CS70 In Simpler Terms - Note 9

written by Kevin Liu cs70.kevinmliu.com

July 31, 2017

1 Modular Arithmetic

There are a number of basic rules that you have to know very well when it comes to mods. But with practice, working with mods can easily and quickly become one of your strenghs.

- $a \equiv a \pmod{n}$
- if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$
  $\Rightarrow (a + c) \pmod{n} \equiv (b + d) \pmod{n}$ and
  $(a * c) \pmod{n} \equiv (b * d) \pmod{n}$
- x is said to have a multiplicative inverse(M.I.) $\pmod{n}$ iff the gcd of x and n is 1 (n, x are relatively prime(coprime))
  $ax \pmod{n} = 1 = 1 \pmod{n}$, where a is the M.I. of $x \pmod{n}$
- If x has a multiplicative inverse(M.I.) $\pmod{n} \Rightarrow$ the M.I. is unique
- *Example on the use of the M.I.: Solve for x where* $2x = 3 \pmod{7}$
  This equation is equivalent to $2x \pmod{7} = 3 \pmod{7}$
  The M.I. of $2 \pmod{7}$ *is* 4 *so we multiply both sides of the equation by 4*
  We get $8x \pmod{7} = 3 \pmod{7}$,
  which equals $(8 \pmod{7}) (x \pmod{7}) = 12 \pmod{7}$,
  which simplifies to $x \pmod{7} = 5 \pmod{7}$.
  So $x = 5 \pmod{7}$
- Bijection: one-to-one and onto. A function, f, is said to be a bijection iff there is an inverse function g, such that $g(f(x) = x$ and $f(g(y)) = y$ for all x, y.

Euclid's Algorithm:
Let $x \geqslant y$, and let $x = yq + r$, where $r < y$
Then $d = \gcd(x, y) = \gcd(y, r)$ because
Taking mod$d$ on both sides, $x \pmod{d} = yq \pmod{d} + r \pmod{d}$. We know that $x \pmod{d} = 0$,and $yq \pmod{d}$ also $= 0$ since both terms are divisible by d, the greatest common denominator. This means that $r \pmod{d}$ must also $= 0$, so our proof is complete.

An important result that stems from Euclid's Algorithm is that $\gcd(x, y) = d = \gcd(x, y - d)$.

Chinese Remainder Theorem:
I will not go over the proof but I will state the result, which is something you will need to know:

- Given a system of equations:
  $x \equiv a_1 (\text{mod } n_1)$
  $x \equiv a_2 (\text{mod } n_2)$...
  $x \equiv a_k (\text{mod } n_k)$
  If the $\gcd(n_i, n_j) = 1$
  $\Rightarrow$ There exists a unique solution for $x \bmod(n_1 * n_2 * ...n_k)$

- You can also go backwards too! Given:
  $n \equiv 1 \bmod(5 * 11 * 17) \Leftarrow$ coprime numbers
  $\Rightarrow n \equiv 1 \bmod(5)$, $n \equiv 1 \bmod(5)$, $n \equiv 1 \bmod(5)$
  Because $n = 1 + (5 * 11 * 17) * q$, and taking (mod 5) on both sides,
  We see that we get $n \pmod 5 = 1 \pmod 5$
  Taking (mod 11) and (mod 17) gives us the other 2 results.

Fermat's Little Theorem:
This is arguably the most important theorem you need to remember when it comes to problems concerning mods. Applying this theorem can often simplify your calculations by a significant amount.

- if p is prime, then $a^p \equiv a \pmod p$ *($a^p - a$ is a multiple of p)*
- if p does not divide a where $a > 0$, then $a^{p-1} \equiv 1 \pmod p$
- $x^a \equiv x^{amod(p-1)}$
- ****IMPORTANT**** $a^{(p-1)(q-1)} \equiv 1 \bmod(pq)$. This can be extended to any number of variables (e.g. p, q, r, s)

  Example: Simplify $11^{97} mod(3 * 5 * 7)$
  From the above theorem, $11^{(3-1)(5-1)(7-1)} \equiv 11^{48} \equiv 1\ mod(3 * 5 * 7))$
  Looking back at our initial problem:
  $11^{97} = (11^{48})^2 * 11 \equiv 1^2 * 11 \pmod{3 * 5 * 7} \equiv 11 \pmod{105}$