MATH 314 Spring 2018 - Class Notes

02/20/2018

Scribe: Connor Gephart

Summary: Today we covered the Chinese Remainder Theorem, Modular Exponentiation, and Fermat's Little Theorem.

Chinese Remainder Theorem: If n and m are coprime integers, then the two equations $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ have a unique solution $\pmod{m * n}$ for any a,b.

Example:

$$x \equiv 17 \pmod{26}$$

$$26 = 13 * 2$$

$$x \equiv 17 \equiv 1 \pmod{2}$$

$$x \equiv 17 \equiv 4 \pmod{13}$$

17 is the only nmber capable of making this combination (which satisfies both equations).

Example:

$$x \equiv 3 \pmod{7}$$

$$x \equiv 12 \pmod{13}$$

The CRT tells us there is a unique number $\pmod{91}$ that satisfies both equations.

How to find this number x?

$$x \equiv 3 + k(7) \equiv 12 \pmod{13}$$

$$7(k) \equiv 9 \pmod{13}$$

Find $7^{-1} \pmod{13}$

$$gcd(13, 7)$$

$$13 \equiv 1(7) + 6$$

$$7 \equiv 1(6) + 1$$

$$1 = 7 - 1(6)$$

$$1 = 7 - 1(13 - 1(7))$$

$$1 = 7 - 1(13) + 1(7)$$

$$1 = 2(7) - 1(13)$$

$$1 \equiv 2(7) \pmod{13}$$
$$7^{-1} \equiv 2 \pmod{13}$$

Multiply equation by 7^{-1} to solve for k

$$7(k) \equiv 9 \pmod{13}$$
$$2(7)(k) \equiv 2(9) \pmod{13}$$
$$k \equiv 18 \pmod{13}$$
$$k \equiv 5 \pmod{13}$$

Plug in k to solve for x

$$x = 3 + k(7)$$
$$x = 3 + 5(7)$$
$$x \equiv 38 \pmod{91}$$

Check to make sure the answer is correct

$$38 \equiv 3 \pmod{7}$$
$$38 \equiv 12 \pmod{13}$$

Modular Exponentiation:

Algorithm to compute $a^k \pmod{m}$ surprisingly fast even if k and m are large

Suppose $5^{273} \pmod{11}$. We cannot simply compute 5^{273} because it is too big of a number.

Repeated Squaring:

Lets us compute $a^2 \pmod{m}$ quickly

Start with a
Square it a^2 and reduce $\pmod{m}$
Square it a^4 and reduce $\pmod{m}$
Square it a^8 and reduce $\pmod{m}$
...
Eventually end with $a^{2^i} \pmod{m}$

- **Modular Exponentiation Steps:**
  1. Write exponent in binary (sum of powers of 2)

2. Use repeated squaring to compute $a^{2^i} \pmod{m}$ for each power of 2 in the binary expansion
3. Multiply these numbers together from step 2 and reduce $\pmod{m}$

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

1. $273 = 2^8 + 2^4 + 2^0$
2. $5^1 \equiv 5 \pmod{11}$
   $5^2 \equiv 3 \pmod{11}$
   $5^4 \equiv 3^2 \equiv 9 \pmod{11}$
   $5^8 \equiv 9^2 \equiv 4 \pmod{11}$
   $5^{16} \equiv 4^2 \equiv 5 \pmod{11}$
   $5^{32} \equiv 5^2 \equiv 3 \pmod{11}$
   $5^{64} \equiv 3^2 \equiv 9 \pmod{11}$
   $5^{128} \equiv 9^2 \equiv 4 \pmod{11}$
   $5^{256} \equiv 4^2 \equiv 5 \pmod{11}$
3. $5^{273} = 5^{256} * 5^{16} * 5^1 = 5 * 5 * 5 = 125$
   $125 \pmod{11} \equiv 4 \pmod{11}$

Example: Find last digit of 3^{212}. This is the same as asking to fine $3^{212} \pmod{10}$

$$212 = 2^7 + 2^6 + 2^4 + 2^2$$
$$3^1 \equiv 3 \pmod{10}$$
$$3^2 \equiv 3^2 \equiv 9 \pmod{10}$$
$$3^4 \equiv 9^2 \equiv 1 \pmod{10}$$
$$3^8 \equiv 1^2 \equiv 1 \pmod{10}$$
$$3^{16} \equiv 1^2 \equiv 1 \pmod{10}$$
$$3^{32} \equiv 1^2 \equiv 1 \pmod{10}$$
$$3^{64} \equiv 1^2 \equiv 1 \pmod{10}$$
$$3^{128} \equiv 1^2 \equiv 1 \pmod{10}$$

$$3^{212} \equiv 1 * 1 * 1 * 1 \equiv 1 \pmod{10}$$

The last digit is a 1.

Fermat's Little Theorem:

If p is a prime number, and a is coprime to p, then $a^{p-1} \equiv 1 \pmod{p}$.

Examples:

$$\text{a} = 2 \text{ and p} = 5$$

$$a^{p-1} \equiv 2^{5-1} \equiv 2^4 \equiv 16 \equiv 1 \pmod{5}$$

$$\text{a} = 2 \text{ and p} = 7$$

$$2^{7-1} \equiv 2^6 \equiv 64 \equiv 1 \pmod{7}$$

$$\text{a} = 3 \text{ and p} = 5$$

$$3^{5-1} \equiv 3^4 \equiv 81 \equiv 1 \pmod{5}$$

Note: This only works if p is prime.

Bad Example:

$$\text{a} = 2 \text{ and p} = 6$$

$$2^{6-1} \equiv 2^5 \equiv 32 \equiv 2 \pmod{6}$$

Note: If we have a prime modulus, and we want to compute $a^k \pmod{p}$ we can write $k = l(p-1) + r$ so

$$a^k = a^{l(p-1)+r} = (a^{p-1})^l (a^r) \pmod{p} = a^r \pmod{p}$$

$$a^k \equiv a^r \pmod{p}$$

because$(a^{p-1})^l$ becomes 1.

Example:

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

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

so

$$5^{273} \equiv 5^3 \equiv 4 \pmod{11}$$