Recitation 1 Notes: Number theory
Feb 15, 2013

We covered some number theory background useful for the class. Below I will provide a list of the topics we covered. All this material is presented in detail in Dana Angluin's Lecture Notes on the "Complexity of Some Problems in Number Theory" in Chapters 3-10 `http://courses.csail.mit.edu/6.857/2013/files/angluin.ps`.

Divisor

We say that "d divides a", written $d \mid a$, if there exists an integer k such that $a = kd$ and that d is a divisor of a.

If d | a and $d \mid b$, then d is a common divisor of a and b.

Example: What numbers divide 9? 1, 3, 9

Prime number

An integer $p > 1$ is prime if its only divisors are 1 and p.

Modular arithmetic

For a and b integers, the quotient expression is

$a = b * q + r$, where $r, q \in \mathbb{Z}$ and $r < b$. We also write:

$a \equiv r \pmod{b}$

Example: What is 19 mod 17? 2. What is 181282347* 34 mod 34? 0.

GCD

The greatest common divisor, gcd(a, b), of two integers a and b is the largest of their common divisors.

Example: What is the gcd(12, 18)? 6.

Example: what is gcd(12, 7)? 1.

Integers a and b are relatively prime if gcd(a, b) = 1.

We then covered Euclid's algorithm for computing the gcd together with proof of correctness. This is detailed in Dana Angluin's notes.

Example:

$$\gcd(234, 108)$$

$$234 = 108 \cdot 2 + 18$$
$$108 = 18 * 6$$

$$\gcd = 18$$

$$\gcd(233, 144):$$

$$233 = 144 * 1 + 89$$
$$144 = 89 * 1 + 55$$
$$89 = 55 * 1 + 34$$
$$55 = 34 * 1 + 21$$
$$34 = 21 * 1 + 13$$
$$21 = 13 * 1 + 8$$
$$13 = 8 * 1 + 5$$
$$...$$
$$3 = 2 * 1 + 1$$
$$2 = 2 * 1$$

$\gcd(233, 144) = 1$ so they are relatively primes.

We also looked at the extended Euclid's algorithm that allows us to compute $x, y \in \mathbb{Z}$ such that $d = xa + yb$, where $d = \gcd(a, b)$.

The number of steps in Euclid's algorithm is $O(\log n)$, where $n = \max(a, b)$. Recall that a function f is $f = O(g)$ for another function g, if for all constants $C > 0$, there exists N such that for all $n > N$, $f(n) \leq Cg(n)$.

Groups

We recalled the definition of groups. A group is a set, G, with an associated operation $\cdot$ such that the following properties hold:

- Closure: For all $a, b \in G$, the result of the operation, $a \cdot b$, is also in G.
- Associativity: For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- Identity element or 1: There exists an element $e \in G$, such that for every element $a \in G$, the equation $e \cdot a = a \cdot e = a$ holds. There is a unique such element.
- Inverse element: For each $a \in G$, there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$.

Multiplicative group mod a prime p

$\mathbb{Z}_p^* = \{1, \ldots, p-1\}$
We argued why $\mathbb{Z}_p^*$ is a group.
Example: What is the inverse of 4 mod 7? 2.
Example: What is the inverse of 3 mod 13? 9.

Multiplicative group mod n

$\mathbb{Z}_n^* = \{x : 1 \le x \le n \text{ and } \gcd(x, n) = 1\}$

The totient function $\phi(n) = |\mathbb{Z}_n^*|$ is the size of the group, also called the order of the group.

Any element of a group raised to the power of the order of the group is 1:

> Euler's theorem: for any $n > 1$ and $a \in \mathbb{Z}_n^*$, $a^{\phi(n)} \equiv 1 (\text{mod } n)$.

> Fermat's little theorem: if p is prime and $a \in \mathbb{Z}_p^*$ then $a^{p-1} \equiv 1 (\text{mod } p)$.

Example: The problem from the signup sheet: $8^{962} (\text{mod } 97) = 8^2 (\text{mod } 97) = 64$.
Consequence of Euler, we have $a^d \equiv a^{d \bmod \phi(p)} \bmod p$.
Example: $7^{78} \bmod 11 = 7^1 \bmod 11 = 7$
If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.
So if $n = pq$, we have $\phi(n) = (p-1)(q-1)$.

<u>Fast exponentiation</u> We covered the algorithm for repeated squaring that computes $a^b \bmod n$ by performing $\log b$ squarings. See Dana Angluin's notes (page 12) for the algorithm.

<u>Generators</u>

A finite group $(G, \cdot)$ may be cyclic, which means that it contains a generator g such that every group element $h \in S$ is a power $h = g^k$ of g for some $k \ge 0$.

The group $\mathbb{Z}_5^*$ is generated by $g = 2$, since the powers of 2 (mod 5) are: $2, 4, 3, 1$.

<u>Chinese remainder theorem (CRT)</u> See page 11 of Dana Angluin's notes for CRT.