2/19/2018 Class Notes

Jonathan Schoene

February 27, 2018

Definition: We say that m and n are coprime if the gcd(greatest common denominator) = 1

- Example: 10 and 21 are coprime 10 and 6 are not coprime

Theorem(Restated): The residue of a(mod m) has an inverse if and only if a and m are coprime

Chinese Remainder Theorem:

- If m and n are coprime integers then the equations x $\equiv a(modm)$ and $x \equiv b(modn)$ have a unique solution modulo m * n
- Example:
  $x \equiv 17(mod26)$
  $x \equiv 1(mod2)$
  $x \equiv 4(mod13)$
  - Notice that the modulo in the second two equations are coprime factors of 26.
  - The Chinese Remainder Theorem tells us that 17 is the only remainder (mod 26) that satisfies both equations
- Pick two small prime numbers
  $x \equiv 6(mod11)$
  $x \equiv 11(mod13)$
  - Chinese Remainder Theorem says that there is a number modulo 11*13 that satisfies both equations.
  - Using these equations we can also say $x \equiv 6 + k(11)$ and using our second equation we have $x \equiv 11(mod13)$
  - Therefore $6 + k(11) \equiv 11(mod13)$
    $k(11) \equiv 5(mod13)$
    $k * 11 * 6 \equiv 5 * 6(mod13)$
    $k \equiv 4(mod13)$

- We need to find 11^{-1} using Euclids Algorithm: gcd(13,11) gives us the equation $1 \equiv 6(11) mod(13)$
- Lets try using k = 4
  $x \equiv 6 + 4(11) \equiv 50$ and $50 \equiv 11(mod 13)$
  Therefore $x \equiv 50(mod 143)$ is the unique solution to both $x \equiv 6(mod 11)$ and $x \equiv 11(mod 13)$

Modular Exponentiation

- Way to compute $a^k(mod m)$ very fast, even if k is a very large number
- Suppose you want to compute $5^{521}(mod 11)$
  - Repeated squaring lets us compute a^{2^k} (mod m) quickly
  - Start with a and square it to get a^2 reduce (mod m), then you square it again to get a^4, then again for a^8
  - Reduce (mod m) after every step to make sure the numbers don't get too big
  - **Example**
    Write k in base 2
    $5^{521} => 521 = 512 + 8 + 1$
    Use repeated squaring to compute $a^{2^i}(mod m)$ for each power of 2 showing up in the binary for k
    $5^1 \equiv 5(mod 11)$
    $5^2 \equiv 3(mod 11)$
    $5^4 \equiv 9(mod 11)$
    $5^8 \equiv 4(mod 11)$
    $5^{16} \equiv 5(mod 11)$
    $5^{32} \equiv 3(mod 11)$
    $5^{64} \equiv 9(mod 11)$
    $5^{128} \equiv 4(mod 11)$
    $5^{256} \equiv 5(mod 11)$
    $5^{512} \equiv 3(mod 11)$
    We know that we need the values for 2^9, 2^3, and 2^0 and then we multiply those values together
    So we have $5^{521} => 5^{521} + 5^8 + 5^0$ which by the repeated squares we did above $5^{521} = 5 * 4 * 3(mod 11) = 5(mod 11)$
  - This means that repeated squaring lets us compute this is time O(logk) and we never need to store numbers larger than m^2
  - We can also use this to find the last digit of 3 raised to the 136th power
    This is asking for $3^{136}(mod 10)$
    $136 = 128 + 8$
    $3^1 = 3(mod 10)$
    $3^2 = 9(mod 10)$

$3^4 = 1(mod10)$
$3^8 = 1(mod10)$
...
$3^{128} = 1(mod10)$
This means that the last digit of the number would be a 1

Femat's Little Theorem

- If p is a prime number and a is coprime to p the $a^p \equiv a(modp)$ and $a^{p-1} \equiv 1(modp)$
  Try this out!
  a=2 and p=5
  $a^{p-1} \equiv 2^{5-1} \equiv 2^4 \equiv 16 \equiv 1(mod5)$
  Let p = 7
  $a^{p-1} \equiv 2^{7-1} \equiv 2^6 \equiv 64 \equiv 1(mod7)$
  So it always works!
- What if we try it with a non-prime number?
  Let p = 6
  $a^{p-1} \equiv 2^{6-1} \equiv 2^5 \equiv 32 \equiv 2(mod6) \neq 1$
  So it doesn't work if p is not prime!
- What if we try it with base 3
  a = 3 p = 5
  $a^{p-1} \equiv 3^{5-1} \equiv 3^4 \equiv 81 \equiv 1(mod5)$
  It works!
- If we want to compute $a^k(modp)$ we can write k as some $l(p-1)+r$ where r is the remainder when we divide k by p-1
  $a^k \equiv a^{l*(p-1)} * a^r \equiv a^{(p-1)^l} * a^r(modp) \equiv a^r(modp)$
  We can say this because according to Femat's little theorem $a^{(p-1)^l} \equiv 1$
- The take home message is...
  We want to compute a^k(mod p) if k = r(mod p-1) then $a^k \equiv a^r(modp)$
  Lets try our original example again
  $5^{521}(mod11)$
  Since $521 \equiv 1(mod10)$
  $5^{521}(mod11) \equiv 5^1 \equiv 5(mod11)$
- General principle of modular arithmetic (prime version) is when you do exponentiation(mod p) you do arithmetic inside the exponent (mod p-1)