ACCESS 2008
Thursday

HW for tomorrow:

Read Chapter 6 of "The Code Book"
and §8,9 of Davis' notes "Cryptography

- Each group should think of a short secret message (less than or equal to 88 "letters", including punctuation, from Davis' table page 9) Also, think of a "signature" less than 30 "letters" long.
- If you want to get a good idea of your week 1 group project assignment, find last year's ACCESS math week 1 assignment - ours will be almost the same, mostly just names & contact info will be changed.

Modular
Powers shortcut - we'll still use the typed notes, in part.

Example 1 in typed notes (converting letter strings into numbers).

new exercise: experiment with powers in modular arithmetic
by completing the residue table below for modulus $p=5$ (p stands for prime)

power → / residue ↓	1	2	3	4	5	6	7...
0							
1							
2							
3							
4							
mod 5							

What do you notice?

Fermat's Little Theorem

Let p be a prime and let a be any non-negative integer, $a = 0, 1, 2, \ldots$
Then
$$a^p \equiv a \mod p$$

proof: We'll use the binomial theorem (Pascal's triangle), and induction

exercise
next, finish the mod 15 power table on page 3 of the typed notes
What do you notice?

Euler - Fermat Theorem (special case)

If $N = pq$ is a product of two (different) prime numbers

let $N_2 = (p-1)(q-1)$.

Let $a = 0, 1, 2, 3, \ldots$ be any counting number.

Then

$$a^{N_2+1} \equiv a \mod N$$

$$a^{2N_2+1} \equiv a \mod N$$

$$a^{3N_2+1} \equiv a \mod N$$

$$\vdots$$

Exercise: for $p = 5$, $q = 3$, what part of the mod 15 power table does E.F.T. explain?

Proof of E.F.T. (it's also in the typed notes).

Corollary (RSA cryptography basis)

Let $N = pq$ a product of two different primes

Let $N_2 = (p-1)(q-1)$.

Let g.c.d. $(e, N_2) = 1$, i.e. e is relatively prime to N_2.

thus e has a multiplicative inverse $\underline{\bmod N_2}$.

call it d.

Then, for residues $0 \le x \le N-1$ $\underline{\bmod N}$.

the encryption function $f(x) \equiv x^e \bmod N$ (range is to the residues)

has an inverse (decryption) function $g(x) \equiv x^d \bmod N$. (range is to the residues)

Exercise What are good encryption powers mod 15?

For $e = 3$, what decryption power d will work?

proof of corollary (also in notes).

$$ed \equiv 1 \mod N_2$$

so $$ed = 1 + mN_2 \quad \text{(some positive integer } m\text{)}$$

$$f(x) \equiv x^e \mod N$$

$$\begin{aligned} g(f(x)) &\equiv g(x^e) \\ &\equiv (x^e)^d \equiv x^{ed} \\ &\equiv x^{mN_2+1} \\ &\equiv x \quad \text{by E.F.T.} \end{aligned}$$

since x and $g(f(x))$ are both in the residue range they are equal!

so d is the decryption power! ∎

We can now explain RSA...