Math 55 - Spring 2004 - Lecture notes # 11 - Feb 26 (Thursday)

Keep Reading Sections 3.1 - 3.4

Goals for today: Revisit modular arithmetic
Begin Sequence, Summations, Induction

We will explain modular arithmetic one more way, to try
to make it clearer why we can do certain manipulations
like the one in the following manipulation, that was part of
the proof of RSA:

We had an integer expression de = 1+m(p-1)(q-1) where p, q are primes,
and another integer M. We wrote

```
  M^(de) = M^(1+m(p-1)(q-1))
```

and so

```
  M^(de) == M^(1+m(p-1)(q-1))  (mod p)
         == M*M^(m(p-1)(q-1))  (mod p)
         == M*(M^(p-1))^(m(q-1))  (mod p)
         == M*(M^(p-1) mod p)^(m(q-1))  (mod p)
                  ... this is the line we want to better explain
         == M*(1)^(m(q-1))   (mod p)
                  ... this is a result of Fermat's Little Theorem
         == M   (mod p)
```

Here is another approach to writing the above manipulations.
We think of modular arithmetic as arithmetic on sets of numbers,
instead of numbers.

We illustrate just for p=5 to make is clearer.
Define the set

```
    { ... -10, -5, 0, 5, 10, ... }
  = {5*m, for all integers m}
  = {all integers n such that n == 0 (mod 5) }
```

We need a shorter name for this set, so we will use "0", which
may be read "the set containing 0".
Similary, define

```
    { ... -9, -4, 1, 6, 11, ... }
  = {1+5*m, for all integers m}
  = {all integers n such that n == 1 (mod 5) }
```

and name this set "1", or "the set containing 1".
The sets "2", "3", and "4" are similarly defined.

Note that the union of these sets
     "0" union "1" union "2" union "3" union "4"
is the set of all integers, and all pairs of sets (line "0" and "3")
are disjoint.

(The formal name for these sets is "equivalence classes", which are
discussed in section 7.5, but we don't need the general case here.)

We need to define arithmetic on these sets, i.e. what it means to
add, subtract and multiply them in a ways that obeys the usual
rules of arithmetic (commutativity, associativity, etc.)

A natural way to define the sum of two sets, say "3" and "4",
is as the set containing all sums a+b where a is in "3" and b is in "4".
```
  "3" + "4" = {a+b such that a IN "3" and b IN "4" }
            = {(3+5*m) + (4+5*n) such that m and n are integers}
            = {7+5*(m+n) such that m and n are integers}
            = {2+5*(1+m+n) such that m and n are integers}
            = {2+5*(k) such that k is any integers}
                  ... because 1+m+n can be any integer
            = "2"
```
So we see that "3" + "4" = "2", which is another way to say
    3+4 == 2 (mod 5)
Subtraction works like addition. Let's try multiplication, which is
slightly different. I will define "x" to mean multiplying two sets
the way I did above:
```
  "3" x "4" = {a*b such that a IN "3" and b IN "4" }
            = {(3+5*m) * (4+5*n) such that m and n are integers}
            = {12+5*(4*m+3*n+5*m*n) such that m and n are integers}
            = {2+5*(2+4*m+3*n+%*m*n) such that m and n are integers}
            SUBSET "2"
```
Note that "3" x "4" does not equal "2" because "2" contains 2, but
"3" x "4" does not (why?). Still since "3" "*" "4" SUBSET "2",
this means we can define multiplication (represented by the different
symbol "*") as "3" * "4" = "2", and more generally
    "i" * "j" = "i*j (mod 5)"
so again we have another way to express modular arithmetic.

Since addition and multiplication with integers is commutative,
associative, distributive etc. one can confirm that the same is
true with the arithmetic with sets that we just defined.

```
Since the sets we defined are disjoint, we can identify them
uniquely choosing any member. For example, "1" = "6" = "10" = "-4"
are all same for the same set. This means that the equations
 "2" + "4" = "6"
 "2" + "4" = "1"
 "-3" + "9" = "16"
are all in fact express the identical equality, because
 "2" = "-3", "4" = "9" and "6" = "1" = "16".

Now return to Fermat's Little Theorem and its use to prove RSA.
Let p be a prime, and think of all numbers mod p, so that
"k" = {k + m*p, m any integer}.
Suppose p \| M. Then Fermat's Little Theorem says
M^(p-1) == 1 (mod p), or equivalently "M"^(p-1) = "1"
Returning to our proof of RSA, we rewrite it as
  "M"^(de) = "M"^(1+m(p-1)(q-1))
           = "M"*"M"^(m(p-1)(q-1))
           = "M"*("M"^(p-1))^(m(q-1))
           = "M"*("1")^(m(q-1))    ... by Fermat's Little Theorem
           = "M"

DEF: A sequence is a function from a subset K of the integers to a set S.
     It usually written a_n, instead of a(n).
EG:  K = N, a_n = 1/n,  often write 1, 1/2, 1/3, 1/4, 1/5, ...
DEF: A summation is the sum of a sequence:
     SUM_{i=1}^n a_i = a_1 + a_2 + ... + a_n
     SUM_{i=m}^n a_i = a_m + a_{m+1} + ... + a_n
     SUM_{i IN {2,4,7}} a_i = a_2 + a_4 + a_7
There are certain summations that appear frequently when you are
analyzing problems. You should learn them well enough to recognize
them:

EG: "Arithmetic progression" is a_i = i,
    we want S = SUM_{i=1}^n i
    write S =  1  +  2  +  3  + ... + n-1 +  n
    and   S =  n  + n-1 + n-2 + ... +  2  +  1  and add them to get
         2S = n+1 + n+1 + n+1 + ... + n+1 + n+1 = n*(n+1)
    so    S = n*(n+1)/2
    (alternate "proof by picture" as a sum of areas of triangles)
EG: SUM_{i=k+1}^n 3i-1 = SUM_{i=1}^n 3i-1 - SUM_{i=1}^{k} 3i-1
                       = 3*SUM_{i=1}^n i - SUM_{i=1}^n 1
```

```
                          -( 3*SUM_{i=1}^k i - SUM_{i=1}^k 1 )
                         = 3(n*(n+1)/2) - n - (3*(k*(k+1))/2 - k)
                         = (3/2)*(n*(n-1) - k*(k-1))

   EG: "Geometric progression" is  a_i = r^i, some fixed r (note a_0 = 1)
       we want S = SUM_{i=0}^n r^i
       Two cases: If r = 1 -> S = n+1
                  If r != 1, then
       write   S = 1 + r + r^2 + r^3 + ... + r^n
       and    rS =     r + r^2 + r^3 + ... + r^n + r^(n+1) and subtract to get
          (1-r)S = 1                              - r^(n+1)
       or      S = (1-r^(n+1))/(1-r)
ASK&WAIT: Suppose -1<r<1. What happens to r^(n+1) as n gets bigger?
          What happens to S?

   Sometimes we just want an approximate value for the sum (motivation later
       in lecture)
   EG: S = SUM_{i=1}^n i^2
       Interpret S as area of region made of n rectangles, of sizes 1-by-i^2
       Bound S above by area A1 of bigger region, under curve y = (x+1)^2
       Bound S below by area A2 of smaller region, under curve y = x^2
       A1 = INTEGRAL_0^n (x+1)^2 dx = (n+1)^3/3
       A2 = INTEGRAL_0^n x^2 dx     = n^3/3
       So n^3/3 <= S <= (n+1)^3/3

   Sometimes we can use differentiation of a known summation to get
   a new one. For example consider
      S(n,r) = SUM_{i=0}^n r^i = 1 + r + r^2 + ... + r^n
   Differentiating both sides with respect to r yields
    d/dr S(n,r) = SUM_{i=1}^n i*r^(i-1) = 1 + 2*r + 3*r^2 + ... * n*r^(n-1)
   Plugging in our expression for S(n,r) and simplifying yields
    1 + 2*r + 3*r^2 + ... * n*r^(n-1) = [ r^n*(n*r -n -1) + 1 ]/(1-r)^2
   if r neq 1. If |r|<1 we get can let n approach infinity and write
    SUM_{i=1}^{infinity} i*r^(i-1) = 1/(1-r)^2

     Proof by induction: a technique for proving theorems like
          "FORALL positive integers n, P(n)"
       (and more general problems later)

   EX: FORALL positive integers n,
       the sum of the first n integers is n*(n+1)/2
             i.e. "sum_{i=1}^n i = 1+2+3+...+n = n*(n+1)/2" is P(n)
```

```
EX: FORALL positive integers n,
    the sum of the first n odd integers is n^2,
          i.e. "sum_{i=1}^n (2*i-1) = 1+3+5+...+(2*n-1) = n^2" is P(n)

    Basic idea: Prove P(1) is true directly
    EX: P(1) means "1=1^2", which is true
    Then show that all of the implications
        P(1)->P(2),P(2)->P(3),..., P(n)->P(n+1),... are true for all n
    Then starting from P(1) which we know to be true, P(m) is true for
       all larger integers m, because P(1)->P(2)-> ... -> P(m)
    I.e. need to prove an infinite number of tiny theorems; but
       can do them all at once by showing that P(n)->P(n+1) is
       true no matter what the integer n is:
    EX: P(n) means that "sum_{i=1}^n (2*i-1) = n^2"
        Assume that P(n) is true, and show that P(n+1) is true, i.e.
            that sum_{i=1}^{n+1} (2*i-1) = (n+1)^2.
            To do this we take P(n), which we know to be true:
                 sum_{i=1}^n (2*i-1) = n^2
            and add 2*(n+1)-1 to both sides to get
                 sum_{i=1}^{n+1} (2*i-1) = n^2 + 2*(n+1)-1
                                         = n^2 + 2*n + 1 = (n+1)^2
            so P(n+1) is true as desired.

  EX: Prove 2^n < n! if n>= 4; P(n) = "2^n < n!"
      Base case: P(4) means we have to confirm that  2^4=16<24=4!
      Induction step: Assume P(n) is true, i.e. 2^n < n!. This implies
      that 2*2^n < 2*n!, or 2^(n+1) < 2*n! < (n+1)*n! < (n+1)! as desired.
      Note that we don't have to start induction at n=1.

  EX: Prove G = sum_{i=0}^n r^i = (1-r^(n+1))/(1-r), if r != 1.
      We proved this in chapter 1 using a different idea (computing r*G-G)
      but here we use induction
      P(n) = "sum_{i=0}^n r^i = (1-r^(n+1))/(1-r)"
      Base case: P(0): sum_{i=0}^0 r^i = 1 = (1-r)/(1-r)
      Induction step: Assume P(n) is true, and confirm P(n+1):

         sum_{i=0}^{n+1} r^i = sum_{i=0}^{n} r^i + r^(n+1)
                             = (1-r^(n+1))/(1-r) + r^(n+1)  by P(n)
                             = ( 1-r^(n+1) + (1-r)*r^(n+1) )/(1-r)
                             = ( 1-r^(n+1) + r^(n+1) - r^(n+2) )/(1-r)
                             = ( 1 - r^(n+2) )/(1-r)
      which proves P(n+1)
```

Another way to use induction idea: show that if the result is true
for all "smaller" problems 1,2,3,...,n, then it is true for
the next bigger one (n+1), or
P(1) and P(2) and ... and P(n) -> P(n+1)

EX: Every positive integer >= 2 can be written as the product of primes
P(k) = "k can be written as product of primes"
Base case: P(2) is true
Induction step: Now suppose P(2),...,P(n) are true. Consider n+1:
Case 1: n+1 prime: done
Case 2: n+1 composite, say n+1 = a*b where a>1, b>1.
Then a = (n+1)/b < n+1 and b = (n+1)/a < n+1. So
P(a) and P(b) are true by induction, and thus n+1 can be
written as the product of sets of prime factors of a and of b.

EX: Show every amount of postage of 12 cents or more can be
formed used only 4 and 5 cent stamps
Proof:
P(m) = "can form postage of m cents out of 4 and 5 cent stamps"
Base case:
P(12) true, since 12=3*4+0*5
P(13) true, since 13=2*4+1*5
P(14) true, since 14=1*4+2*5
P(15) true, since 15=0*4+3*5
Induction step: Suppose P(12),...,P(n), true, where n>=15.
Since n>=15, n-3>=12 so P(n-3) is true. Then to show P(n+1),
use postage for P(n-3) plus a 4 cent stamp.