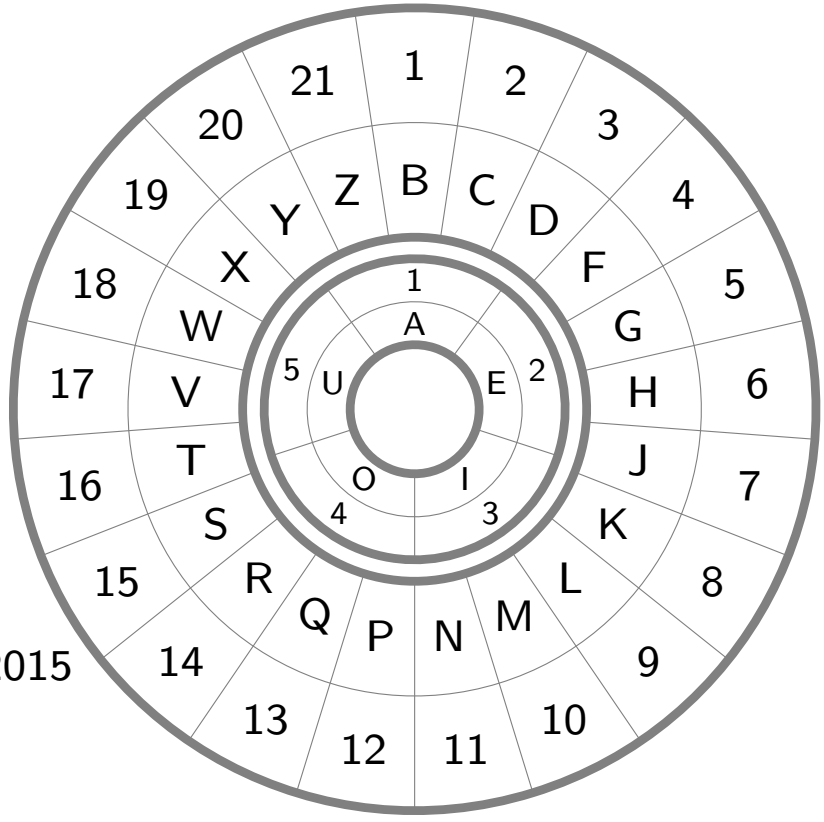
MA111: Contemporary mathematics

Mini Exam (due 20 min past the hour):



Schedule:

- HW 1 was due Tuesday, Oct 6th, 2015
- Mini-Exam 2 is in-class Today, Oct 8th, 2015
- HW 2 is due Tuesday, Oct 13th, 2015
- HW 3 is due Thursday, Oct 15th, 2015
- HW 4 is due Tuesday, Oct 20th, 2015
- Exam 2 is in-class on Thursday, Oct 22nd, 2015

Today we look at a "keyed" version of the double-it cipher

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)

double-it cipher (double and half with wrap around)

New words: modular arithmetic

- When we added and subtracted and doubled and halved

  Vowels weren't changed if we added or subtracted 5

  Consonants weren't changed if we added or subtracted 21

- Math has a short way to write this, $\mod 5$ and $\mod 21$
- "5s don't matter" and "21s don't matter"
- For instance $2 \times 11 = 22 \equiv 2 \mod 5$ and $2 \times 11 = 22 \equiv 1 \mod 21$
- I think everyone understands addition and subtraction,
- I want us to think about multiplication and division

Worksheet: really bad ciphers

- Instead of "multiply by 2" what if we used "multiply by 3"?

  What happens to the word `mom` or `dad`?

- Why is that really bad?

- What if we used "multiply by 5"?

  What happens to the word `facetiously`?

- What happens to `mom and dad` if we multiply by 15?

- Exam question: which numbers are ok to multiply by?

New words: zero divisors and units

- **zero** - not only 0, but any number that is $\equiv 0 \mod$ whatever

  5 for vowels ($5 \equiv 0 \mod 5$)

- **zero divisor** - two nonzero numbers that multiply to zero

  3 for consonants ($3 \times 7 = 21 \equiv 0 \mod 21$)

- **unit** - two numbers that multiply to one (mod whatever)

  2 for vowels and consonants ($2 \times 3 = 6 \equiv 1 \mod 5$,
  $2 \times 11 = 22 \equiv 1 \mod 21$)

  the "other" number is a way to do division. $\div 2 \mod 5$ is the same as $\times 3 \mod 5$

Exit quiz

- For each number decide if it is zero, a zero divisor, or a unit
- If it is a zero divisor or unit give the "other" number
- 10 for vowels
- 42 for consonants
- 42 for vowels
- 14 for consonants