```
Math 55 - Spring 2004 - Lecture notes # 10 - Feb 25 (Tuesday)

   Keep Reading Sections 3.1 - 3.4

  Homework, due Mar 3
        2.6-16
        3.1-16, 30, 36, 44
        3.2-6, 10, 12, 16, 20, 22

   Goals for today: Finish cryptography from last time
                    Begin Sequence, Summations, Induction

   To finish cryptography, need proof of Fermat's Little Theorem:
   Thm: IF p is prime and p \| a, then a^(p-1) == 1 mod p

   Some "numerical experiments" to devise proof conjecture:

      consider integers 1 <= i < p, for some prime p, say p=7.
      Try multiplying them by any integer mod p, see what you get:
                   1 2 3 4 5 6
       *2 mod 7 => 2 4 6 3 5 7
       *3 mod 7 => 3 6 2 5 1 4
       *4 mod 7 => 4 1 5 2 6 3
       *5 mod 7 => 5 3 1 6 4 2
       *6 mod 7 => 6 5 4 3 2 1
ASK&WAIT:  What is the pattern?
       Can see same pattern for any prime p
    Conjecture (proven shortly): given any prime p and any 1 <= a < p,
      the numbers a*1 mod p, a*2 mod p , ... a*(p-1) mod p are
      all different, i.e. just a permutatation of 1,...,p-1

    Now take there product:
      (p-1)! = (a*1) mod p * (a*2) mod p *...*(a*(p-1)) mod p
    or
      (p-1)! == (a*1*a*2*...a*(p-1)) mod p
             == a^(p-1) (p-1)! mod p

    Suppose we could "divide by" (p-1)!;
    would get 1 == a^(p-1) mod p as desired

    Now let's do proof carefully:
    Proof of Conjecture: suppose 1 <= x,y < p , x \= y
```

```
            so -(p-1) <= x-y <= p-1, x \= y
            so p \| x-y
            so p \| a*(x-y)
            so a*x mod p \= a*y mod p
      In other words, a*1 mod p, a_2 mod p , ... , a*(p-1) mod p
      all different as conjectured.

  So now we have (p-1)! == a^(p-1)*(p-1)! mod p, and want
  to conclude 1 == a^(p-1) mod p
ASK&WAIT: What did we prove last time that lets us do this?
  Thus (p-1)!*x == 1 mod p has unique solution, multiply through to get
  (p-1)!*x == a^(p-1)*(p-1)!*x mod p
    or
         1 == a^(p-1)*1 mod p
    as desired
For homework, you will show more, that
  (p-1)! == -1 mod p (Wilson's Theorem)
```