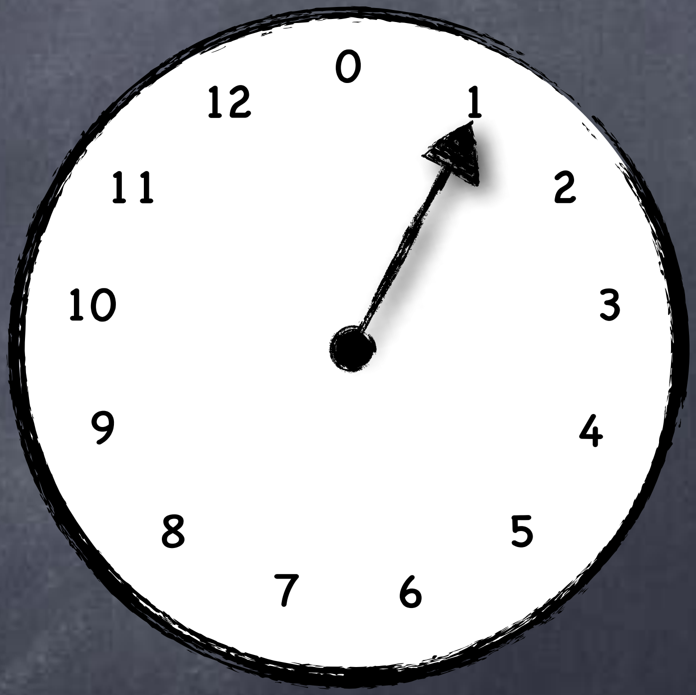
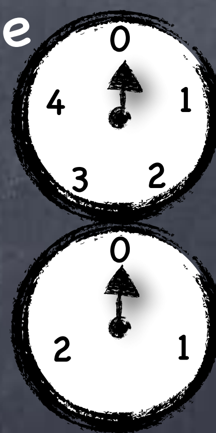
Numb3rs

Modular Exponentiation



Story So Far

- Quotient and Remainder, GCD, Euclid's algorithm, $L(a,b) \triangleq \{ au + bv \mid u,v \in \mathbb{Z} \} = \{ n \cdot gcd(a,b) \mid n \in \mathbb{Z} \}$
- Primes, Fundamental Theorem of Arithmetic
- Modular Arithmetic ($\mathbb{Z}_m$) : Addition, Multiplication
- Chinese Remainder Theorem : for $m = a_1 \cdot \ldots \cdot a_n$ where a_i's coprime
  - CRT representation in $\mathbb{Z}_m$: $x \mapsto (r_1,\ldots,r_n)$ where $r_i = rem(x,a_i)$
  - $(r_1,\ldots,r_n) \mapsto x$ s.t. $\forall i,\ x \equiv r_i \pmod{a_i}$ (computable using EEA)
    - Can tell time in a big clock from time in n small clocks



- Multiplicative Inverse and $\mathbb{Z}_m^*$:
  - $a \in \mathbb{Z}_m^*$: $gcd(a,m)=1 \leftrightarrow \exists u,v\ au+mv=1 \leftrightarrow \exists u\ [a]_m \times_m [u]_m = [1]_m$
  - $\mathbb{Z}_m^*$ closed under multiplication and inversion
- Euler's Totient function : $|\mathbb{Z}_m^*| = \phi(m) = m(1-1/p_1)\ldots(1-1/p_n)$, where $a_i = p_i^{d_i}$
  - Euler's Totient theorem: $\forall x \in \mathbb{Z}_m^*,\ x^{\phi(m)} = 1$
- Generators of $\mathbb{Z}_p^*$ for prime p : $\mathbb{Z}_p^* = \{1,g,g^2,\ldots,g^{p-2}\}$

Modular Exponentiation

Recall

- 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 $\mathbb{Z}$

  Can be $\mathbb{Z}_{\phi(m)}$

Modular Exponentiation

Using Euler's Totient Function

- $\forall a \in \mathbb{Z}_m^*$, if $c \equiv d \pmod{\phi(m)}$ then $a^c = a^d$
  - $a^{\phi(m)} = 1 \Rightarrow$ if $\phi(m)|x$, then $a^x = (a^{\phi(m)})^q = 1$ (where $x=\phi(m)q$, $q \in \mathbb{Z}$)

    $\Rightarrow$ if $\phi(m) \mid c-d$, then $a^{c-d} = 1$

    $\Rightarrow$ if $c \equiv d \pmod{\phi(m)}$, then $a^c = a^d$
- i.e., in $\mathbb{Z}_m^*$, a^d can be defined for $a \in \mathbb{Z}_m^*$ and $d \in \mathbb{Z}_{\phi(m)}$
- Finding the e^{th}-root: given x^e find x
  - Find d s.t. $ed \equiv 1 \pmod{\phi(m)}$. Then, $(x^e)^d = x$.
  - Only if $\gcd(e,\phi(m)) = 1$

$a^{1/e}$ is a value b s.t. $b^e = a$. May or may not exist/be unique

Modular Exponentiation

Using Euler's Totient Function

- 9^{10} in $\mathbb{Z}_{13}^*$?
  - $\phi(13) = 12$
  - $10 = -2$ in $\mathbb{Z}_{12} \Rightarrow x^{10} = x^{-2} = (x^{-1})^2$ in $\mathbb{Z}_{13}^*$
  - Now, in $\mathbb{Z}_{13}^*$, $9^{-1} = ?$ $9 \cdot 3 + 13 \cdot (-2) = 1$
    - $9^{-1} = 3 \Rightarrow 9^{10} = 9^{-2} = 3^2 = 9$ in $\mathbb{Z}_{13}^*$
- Note: $3^3 = 1$ in $\mathbb{Z}_{13}^*$. In fact $x^3 = 1$ for $x \in \{1,3,9\}$. So, $x^{1/3}$ not well-defined in $\mathbb{Z}_{13}^*$.
- $x^{1/5}$ in $\mathbb{Z}_{13}^*$?
  - gcd(5,12) = 1. So uniquely determined.
  - $5^{-1} = 5$ in $\mathbb{Z}_{12}^* \Rightarrow x^{1/5} = x^5$ in $\mathbb{Z}_{13}^*$

Modular Exponentiation
Using Euler's Totient Function

- Suppose $m = pq$, with $\gcd(p,q)=1$ and $a \mapsto (x,y)$ by CRT
  - If $x \in \mathbb{Z}_p^*$, $y \in \mathbb{Z}_q^*$, then $a^{\phi(m)} = a^{\phi(p)\cdot\phi(q)} \mapsto (x^{\phi(p)\cdot\phi(q)}, y^{\phi(p)\cdot\phi(q)}) = (1,1)$
    - $a^{\phi(m)} = 1$ and $a^{\phi(m)+1} = a$
  - If $x \in \mathbb{Z}_p^*$, $y = 0$, then $a^{\phi(m)} = a^{\phi(p)\cdot\phi(q)} \mapsto (x^{\phi(p)\cdot\phi(q)}, 0) = (1,0)$
    - $a^{\phi(m)} \neq 1$ but $a^{\phi(m)+1} = a$
  - Similarly when $x=0$, $y \in \mathbb{Z}_q^*$.
  - When p,q prime these (and a=0) cover all the cases
- If m is a product of distinct primes, then $\forall a \in \mathbb{Z}_m$:
  - $a^{k\cdot\phi(m)+1} = a$
  - If $\gcd(e,\phi(m)) = 1$, $\exists d$ s.t. $a^{ed} = a$ ($d=e^{-1}$ in $\mathbb{Z}_{\phi(m)}$)

Modular Exponentiation
Using Euler's Totient Function

- $15^{1/3}$ in $\mathbb{Z}_{33}$?
  - Is there a 1/3 in $\mathbb{Z}_{\phi(33)}$?
    - Yes: $\phi(33) = \phi(3)\cdot\phi(11) = 20$. $\gcd(3,20) = 1$
    - From the Extended Euclidean Algorithm: $3\cdot7 + 20\cdot(-1) = 1$
    - $3^{-1} = 7$ in $\mathbb{Z}^*_{20}$
  - $15 \notin \mathbb{Z}^*_{33}$ but 3,11 prime $\Rightarrow 15^{1/3} = 15^7$
    - By repeated squaring:
      - $15^2 = 27$
      - $15^4 = 27^2 = (-6)^2 = 3$
      - $15^7 = 15^4 \cdot 15^2 \cdot 15$
        $= 3\cdot27\cdot15 = 27$
    - By CRT: $\mathbb{Z}_{33} \cong \mathbb{Z}_3 \times \mathbb{Z}_{11}$
      - $15 \mapsto (0,4)$
      - $15^7 \mapsto (0,4^7) = (0,5)$
      - $15^7 = 27$

In $\mathbb{Z}^*_{11}$

$4^7 = 4^{-3} = 3^3 = 5$

Modular Exponentiation
Using Euler's Totient Function

- $15^{1/2}$ in $\mathbb{Z}_{33}$?
  - Is there a 1/2 in $\mathbb{Z}_{\phi(33)}$?
    - No! $\gcd(2,\phi(33)) = 2$
  - But $9^2 = [81]_{33} = 15$

- By CRT: $\mathbb{Z}_{33} \cong \mathbb{Z}_3 \times \mathbb{Z}_{11}$
  - $15 \mapsto (0,4)$
  - $15^{1/2} \mapsto (0,4^{1/2}) = (0,\pm 2)$
  - $15^{1/2} = 24$ or 9

Squares and Square-Roots

- Squaring is not an invertible operation in $\mathbb{Z}_m$, for m>2
  - gcd(2,ϕ(m)) = 2 for all m>2 [Why?]
  - $a^2 = (-a)^2$
  - Every element has one square, but many elements have at least two square roots
    - $\Rightarrow$ Many elements do not have any square roots!
- Quadratic Residues: Elements in $\mathbb{Z}_m^*$ of the form x^2

Squares in $\mathbb{Z}_p^*$

- Quadratic Residues in $\mathbb{Z}_p^*$, for prime p:

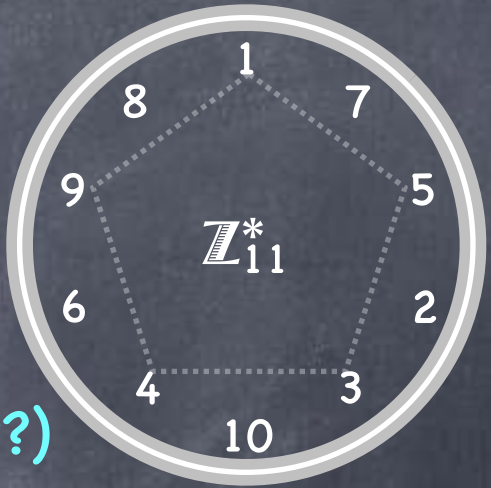
  "even powers" $1, g^2, g^4, \ldots, g^{p-3}$

- Exactly half of $\mathbb{Z}_p^*$ are quadratic residues (p>2)
  - Will call them $\mathbb{QR}_p^*$
- Given (z,p) can we "efficiently" check if $z \in \mathbb{QR}_p^*$?
  - Bad idea: Compute discrete log (w.r.t. some generator g) and check if it is even
  - Good idea: Just check if $z^{(p-1)/2} = 1$.

    If $z = g^{2k}$, $z^{(p-1)/2} = g^{k(p-1)} = 1$.

    If $z = g^{2k+1}$, $z^{(p-1)/2} = g^{k(p-1) + (p-1)/2} = g^{(p-1)/2} \neq 1$ (why?)

Square-roots in $\mathbb{Z}_p^*$



- What are all the square-roots of x^2 in $\mathbb{Z}_p^*$?
- Let's find all the square roots of 1
  - $x^2=1 \Leftrightarrow (x+1)(x-1) = 0 \Leftrightarrow (x+1)=0$ or $(x-1)=0$ (why?)

    $\Leftrightarrow x=1$ or $x=-1$
  - $\sqrt{1} = \pm 1$
  - $g^{(p-1)/2} = -1$, because $(g^{(p-1)/2})^2 = 1$ and $g^{(p-1)/2} \neq 1$
  - More generally $\sqrt{(a^2)} = \pm a$ (i.e., only a and $-1 \cdot a$)

In $\mathbb{Z}_p^*$, $1^{1/e}$ has exactly gcd(e,p-1) values (Exercise)

In $\mathbb{Z}_p^*$, $(a^e)^{1/e}$ has exactly gcd(e,p-1) values (Exercise)

Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on p!
  - e.g. $\mathbb{QR}_{13}^* = \{\pm 1, \pm 3, \pm 4\}$
    - 1,3,-4 have 2 square-roots each. But -1,-3,4 have none within $\mathbb{QR}_{13}^*$
    - Since $-1 \in \mathbb{QR}_{13}^*$, $x \in \mathbb{QR}_{13}^* \Rightarrow -x \in \mathbb{QR}_{13}^*$
    - $-1 \in \mathbb{QR}_p^*$ iff (p-1)/2 even
- If (p-1)/2 odd, exactly one of $\pm x$ in $\mathbb{QR}_p^*$ (for all x)
  - Then, squaring is a permutation in $\mathbb{QR}_p^*$

Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- If $(p-1)/2$ odd, squaring is a permutation in $\mathbb{QR}_p^*$
- Easy to compute both ways
  - In fact $\sqrt{z} = z^{(p+1)/4} \in \mathbb{QR}_p^*$ (because $(p+1)/2$ even)

Modular Exponentiation

Summary

- $\forall a \in \mathbb{Z}_m^*, \ a^{\phi(m)} = 1$
  - In $\mathbb{Z}_m^*$, a^d can be defined for $a \in \mathbb{Z}_m^*$ and $d \in \mathbb{Z}_{\phi(m)}$
  - In $\mathbb{Z}_m^*$, if $\gcd(e,\phi(m)) = 1$, $\exists d$ s.t. $a^{1/e} = a^d$ $\quad (d=e^{-1}$ in $\mathbb{Z}_{\phi(m)}^*)$
- $\forall a \in \mathbb{Z}_m, \ a^{\phi(m)+1} = a$, provided m is a product of distinct primes
  - But $a^{\phi(m)}$ need not be 1
  - In $\mathbb{Z}_m$, if $\gcd(e,\phi(m)) = 1$, $\exists d$ s.t. $a^{1/e} = a^d$ $\quad (d=e^{-1}$ in $\mathbb{Z}_{\phi(m)}^*)$
- $\forall a \in \mathbb{Z}_p^*, \sqrt{(a^2)} = \pm a$, provided p is a prime
- $\forall a \in \mathbb{QR}_p^*, \sqrt{(a^2)} = a$, provided p is a prime and $(p-1)/2$ odd