MATH 314 Spring 2019 - Class Notes

02/19/2019

Scribe: Shannon Miko

Summary: In today's class, we discussed modular arithmetic and modular exponentiation, and we learned how to use modular exponentiation when finding $a^b \pmod{n}$. We also learned about Fermat's Little Theorem and how to apply it when using modular exponentiation with a prime modulo.

Modular Arithmetic: Define $a \equiv b \pmod{n}$ if $(b-a)$ is divisible by n

Lemma: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv (b + d) \pmod{n}$

Proof:

Since $a \equiv b \pmod{n}$, then $(b-a) = kn$ for some integer k, and $(d-c) = jn$ for some j

Check $(b+d) - (a+c) = (b-a) + (d-c) = kn + jn = n(k+j)$

The above equation $(n(k+j))$ is divisible by n, so $(a+c) \equiv (b+d) \pmod{n}$

Residue Classes: the collection of all of the numbers with the same remainder when divided by n.

Example: $[1, 4, 7, 10, 13, ...]$ of numbers $\equiv 1 \pmod{3}$ forms a residue class.

Rings: objects that can be added, multiplied, or subtracted to form another object

Examples: matrices (of a fixed size), a set of residues $\pmod{n}$, integers, rational numbers, real numbers, complex numbers, and polynomials

Multiplying by an Inverse in Residue Classes:

- $a \pmod{n}$ has an inverse if and only if $gcd(a, n) = 1$.
- to find $a^{-1} \pmod{n}$, use Euclid's algorithm to find x, y so that $ax + ny \equiv 1 \pmod{n}$.

Example: Find $19^{-1} \pmod{79}$

$$25(19) - 6(79) = 1$$

$$19^{-1} \equiv \underline{25 \pmod{79}}$$

Modular Exponentiation: We want to compute $a^b \pmod{n}$ when b is very large. We do this through modular exponentiation. The trick is to use repeated squaring.

1. Take the exponent and write it in binary.
2. Compute a^{2^i} for each power of 2 showing up in the binary expression of b. To do this, compute $a^{2^i} \equiv a^{2^{(i-1)2}} \pmod{2}$
3. Multiply together the terms of the binary expression of b.

Example:

- $5^{273} \pmod{11}$

  1. $273 = 256 + 17 \equiv 256 + 16 + 1 \equiv 2^8 + 2^4 + 2^0 \equiv 100010001$
  2. $5^1 = 5 \pmod{11}$
     $5^2 \equiv 25 \equiv 3 \pmod{11}$
     $5^4 \equiv (5^2)^2 \equiv 3^2 \equiv 9 \pmod{11}$
     $5^8 \equiv (5^4)^2 \equiv 9^2 \equiv 81 \equiv 4 \pmod{11}$
     $5^{16} \equiv (5^8)^2 \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$
     $5^{32} \equiv (5^{16})^2 \equiv 5^2 \equiv 25 \equiv 3 \pmod{11}$
     $5^{64} \equiv (5^{32})^2 \equiv 3^2 \equiv 9 \pmod{11}$
     $5^{128} \equiv (5^{128})^2 \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$
  3. $5^{273} \equiv (5^{256}) * (5^{16}) * (5^1) \equiv 5 * 5 * 5 \equiv \underline{4 \pmod{11}}$

Fermat's Little Theorem: If p is a prime number and a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Basic Principle: When computing an exponent modulo a prime number, the term in the exponent can be reduced $\pmod{p-1}$. For numbers that are not prime, though, **this will not work**.

Example:

$$5^{273} \pmod{11}$$

Reduce exponent $\pmod{10}$:

$$273 \pmod{10} \equiv 3 \pmod{10}$$

$$5^3 \pmod{11} \equiv 125 \equiv \underline{4 \pmod{11}}$$