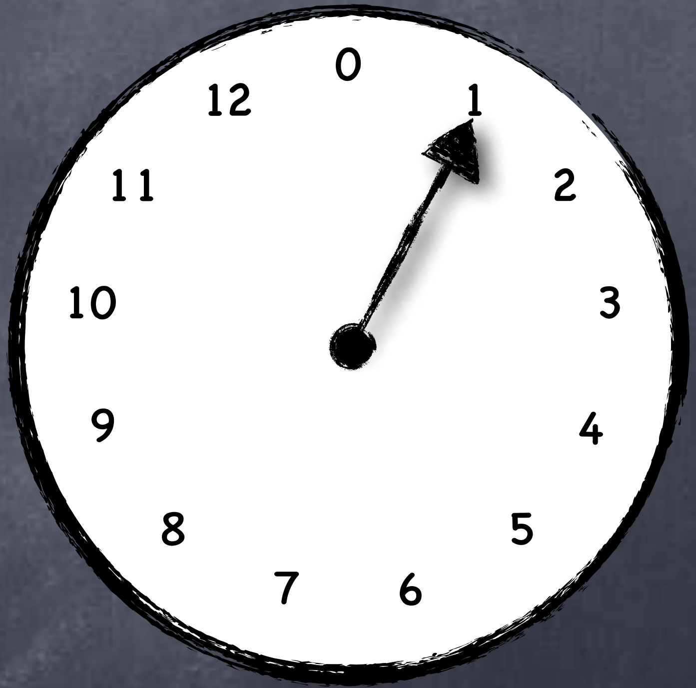
Numb3rs

$\mathbb{Z}_m^*$ and its Structure:

Euler's φ and Discrete Log



$\mathbb{Z}_m^*$

- $\mathbb{Z}_m^*$ denotes the set of elements in $\mathbb{Z}_m$ which have multiplicative inverses
  - $\mathbb{Z}_m^* = \{ a \in \mathbb{Z}_m \mid \exists b \;\; ab = 1 \}$
  - Such an element is called a unit of $\mathbb{Z}_m$
  - e.g., $\mathbb{Z}_2^* = \{1\}$, $\mathbb{Z}_3^* = \{1,2\}$, $\mathbb{Z}_4^* = \{1,3\}$
- Recall: a^{-1} exists in $\mathbb{Z}_m$ iff $\gcd(a,m) = 1$
  - $\mathbb{Z}_m^* = \{ [a]_m \mid a \in \mathbb{Z}, \gcd(a,m) = 1 \}$

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_m^*$

- **How many units are there in $\mathbb{Z}_m$?**
- When m is prime? m-1 (all except 0)
- When $m = p^2$, where p is prime?
  - A number has a common factor with p^2 iff it is a multiple of p (i.e., $\in \{0,p,2p,\ldots,(p-1)p\}$)
  - i.e., $p^2 - p$ units
- When $m = p^k$, where p is prime?

  $p^k - p^{k-1} = m(1-1/p)$ units
- When $m = p_1^{d_1} \cdot \ldots \cdot p_n^{d_n}$ where p_i are primes?
  - By **CRT**, units have the form $(r_1,\ldots,r_n)$, where each r_i is invertible modulo $p_i^{d_i}$
  - $\Pi_i \; p_i^{d_i} (1-1/p_i) = m(1-1/p_1) \cdot \ldots \cdot (1-1/p_n)$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Euler's Totient Function

- How many units are there in $\mathbb{Z}_m$?
  - $\phi(m) = m(1-1/p_1)\cdot \ldots \cdot(1-1/p_n)$ where $p_1,\ldots,p_n$ are the prime factors of m
- i.e., $|\mathbb{Z}_m^*| = \phi(m)$
- Euler's ϕ function (a.k.a. Euler's totient function)
  - e.g. $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 4(1-1/2) = 2$
- Exercise: If $\gcd(a,b) = 1$, then $\phi(ab) = \phi(a)\cdot\phi(b)$

Such a function is called a multiplicative function

$\mathbb{Z}_m^*$

- Examples
  - m=6
    - $\phi(6) = (2-1)(3-1) = 2$
    - $\mathbb{Z}_6^* = \{1, 5\}$
  - m=10
    - $\phi(10) = (2-1)(5-1) = 4$
    - $\mathbb{Z}_{10}^* = \{1,3,7,9\}$

×	0	2	3	4	5	1
0	0	0	0	0	0	0
2	0	4	0	2	4	2
3	0	0	3	0	3	3
4	0	2	0	4	2	4
5	0	4	3	2	1	5
1	0	2	3	4	5	1

×	0	2	4	6	8	5	1	3	7	9
0	0	0	0	0	0	0	0	0	0	0
2	0	4	8	2	6	0	2	6	4	8
4	0	8	6	4	2	0	4	2	8	6
6	0	2	4	6	8	0	6	8	2	4
8	0	6	2	8	4	0	8	4	6	2
5	0	0	0	0	0	5	5	5	5	5
1	0	2	4	6	8	5	1	3	7	9
3	0	6	2	8	4	5	3	9	1	7
7	0	4	8	2	6	5	7	1	9	3
9	0	8	6	4	2	5	9	7	3	1

$\mathbb{Z}_m^*$

×	0	2	3	4	5	1
0	0	0	0	0	0	0
2	0	4	0	2	4	2
3	0	0	3	0	3	3
4	0	2	0	4	2	4
5	0	4	3	2	1	5
1	0	2	3	4	5	1

- If $a \in \mathbb{Z}_m \setminus \mathbb{Z}_m^*$ then, in $\mathbb{Z}_m$, $\exists u \neq 0$ s.t. $au=0$
  - a not unit $\Rightarrow$ gcd(a,m)>1
    $\Rightarrow$ in $\mathbb{Z}$, $u = m/\gcd(a,m)$, $0 < u < m$
    $\Rightarrow$ in $\mathbb{Z}_m$, $\exists u \neq 0$ s.t. $au = 0$
- Converse also holds: If $a \in \mathbb{Z}_m^*$ then, in $\mathbb{Z}_m$, $\forall u \neq 0$, $au \neq 0$
  - Suppose $\exists a \in \mathbb{Z}_m^*$ and $\exists u \neq 0$ s.t. $au=0$.
    Then $u = a^{-1}au = 0$!
- $a \in \mathbb{Z}_m^* \rightarrow a^{-1} \in \mathbb{Z}_m^*$
- $a,b \in \mathbb{Z}_m^* \rightarrow ab \in \mathbb{Z}_m^*$, because $(ab)(b^{-1}a^{-1}) = 1$

$\mathbb{Z}_m^*$

- $a \in \mathbb{Z}_m^* \rightarrow a^{-1} \in \mathbb{Z}_m^*$
- $a,b \in \mathbb{Z}_m^* \rightarrow ab \in \mathbb{Z}_m^*$, because $(ab)(b^{-1}a^{-1}) = 1$
- For each $a \in \mathbb{Z}_m^*$, $a \cdot \mathbb{Z}_m^* \triangleq \{ ab \mid b \in \mathbb{Z}_m^* \} = \mathbb{Z}_m^*$
  - We have $a \cdot \mathbb{Z}_m^* \subseteq \mathbb{Z}_m^*$,
    since $a,b \in \mathbb{Z}_m^* \rightarrow ab \in \mathbb{Z}_m^*$,
  - Similarly, $a^{-1} \cdot \mathbb{Z}_m^* \subseteq \mathbb{Z}_m^*$
    - $\Rightarrow \forall x \in \mathbb{Z}_m^*$, $a^{-1} \cdot x \in \mathbb{Z}_m^*$
    - $\Rightarrow \forall x \in \mathbb{Z}_m^*$, $x \in a \cdot \mathbb{Z}_m^*$
    - $\Rightarrow \mathbb{Z}_m^* \subseteq a \cdot \mathbb{Z}_m^*$
  - So $a \cdot \mathbb{Z}_m^* = \mathbb{Z}_m^*$

×	0	2	3	4	5	1
0	0	0	0	0	0	0
2	0	4	0	2	4	2
3	0	0	3	0	3	3
4	0	2	0	4	2	4
5	0	4	3	2	1	5
1	0	2	3	4	5	1

×	0	2	4	6	8	5	1	3	7	9
0	0	0	0	0	0	0	0	0	0	0
2	0	4	8	2	6	0	2	6	4	8
4	0	8	6	4	2	0	4	2	8	6
6	0	2	4	6	8	0	6	8	2	4
8	0	6	2	8	4	0	8	4	6	2
5	0	0	0	0	0	5	5	5	5	5
1	0	2	4	6	8	5	1	3	7	9
3	0	6	2	8	4	5	3	9	1	7
7	0	4	8	2	6	5	7	1	9	3
9	0	8	6	4	2	5	9	7	3	1

Modular Exponentiation

- Exponentiation in $\mathbb{Z}_m$ defined using repeated multiplication
  - For $a \in \mathbb{Z}_m$ and $d \in \mathbb{Z}^+$, define $a^d \triangleq \underbrace{a \times_{(m)} \dots \times_{(m)} a}_{d \text{ times}}$

    Important: The exponent is not modulo m
  - Recursive definition: $a^1 = a$, and $\forall d > 1$, $a^d = a \times_{(m)} a^{d-1}$
  - Alternately, for $a \in \mathbb{Z}$, define $([a]_m)^d \triangleq [a^d]_m$
- In $\mathbb{Z}_m^*$, can extend the definition to $d \in \mathbb{Z}$
  - $a^0=1$ and $a^{-d} = (a^{-1})^d$
- Note: $a^e a^d = a^{e+d}$ and $(a^e)^d = a^{ed}$ where operations in the exponent are in $\mathbb{Z}$

Euler's Totient Theorem

- $\forall a \in \mathbb{Z}_m^*, \quad a^{\phi(m)} \equiv 1 \pmod{m}$

In $\mathbb{Z}_m$, $\forall a \in \mathbb{Z}_m^*$, $a^{\phi(m)} = 1$

$a^{\phi(m)-1} = a^{-1}$

Not necessarily the smallest d such that $a^d = 1$

E.g., If $a = b^2$, then $a^{\phi(m)/2} = 1$

Exercise: If m>2, $\phi(m)$ is even

Proof: Fix any m>1 and $a \in \mathbb{Z}_m^*$.

Let $\mathbb{Z}_m^* = \{x_1,\ldots,x_n\}$ where $n = \phi(m)$.

Let $u = x_1 \ldots x_n$ and $w = (a \cdot x_1) \cdot \ldots \cdot (a \cdot x_n)$.

$\Rightarrow w = a^n \cdot u$.

But also, $w = \prod_{x \in a\mathbb{Z}_m^*} x = \prod_{x \in \mathbb{Z}_m^*} x = u$ (because $a \cdot \mathbb{Z}_m^* = \mathbb{Z}_m^*$)

$\Rightarrow u = a^n \cdot u$, where $u \in \mathbb{Z}_m^*$

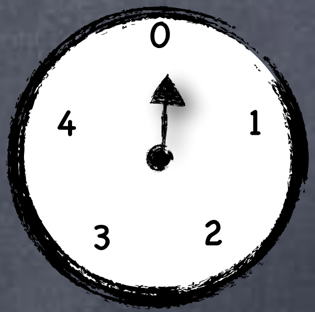
$\Rightarrow 1 = a^n$ by multiplying both sides with u^{-1} □

- Special case, when m is a prime
  - Fermat's Little Theorem:

    For prime p and a not a multiple of p, $a^{p-1} \equiv 1 \pmod{p}$

Cyclic Structure of $\mathbb{Z}_p^*$

- The multiplicative clock!
  - Clock's hand starts at 1 (not 0) and multiplies the current position by some g≠0 to get to the next one
  - $1, g, g^2, \ldots, g^{p-2}, g^{p-1}=1$
    - If g=1, it never moves
    - If g=-1, it keeps switching positions between 1 and -1
    - It never reaches 0
  - A g which will make the hand go everywhere (except 0)?



- Important Fact (won't prove): If p is a prime, then there is a g s.t. every element in $\mathbb{Z}_p^*$ is of the form g^k
  - e.g., p=5, g=2: 1, 2, 4, 3.
    p=7, g=3: 1, 3, 2, 6, 4, 5.

True for some other values also

Cyclic Structure of $\mathbb{Z}_p^*$

- Important Fact (won't prove): If p prime, then $\exists g \in \mathbb{Z}_p^* \ \ \forall x \in \mathbb{Z}_p^* \ \ \exists k \in [0,p-1) \ \ x = g^k$
  - Such a g is called a "generator of $\mathbb{Z}_p^*$"

a.k.a. a primitive root of p

- There is a $\mathbb{Z}_{p-1}$ hiding in $\mathbb{Z}_p^*$!
  - Can order the numbers in $\mathbb{Z}_p^*$ as $1, g, g^2, \ldots$ (for some g)
    - $g^k \in \mathbb{Z}_p^*$ is labelled by $k \in \mathbb{Z}_{p-1}$ in this ordering. Then, multiplication in $\mathbb{Z}_p^*$ becomes addition of the labels in $\mathbb{Z}_{p-1}$!
  - Discrete Log: Given x and a generator g of $\mathbb{Z}_p^*$, $\exists k$ s.t. $g^k = x$.
  - Can "efficiently" go from k to g^k, for any $k \in \mathbb{Z}_{p-1}$, but apparently not easy to go backwards

A candidate for a "one-way function"