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.

- The prime numbers are multiplicative building blocks.

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

- Can construct runs of composites using factorials.

Divisors and relative primes

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

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

Fractions in modular arithmetic

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

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 $a^2, a^4, a^8, a^{16}, \ldots.$

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

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

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 $\gcd\left(k, \phi(n)\right) = 1$.

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%.

Cryptography

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

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

- 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?