq n_0$:

1) Prove $P(n_0)$ **(Basis)**

2) Prove that $P(n) \rightarrow P(n+1)$ for all $n > n_0$ **(Inductive step)**

(Inductive assumption)

The above sounds slightly more general (because I let you start at n_0), but easily seen to be equivalent.

Also equivalent: "**strong**" form of induction:

To prove a proposition $P(n)$ for all integers $n \geq n_0$:

1) Prove $P(n_0)$ (Basis)

2) Prove that $(P(1) \wedge \ldots \wedge P(n)) \rightarrow P(n+1)$ for all $n > n_0$ **(inductive step)**

Again equivalent. Sometimes easier to apply. The stronger inductive assumption may make it easier to get the conclusion.

EXAMPLE 0: Prove that the sum of the first n integers $n(n+1)/2$. Do this in two ways, either: (a) pictorially; (b) by induction. But where does the formula come from? Options: (i) write a table; (ii) use a definite integral to help make a guess; (iii) solve a system of equations using values from table.

EXAMPLE 1: Prove that the sum of the **odd** integers 2 .. $2n$-1 is n^2

$1 + 3 + \ldots + (2n-1) = n^2$.

Basis: n=1, check

Inductive step:

$1 + 3 + \ldots (2n - 3) \quad = (n-1)^2$

$\qquad + 2n - 1 \quad = \qquad + 2n - 1$

$\qquad = n^2 - 2n + 1 \ + 2n - \ 1 = 1$

$\qquad = n^2$

EXAMPLE 2: Use induction to prove that n^2+n is always even (divisible by 2).

Basis: n=0: fine.
Inductive step: Assume that the statement is true for $n=k$. Thus, k^2+k is even. That is, $k^2+k = 2j$ for some integer j. Now what about $(k+1)^2+(k+1)$ – is it necessarily even?? Expanding out, this expression is

$$k^2 + 2k + 1 \quad + \quad k + 1 = k^2 + 3k + 2 \quad = k^2 + k \quad + \quad 2k + 2$$
$$= \ 2j + 2k + 2 = 2(j+k+1)$$

so it is even

Now, write k2+k{k^2} + kk2+k as part of an equation which denotes that it is divisible by 222.

EXAMPLE 3. Sam's Dept. Store sells envelopes in packages of 5 and 12. Prove that, for any $n \geq 44$, the store can sell you exactly n envelopes. [GP, p.147]

Basis: $44 = 2(12) + 4(5)$
$45 = \quad 9(5)$
$46 = 3(12) + 2(5)$
?...?

SUPPOSE: It is possible to buy n envelopes for some **$n \geq 44$.**
SHOW: It is possible to buy n+1 envelopes

```
    x    x xx x x  x x xx x  x x  xx   x x xxxxxxxxxxxxxxxxx
123456789012345678901234567890123456789012345678901234567890
0        1         2         3         4         5         6
```

- If purchasing **at least** 7 packets of 5: **trade in seven packets of five** for **three packets of 12**:

7(5) → 3(12)
35 36

- If purchasing **fewer** than 7 packets of 5: i.e., purchasing **at most** 6 packets of 5, so **at most 30** of the envelopes are in packets of 5; so what remains are ≥ **44 - 30 = 14 envelopes** being bought in packets of 12, so ≥ 2 packets of twelve. So take **2 of the packets of 12** (i.e., 24 envelopes) and **trade them for 5 packets of 5:**
  2(12) → 5(5)
  24 25

EXAMPLE 4: Show that you can tile **any** "punctured" $2^n \times 2^n$ grid by *triominoes* https://undergroundmathematics.org/divisibility-and-induction/triominoes/solution

#
(may be rotated)

Illustrate and prove, dividing board in into four $2^n \times 2^n$ to prove. Puncture the $2^{n+1} \times 2^{n+1}$ grid; tile that one of the four subgrids (by inductive assumption); puncturing three the three near-center center points (for the three $2^n \times 2^n$ pieces that lacking the puncture); recurse on those three pieces; add one more tromino.

EXAMPLE 5: Fundamental theorem of arithmetic. – Almost verbatim from https://www.cs.wm.edu/~tadavis/cs243/ch05s.pdf An example of "strong" induction".

Claim: if n is an integer greater than 1, then n can be written as the [unique] product of primes. Solution: Let $P(n)$ be the proposition that n can be written as a product of primes. // Leave uniqueness for later, or omit it.

Basis: $P(2)$ is true since 2 itself is prime.

Inductive step: The inductive hypothesis is $P(j)$ is true for all integers j with $2 \leq j \leq k$. To show that $P(k + 1)$ must be true under this assumption. Two cases need to be considered:

• If $k + 1$ is prime, then $P(k + 1)$ is true.

• Otherwise, $k + 1$ is composite and can be written as the product of two positive integers a and b with $2 \le a \le b < k + 1$. By the inductive hypothesis a and b can be written as the product of primes and therefore $k + 1$ can also be written as the product of those primes. Hence, it has been shown that every integer greater than 1 can be written as the product of primes.

Uniqueness:
Let N be the *smallest* number that can be written in *two different ways* as the product of primes. Those two ways can have no prime in common or else we'd divide by it and have a smaller number that could be written in two different ways as the product of primes. Thus

$$N = p_1\, p_2 \dots p_m = q_1\, q_2 \dots q_n$$
$$= p_1\, P = q_1\, Q$$

Where $p_1 < q_1$ and the primes on the left, listed in increasing order, are disjoint from those on the right, also listed in increasing order. Now

$$(q_1 - p_1)\, Q < N$$

I claim that $(q_1 - p_1)\, Q$ is a multiple of p_1, namely

$$p_1\, (P - Q) = (q_1 - p_1)\, Q$$

because

$$p_1\, P - p_1 Q = N - p_1\, Q$$

and

$$(q_1 - p_1)\, Q = q_1\, Q - p_1\, Q = N - p_1\, Q.$$

By the unique factorization of number less than N we know that p_1 must occur in the factorization of $(q_1 - p_1)$ or in the factorization of Q.

- The first is impossible because if p_1 divides $q_1 - p_1$ then it divides q_1, but p_1 and q_1 are distinct primes.
- The second is impossible because the factors of Q were bigger than (as well as distinct from) p_1

Done.

The fundamental theorem of arithmetic is useful. We routinely like to think of numbers in terms of their prime factorization. Many questions become easier if presented a number in this form. Example:

How many factors does 360 have?
First, write 360 in its prime factorized form:
$360 = 2^3 \cdot 3^2 \cdot 5$
A factor must be of the form 2a 3b 5c where $a\in[0..3]$, $b\in[0..2]$, $c\in[0..1]$.
So the number of factors 360 has is $4 \cdot 3 \cdot 2 = 24$.

If I asked you how many factors $2450250000 = 2^4\, 3^4\, 5^6\, 11^2$ has, you would answer …. $5 \cdot 5 \cdot 7 \cdot 3 = 525$

Is 1873215592 a square? No, because you can divide it by 2 three times, but no no more, so the factorization is $2^3 \cdot M$ where the prime factorization of M has no 2s in it; and a number is going to be a square iff all the powers of primes in the prime factorization are *even*.

EXAMPLE 6: Cake cutting

See http://www.cs.berkeley.edu/~daw/teaching/cs70-s08/notes/n8.pdf for a nice writeup

1. If $n = 2$, use the cut-and-choose protocol. Otherwise:
2. The first $n-1$ participants divide the cake by recursively invoking this procedure.
3. For i = 1,2,...,$n-1$, do:
   a) Participant *i* divides her share into *n* pieces she considers of equal worth (by her measure).
   b) Participant n collects whichever of those n pieces he considers to be worth most (by his measure).

Number of cuts:

$T(n) = T(n-1) + (n-1)^2$

1	2	3	4	5	6
0	1	5	14	30	55

$T(n) = T(n-1) + (n-1)^2$
$= T(n-2) + (n-1)^2 + (n-2)^2$
$= T(n-3) + (n-1)^2 + (n-2)^2 + (n-3)^2$
$= T(n-3) + (n-1)^2 + (n-2)^2 + (n-3)^2$
$= 1 + 2^2 + 3^2 + 4^2 + \ldots + (n-1)^2$
approx. Integeral_1^n x2 approx $n^3/3$

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Prove by induction.

Axioms of arithmetic (“Peano arithmetic”)(Giuseppe Peano, 1889)

1. $(\forall x)\ (S(x) \neq 0)$
2. $(\forall x)(\forall y)(S(x) = S(y) \ \rightarrow\ x = y)$
3. $(\forall x)\ (x + 0 = x)$
4. $(\forall x)(\forall y)(x + S(y) = S(x+y))$
5. $(\forall x)\ (x \cdot 0 = 0)$
6. $(\forall x)(\forall y)(x \cdot S(y) = x \cdot y + x)$
7. $(\forall x)(\forall y)\ )(\forall c)\ (\mathrm{x} < \mathrm{y} \rightarrow\ x + c \leq y + c)$
8. $(\forall x)(\forall y)\ )(\forall c)\ (\mathrm{x} < \mathrm{y} \rightarrow\ x \cdot c \leq\ y \cdot c)$

9. For all predicates P

   $$(P(0) \quad \wedge \quad (\forall n)(P(n) \rightarrow P(n+1)) \qquad \rightarrow \qquad \wedge \quad (\forall n)(P(n))$$

Not a 1st order property