MA111: Contemporary mathematics

Entrance Slip (due 5 min past the hour):

For each problem give the standard representation of the answer. Try not to use a calculator.

- $2^1 \pmod{11}$
- $2^2 = 2 \times 2 \pmod{11}$
- $2^4 = (2 \times 2) \times (2 \times 2) \pmod{11}$
- $2^8 = (2^4) \times (2^4) \pmod{11}$
- $2^{10} = (2^8) \times (2^2) \pmod{11}$
- $2^{34} = (2^{10}) \times (2^{10}) \times (2^{10}) \times (2^4) \pmod{11}$

Schedule:

- HW 3 is due 7am Tuesday, Oct 28th, 2014 [extended]
- Exam 2 is in-class on Thursday, Oct 23rd, 2014

Today we practice exponents and experiment with key exchange

While we are passing out the worksheet...

- Please turn in your entrance slips. We will do this every non-exam day.
  Please bring your own 3x5 index cards.
- $2^1 = 2 \equiv \boxed{2} \pmod{11}$, no tricks
- $2^2 = 2 \times 2 = 4 \equiv \boxed{4} \pmod{11}$, no tricks
- $2^4 = (2^2) \times (2^2) = 4 \times 4 = 16 \equiv 16 - 11 = \boxed{5} \pmod{11}$,
  sort of a trick, 4×4 not $2 \times 2 \times 2 \times 2$
- $2^8 = (2^4) \times (2^4) = 5 \times 5 = 25 \equiv 25 - 22 = \boxed{3} \pmod{11}$
- $2^{10} = 2^8 \times 2^2 = 3 \times 4 = 12 \equiv 12 - 11 = \boxed{1} \pmod{11}$
- $2^{34} = 2^{10} \times 2^{10} \times 2^{10} \times 2^4 = 1 \times 1 \times 1 \times 5 = \boxed{5} \pmod{11}$

VERY Small number version of worksheet

- Two volunteers needed
- $2^1 = \boxed{2} \pmod{11}$
- $2^2 = \boxed{4} \pmod{11}$
- $2^4 = \boxed{5} \pmod{11}$
- $2^8 = \boxed{3} \pmod{11}$
- Both volunteers choose secret numbers A (between 2 and 9)
- Both volunteers secretly compute $2^A \pmod{11}$
- Both volunteers publically share those final answers, c
- Both volunteers secretly compute $c^A \pmod{11}$
- What are their (secret) answers?

Old words

plaintext (plain message, "**`can you keep a secret`**")

ciphertext (hidden version, "**`DEP ZUA LIIQ E TIDSIV`**")

encryption (how to convert plaintext to ciphertext)

decryption (the reverse, cipher to plain)

cipher (both encryption and decryption methods)

key (a small secret that lets you change the cipher)

numbers (are used to represent consonants and vowels)

shift cipher (use addition and subtraction with wrap around)

Old words: modular arithmetic

- **equivalent numbers** (mod N)**:** two numbers that differ by a multiple of N
- **standard representative:** the unique number between 1 and N equivalent to it
- **zero:** any number equivalent to 0
- **zero divisor:** a nonzero number that can be multiplied by a nonzero number to get zero
- **one:** any number equivalent to 1
- **unit:** a nonzero number that can be multiplied by a nonzero number to get one
- **multiplication cipher:** take the plaintext and multiply it by the key
- **good keys** are units. **bad keys** are zeroes and zero divisors

New words: Diffie-Hellman key exchange

- You and a friend publically agree on a system (b, N):
  raise a number b to a secret power mod N
- You choose a secret number A (not too small, b^A should wrap around; not too big, no bigger than $N/2$ to be safe; if $N = 11$, then $A = 10$ has gotten too big)
- You secretly compute $b^A \pmod{N}$
  and tell the answer publically to your partner
- You take your partner's answer c
  and secretly compute $c^A \pmod{N}$
- Now both you and your partner have
  computed the same SECRET number
- You can use it as a key to another cipher

Exit quiz

- This is kind of hard. You may work in groups.

  It is like #2 on the worksheet, but the eavesdropping version.

- You hear one partner say $8 \pmod{23}$

  and the other partner says $2 \pmod{23}$.

- What number will they say together?