Modular Arithmetic

"Clock math", numbers limited to predefined range

$x \equiv r \bmod m \Rightarrow x = mq + r,\ 0 \le r \le m-1$, q in integer

m also divides $(x-y)$ iff

mod m universe produces m disjoint sets

Theorem: If $a \equiv c \bmod m$ and $b \equiv d \bmod m$, then $a+b = c+d \bmod m$ and $a \cdot b = c \cdot d \bmod m$.

Proof: $c = mk + a$, $d = mj + b$

$c + d = a + b + m(k+j)$ - addition

$c \cdot d = ab + amj + bmk + m^2jk$

$c \cdot d = ab + m(aj + bk + mjk)$

Exponentiation (modular)

algorithm mod-exp(x, y, m)
 if $y = 0$ then return (1)
 else
  $z =$ mod-exp$(x, y \text{ div } 2, m)$
  if $y \bmod 2 = 0$ return $(z * z \bmod m)$
  else return $(x * z * z \bmod m)$

$O(n)$ time in the number of bits

Alternate: $x^k \bmod m$ where $k = k_r 2^r + \dots + k_0 2^0$

$x^k = \prod_{k_i=1} x^{k_i 2^i}$

Inverses

Division is equivalent to multiplication by inverse

An inverse for x only exists if $\gcd(x, m) = 1$, in mod m

Theorem: Let m, x be positive integers such that $\gcd(m, x) = 1$. Then x has a multiplicative inverse modulo m, and it is unique (modulo m).

Proof: claim that in seq $0, x, 2x, \dots, (m-1)x$ that all are distinct modulo m, so only one $= 1 \bmod m$. Suppose we have $ax \equiv bx \bmod m$ for $0 \le b \le a \le m$

$(a-b)x \equiv 0 \bmod m = km$, meaning either:

~~m~~ divisible by x (no because they are coprime) or ~~m~~ divisible by $(a-b)$ - no bc it is smaller than m

Computing Multiplicative Inverses

Related to finding $d = \gcd(x, y) = ax + by$

If $1 = \gcd(x, m) = am + bx$, b is x^{-1}

Theorem: Let $x \ge y$ and q, r be natural numbers such that $x = yq + r$ and $r < y$. Then $\gcd(x, y) = \gcd(r, y)$

Proof: Given $\gcd(x, y) = d$, $x = dk$, $y = dm$

$r = x - yq = dk - dmq = d(k - mq)$

algorithm gcd(x, y)
 if $y = 0$ then return (x)
 else return (gcd$(y, x \bmod y)$)

Theorem: This algorithm correctly computes gcd

Proof: Strong induction on y, starting from 0.

Base case: $\gcd(x, 0) = x$, correct in this case

Inductive Hypothesis: Assume that this works for all $z < y$, $\gcd(x, z)$ computes the correct result.

Inductive Step: Given some $\gcd(x, y)$, we know by the previous proof that $\gcd(x, y) = \gcd(y, x \bmod y)$, which works because $x \bmod y < y$.

Runtime: Two cases - $y \le \frac{x}{2}$, so after two calls, even smaller than $\frac{x}{2}$

$x \ge y > \frac{x}{2}$, y will be smaller than $\frac{x}{2}$ in two calls — $O(n)$, $2n$ max

Extended Euclid's Algorithm

algorithm extended-gcd(x, y)
 if $y = 0$ then return $(x, 1, 0)$
 else
  $(d, a, b) =$ extended-gcd$(y, x \bmod y)$
  return $((d, b, a - (x \text{ div } y) * b))$

First, we know $d = ay + b(x \bmod y)$ is valid.

$d = ay + b(x \bmod y)$

$= ay + b(x - \lfloor x/y \rfloor y)$

$= bx + (a - \lfloor x/y \rfloor b)y$

Linear time algorithm with constant factors $\rightarrow$ mult. inverse efficient!

Chinese Remainder Theorem

Given $x \equiv a \bmod p$, $x \equiv b \bmod q$ and values p, q coprime:

$x = a(q)(q^{-1} \bmod p) + b(p)(p^{-1} \bmod q)$

Suppose $z \equiv a \bmod p$, $z \equiv b \bmod q$, we will claim that $z \equiv x \bmod pq$.

$(z - x) \equiv 0 \bmod p$, $(z - x) \equiv 0 \bmod q \Rightarrow z - x \equiv 0 \bmod pq$

General: Suppose we have $m_1, m_2, \dots, m_n$ all rel prime.

$x \equiv a_1 \bmod m_1 \dots x \equiv a_i \bmod_i \dots x \equiv a_n \bmod m_n$

$x = \sum_{i=1}^{n} a_i \cdot b_i b_i'$, Let $b_i = \prod_{j \ne i} m_j$

$b_i' = b_i^{-1} \bmod m_i$

Public Key Cryptography

Bijections

A function for which every $b \in B$ has a unique pre-image $a \in A$ such that $f(a) = b$

so: f is onto: every $b \in B$ has preimage $a \in A$

f is one-to-one: for all $a, a' \in A$, if $f(a) = f(a')$, then $a = a'$.

Lemma: For a finite set A, $f: A \to A$ is a bijection if there is an inverse function $g: A \to A$ such that $\forall x: g(f(x)) = x$.

Proof: If $f(x) = f(x')$, then $x = g(f(x)) = g(f(x')) = x'$ so f must be one-to-one. Since f is one-to-one, there must be $|A|$ elements in the range of f, so f must also be onto.

RSA

$N = pq$ (p and q are large primes)

$E(x) \equiv x^e \bmod N$ (e prime to $(p-1)(q-1)$)

$E: \{0, \dots, N-1\} \to \{0, \dots, N-1\}$

$D(x) \equiv x^d \bmod N$ (d inverse of e mod $(p-1)(q-1)$)

Fermat's Little Theorem

For any prime p and any $a \in \{1, 2, \dots, p-1\}$, we have that $a^{p-1} = 1 \bmod p$.

Proof: Define $f: S \to S$ such that $f(x) \equiv ax \bmod p$

Any $a \cdot i \bmod p$ must be distinct since if $a \cdot i \equiv a \cdot j \bmod p$, then $i \equiv j \bmod p$.

Now, since f is a bijection, we can take the product of all: $(p-1)! = a^{p-1}(p-1)! \bmod p$

Divide to obtain $1 = a^{p-1} \bmod p$

Euler's Totient Theorem

Given $\gcd(a, m) = 1$, $a^{\phi(m)} \equiv 1 \bmod m$,

$\phi(m)$ - number of #'s coprime with m

Theorem: Knowing E and D, we have $D(E(x)) = x \bmod N$ for every possible $x \in \{0, 1, \dots, N-1\}$

Proof: Show that $(x^e)^d = x \bmod N$ for $x \in \{0, 1, \dots, N-1\}$

$x^{ed} - x = 0 \bmod N$ to prove the above

$x(x^{ed-1} - 1) = 0 = x(\cancel{x}^{k(p-1)(q-1)} - 1)$

Cases: 1. x a multiple of p, so we're done.

2. x not mult of p, but $(x^{p-1}) = 1$ by Fermat, and similarly with q. And so div by N.

RSA built on the following assumption:

Given N, e and $y = x^e \bmod N$, there is no efficient algorithm for determining x.

This is hard because:

The factoring problem $\rightarrow$ regards to N, is NP-complete

Trying all x requires $O(N)$, hard for large N

Computing $(p-1)(q-1)$ essentially like factoring N

Bob just needs to find p and q to use and him + Alice must compute modular exp, which is efficient.

Polynomials

Property 1: A non-zero polynomial of degree d has at most d roots.

Property 2: Given $d+1$ pairs $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ with all the x_i distinct, there is a unique polynomial $p(x)$ of degree (at most) d such that $p(x_i) = y_i$ for $1 \le i \le d+1$.

1 $\rightarrow$ 2: Need to show at most one, at least one

Using Lagrange Interpolation, we know at least one.

Consider $P(x)$ and $Q(x)$ match at d points:

Case 1: $P(x) - Q(x) = 0$ unique!

Case 2: $P(x) - Q(x) \ne 0$, $r(x)$ must have $d+1$ roots which is a contradiction.

Lagrange Interpolation

Given x_i, y_i pairs construct $p(x)$

$$P(x) = \sum_{j=1}^{d+1} y_j \Delta_j(x_i) \text{ where}$$

$$\Delta_j(x_i) = \frac{\prod_{i \ne j} (x - x_i)}{\prod_{i \ne j} (x_j - x_i)} \quad \begin{cases} 0 & \text{if } i \ne j \\ 1 & \text{if } i = j \end{cases}$$

Polynomial Division

Dividing $p(x)$ by $q(x)$: $p(x) = q'(x)q(x) + r(x)$

degree of $r(x)$ smaller than $p(x), q(x)$

Claim 1: If a is a root of a polynomial $p(x)$ with degree d, then $p(x) = (x-a)q(x)$ for a polynomial $q(x)$ w/ deg $d-1$.

Claim 2: A polynomial with distinct roots $a_1, \dots, a_d$ can be written as $p(x) = c(x-a_1)\dots(x-a_d)$

Proof of Claim 1:

Dividing $p(x)$ by $(x-a)$ yields the relation $P(x) = (x-a)q(x) + r(x)$. Deg of $r(x)$ smaller than $(x-a)$, so $\rightarrow c$. Substituting in a, we get $P(a) = c$, but a is a root, so $c = 0$. Thus, $p(x) = (x-a)q(x)$.

Proof of Claim 2:

Base Case: A polynomial of degree 1 can be written in the form $p(x) = c(x - a_1)$. By claim 1, $q(x) \Rightarrow \deg = 0$, constant.

Inductive Hypothesis: Suppose that a polynomial of degree $d-1$ can be written in the form $p(x) = c(x - a_1)\dots(x - a_{d-1})$.

Inductive Step: Let $p(x)$ be polynomial with distinct roots $a_1, \dots, a_d$. $p(x) = (x - a_d)q(x)$ by claim 1. We know $0 = p(a_i) = (a_i - a_d)q(a_i)$ for all $i \ne d$ and $a_i \ne a_d$ so $q(a_i)$ must be equal to 0. Then $q(x)$ can be written as $c(x - a_1)\dots(x - a_{d-1})$ b/c $\deg = d-1$. Substitute to obtain $p(x) = c(x - a_1)\cdots(x - a_d)$.

Using claim 2, we can show that $a \ne a_i$ for $i = 1, \dots, d$ cannot be a root of $p(x)$, so it can only have at most d roots.

Giulio Zhou 23623211

Finite Fields

A field is defined as a set of "numbers"
Operations add and multiply should exist,
subtraction and division are just inverses
Add/mult. commute and distribute
0 - additive identity, 1 - multiplicative identity
smallest field must have ≥ 2 values, additive
and multiplicative inverses cannot be the same
Fields must be prime, or power of prime for GF

Counting Polynomials

Working in GF(m), we find that there exists
1 polynomial given d+1 points, m polynomials given d points,
... m^{d+1} polynomials given 0 points.
Mapping from $Z_p \to Z_p$ yields p^p possible functions.
$\Rightarrow$ p polynomials of deg 0, p^2 deg. 1 $\to$ p^{k+1} of deg. k

Secret Sharing

We want to take a secret and split it into
k shares such that all k people must come
together to reveal the secret, otherwise you
will learn nothing.
Give people evaluations of a polynomial at different
points, different number must come together dep.
on the degree.
Can use either value encoding or coefficient encoding.