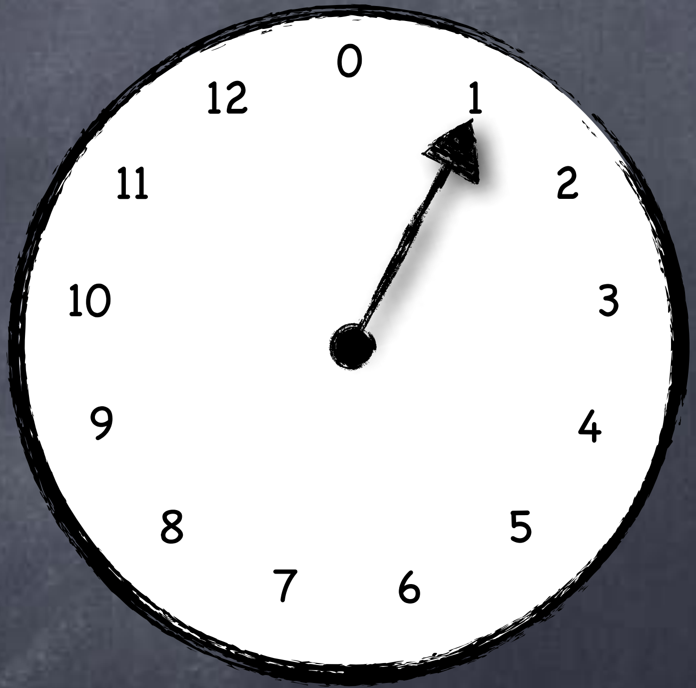
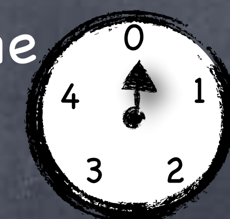
Numb3rs

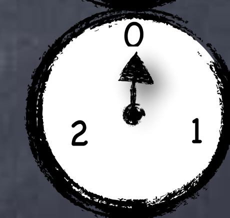
Lecture 7
Modular Arithmetic
And Some Cryptography



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 $r_i = \mathrm{rem}(x,a_i)$
  - $(r_1,\ldots,r_n) \mapsto x$ s.t. $\forall i,\ x \equiv r_i \pmod{a_i}$ (computable using EEA)
    - Can tell time in the 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** : $|\mathbb{Z}^*_m| = \varphi(m) = m(1-1/p_1)\ldots(1-1/p_n)$, where $a_i = p_i^{d_i}$
  - Euler's Totient theorem: $\forall x \in \mathbb{Z}^*_m,\ \ x^{\varphi(m)} = 1$

Euler's Totient Theorem

- $\forall a \in \mathbb{Z}_m^*, \quad a^{\varphi(m)} \equiv 1 \pmod{m}$
- Proof: Fix any m>1 and $a \in \mathbb{Z}_m^*$.

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

  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, $a^{p-1} \equiv 1 \pmod{p}$

Euler's Totient Theorem

- $\forall a \in \mathbb{Z}_m^*,\ \ a^{\varphi(m)} \equiv 1 \pmod{m}$
- In many cases (e.g., m prime), $\varphi(m)$ happens to be the smallest positive number for which this holds for all $a \in \mathbb{Z}_m^*$
  - But for specific a, we can have $a^d \equiv 1$ for $d < \varphi(m)$
  - e.g., if $a = b^2$ then $a^{\varphi(m)/2} \equiv 1 \pmod{m}$
    - Note: for all m>2, $\varphi(m)$ is even (why?)
- If $b \equiv c \pmod{\varphi(m)}$, then for all $a \in \mathbb{Z}_m^*$, $a^b \equiv a^c \pmod{m}$
  - e.g. $8^8 \equiv 3^0 \pmod{5}$ because $\varphi(5) = 4$

> Let $m = 2^d \cdot k$ for odd k.
> Then, $\varphi(m) = 2^{d-1}\varphi(k)$.
> If d>1, 2^{d-1} even. ✓
> If d=0 or 1, since $m \geq 3$, we have $k \geq 3$ and so has k an odd prime factor p
> $\Rightarrow (p-1) | \varphi(m) \Rightarrow \varphi(m)$ even

Modular Exponentiation

- For $a \in \mathbb{Z}_m$, we have already (implicitly) defined a^n in $\mathbb{Z}_m$ as $a \times_{(m)} a \times_{(m)} \dots \times_{(m)} a$ (n times)
  - Note: n is a non-negative integer here (with $a^0 \triangleq 1$, the multiplicative identity)
  - Familiar laws hold: For $b,c \in \mathbb{N}$, $a^b \cdot a^c = a^{b+c}$, and $(a^b)^c = a^{bc}$, operations in the exponent being in $\mathbb{N}$, others in $\mathbb{Z}_m$
- In $\mathbb{Z}_m^*$, can allow negative n too: for $n<0$, $a^n \triangleq (a^{-1})^n$, where a^{-1} is the multiplicative inverse of a.
  - For $a \in \mathbb{Z}_m^*$, and $b,c \in \mathbb{Z}$, $a^b \times_{(m)} a^c = a^{b+c}$ and $(a^b)^c = a^{bc}$, where again, the multiplication in the exponent is for integers
    - Also, if $\alpha a^b = \beta a^c$, then $\alpha = \beta\, a^{c-b}$, again the exponent in $\mathbb{N}$

Modular Exponentiation

And Euler's Totient Function

- **In $\mathbb{Z}_m^*$, $a^{\varphi(m)} = 1$**
  - $\Rightarrow a^b = 1$ if $\varphi(m)|b$
  - $\Rightarrow a^{b-c} = 1$ if $\varphi(m) \mid b-c$, i.e., if $b \equiv c \pmod{\varphi(m)}$
- So $x^y \equiv \text{rem}(x,m)^{\text{rem}(y,\varphi(m))} \pmod{m}$
  - Offers a way to speed up modular exponentiation, if we know $\varphi(m)$

Question

02:00

- $9^{10} \equiv x \pmod{13}$, where x = ?
  (Hint: $9^{-1} \equiv 3 \pmod{13}$)

A. 3
B. 6
C. 7
D. 9
E. 10

Cryptography from $\mathbb{Z}_m^*$

- A building block in "public key encryption" schemes is a "trapdoor one-way permutation"
  - Roughly, it is a bijection (permutation) that is easy to compute but hard to invert (one-way); but while defining the function you can setup a hidden mechanism (trapdoor) that makes it easy to invert too
- Will see two trapdoor one-way permutation candidates
  - Rabin's function: Based on square-roots
  - Rivest-Shamir-Adleman (RSA) function: Based on Euler's Totient theorem
- Both use a modulus of the form m=pq (p,q large primes)
  - Breaking would be easy if m prime. Also can be broken if factors of m known (via CRT).

A Word on Efficiency

- Very huge numbers have very short representation
- Take a 256 bit integer, 11...1 = $2^{256}-1$
- How long would it take for a computer to just count up to this number? Not even if it runs
  - at the frequency of molecular vibrations (10^{14} Hz)
  - for the entire estimated lifetime of the universe ($< 10^{18}$ s)
- What if you recruited every atom in the earth ($\approx 10^{50}$) to do the same?
  - OK, but still will get only to $10^{82} \approx 2^{272}$.
  - And even if you recruited every elementary particle in the known universe ($\approx 10^{80}$), only up to $10^{112} \approx 2^{372}$
  - The whole universe can't count up to a 400-bit number!

A Word on Efficiency

- The whole universe can't count up to a 400-bit number!
- But we can quickly add, multiply, divide and exponentiate much larger numbers
- Roughly, can "compute on" n-bit numbers in n or n^2 steps
  - But not if you try an algorithm based on counting through all the numbers! That takes 2^n steps. (e.g., exponentiation can use repeated squaring, but not naïve repeated multiplication)
- For some problems involving n-bit numbers we don't <u>know</u> algorithms that do much better than 2^n, $2^{n/2}$ etc.
  - We believe for some such problems no better algorithms <u>exist</u>!
  - (Currently, only a belief based on failure to discover better algorithms)
- Such hardness forms the basis of much of modern cryptography

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 is a prime, then $\exists g \in \mathbb{Z}_p^* \; \forall x \in \mathbb{Z}_p^* \; \exists k, \; 0 \leq k < p-1, \;\; x = g^k$
  - Such a g is called a "generator of $\mathbb{Z}_p^*$"
- There is a $\mathbb{Z}_{p-1}$ hiding in $\mathbb{Z}_p^*$!
  - Can order the numbers in $\mathbb{Z}_p^*$ as $1, g, g^2, ..$ (for some g)
  - Number g^k is relabelled as k. Multiplication in $\mathbb{Z}_p^*$ becomes addition in $\mathbb{Z}_{p-1}$!
  - Discrete Log: Given x and a generator g of $\mathbb{Z}_p^*$, a k s.t. $g^k = x$.
  - Can "efficiently" go from g 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"

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

- Quadratic Residues: Elements in $\mathbb{Z}_m^*$ of the form x^2
- In $\mathbb{Z}_p^*$, for prime p: "even numbers", 1, g^2, g^4, ..., 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?)

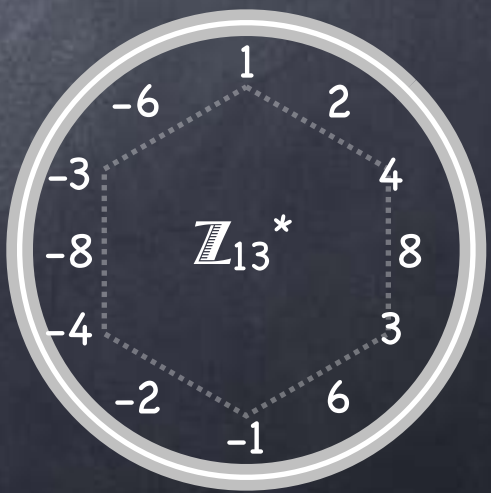
Square-roots in $\mathbb{Z}_p^*$

- 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 $-1 \cdot a$) [Why?]

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 $\mathbb{QR}_p^*$
- But easy to compute both ways
  - In fact $\sqrt{z} = z^{(p+1)/4} \in \mathbb{QR}_p^*$ (because (p+1)/2 even)
- Rabin function defined in $\mathbb{QR}_m^*$ and relies on keeping the factorisation of m=pq hidden

Rabin Function

- $Rabin_m(x) = x^2 \bmod m$
  - with m=pq (p,q random k-bit primes for, say k=1024)
  - Conjectured to be a one-way function
  - If p, q ≡3 (mod 4), then in $\mathbb{QR}^*_m$ this function
    - Is a permutation
    - Has a trapdoor for inverting, namely (p,q)
      - Exercise (Hint: CRT)
- Candidate Trapdoor One-Way Permutation

RSA Function

- $RSA_{m,e}(x) = x^e \bmod m$
  - where m=pq, and $\gcd(e,\varphi(m)) = 1$ (i.e., $e \in \mathbb{Z}^*_{\varphi(m)}$)
  - A commonly used version (for efficiency) fixes e=3
- $RSA_{m,e}$ is a permutation with a trapdoor (namely d)
  - In fact, there exists d s.t. $RSA_{m,d}$ is the inverse of $RSA_{m,e}$
    - $\gcd(e,\varphi(m)) = 1 \Rightarrow \exists d$ s.t. $ed=1 \pmod{\varphi(m)}$

      $\Rightarrow x^{ed} = x$ in $\mathbb{Z}^*_m$ (by Euler's Totient Theorem)
- We defined $RSA_{m,e}: \mathbb{Z}^*_m \to \mathbb{Z}^*_m$. An alternative uses $RSA_{m,e}: \mathbb{Z}_m \to \mathbb{Z}_m$
  - Does inversion still work? (Euler's Totient Theorem doesn't hold)
  - Yes, by CRT [Exercise]
- Conjectured to be a one-way function when m=pq generated randomly (p, q both large primes)