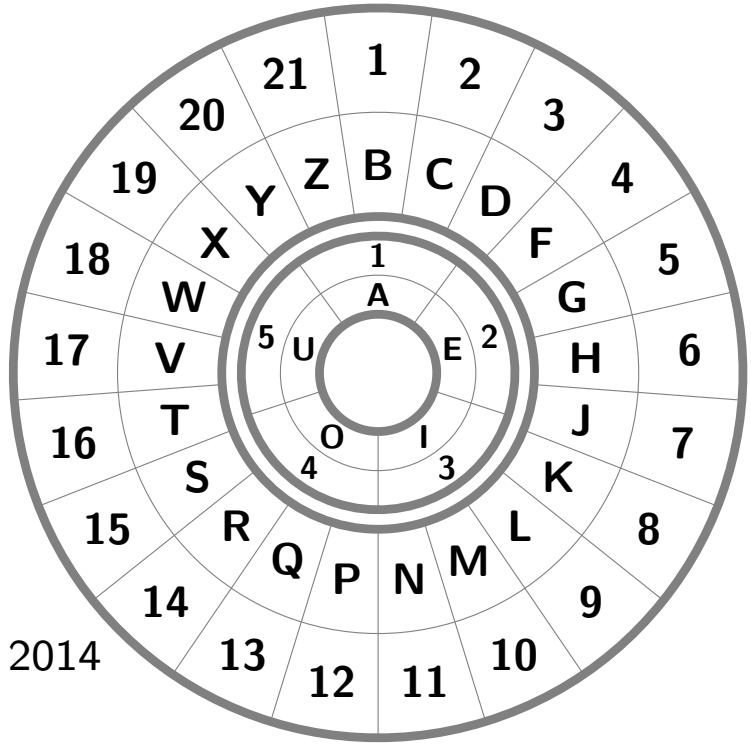
MA111: Contemporary mathematics

Entrance Slip (due 5 min past the hour):

Use a shift of 6 (so that **d**=3 becomes **L**=9) to encrypt the message:

"**this quiz is too easy**"



Schedule:

- HW 1 is due 7am Wednesday, Oct 8th, 2014
- Mini-Exam 2 is in-class on Thursday, Oct 9th, 2014
- HW 2 is due 7am Wednesday, Oct 15th, 2014
- HW 3 is due 7am Wednesday, Oct 22nd, 2014
- Exam 2 is in-class on Thursday, Oct 23rd, 2014

Today we use numbers to make using the codes easier.

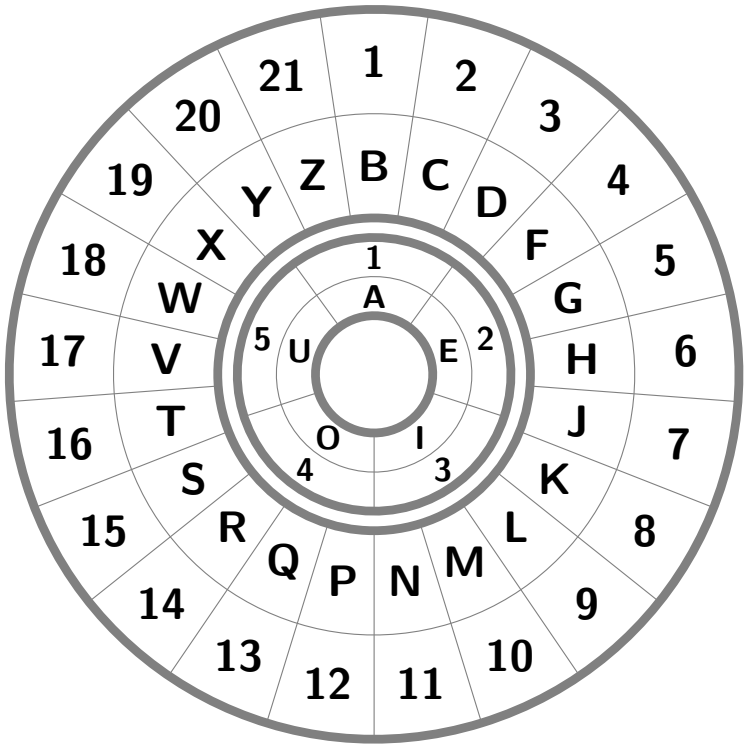
While we are passing out the worksheet...

- Please turn in your entrance slips. We will do this every non-exam day.

  Please bring your own 3x5 index cards.

  Use a shift of 6 (so that **d**=3 becomes **L**=9) to encrypt the message:

  "**this quiz is too easy**"



- What is 16 + 6?
- Where does **t**=16 go? **A**=1?
- Is there a simpler way of describing the vowel shift?
- What about a shift of 11?

Old words

- General 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)

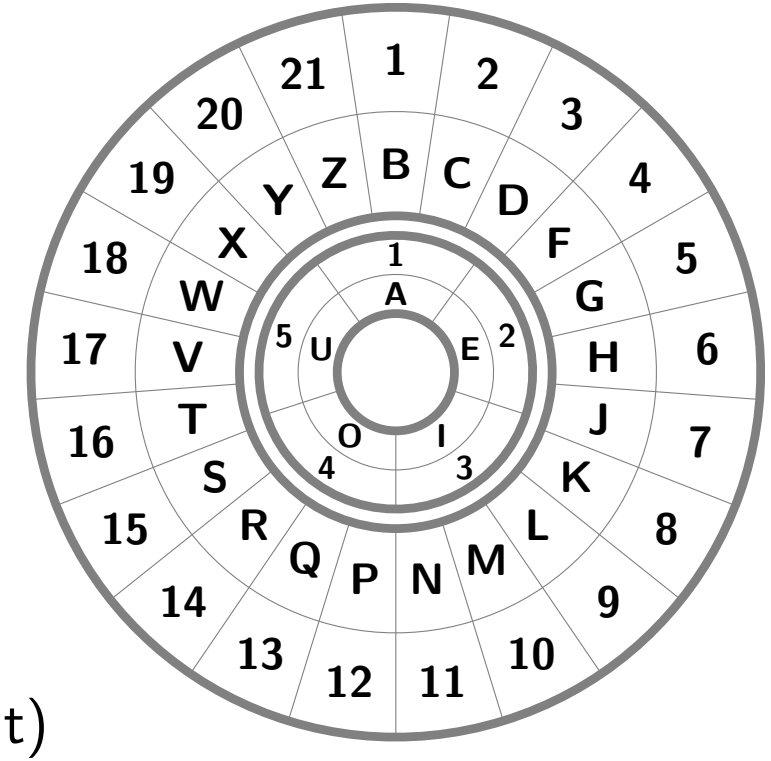
  key (a small secret that lets you change the cipher)

- Shift cipher

  Encrypt: shift vowels and consonants right by an amount according to the key

  Decrypt: shift vowels and consonants left by an amount according to the key

New words: shift cipher with numbers



- To encrypt with shift cipher,
  add the key to the number,
  using wrap-around if too big
  (subtract 5 if a vowel, or
  subtract 21 if a consonant)
- To decrypt with shift cipher,
  subtract the key from the number,
  using wrap-around if too small,
  (add 5 if a vowel, or add 21 if a consonant)
- For example if the shift key is 7, then
  g$= 5 \rightarrow$ **P**$=12$, since $5 + 7 = 12$ and
  w$=18 \rightarrow$ **F**$=4$, since $18 + 7 = 25$ and $25 - 21 = 4$.
- And to decrypt,
  P$=12 \rightarrow$ **G**$= 5$, since $12 - 7 = 5$ and
  F$= 4 \rightarrow$ **W**$=18$, since $4 - 7 = -3$ and $-3 + 21 = 18$.

New words: double-it cipher

- The double-it cipher has no key (we'll fix that next week).
- To encrypt, double the number using wrap-around.
- To decrypt, . . . fill in the decoder wheel? (we'll find a faster way next week)

Exit quiz

- Decode this message knowing that it is encoded using a shift cipher that takes **`b`** to **`P`**

- "**`KVIFI ROR HVI EBOZEYG TU?`**"