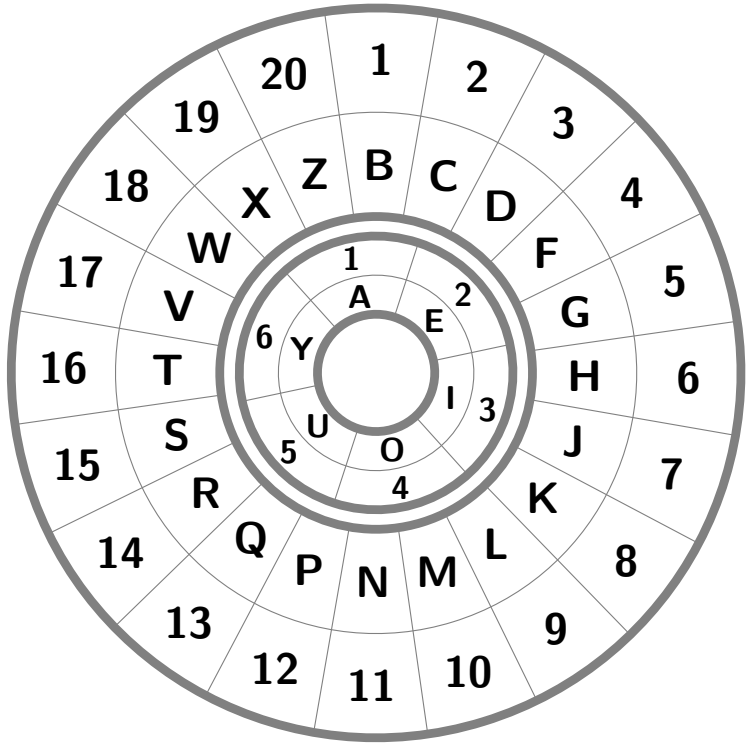
MA111: Contemporary mathematics

Entrance Slip (due 5 min past the hour):

A new wheel makes **y** a **vowel**(y)! Someone encrypted a standard English phrase using double-it with these new wheels to get **KEKZ KEEH**.



What did the original say?

Schedule:

- 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 study mod 5 and mod 21 versus mod 6 and mod 20.

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.

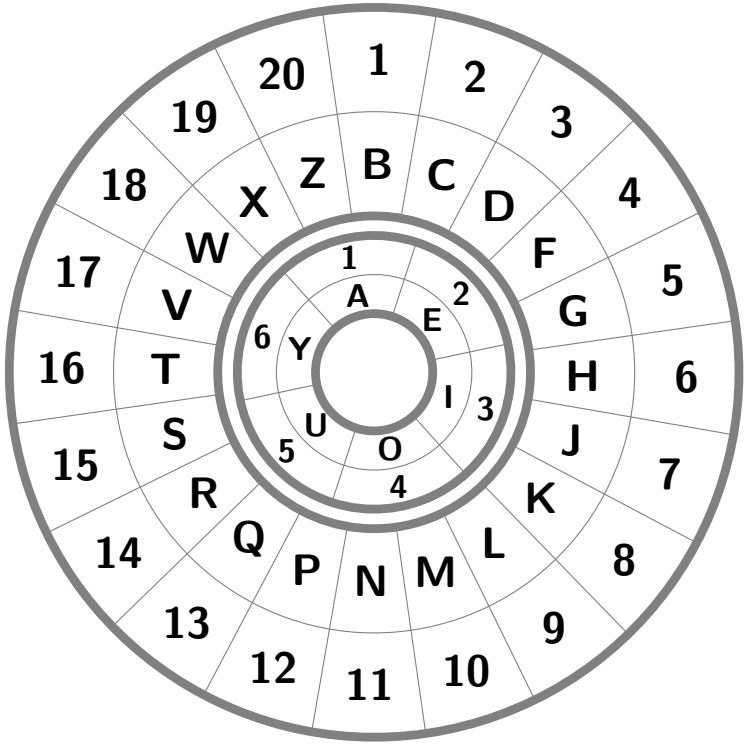
- Might be easier to use numbers:

  KEKZ KEEH 8,2,8,20, ,8,2,2,6

  ↓ ↓

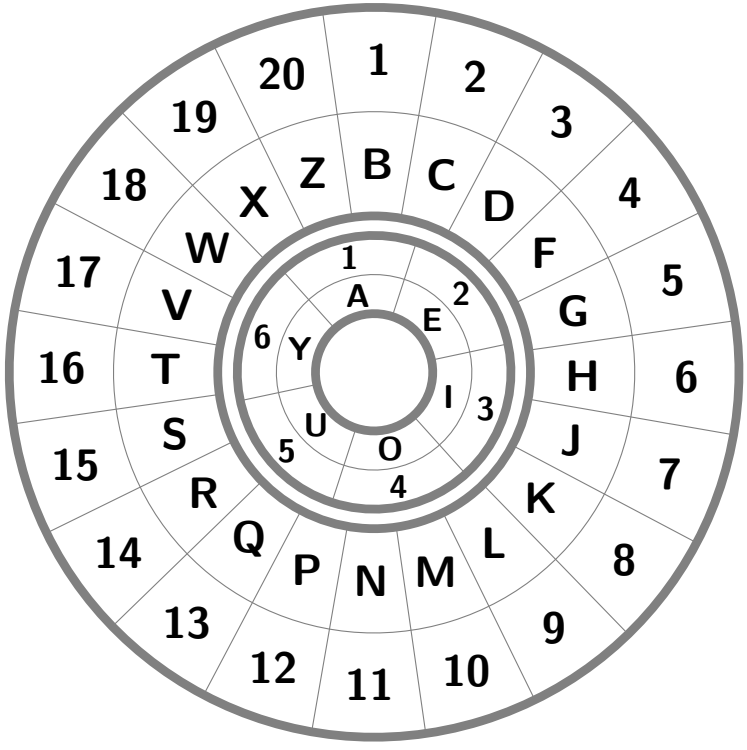
  fafm faad 4,1,4,10, ,4,1,1,3

- That seems unlikely.
  Did anyone get a better decoding?



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.



- Might be easier to use numbers:

  KEKZ KEEH 8,2,8,20, ,8,2,2,6

  ↓ ↓

  fafm faad 4,1,4,10, ,4,1,1,3

- That seems unlikely.
  Did anyone get a better decoding?

- Can we use different numbers?
  +6 for vowel(y)s and +20 consonant(y)s

  KEKZ KEEH 28,8,28,40, ,28,8,8,26

  ↓ ↓

  rorz rooq 14,4,14,20, ,14,4,4,13

- What if we add 6 and 20 again?

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)

New words: modular arithmetic

- **equivalent numbers** $\pmod N$**:** two numbers that differ by a multiple of N

  5, 10, 15, 20, 0, -5, -10 are all equivalent mod 5

- **standard representative:** the unique number between 1 and N equivalent to it

  4 is the standard representative of $104 \pmod{20}$

- **zero:** any number equivalent to 0

  60 is a zero $\pmod 5$, $\pmod 6$, and $\pmod{20}$, but not $\pmod{21}$

- **zero divisor:** a nonzero number that can be multiplied by a nonzero number to get zero

  $2 \pmod 6$ is a zero divisor since $2 \times 3 = 6 \equiv 0 \pmod 6$

New words: multiplication cipher

- A **multiplication cipher** takes the plaintext and multiplies it by the key
- A zero divisor makes a very poor key, because many plaintext letters go to the same ciphertext letter
- How many?

  Either 0 or $\gcd(K, N)$ if $K \pmod N$ is a zero.
- Which?

  If the ciphertext letters number (any/every) is divisible by $\gcd(K, N)$ then $\gcd(K, N)$, otherwise 0
- So the good keys are exactly the ones with $\gcd(K, N) = 1$

  These are called **units**

Exit quiz

- List all good multiplication keys for consonant(not y)s,

  that is all units (mod 20)