Week 7 Thursday

Iðunn's Apples

Loki, the Norse god of mischief, has stolen Iðunn's apples of immortality. He tells her that he'll give them back if she can give him an example of finitely many distinct prime numbers $p_1, p_2, \ldots, p_n$ such that

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$$

is an integer.

Make sure you know your neighbors names, and then work with them to help Iðunn get her apples back!

Quiz 4 Announcement

Please make sure to check the website for some information about quiz 4. One of the problems will require you to do some advance preparation.

RSA

1. (a) If you don't have a computer, sit next to someone who does.

(b) Use SageCell 4.5.8 to generate a 150-bit RSA key.

(c) Post your public key to the Zulip topic titled `in class RSA play`. Make sure to keep your private key secret!

(d) When someone else in the class posts their public key, send them a message! You'll want to keep it under 30 characters. Make sure to tag them so they know that the message is intended for them.

(e) When someone sends you a message, decrypt it!

(f) If you're feeling sneaky, intercept and break a message that wasn't intended for you. If you're feeling both sneaky and brazen, post the plaintext to Zulip! (This is only possible because 150-bits is not big enough to be secure; the modern recommendation is about 4096 bits!)

2. Using the standard letter-to-number correspondence, `BE` represents an integer expressed in base 26. What is that integer?

(A) 14

(B) 30

(C) 105

(D) None of the above

3. When generating his RSA public key, Bob picks the primes $p = 7$ and $q = 11$ and the encryption exponent $e = 23$. What is his decryption exponent d?

4. Bob's RSA public key has modulus $n = 77$ and encryption exponent $e = 23$. Alice encrypts an integer m and sends Bob the ciphertext $c = 2$. Eve intercepts this ciphertext. What is m?

5. Bob would like to choose his RSA public key so that his modulus n is large enough for him to receive 2-letter messages. What is the smallest value of n he can choose?