# Final Exam Review
# Lecture 12c: 2022-04-06

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

# Final Exam outline

1. Prime and composite numbers
   - Sieve of Eratosthenes
   - Runs of composite numbers (recall factorial construction)
2. Divisors and relative primes
   - How to use a factorization to compute these things
3. Fractions/division in modular arithmetic
   - Using reverse Euclidean algorithm and combinations
4. Powers in modular arithmetic
   - Successive squaring, Fermat's Little Thm, Euler's Thm
5. Roots in modular arithmetic
   - Reverse Euclidean algorithm + equivalent powers
6. Fermat primality test
   - Use Fermat's Little Theorem and look for witnesses.
7. Cryptography
   - Caesar cipher, RSA public/private key encryption

# Prime and composite numbers

- A prime number is any number greater than 1 that is only divisible by 1 and itself. Composite otherwise.

Ex. 2, 3, 5, 17, 23, 97

- The prime numbers are multiplicative building blocks.

$36 = 2^2 \cdot 3^2$ $150 = 2 \cdot 3 \cdot 5^2$

- Can find prime numbers up to $n$ by Sieve of Eratosthenes up to $\sqrt{n}$.

2, 3, 5 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~

- Can construct runs of composites using factorials.

Run of 3 composites

8, 9, 10 are 3 non-primes

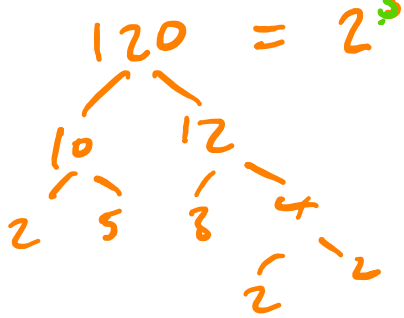
2, 3, 7, 11

$4!+2$ $4!+3$ $4!+4$

$\frac{26}{2}$, $\frac{27}{3}$, $\frac{28}{4}$

# Divisors and relative primes

- Given a factorization, can use the exponents to determine number of divisors.




$\#\ \text{divisors} = (3+1)(1+1)(1+1)$

$= 16$

- Given a factorization, can use the primes present to determine the number of relative primes / compute Euler's totient function.

$\phi(120) = 120\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= 60\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= 40\left(1-\frac{1}{5}\right)$

$= 32$

# Fractions in modular arithmetic

- One algorithm: compute the reciprocal by finding a combination for 1, and then multiply.

$\frac{3}{12} \mod 17$

$17 = 12 \cdot 1 + 5$

$12 = 5 \cdot 2 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2$

$1 = 5 - (12 - 5 \cdot 2) \cdot 2$

$1 = 5 \cdot 5 - 12 \cdot 2$

$1 = (17 - 12) \cdot 5 - 12 \cdot 2$

$1 = 17 \cdot 5 - 12 \cdot 7$

$1 \equiv 17 \cdot 5 - 12 \cdot 7 \mod 17$

$1 \equiv -12 \cdot 7 \mod 17$

$\frac{1}{12} \equiv -7 \mod 17$

$\frac{1}{12} \equiv 10 \mod 17$

$\frac{3}{12} \equiv 3 \cdot 10 \mod 17$

$\equiv 30 \mod 17$

$\equiv 13 \mod 17$

Check: $13 \cdot 12 \equiv 3 \mod 17$

# Powers in modular arithmetic

- Successive squaring algorithm: to find $a^n$, write $n$ as a sum of powers of 2, and then square to find $a^2, a^4, a^8, a^{16}, \ldots$.

$a^{18} = a^{16} \cdot a^2$

$a^1$
$a^2$
$a^4$
$a^8$
$a^{16}$

- Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$ if $\gcd(a, p) = 1$ for prime $p$.

$2^4 \equiv 1 \mod 5$ so $2^{16} \equiv 2^2 \mod 5$

- Euler's Theorem: $a^{\phi(n)} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$

$\phi(15) = 3 \cdot 5 \cdot (1 - \frac{1}{3})(1 - \frac{1}{5}) = 8$

$2^8 \equiv 1 \mod 15$, so $2^{17} \equiv 2^1 \mod 15$

# Roots in modular arithmetic

- Given $\sqrt[k]{a} \pmod{n}$, find $a^{mk} \equiv a$ using Euler's Thm, and then $\sqrt[k]{a} \equiv a^m$. Need to check conditions $\gcd(a, n) = 1$ and $\gcd\big(k, \phi(n)\big) = 1$.

$\sqrt[3]{2} \mod 15$

$\phi(15) = 8$

$\gcd(2, 15) = 1$

$\gcd(8, 3) = 1$

$8 = 3 \cdot 2 + 2$

$3 = 2 \cdot 1 + 1$

$1 = 3 - 2$

$1 = 3 - (8 - 3 \cdot 2)$

$1 = 3 \cdot 3 - 8$

$1 + 8 = 3 \cdot 3$

$\sqrt[3]{2} \equiv \sqrt[3]{2^{3 \cdot 3}} \equiv 2^3 \mod 15$

$\Rightarrow \sqrt[3]{2} \equiv 2^3 \mod 15$

$\equiv 8 \mod 15$

# Primality testing

- Consider a number $n$.
- Pick a random number $a$.
- If $a^{n-1} \not\equiv 1 \pmod{n}$, then $a$ is composite.
- Otherwise, $n$ passes the Fermat primality test, which decreases the chance of it being composite by at least 50%.

Ex. $n = 11$

$2^{10} \bmod 11$

$\equiv 1024 \bmod 11$

$\equiv 1 \bmod 11$

$3^{10} \bmod 11$

$\equiv 9^5 \bmod 11$

$\equiv (-2)^5 \bmod 11$

$\equiv -32 \bmod 11$

$\equiv 1 \bmod 11$

$\Rightarrow \frac{3}{4}$ chance prime

Ex. $n = 9$

$2^8 \bmod 9$

$\equiv 256 \bmod 9$

$\equiv 4 \bmod 9$

$\Rightarrow$ 9 is composite.

# Cryptography

- Caesar cipher just shifts all the letters by a fixed amount in the alphabet; a symmetric cipher.

ABC $\xrightarrow{+2}$ CDE $\xrightarrow{-2}$ ABC

- RSA public-key encryption makes use of the fact that factoring and square roots are hard in modular arithmetic.

See prev. interaction

- Hybrid cryptography combines both together, using public-key encryption to send a symmetric key, and then using the symmetric cipher for everything else.

# How do you feel about the final?

A: So ready


B: Hopeful

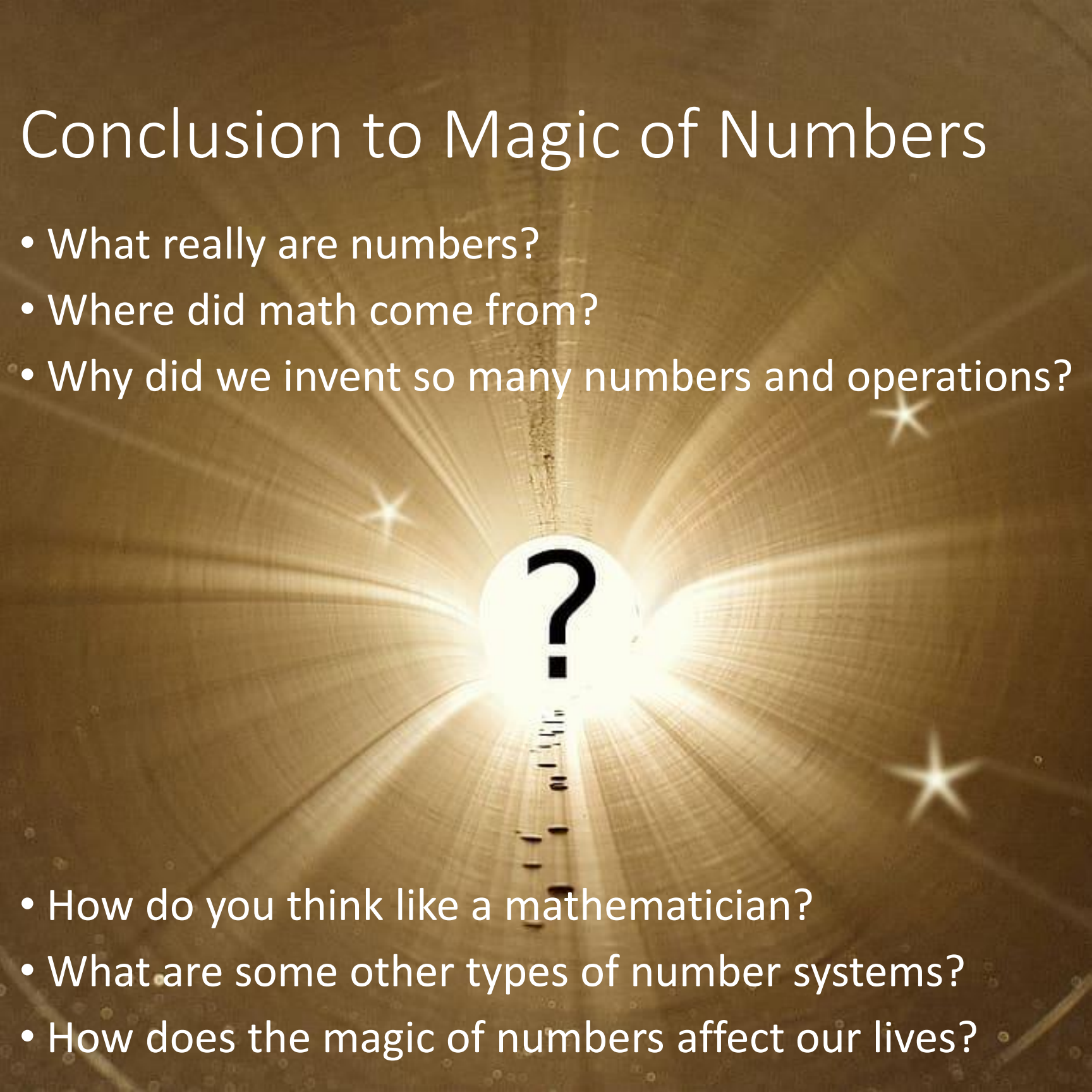

E: This is *fine*


D: Preparing for the worst


C: Meh

# Conclusion to Magic of Numbers

- What really are numbers?
- Where did math come from?
- Why did we invent so many numbers and operations?




- How do you think like a mathematician?
- What are some other types of number systems?
- How does the magic of numbers affect our lives?