Number Theory I:

Extended Euclidean Algorithm

02/17 Prof. Forrest

Warm-up

1. Discuss with your neighbors whether desserts can be savory (i.e. must they be sweet)

2. Give the Lagrange basis polynomials (e.g. $\{\ell_0(x), \ell_1(x), \ell_2(x), \ell_3(x)\}$) for the following shares (or points): $f(1)=3$, $f(2)=6$, $f(3)=1$, $f(4)=2$

$$\ell_0(x) = \frac{x-2}{1-2} \cdot \frac{x-3}{1-3} \cdot \frac{x-4}{1-4} \leftarrow$$

$\ell_0(1) = 1 \quad f(3) = 0$

Logisitics

- Codelet 2 has been graded everyone did fine.

Recall Shamir's Secret Sharing

Secret

$$f(x) = \text{secret} + \sum_{i=1}^{k-1} a_i x^i \quad \text{where} \quad a_i \in_{\text{random}} \text{Domain}$$

distribute n shares $n \geq k$

$(1, f(1))$ $(2, f(2))$ $(3, f(3))$ $\ldots$ $(k, f(k))$ $\ldots$ $(n, f(n))$

k people are need to reconstruct the secret and no group of people $< k$ learn anything about the secret.

Challenge: (1) integer overflow (e.g., what if coefficients are large)

(2) precision (e.g., $2/3$)

$x, y \in \mathbb{R}$ $\quad 1.2 \quad 1.3333\ldots$

$x \cdot y = 1$

$\Leftrightarrow$ multiplicative inverse of x

$x \cdot x^{-1} = 1 \equiv x \cdot \frac{1}{x} = 1$

$x = 3 \quad x^{-1} = 1/3$

$1 = 2\ x^{-1}, \quad x^{-1} \in \mathbb{Z}$

$x^{-1} \in \mathbb{Q}$

$1/2$

Division $\quad \frac{x}{y} \equiv x\, y^{-1}$

Division Theorem

For integers $d > 0$ and n, the quantity $n \bmod d$ is the unique integers r and q when $0 \leq r < d$ and $dq + r = n$

$$n \bmod d = r$$

↑ remainder

$$q := \left\lfloor \frac{n}{d} \right\rfloor$$

$$n = \left\lfloor \frac{n}{d} \right\rfloor \cdot d + (n \bmod d)$$

↑ quotient ↑ divisor ↑ remainder

(1) $n = 7 \qquad d = 3$

$7 = 7 \bmod 3 + \_\_$

$r=1 \quad q=2$

$7 = q \cdot 3 + r$

$-21 \bmod 10$

$-21 = q \cdot 10 + r$

-3

9

Properties Mod. arithmetic

$$n \mod n = 0$$

$$(a+b) \mod n = (a \mod n + b \mod n) \mod n$$

$$ab \mod n = (a \mod n \cdot b \mod n) \mod n$$

$$2 \cdot 5 \mod 6 = 4$$

$$\underbrace{2 \mod 6}_{2} \cdot \underbrace{5 \mod 6}_{5} = 10 \mod 6 = 4$$

$$a \cdot b \mod n \equiv (a \mod n \cdot b \mod n) \mod n$$

$$a \to r \qquad b \to s$$

$$a \equiv cn + r$$

$$r \equiv a \mod n$$

$$b \equiv dn + s$$

$$s \equiv b \mod n$$

$$a \cdot b \mod n \equiv$$

$$\equiv ((cn + r) \cdot (dn + s)) \mod n$$

$$\equiv (cdn^2 + cns + dnr + rs) \bmod n$$

$$\equiv ((cdn + cs + dr)n + rs) \bmod n$$

$$\equiv (cdn + cs + dr)n \bmod n + rs \bmod n$$

$$\equiv rs \bmod n$$

$$\equiv ((a \bmod n) \cdot (b \bmod n)) \bmod n$$

□

Definition: Divisibility

For two integers $m > 0$ and n we write $m \mid n$ to denote the proposition that $n \bmod m = 0$. If $m \mid n$, then we say that m **divides** n (or that m evenly divides n), that n is a **multiple** of m, and that m is a **factor** of n.

$a \mid 0$

$1 \mid a$

are these true?

for some positive integer a

$\hookrightarrow a \mod 1 = 0$

$0 \mod a = 0$

$r = 6 \mod 1$

$1 \cdot q + \textcircled{r} = 6$

def Greatest common divisor

GCD

The greatest common divisor of two positive integers n, m ($\gcd(n, m)$) is the largest $d \in \mathbb{Z}^{>0}$ s.t. $d|n$ and $d|m$

$\gcd(6, 27) = 3$

$\gcd(12, 18) = 6$

$\gcd(1, 9) = 1$

Euclid(n, m)

Input: $n, m \in \mathbb{Z}^{>0}$ and $m \geq n$

Output: $gcd(n, m)$

```
1. If   m mod n = 0 then
2.      return n
3. else
4.      return Euclid( m mod n, n )
```

Euclid(7, 42)

Bezout's Identity:

Let n, m be any positive integers and let $gcd(n, m)$ be r, then there exists $x, y \in \mathbb{Z}$ such that $xn + ym = r$

2, 9

$$\gcd(2,9) = 1$$

$$1 \equiv x(2) + y(9) \pmod 9$$

$$1 \equiv 5 \cdot 2 + (-1)(9)$$

$$\equiv 10 + (-9)$$

$$\equiv 1$$

$$gcd(2, 9)^{1} = (x \cdot 2 + y \cdot 9)^{0} \mod 9$$

$$1 = x \cdot 2 \mod 9$$

x is inverse of 2 on $\mathbb{Z}_9$

$\{0, 1, 2, 3, \cdots, 8\}$

$x = 5$

Extended Euclidean Algorithm (n, m)

Input: $n, m \in \mathbb{Z}^{\geq 0}$ and $m \geq n$

OAnct: $x, y, r \in \mathbb{Z}$ where $\gcd(n, m) = r = xn + ym$

1. if $m \bmod n = 0$ then
2. return $1, 0, n$ // $(1) \cdot n + (0) \cdot m = n = \gcd(n, m)$ as $n \mid m$
3. else:
4. $x, y, r = \text{extended Euclidean Algorithm}(m \bmod n, n)$
5. return $y - \lfloor \frac{m}{n} \rfloor \cdot x, x, r$

if p is prime then every nonzero $a \in \mathbb{Z}_p$ has a multiplicative inverse

- Pick up next class w/ proof of Euler's and a better trace of the algo.